



# CYBER DEFENSE MAGAZINE

eMAGAZINE

AUGUST  
2024

## In This Edition

*Cybersecurity In Critical Infrastructure:  
Protecting Power Grids and Smart Grids*

*What CIRCIA Means for Critical  
Infrastructure Providers and How  
Breach and Attack Simulation Can Help*

*The Next Iteration of Privacy: What  
Businesses Should Know About New  
Privacy Laws in Oregon, Texas, and  
Florida*

*...and much more...*

**MORE INSIDE!**



# CONTENTS

<b>Welcome to CDM's August 2024 Issue</b> -----	9
<b>Cybersecurity In Critical Infrastructure: Protecting Power Grids and Smart Grids</b> -----	22
By Kehinde Ayano, Assistant Professor of Computer and information Science, Indiana Wesleyan University Marion Indiana USA	
<b>What CIRCIA Means for Critical Infrastructure Providers and How Breach and Attack Simulation Can Help</b> -----	27
By Guy Bejerano, CEO, SafeBreach	
<b>The Next Iteration of Privacy: What Businesses Should Know About New Privacy Laws in Oregon, Texas, and Florida</b> -----	33
By Sarah Rugnetta and Carolyn Ho, attorneys with the Constangy Cyber Team, Constangy, Brooks, Smith & Prophete LLP	
<b>The First 10 Days of a vCISO'S Journey with a New Client</b> -----	37
By Pete Green, Reporter for Cyber Defense Magazine	
<b>SEC Cybersecurity Disclosure Rules – Are CISOs Ready to Go Beyond the Tip of the Iceberg?</b> -----	43
By Brian Levin, Chief Customer Officer, Panaseer	
<b>Escalating Cyberattacks in the Healthcare Sector</b> -----	46
by Ariel Novak, Vice President, Cybersecurity, PAN	
<b>It's Time to Sound the Alarm on SMB Cyber Threats</b> -----	49
By Jamie Levy, Director, Adversary Tactics, Huntress	
<b>Beyond Fines: The Real Value of Achieving Cybersecurity Compliance</b> -----	53
By Colton Murray, Security & Compliance Manager, Allegiant a Crexendo Company	
<b>How Automation Can Help Security Policy Optimization</b> -----	57
By Erez Tadmor, Field CTO, Tufin	
<b>The Role of Intelligence in Cyber Threat Response</b> -----	61
By Kurt Xavier Schumacher, Product Manager, MONITORAPP	
<b>Worried about Insider Risk? Pay More Attention to Offboarding</b> -----	67
By Cris Grossmann, CEO and Co-Founder, Beekeeper	

<b><i>How AI-Driven Cybersecurity Offers Both Promise and Peril for Enterprises</i></b> -----	<b>70</b>
By Metin Kortak, Chief Information Security Officer, Rhymetec	
<b><i>NextGen Identity Management</i></b> -----	<b>74</b>
By Dr. Sarbari Gupta, Founder and CEO, Electrosoft Services, Inc.	
<b><i>RegreSSHion, Critical RCE Vulnerabilities, and When Should You Be Scared?</i></b> -----	<b>78</b>
By Jonathan Jacobi, CTO Office, Dazz	
<b><i>70% of Enterprises Established SaaS Security Teams, Cloud Security Alliance Survey Finds</i></b> -----	<b>81</b>
By Hananel Livneh, Head of Product Marketing, Adaptive Shield	
<b><i>Transforming Security Testing With AI: Benefits and Challenges</i></b> -----	<b>89</b>
By Haresh Kumbhani, CEO, Zymr Inc.	
<b><i>Strategies for Building an Effective, Resilient Security Operations Center</i></b> -----	<b>95</b>
By William Wetherill, Chief Information Security Officer, DefenseStorm	
<b><i>AI-Powered Fraud Detection Systems for Enhanced Cybersecurity</i></b> -----	<b>100</b>
By April Miller, Managing Editor, ReHack Magazine	
<b><i>The Unsolvable Problem: XZ and Modern Infrastructure</i></b> -----	<b>104</b>
By Josh Bressers, Vice President of Security, Anchore	
<b><i>Zero-Trust Endpoint Security</i></b> -----	<b>107</b>
By Dr. Ran Dubin, CTO, BUFFERZONE Security LTD	
<b><i>The Ugly Truth about Your Software Vendor which CISOs Won't Want (But Do Need) to Hear</i></b> -----	<b>111</b>
By Iain Saunderson, CTO, Spinnaker Support	
<b><i>Team-Based Training and the Power of Simulation</i></b> -----	<b>115</b>
By Tom Marsland, VP of Technology, Cloud Range	
<b><i>Securing E-commerce</i></b> -----	<b>118</b>
By Andy Lulham, Chief Operating Officer at VerifyMy	
<b><i>The 3 Questions at the Core of Every Cybersecurity Compliance Mandate</i></b> -----	<b>121</b>
By Cam Roberson, VP Sales & Channel Development, Beachhead Solutions Inc.	
<b><i>Safeguarding Corporate Secrets: Best Practices and Advanced Solutions</i></b> -----	<b>125</b>
By Mr. Dhruv Khanna, Co-Founder, CEO, Data Resolve	

<b><i>How Has Video Analytics Enhanced Security and Efficiency?</i></b> -----	<b>128</b>
By Harshada Dive, Senior Writer, Allied Market Research	
<b><i>The Imperative of Penetration Testing AI Systems</i></b> -----	<b>132</b>
By Jesse Roberts, SVP of Cybersecurity, Compass Cyber Guard	
<b><i>Why Did Snowflake Have a Target on It? Handling Data Warehouse Security Risks</i></b> -----	<b>136</b>
By Kapil Raina, VP of Marketing, Bedrock Security	
<b><i>Detection Engineering in Post SIEM and SOAR World</i></b> -----	<b>140</b>
By Venkat Pothamsetty, CTO, Network Intelligence	
<b><i>Strategy Must Adapt</i></b> -----	<b>145</b>
By Simon Wijckmans, CEO, c/side	
<b><i>Demystifying Zero Trust</i></b> -----	<b>148</b>
By Ashish Arora, AVP - Network Security, Chubb	
<b><i>How AI Is Transforming Cyber Risk Quantification</i></b> -----	<b>153</b>
By Jose Seara, Founder and CEO, DeNexus	
<b><i>Spotlight on Dashlane</i></b> -----	<b>156</b>
By Dan K. Anderson vCISO and On-Call Roving Reporter, Cyber Defense Magazine	
<b><i>Spotlight on Onyxia</i></b> -----	<b>162</b>
By Dan K. Anderson vCISO	
<b><i>Empowering Security Through Timely Nudges: Harnessing Behavioral Science for Real-Time Interventions</i></b> -----	<b>167</b>
By Tim Ward, CEO of ThinkCyber Security	
<b><i>Unlocking the Right Encryption</i></b> -----	<b>171</b>
By Ben Warner, VP of Strategic Accounts, CRU Data Security Group	
<b><i>Cyber Threat Intelligence (CTI) for Supply Chain Monitoring</i></b> -----	<b>175</b>
By Shawn Loveland, COO, Resecurity	
<b><i>Cyber Risks for Government Agencies Are on the Rise. Why Security Is Still an Uphill Battle.</i></b> -----	<b>182</b>
By Sarah Gray, Director of Product Marketing at Adaptiva	



<b><i>The AT&amp;T Phone Records Stolen</i></b> -----	<b>185</b>
By James Gorman, vCISO, Hard2Hack	
<b><i>Uncovering the Gaps in Cyberthreat Detection &amp; the Hidden Weaknesses of SIEM</i></b> -----	<b>188</b>
By Garath Lauder, Director, Cyberseer	
<b><i>Data Breaches are a Dime a Dozen: It's Time for a New Cybersecurity Paradigm</i></b> -----	<b>193</b>
By Ev Kontsevoy, Co-Founder and CEO, Teleport	
<b><i>DNS Security Strategies: Protecting Against Ransomware, Botnets, And Data Theft</i></b> -----	<b>197</b>
By Alexander Biushkin, Business Development Executive, SafeDNS	
<b><i>Embracing Proactive Fraud Management with Real-Time Orchestration</i></b> -----	<b>201</b>
By Mario Dusaj, Senior Solutions Engineer - US, Callsign.com	
<b><i>5 Essential Features of an Effective Malware Sandbox</i></b> -----	<b>204</b>
By Vlad Ananin, Technical Writer, ANY.RUN	
<b><i>Fortifying the Future: AI Security Is The Cornerstone Of The AI And GenAI Ecosystem</i></b> -----	<b>211</b>
By Rony Ohayon, CEO and Founder, DeepKeep	
<b><i>Guarding the Games: Cybersecurity and the 2024 Summer Olympics</i></b> -----	<b>216</b>
By Desrah Kraft, Cyber Threat Intelligence Engineer, DefenseStorm	
<b><i>High Performance Software Defined Receivers</i></b> -----	<b>220</b>
By Brandon Malatest, COO, Per Vices Corporation	
<b><i>How Ransomware Jeopardizes Healthcare Organizations</i></b> -----	<b>226</b>
By Kartik Donga, Founder, PeoplActive	
<b><i>Illegal Crypto Mining: How Businesses Can Prevent Themselves From Being 'Cryptojacked'</i></b> -----	<b>231</b>
By Andy Syrewicze, Security Evangelist at Hornetsecurity	
<b><i>Maintaining File Security While Working Remotely</i></b> -----	<b>235</b>
By Majed Alhajry, CTO of MASV	
<b><i>Mitigating the Risk of Cybercrime While Traveling Abroad</i></b> -----	<b>238</b>
By Dana Hummel, Senior Manager of Digital PR, All About Cookies	
<b><i>Modern Phishing Challenges and the Browser Security Strategies to Combat Them</i></b> -----	<b>241</b>
By Kenneth Moras, Security GRC Lead, Plaid	

<b><i>Navigating the Complexities of AI in Content Creation and Cybersecurity</i></b> -----	<b>244</b>
By Rachel Strella, Founder & CEO, Strella Social Media	
<b><i>New Levels, New Devils: The Multifaceted Extortion Tactics Keeping Ransomware Alive</i></b> ---	<b>247</b>
By Jacques de la Riviere, CEO, Gatewatcher	
<b><i>Perimeter Security Is at the Forefront of Industry 4.0 Revolution</i></b> -----	<b>250</b>
By Avinash Dhanwani, Research Director, The Brainy Insights	
<b><i>Greater Security for Small Businesses: Why Do SMEs Need a SIEM System?</i></b> -----	<b>253</b>
By Sergio Bertoni, the Leading Analyst at SearchInform	
<b><i>Securing AI Models - Risk and Best Practices</i></b> -----	<b>257</b>
By Arun Mamgai, Cybersecurity and Data Science Specialist	
<b><i>Supply Chains Make Insider Threat Defense More Complex</i></b> -----	<b>262</b>
By Zac Amos, Features Editor, ReHack	
<b><i>Giving a Voice to Future Generations of Female Cybersecurity Leaders</i></b> -----	<b>265</b>
By Nazy Fouladirad, COO of Tevora	
<b><i>The Evolution of Cloud Strategy: Beyond "Cloud First"</i></b> -----	<b>269</b>
By Tanvir Khan, Executive Vice President of Cloud, Infrastructure, Digital Workplace Services and Platforms, NTT DATA	
<b><i>The Last Stop: Protecting an NHL Franchise Against Cyberattacks</i></b> -----	<b>272</b>
By Marc Laliberte, Director of Security Operations at WatchGuard	



@MILIEFSKY

From the

Publisher...



Through Cyber Defense Magazine, and our parent company Cyber Defense Media Group (CDMG), we have several valuable initiatives now open for the benefit of our readers and followers.

We will be participating in force at Black Hat USA the first week of August. You can meet our reporters at Black Hat USA and learn about many of the top infosec innovator finalists for 2024 on the expo floor and in private meetings. The current issue of Cyber Defense Magazine features articles by many of the participants, and our website carries many more informational and promotional features.

SPOTLIGHT OPPORTUNITIES! You will notice in this August issue of CDM the addition of a new line of "Spotlight" articles, provided by specialized reporting staff, with in-depth coverage of the products and service of individual companies in the cybersecurity industry. We would be pleased to discuss how your company can benefit from participating in this program.

We would like to remind our readers that The Black Unicorn awards program is now part of the Top InfoSec Innovator awards program. Please see detailed information at the Conference and Awards website:

<https://cyberdefenseconferences.com/top-infosec-innovator-awards-2024-apply-today/>

The virtual red carpet is already set up, with the incredible high traffic website and social media marketing, and much more to help bolster the good news around our winners during our 2nd half of 2024, 12th anniversary and 12th annual awards during [CyberDefenseCon 2024](#).

#### **World's First Cyber Defense Genius™**

For those readers who have not yet accessed this new facility, we are also pleased to remind you that Cyber Defense Magazine has launched the World's First Cyber Defense Genius™ the world's first AI GPT trained specifically on over 17,000 pages of infosec expertise and learning more, daily. It is now available on our home page at <https://www.cyberdefensemagazine.com/> on the ride side of the screen. We welcome your comments and feedback as you take advantage of this excellent professional resource.

Our mission is constant - to share cutting-edge knowledge, real-world stories and awards on the best ideas, products, and services in the information security industry to help you on this journey.

Warmest regards,

*Gary S. Miliefsky*

Gary S. Miliefsky, fmDHS, CISSP®  
CEO/Publisher/Radio/TV Host

*P.S. When you share a story or an article or information about CDM, please use #CDM and @CyberDefenseMag and @Miliefsky – it helps spread the word about our free resources even more quickly*



**@CYBERDEFENSEMA**

## CYBER DEFENSE eMAGAZINE

Published monthly by the team at Cyber Defense Media Group and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

### EDITOR-IN-CHIEF

Yan Ross, JD

[yan.ross@cyberdefensemagazine.com](mailto:yan.ross@cyberdefensemagazine.com)

### ADVERTISING

Marketing Team

[marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)

### CONTACT US:

Cyber Defense Magazine

Toll Free: 1-833-844-9468

International: +1-603-280-4451

<https://www.cyberdefensemagazine.com>

Copyright © 2024, Cyber Defense Magazine, a division of  
CYBER DEFENSE MEDIA GROUP

1717 Pennsylvania Avenue NW, Suite 1025

Washington, D.C. 20006 USA

EIN: 454-18-8465, DUNS# 078358935.

All rights reserved worldwide.

### PUBLISHER

**Gary S. Miliefsky, CISSP®**

Learn more about our founder & publisher at:

<https://www.cyberdefensemagazine.com/about-our-founder/>



## 12 YEARS OF EXCELLENCE!

Providing free information, best practices, tips, and techniques on cybersecurity since 2012, Cyber Defense Magazine is your go-to-source for Information Security. We're a proud division of Cyber Defense Media Group

[CYBERDEFENSEMEDIAGROUP.COM](https://www.cyberdefensemediagroup.com)

[MAGAZINE](#)

[TV](#)

[RADIO](#)

[AWARDS](#)

[PROFESSIONALS](#)

[WIRE](#)

[WEBINARS](#)

[CYBERDEFENSECONFERENCES](#)



# Welcome to CDM's August 2024 Issue

## From the Editor-in-Chief

The August 2024 issue of Cyber Defense Magazine includes numerous articles addressing the increasing number of cyber attacks and failures involving sectors of the critical infrastructure. While the protection of critical infrastructure is not at all new, the surprising aspect is that the 16 sectors have been recognized and discussed for over 25 years – but the official responses to the obvious vulnerabilities are still reactive, not pro-active.

Once again, we received some 50 articles from sources in the cybersecurity industry this month. They run the gamut from practical applications to theoretical commentary, from financial services to health care, and from large-scale enterprises to SMEs – and beyond. One aspect our authors have in common is that they write predictively as well as in response to cyber threats already experienced.

We are already getting inquiries about interest in publishing articles on the broad-based outage resulting from the CrowdStrike interface with MicroSoft systems. While there has been assurance that it was not based on a cyber attack from outside, it has not been reassuring that it reflects some shortcoming in the internal operations of the two companies involved. Stay tuned!

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  
Editor-in-Chief  
Cyber Defense Magazine

### About the US Editor-in-Chief

Yan Ross, J.D., is a Cybersecurity Journalist & U.S. 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@cyberdefensemagazine.com](mailto:yan.ross@cyberdefensemagazine.com)





# SPONSORS







NIGHTDRAGON



**“NightDragon** Security is not looking to invest in ‘yet another endpoint’ solution or falling for the hype of ‘yet another a.i. solution’, it’s creating a unique platform for tomorrow’s solutions to come to market faster, to breathe new life into a stale cyber defense economy”

-David DeWalt

Managing Director and Founder NightDragon Security

### **ADVISE**

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

### **INVEST**

WE ARE FLEXIBLE INVESTORS ACROSS ALL STAGES OF GROWTH TO PRE-IPO

### **ACCELERATE**

WE HELP OUR COMPANIES ACCELERATE THEIR GROWTH THROUGH STRATEGY TUNING AND RELATIONSHIP BUILDING

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



**UNKNOWN**  
CYBER

**"70% of Malware Infections Go Undetected by Antivirus..."**

**Not by us. We detect the unknowns.**

**[www.unknowncyber.com](http://www.unknowncyber.com)**



2001



2024

ALLEGIS CYBER CAPITAL

# The first dedicated cybersecurity venture firm in the world.

AN INTEGRATED GLOBAL, STAGE-AGNOSTIC CYBERSECURITY INVESTMENT PLATFORM SPANNING SEED THROUGH GROWTH.

For 20 years, AllegisCyber Capital has offered a proven investment platform that actively engages with the most promising entrepreneurs in cyber and delivers the market access, team building, and operating experience essential to their success.

BUILDING AND FUNDING THE MOST INNOVATIVE COMPANIES IN CYBER



ALLEGISCYBER  
CAPITAL

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





DATATRIBE

# CYBER STARTUP FOUNDRY

Forging dominant companies  
from nation-state domain expertise

CAPITAL | RESOURCES | GUIDANCE | SUCCESS

HOME TO THE WORLD'S FASTEST GROWING  
CYBERSECURITY AND DATA SCIENCE COMPANIES

quickcode

DRAGOS

EN|VEIL  
ENCRYPTED VEIL

INERTIALSENSE

PREVAILION

the  
cyberwire

Ntrinsec  
Data Security Automation

SIXMAP

STRIDER

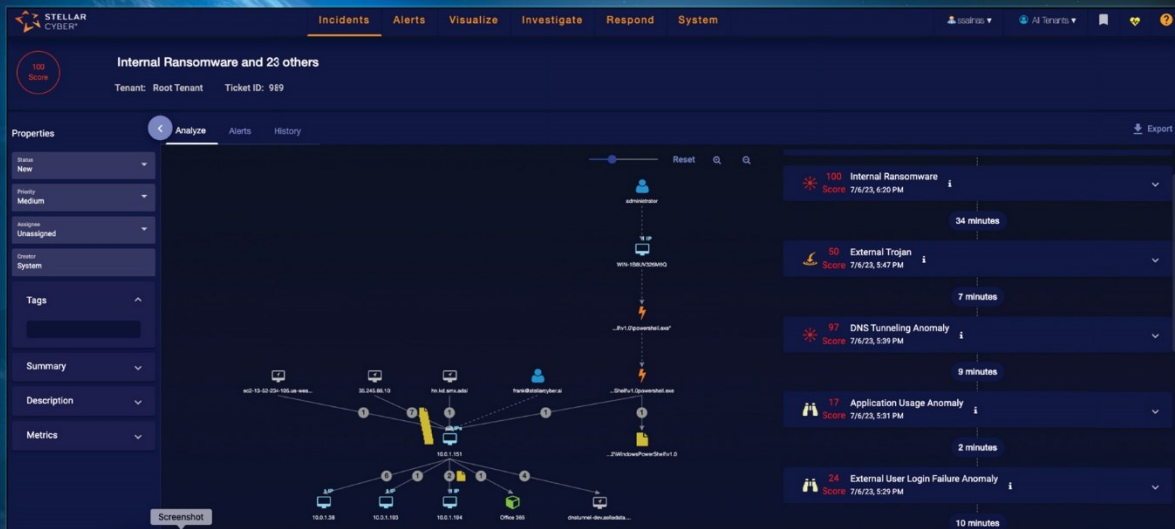
CONTRAFORCE

BLACKCLOAK™

SightGain

JOIN THE TRIBE

DATATRIBE.COM



# We are Open XDR

Making Security Operations Simpler

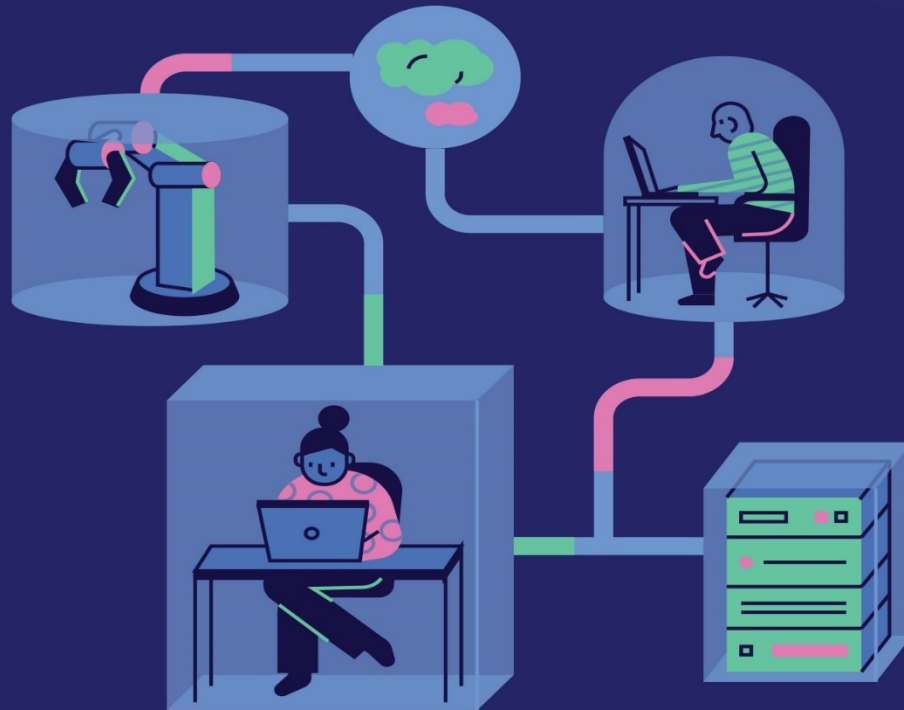
It's your security stack. Our job is to make it work better to deliver the security outcomes you need.

stellarcyber.ai





# Radically simple segmentation *in a click.*



Don't believe us?

*Neither did they!*

SCAN ME





# RidgeBot® AI-Powered Security Validation Platform



Exposure Management

Automated Pentesting

Avoid Staff Shortage

## RidgeBot® CTEM Support

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

[Learn More](#)



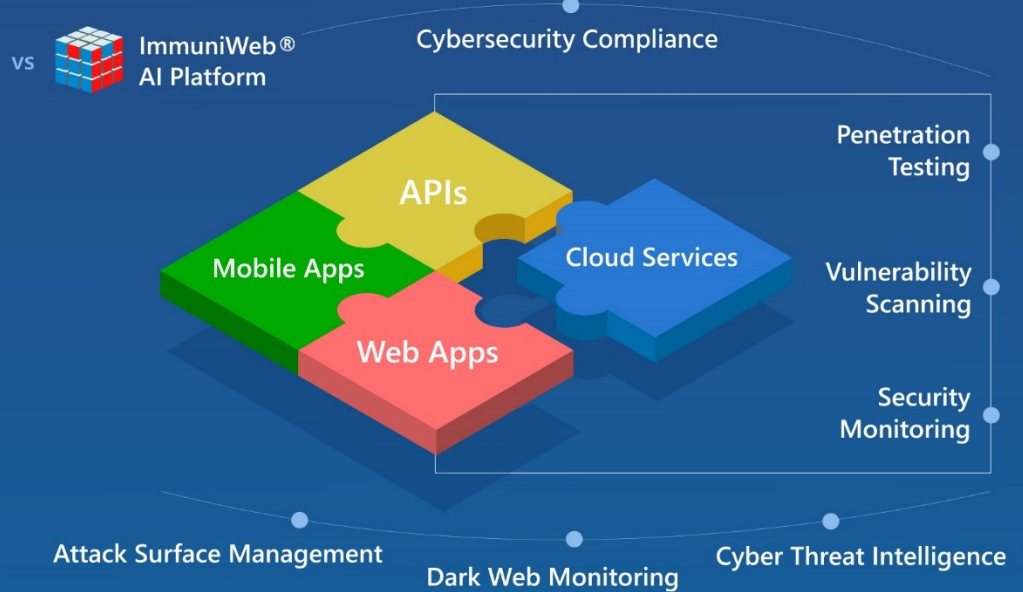


**ImmuniWeb®**  
AI for Application Security

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)





# Partner to Close Gaps.



NSA's no-cost **vulnerability assessment** quickly finds issues before they become compromises.

GET STARTED TODAY WITH THIS AND OTHER SERVICES

[nsa.gov/cc](https://www.nsa.gov/cc)







# **We will focus on your cybersecurity, so you can focus on your business.**

We have the right mix of people, processes, and technology to build your robust security program and respond successfully to any threat that comes your way.

**Cyber Defense  
& Response.**

**It's what we do.**

**[cyderes.com](https://cyderes.com)**

A hand holding a pen over a spiral notebook on a desk, with a keyboard and a glowing blue network overlay in the background.

# ARTICLES





## Cybersecurity In Critical Infrastructure: Protecting Power Grids and Smart Grids

By Kehinde Ayano, Assistant Professor of Computer and information Science, Indiana Wesleyan University Marion Indiana USA

Infrastructure like water system, supply system, telecommunication networks, and power plants are critical assets for any country in that the destruction and incapacity of such systems poses an adverse effect on security, economy, health, and overall welfare and existence of any country. The integration of digital and cyber warfare into traditional warfare has necessitated the need to adequately secure those critical infrastructures as they become top target by state actors in case of conflict and war.

Most systems in modern society are electricity driven which makes power and smart grids very crucial as they underpin nearly all other critical infrastructure. A successful attack on this infrastructure will have a cascading effect on all other critical infrastructures. This article discusses the evolution of power grids, threat landscape and vulnerabilities in power and smart grids. It also examines real world case studies of cyber- attacks on power and smart grids analyzing the incidents and concludes with security strategies and best practices for protecting power and smart grids.



## Evolution of Power and Smart Grids

Traditional power system also known as power grids are a one-way system for distribution of electricity from producers to consumers and are vital for functioning of businesses, society, and government at large. They are manually controlled with limited capacity for integration with renewable energy. Advance in technology and digital evolution led to the development of modern versions of the traditional power system that makes use of digital technologies for monitoring, management, synchronization, and transportation of energy from multiple sources to meet the varying demands of the consumers. These smart grids, unlike the power grids, are two-way communication systems with automated control and real time monitoring and allows for easy integration of renewable energy which improves the reliability and efficiency of electrical power systems.

## Components of Smart Grids Communication Network

Some of the major components of the smart grid communication network include the following which allows for seamless two-way communication between utilities and consumers include the following.

**Control Center:** This is the central hub for monitoring and managing the entire grid. It accepts data from all other components and sends control signals for grid operation management.

**Substation:** Transforms high voltage from the transmission network to lower levels suitable for distribution. Smart grids substations are equipped with sensors and devices that can send data on power quality, load condition and status of equipment to the control center.

**Smart Meter:** Smart meter measures and communicates consumption with both consumer and the utility in real time.

**Advanced Metering Infrastructure:** It facilitates communications between smart meters and utilities, and send smart meter data to the control center and other grid components

The components listed above and many more make smart grids a fully digitalized communication network improve reliability and efficiency of electrical power system. However, the integration of digital technology in smart grids also introduces new vulnerabilities and cybersecurity threats that must be addressed for robust operation. Ensuring that power and smart grids are secured is critical to the existence of business, organization, and government as the resultant of these attacks could be catastrophic and life threatening.

## Threat landscape in Power and Smart Grids

**Malware:** These are malicious software designed to disrupt damage and gain access to the system. This includes trojans, virus, ransomware, and many others. Malware exploits known and zero-day vulnerabilities in software, hardware and network protocols used in power systems and can disable or disrupt Supervisory control and Data Acquisition systems SCADA, DCS and other operational technologies.

**Phishing:** This is a form of attack whereby an attacker disguises and attempt to acquire sensitive information such as usernames and passwords by posing to be a legitimate entity.

**Network Intrusion:** Network communication systems of power and smart grids can be intruded through weak security configurations like default password, unsecured remote access, or unpatched systems and other vulnerabilities to gain control into the system.

**Distributed Denial of Service (DDOS):** This is an attempt to disrupt the availability of services provided by smart grids and make them unavailable by overwhelming the system with traffic from multiple sources. The DDOS are usually launched from malware infected hosts and could be volume-based attacks like UDP and ICMP floods, protocol attacks like SYN flood and Smurf DDOS or Application layer attack GET/POST floods.

**Advanced Persistent Threats (APT):** This is a prolonged and targeted cyber-attack whereby state actors or highly skilled cyber criminals gain access to a network and remain undetected for an extended period.

## Vulnerabilities in Power and Smart Grids

The attack surface has significantly expanded in smart grids due to complex network of devices which includes sensors, smart meters, smart switches, communication networks and control systems with each of these components being a target for cyber-attacks. Increased connectivity and data exchange within the control center and other components of smart grids make it more vulnerable to attack. Therefore, to maintain the resilience and security of smart grids, understanding and addressing the vulnerabilities inherent in smart grids systems is critical.

These vulnerabilities include the following:

**Legacy Systems:** The continuous use of Legacy systems which are outdated technologies due to certain constraints within an organization, poses significant risk to the security of such systems. This is because such systems may no longer be patched for updates and may also have limited monitoring capability.

**Interconnected Networks:** The vast interconnection of devices and increased connectivity of communication systems of smart grids if not properly secured, make them highly vulnerable to attack.

**Remote Access:** The management and monitoring of grids system are usually done through remote access. Vulnerabilities in remote access connection may be exploited by attackers to gain access into the system.

**Supply Chain Risk:** Smart grids heavily rely on complex supply chain of hardware and software components which are majorly contracted out to manufacturers and suppliers. The security practices of such 3<sup>rd</sup> party vendors, if not robust, may pose significant risk when integrated into the power and smart grids. Attackers can also target the software development lifecycle by compromising legitimate software and software updates which in turn makes the system in which they are deployed vulnerable to attack. An example of such supply chain vulnerabilities is the SolarWinds attack (2020) where malware is injected into routine software update.

**Human Factor:** Human factor is one of the most common vulnerabilities in cybersecurity framework. Error and negligence or malicious intent by staff despite the solid technological defenses have led to system compromise. This compromise comes because of inadequate training and awareness, poor password practices and insider threats.



## Real World Examples of Cyber-Attacks on Power and Smart Grids

Due to the digital evolution of electrical power systems, power and smart grids are increasingly becoming ground zero for cyberwarfare. Over the past two decades, several attacks have been launched against smart grids resulting in outages and financial loss resulting from payment of huge ransom. Example of such is the attack on Ukraine Power Grid in 2015 in which BlackEnergy malware was used to compromise three Ukrainian distribution system using spear-phishing email. The attacker gained access to the Supervisory Control and Data Acquisition (SCADA) systems and compromised the circuit breaker remotely and disabled the UPS and Backup. Also, in 2016, Ukrainian transmission station was targeted by a custom-built malware named Industroyer which compromised the Industrial Control System and disrupt power distribution for about an hour. In the United States, Florida Municipal Power agencies were also targeted in June 2021 using phishing and remote vulnerabilities as attack vectors. While the attackers gained some level of access, the attack was mitigated before it could cause catastrophic effect. These cases underscore the importance of security strategies and best practices in power and smart grids management.

## Security Strategies and Best Practices for Managing Power and Smart Grids

Cyberattacks on power grids and smart grids have become more frequent and sophisticated in recent years and can have devastating consequences which include blackouts, economic losses, disruptions to vital infrastructure, and theft of sensitive data. Therefore, there is a need to put in place sound security strategies and best practices to safeguard this critical infrastructure from attack. Some security strategies and best practices for power and smart grids are discussed below.

**Risk assessment and management:** Risk assessment and management plays a vital role in the security of power and smart grids as they help to detect and mitigate vulnerabilities and help in incidence response. Implementing Risk assessment and management using the NIST **Interagency Report (IR) 7628 Revision 1** which provides a comprehensive framework for securing smart grid systems will go a long way in securing this critical infrastructure.

**Defense-in-Depth:** Implementing a layered security approach using various security controls and protocols (firewalls, encryption, IDS, IPS, SIEM, access controls) will enhance the security posture of smart grid systems.

**Vulnerability Assessment and Penetration Testing:** Detecting inherent weakness in smart grid systems before an attacker does through comprehensive vulnerability assessment and simulation of real attack to discover vulnerabilities that are hidden and remain undiscovered by automated scanning will allow those security lapses in the system to be tightened before they are exploited on by attackers.

**Patch Management:** Apart from ensuring system reliability, effective patch management also reduces attack surface. It is more cost-effective to proactively address vulnerabilities in smart grid through effective patch management than to reactively mitigate the resultant effect of security breaches.

**Network Segmentation:** Segmentation of communications network system of a smart grid system inhibits lateral movement preventing attacker from gaining access to the entire system in case of breach thereby minimizing the impact of the attack. It also helps remediation as focus can be only on the compromised segment.

**Data Backup and Recovery (BCP and DRP) Plan:** Having a Business Continuity Plan and Disaster Recovery Plan in place will help to facilitate recovery from cyber-attacks, reducing time and mitigate the impact on services.

**Employee Training and Awareness Programs:** The importance of employee training and awareness could not be overemphasized as research has shown that humans are the missing link in the cybersecurity chain as they are highly susceptible to social engineering, phishing, insider threats and prone to commit errors. Training and awareness will help employees to have good cyber hygiene and cultivate strong cybersecurity structure.

## Conclusion

In conclusion, power and smart grids security requires a multidimensional approach that combines implementation of security controls which are administrative, physical, and technological, and proactive risk assessment and management, and continuous training and retraining of human elements. Making cybersecurity a top priority and fostering cybersecurity culture will safeguard this critical infrastructure from attacks.

### About the Author

Kehinde Ayano Ph. D. is an assistant professor of Computer and Information Science at Indiana Wesleyan University Indiana. He is also a Certified Information System Security Specialist. Kenny can be reached on [Kenny.ayano@indwes.edu](mailto:Kenny.ayano@indwes.edu) .







## What CIRCIA Means for Critical Infrastructure Providers and How Breach and Attack Simulation Can Help

By Guy Bejerano, CEO, SafeBreach

On July 3rd the period for public comment closed for the [U.S. Cybersecurity and Infrastructure Security Agency's](#) proposed [Cyber Incident Reporting for Critical Infrastructure Act of 2022](#) (CIRCIA) reporting rules announced earlier this year. CIRCIA's enhanced reporting obligations have the potential to drive greater transparency, accountability and, ultimately, much-needed improvements in cyber readiness and resilience across all U.S. critical infrastructure sectors.

Below, I'll discuss what CIRCIA means to organizations covered by these rules, the reason for its focus on critical infrastructure, and how organizations can prepare to meet its reporting requirements. I'll also explore how breach and attack simulation (BAS) programs can help organizations not only comply with the rules, but also prepare for future threats and regulations with new simulation, incident response, and reporting capabilities.

## What CIRCIA Demands

The rules require covered organizations to report ransomware payments to CISA within 24 hours and all covered cyber incidents within 72 hours. The rules apply to a broad array of entities across [16 critical infrastructure sectors](#) as defined by CISA, including energy, water, transportation, healthcare, and financial services, among others.

CISA anticipates CIRCIA will affect more than 316,000 entities, result in around 210,525 reports and cost critical infrastructure providers an estimated \$2.6 billion in rule familiarization, data and record preservation, and reporting expenses.

## Why Critical Infrastructure

We have substantial evidence from governments and private sector threat researchers that nation-state threat actors are attempting to compromise and pre-position cyber-attack infrastructure within U.S. and allied critical infrastructure systems.

The [Volt Typhoon](#) revelations of the last several months have helped expose the extent of these efforts. They also highlight that 85% of U.S. critical infrastructure is run by [private sector](#) organizations.

Any nation-wide effort to detect, contain, and recover from cyber attacks on U.S. critical infrastructure would require speed in situational awareness and greater visibility into the nature and scope of an adversary's offensive cyber operations.

Without visibility into cyber incidents across critical infrastructure sectors, it will be very difficult for the government, private sector operators, and the threat research community to understand and pre-empt future attacks, let alone coordinate effective responses to minimize impact during major incidents.

## What CIRCIA Means for CISOs

Every new rule, requirement and guideline initially tends to pose more questions than clarity. Fortunately, the CIRCIA draft rules will likely answer many CISOs' questions around definitions, compliance requirements, and potential costs associated with them. The comprehensive nature of the rules demonstrates how serious the U.S. government is about the information sharing required to protect these systems. It also acknowledges previous private-sector concerns around reporting definitions, confidentiality, and accountability.

CISA acknowledged incident reporting concerns raised by the [SEC reporting](#) mandates of 2023. In areas such as the confidentiality of shared cyber attack information, CISA commits to only releasing such information as anonymized, aggregated data within quarterly reports. The agency states it will not consider information shared in good faith early in a cyber incident as false or misleading if subsequent information shows initial disclosures were inaccurate. CISA even commits to working with other agencies to harmonize all U.S federal incident reporting requirements, hopefully making the CISO's already difficult role of complying with them somewhat easier.



As a former CISO myself, I understand the concerns that 72 hours may not provide many organizations adequate time to fully comprehend the nature, extent and potential impact of an incident in their environment. But such rules will force the discipline necessary for CISOs to implement a more proactive approach to security that is focused on developing a continuous understanding of the efficacy of their security tools and their vulnerability to security events, which in turn will allow them to take action faster and engage government partners in a more timely manner.

Increased reporting will likely enable CISOs to better prepare for cyber attacks through attack simulations trained on a much larger body of threat intelligence. Those essential preparations cannot be effective if information sharing fails to provide threat data specific to their critical infrastructure sectors and specific functions within those sectors.

### **How to Prepare for CIRCIA Reporting (and the Future)**

To prepare for the reporting to come, CISOs must engage with legal, risk-management, and security teams to understand CIRCIA's requirements, assess their cybersecurity postures, and implement robust detection, simulation and reporting mechanisms.

While CIRCIA poses a tremendous opportunity to operationalize intelligence in their defense, forward-looking operators will also take the initiative to implement solutions and processes that prepare them for greater scrutiny of their cyber readiness from regulators and cyber insurance auditors.

Industries such as the defense industrial base, healthcare, nuclear power, financial institutions, and electric power face higher minimum standards for required cyber defenses and practices. In some circumstances, operators are even required to detail incident response and recovery plans and produce posture assessments. Other critical infrastructure provider sectors are not required to present such plans to operate, but will increasingly be required to produce such plans and assessments for auditors.

### **How Breach & Attack Simulation Can Help**

Breach and attack simulation (BAS) solutions can play an important role in helping critical infrastructure organizations prepare for and comply with these rules, as well as prepare for future assessments and audits. BAS solutions are designed to safely and continuously run real-world attacks—based on the tactics, techniques and procedures (TTPs) used by cyber adversaries—against an organization's production applications and infrastructure to validate how their security controls are performing and identify gaps before attackers do.

At its core, BAS is about applying the cyber incident experiences of organizations to the defense of other organizations. It can be used to develop cyber risk mitigation and incident response plans that strengthen defenses and better prepare organizations to fend off future attacks. Both capabilities can benefit from sector information and help produce cyber-readiness reports for executive teams, insurers, and regulators.

## Testing defenses with sector- & function-specific threats.

To prepare themselves for future attacks, organizations can utilize BAS to simulate real-world attacks against their security ecosystem, recreating attack scenarios specific to their critical infrastructure sector and function within that sector, including specific TTPs.

The most effective BAS solutions are continuously and quickly updated with new cyber threat information, including incorporating the latest content from [US-CERT and FBI Flash alerts](#). Attack simulations must also be informed by a broad base of industry research findings, making integration between BAS platforms and external threat intelligence networks essential.

A notable example can be found in the recent US-CERT alert around the indicators of compromise (IOCs) and TTPs for [Akira Ransomware](#) that were disclosed by the US FBI, CISA, Europol's European Cybercrime Centre (EC3), and the Netherlands' National Cyber Security Centre (NCSC-NL). The disclosure was based on research from the FBI, as well as an industry threat research partner.

Evidence suggests Akira has been targeting a wide range of businesses and critical infrastructure entities since March 2023 across North America, Europe, and Australia. During the initial attacks, threat actors leveraging Akira ransomware targeted Windows-only systems. However, in April 2023, they began targeting VMware ESXi virtual machines through a new Linux variant. It is believed that as of the beginning of this year, the Akira ransomware group successfully impacted over 250 organizations and extorted nearly \$42 million USD from its victims.

BAS enables organizations with a similar profile to the victims of Akira Ransomware to implement information from such disclosures within their simulations and, in doing so, regularly validate their security controls—at scale and in a production environment—to ensure optimal performance against this and other new and evolving cyber threats.

## Understanding exposure & developing mitigation responses.

As simulations proceed, CISOs will be best served by utilizing BAS platforms that can not only create highly customized attacks, but also integrate into their solutions to inform their mitigation priorities and develop defensive strategies against the most novel of attack vectors.

For instance, a global financial services firm recently used BAS to validate the end-to-end efficacy of its security tools, alert and detection systems, and incident response workflows. They utilized simulations that included both known attacks and attacks customized to the organization's specific architecture and industry. They also integrated both their ticketing system and security information and event management (SIEM) system with the BAS platform to determine whether their detection mechanisms and alert notifications were operational, effective, and capable of identifying and responding to specific security events.

The organization found that notifications around potential malicious activity often were not delivered to incident responders. In fact, many were being delayed for hours due to the complex pipeline of



technologies the alerts were required to traverse. This created a critical time gap that real malicious actors could have exploited.

Given these revelations, the organization has made critical adjustments to its alert pipeline and now plans to expand the scope of these BAS-enabled health checks beyond endpoint alerts to cover a broader range of event types, such as web application firewall and email scenarios.

Such improvements begin with providing SOC teams with a clear understanding of how security controls detect, prevent, and mitigate attacks across the entire cyber kill chain. Teams should be able to leverage the MITRE ATT&CK framework to understand overall organizational risk exposure, and even visualize attack paths and explore alternative mitigation approaches. Such incident response plans have and will continue to become more relevant in the regulatory regimes and cyber insurance audits in the years to come.

### **Plan, measure & report progress.**

BAS platforms can enhance visibility when they incorporate customizable dashboards and reports to help stakeholders quickly understand existing security gaps, evaluate risks, and recognize security drift. Reports can also provide important security posture assessments that allow CISOs to measure their baseline, track improvement over time, and align security program reporting, KPIs, and investments with business goals.

These priorities require BAS platforms that are able to identify risk exposure with security scores, establish benchmarks against which improvement is measured, and help effectively communicate progress over time through personalized reports that define investment priorities.

Benchmarking, specifically, can be particularly useful where it allows organizations to compare their security posture to that of similar organizations within their industry. When given access to this type of information, organizations can evaluate their performance across different security control categories via side-by-side comparisons of blocked percentage scores and proactively identify areas for improvement to bring them more in line with industry standard performance. By communicating score differences compared to peers, key stakeholders are better able to make informed decisions about which cyber defenses must be prioritized for focus and investment.

### **Recover quickly with confidence.**

Finally, if an attack does occur, BAS frameworks can assist organizations not only in reporting the details of the incident, but they can also be transformative in identifying weaknesses that may have contributed, providing remediation advice, and retesting the resilience of the environment to ensure any gaps are closed.

## Rising Waves of Accountability

CIRCIA should be understood within the context of the rising waves of government regulation, growing legal liabilities, and insurance costs commensurate with the scale and seriousness of today's nation-state cyber threats to our critical infrastructure. These waves are inevitable given the stakes, and we should expect a continued drive toward greater public-private sector coordination in threat landscape awareness and cyber preparedness.

Ultimately, no organization can effectively prepare for future cyber attacks if it lacks an understanding of the threats specific to its sector and potential implications to its business. In this regard, the CIRCIA rules could prove an important step in opening a floodgate of shared security-controls-efficiency data specific to critical infrastructure providers and the life-supporting systems they operate.

This development, when combined with a comprehensive BAS program, will empower organizations to achieve their objectives of becoming more proactive in cyber defense, more efficient in risk reduction, and better informed to report on such matters to their executive teams and boards.

### About the Author

Guy Bejerano, CEO, SafeBreach. Guy Bejerano has over 30 years of security leadership experience. He began his career as an Information Security Officer in the Israeli Air Force, where he oversaw security ops and red team efforts. He then continued his career in the private sector, where he defined and executed security strategies as CISO for several global, public companies. In 2014, Guy co-founded SafeBreach, where he currently serves as CEO.

Guy can be reached online at [safebreachpr@kesscomm.com](mailto:safebreachpr@kesscomm.com), <https://www.linkedin.com/in/guy-bejerano-3a6524/>, and at our company website <https://www.safebreach.com/>





## The Next Iteration of Privacy: What Businesses Should Know About New Privacy Laws in Oregon, Texas, and Florida

By Sarah Rugnetta and Carolyn Ho, attorneys with the Constangy Cyber Team, Constangy, Brooks, Smith & Prophete LLP

As businesses enter the third quarter of 2024, they need to contend with three new state privacy laws. The Texas Data Privacy and Security Act, Oregon Consumer Privacy Act, and Florida Digital Bill of Rights all came into effect on July 1. With consumer data privacy laws already in effect in California, Colorado, Connecticut, Utah, and Virginia, many national and international companies need to confirm compliance with the eight state privacy laws currently in force.

With even more state privacy laws scheduled to come into effect within the next two years, consumer privacy regulation in the United States has become increasingly challenging for businesses. Many businesses are struggling with the daunting task of determining which laws apply to them and what they need to do to comply. Although there are many similarities between these laws, there are some nuances that businesses should take into consideration as they seek to update their external website documentation and internal compliance procedures.

In this article, we take a look at some of the more significant differences between the Texas, Oregon, and Florida laws.



## Applicability Thresholds

How can a company determine whether it falls within the scope of a particular state consumer privacy law? Typically, state privacy laws specify a minimum number of consumers for which personal data is processed, or a smaller minimum number of consumers if the business derives a specific percentage of revenue from selling personal data. These are the primary thresholds that trigger the applicability of a state privacy law, although some, like the California Consumer Privacy Act and the Utah Consumer Privacy Act, incorporate revenue directly into the applicability analysis.

Consistent with the majority of state privacy laws, the Oregon Consumer Privacy Act includes a data processing volume threshold, applying to any entity that conducts business in Oregon or provides products or services to Oregon residents, and that, during a calendar year, controls or processes (1) the personal data of 100,000 or more consumers (other than personal data controlled or processed solely for the purpose of completing a payment transaction); or (2) the personal data of 25,000 or more consumers while deriving 25 percent or more of annual gross revenue from selling personal data.

In contrast, the bulk of the obligations under the Florida Digital Bill of Rights apply to entities that, among other things, make more than \$1 billion in global gross annual revenue and that satisfy at least one of the following: (1) derive 50 percent or more of global gross annual revenue from the sale of advertisements online (including providing targeted advertising); (2) operate a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation; or (3) operate an app store or a digital distribution platform that offers at least 250,000 different software applications for consumers to download and install. In other words, FDBR applicability does not depend on exceeding a threshold number of consumers for data processing. Instead, FDBR applicability is narrowly confined to a specific set of very large businesses based on revenue and certain business activities.

The Texas Data Privacy and Security Act takes yet another approach to applicability. The TDPSA generally applies to entities that (1) conduct business in Texas, or produce products or services used by Texas residents; (2) process or engage in the sale of personal data; and (3) are not small businesses as defined by the U.S. Small Business Administration. There are no revenue thresholds or minimum numbers of individuals here. Instead, applicability will depend on the size of a business relative to a specific industry, as defined by the Small Business Administration.

## Entity-Type Exemptions

All state data privacy laws contain an assortment of entity or data-specific exemptions, although the laws vary significantly in this area as well. Some exempt certain types of entities (for example, financial institutions subject to the Gramm-Leach-Bliley Act (GLBA) or health care entities subject to the Health Insurance Portability and Accountability Act (HIPAA)). Others exempt certain categories of data (for example, data subject to Title V of the GLBA, or protected health information subject to HIPAA). Therefore, it is important to confirm whether the exemption applies to the entity as a whole or to a specific type of data. For example, the Texas law does not apply to financial institutions or data subject to the

GLBA. In contrast, the Oregon law exempts only *information* collected, processed, sold, or disclosed in accordance with the GLBA.

Most but not all of the state privacy laws also contain exemptions for other categories of businesses, such as nonprofit organizations or institutions of higher education. It is important for businesses to be cognizant of these other exemptions and any exceptions to the typical exemptions. For example, unlike most state privacy laws, the Oregon law does not contain a general exemption for nonprofit organizations. The Oregon law exempts public corporations, including the Oregon Health and Science University and the Oregon State Bar, as well as nonprofits established to detect and prevent fraudulent acts in connection with insurance, or those that are engaged in noncommercial activity when providing programming to radio or television networks. Oregon does provide additional time for nonprofit organizations to comply – until July 1, 2025.

## Privacy Policy Disclosures

All data privacy laws require businesses to publish privacy policies that describe how personal information is collected and used. They also generally require privacy policies to disclose whether the business sells personal data to third parties, or processes it for purposes of targeted advertising or profiling. For example, the Oregon law requires privacy policies to include a clear and conspicuous description of any processing of personal data for the purpose of targeted advertising or profiling. But under the Florida and Texas laws, businesses that engage in the sale of sensitive data must specifically include the following disclosure in their privacy policies: “NOTICE: We may sell your sensitive personal data.” Businesses that engage in the sale of biometric data must also specifically include the following disclosure in their privacy policies: “NOTICE: We may sell your biometric personal data.”

## Data Subject Rights

Data subject rights commonly granted by state consumer privacy laws include the right to know and access, right to correct, right to delete, right to data portability, and right to opt out of the sale of personal data, targeted advertising, or profiling. Oregon grants consumers an additional right to obtain a list of specific third parties to which a business has disclosed personal data. The Florida law also includes a right to opt out of the collection or processing of sensitive data, as well as the right to opt out of the collection of personal data collected through the operation of a voice recognition or facial recognition feature.

## Definition of “Sensitive Data”

Many state privacy laws define “sensitive data” to include personal data revealing an individual’s racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship or immigration status, as well as genetic or biometric data processed for the purpose of uniquely identifying an individual, the personal data of a child, and precise geolocation data. The definition of sensitive data

in the Oregon law also includes a consumer's national origin, status as transgender or non-binary, and status as a victim of crime.

## Looking Ahead

As more state consumer privacy laws come into effect over the course of the next couple of years, businesses should carefully consider whether they are covered and adjust their privacy compliance programs to account for the different requirements and nuances in the applicable laws. The Montana Consumer Data Privacy Act will become effective in October. Other states with privacy laws coming into force within the next several years include Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, Rhode Island, and Tennessee. These laws contain many of the same major features found in the eight laws that are already in effect, but there are slight differences and nuances that can have a significant impact on applicability and requirements. As more states enact data privacy laws, keeping track of the differences will be an important, and in some ways, challenging exercise in developing and maintaining an adaptable compliance program. Furthermore, the possibility that Congress will pass a comprehensive federal privacy law anytime soon seems unlikely. [On April 7](#), U.S. Senator Maria Cantwell, Chair of the Senate Committee on Commerce, Science and Transportation, and U.S. Representative Cathy McMorris Rodgers unveiled draft legislation for the American Privacy Rights Act. There have been some updates to the draft since as well as a Senate Commerce Committee [hearing](#) on the "Need to Protect Americans' Privacy and the AI Accelerant". However, significant hurdles remain, and we do not anticipate a federal data privacy law passing this year.

### About the Authors

[Carolyn Ho](#) and [Sarah Rugnetta](#) are New York-based attorneys at Constangy, Brooks, Smith & Prophete LLP and members of the firm's Constangy Cyber Team, which may be reached at [cyber@constangy.com](mailto:cyber@constangy.com).







## The First 10 Days of a vCISO'S Journey with a New Client

By Pete Green, Reporter for Cyber Defense Magazine

“In a quaint village nestled between rolling hills and dense forests, a young apprentice named Eli was learning to throw pottery from a master potter. On the first day by the riverbank, the master potter emphasized nature's lessons of patience and persistence, likening flowing water to the dedication needed to shape clay – and the growth of the flowers along the river bank to the growth of the apprentice's skill.

Observing nature, Eli noticed seeds sprouting and plants growing, reflecting on how skills require care and attention to flourish. Inspired, Eli practiced diligently, learning from every detail and mistake, much like nature's way of evolving. He practiced every waking hour. By the tenth day, Eli's hands moved with a fluid grace, transforming raw clay into beautiful pottery.

As they admired the sunset, the master potter smiled, noting that true mastery lies in embracing each moment of learning, akin to nature's continuous cycle of growth and adaptation, and in only ten days, Eli had blossomed, understanding the rhythm of patience and evolution.”

What can truly be accomplished in ten days? Could an apprentice truly become a master in that time or is ten days a metaphor for a lifetime of work?

This question probes the nature of mastery and growth, suggesting that while substantial progress can be made in a short period of time, true mastery often represents a longer journey.

Becoming a master in any field typically requires years of dedication, practice, and experience. The ten-day timeframe in the parable can be seen as a metaphor for the concentrated effort and accelerated learning that can happen when one is fully immersed in a task. But it somehow also symbolizes how significant growth and transformation can occur in a short period when one is highly focused and guided by an experienced mentor. True mastery is a lifelong pursuit that extends beyond a brief, intense period of learning.

So is it with the vCISO. A vCISO can transform their skillset through periods of intense learning, enabling them to stay ahead of emerging threats, adopt the latest security technologies, and continuously refine their strategic approach to cybersecurity. But it is up to the vCISO to spend the time and effort in becoming the greatest possible resource for an organization.

Countless books and articles detail the path to becoming a successful CISO or virtual CISO, but this writing does not aim to cover all those necessary qualities. Instead, it focuses on the most valuable activities that can be undertaken within a critical two-week (10 working day) period to significantly enhance an organization's security. While an experienced vCISO must develop skills over a lifetime of work, the “10 days” parable may be an indicator of how intensive his or her learning curve - which perspective will show through with the right vCISO.

## Budget of Time

The virtual Chief Information Security Officer is working on a budget of time. The vCISO is unlike a full-time CISO in that there is a time-boxed border around the work the vCISO does as a contractor and therefore, time is of the utmost importance. Every day of engagement must “move the needle” and the first 10 days can provide a good measuring stick of how the engagement will go over the long term.

## 10 Days Before Engagement Starts

To effectively vet a vCISO before starting an engagement, an organization should undertake a comprehensive evaluation process. First, the organization should clearly define its specific needs, objectives, and expectations, identifying key areas such as risk management, compliance, incident response, or security strategy development.

Verifying the vCISO's credentials and experience is crucial, including checking for certifications like CISSP, CISM, GIAC, CRISC, CEH or CISA (amongst others) and reviewing their professional background in similar industries or organizational sizes. Evaluating their expertise and skills through technical interviews or assessments helps gauge their problem-solving abilities and technical proficiency. Requesting case studies and references from past clients or employers provides insights into their performance, reliability, and professionalism.

Furthermore, assessing the vCISO's communication skills and cultural fit is essential to ensure they can articulate complex security concepts to non-technical stakeholders and collaborate effectively with executive leadership teams as well as technical teams.

Reviewing contractual terms and service level agreements (SLAs) ensures that the scope of work, deliverables, and engagement terms align with the organization's expectations. Arranging an initial consultation or project kick-off allows the organization to discuss its current security posture, challenges, and goals, providing an opportunity to evaluate the vCISO's approach to problem-solving and strategic planning.

Additionally, verifying the vCISO's legal and regulatory knowledge ensures they understand relevant requirements such as GDPR, HIPAA, NYCRR, CCPA/CPRA, and industry-specific standards, and their experience in ensuring compliance and handling regulatory audits.

Confirming the vCISO's availability and commitment to dedicating sufficient time and resources to the engagement is crucial, as is ensuring their commitment to continuous learning and staying updated with the latest cybersecurity trends and threats.

Finally, performing a trial engagement can provide a practical assessment of their performance and fit within the organization before committing to a longer-term contract. By thoroughly vetting a vCISO through these steps, an organization can ensure they select a qualified, experienced, and compatible security leader who can effectively enhance their cybersecurity posture.

## Day 1

On day one, a vCISO should focus on laying a solid foundation for their role by engaging in critical introductory tasks.

The day begins with meeting key stakeholders, including executives, IT leaders, and security team members, to understand their expectations and establish effective communication channels. This helps the vCISO get acquainted with the organization's culture, mission, and values, ensuring that their security strategy aligns accordingly.

Reviewing existing security policies, procedures, and incident response plans is essential to comprehend the current security posture and identify immediate gaps or concerns. Additionally, examining recent security audit reports, risk assessments, and compliance documentation provides insights into past and present security issues.

Gaining a high-level overview of the organization's IT architecture, including networks, systems, applications, and data flows, allows the vCISO to identify key assets, critical data, and potential high-risk areas requiring immediate attention.

Conducting a preliminary risk assessment to pinpoint the most pressing threats and vulnerabilities, and prioritizing these risks based on potential impact and likelihood, sets the stage for a more detailed analysis later. Addressing any urgent security issues or vulnerabilities that require immediate action helps establish short-term goals and objectives for the first week, ensuring quick wins and building momentum for longer-term initiatives.

Finally, developing a communication plan to keep stakeholders informed about the vCISO's activities, findings, and progress, and scheduling regular check-ins and status updates, ensures transparency and



builds trust with the team. By focusing on these tasks, a vCISO can quickly get up to speed with the organization's security landscape, establish critical relationships, and lay the groundwork for effective security management.

## Days 2 – 5

On days 2 to 5, a vCISO should focus on conducting a thorough assessment and laying the groundwork for a strategic cybersecurity plan to ensure a successful engagement. On day 2, the vCISO should continue with in-depth meetings with key stakeholders across various departments to gather insights into the organization's critical assets, ongoing projects, and specific security concerns. This includes collaborating with IT, legal, compliance, and risk management teams to understand their perspectives and requirements. Additionally, the vCISO should review and analyze existing security policies, procedures, and incident response plans to identify strengths and weaknesses.

By day 3, the vCISO should initiate a comprehensive risk assessment to identify and evaluate potential threats and vulnerabilities within the organization's IT infrastructure. This involves conducting vulnerability scans, penetration tests, and reviewing past security incidents to understand the current threat landscape. The vCISO should prioritize these risks based on their potential impact and likelihood, creating a risk register that will serve as a foundation for future security initiatives. Concurrently, the vCISO should start mapping out the organization's compliance requirements, ensuring that all regulatory and industry standards are being met.

On day 4, the focus should shift to developing a strategic cybersecurity roadmap. This roadmap should outline short-term and long-term goals, addressing the most critical risks identified during the assessment. The risks identified should be captured and tracked in the risk register to follow the progress around the risks.

The vCISO should propose actionable steps and recommend specific technologies, policies, and procedures to enhance the organization's security posture. This plan should also include a timeline and resource allocation (including a RACI chart to indicate who is Responsible, Accountable, Consulted, and Informed), ensuring that the organization can realistically achieve these objectives. Engaging with the executive team to present and refine this roadmap is crucial for securing buy-in and support.

By day 5, the vCISO should begin implementing immediate, high-priority actions from the strategic roadmap. This could include quick wins such as updating critical software, enhancing endpoint security, or implementing stronger access controls.

Additionally, the vCISO should establish a regular communication cadence with stakeholders, including setting up weekly or bi-weekly meetings to provide updates on progress, discuss challenges, and adjust plans as needed.

Building a strong foundation of trust and collaboration with the team is essential for the ongoing success of the engagement, ensuring that everyone is aligned and committed to improving the organization's cybersecurity resilience.

## Days 6 – 10

On days 6 to 10, a vCISO should focus on deepening their engagement with the organization and ensuring the initial groundwork is effectively translated into actionable steps.

During this period, the vCISO should begin implementing the strategic cybersecurity roadmap developed earlier, prioritizing key initiatives such as enhancing network security, establishing robust access controls, and fortifying data protection measures.

Collaboration with IT and security teams is crucial to ensure these measures are implemented smoothly and effectively. The vCISO should also enable training sessions and awareness programs to educate employees about cybersecurity best practices, fostering a culture of security within the organization.

Additionally, setting up continuous monitoring and incident response mechanisms is vital for proactive threat detection and management. Regular check-ins with executives and stakeholders to provide updates on progress, discuss any challenges, and refine strategies ensure alignment and support for ongoing initiatives. By the end of this period, the vCISO should have established a clear, actionable security framework, demonstrated quick wins, and built strong relationships with the team, paving the way for a successful engagement.

## 10 Days and Beyond

The first 10 days of a vCISO engagement are the most critical because they set the foundation for the entire cybersecurity strategy and establish the tone for future collaboration. During this period, the vCISO conducts essential assessments, identifies key vulnerabilities, and prioritizes immediate actions to safeguard the organization's assets.

By quickly building trust, aligning with the organization's goals, and demonstrating expertise, the vCISO can effectively lead the team towards a robust security posture. This initial phase is crucial for establishing momentum, fostering a proactive security culture, and ensuring long-term success in mitigating cyber risks.

What can be accomplished in the vCISO's first 10 days that could help put the organization on a new path – or, if not accomplished – may signal the need for a new vCISO candidate, organization, or methodology to replace the one that's not being properly managed? These questions need to be asked in order to determine whether or not success can be achieved and measured in quantifiable and qualifiable ways through various Key Performance Indicators (KPIs).

## Success or Failure

If a vCISO does not perform the necessary activities in the first 10 days—such as conducting thorough assessments, engaging with key stakeholders, developing a strategic cybersecurity roadmap, and addressing immediate high-priority risks—it may suggest a misalignment with the organization's needs and objectives.

This initial period is critical for establishing a solid foundation, and any significant missteps or delays could jeopardize the organization's security posture. In such cases, it might be necessary to consider replacing the vCISO to ensure the organization is protected and that a more suitable candidate is in place – someone who can effectively manage and enhance the cybersecurity program.

The first 10 days of a vCISO engagement are critical because they set the stage for the organization's entire cybersecurity strategy. During this period, the vCISO conducts a comprehensive assessment to identify vulnerabilities, engages with key stakeholders to align security efforts with business objectives, and develops a strategic roadmap to prioritize actions and resources. Immediate attention to high-priority risks demonstrates effectiveness and builds trust, while establishing governance and policies ensures a strong framework for ongoing security management.

Successfully executing these tasks within the initial days not only enhances the organization's security posture but also signals the vCISO's capability to lead effectively. The parable of the potter's apprentice is a way to visualize the effort that needs to be put into the practice of becoming an effective vCISO. Failure to achieve these objectives may indicate misalignment, lack of direction, or inadequate risk management, necessitating a reassessment of the vCISO's approach or the overall strategy within 10 days.

### About the Author

Pete Green is a Reporter for Cyber Defense Magazine and a well-respected Cybersecurity Expert. Pete Green has over 20 years of experience in Information Technology related fields and is an accomplished practitioner of Information Security. He has held a variety of security operations positions including LAN / WLAN Engineer, Threat Analyst / Engineer, Security Project Manager, Security Architect, Cloud Security Architect, Principal Security Consultant, Manager / Director of IT, CTO, CEO, and Virtual CISO. Pete has worked with clients in a wide variety of industries including federal, state and local government, financial services, healthcare, food services, manufacturing, technology, transportation, and hospitality.



Pete holds a Master of Computer Information Systems in Information Security from Boston University, an NSA / DHS National Center of Academic Excellence in Information Assurance / Cyber Defense (CAE IA / CD), and a Master of Business Administration in Informatics.

Pete can be reached online at [pete.green@cyberdefensemagazine.com](mailto:pete.green@cyberdefensemagazine.com), [@petegreen](https://www.linkedin.com/in/petegreen), <https://www.cyberdefensemagazine.com>.





## SEC Cybersecurity Disclosure Rules – Are CISOs Ready to Go Beyond the Tip of the Iceberg?

By Brian Levin, Chief Customer Officer, Panaseer

It's been more than six months since the SEC's updated [Cybersecurity Disclosure](#) rules came into force. These rules represent a sea change for CISOs; both in terms of the burden of additional cybersecurity reporting, and the threat of legal action for providing reports that turn out to be inaccurate or misleading.

The CISO's role is in the middle of a generational shift. While not solely responsible for organizations' risk posture, CISOs need to work with disclosure teams and accurately portray risk posture and security processes to the Enterprise Risk Management (ERM) team and the board. CISOs need to understand and communicate their company's cybersecurity practices clearly, with a data-driven approach that enables factual filings. Understanding the SEC's new rules, and what they mean for reporting, will be a critical part of this.

## The hard numbers

Listed enterprises now need to make sure their 10-K filings – comprehensive annual reports of critical information including financial performance – and 8-K filings – reports announcing major events shareholders should know about – accurately portray cybersecurity posture. In particular, 8-K filings need to be made for “material cybersecurity incidents”, and in a timely fashion, i.e. within four days of determining whether the incident was “material”. The question is, what do these new requirements mean for the volume of reporting?

[Analyzing](#) SEC cyber disclosures from the first half of 2024, and comparing to the same period in 2023, we found that mentions of NIST (National Institute of Standards and Technology) and variations had increased by almost 14 times year-on-year: from 221 to 3,025. Given the pattern of filings in 2023, and that it seems almost every listed company now feels the need to disclose its security posture, we’d expect this to increase to nearly 20 times by the end of the year.

However, at the other end of the scale, the number of relevant 8-K filings seems surprisingly low. Across [more than 4,000](#) listed companies in the US, only 17 experienced a potentially material cybersecurity incident. And of those, none would say that the incident was, in fact, material.

## The buck stops here

It might seem unlikely that, in a world where we are constantly bombarded with news of catastrophic cyberattacks and data breaches, less than half of one percent of listed companies have suffered an incident they believed could have been “material”. But as the regulatory environment becomes increasingly complex, these statistics lay bare the increasing pressure being put on CISOs.

First, there is the burden of additional reporting – both from 8-Ks and from the additional detail needed in 10-Ks. CISOs might not be directly responsible for compiling reports, but they’ll need to work closely with the ERM team to ensure reports are accurate. This means ensuring factors such as the relevant expertise of people managing and assessing risk, like CISSP accreditation, and the relative exposure of critical systems, are accurately represented. This is a challenge for a role that, traditionally, has had to rely on data from disparate tools with no single, trusted view to build an often-fragmented picture of its environment. While Business Intelligence and analytics tools have been commonplace in finance, sales, and leadership for decades, CISOs are still forced to work with one hand tied behind their back, and a sword of Damocles hanging over their heads.

That sword is the threat of legal action. Providing reports that are inaccurate or misleading – for instance by giving investors a false sense of confidence in an organization’s exposure to risk – is tantamount to lying to investors. And as the role held responsible for those reports, CISOs will be directly in the firing line. We’ve already seen CISOs [charged by the SEC](#) for fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities, and this is only likely to increase. Especially if those 8-K reports so far turn out to be significantly underplaying the real level of threat organizations – and their investors – are facing.

## Finding the golden source of truth

Ultimately the SEC's regulations provide greater transparency, and give investors a fuller picture of an organization's cyber risk posture and what they are actually investing in. But this will put some CISOs in a delicate position. While investors will be put off by what they see as a poor posture, the SEC will come down hard on inaccurate reports. Yet this doesn't mean those CISOs are in an unwinnable Catch-22.

Instead, as the stakes keep getting higher, CISOs need a system of record they can trust to ensure they are reporting accurately and in good faith. A unified view of every asset throughout the business – where it sits, who owns it, and who is responsible for its security – will let CISOs turn the lights on. They can sue this contextual data to quantify risk, plug gaps, and tell a story to the board and ERM team in a language they'll understand.

The upshot of this should be a culture of accountability, where CISOs can hold colleagues responsible by translating security into the language of technical and non-technical stakeholders alike. Each will have their own relevant view of the same golden source of truthful data, and CISOs can use this to guide their actions.

CISOs can then protect themselves on all sides: showing they have taken every step to improve risk posture, demonstrating this improved posture to investors, and presenting the most accurate picture to the SEC.

**EDITOR'S NOTE:** Prior to publication of this issue of Cyber Defense Magazine, a major portion of the SEC action was rejected by the Federal District Court. <https://www.msn.com/en-us/money/companies/solarwinds-defeats-part-of-sec-s-fraud-case-over-hack/ar-BB1qedHX>

"The SEC's claim that SolarWinds didn't reveal to shareholders the full scope of the attack was based on "hindsight and speculation," U.S. District Judge Paul Engelmayer wrote. However, the judge let the agency's lawsuit proceed based on other claims SolarWinds made before the attack about its cybersecurity defenses and risks."

### About the Author

As the Chief Customer Officer at Panaseer, a leading cybersecurity analytics platform, Brian Levin leads the go-to-market (GTM) strategy and execution for marketing, sales, and customer success. He has over 15 years of experience in scaling early-stage B2B SaaS companies, achieving growth rates of 30-200% annually at scales from \$4M-\$150M ARR. Brian can be reached online at [LinkedIn](#) and at our company website <https://panaseer.com/>.







## Escalating Cyberattacks in the Healthcare Sector

by Ariel Novak, Vice President, Cybersecurity, PAN

The healthcare sector has become a prime target for cyberattacks, with the frequency and sophistication of these attacks increasing rapidly over the last several months. More than [124 million records](#) were compromised in healthcare hacks last year. This escalation poses significant risks, including the potential for compromised patient data, severe financial losses for healthcare organizations, and – most concerning – disrupted healthcare services. Earlier this year, the Change Healthcare cyberattack, which cost UnitedHealth [\\$872 million](#), may have [encouraged bad actors](#) to target the healthcare industry further, seeking financial gain. The cybersecurity industry is evolving in response to these types of attacks, and healthcare organizations – and the tech industry at large – are adopting new strategies and technologies to protect themselves.

### Why the healthcare sector?

The number of reported cyberattacks directed at American hospital systems [nearly doubled](#) from 2022 to 2023. The healthcare sector is particularly vulnerable to cyberattacks for several reasons. Generating about [30%](#) of the world's data volume, healthcare organizations hold vast amounts of valuable data, including personal health information (PHI), medical records, and financial information. This data is in high demand on the black market because it can be used for identity theft, insurance fraud, and other

malicious activities. [Recent data](#) showed that medical records sell for 20 times more than credit card information.

**Additionally**, the critical nature of healthcare services makes hospitals and clinics prime targets for ransomware attacks since cybercriminals know that disrupting healthcare operations can have life-threatening consequences. This increases the likelihood that the targeted organization will pay the ransom to restore services quickly. Given the sensitivity and importance of healthcare data, healthcare organizations are more likely to pay ransom or extortion demands to regain control over their systems and data quickly. **A [survey](#) found 61% of healthcare IT professionals acknowledged that their organizations have paid a ransom, when the average for all industries is 46%.** When it comes down to it, law enforcement and cybersecurity experts actually advise against paying ransoms, as this can encourage further criminal activity. Additionally, there's no assurance that ransomware groups will restore access to systems after receiving the ransom, or that they won't demand additional payments.

The public trusts healthcare organizations to protect their personal and medical information; a successful cyberattack can severely damage this trust and the organization's reputation, leading to long-term financial and operational consequences. Attackers exploit this vulnerability, knowing that healthcare providers are under pressure to maintain their reputations and provide consistent, quality care. Healthcare organizations must also comply with stringent regulations like the Health Insurance Portability and Accountability Act (HIPAA) in the United States, which mandates the protection of patient data. Non-compliance can result in hefty fines and legal consequences, making healthcare providers even more vulnerable to extortion.

**On the logistical front**, [73%](#) of healthcare provider organizations operate on legacy systems, and this outdated technology can cause them to be more vulnerable to cyberattacks. These older systems often lack modern security features and can be challenging to update or replace due to cost and complexity – making them a prime target for malicious actors.

## What can the healthcare industry do?

Healthcare companies should prioritize robust defenses and investments in technology to prevent cyberattacks from occurring in the first place. Although cyber criminals are evolving quickly, cybersecurity technology, like artificial intelligence (AI) and zero trust architecture, is also developing rapidly to help sectors such as healthcare stay protected. Through these advanced technologies, enhanced encryption, and cloud security solutions, healthcare organizations have increasing opportunities to protect against evolving threats. However, these efforts alone are insufficient to change the trajectory of cybercrime. Protecting the healthcare industry should be a widespread effort involving a law enforcement and legislation.

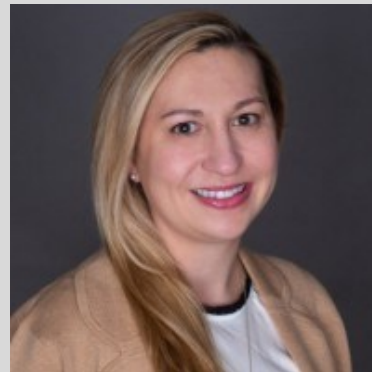
The tech sector has also mobilized to address these threats. Recently, Microsoft and Google [announced](#) they will offer free or discounted cybersecurity services to rural hospitals across the United States, to make them less susceptible to cyberattacks that would disrupt patient care and threaten lives. We're likely to see similar responses from the industry as this problem becomes more and more costly financially and for individuals' well-being.

As cyber threats continue to grow in complexity, the partnership between healthcare providers and cybersecurity professionals will be crucial in safeguarding patient data and ensuring the uninterrupted delivery of healthcare services.

### About the Author

Ariel Novak is the Vice President, Cybersecurity at [PAN](#), a global, integrated, data-driven marketing and PR firm for B2B tech and healthcare brands. At PAN, Ariel has worked with B2B technology brands, with a passion for cybersecurity, including Booz Allen Hamilton, HPE, Citrix, Thales and Vercara.

Ariel began her career as a reporter, receiving an award from the New England Press Association. Her passion for compelling storytelling is evident in her award-winning campaigns helping clients build strong narratives. Ariel is based in Maine and graduated from Bates College.







## It's Time to Sound the Alarm on SMB Cyber Threats

Complacency is imperiling SMBs against 2024's gravest threats. Here's how businesses can start building a meaningful defense.

By Jamie Levy, Director, Adversary Tactics, Huntress

There's an unnerving secret many of us in cybersecurity have noticed. And if you think your company is "too small" to be worried about a potential attack, think again.

As it turns out, small and medium-sized businesses (SMBs) are a new playground for creative adversaries to hone the skills they need before attacking more lucrative, larger enterprises. It's time the cybersecurity community got the word out: the tides have officially *turned*.

SMBs may have once assumed themselves "too small" to attract attackers' attention. But today, SMBs are increasingly attracting adversaries as an ideal testbed environment on their way to larger, more destructive attacks. And disturbingly, SMBs just stand to lose more in a cyber attack:

Some 83% of SMBs are not prepared to recover<sup>1</sup> from the financial damages of a cyber attack

Only 14% of SMBs reported feeling that their cyber attack and risk mitigation plans were highly effective<sup>2</sup>

Around 43% of SMBs do not have any cybersecurity plan in place and 52% don't have any IT security experts in-house<sup>3</sup>

Proof points on the evolving tactics, techniques, and procedures (TTPs) used against these companies are becoming easier to find. And while cyber threats bring a unique level of uncertainty to the SMB segment, one thing is for sure. The SMB segment represents the ideal environment for getting new TTPs “over the threshold” to become effective in larger enterprise environments.

## A Low Bar to Entry

There are a lot of reasons that even small businesses can attract attackers. SMBs may fall below the ideal seat count, budgetary zone, or other parameters for leading cybersecurity solutions or services, leaving them especially susceptible to threats a larger enterprise may be capable of quashing. What's more, SMBs often lack in-house expertise or strong planning for a response.

In industries from manufacturing to healthcare, this SMB threat is playing out before our eyes in headlines and offices across the country. One example we've seen in Huntress research revolves around industrial manufacturing—particularly government contractors, often so small they may only have 5-10 employees. When a government contractor bids on and secures contracts in that space, it is publicly available information and can draw the eye of threat actors. If an attacker can use legitimate tools like remote monitoring and management (RMM) software, a trend we noticed in 2023 at Huntress, they can be hidden in such an SMB's system and ready to unleash chaos at a moment's notice.

With smaller businesses and smaller budgets for hardening systems against attackers, threat actors see the ideal “easy prey” they're looking for to leverage legitimate tools, remain hidden, and build their campaigns before deploying in larger enterprises. Whether by using a ScreenConnect vulnerability like we saw plaguing businesses in early 2024 or other tools like Cobalt Strike, it's clear that SMBs must be on the watch for malicious entities operating within their legitimate systems and tools.

## Use, Discard. Rinse, Repeat.

What's so frustrating for teams like the one I lead at Huntress, is how SMBs are targeted and sustain widespread financial and reputational damage. Then, just as quickly as the threat arrives, it may move on to larger enterprises who stand a much better chance of surviving the attack. We've seen this pattern take place in smaller healthcare settings, another prime target Huntress observed malicious threats plaguing in 2023 and into 2024.

In the February 2024 hack of Change Healthcare, a smaller subsidiary of healthcare giant UnitedHealth, a lack of basic security controls<sup>4</sup> led to the disruption of healthcare systems across the country. And it began in the same place many SMB attacks do: a lack of good security controls, and not enough expertise to know where they were lacking. Change Healthcare's technology—which is used to process billions of

insurance claims each year—was taken down in a ransomware attack that happened simply due to a lack of multifactor authentication (MFA), a basic security control that enhances endpoint security<sup>5</sup>.

At Huntress we have seen some variants of malware and ransomware popping up that are newer or even homemade. And SMBs, especially in healthcare, are an ideal place to try these variants out. For one thing, these SMBs are an easy target to exploit, sometimes as small as a single physician's office or a smaller chain of dental offices. And once threat actors gain a foothold in that environment, thanks to HIPAA and other requirements, those targets are more likely to give into demands and pay a ransom—leaving the attacker to skip off to their next target.

In 2023, attackers exploited known vulnerabilities early on, such as MOVEit<sup>6</sup>, 3CX, and ScreenConnect. And very often, they used SMBs as the “sandbox” to try out their tricks before moving onto the enterprise arena. And so, the old cycle of use/discard continues as attackers try out TTPs on SMBs like small healthcare offices and then move on to bigger, greener pastures.

And left in the wake? The vulnerable SMBs trying to move forward from a breach.

## Arming SMBs to Fight Back

For SMBs who want to get ahead of the growing threat against them, now is the time to embrace and adopt proven security controls and build endpoint security like never before. As endpoints act as the gateway to an organization's digital environment, 70% of breaches start here<sup>7</sup>. Some useful strategies to help SMBs build better endpoint security and proactively fight threats:

- Implement an asset management tool to help you keep track of all of your endpoints and prioritize security measures for the most critical ones in your infrastructure.
- Embrace auto-patching and make sure systems are regularly updated through a proactive patch management strategy.
- Immediately implement MFA if it's not already in place across your devices and programs/tools.
- Use role-based access controls to align permissions and job responsibilities, performing regular audits to ensure your security is aligned to the principle of least privilege.
- Look at endpoint detection and response (EDR) solutions to help your SMB gain real-time insight and alerts that will empower a stronger response against threats.

SMBs should also be mindful of changes resulting from work-from-home shifts, with more exploits happening thanks to multiple devices on a home network, improperly configured (or just plain old and unsecured) home routers, and personal use of business-owned devices and systems. Proactive SMBs should consider cyber awareness training for their team to build vigilance and knowledge ahead of the threat.

Finally, if an SMB hopes to successfully defend against the fray of attackers they're now vulnerable to, it's time to build a comprehensive security plan to defend your endpoints. And if you're not ready to do that or don't have the in-house talent to achieve that goal, it may be a great time to bring in an MSP or similar partner to help you achieve the security you need in order to keep your business healthy for the long term.



In 2023, the team at Huntress saw clearly that SMBs are and will continue to be an ideal sandbox environment for hackers, simultaneously vulnerable and valuable as a space to develop and test new TTPs. In 2024, it's time to acknowledge that threat, arm SMBs against it, and ensure that in 2025, those businesses are still healthy and operational.

To read more about unique TTPs being leveraged against SMBs, read the [Huntress 2024 Cyber Threat Report](#)

### About the Author

Jamie Levy is the Director of Adversary Tactics at Huntress. She is also a researcher, developer and board member of the Volatility Foundation. She has worked over 15 years in the digital forensics industry, conducting investigations as well as building out software solutions. Jamie is also a co-author of [The Art of Memory Forensics](#), the first book of its kind covering various facets of how to investigate RAM artifacts. Jamie can be reached at our company website here: <https://www.huntress.com/>.





## Beyond Fines: The Real Value of Achieving Cybersecurity Compliance

Why integrating security and compliance is essential for long-term business success

By Colton Murray, Security & Compliance Manager, Allegiant a Crexendo Company

Achieving cybersecurity compliance is often seen as a regulatory necessity, primary to avoid hefty fines and legal repercussions. However, the true value of compliance extends far beyond financial penalties. It is about building trust, enhancing security and fostering a culture of resilience and integrity within an organization. Let's dive into the multifaceted benefits of achieving compliance and why businesses should view it as a strategic advantage rather than a mere obligation.

### Build Trust and Credibility

Compliance with cybersecurity regulations signifies to clients, partners, and stakeholders that an organization takes data protection seriously. In an era where data breaches and cyberattacks make headlines regularly, customers today are more concerned than ever about how their data is handled. Demonstrating compliance with data protection regulations, significantly enhancing a company's reputation. When customers know their sensitive information is safeguarded, their trust in the

organization deepens. This trust can boost customer advocacy, retention and loyalty. In fact, research reveals that 84% of consumers are more loyal to companies that have strong security protocols ([Salesforce](#)).



In a competitive market, being compliant with industry regulations can set a company apart from its competitors. Clients and partners often prefer to engage with businesses that have a proven track record of compliance and data security. This preference can translate into a competitive advantage, enabling compliant organizations to win contracts and expand their market share. Furthermore, compliance can open doors to new business opportunities, especially in sectors that mandate strict adherence to cybersecurity standards.

### Enhance Security Posture

Achieving compliance often requires implementing robust security measures and practices. These measures are not just about meeting minimum standards; they push organizations to adopt best practices in cybersecurity. This proactive approach to security helps in identifying and mitigating risks before they escalate into significant issues. By continuously improving security controls and protocols, organizations can better defend against the evolving landscape of cyber threats.

### Foster a Culture of Security

Achieving and maintaining compliance requires the collective effort of the entire organization. It necessitates ongoing training and awareness programs to ensure that employees understand the importance of cybersecurity and their role in maintaining it. This fosters a culture of security within the organization, where cybersecurity becomes a shared responsibility. A security-conscious workforce is better equipped to recognize and respond to potential threats, thereby enhancing the overall security posture of the organization.

### Operational Efficiency and Risk Management

Compliance frameworks such as GDPR, HIPAA, and CCPA require detailed documentation, regular audits, and stringent data management practices. While these requirements may seem burdensome, they compel organizations to streamline their processes and improve operational efficiency. Effective compliance programs identify potential vulnerabilities and inefficiencies, allowing organizations to



address them proactively. This leads to better risk management and a more resilient operational framework.

## Compliance is less expensive than noncompliance

According to [IBM's 2023 Cost of a Data Breach Report](#), the average cost of breaches increases by nearly \$220,000 when non-adherence to regulations is identified as a contributing factor to a cyber incident.

Cost of a data breach increases by nearly  
**\$220,000** when non-compliance  
is a contributing  
factor to a cyber incident

(Source: IBM's 2023 Cost of a Data Breach Report)



From a financial standpoint, investing in compliance is far more cost-effective than facing the financial repercussions of non-compliance. The costs of non-compliance, such as hefty fines and data breach expenses, are both dreadful and entirely avoidable. By proactively investing in compliance, businesses can safeguard against these penalties and protect their reputation. The question isn't whether compliance is costly, but whether it's as costly as the fines and losses incurred from non-compliance. Can your business afford the risk? The answer is clear: compliance is a wise, necessary investment for long-term security and financial health.

## Conclusion

Cybersecurity threats are constantly evolving, and regulatory requirements are likely to become more stringent over time. By embracing compliance as a continuous process, organizations can future-proof their business against emerging threats and regulatory changes. Staying ahead of compliance requirements ensures that an organization is always prepared for new challenges, reducing the risk of falling behind and facing penalties or breaches. However, the true value of compliance extends far beyond financial penalties. It is about building trust, enhancing security, and fostering a culture of resilience and integrity within an organization so you can remain competitive. This proactive approach not only safeguards sensitive data but also demonstrates a commitment to excellence, thereby attracting and retaining customers and partners. In an increasingly digital world, such dedication to compliance and security becomes a key differentiator.

**Editor's Note: Depending on the jurisdiction, there may be private rights of action available for individuals who are adversely affected by cyberattacks against regulated organizations. In some jurisdictions, compliance with regulatory requirements may not provide a complete defense against such private claims. If in doubt, it is advisable to seek advice from legal counsel.**

## About the Author

Colton Murray is the Security & Compliance Manager Allegiant a Crexendo Company, an industry leading managed service provider of comprehensive cybersecurity compliance solutions. With a career spanning over 4 years in the cybersecurity space, Colton leads a dedicated team focused on implementing robust security protocols and compliance frameworks to safeguard sensitive data and mitigate risks for clients. In his free time, Colton enjoys an active outdoor lifestyle playing golf and working out.

Colton can be reached at our company website <https://allegiantnow.com>





## How Automation Can Help Security Policy Optimization

Why aren't our security policies optimized?

By Erez Tadmor, Field CTO, Tufin

One of the recurring questions we hear from network security leaders is “why aren't our security policies optimized?” The answer, however, is far from simple. The truth is that a myriad of factors converge to create a challenging landscape where optimization becomes a daunting task.

To understand how to solve a problem, you first need to understand what is causing the problem in the first place. That's basic troubleshooting 101 - and it's as true for cybersecurity as it is for any industry.

### Common Security Policy Issues

Let's run down the checklist of common issues that could impact overall security policy adoption and adherence:

- **Volume:** One of the foremost challenges stems from the sheer volume of network security controls. These controls, such as a firewall or security group, are each adorned with hundreds to thousands of access rules. Adjustments become difficult as the rules themselves are often scattered across various locations - and teams have to take into consideration the impact a change to one rule may have on another.



- **Review Processes:** Periodic review of access rules, regardless of whether they protect legacy networks, cloud, or edge environments, is often neglected, rendering the security policies connected to them both stagnant and vulnerable.
- **Out of Process Changes:** Another issue is that team members sometimes make policy modifications without adhering to any controls whatsoever. Adjusting or updating rules outside of the approved process not only undermines the integrity of the security infrastructure as a whole - but also introduces unforeseen vulnerabilities.
- **Urgent Changes:** In the frenzied quest to resolve issues swiftly, changes are sometimes implemented hastily, often without due approval or documentation. Many of these changes are intended to be temporary in nature, but reverting back to the original rules after the fact rarely happens. Taking a "band-aid" approach to adjusting security policy only exacerbates the larger problem, creating clutter and leaving the system susceptible to exploitation as urgent changes are not documented well, forgotten forever, or have unintended consequences.
- **Documentation:** Proper documentation is seen as a chore, and is either sorely inadequate or relegated to an afterthought. Security teams are forced to grapple with the task of identifying and rectifying misconfigurations or vulnerabilities - often at times when speed is critical. A lack of information not only slows them down, but can hinder their ability to accurately understand the situation. Conducting audits or confirming regulatory compliance without accurate, updated information is also a nightmare for security teams.
- **Fear:** A prevailing fear of disrupting the status quo inhibits teams from removing redundant or conflicting rules. Because there is so little knowledge or documentation about existing rules, the possibility of inadvertently causing application or network outages looms large. Proactive rule optimization efforts are often abandoned out of fear, or left to become "the next person's problem." While the saying goes "if it ain't broke, don't fix it," - an accumulation of unnecessary rules clutters the security framework, compounding its inefficiencies, and opening companies up to other problems in the future.

Any one of these could be the cause for security policy optimization challenges, and lead to organizational security issues that result in a breach or attack. The truth of the situation is that many organizations have several of these issues impacting their policies and rules - at the same time. With stagnant security budgets and the ongoing battle for organizations to find and retain cybersecurity talent, it is easy to see how these issues can snowball if left unaddressed for too long. No one likes to clean up after the party.

It is also easy to see that security teams need help in order to overcome these issues and establish a lean and efficient security policy. That's why embracing automation is so important. Automation is a must-have for today's organizations; without it, teams find it impossible to catch up and work on truly optimizing their processes.

## Embracing Automation - Critically Important, But Often Not Enough

Security automation is often seen as the solution for the need to get more out of existing resources, while still being able to fight the good fight against attackers. But just implementing automated tools is not enough; to truly address the problems above once and for all and optimize your security policies there are specific best practices to follow.

Let's take a look at these steps and what is needed for each:

1. **Identification:** Identification is the true beginning of security policy automation. Organizations must meticulously catalog their existing security policies, unraveling the intricate web of rules and controls to understand what is connected to what - and most importantly, why. A comprehensive audit serves as the foundation upon which subsequent optimization efforts are built.

That said, visibility simply isn't enough to be impactful by itself. There has to be an automated insight platform that can help identify, in a timely manner, the various policy aspects that need to be optimized. For example, automation could identify unused or unneeded rules that hinder optimization and could be eliminated, but wouldn't have been noticed by teams because of their lack of use.

2. **Continuous Policy Assessment:** Following the identification phase, assessment becomes imperative. Enterprises must scrutinize each policy, evaluating its relevance, effectiveness, and compliance with regulatory standards. What exactly is needed, what isn't, and what is missing. This critical appraisal unveils both vulnerabilities and inefficiencies, paving the way for targeted mitigation strategies and helping to establish a practice of continuous compliance. It's not all doom and gloom, however. The process also can help teams understand what is working well - and should be continued or repeated.
3. **Proper Policy Definition:** The guardrails you set up to track access and potential policy violations need to be accurate, to ensure that all deviations are captured and can be addressed. Without accuracy in definitions and rules, it becomes impossible to capture everything that's potentially dangerous, thereby further limiting optimization efforts.
4. **Mitigation:** Mitigation is when organizations work to rectify identified shortcomings and fortify their security posture. Actions include streamlining policies, eliminating redundancies, maintaining policies that work, and bolstering defenses against emerging threats. It is important for organizations to remain vigilant and understand that their actions here will establish the foundation for future policies.
5. **Tracking and Reporting:** Equally vital is the tracking and reporting of progress. Enterprises must deploy robust monitoring mechanisms to gauge the success of their automation endeavors - and to give them the documentation needed to explain decisions and revert changes if necessary. Transparent reporting also helps to ensure accountability and facilitate informed decision-making now and in the future.

By adhering to these best practices, an organization can put themselves in the best possible position for automation efforts to truly make a difference when it comes to security policies.

## Looking Ahead

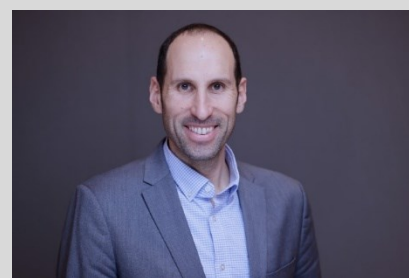
Once an organization has corrected their past security policy mistakes and established a true, streamlined, and efficient set of rules and processes, the next battle becomes keeping it that way. As any security team member knows, this is often easier said than done.

To retain their newfound security policy efficiency, enterprises must cultivate a culture of proactivity. Regular audits, periodic reviews, and stringent documentation practices are non-negotiable moving forward. In addition, collaboration within the organization is key, so needed policy changes or issues can be identified and corrected without creating a new set of issues. Organizations must also understand that policy needs will constantly evolve - as do security threats. Security policy optimization needs to become a continuous process, where new technologies and employee needs are recognized with approved policy adjustments, not ad hoc changes.

By embracing automation and adhering to a systematic approach, organizations can navigate policy issues with confidence. A culture of proactive policy management and continuous refinement will give employees the access they need to be successful, and ensure defenses remain strong in the face of ever-evolving threats.

### About the Author

Erez Tadmor is the Field CTO of Tufin. He holds a two-decade career in the ever-evolving information security field, marked by his diverse background in managing various product portfolios and verticals. His expertise spans cloud and network security, automation & orchestration, IAM, fraud detection and prevention. As Tufin's Field CTO, he bridges the gap between customers, marketing, and product teams, educating stakeholders on network security technologies, cybersecurity best practices and Tufin's solutions. Erez holds a track record of strong leadership in both enterprise and startups cybersecurity product management and strategy development. Erez can be reached online at [erez.tadmor@tufin.com](mailto:erez.tadmor@tufin.com) and at our company website <https://www.tufin.com/>.







## The Role of Intelligence in Cyber Threat Response

By Kurt Xavier Schumacher, Product Manager, MONITORAPP

### 1) The Reality of Cybersecurity Threats and Response

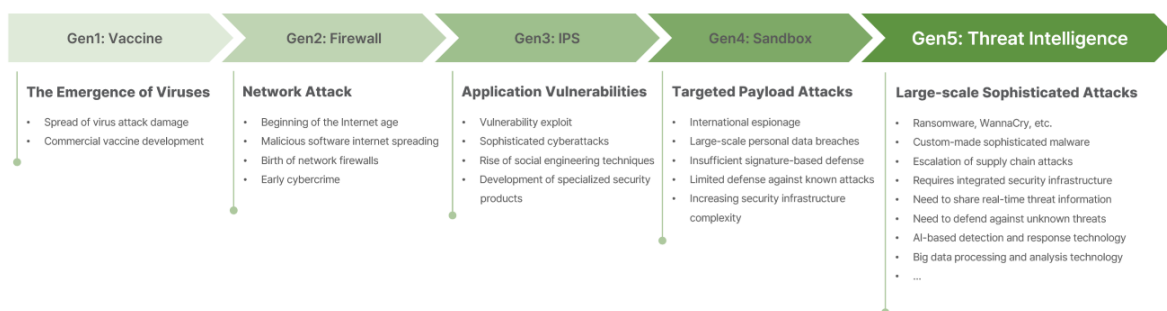
As technology develops and digitalization progresses, cybersecurity threats are becoming increasingly diverse and sophisticated. As a result, responding to these cybersecurity threats has become one of the most critical priorities for modern society.

Advances in modern technologies, such as artificial intelligence, big data, and cloud computing, have revolutionized our lives and business operations. However, on the other hand, these advancements have also provided cyber threat actors with new tools and opportunities, significantly increasing the complexity and frequency of cyber threats. The economic and security impacts of these threats are expected to continue rising.

In recent years, we have witnessed several high-profile cyber incidents. In 2021, vulnerabilities in open-source Log4J and Microsoft Exchange Server were exploited extensively; in 2022, the focus shifted to combating a surge in ransomware attacks; and in 2023, there were reports of cyberattacks using generative AI, including ChatGPT, to develop new threat tools.

The landscape is continuously evolving, and Cyber Threat Actors are now said to be leveraging generative AI to improve their attack tools rapidly. Despite generative AI's built-in safeguards, attackers have found ways to create malware by breaking down the development process into smaller and more manageable tasks to exploit these programs. This has led to the rapid emergence of previously unknown threats.

Putting things into context, the evolution of the cybersecurity landscape can be categorized into five generations:



1. The first generation – Vaccine: The advent of computers and the emergence of viruses, which were effectively countered by antivirus solutions.
2. The second generation – Firewall: The appearance of firewalls in the Internet era generated new malware and network attacks.
3. The third generation - IPS: Attackers began exploiting application vulnerabilities.
4. The fourth generation – Sandbox: The realization that traditional signature-based defenses were insufficient as payload-targeted attacks became prevalent.
5. The fifth generation – Threat Intelligence: The current era is marked by large-scale intelligent attacks, ransomware, sophisticated malware, advanced supply chain attacks, and unknown threats. This generation necessitates an integrated security infrastructure, real-time threat information sharing, and the ability to defend against unknown threats. Threat intelligence plays a crucial role in this defense strategy.

## 2) What Is Threat Intelligence?

Now that we are in the fifth generation of the cybersecurity landscape, threat intelligence has become a fundamental component of the modern organization's cybersecurity strategy. An effective threat intelligence strategy involves continuous collection and analysis of the information needed to identify and respond to threats.

*“Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.”*

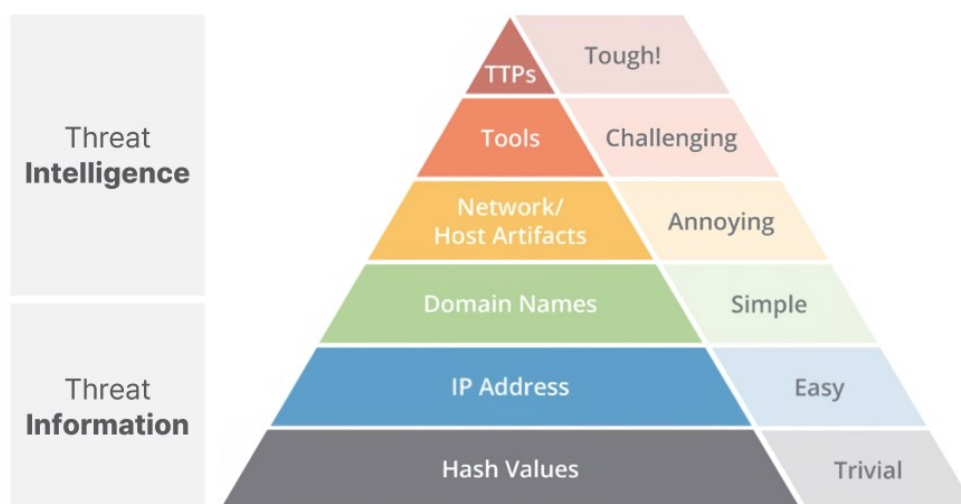
- Gartner -

In other words, threat intelligence is knowledge based on various data and information to respond to threats.

To understand threat intelligence, it is essential to distinguish between “data,” “information,” and “intelligence.”

- Data: Raw, unprocessed metrics such as IP addresses, URLs, and hash values.
- Information: Analyzed and processed data that provides context but may not offer actionable insights.
- Intelligence: The result of analyzing and processing various data points to create meaningful information within a specific context, guiding decision-making and action.

### **The Pyramid of Pain**



The “Pyramid of Pain”, introduced by security expert David J Bianco in 2013, illustrates how different levels of cyber threat indicators impact attackers. The pyramid emphasizes TTPs (Tactics, Techniques, Procedures) as the most effective method of preventing attacks. Blocking lower-level indicators, like hash values, IP addresses, and domain names, imposes minimal stress on attackers while blocking high-level indicators requires them to expend significant effort and resources. Using TTP indicators for defensive measures allows organizations to detect all steps of an attack from start to finish, posing a significant challenge to attackers.

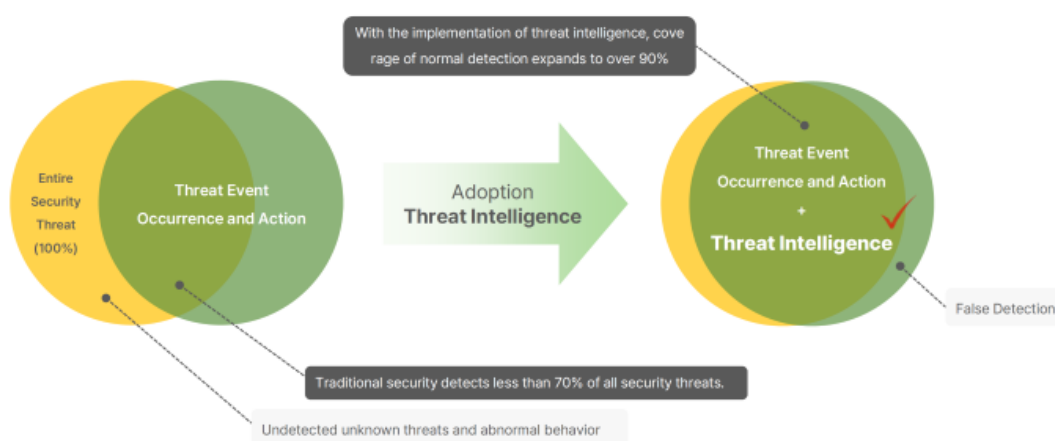


In order to reach intelligence-level threat indicators, the threat intelligence lifecycle is commonly used. The threat intelligence life cycle refers to the process of transforming raw data into actionable intelligence for decision-making through a continuous, iterative process involving requirements, collection, processing, analysis, distribution, and feedback.

- Requirements: Establishing goals and a road map for threat intelligence.
- Collection: Gathering threat information from various sources.
- Processing: Preprocessing collected data into a format suitable for analysis.
- Analysis: Deriving answers for requirements.
- Distribution: Sharing analyzed results.
- Feedback: Receiving feedback on the distributed results.

This life cycle helps organizations systematically manage the collection, analysis, sharing, and utilization of threat intelligence to respond effectively to security threats.

The increasing sophistication of cyber threats and the rise of advanced persistent attacks necessitate the integration of threat intelligence into cybersecurity strategies. Existing passive responses based on fragmented data and information appear to be insufficient. Moreover, traditional security measures often detect less than 70% of threats, leaving a significant portion of unknown threats undetected and a portion of threat events likely to be false positives. Applying threat intelligence will help upgrade cybersecurity strategies, reduce false positives, enhance detection, and expand the effective detection area to over 90%.



### 3) AILabs Threat Intelligence Platform

AILabs, developed by MONITORAPP's CTI Division, is an advanced threat intelligence platform that integrates unstructured data from various sources, stores it in big data, and performs multi-dimensional analysis using an AI-based engine.

The platform follows a lifecycle similar to general threat intelligence, involving a continuous and iterative process of requirements, collection, analysis, processing, distribution, and feedback. Its key features include an AI-based analysis and processing system and a web-based portal that provides valuable



threat intelligence and performs proactive threat response, post-analysis, and information sharing of incidents.

Future developments in threat intelligence will likely evolve in various environments, involving further automation, enhanced AI capabilities, big data analytics, and advanced decision-making processes.

Continuous updates and collaboration are essential to keep pace with evolving threats and maximize the effectiveness of threat intelligence. While the nature of threats is changing along with technological advancements, it is crucial to continuously collect and analyze the latest information. In today's digital environment, threat intelligence is not just a tool but a strategic approach that requires integrated efforts to protect against cyber threats.

## About the Author

Kurt Xavier Schumacher is a Cybersecurity Professional working at MONITORAPP, a global cybersecurity company headquartered in South Korea that specializes in Security Appliances, Cloud-based Security Services, and Cyber Threat Intelligence. He is currently working as a Product Manager and Support Engineer and holds multiple industry certifications, such as the CCNA, CompTIA Security+, and AWS CCP.

Kurt can be reached online at [kurt.schumacher@monitorapp.com](mailto:kurt.schumacher@monitorapp.com) and at our company website <https://www.monitorapp.com/>







## Worried about Insider Risk? Pay More Attention to Offboarding

Insider risk in a frontline context: how optimized offboarding can help

By Cris Grossmann, CEO and Co-Founder, Beekeeper

Discussions of insider risk inevitably conjure images of disgruntled IT employees stealing sensitive data from the comfort of an air-conditioned office. However, insider risk is significantly more complex, and any business that fails to account for this complexity is courting potential disaster.

For one thing, insider risk is no longer confined to the cubicle: frontline workers are just as likely to come into contact with — and potentially mishandle — proprietary information. Then there's the fact that many of these insider incidents are not malicious but result from [human error](#). In a frontline context, if someone mistakenly allows an offboarding employee continued access to internal communication channels and company information, the door is left open for that employee and hackers looking for a backdoor into a company's systems.

However they occur, the impact of these insider incidents cannot be overstated. Per a recent report, the average cost of an insider risk event has [skyrocketed to \\$16.2 million](#) in recent years. Working proactively to prevent these events needs to be a central part of any comprehensive security plan.

Businesses know this — many are already taking serious measures to prevent insider incidents. But surprisingly, in all of these discussions, one crucial component of the frontline worker lifecycle has continued to go largely under-discussed: the importance of offboarding.

## Why offboarding matters

For many businesses, offboarding is an afterthought — a matter of sorting out paperwork and adjusting the payroll. In fact, optimized offboarding experiences can be just as central to your business' overall health as optimized onboarding experiences — and are perhaps even more critical when it comes to insider risk reduction.

Again, a substantial proportion of insider risk events have little to do with active malice on the part of employees (current or former) and more to do with inadequate security protocols. Phishing attacks, for instance, are continually on the rise, and without adequate training, any employee — current or former — is potentially susceptible. For example, a hacker can easily pose as someone from your company and ask for sensitive information like old passwords.

How can employers prevent this from happening? First and foremost, organizations need to consider the employee's entire lifecycle and take time to thoroughly remove a departing employee's access to private company data and communications channels. This process is significantly easier for companies that have already taken steps to digitize their frontline workforce. After that, they need to engage in comprehensive post-departure security training. That means ensuring your departing employee knows they will not be contacting them for personal information down the line and that they should forward any such fraud attempts to HR. The benefits of this approach are manifold. Beyond keeping your company's sensitive information safe and secure, hands-on offboarding ensures your employee leaves with a positive impression of the company. This can go a long way towards preventing threat events that are intentional.

## Optimizing the offboarding process

Right now, HR personnel are more stressed than ever — and the offboarding process only compounds that stress. A departing employee, after all, needs to be replaced — and finding the right employee for an open position is perhaps the most challenging part of the job. Juggling the demands of the hiring process with the million micro-tasks of the offboarding process is a recipe for disaster, with HR personnel (understandably) struggling to stay on top of the requisite tasks.

Crucial paperwork often goes unfiled, access controls stay unchanged, and departure protocols are neglected. This is not a reflection on HR personnel, who are doing their best in a tough workplace. However, this situation isn't sustainable and ignoring it has serious implications for insider risk.

Fixing this situation means mending the broken lines of communication between HR personnel and frontline workers — what I call the Frontline Disconnect. And this simply cannot happen until frontline workers have access to frontline-catered versions of the digital HR tools that have so radically overhauled desk-based work in the last decade.

In my time observing countless frontline workplaces, I've been shocked to discover that offboarding procedures have gone unchanged for decades. Where offboarding processes for desk workers have been almost entirely digitized, many frontline workplaces — construction sites, restaurants, warehouses — still live in a pen-and-paper world. Reducing insider risk means bringing frontline work into the 21st century — making life easier for both HR personnel and frontline workers.

Notably, recent technological developments give employers the chance to engage in a kind of pre-offboarding. By deploying mobile surveys and using AI-enhanced sentiment analysis, employers can now determine well in advance when a particular employee might be on the way out and intervene accordingly. If that employee ultimately chooses to leave anyway, they will nonetheless depart with a much more positive relationship to your business.

This speaks to the critical function of empathy in an insider risk context. Even under the best conditions, frontline work can be unbelievably stressful, and employers are incumbent on not letting that negative sentiment transfer over to the company itself. It's a delicate balancing act but an essential one. Given the average cost of an insider incident, getting it right should be a priority.

### About the Author

Cristian Grossmann, the author of *The Rise of the Frontline Worker*, is a tech entrepreneur whose company Beekeeper has raised \$196.5M in funding and supplies its mobile productivity and collaboration platform to some of the world's biggest and best-known organizations, including Heathrow Airport, Domino's Pizza, and Hilton Hotels. Cristian, a former frontline worker himself, understands first-hand the technology that is required to make the frontline workforce more effective. Prior to founding Beekeeper, he worked for Accenture on high profile international projects in the field of IT Strategy for the financial and public sectors. Cristian studied Chemical Engineering and got his Ph.D. in Electrical Engineering, both at ETH Zurich. Before moving to beautiful Zurich, he was born and raised in an entrepreneurial Swiss-Mexican family in Mexico City. Cris can be reached via email at [beekeeper@touchdownpr.com](mailto:beekeeper@touchdownpr.com) and at our company website <https://www.beekeeper.io/company/>.





## How AI-Driven Cybersecurity Offers Both Promise and Peril for Enterprises

By Metin Kortak, Chief Information Security Officer, Rhymetec

Artificial Intelligence (AI) is transforming multiple sectors, driving innovation and enhancing productivity and cybersecurity. The AI market is projected to rise from an estimated \$86.9 billion in revenue in 2022 to \$407 billion by 2027. This technology is reshaping industries and is expected to have a significant economic impact, with a projected 21% net increase in the US GDP by 2030. However, despite its advantages, AI also creates cybersecurity challenges in the hands of malicious actors. Businesses must navigate this complex issue to harness the benefits of AI, while safeguarding against its misuse.

### Recognizing the Threat of Malicious AI

Malicious AI can cause sizable problems for cybersecurity crews. For example, its increased use in phishing attempts is a concern, as it mimics human interaction to craft targeted, convincing phishing emails. Additionally, AI can be used to identify security vulnerabilities that humans may sometimes miss and allow attackers to exploit these vulnerabilities. Many of these threats are currently still theoretical, but they are likely advancing faster than we realize.



## Prioritizing Security in Product Design

In light of the growing threat of malicious AI, embedding cybersecurity principles into product design is critical. Incidents such as the [Samsung data breach attributed to ChatGPT](#) underscore the risks of sidelining security. As AI draws data from multiple sources, businesses must implement AI policies and tools like mobile device management and endpoint protection software to prevent misuse. Prioritizing security from the outset of product development is key to building user trust.

## Achieving Collaboration Among Teams

While dedicated cybersecurity teams are common in enterprise companies, security remains a collective responsibility for all employees. A vigorous approach to security requires collaboration across departments to keep everyone aligned with best practices. Security awareness training is one of the best ways organizations can remind their employees about their responsibilities when it comes to cyber security risks. Paying attention to suspicious emails and protecting corporate credentials are some of the best practices employees may need training on. Dedicated product security managers, working with competent, collaborative teams can ensure companies continuously update their security measures and deploy AI to identify vulnerabilities effectively.

## Guarding Against AI Exploitation

Generative AI tools like ChatGPT have changed how people work and improved productivity, but their ability to simulate human communication poses risks. While no AI-specific security regulations exist yet, initiatives like ISO's AI cybersecurity framework are in the works. Additionally, discussions are taking place about using AI to automate processes like network penetration tests, because it can identify vulnerabilities as well as human experts do. Due to AI's "new" nature, [many organizations are implementing internal AI policies](#) to control how their employees and systems interact with AI. Some are even completely banning the use of generative AI tools to guard themselves against exploitation. These initiatives reflect the industry's commitment to secure AI use.

## Streamlining Cybersecurity with AI Automation

Businesses are using automation more and more for cybersecurity. While tools like AI perform security tasks faster, no automation solution can guarantee 100% accuracy. Over-reliance on automation can lead to assumptions that might not fit every scenario. Regular audits and human oversight are essential to ensure the effectiveness of AI tools.

AI significantly speeds up certain tasks, such as responding to lengthy security questionnaires or RFQs. These can often be long, with some containing over 1000 questions. Businesses can answer these much faster with AI, saving both time and human resources.

In addition, incorporating AI into intrusion detection can enable systems to go beyond simple rule-checking to identify suspicious user behavior and network activity. For example, if a high-privilege user behaves unusually, AI can promptly sound the alert.

## Navigating Compliance and Ethics in AI

As AI-driven security measures become more common, companies must follow existing regulations like GDPR and CCPA. These regulations are designed to protect user data and privacy, and any AI system, including security protocols, *must* adhere to them. AI can benefit cybersecurity only if it does not compromise user privacy or data protection standards. Compliance with regulations safeguards users and protects organizations from potential legal fallout.

Ethical considerations are also paramount for companies implementing AI in cybersecurity. While enforcing information security policies is advisable, it's equally important to ensure employees understand and acknowledge them. This understanding gives organizations a level of assurance. If employees act against the policies, companies have a foundation for actions ranging from disciplinary measures to potential termination.

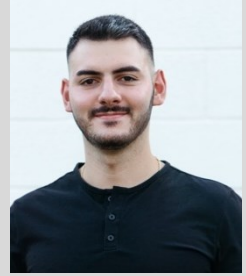
## Anticipating an AI-Driven Cybersecurity Future

A lot is happening that is very exciting. Integrating AI with technologies like IoT and blockchain presents both opportunities and risks. Quantum computing's potential, though still in the early stages, promises computational power that can both bolster AI's capabilities and pose threats if misused. The tech world is abuzz with the potential of deep learning AI and LLMs, especially for automation.

AI's future role in cybersecurity is undeniable, but it offers promise and peril for companies. Enterprise organizations must find a way forward, benefitting from its strengths while staying vigilant against its potential pitfalls.

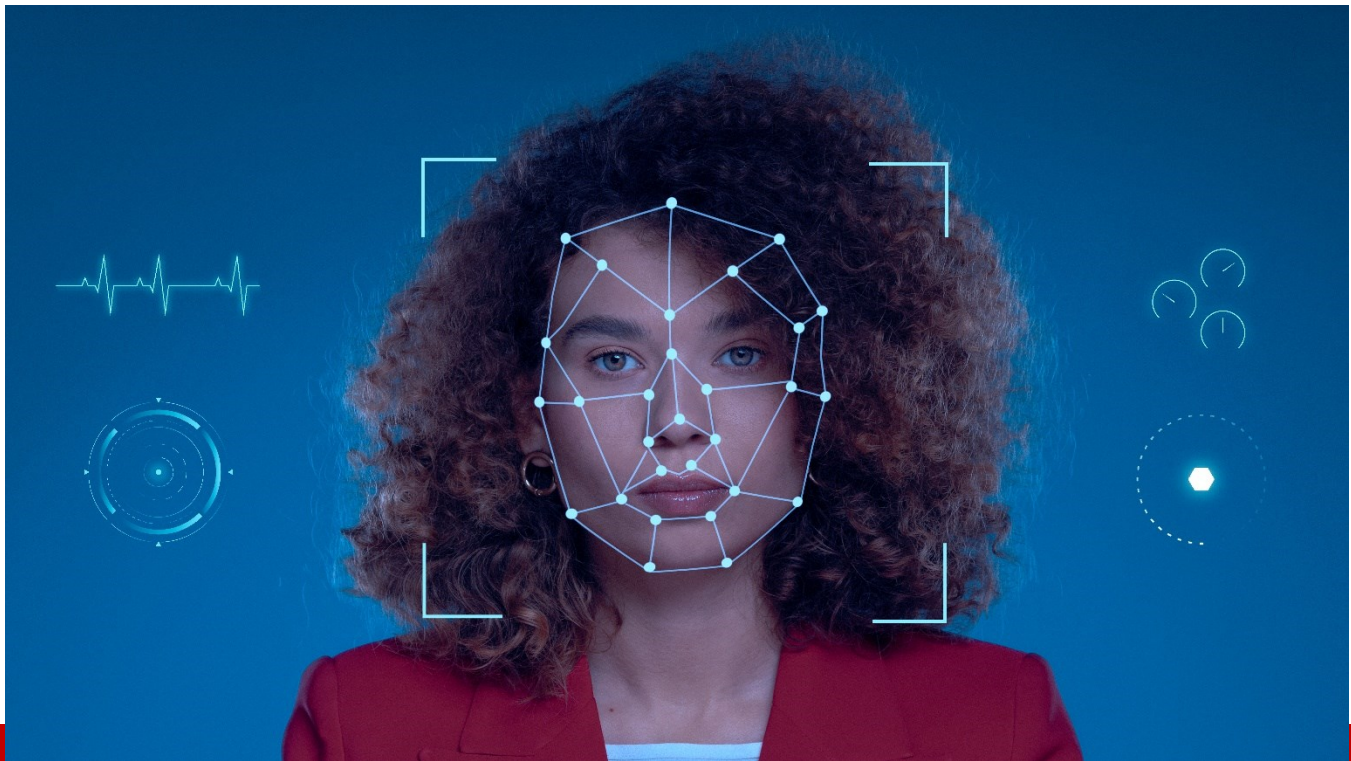
## About the Author

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 as a service offering and 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/>



## NextGen Identity Management

How to Harness Government Standards and Tech Innovations

By Dr. Sarbari Gupta, Founder and CEO, Electrosoft Services, Inc.

Federal agencies face a pivotal cybersecurity challenge: prevent unauthorized entities from accessing systems and facilities, while granting authorized federal employees and contractors access commensurate with verified need. Two factors complicate this objective: (1) relentless efforts by ever-more-sophisticated cybercriminals and (2) myriad agency systems, many antiquated with ill-defined interfaces that rely on outdated defense mechanisms.

Digital modernization and migration to the cloud comprise important responses. Additionally, technological advancements, combined with federal identity, credential, and access management (ICAM) standards and guidelines, offer federal agencies robust identity management tools.

### ICAM Meets Zero Trust

Traditional federal authentication and access control mechanisms relied on perimeter-based trust. Here, users authenticate their identity at the network entry point. Thereafter, the roles assigned to that identity govern further access.

Office of Management and Budget Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, inaugurated a shift to a zero trust architecture (ZTA). Here, trust is not



accorded to any person, non-person entity, system, or network—whether within or beyond the security perimeter. ZTA emphasizes enterprise-level controls, especially phishing-resistant multifactor authentication.

Demand for robust ICAM solutions, complemented by the right mix of standards and policies, is the result. Standards and innovation are the watchwords on our NextGen journey.

## Key Identity Standards Guiding Federal Implementations

The three most important identity management standards for federal agency adoption are:

1. **NIST Special Publication 800-63.** The four-volume publication [Digital Identity Guidelines](#) forms the cornerstone of federal identity management. It prescribes the technical requirements for implementing digital identity in federal agencies and offers processes for risk assessment, assurance level selection, and appropriate controls.

This document combines the best thinking of public and private information security professionals and offers both worlds a risk-based approach to digital identity management. Important enhancements include the infusion of an updated digital identity model, greater process orientation in risk management, and a revised assurance level selection methodology.

2. **Federal Information Processing Standards 201.** [FIPS 201](#) implements the requirements of Homeland Security Presidential Directive 12 relative to Personal Identity Verification (PIV) of federal employees and contractors. It addresses logical and physical access applications with special focus on smart card–based identity credentials.

This mandatory standard, issued by NIST, defines the technical specifications and operational requirements for creating, issuing, and managing PIV credentials, which include smart cards used for accessing federal facilities and information systems.

3. **X.509v3.** [X.509v3](#) is the international standard for issuing and managing PKI identity credentials. PKI facilitates the secure electronic transfer of information by using digital certificates and cryptographic key pairs.

The combination of digital certificates and key pairs based on asymmetric cryptography establishes the trust ZTA requires – sender (user and device) authentication, content authentication (secure data transmission), and non-repudiation.

## Emerging Innovations

Continuous innovation is a feature of the identity management space. While there are far too many advances to cover, every federal ICAM leader should be aware of these technologies:

- **AI.** Artificial intelligence already plays a role in identity and access management, performing a range of critical tasks without human intervention. By all predictions, future applications — especially those relying on generative AI and machine learning — will transform the identity and access management world.

AI offers many benefits. For example, faster pattern recognition can quickly trigger automatic network-protecting measures. On the other hand, AI in the wrong hands – or applied with evil intent – can create threats beyond imagination.

- **Fast Identity Online (FIDO).** Developed by the [FIDO Alliance](#), FIDO is an industry standard for strong, easy-to-use asymmetric cryptography-based identity credentials that are available across popular operating system platforms and browsers.

Derived PIV Passkeys (DPPs) – FIDO2 credentials implemented as derived PIV credentials in accordance with FIPS 201 and NIST Special Publication 800-157r1 – are user-friendly, multifactor, and phishing-resistant authenticators that can be used by federal enterprise users. I recently proposed an authentication model using DPPs for authentication to federal online services. It could represent a leap into modern authentication.

- **Attribute-based access control.** ABAC is a versatile approach for dynamically managing access. Access decisions compare real-time attributes with those assigned to the user, the resource, and the environment and digital policies governing the same.

Many postulate an either-or proposition when it comes to ABAC and role-based access control models. I tend to agree with OMB M-22-09, which suggests that using the two in conjunction offers greater assurance than either model individually.

- **Identity governance and administration (IGA) tools.** Enterprise-level tools that manage digital identities across their lifecycle and control user access across the digital ecosystem via data aggregation and correlation.

Complex digital ecosystems – on-site, cloud, and hybrid – make tracking and reporting on the activities of multiple users, devices, and access requirements across differing environments a manual nightmare. IGA tools apply automation to make risk management and regulatory compliance manageable.

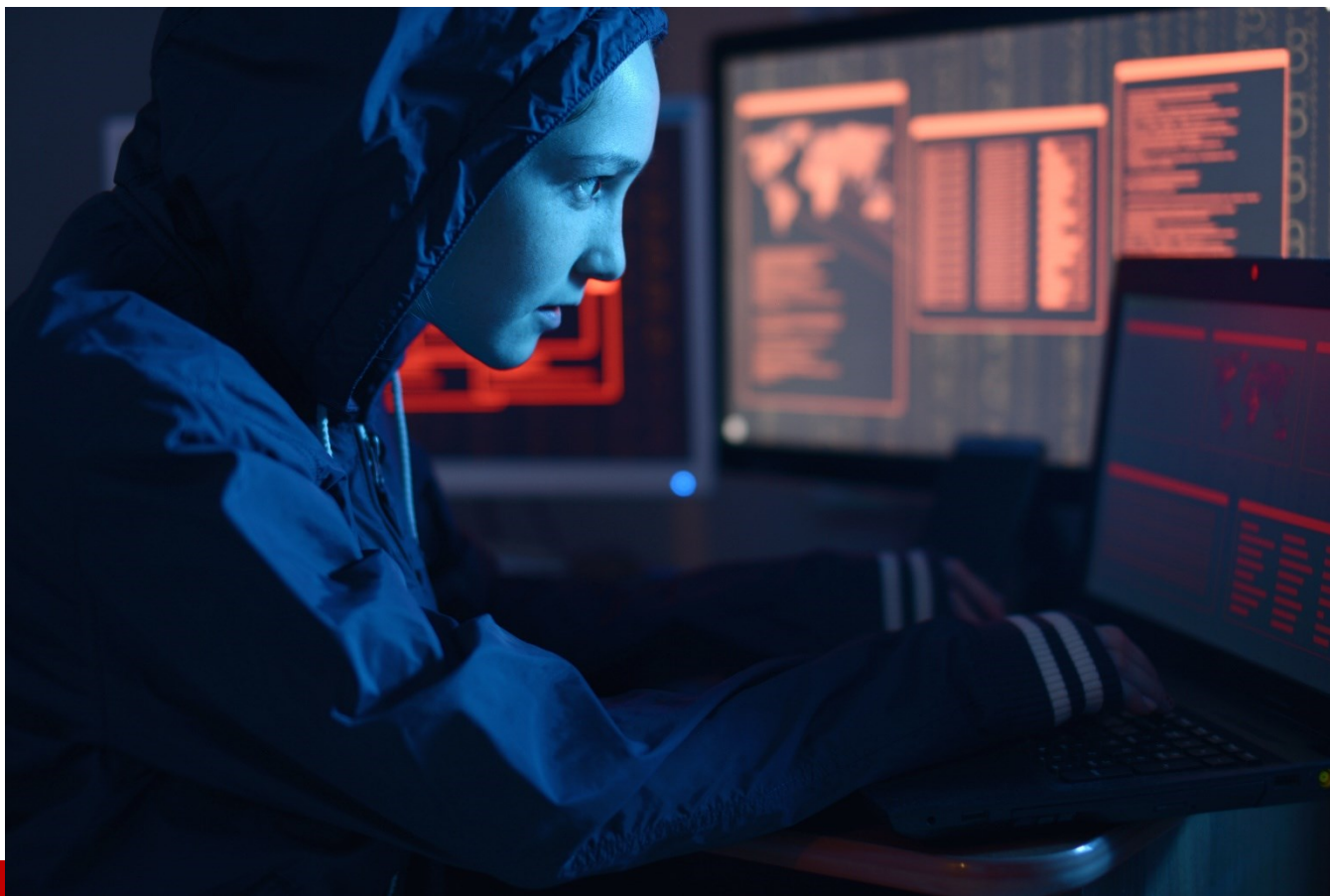
Limitless possibilities attend ZTA implementation. What an exciting time to be part of the federal identity, credential, and access management landscape!

## About the Author

Dr. Sarbari Gupta is the Founder and CEO of Electrosoft Services, Inc. She is a recognized thought leader and speaker on cybersecurity, zero trust, ransomware, ICAM, FIDO passkeys, OSCAL and more. She is an active NIST collaborator and co-author, helping to shape cybersecurity standards and guidelines to improve federal cyber resilience. 2022 was a banner year for Electrosoft, with record revenue and 25% Y/Y growth – and the company is on track for 60% growth in 2023. Dr. Gupta is passionate about STEM education and encouraging women to embrace and stay in STEM fields. She serves as a mentor for Women in Technology (WIT) and is a member of the board of advisors for University of Maryland Women in Engineering (WIE), providing support and mentoring to women entering an engineering field.



Dr. Gupta can be reached online via [LinkedIn](#) and at our company website <https://electrosoft-inc.com/>



## RegreSSHion, Critical RCE Vulnerabilities, and When Should You Be Scared?

By Jonathan Jacobi, CTO Office, Dazz

On July 1st, 2024, the cybersecurity community was rocked by the discovery of a critical Remote Code Execution (RCE) vulnerability in OpenSSH, aptly named regreSSHion. This revelation triggered a frenzy among security teams who scrambled to locate and secure their SSH servers, while security vendors rushed to develop and deploy fixes and detections. The chaos was palpable, underscoring the need for a deeper understanding of such vulnerabilities. In this article, we will explore the nature of RCE vulnerabilities, their potential impact, and how to assess their severity and urgency.

Remote Code Execution (RCE) vulnerabilities enable attackers to execute arbitrary code on a target machine remotely due to a software bug. These vulnerabilities can vary widely in their criticality, influenced by several key factors that you should check, before you panic.

One of the most critical aspects of RCE vulnerabilities is whether they are pre-authentication (pre-auth). Pre-auth vulnerabilities do not require any form of authentication, allowing attackers to execute code without needing to know any passwords, keys, or secrets. This dramatically lowers the barrier to



exploitation. Notable examples include EternalBlue and regreSSHion, which have caused widespread concern due to their pre-auth nature.

Vulnerabilities that require no user interaction, known as "zero-click" (0-click) vulnerabilities, are particularly dangerous. These vulnerabilities can be exploited without the victim doing anything, such as clicking a link or opening a file. Zero-click vulnerabilities are often contrasted with "one-click" or "multi-click" vulnerabilities, which require some degree of user interaction. The FORCEDENTRY exploit for Apple iOS devices is a prime example of a 0-click vulnerability.

The ease with which a vulnerability can be exploited is another crucial factor. While having a public exploit available significantly increases the danger, other factors also play a role. Modern exploits often consist of multiple smaller vulnerabilities chained together, referred to as "primitives." This complexity can make exploitation a challenging "cat and mouse" game between attackers and defenders. Some vulnerabilities rely on rare conditions to trigger, known as statistical exploits. This can lead to Denial of Service (DoS) attacks if the exploit fails, or make exploitation inherently difficult and unreliable.

The impact of an RCE vulnerability is also influenced by the popularity of the affected software. A vulnerability in widely used software like Windows or OpenSSH is inherently more critical than one in a little-known application. For instance, the EternalBlue vulnerability in Windows had a massive impact because of Windows' ubiquity.

How easy it is to patch vulnerability also affects its criticality. Some vulnerabilities can be patched with a simple update, while others might require significant changes to infrastructure or even new hardware. The RowHammer vulnerability, for example, highlighted the difficulties in patching certain hardware-level vulnerabilities. Additionally, vulnerabilities that are exploitable in the default configuration of an application are particularly dangerous, as they affect a broader base of installations. Many users and organizations do not change default configurations, making these vulnerabilities more likely to be exploited.

EternalBlue is one of the most infamous RCE vulnerabilities, affecting Windows SMB functionality in its default configuration. The availability of a public exploit made millions of Windows machines vulnerable, leading to widespread exploitation and significant impact on organizations worldwide. Several factors contributed to its severity: it required only network communication with a Windows machine, making it a 0-click, pre-auth vulnerability. The Shadow Brokers leak included a functioning exploit, lowering the bar for attackers. Windows' widespread use amplified the vulnerability's impact, and patching legacy Windows systems proved challenging, exacerbating the vulnerability's effects.

The regreSSHion vulnerability, discovered in OpenSSH, is another significant pre-auth RCE. Despite its alarming nature, a deeper analysis reveals mitigating factors. OpenSSH is widely used, making any vulnerability in it potentially impactful. regreSSHion is a 0-click, pre-auth vulnerability that affects the default configuration. However, the underlying issue is a race condition, a statistical vulnerability that is hard to exploit reliably. The best-known exploit requires continuous attempts over several hours and is prone to detection by security tools. While a proof-of-concept was quickly available, no fully functioning exploit has been released, and existing ones are highly complex and environment-dependent.

Despite its potential for widespread impact, the complexity of exploiting regreSSHion and the availability of mitigations reduce the immediate risk. Organizations are advised to patch critical assets, prioritizing internet-facing SSH servers.

Analyzing a risk, by understanding its criticality factors (preauth, default config, exploitability, popularity, etc) is the way to tackle the problem of a “new critical vulnerability” incident, in a very efficient way, similarly to how we broke down the EternalBlue and regreSSHion cases to their criticality factors.

Beyond analyzing the criticality and regular patching, a structured response to critical vulnerabilities is essential too. First, identify all affected assets to prioritize efforts, focusing on internet-facing and business-critical assets first. Then, automate patching where possible to ensure swift and effective remediation. Remember, the goal is to avoid panic, assess criticality accurately, and act decisively to protect your organization!

We have broken down RCE vulnerabilities into their criticality factors to provide a framework for assessing their severity. By examining case studies like EternalBlue and regreSSHion,, we have highlighted what makes certain vulnerabilities more dangerous than others. The key takeaway is to stay informed, analyze risks carefully, and prioritize actions to maintain a robust security posture.

## About the Author

Jonathan Jacobi is part of the CTO office at cybersecurity startup Dazz. He focuses on product development and innovation within the company. Coming from a wide background in the cybersecurity field, Jonathan started his college degree in computer science as a 13-year-old, worked as a Vulnerability Researcher at Check Point Research, and was the youngest Microsoft employee as part of Microsoft’s MSRC.

In his military service, Jonathan served in the Elite Israeli Cyber & Intelligence Unit, 8200, in various security research and leadership positions.

Jonathan’s hands-on experience ranges from real-world security research and finding 0-day vulnerabilities to speaking at world-renowned events like TEDx and CCC (Chaos Communication Congress). He is also a Co-Founder of Perfect Blue, ranked as the #1 hacking (CTF) team in the world (2020-2021, 2023). Jonathan can be reached online at [jonathan.j@dazz.io](mailto:jonathan.j@dazz.io) | <https://twitter.com/j0nathanj> and at Dazz’ website <https://www.dazz.io/who-we-are>





## 70% of Enterprises Established SaaS Security Teams, Cloud Security Alliance Survey Finds

By Hananel Livneh, Head of Product Marketing, Adaptive Shield

More than 70 percent of enterprises have prioritized SaaS security by establishing dedicated teams to secure SaaS applications, a trend identified for the first time in the fourth [Annual SaaS Security Survey Report: 2025 CISO Plans and Priorities](#).

In an era where SaaS platforms power a wide spectrum of industries and the threat of SaaS breaches looms large, this is one of many aspects of SaaS security that is taking precedence now more than ever, according to the new survey, released this month by the [Cloud Security Alliance](#) (CSA) and commissioned by Adaptive Shield.

[Download the full SaaS security survey report](#)

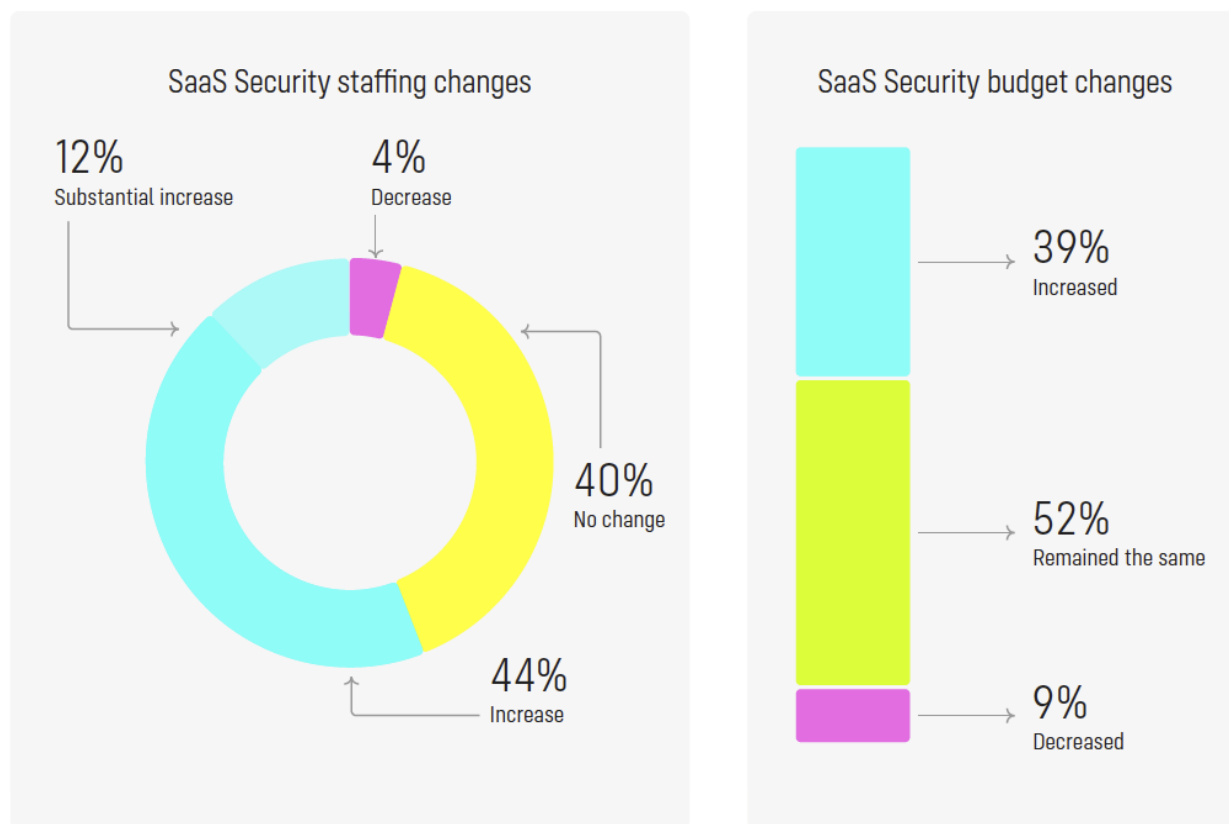
Here are the key findings:

## 1. 70% of Organizations Have Dedicated SaaS Security Teams

Despite economic instability and [major](#) job cuts in 2023, organizations drastically increased investment in SaaS security. In fact, the survey found, enterprises added headcount to SaaS security in 2023, with 56% increasing SaaS security staff.

The emergence of SaaS-specific security roles was identified for the first time in the annual survey: 57% percent reported having a SaaS security team of at least two full-time staffers, while another 13% said they had one person dedicated to securing SaaS applications.

SaaS security budgets are also increasing. The survey found that 39% of organizations increased SaaS cybersecurity budgets in 2023 compared to the previous year.

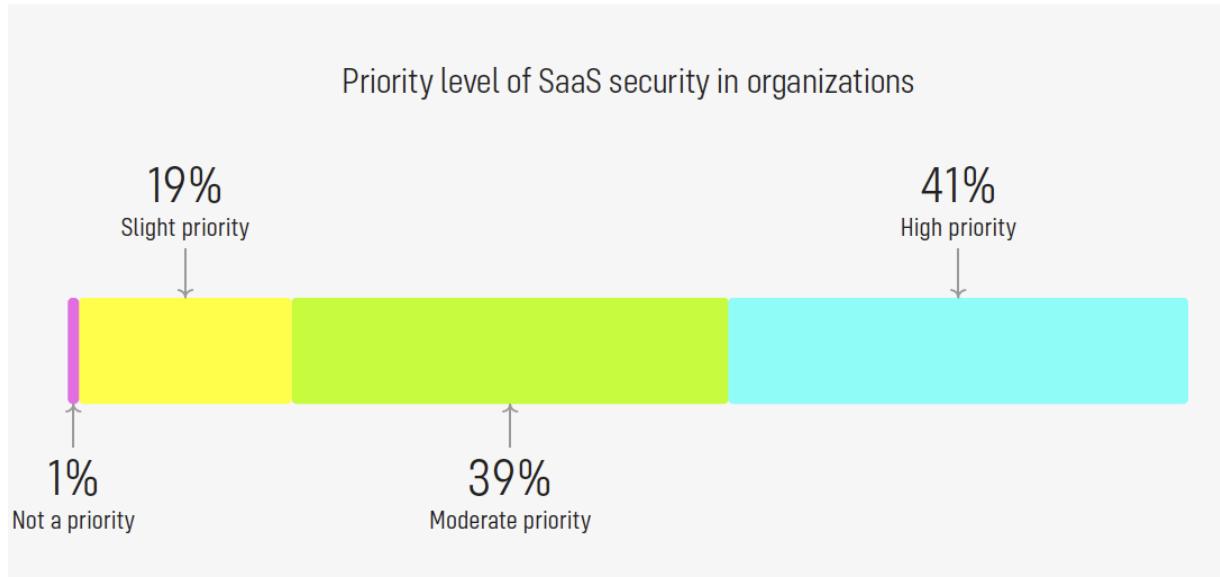


[Figure 1: How investment in SaaS security has shifted from 2022 to 2023]

“For years, SaaS security has been an afterthought. However, the landscape depicted in this year's survey paints a dramatically different picture, one where SaaS security has surged to the forefront of corporate agendas,” the CSA says in the report.



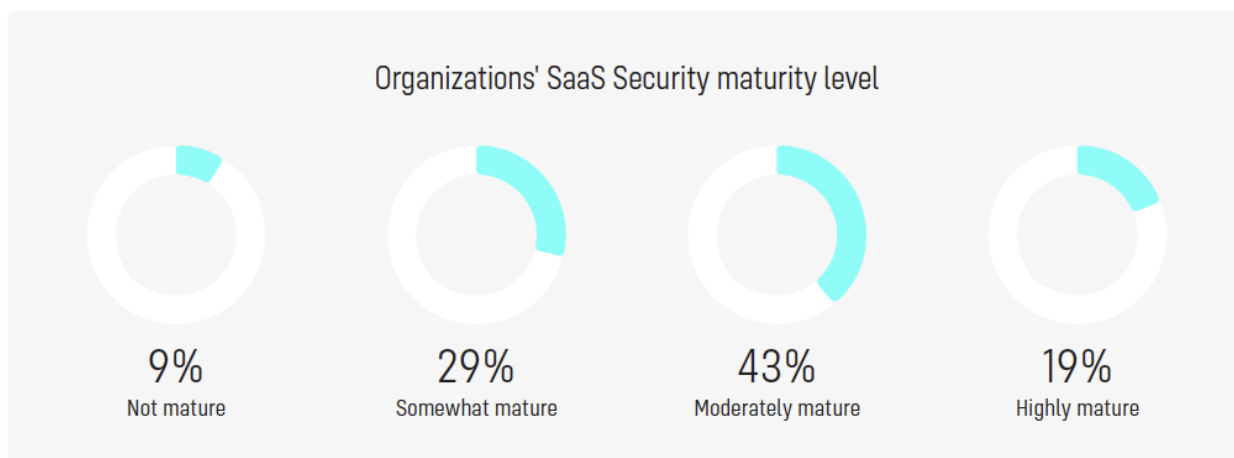
This trend is confirmed in the survey findings where 80% of respondents now classify SaaS security as a moderate or high priority.



[Figure 2: Security professionals rate the priority level of SaaS security in their organization]

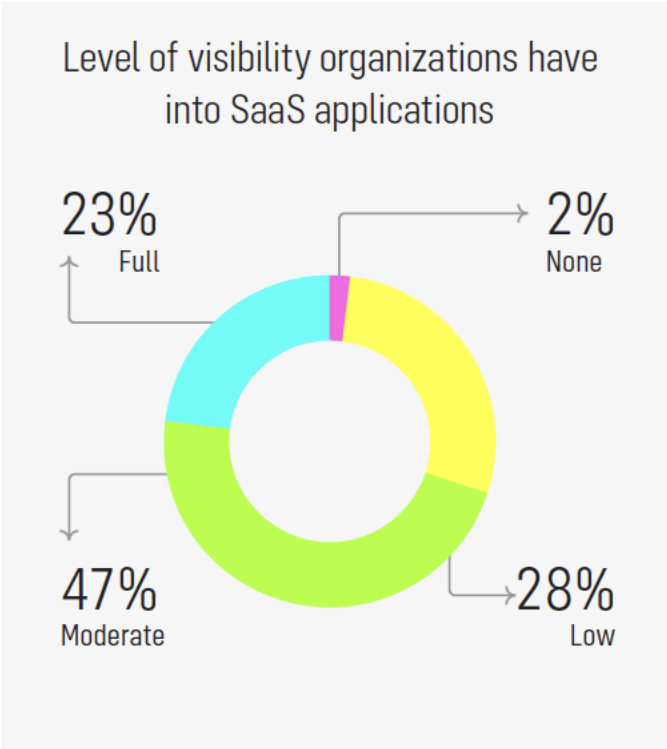
## 2: Organizations Have Improved Key SaaS Security Capabilities

Organizations have also significantly improved key SaaS security capabilities in the past year, the survey found. In fact, 19% percent of organizations now consider their SaaS security posture to be highly mature, with another 43% deeming it moderately mature.



[Figure 3: How organizations perceive their SaaS security maturity]

Thanks to acquiring SaaS security capabilities, visibility into the SaaS stack is increasing. Today, 70% of organizations have moderate (47%) to full visibility (23%) into their SaaS applications, with those achieving full visibility having more than doubled over the past year, the report said.



[Figure 4: Security professionals rate their visibility into SaaS applications]

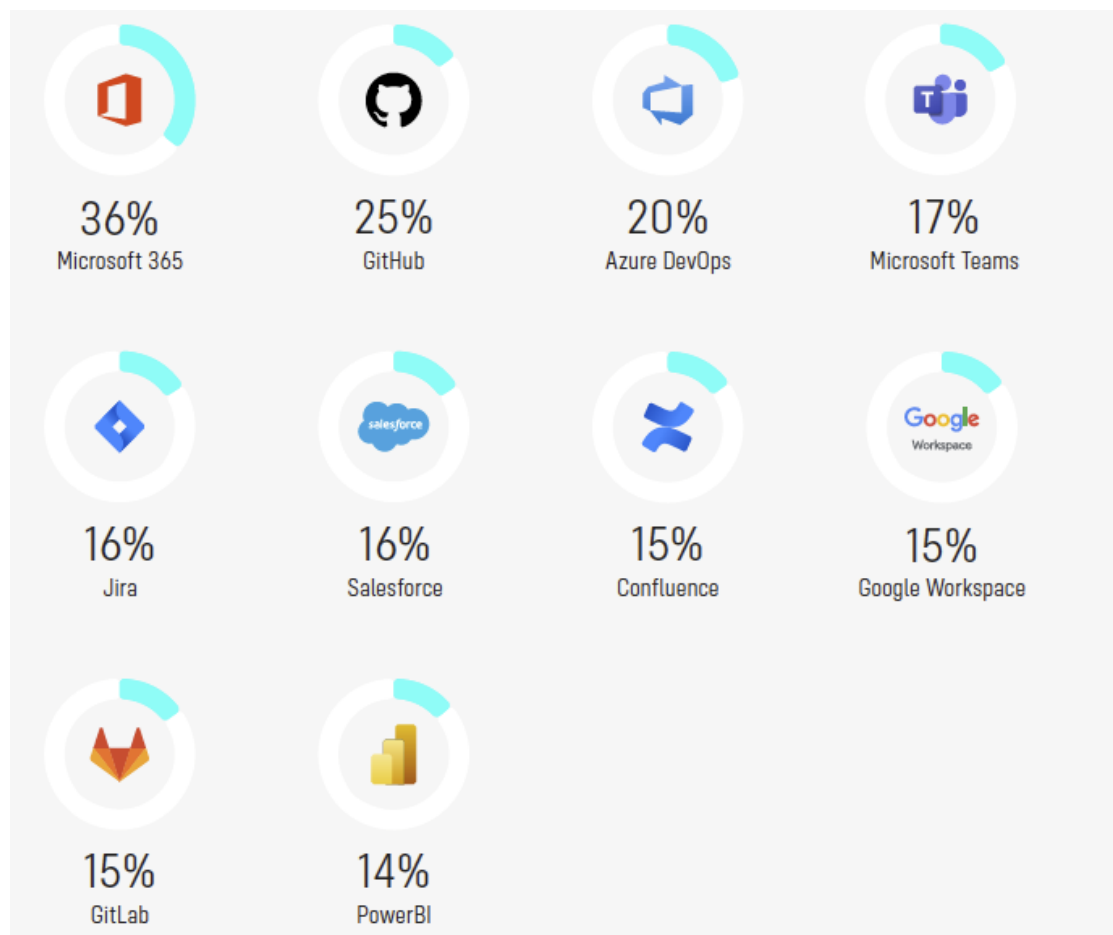
Detection capabilities surrounding multi-factor authentication (MFA) attacks have also improved from to 62% from 47% a year ago. In threat detection, 62% percent of respondents state their ability to detect abnormal user behavior, compared with 44% a year ago.

“This enhanced oversight is pivotal for effective configuration and user management. It also plays a crucial role in identifying mistakenly or unwanted publicly shared data resources, such as documents and repositories,” the report notes.

### 3: Organizations Are Still Facing Challenges, Due to Using the Wrong Tools

While organizations have improved SaaS security oversight, 73 percent surveyed pointed to achieving visibility into business-critical apps as their biggest challenge.

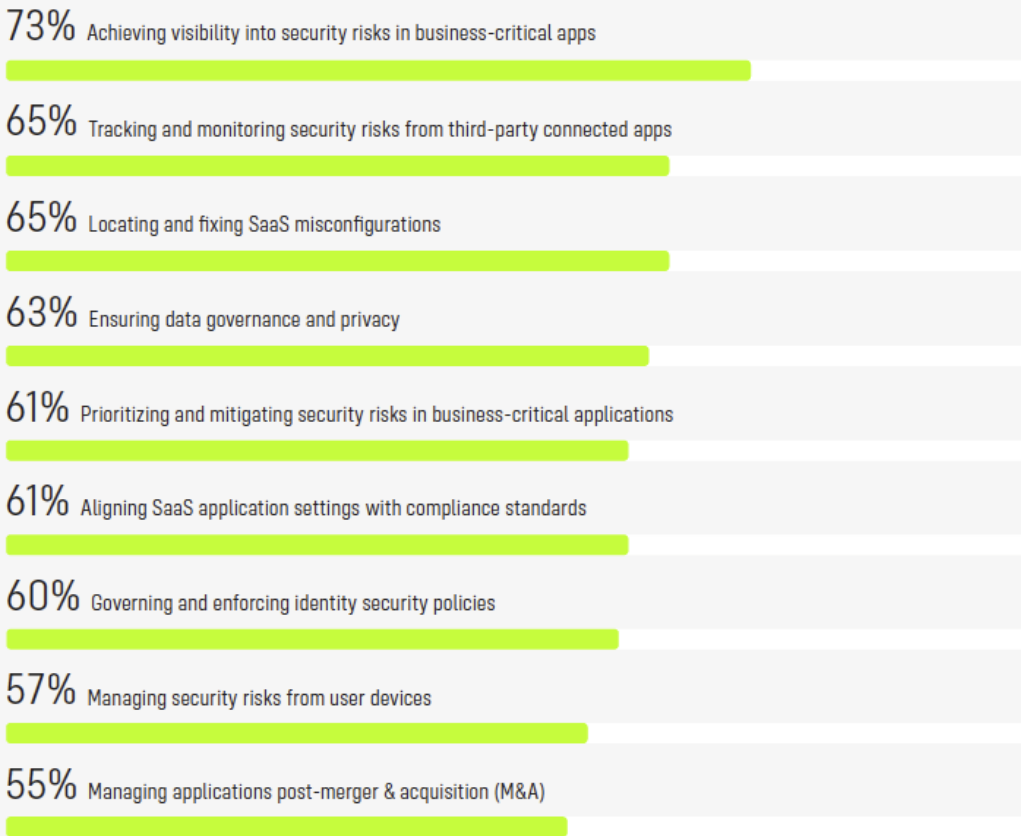
According to respondents, the top 10 most difficult apps to secure include business-critical apps such as Microsoft 365, GitHub, Microsoft Teams, Jira, Salesforce, and Google Workspace.



*[Figure 5: Top 10 most challenging applications to manage from a security perspective]*

Additional challenges include tracking and monitoring security risks from third-party connected apps (65%); locating and fixing SaaS misconfigurations (65%); ensuring data governance and privacy (63%); and aligning SaaS application settings with compliance standards (61%).

### Most difficult aspects of SaaS Security to manage



[Figure 6: Security professionals rate the biggest challenges in SaaS security]

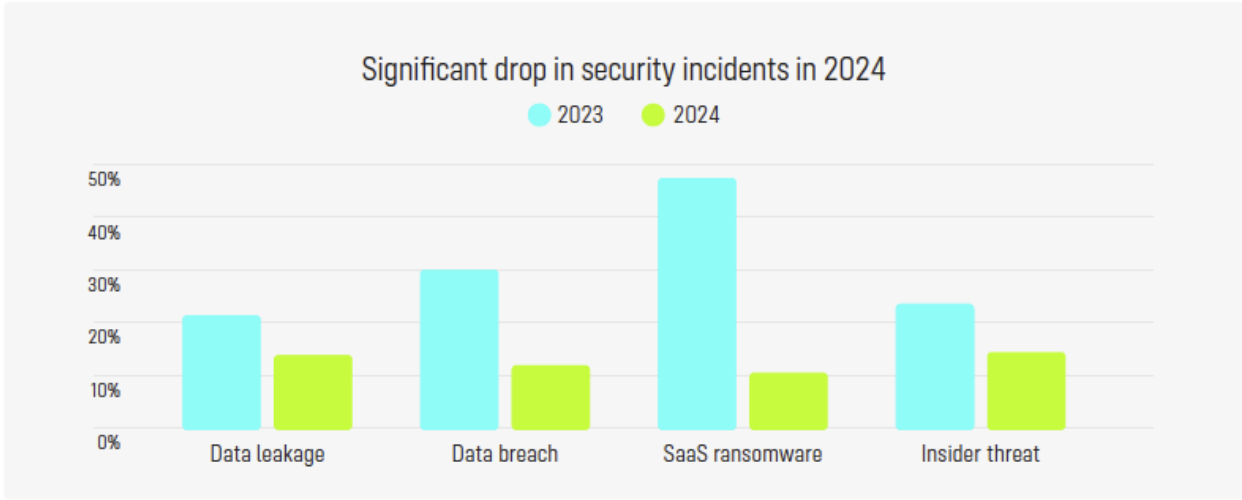
Survey data indicates a widespread utilization of tools such as CASB and manual audits, among others, for securing the SaaS stack. These organizations indicated they had significantly greater challenges securing their applications than those organizations that used SSPM.

Despite their utility, these tools lack the ability to address the full spectrum of requirements essential for robust SaaS security, the report notes, making them misaligned with SaaS attack vectors.

#### 4: Despite Challenges, SaaS Security Investment is Paying Off

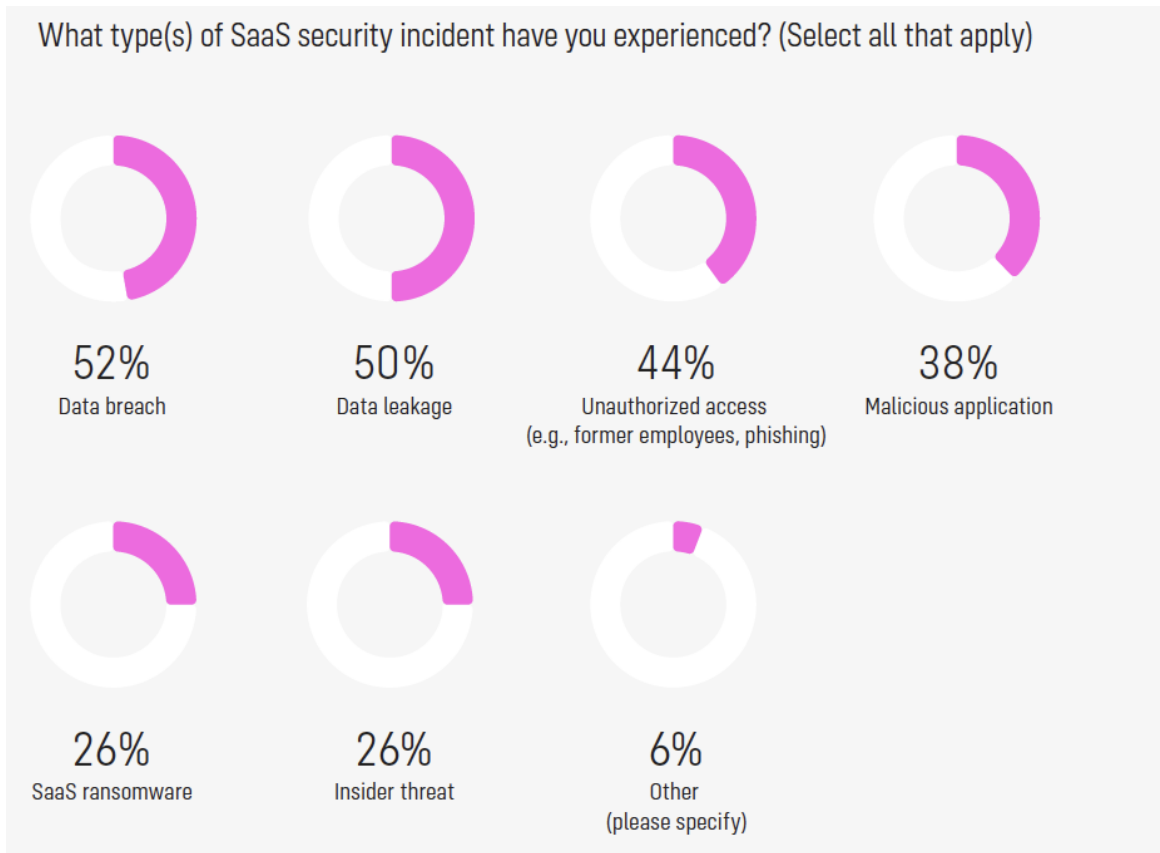
The investment the survey identified clearly demonstrates that organizations are taking SaaS security seriously. In fact, the survey identified a positive trend: 25% of respondents experienced a SaaS security incident in the past two years, compared with 53% last year.





[Figure 7: Thanks to investment in SaaS security, the number of breaches declined over the past year]

The most common security incidents reported were data breaches (52%) and data leakage (50%), followed by unauthorized access (44%) and malicious applications (38%).



[Figure 8: Most common types of SaaS security incidents in 2023]

Companies who have adopted SaaS Security Posture Management (SSPM) are faring better than those using other tools such as CASB, Cloud Security Posture Management (CSPM), and SASE, among others, for securing the SaaS stack.

Organizations that reported using SSPM as their SaaS security strategy enablers show a marked improvement in their ability to scale and monitor a larger portion of their SaaS stack, the report notes.

Those using SSPM are more than twice as likely to have full visibility into their SaaS stack — 62% of these organizations are able to oversee over 75% of their SaaS environment compared to those who utilize other tools and manual processes in their strategy (31%).

SSPM users were also more likely to find key SaaS Security tasks to be easy, while non-SSPM users found them to be very hard.

## Conclusion

In conclusion, the CSA says the survey demonstrates a positive momentum in SaaS security strategy. In particular, the integration of SSPM emerges as a factor in enabling an organization's SaaS security.

The survey highlights the importance of revisiting and refining SaaS security strategies within organizations to include tools that specifically address SaaS security, thus reducing the likelihood of a SaaS security incident in the future.

[\*Download the full SaaS Security Survey: 2025 CISO Plans and Priorities report\*](#)

### About the Author

Hananel Livneh is head of Product Marketing at Adaptive Shield. He joined Adaptive Shield from Vdoo, an embedded cybersecurity company, where he was a Senior Product Analyst. Hananel completed an MBA with honors from the OUI, and has a BA from Hebrew University in Economics, Political Science and Philosophy (PPE). Oh, and he loves mountain climbing.

Hananel can be contacted on [linkedin](#) and at [adaptive-shield.com](https://adaptive-shield.com).





# Transforming Security Testing With AI: Benefits and Challenges

Empowering Better Vulnerability Detection with Artificial Intelligence and Security Testing

By Haresh Kumbhani, CEO, Zymr Inc.

Security testing plays a critical role in ensuring that applications are protected against vulnerabilities and attacks. In times when cyber attacks like data breaches and ransomware are rising, security testing is one of the most important parts of the software development lifecycle. However, to keep up with modern, complex software demands, security testing needs to ditch manual processes and static tools, which can be time-consuming and prone to human error. Integration with artificial intelligence (AI) can evolve security testing for automation, predictive analysis, and improved accuracy.

## The Benefits of AI in Security Testing

### 1. Automated Vulnerability Detection

AI automates the detection of security vulnerabilities by leveraging machine learning algorithms and pattern recognition techniques. Automated vulnerability detection tools can quickly scan codebases, applications, and networks to identify potential weaknesses. For example, AI-powered static code

analysis tools can analyze millions of lines of code in a fraction of the time it would take a human, highlighting issues such as SQL injection, cross-site scripting (XSS), and buffer overflow vulnerabilities.

According to a report by MarketsandMarkets, the global AI in cybersecurity market is expected to grow from [\\$8.8 billion in 2019](#) to [\\$38.2 billion by 2026](#), at a CAGR of 23.3%. This growth underscores the increasing reliance on AI for tasks like vulnerability detection, which enhances organizations' overall security posture.



Source: MarketsandMarkets

## 2. Predictive Analysis and Threat Modeling

AI excels in predictive analysis, allowing security teams to anticipate and mitigate potential threats before they materialize. By analyzing historical data and identifying patterns, AI can predict which areas of an application are most likely to be targeted by attackers. This predictive capability is invaluable for threat modeling, a process where potential security threats are identified, quantified, and addressed during the application's design phase.



A study by IBM found that organizations using AI and automation in their cybersecurity initiatives experienced an average cost savings of [\\$3.58 million per data breach](#), compared to those that did not use these technologies. This significant cost reduction highlights the value of AI in proactive threat identification and mitigation.

### 3. Continuous Monitoring and Real-Time Response

AI-driven tools enable continuous security monitoring, providing real-time insights into an application or network's security state. These tools can detect anomalies and potential security breaches as they occur, allowing for immediate response and remediation. For example, AI-powered Security Information and Event Management (SIEM) systems can analyze vast amounts of data in real-time, identifying suspicious activities and triggering alerts.

Continuous monitoring and real-time response capabilities are crucial for penetration testing services, which aim to identify and exploit vulnerabilities before malicious actors can. By integrating AI into penetration testing, organizations can enhance the effectiveness of their security assessments and ensure timely identification and resolution of security issues.

### 4. Improved Accuracy and Reduced False Positives

One of the significant advantages of AI in security testing is its ability to improve the accuracy of test results and reduce false positives. Traditional security tools often generate many false positives, which can overwhelm security teams and lead to alert fatigue. AI algorithms, particularly those based on machine learning, can distinguish between genuine threats and benign activities more accurately, reducing false alerts.

According to a survey by Capgemini, [69% of organizations](#) believe that AI will be necessary to respond to cyber threats in the future. This belief is driven by AI's ability to provide more precise threat detection, reducing the workload on security teams, and enabling them to focus on genuine threats.

### 5. Scalability and Efficiency

AI enhances the scalability and efficiency of security testing processes. Traditional security testing methods can struggle to keep up with the dynamic and complex nature of modern IT environments, especially in large-scale and cloud-based infrastructures. AI can handle these complexities with ease, performing comprehensive security assessments across extensive and heterogeneous environments.

For example, AI-powered tools can automate the process of security testing in continuous integration and continuous delivery (CI/CD) pipelines, ensuring that security checks are performed at every stage of the software development lifecycle. This integration not only improves efficiency but also ensures that security is a continuous and integral part of the development process. Integrating AI with DevOps services further enhances this synergy, ensuring that security is built into every phase of the development and deployment process.

## The Challenges of AI in Security Testing

### 1. Data Quality and Quantity

AI algorithms require high-quality and large datasets to train effectively. In the context of security testing, this means having access to comprehensive datasets that include various types of security vulnerabilities, attack patterns, and threat scenarios. However, obtaining and curating such datasets can be challenging, particularly for smaller organizations with limited resources.

The quality of data is equally important. Poor-quality data can lead to inaccurate models and unreliable test results. Ensuring that datasets are accurate, diverse, and representative of real-world scenarios is crucial for the effectiveness of AI in security testing.

### 2. Complexity and Integration

Implementing AI in security testing involves technical complexities, particularly in integrating AI tools with existing security frameworks and development processes. Organizations may face challenges in aligning AI-driven processes with traditional security protocols and ensuring seamless interoperability between different tools and systems.

Moreover, the integration of AI requires a deep understanding of both AI technologies and cybersecurity principles. Organizations need skilled professionals who can bridge the gap between these domains and effectively manage AI-driven security initiatives.

### 3. False Positives and Negatives

While AI can significantly reduce the number of false positives, it is not immune to them. False positives can still occur, leading to unnecessary investigations and resource allocation. Conversely, false negatives, where genuine threats are overlooked, can have severe consequences for an organization's security.

Managing and mitigating these issues requires continuous refinement of AI models, regular updates to threat intelligence, and a robust feedback loop that allows AI systems to learn and improve over time.

### 4. Ethical and Privacy Concerns

The use of AI in security testing raises ethical and privacy concerns. AI systems often require access to sensitive data to function effectively, which can lead to potential privacy violations if not managed properly. Additionally, the decision-making processes of AI systems can sometimes be opaque, leading to questions about accountability and transparency.

Organizations must ensure that their use of AI in security testing adheres to ethical standards and regulatory requirements. This includes implementing robust data governance practices, ensuring transparency in AI decision-making, and maintaining accountability for the outcomes of AI-driven processes.

## 5. Skill Gaps and Training

The successful implementation of AI in security testing requires specialized skills that combine knowledge of AI technologies with cybersecurity expertise. However, there is a notable skills gap in the industry, with a shortage of professionals who possess this unique combination of skills.

To address this challenge, organizations need to invest in training and upskilling their workforce. This includes providing opportunities for continuous learning, fostering a culture of innovation, and encouraging collaboration between AI and cybersecurity teams.

## Future Trends and Developments

### 1. Advancements in AI Technologies

Emerging AI technologies are set to further enhance the capabilities of security testing. For instance, AI-driven penetration testing tools are being developed to automate and improve the efficiency of penetration testing services. These tools can simulate sophisticated attack scenarios, providing deeper insights into potential security weaknesses and enabling more effective remediation strategies.

### 2. Collaboration Between AI and Human Expertise

The future of AI in security testing lies in the collaboration between AI systems and human expertise. While AI can automate and enhance many aspects of security testing, human oversight and judgment remain crucial. Security professionals can leverage AI to augment their capabilities, focusing on strategic decision-making and addressing complex security challenges that require human intuition and experience.

## Conclusion

AI is transforming security testing by automating vulnerability detection, enhancing predictive analysis, enabling continuous monitoring, improving accuracy, and increasing efficiency. However, the integration of AI also presents challenges, including data quality, technical complexity, false positives and negatives, ethical concerns, and skill gaps.

Despite these challenges, the benefits of AI in security testing are undeniable. As technology continues to evolve, AI will play an increasingly vital role in enhancing cybersecurity and protecting organizations against ever-evolving threats. By embracing AI and addressing the associated challenges, organizations can achieve a more robust and resilient security posture, ensuring that they stay ahead of cyber adversaries and safeguard their digital assets.

For more information on how AI can enhance your security testing explore [penetration testing services](#), and discover how our solutions can help you stay secure in the digital age.

For further reading on related topics, you can check out these insightful articles from Cyber Defense Magazine:

[Zero Trust in DevOps: Implementing Robust Security Measures](#)

[Automating Security in DevOps: Tools and Techniques for Continuous Compliance](#)

### **About the Author**

Haresh Kumbhani the CEO of Zymr Inc. I am a technical leader and serial entrepreneur with 30+ years of experience in complex product development and deployment. As CEO of Zymr, Inc., I have been working with innovative technology companies globally to help them build their cloud strategy and products. I invest the rest of my time mentoring our cloud-savvy development team in 'design thinking' and 'agile development.'

Haresh can be reached online at <https://www.linkedin.com/in/hareshkumbhani/> and at our company website <https://www.zymr.com>





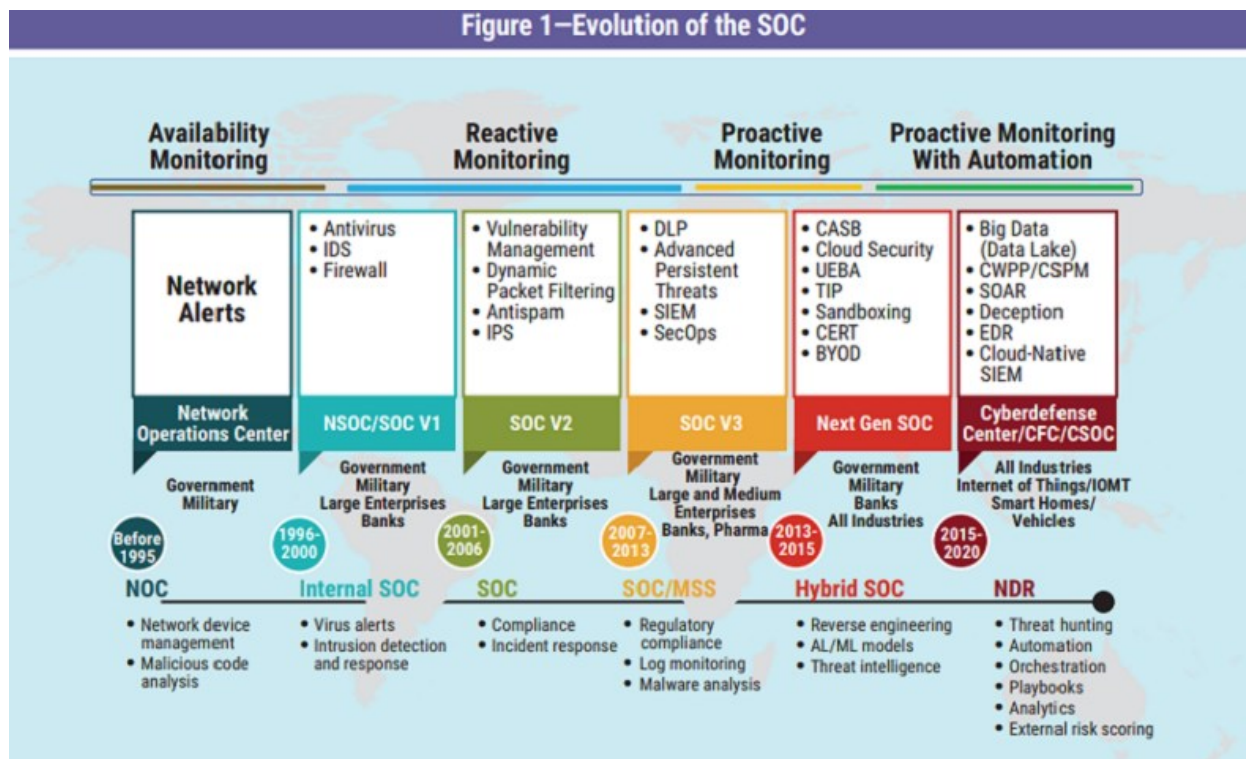


## Strategies for Building an Effective, Resilient Security Operations Center

By William Wetherill, Chief Information Security Officer, DefenseStorm

The modern Security Operations Center (SOC) has morphed and matured since its infancy in the early 1990s. The primary responsibility of monitoring for any indication of intrusion or compromise has remained a critical and valuable control. The modern SOC now encompasses more robust information to assist in its primary objective, including correlating data from asset management, vulnerability management, data loss prevention systems, and cloud access security brokers to events to provide enriched information to our investigators. Modern SOC's can deploy more proactive systems that become much more powerful when combined with security orchestration and automated response. However, even with all of the technology at our disposal, the fundamental challenges of a SOC remain. In order to be an effective and efficient control within our environments, we must manage and mature our SOC's along five fundamental channels.

- Visibility
- Alert effectiveness
- Investigative prowess
- Threat intelligence
- Incident response



## Visibility

At the core of any SOC is monitoring, and effective monitoring hinges on visibility. Gaps in visibility can result in unmanaged risks and present real danger in the event of a cyber incident. Still, not every event holds the same level of security value. While every security professional desires abundant data, we all struggle to prioritize data based on its potential impact for an investigation.

An investigation is only as good as the data it is based on; as such we must first take steps to ensure the integrity of events. As a baseline, ensure that all devices are reliably receiving their network time protocol sync from the same sources, that the events in the SIEM have the needed information, and that the ingestion uptime is reliable.

Since the vast majority of incidents will involve either a user, a device, or multiples of both; use the rule of non-repudiation to find gaps within monitoring. Every event should correlate to the account or device it originated from. Performing exercises to practice non-repudiation within logged events will ensure we are prepared for any investigation and speed up the root cause analysis process during an incident. The operational and investigative teams should be challenged to answer simple investigative questions: who,

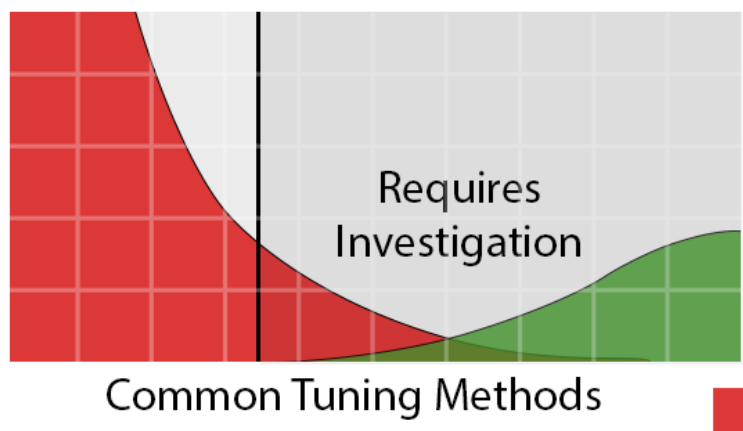
what, when, where, why, and how. Regularly practicing these challenges not only familiarizes the team with the network but also helps keep them calm and confident in the face of a true incident.

## Alert Effectiveness

There are many articles discussing analyst burnout or false positive churn, leading most of us to believe it is inevitable. This certainty has fostered a culture of “burn and churn,” where we inadvertently devalue our newest employees in the name of giving them a “foot in the door.” Regrettably, the expectation that they will leave in a year or so also often leads security leaders to neglect investing in their employees.

This process becomes endemic, and the effectiveness of the SOC becomes stagnant and subject to regression. The last line of defense is when an attacker gains access to YOUR network, and it is staffed with untrained, burnt-out, tier-one analysts. No wonder so many have decided to outsource to managed services. Unfortunately, that is not always a remedy, as most managed shops suffer from the same challenges.

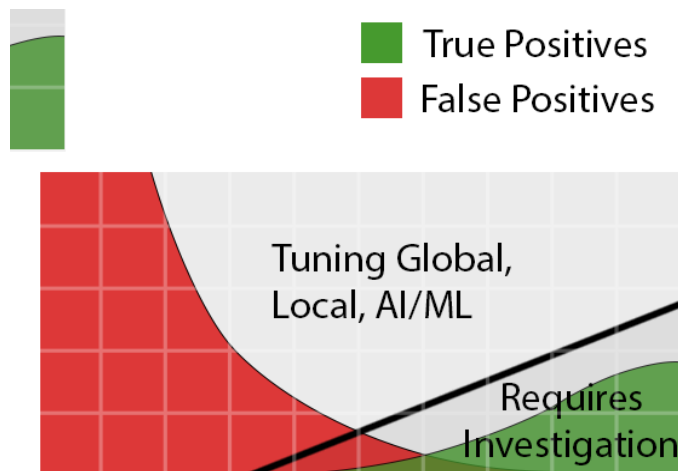
So, how do we get out of this deep rut? The answer lies in alerting effectiveness.



Common tuning methods require that we stomach a large load of false positives in order to never accidentally get a false negative. The false positive load does more damage than good, causing our analysts to become “snow blind” and miss the real events as they pass. We essentially move the problem from the technology side to the human side. Since humans are not good at processing large amounts of data, we are setting them and ourselves up for disappointment, failure, and quite possibly setting our companies up for material impact from a cyber event.

Any good engine must be tuned, and that tuning requires checkups to ensure effective and efficient operation; our operations software is no different. Tuning can and should be done to mold the alert system to the environment. Train the alerts to know their environment, and the operations team will catch more. The more we tune into our infrastructure, the better the results.

But what about the dreaded false negative? Well, if we also spread alerts to fire throughout the cyber kill chain, it is less likely that a single miss will compromise the environment. In fact, having a deep bench of alerting throughout the stages of an attack builds trust and confidence in our systems that malicious actions will not go unnoticed.



## Investigation

Consider this scenario: the team has seen something strange, but before they reach out to the Cybersecurity Incident Response Team, they need to dig in and confirm the event is truly an indicator of a successful attack or compromise. This requires investigation. Remember when I spoke about training analysts earlier? This is where it needs to be. Analysts are digital investigators. They need to understand the investigation principles and incident response and be constantly exposed to attacker's tactics, techniques, and procedures to recognize them when found in the logs.

There should be a sense of trust that investing in our analysts with the intent of creating professional investigators and incident responders will yield a high return on investment. They cannot be considered entry-level security employees, but rather, like architects or engineers with distinct skills and abilities who gain the same level of commitment from security leaders. When analysts can trace every step the penetration tester took within the environment, we can all rest easier.

## Threat Intelligence

Every incident response flow chart should start with sensor data. Sensor data are the alerts that kick off response. This could be everything from signature or behavioral findings to an article or random conversation in the hall. Quite often, though, the best sensor data comes from indicators delivered from investigating real events. The more related those events are to the company, the better.

There are many threat intelligence feeds out there, and quite often, we add them only to never hear from them again, or we remove them a few days later as they are alerting on standard processes. Threat intelligence feeds vary in quality, and like most things in cybersecurity, there is a balance between the



amount of effort put into managing the system and the return on effort. Properly investing in threat intelligence by actively managing the indicators within the feeds yields much higher value. Curating feeds with data for the business vertical or even data from the security operation team's investigations can be incredibly powerful. Unfortunately, threat feeds are rarely valuable as a set-and-forget alert producer.

## Incident Response

Finally, a SOC is essential to cyber incident response flows. When we need them most, there must be full confidence that the SOC team can investigate and provide timely evidence. Train them, involve them, tabletop with them, and you will be thankful for the confidence in the face of adversity.

The cyber security operations center is a longstanding control. It plays a crucial role in our efforts to minimize the effects of cyber incidents on our organization. Ultimately, investing time and energy into the control can yield high returns.

### About the Author

William Wetherill is currently the Chief Information Security Officer (CISO) for DefenseStorm. He is a Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) with extensive training, background, and experience in various aspects of IT systems and applications. He has over 27 years of IT experience, almost a third of it directly in cybersecurity. William was the Director of Cybersecurity Operations overseeing the 24/7 SOC at DefenseStorm before being promoted to CISO in January 2024. William was previously the Chief Information Security Officer at the University of North Carolina in Wilmington (UNCW) where he built and managed their Information Security Program.



William can be reached online at [William.Wetherill@defensestorm.com](mailto:William.Wetherill@defensestorm.com) and at our company website <https://www.defensestorm.com/>



## AI-Powered Fraud Detection Systems for Enhanced Cybersecurity

How AI Is Making Fraud Detection Faster and More Reliable

By April Miller, Managing Editor, ReHack Magazine

Artificial intelligence (AI) has many applications in cybersecurity. Automated fraud detection is one of the most impactful of these use cases.

Fraud can be difficult for humans to spot, but machine learning excels at detecting anomalies in user or system behavior. As a result, AI is an ideal anti-fraud tool. Here are five ways this technology is making an impact across various industries.

## 1. AI Fraud Detection in Finance

The banking and finance industry was an early adopter of AI-powered fraud detection, and it's easy to see why. Machine learning models can spot stolen credit cards quickly and accurately by detecting purchase behavior that doesn't match a customer's previous buying history.

Banks monitored transactions for unusual activity long before the advent of AI. However, machine learning can perform this work faster and more reliably than humans. As a result, fraud detection has emerged as [the number one AI use case](#) among financial institutions.

## 2. AI Fraud Detection in E-Commerce

E-commerce is another sector that can gain a lot from AI fraud detection. As online sales grow, these stores and their customers' accounts become bigger targets for cybercriminals. Consequently, they must find breaches quickly, but doing so amid such high transaction volumes can be difficult. Automation through AI is the answer.

Online stores have extensive user data, as [65% of American shoppers](#) prefer self-service through chatbots and other AI tools. As a result, e-commerce companies already have enough information on each user to recognize abnormal behavior. Connecting these AI solutions to fraud detection algorithms makes security faster and more accurate than manual alternatives.

## 3. AI Fraud Detection in Government

AI-powered fraud detection has also seen rising use among government organizations. The same algorithms that let banks catch breached accounts enable government agencies to detect fraudulent tax and benefit claims.

The U.S. Treasury [recovered more than \\$375 million](#) in 2023 alone after using AI fraud detection tools. Part of this success stems from AI's accuracy in identifying suspicious trends, but the automation aspect plays a part, too. Uncovering potential fraud with technology takes much less time than the conventional approach, so government agencies can manage more cases with fewer resources.

## 4. Phishing Detection

Fraudulent transactions may be the most obvious targets for AI fraud detection, but they're not the only ones. This technology is also useful in more cybersecurity-specific use cases. Phishing prevention is an excellent example.

Phishing is by far [the most reported type of cybercrime](#), and this popularity is largely due to its efficacy. It's hard for users to spot every phishing attempt. AI can help by analyzing real-life phishing examples to learn common markers of these fraudulent messages. It can then flag messages as possible phishing to make people more aware of these risks, preventing costly errors.

## 5. User and Entity Behavior Analytics

AI fraud detection can also improve cybersecurity through User and Entity Behavior Analytics (UEBA). This practice deploys AI to monitor how users and devices behave on a company network. When the models detect suspicious behavior like unusual file transfers or login attempts, they lock the account and alert security teams.

UEBA can stop cyberattacks from spreading after initial defenses fail to prevent them. It also helps work around [the 4 million worker shortage](#) in cybersecurity, ensuring strained security workforces can still provide 24/7 protection.

## Considerations for Implementing AI Fraud Detection

As these use cases highlight, AI fraud detection has significant advantages. However, it requires attention to a few best practices to reach its full potential.

One of the most common challenges in anti-fraud AI is its tendency to produce false positives. Machine learning models often over-fit fraud definitions, which can lead to high false alarms. These cases may worsen the alert fatigue that [62% of IT teams](#) say is driving turnover.

Careful training reduces false positives. Organizations should provide plenty of data on both real fraud examples and legitimate cases to drive more reliable AI results. Tweaking the model over time will also help it better distinguish between real fraud and benign activity.

Data privacy is another issue that deserves attention. Tailoring behavior analytics to specific users requires a considerable amount of sensitive user data. Consequently, AI fraud detection entails significant privacy risks. Some users may not feel comfortable giving away that much information, and storing it opens the door to far-reaching breaches.

In light of these risks, brands should be upfront about their AI use and allow users to opt out of these services. They should also encrypt all AI training databases and monitor these systems closely for intrusion. Regular audits to verify the model's integrity are also ideal.

## AI-Powered Fraud Detection Has Many Applications

While AI fraud detection is still imperfect, it's a significant step forward compared to conventional methods. Industries from finance to e-commerce to cybersecurity can benefit from this innovation.

As machine learning techniques improve, these applications will become even more impactful. Before long, AI-powered fraud detection will reshape multiple sectors.



## About the Author

April Miller is the Managing Editor of ReHack Magazine. She is particularly passionate about sharing her technology expertise, helping readers implement technology into their professional lives to increase their productivity, efficiency and personal enjoyment of their work.

April can be reached online on [Twitter](#), [LinkedIn](#) and at our company website <https://rehack.com/>.





## The Unsolvable Problem: XZ and Modern Infrastructure

By Josh Bressers, Vice President of Security, Anchore

The ongoing prevalence (and rise) of software supply chain attacks is enough to keep any software developer or security analyst up at night. The recent XZ backdoor attack is finally behind us, and luckily there was no widespread reach of the backdoored library. If you hadn't heard, this [software supply chain attack](#) was a malicious effort that targeted Linux systems, and this attack had been years in the making.

There's no denying that an event like XZ will happen again, and we may not be so lucky next time. But what hasn't been discussed is how what happened with XZ isn't a problem we can solve with best practices today. So, if we can't solve this problem of backdoor supply chain attacks, how do we chart a safe route forward?

### The Unsolvable Problem

Sometimes reality can be harsh, but the painful truth about this sort of backdoor attack is that there is no solution, we simply don't know how to solve this one. Many projects and organizations are happy to explain how they keep you safe, or how you can prevent software supply chain attacks, by doing this one simple thing. However, the industry as it stands today lacks the ability to prevent an attack created by a motivated and resourced threat actor. In fact, the [Anchore 2022 Software Supply Chain Security Report](#)

shows that the security of open source software containers is ranked as the number one challenge by 24% of respondents, so this is not an isolated business concern. The same survey also reports that more than half of respondents say that securing the software supply chain is a top or significant focus. This indicates that recent, high-profile attacks like the XZ attack have put software supply chain security on the radar for the majority of organizations.

If there is a malicious open source maintainer, we (as an industry) lack the tools and knowledge to prevent this sort of attack, as you can't actually stop such behavior until after it happens. When we use open source software, there is so much of it, we can't possibly vet it. We rely on the community to help find and fix problems, which is exactly what happened with the XZ backdoor attack.

HOWEVER, that doesn't mean we are helpless. We can take a page out of the playbook of the observability industry. Sometimes we're able to see problems as they happen or after they happen, then use that knowledge from the past to improve the future, that is a problem we can solve. And it's a solution that we can measure. If you have a solid inventory of your software, past, present, and future, then looking for affected versions of XZ becomes simple and effective.

## Today and Tomorrow

Looking for a vulnerable version of XZ, specifically versions 5.6.0 and 5.6.1, sounds like it should be an easy task, but trying to solve a problem like this at scale is always a challenge. We don't know what we will need to quickly search for in the future. Will it be a binary file, a python package, or maybe just a checksum. We don't know what the next attack will be, an accurate inventory will be important.

The industry is currently putting a focus on using a software bill of materials, or SBOM, as the way to track the contents of software. We see a focus on these inventories in new development standards such as the secure software development framework, or SSDF. By using an SBOM to track software inventory, we have a standardized way to not only track our own software, but to also share those inventories with our customers and partners, and to receive an SBOM from our suppliers. SBOMs aren't perfect, but they are the first step to having software inventories we can use in the future.

## What Now?

Anyone who has been following industry news is probably wondering what supply chain story will happen next. The size and complexity of open source software is enormous and growing more complex every day. Open source is so embedded in our products and services now there's no way we can stop using it, it's here to stay, so what responsibilities do we have? If it's too big to fail, and too big to fix, we have to figure out how we can use open source in ways that make sense. We have technologies now to help keep track of your open source software components, but just keeping track is the first step. It's just as important to move quickly when the next XZ shows up. If we're going to use open source, we have to move at the speed of open source. We can't solve the problem that brought us to XZ, but we can make sure when the next one happens, we can start responding in minutes instead of days.

## About the Author

Josh Bressers is the Vice President of Security at Anchore, a modern software composition analysis company that automates software compliance to save time and reduce risk. At Anchore he guides security feature development for the company's commercial and open source solutions. He is a co-lead of the OpenSSF SBOM Everywhere project, and is a co-founder of the Global Security Database project at the Cloud Security Alliance.

Bressers can be reached on [LinkedIn](#) or by visiting <https://www.anchore.com/>.







## Zero-Trust Endpoint Security

How Preventive Approach Can Limit Your Endpoint Attack Surface

By Dr. Ran Dubin, CTO, BUFFERZONE Security LTD

### Zero-Trust Endpoint Security: How a Preventive Approach Can Limit Your Endpoint Attack Surface

Endpoint security has become more critical than ever in today's rapidly evolving threat landscape. As enterprises become more interconnected, the potential attack surface expands, leaving endpoints increasingly vulnerable to many external risks. These risks originate from a variety of sources, including removable media, web browsing, file downloads, and email links and attachments. Traditional security measures, while essential, are insufficient on their own. A shift towards a preventive approach, emphasizing application isolation and zero-trust file security, is necessary to safeguard enterprises from sophisticated threats.

### The Shortcomings of Traditional Detection-Based Security

Detection-based security solutions, including antivirus (AV) and Endpoint Detection and Response (EDR) systems, play a vital role in identifying and mitigating threats. Detection-based security measures, while essential, have notable limitations that leave systems vulnerable. No detection mechanism is foolproof, as advanced threats like zero-day exploits and polymorphic malware can evade even the most

sophisticated detection systems, especially in the new AI era [1], resulting in exposed systems. Cybercriminals continuously develop techniques to bypass Endpoint Detection and Response (EDR) solutions. Once these defenses are bypassed, the threats can operate undetected, causing extensive damage.

Additionally, detection-based systems often reactively identify threats only after infiltrating the network. This delay in response time can lead to significant data breaches and operational disruptions, highlighting the need for more proactive security measures. Given these limitations, a paradigm shift towards a preventive approach is imperative.

## The Role of Application Isolation and Zero-Trust File Security

To effectively counter the evolving threat landscape, enterprises must implement a comprehensive endpoint security strategy that minimizes the attack surface and prevents threats from executing. This can be achieved by combining two zero-trust approaches: application isolation and zero-trust file security named Content Disarm and Reconstruction (CDR).

### Application Isolation

Application isolation involves segregating applications from the rest of the system to prevent malicious code from spreading. By running applications in isolated environments, any potential threats are contained within the virtual container (isolated environment), safeguarding the primary system. This approach limits the damage that malware can inflict, as even if an application is compromised, the threat remains confined and unable to affect other parts of the system. There are various ways to create endpoint isolation, including virtual machine-based and kernel agent-based methods. Remote Browser Isolation (RBI) offers a server-based approach for web browsing isolation but does not provide a solution for removable media, links, and attachments from non-web-based email.

### Zero-Trust File Security

Zero-trust file security is a proactive approach to protecting systems from malicious files by not trusting any file by default, regardless of its source or type. Content Disarm and Reconstruction (CDR) is an effective technique within this framework. CDR analyzes and breaks down a file into its basic components, removes any potentially malicious elements, and then reconstructs the file as a secure version [2,3]. The files can be images, videos, Artificial Intelligence (AI) models [3], office documents [2], and more. This process ensures that any embedded threats, such as malware or executable scripts, are stripped away, leaving the user with a functional and secure file. Organizations can significantly reduce the risk of file-based attacks by employing zero-trust file security with CDR, safeguarding their systems and data from potentially harmful content.

By combining isolation technology and CDR, we enable a fully zero-trust file security solution that isolates the threat and enables a secure and safe methodology to move the file into the trusted organization's resources.

## The Need for Removable Media Isolation

Today, organizations typically employ device control solutions to reduce the attack surface posed by removable media such as USB drives, CDs, and DVDs. However, restricting user access is inherently flawed, as employees often need to connect removable media for legitimate purposes. This dilemma leaves organizations with two options: disabling device control entirely, thereby sacrificing security, or directing users to a sanitization station or kiosk where they can scan removable media and utilize CDR for zero-trust file security. A third, more effective option is to use endpoint isolation technology. With this approach, when a user inserts removable media, it is automatically isolated, allowing the user to securely access the removable media and select which content to save and transfer to the organization's network. By automatically combining isolation and CDR, users no longer need to visit a sanitization station or request the organization to bypass its security mechanisms, thus maintaining robust security while accommodating legitimate needs.

## Conclusion

As cyber threats become more sophisticated, the limitations of detection-based security solutions become increasingly apparent. Enterprises must embrace a preventive approach to endpoint security centered around application isolation and zero-trust file security. By doing so, they can significantly reduce their attack surface and safeguard their systems against even the most advanced threats. The future of endpoint security lies in proactive measures that prevent threats before they can cause harm, ensuring a resilient and secure digital environment for all.

## References

- [1] S. Cohen, R. Bitton, and B. Nassi. "Here Comes the AI Worm: Unleashing Zero-click Worms that Target GenAI-Powered Applications." arXiv preprint arXiv:2403.02817 (2024).
- [2] Ran Dubin, "Content Disarm and Reconstruction of Microsoft Office OLE files." *Computers & Security* 137 (2024): 103647.
- [3] Ran Dubin, "Content Disarm and Reconstruction of PDF Files," in *IEEE Access*, vol. 11, pp. 38399-38416, 2023, doi: 10.1109/ACCESS.2023.3267717

## About the Author

Dr. Ran Dubin is a BUFFERZONE Security CTO and a Cyber and AI veteran with over 20 years of experience in Artificial Intelligence, zero-trust attack prevention, malware research, and network analysis. Ran is the author of more than 30 academic papers in various areas of Cybersecurity. He received his B.Sc., M.Sc., and Ph.D. degrees in communication systems engineering from Ben-Gurion University, Israel.

For more information, please contact us through [email](#) or browse to our company website <https://bufferzonesecurity.com/>







## The Ugly Truth about Your Software Vendor which CISOs Won't Want (But Do Need) to Hear

By **Iain Sauderson, CTO, Spinnaker Support**

We've got a hard truth to share with you, and you might not like it:

### **You are not your software vendor's top priority.**

Your vendor is focused on their own business-critical priorities: improving profit margins, getting customers migrated to the cloud, and ending support for their legacy products because the revenue margins are dwindling. They want to sell you new add-ons and expensive upgrades, and as a result, you're frantically trying to keep up with your vendor's timeline and expectations to keep your systems supported and optimized.

You've probably heard about third-party software support as the alternative to your vendor lock-in woes. Third-party software support is a way of maintaining and supporting your systems with a partner who

intimately understands SAP and Oracle infrastructures and will work with you directly to ensure your environment is secure, compliant, and delivering real and competitive ROI.

But as a CISO, we know that it's not as easy for you to just click your fingers and swap out your software support provider, and we know there are many questions – and assumed issues – that you may have around moving your support away from your vendor's in-house offering. Whether you're concerned about security, compliance, cost effectiveness, or interoperability, let's have a look at why and how third-party software support might have the edge over your vendor's in-house support.

## Security

This is, we believe, the number one hurdle when it comes to looking at alternative software support providers for ERP systems, and we understand why. But what if we told you that your enterprise's overall security posture could improve with the support and expertise from a third-party software support provider?

With third-party support, your provider takes a bespoke approach to your security and compliance requirements. Take vulnerability management, for example.

As it stands, your existing vendor may offer patches to fix open-door vulnerabilities. But these patches are delivered to you only after the vulnerability is discovered: an approach that resembles sticking a band-aid on multiple wounds instead of minimizing the threats that caused the injury in the first place. This can be [evidenced](#) by the recent discovery that a seven-year-old Oracle patch failed to fully address a security vulnerability, which is now being exploited publicly.

Your enterprise probably already takes a comprehensive approach to its security and vulnerability management, proactively testing and remediating your internal and external attack surfaces and working to improve any gaps in your security infrastructure. So why wouldn't you want to work with a partner who adopts this very same, full-stack approach to security and vulnerability management?

## Compliance

Compliance is a top priority for information security teams, and your risk, legal, business management and continuity colleagues rely on you to get it right. Whether it's meeting government regulations on cybersecurity and data protection or adhering to specific industry standards for financial reporting and legal compliance, you must ensure your software system doesn't expose the business to non-compliance, regulatory penalties, or data breaches.

We often hear that fear of non-compliance deters enterprises from considering third-party support. Fear not: working with a third-party software support partner could enhance your compliance objectives. These partners provide comprehensive support to ensure your software environments meet all regulatory requirements, offering tailored guidance on frameworks like GDPR, HIPAA, SOX, and more. They achieve this through proactive monitoring, timely updates, and in-depth audits to identify and rectify compliance gaps.

Contrast this with traditional vendor support services, which often focus on generic updates and patches that may not fully address your unique compliance needs. A third-party software support partner will ensure your systems are compliant, even if you're running a legacy software version that Oracle or SAP no longer support. They also tackle complex, time-sensitive tax and regulatory issues, customizing solutions to meet your exact needs based on your industry and geography.

## Interoperability

Your enterprise software system is complex, customized, interconnected, and requires seamless integration with your external systems and surrounding technologies. Critically, you need to ensure that all data transferred and used within your systems – and between different systems, apps, and platforms – is secured appropriately and adheres to your data protection and privacy policies.

Unfortunately, we often find that software vendors do not provide the level of interoperability support that businesses require for their complex and customized software instances. This can have severe repercussions for your data protection and security efforts.

When you choose to work with a third-party support partner, you'll benefit from fewer headaches in managing a heterogeneous software environment. Your partner will work closely with you to resolve interoperability issues, ensure adherence to data protection and security protocols, and identify opportunities to optimize workflows and productivity. This collaboration offers long-term benefits for your business by ensuring that your systems work smoothly together. As a result, you can extend the life cycle of your software and avoid unnecessary and expensive upgrades and updates whenever an interoperability issue arises.

## Maximizing ROI

OK, so you've secured your software systems, and you're meeting all your compliance requirements. But you're also under pressure to ensure that you're maximizing ROI from your software investments.

This is where a third-party software support partner can offer extraordinary value.

A third-party support partner will save you, on average, 60%+ the cost of your expensive vendor support contract. These savings can be reallocated to strategic initiatives that drive business growth and innovation – like that digital transformation project you've been trying to find the budget and business case for.

Crucially, these initiatives are driven by you. Say goodbye to pressure from software vendors to upgrade to the newest software or database version. Say goodbye to your fear of losing critical support for systems when your vendor considers them too old to support and maintain. Instead, you'll be working with a software partner who extends the lifespan of your existing software assets, allowing your organization to extract maximum value from its investments.

Traditional vendor support contracts, like those from SAP and Oracle, often come with high costs and rigid terms that do not always align with the strategic goals of your organization.

Just take the costs associated with mandatory upgrades and the limited scope of support available to you, which can strain IT budgets and pile additional pressure onto your teams, without delivering tangible business value. This, coupled with the reality that your software vendor just isn't motivated to work with you to achieve your business goals, makes for an uncomfortable situation.

Why settle for that when you can benefit from a flexible support model that prioritizes performance tuning and optimization? This approach ensures your software applications run efficiently, enhancing productivity and reducing operational costs.

When your organization achieves a more favorable ROI on its software expenditures, you'll free up resources for other critical projects. For CISOs, this translates into a more sustainable IT budget and the ability to invest in security initiatives that directly improve your organization's risk posture.

How's that for a hard truth?

### **About the Author**

As Spinnaker Support's CTO, Iain Saunderson is responsible for the internal and external facing technology leveraged at Spinnaker Support, as well as managing the security practice. Iain Saunderson has over 30 years of experience implementing complex technologies across a wide variety of commercial and government verticals. He has served in leadership roles in organizations including Oracle Corporation, P2 Energy Solutions, and DBAK. Iain's experience is in leading enterprise architecture, development, and managed services organizations.







## Team-Based Training and the Power of Simulation

By Tom Marsland, VP of Technology, Cloud Range

In the constantly evolving realm of cybersecurity, it is critical for incident responders to be prepared and effective. As cyber threats grow more complex, the training approaches for these defenders must evolve to anticipate and address emerging vulnerabilities. While there is a place for knowledge-based certifications, training “like you fight” as a team is essential. This article highlights key practices in training cybersecurity incident responders, emphasizing the benefits of team-based exercises and the strategic use of simulated environments such as cyber ranges.

### Emphasizing Team-Based Training

Cybersecurity incidents often demand a well-coordinated response from a team equipped with diverse expertise. Here’s why team-based training is not just beneficial but necessary:

1. **Real-world Simulation:** Effective training should mirror real cyber attack scenarios, ranging from data breaches to sophisticated persistent threats. These exercises allow teams to hone their strategies and improve decision-making under pressure.
2. **Cross-functional Skills:** It's crucial that team members are not only experts in their specific roles but also have an understanding of their colleagues' duties. Such cross-training ensures flexibility and comprehensive coverage during crises.
3. **Iterative Learning:** Post-training debriefs are vital. They provide a platform for team members to reflect on successes and areas for improvement, reinforcing lessons learned and fostering a culture of continuous enhancement. From these post-training debriefs, action items can be identified, and remedial training to close gaps in knowledge can be assigned to individual participants.

## Leveraging Simulated Environments, or Cyber Ranges

Cyber ranges are controlled environments that simulate real cyber threats, offering an invaluable space for hands-on training.

1. **Practical Engagement:** These environments allow teams to engage with a suite of real tools and live-fire attack simulations in a safe, non-production environment, offering insights into the dynamics of cyber warfare without the associated risks.
2. **Tailored Scenarios:** Cyber ranges can be customized to reflect recent threats or specific training needs, ensuring that exercises are as relevant and challenging as possible.
3. **Performance Metrics:** With live trainers and built-in analytics, cyber ranges can measure team and individual performance, pinpointing strengths and areas needing attention and enabling targeted training interventions.

## The ROI of Training Versus Buying New Tools

Investing in the training of your cybersecurity team can yield substantial returns compared to merely purchasing new security tools. Here's how:

- **Enhanced Problem-solving Capacity:** Well-trained teams are more adept at identifying, responding to, and mitigating cyber threats, often using existing tools more effectively. This is shown with outcomes such as a reduced time to detect, time to contain, and time to remediate.
- **Reduced Incident Impact:** Effective response teams can significantly diminish the potential damage from incidents, saving costs associated with breaches such as downtime, data loss, and recovery.
- **Long-term Resilience:** Continuous training cultivates a knowledgeable and adaptable workforce, capable of handling new threats as they emerge, thus future-proofing your organization against evolving cyber risks.

## Why Does This Matter?

CISOs will want to know why cybersecurity team training matters in the day-to-day discharging of their cybersecurity responsibilities. Continuous training, whether it be in the form of [simulated exercises](#) in a technical cyber range, certifications, or conducting process reviews and tabletop exercises, all contribute to risk reduction for the organization. By educating the cyber workforce, we also give them the skills to drive outcomes in your organization. These range from things in incident response like Minimum-Time-To-Detect, all the way up to risk reduction, improving your bottom line, and enhancing overall cyber resilience. It is imperative to invest in our people just as much as we invest in the tools we use.

## Conclusion

As the cybersecurity landscape continues to shift, the training of incident responders should be a proactive and adaptive strategy, focused on robust team dynamics and practical, immersive experiences in simulated settings. This approach not only prepares teams for immediate threats but also builds a resilient organizational culture capable of withstanding future challenges. In the long run, the investment in training your cybersecurity team is likely to offer more substantial returns than simply acquiring another tool. Effective training ensures operational readiness and adaptability, key components for thriving in today's volatile cyber environment.

## About the Author

Tom Marsland, VP of Technology at Cloud Range, is a cybersecurity professional with over 22 years of experience in the information technology and nuclear power industry. He served over 22 years in the US Navy as a Nuclear Reactor Operator and Instrumentation and Controls Technician, working in nuclear engine rooms on a myriad of Navy submarine platforms. His final tour of duty was as the head of the nuclear-powered engine room for a fast attack Navy submarine with oversight of the entire propulsion and electric plant, and then as the lead nuclear supervisor for a squadron of three submarines. He has a bachelor's degree in IT security and a master's degree in cybersecurity. He's married to Jennifer, an Emergency Management Planner, and they have four children and two grandchildren. They reside in the Pacific Northwest, and in his free time, he enjoys backpacking through the Olympic and Cascade Mountains. Tom can be reached online at [tmarsland@cloudrange cyber.com](mailto:tmarsland@cloudrange cyber.com), [@tmarsland on X](#) and at our company website <https://www.cloudrange cyber.com/>.





## Securing E-commerce

### Navigating Regulatory Hurdles for Online Sales of Age-Restricted Products

By Andy Lulham, Chief Operating Officer at VerifyMy

E-commerce is poised to account for over [20% of global purchases](#) by 2024. This surge is fueled by a confluence of factors: the expansion of online product offerings, consumer pursuit of discounts, and the lure of convenience and broader selection. For e-commerce platforms, this trend underscores the critical need to ensure compliance with age verification laws to prevent underage sales of items such as alcohol, tobacco, vaping products, and firearms.

### The Complex Landscape of E-commerce Legislation

Navigating the labyrinth of e-commerce legislation is a formidable task, characterized by its complexity and variability across jurisdictions. Legal requirements fluctuate based on cultural norms, geographic regions, and regulatory frameworks, creating a patchwork of rules that e-commerce businesses must adhere to. For example, the shipment of alcohol is regulated by each state, and the requirements vary



greatly. While some states impose no restrictions on the types of alcohol products that can be shipped to their residents, others allow only beer or wine. For residents of Utah, all online alcohol sales are prohibited.

This lack of uniform regulations means that e-commerce businesses looking to sell age-restricted products must meticulously research and comply with local legislation. For the companies selling these products, understanding diverse regulatory landscapes is crucial to avoiding legal pitfalls and enhancing platform security.

## Challenges in Implementing Age Assurance

Implementing effective age assurance mechanisms presents a complex challenge, fraught with technological, ethical, and practical hurdles. The multifaceted challenges that these platforms face in integrating robust age assurance systems highlight the need for innovative solutions that can keep pace with compliance requirements and evolving threats. Key considerations include:

**User Experience:** One of the primary challenges in implementing age assurance is balancing diligence with user convenience. Consumers flock to online shopping for its ease, and any friction in the age verification process can lead to cart abandonment and lost sales. If customers face cumbersome verification steps, they may defect to competitors, potentially those with less stringent controls. Therefore, it is imperative for e-commerce platforms to deploy seamless and user-friendly age verification technologies that don't turn off their customers.

**Technology Solutions:** There is no universal solution for age verification; the approach must be tailored to the specific needs and compliance demands of different markets. Age assurance technologies range from email and facial age estimation to verification methods involving government-issued IDs, credit cards, mobile numbers, and even address checks. The chosen method must not only comply with legal requirements but also be inclusive and mitigate risks of bias and exclusion. E-commerce platforms must transparently communicate the necessity and usage of data collected during the age verification process. This transparency builds consumer trust, reassuring them that their data is being handled responsibly and securely.

**Collaboration and Compliance:** Compliance with age assurance regulations is a shared responsibility between online vendors and regulators. Vendors must implement rigorous verification processes, while regulators must ensure equitable enforcement. Effective collaboration with certified technology providers can help vendors develop frictionless, compliant age assurance solutions. This partnership is vital to prevent underage consumers from circumventing the system by exploiting less stringent platforms.

## Ensuring Safety Through Age Assurance

For online vendors, implementing seamless age assurance solutions is not just a legal obligation but also a business imperative. Proper age verification protects the company's reputation and prevents legal repercussions, ensuring that age-restricted products remain out of reach for underage consumers.

Vendors who fail to enforce these safeguards risk significant reputational damage and potential regulatory action.

## Final Thoughts

As the digital marketplace expands, the sale of age-restricted products online presents unique challenges that require diligent adherence to a complex web of regulations. E-commerce businesses must stay informed and agile, employing advanced age verification technologies that align with both global standards and local legislation. By doing so, they can safeguard their operations, protect their customers, and uphold the integrity of their platforms in an increasingly digital world.

### About the Author

Andy Lulham is the Chief Operating Officer at [VerifyMy](#), the safety technology provider on a mission to provide frictionless, trustworthy solutions for online platforms to maintain their integrity, protect their reputation and safeguard their users. VerifyMy safeguards children and society online by providing robust, yet proportionate, privacy-preserving age assurance, identity verification and content moderation solutions.



An industry veteran of 15+ years, Lulham has held previous roles in operations, marketing and international at brands including Betfair and Oddschecker. He is passionate about making the online ecosystem a safer environment for all, with a key focus on the implementation of enhanced content moderation solutions and privacy preserving age assurance technologies.

In his role at VerifyMy, Andy oversees the operations, marketing, legal & regulatory affairs and people divisions.



## The 3 Questions at the Core of Every Cybersecurity Compliance Mandate

By Cam Roberson, VP Sales & Channel Development, Beachhead Solutions Inc.

Cybersecurity compliance is undergoing a massive shift, with regulatory frameworks rapidly introducing more complex rules, stricter enforcement, and tougher penalties for non-compliance. We see this exemplified through the vast reach of the FTC Safeguards Rule now affecting millions of businesses, the recent changes in HIPAA enforcement to levy fines against more businesses, and the imminent arrival of CMMC 2.0's tighter controls.

To thrive in this more perilous regulatory environment, security and IT teams must adhere to even more comprehensive cybersecurity strategies that demonstrate effective protections to regulators and prevent data breaches. Fortunately, businesses can cut through the complexity of their cybersecurity compliance responsibilities with one simple technique. It all comes down to asking yourself three fundamental questions:

## 1. “Where is my data?”

The first step to securing data is knowing where it to find it. Once you catalog each device, data source, storage location and transfer point where data resides, you can define a cybersecurity strategy that builds a fortress around those targets. Pursue a process of data mapping and classification. Detail all data assets and classify data so that you fully understand what data is sensitive and subject to regulatory protections.

For instance, medical facilities with Personally Identifiable Information (PII) and health data covered by HIPAA, or a business with financial data regulated by FINRA, should flag that data as carrying special responsibilities for how it must be handled and secured. Crucially, a business should treat all devices and environments with the assumption that sensitive data resides there (even after performing data mapping) because, in practice, this is too often true—and under-securing such blind spots is a common recipe for a data breach.

To complete the picture on your data’s locations, perform a data flow analysis to track the flow of data through your business, from its creation to its deletion. Doing so will identify any channels where data transmission needs to be secured. Make sure that trustworthy file transfer solutions and encrypted communication protocols are in place to fully secure all data in transit.

## 2. “Who can access my data?”

Regulatory compliance often hinges on whether or not a business can prevent unauthorized access. Securing device and system access—thereby securing data against breaches and your business against regulatory action—should be accomplished via layers of safeguards and active security measures.

Implementing role-based access control (RBAC) empowers businesses to closely manage who can access data within its organization. By allowing each employee to access only the data they need to fulfill their role and tasks, a business vastly reduces internal threats and the risks that arise when a single employee’s device or credentials are compromised. Adding multi-factor authentication (MFA) will then protect data even in that inevitable credentials-have-been-compromised scenario.

Implementing continuous security monitoring to detect anomalous behavior and take automated and manual actions to mitigate attacks is essential, as is automated alerting to ensure swift security responses. Performing access audits to verify the effectiveness of access controls and recognize attack attempts is another important practice. Businesses can also harden access controls with automated protections that make data inaccessible when a device shows signs of compromise. This can include removing or quarantining a device’s data when the user fails too many login attempts, or when the device exits a geo-fenced area where access is approved.



### 3. “How do I keep data available but confidential?”

Going beyond robust access control, businesses must introduce layers of administrative and technical protections to ensure that data remains available to those that should have access, but confidentially protected from those that should not.

Among these protections, data encryption is an absolute requirement, for data at rest and data in transit. Implement end-to-end encryption with strong encryption protocols, and protect every device able to access your data with system- and user-level encryption to prevent both internal and external network-based threats. With effective encryption, even if an attacker does access data, they won't be able to read it.

Have robust backup and disaster recovery capabilities to make sure data remains available and that you maintain business continuity throughout and after an incident. This functionality should include regular data backups, off-site storage so that data remains secure even if attackers target backup data (which they often do), and regular testing to ensure you can execute an optimal recovery if and when the need arises.

A detailed incident response plan is another critical measure for achieving the best outcome in a high-risk scenario. Make a plan that includes a step-by-step procedure to follow when you need to detect, swiftly respond, contain, and recover from a data breach. At the end of the day, having a strong plan will meaningfully improve a business's circumstances and standing with regulators following an attack.

Finally, employee training is a key aspect of data confidentiality, because unsecure behavior by businesses' own workers is still the chief cause of data breaches. Continuously training and testing employees in the latest threats, from phishing schemes to credential management to safe internet browsing, pays dividends when it comes to maintaining security and compliance.

### Ask the right questions, get the right answers

With the consequences of insufficient cybersecurity and regulatory non-compliance growing more severe, businesses must take decisive steps to protect their customers from harm, and themselves from steep fines and damaged reputations. By asking the right questions about where sensitive data resides, who has access and how to keep data confidential and available, businesses can arrive at the right answer and implement comprehensive and compliant layered security protections.

## About the Author

Cam Roberson, Vice President, [Beachhead Solutions](#), a cloud-based platform providing PC & device encryption, security, and access controls necessary for compliance to CCMC 1 & 2, FTC Safeguards, HIPAA, ISO 27001, NIST guidelines, and more. Cam began his career with Apple Computer, where he held several senior product management roles in the computing and imaging divisions.

Cam Roberson

408.496.6936 x6866 (direct)

[croberson@beachheadsolutions.com](mailto:croberson@beachheadsolutions.com)





## Safeguarding Corporate Secrets: Best Practices and Advanced Solutions

How inDefend Ensures Comprehensive Security and Employee Monitoring for Modern Enterprises

By Mr. Dhruv Khanna, Co-Founder, CEO, Data Resolve

### Do you know where all the secrets are?

The probable answer to this might be NO and believe me you are not alone. The advancement of technology has overtaken us. Each individual has so many devices that it's difficult to keep track as to where all the data is!

### What would you classify as Secrets?

Passwords, API keys, Secure Tokens and all the confidential data of an organization.

Secrets (data) spreads everywhere in your system before you realise it. They can be copied and pasted easily. Insufficient audit and remediation capabilities are some of the reasons why secret management is hard. They are also least addressed by security frameworks. Yet these grey areas – where unobserved weaknesses remain hidden for a long time are blatant holes in your defense system.

A modern application uses many external resources that requires credentials. A company has people spread over in the premises, working remotely, using cloud storage, USB devices, etc. any leak of credentials or passwords can cost company dearly. Today's hyper connected systems bring an immense challenge to security in general and secret management in particular since the use of credentials has increased exponentially.

### So, how should you store such data?

All the sensitive data must be encrypted. It shouldn't be just lying around. It must not be stored in plaintext in any location.

Some points to be kept in mind:

- Control who in your team can do what.
- Share secrets with those team members only who need them.
- Control which application can do what.
- Monitor and audit secrets usage.
- Revoke access when team members leave.

Security Management consists of nurturing a security-conscious organizational culture, developing tangible procedures to support security and managing the myriad of pieces that make up the system. An effective system security depends on creating workplace environment and organizational structure where management understands, fully supports security efforts and users are encouraged to exercise caution.

### Certain points to be kept in mind:

- Staff must be made aware that protecting or safeguarding the secret is the responsibility of each employee having access to the sensitive information. Their awareness should be increased and also proper training must be provided.
- File Sharing is common in businesses but it must be done securely to protect sensitive data.
  - Encourage employees to send and receive files via email only
  - Use a security system that gives optimal security-appropriate visibility-access control-compliance system

Software to safeguard and monitor each activity must be installed that will protect the organization not only from internal threat but also from cyberattacks

### Some risks of File Sharing

- Release of Sensitive Data – When file is transferred from one end to another then there is a risk of an unknown person/party getting access to the information.
- Opportunity for attacks – When files are shared, there is a possibility of secrets falling into the hands of unknown who become the reason for attacks



- Installation of Malicious Software – when files are shared by mistake a dangerous file might be downloaded which would infect the system.
- Phishing/Ransomware attacks

These are the reasons that all companies must adopt ways of safeguarding their secrets through effective methods.

## Have you heard of inDefend?

inDefend is a Unified Suit for Insider Threat Management and Employee Behavior Analysis by Data Resolve – India's top leading company to protect us from Cyber Crime and Cyber Attacks and at the same time to monitor the employees of the organisation and their productivity.

This one product gives you so many features that it becomes a must for all organisations. It works from a single dashboard. Gives real time alerts through SMS and emails on any probability of data leakage. The product analyses the full system, knows exactly where all the secrets lie and forms a shield around it. Access to the data is allowed to only a few employees and a log of all the data sent or received is maintained. The best part is that this same product is used for our remote staff also. It monitors each and every employee of the organization irrespective of the strength and also manages BYOD. There is the screenshot facility that enables for the accountability of the employee. Application Sandboxing is yet another feature of the product wherein limited and required applications are allowed access and that too only on the company's network.

To know more, log on to <https://www.dataresolve.com/>

### About the Author

Mr. Dhruv Khanna, Co-Founder & CEO Data Resolve Technologies Pvt. Ltd.

With over 22 + years of experience in Enterprise Security and Privacy Service Industry, Dhruv Khanna, an Alumnus from IIMC, is successfully leading to build a robust environment to achieve a Cyber Secured Indian Market.

Before joining Data Resolve, Dhruv was associated with IBM for India-South Asia Service Line Leader for security and privacy services.

He is an active Cyber Security mentor with DSCI-Nasscom, India Accelerator, and many B-Schools, he is also mentoring Deep Tech CEOs on Business Strategy, Growth Strategy, GTM and Fund-raise for the last few years.

For more insights, visit at LinkedIn

<https://www.linkedin.com/in/dhkhanna/>

and at our company website

<https://www.dataresolve.com/>





## How Has Video Analytics Enhanced Security and Efficiency?

By Harshada Dive, Senior Writer, Allied Market Research

In recent years, video analytics has significantly transformed the interpretation and utilization of visual data. Through advanced algorithms and artificial intelligence methods, video analytics can perform tasks such as object detection, tracking, behavior analysis, facial recognition, and anomaly detection on recorded or live video streams. The primary objective is to convert raw video data into valuable insights applicable across various domains such as retail, healthcare, transportation, and security.

This advanced technology enhances surveillance, improves operational efficiency, and strengthens security protocols. By utilizing AI and machine learning, organizations can now extract insights from video content that were previously out of reach, enabling data-driven decisions and enhancing performance. According to a recent report published by Allied Market Research, the [global video analytics industry](#) is anticipated to showcase a remarkable CAGR of 22.7% during the forecast period.

The evolution of video management systems through IP-based surveillance and advanced analytics

There has been a notable surge in the adoption of IP-based surveillance systems, driven by the availability of high-resolution IP cameras and network video recorders (NVRs). This growth is further attributed to the expansion of IP infrastructure, increased tele-density, and a growing demand for remote

accessibility. Leading companies are responding by expanding their product offerings to include integrated video analytics features in IP-based security solutions. For instance, Bosch launched its "IP 3000i Cameras" in October 2019, which feature built-in video analytics capabilities.

The advantages of IP-based security cameras combined with advanced video analytics are manifold. They allow for remote viewing, smart data capture, and features such as identifying blocked emergency exits, managing queues, detecting intrusions, monitoring crowds, and even facial recognition. These technologies are widely used in various industries, such as retail, to effectively study customer behavior and demographics using IP-based cameras.

The increasing use of IP-based security cameras in various industries highlights the growing demand for robust video analytics solutions. This evolution enhances security measures, improves operational efficiency, and facilitates gathering business intelligence. For example, in the retail sector, IP-based security cameras equipped with advanced video analytics can offer valuable insights into customer behavior. By analyzing demographic data and shopping patterns, retailers can optimize store layouts, improve product placement strategies, and personalize marketing efforts, thus enhancing the customer experience and increasing sales potential.

### **Enhancing security through AI and machine learning in video analytics**

Enhancing security with the help of AI and machine learning in video analytics involves using advanced algorithms to analyze video streams in real-time, thus improving the ability to detect and respond to threats. AI can detect unusual behaviors, identify individuals, and categorize objects, reducing the necessity for manual monitoring and enhancing accuracy.

For example, AI-powered video analytics have the ability to detect suspicious behaviors, such as unauthorized access or abandoned objects, in airports or train stations. These systems can also recognize specific individuals through facial recognition, aiding in tracking persons of interest or improving access control in secure facilities.

Furthermore, machine learning algorithms can learn from previous incidents to refine their detection capabilities over time, adapting to emerging threats and enhancing security effectiveness. By integrating artificial intelligence into video analytics, organizations can achieve proactive security measures, faster incident responses, and more robust surveillance systems capable of handling complex environments with minimal human intervention.

### **Awiros implements AI-powered video analytics in Bengaluru's Safe City project**

On October 14, 2022, Awiros, a technology startup focused on advanced technology, announced a strategic collaboration with the Bengaluru City Police to enhance the city's surveillance capabilities as part of the Bengaluru Safe City project. This initiative, supported by India's Ministry of Home Affairs through the Nirbhaya Fund, aims to create a safer environment for women and girls in public spaces using cutting-edge technology.

Awiros implemented its video intelligence platform powered by artificial intelligence, which includes features like facial recognition and automatic number plate identification systems. This platform analyzes footage from over 7,000 high-resolution cameras installed across 3,000 locations in Bengaluru. The technology enables real-time monitoring and analysis of situations, enabling law enforcement to take preemptive actions against potential crimes, particularly those affecting women and children.

Yatin Kavishwar, Co-Founder and COO of Awiros emphasized the significance of deploying locally developed technology on such a large scale. He highlighted its role in enhancing citizen safety through capabilities such as suspect identification, real-time intelligence gathering, and ongoing monitoring of criminal activities.

### **Collaborative strategies for success in competitive industries**

Major industry players are making significant investments in advancing video analytics capabilities through extensive research and development initiatives. Their primary goal is to enhance algorithms, features, and overall performance to meet evolving industry demands. Simultaneously, they are also focused on developing user-friendly interfaces and providing scalability and customization options.

Moreover, these companies are implementing strategic collaborations with technology partners, system integrators, and industry stakeholders to broaden the accessibility of video analytics solutions on a global scale. For example, in May 2023, VinAI partnered with Qualcomm Technologies, Inc. to launch GuardPro, an AI-powered safety and compliance solution designed for smart cities. This solution emphasizes real-time monitoring of residential and commercial buildings in smart cities, aiming to improve safety measures and ensure adherence to regulations.

On the other hand, in May 2023, Claro Enterprise Solutions, a leading company in cybersecurity and IT services, introduced a new AI Video Analytics product developed by Iveda. This innovative solution aims to improve monitoring in public spaces, including schools and campuses.

To sum up, the rapid evolution of video analytics, fueled by AI and machine learning, is transforming surveillance across various industries. These advancements are enhancing security, streamlining operations, and enabling data-driven decision-making, resulting in safer, smarter, and more efficient environments for all.

### **How Has Video Analytics Enhanced Security and Efficiency?**

Video analytics uses advanced algorithms and AI to derive valuable insights from video data, continuously monitoring in real-time. It enhances security measures, improves operational efficiency, and facilitates data-driven decision-making in various industries such as retail, healthcare, and public safety. This technology is revolutionizing global surveillance techniques and enabling proactive security measures.



## About the Author

Harshada Dive is a Computer Engineer who loves to experiment with trending topics and is passionate about presenting these topics creatively to her audience. When Harshada's not writing, she is either gardening or listening to inspirational podcasts.

For More Details About This Topic: <https://www.alliedmarketresearch.com/video-analytics-market>





## The Imperative of Penetration Testing AI Systems

**Ensuring Robust Security and Integrity in Artificial Intelligence Applications**

**By Jesse Roberts, SVP of Cybersecurity, Compass Cyber Guard**

In the modern era of technological advancement, artificial intelligence (AI) is revolutionizing business operations, presenting unparalleled opportunities for efficiency and innovation. However, as AI systems become integral to our business processes, securing these systems has become more crucial than ever. Recognizing this critical need, President Joe Biden issued Executive Order 14410 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. This order mandates that the government conduct penetration testing on AI systems. Businesses should follow suit and start planning out testing before it is too late.

## Understanding Penetration Testing for AI Systems

[Penetration testing](#), often referred to as pen testing, involves simulating cyberattacks on a system to identify vulnerabilities before malicious actors can exploit them. For AI systems, pen testing is not just a precautionary measure but a necessity. AI systems, due to their complexity and the vast amount of data they handle, present unique security challenges. Vulnerabilities in these systems can lead to significant consequences, including data breaches, operational failures, and loss of trust. Imagine an AI system in charge of financial transactions or healthcare data being compromised. The fallout could be catastrophic, affecting not only the bottom line but also the company's reputation and legal standing.

## Why Pen Testing is Essential for AI Systems

The increasing reliance on AI across various sectors means that any [vulnerabilities](#) can have far-reaching impacts. The nature of AI systems—often built on intricate algorithms and extensive datasets—makes them particularly susceptible to specific types of attacks. Here are a few reasons why pen testing is essential:

1. **Complexity and Interconnectivity:** AI systems are often part of larger, interconnected networks. A vulnerability in the AI component can compromise the entire network.
2. **Data Sensitivity:** AI systems frequently handle sensitive and personal data. A breach could result in severe privacy violations and legal repercussions.
3. **Operational Impact:** Many AI systems are integral to critical operations. A failure could disrupt services, leading to significant operational losses.

## Key Steps in AI Penetration Testing

Approaching AI penetration testing with a trusted methodology is essential. Experienced penetration testers can conduct thorough tests if provided with adequate information. Here is a detailed roadmap for conducting effective pen testing on AI systems:

1. **Understand the Architecture:**
  - Comprehend the AI model architecture (e.g., neural networks, decision trees, etc.), the data flow, and how it integrates into the overall system.
2. **Analyze Data Handling:**
  - Know the types of data used for training and inference, including data sources, preprocessing steps, and how data is stored and managed.

### 3. **Conduct a Risk Assessment:**

- Identify potential threats and vulnerabilities specific to your AI systems. This initial assessment sets the stage for targeted and effective pen testing.

### 4. **Engage Experts:**

- Collaborate with experienced pen testers who understand the nuances of AI. These experts can provide insights and solutions tailored to your unique needs.

## Specific Testing Techniques

Pen testing should be tailored to the AI system in question. Here are some specific techniques to consider:

### 1. **Data Poisoning Testing:**

- Attempt to introduce corrupted or biased data into the training process and observe the effects. This helps in understanding how robust the model is against data manipulation.

### 2. **Adversarial Attack Testing:**

- Generate adversarial examples using techniques like Fast Gradient Sign Method (FGSM) or Projected Gradient Descent (PGD) and test the model's robustness.

### 3. **Model Extraction:**

- Try to replicate the model by querying it extensively and using the responses to reconstruct the model. This can reveal if proprietary models can be reverse-engineered.

### 4. **Input Validation Testing:**

- Test the system's handling of various inputs, including malformed, boundary, and large inputs, to check for vulnerabilities.

### 5. **API Security Testing:**

- Assess the security of APIs that serve the AI model, looking for issues like insufficient authentication, authorization, and rate limiting.

## Conclusion: The Imperative for Business Leaders

Ignoring the security of AI systems is no longer an option in a world where cyber threats are becoming more sophisticated. A single vulnerability can lead to significant financial loss, regulatory penalties, and damage to your company's reputation. Penetration testing is a proactive approach to identifying and



mitigating these risks before malicious actors can exploit them. It provides a comprehensive understanding of potential weaknesses and allows for the development of robust defenses.

Furthermore, as regulatory bodies worldwide begin to establish more stringent guidelines for AI security, companies that proactively implement thorough security measures will be better positioned to comply with these regulations. This not only helps in avoiding legal issues but also demonstrates a commitment to responsible AI usage, which can enhance trust among customers and stakeholders.

Investing in the security of AI systems also fosters innovation. By understanding and addressing potential vulnerabilities, businesses can confidently integrate AI into more aspects of their operations, driving efficiency and competitive advantage. Security measures should be viewed not as a hindrance but as an enabler of innovation and growth.

To effectively secure AI systems, continuous monitoring and regular updates are essential. Cyber threats are constantly evolving, and so should your security strategies. Penetration testing should be an ongoing process, integrated into the development lifecycle of AI systems to ensure that new vulnerabilities are promptly identified and addressed.

In conclusion, the future of business is inextricably linked with the safe and secure deployment of AI systems. By prioritizing penetration testing and comprehensive security measures, companies can protect their assets, maintain customer trust, and comply with regulatory requirements. The time to act is now. Engage with experts, conduct thorough risk assessments, and implement continuous monitoring to ensure your AI systems are secure and resilient against potential threats. The proactive steps you take today will safeguard your business's future and unlock the full potential of AI in your operations.

### About the Author

Jesse Roberts is SVP of Cybersecurity with Compass Cyber Guard. Jesse is an information technology & cybersecurity professional with over 20 years of experience in the field. He is a former professor of Network Engineering & Cyber Security at the New England Institute of Technology. Jesse holds multiple industry level certifications & has been invited to speak at events across the country. His presentations often include real-time live hacking demonstrations. He has also mentored students at various local schools and colleges through cybersecurity clubs over the years. In his role with Compass Cyber Guard, Jesse leads the organization's IT Security, Digital Forensics, and Incident Response teams. He is responsible for implementing innovative techniques and strategies to drive growth and improvement in these areas. Jesse can be reached online via [LinkedIn](#) and at our company website <https://www.compassitc.com/>.





## Why Did Snowflake Have a Target on It? Handling Data Warehouse Security Risks

By Kapil Raina, VP of Marketing, Bedrock Security

In early June, the Ticketmaster breach brought widespread attention to the fact that Snowflake accounts did not require multi-factor authentication (MFA) and some were compromised as a result. If only it were that simple. While MFA is an excellent compensating control, it alone is not sufficient to stop data breaches. Adversaries have no governing rules and can leverage several other techniques to bypass compensating controls, including MFA. For example, MFA doesn't work for non-human identities (that is, service accounts), which can make up 20% or more of a typical organization's credentials. It isn't just a question of whether MFA should have been enabled — MFA isn't enough. The question we really need to ask is, why are adversaries targeting systems like Snowflake and how can we harden these data-rich environments more effectively?

### Why Snowflake? Understanding the Target

Snowflake is a data-rich environment holding an organization's structured and semi-structured data sets for data storage, analysis, and processing. Many organizations use Snowflake because it's faster, more flexible, and easier to use than other database offerings. It's designed for the cloud as a self-managed

service, ideal for digital transformation initiatives. That ease of use has resulted in the aggregation of vast amounts of sensitive data from multiple sources. Inevitably, these data stores attract cyber adversaries because that data is ideal for identity theft, ransomware, social engineering, and other malicious activities.

Beyond the data held in Snowflake databases, it also offers extensive data integration capabilities that make it easy to move data into and out of the cloud data platform. Snowflake also offers [dozens of data integration tools and technologies](#) (Amazon Data Firehose, Google Cloud, Informatica, Apache Kafka, and SAP to name just a few). Its ecosystem of technology partners delivers connectors that make it simple to integrate with popular applications, databases, and cloud platforms. This ecosystem is easy to use, but also increases the potential attack surface for malicious actors. Snowflake is also part of a larger IT stack. As such, it may not always get security team attention. In addition, attackers may target vulnerabilities in other parts of the IT stack to gain access to the troves of data Snowflake holds.

## Modern Enterprises Are Data Dumping Grounds

As data continues to grow, organizations seek to find ways to use it, and Snowflake is integral to this use. Data pipelines automate many of the steps organizations had to take manually to transform and optimize those continuous data loads. The pipelines make it easy to move, analyze, use, and store data for future use; all of this is vital for business growth. However, data pipelines become, in effect, business-sanctioned Trojan horses. Lines of business use those pipelines to move customer data to warehouses for analysis without understanding how they may have created new attack paths for adversaries.

Data warehouses are also collaborative; businesses grant wide access to their employees to analyze and use that data, further increasing the data attack surface because it's so easy to move, copy, and share. Unfortunately, most employees often do not have the same security awareness training or accountability as a database administrator. Nevertheless, their accounts have access to massive amounts of sensitive data. What organizations must understand is that, fundamentally, data itself has no rules unless your organization puts protections in place to secure that data as it grows, moves, and changes.

## Reduce the Data Risk Surface

Attackers have already shown that they can [access sensitive data](#) using Snowflake accounts; in response, organizations must now act to reduce the data risk surface. They can do this in a few key ways: by minimizing data access, eliminating stale data, and hardening the data they have.

- **Minimizing data access** is critical when organizations have opened up data warehouses to allow multiple lines of business easy access to data. Security teams need to assess identity access to ensure that they are only granting users the minimum level of access required to perform their jobs, adopting the principle of least privilege. If a user's account is compromised, the attacker will only have access to a small subset of the data.

- **Using role-based access controls (RBAC)** to define user roles, for people and non-human identities alike, to manage permissions for reading, writing, and modifying data — with the context of the data being accessed.
- **Identifying and eliminating stale data.** Security teams must ensure that they know about all the data in the corporate environment. Often, stale data or “ghost” data exists that has been forgotten or lost, increasing the risk surface but providing no benefit to the organization. By finding and removing this information, organizations can reduce the overall risk surface without negatively impacting business outcomes.
- **Hardening data** is important, but only possible by identifying all sensitive data in order to encrypt, tokenize, mask, and anonymize data. This makes the data much harder for adversaries to use if they do manage to gain access.
- **Classifying and mapping data** comprehensively and continuously enables security teams to quickly identify the location, type, and business context of data if a breach occurs, thus making it easier to respond quickly and mitigate the impact of a breach.
- **Identifying and protecting intellectual property.** Many organizations don’t realize that there are categories of data that are part of their core IP. This may be information related to buyer technology, investment strategies, or something else. Regardless, this IP is important to the business and must be identified and protected, whether from a malicious attacker or inadvertent ingestion by an artificial intelligence model or chatbot.

## Minimize Overall Risk with Trust Boundaries

Modern organizations must manage and secure vast and growing amounts of data across diverse environments without unnecessarily limiting how the business can use the data. To protect data effectively, organizations need automatic and adaptable controls, such as trust boundaries. A trust boundary is the concept of establishing logical frameworks for grouping and managing data or systems access and control based on the sensitivity or classification level of that data to manage risk. While security teams can control access so that only those with a legitimate need have access to sensitive data, the volume of data today makes it all but impossible to manage without the automation and intelligent adjustments based on data context and needs that a trust boundary can provide. Static rules and human intervention simply cannot keep up with the scale and speed at which modern enterprises use data.

The Ticketmaster breach is far from unique. Indeed, it’s estimated that [about 165](#) of Snowflake’s customer accounts were affected in the recent hacking campaign targeting Snowflake’s customers. This should serve as a wake-up call for organizations worldwide: it’s time to prioritize data security. This is not the responsibility of the data warehouse or technology vendor, but of each organization to ensure that the right people have the right access to the right data at the right time.



## About Kapil Raina

As VP of Marketing, Kapil leads the Marketing Team at Bedrock Security, a leader in Data Security. As a Cybersecurity Marketing Executive for 20+ years, Kapil has built and led product, marketing, sales, and strategy teams at startups and large cybersecurity brands including CrowdStrike, Zscaler, VMware, and VeriSign.

Before joining the Bedrock team, Kapil led marketing for Preempt Security, which was acquired by CrowdStrike in 2020. He then went on to lead marketing for identity protection, cloud, observability, and zero trust products at CrowdStrike.

Kapil holds a BS in Computer Engineering from the University of Michigan, Ann Arbor, and he is a recognized speaker and author of books on AI, PKI, mobile commerce, biometrics, and other security topics.

Kapil can be reached on [LinkedIn](#) or via Bedrock's website, [www.bedrock.security](http://www.bedrock.security).





## Detection Engineering in Post SIEM and SOAR World

By Venkat Pothamsetty, CTO, Network Intelligence

A few years back, my security team was tasked to create and maintain a green field environment for FEDRAMP compliance. We made a radical decision, we opted to forego a Security Information and Event Management (SIEM) system entirely. This decision was not made lightly, but it was driven by two primary considerations. First, we wanted to eliminate any instance that required patching, and second, there was no off-the-shelf SIEM solution that was FEDRAMP compliant.

### Navigating SIEM-less Security and Compliance

In the absence of a SIEM, we had to navigate through the myriad of controls that a typical SIEM would cover. This included:

- **Logging Controls:** Every control mandates extensive logging.
- **Alerting Controls:** Particularly under Audit (AU) and System Integrity (SI) families.

- **Correlation Controls:** Necessary for detecting patterns and anomalies that many control families mandate.
- **Threat Intelligence / Malware controls:** SC related controls specifically related to malware.

We designed the architecture where subdivided the functionality that SIEM traditionally provided and distributed those functionalities to various components. Primarily -

- We leveraged AWS S3 (Amazon Simple Storage Service) for storage and
- We deployed numerous Lambda functions to funnel logs from various non-AWS-native applications into AWS S3.
- Several compute jobs to correlate logs from multiple sources

The effort is super successful. We managed the environment with barely one full time person, we come out of yearly audits in full colors, through multiple years of audits. Our success was largely due to the role security played in shaping the entire organization's practices.

We collaborated with all departments to ensure the following -

- We were able to collaborate with all the application teams and get all the logs in specific standard formats we needed them to
- We were to work with devops teams and make the environment managed and operated only through CI/CD pipelines, the DevOps team delivered. This seamless integration made correlating production alerts to approved change tickets effortless.

## Challenges Outside FEDRAMP Environments

However, replicating this architecture outside FEDRAMP environments proved challenging. I pondered about the reasons over multiple months as we encountered the hurdles. The reasons for the challenges are the same challenges that led the rise of SIEM and SOAR technologies in mainstream security engineering.

- **Log Format Control:** It is impractical to enforce a uniform log format across diverse sources, and so SIEM became a dump of all logs and a place to bring uniformity into all logs
- **Rule Development:** Writing rules against the various vendor-specific log formats at source is cumbersome, so learning a single SIEM DSL became preferable.
- **Centralized Intelligence:** Since logs are in a central place, SIEM systems evolved to provide intelligent log dumps, abstracting rule development and offering comprehensive dashboard capabilities.
- **Reach into the sources with API and conduct actions (SOAR):** As the SIEM management complexity grew, SOAR systems emerged to automate the response actions, checking sources, and conducting interventions.

## Rethinking Detection with GenAI

Let's flip the scenario. Imagine a world where all event and state data from internal and external sources neatly organized in well-structured JSON store. You have access to an unlimited, cost-effective log store that can organize these JSONs by various attributes like date and service. Correlating them becomes a manageable problem.

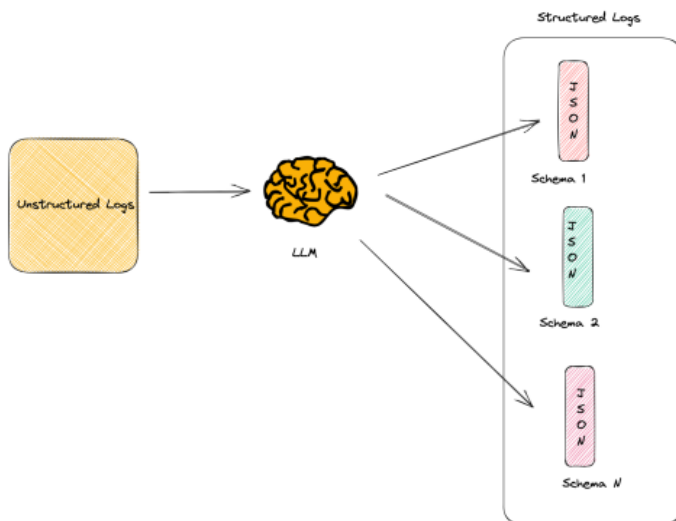
Let's look at the three major technical problems that are acting as hurdles for the dream

- **Normalization of Events:** Converting unstructured log data from each of the sources into JSONs of predefined, well-structured schemas.
- **Abstraction of Events:** Picking out relevant logs to query based on a procedure in MITRE TTP parlance for understanding the detection coverage
- **Writing rules for new attack patterns:** Writing rules as new threats arise, intelligently picking the right set of procedures and corresponding logs

GenAI presents solid solutions to the key problems above.

### Log normalization into structured schemas.

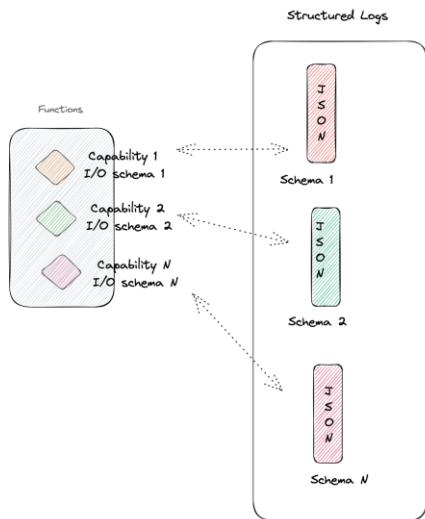
LLMs front ending some of the unstructured log content and making structured JSON to store into a JSON store





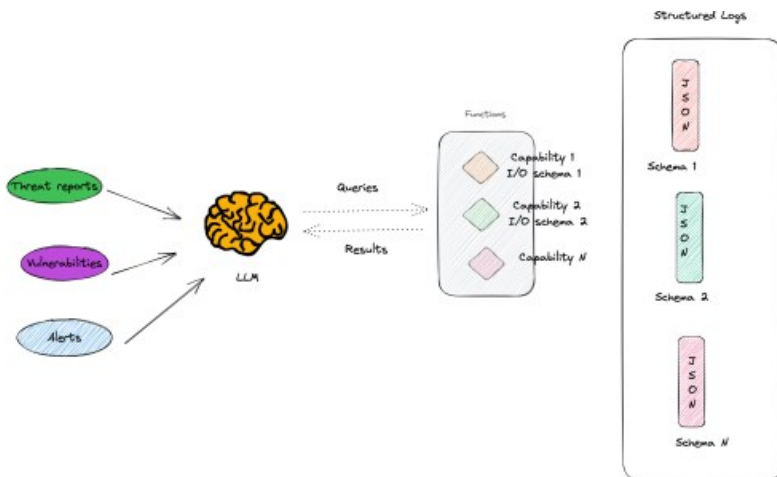
## Correlating logs and identifying patterns.

Callable functions based on the schema of each of the micro structured logs and has the description that describes the capabilities (essentially each function can be thought as a procedure finder in Mitre attack TTP parlance)



## Understanding threats and executing precise queries to detect emerging threats

An LLM agent that comprehends a described threat, makes queries various stores with specific schemas, and identifies emerging threats.



The above approach not only will make detection engineering possible without SIEM and SOAR but would make security engineers focus on actual development of code to detect new and emerging procedures as opposed to learn how to work with SIEM and write SOAR playbooks.

## About the Author

Venkat Pothamsetty is the CTO of Network Intelligence. Venkat took companies through their first 100K, first 1M, first 10M and 100M years to successful exits as products and security leader. With extensive leadership experience in product, engineering, pre-sales, and services teams at both Fortune 100 companies and startups, Venkat consistently hires and leads high-energy teams to deliver successful products in both SaaS and on-premise worlds. Notably, all of the startups that Venkat worked with went through successful liquidity events while he served as product head.





## Strategy Must Adapt

**Progressive web apps are great for user experience, but their browser capabilities demand more attention from security leadership**

**By Simon Wijckmans, CEO, c/side**

The release of iOS 16.4 has been a game-changer for mobile app developers: suddenly, teams can put full-fledged web browser capabilities into their applications. Almost any iOS mobile app can now be a [progressive web app](#) (PWA)—significantly reducing development and maintenance costs while also improving app performance and the all-important user experience. PWAs offer the best of both worlds when it comes to website and native app capabilities: they combine push notifications, offline usability, and access to device hardware (such as location tracking and the camera and microphone). Developers turning to PWAs give users a more powerful version of their company's website, with instant load times (since content is included in the app) and expanded feature sets.

All great stuff—except, in many cases, when it comes to security.

## The PWA security challenge

Functionally, PWAs turn almost every app into a browser, and teams need to better understand the specific and unique security issues that change invites. A typical modern website depends on dozens of third-party scripts from outside sources, scripts which are then executed in users' web browsers. These code scripts enable all kinds of common and necessary functions, from chatbot interactivity to captchas to social media features to marketing monitoring and analytics. Collectively, this browser supply chain has been an increasing target for hacks. But with businesses now leveraging their website browser supply chains within their mobile apps as well, this security risk (which has affected major companies from British Airways to [Kaiser Permanente](#)) has expanded even more quickly in the past few months.

## How to approach PWA security

Securing the browser supply chain to safeguard PWAs and end users' data requires a thoughtful and comprehensive approach. An effective browser-side security strategy should include continuous monitoring and alerting of these third-party scripts, regular auditing, infrastructure protections, and employee security training.

More specifically, comprehensive monitoring should cover both registry monitoring and browser-side script monitoring, vet all script requests in real-time, and detect and block any malicious activities as they occur and before damage is done. Third-party scripts should undergo full code integrity checks every time they run—and absolutely before they are ever sent to a user's browser. For registry monitoring, tools should be in place to proactively identify and eliminate threats, even before they reach the development environment. Sufficient monitoring should continuously scan and monitor the attack surface for threats, and provide immediate alerting and automated countermeasures when vulnerabilities, harmful scripts, and other active threats are surfaced.

Monitoring should also actively measure web script performance—with the multiple benefits of recognizing anomalies while flagging optimization opportunities and better experiences for end users. (Additionally, logging is crucial for enabling detailed historical analysis, especially in the aftermath of an incident.) Studying this analysis provides key guidance for understanding the most acute risks and improving security protections going forward. Conducting code reviews and audits at a regular cadence will also help make sure every script supporting a PWA meets its organization's established security requirements and policies.

On the infrastructure security front, implementing a web application firewall will detect and block inbound threats before they can reach web applications and exploit vulnerabilities. Organizations should also implement malware scanning to safeguard script functionality, such as form uploads or any other avenue where attackers might attempt to introduce malicious files or code. DNS security is also essential for preventing malicious attempts to hijack traffic and data.

Finally, regular security training must be provided to development and operations teams working on PWAs—continually keeping folks educated on the newest threats and evolving security safeguards. Even with tools in place, employees and their security awareness (or lack thereof) often still play a decisive role in whether attacks succeed or fail.



## Enable powerful mobile apps, curtail security risks

Organizations now have tremendous opportunities to harness the power of browser-enabled apps to deliver more engaging and valuable user experiences. By adopting and adhering to browser-side security best practices, teams can keep attacks on third-party browser scripts at bay without holding back on realizing PWA modernization.

### About the Author

Simon Wijckmans is the CEO of c/side. An expert on client-side security, he founded the company in 2024 after working in product management roles at Cloudflare and Vercel. Simon can be reached via LinkedIn (<https://www.linkedin.com/in/wijckmans/>) and at <https://cside.dev/>





# Demystifying Zero Trust

By Ashish Arora, AVP - Network Security, Chubb

## 1. What is Zero Trust

It was 2010 when term “Zero Trust” was coined by John Kindervag, a thought-leader in Cyber Security industry with a motto of “never trust, always verify”. Many high-tech organizations like Google analyzed the benefits of Zero Trust security and announced its adoption a few years later.

Zero Trust is a security framework of eliminating implicit trust from entities whether inside or outside of organization’s environment by authenticating, authorizing, and continuously validating them for security at each stage, to grant and keep access to application and data.

Zero Trust security includes several implementation models including Zero Trust Architecture (ZTA), Zero Trust Network Access (ZTNA), and Zero Trust Edge (ZTE) that are described below in brief. However, all these models are built around the same core concepts of Zero Trust security.

**Zero Trust Architecture (ZTA):** ZTA is the most popular security model for implementing Zero Trust. It renders security by eliminating implicit trust for all users whether inside or outside of organization’s network and continuously validating every stage of communication. In 2020 Zero Trust Architecture (ZTA) was accentuated with release of NIST publication 800 – 27<sup>1</sup> on the topic. The publication describes various approaches that can adopted for ZTA based on Identity Governance, Micro-Segmentation, and Software Defined Network. Furthermore, the publication describes the ZTA use-cases, associated threats, and migration approach for ZTA.

**Zero Trust Network Access (ZTNA):** Leveraging ZTNA model organizations can provide secure remote access to applications by creating identity and context based logical access boundaries based on access controls policies. Unlike VPN that grants access to entire corporate network, ZTNA defaults to deny and

provides only explicit access to selected applications or services. In ZTNA user's remote access request for application is authenticated via Identity Provider/Trust Brokers and assessed for risk based on various contextual parameters to result in approval or denial.

Zero Trust Edge (ZTE): ZTE is the refinement of Secure Access Services Edge (SASE), latter was introduced by Gartner, it combines the network and security functions in a cloud-based model. Secure access service edge (SASE) and Zero Trust edge (ZTE) share common principles and goals such as the consolidation of network functionality and cloud-delivered security. However, they differ in their emphasis and approach. ZTE considers every network transaction as risky regardless of nature or origin; emphasizing on zero-trust it amalgamates security solutions like ZTNA, Security Web Gateway, CASB, IDS/IPS, and Sandbox to provide a more secure access to application and data.

## 2. How Zero Trust Works

Zero Trust Security works following the security principles enumerated below:

- **Continuous Monitoring and Validation:** Monitor the access of resources all the time with re-verification of access continually and as the risk level changes.
- **Identity Verification:** Stringent verification of user identity against authoritative user repository or identity provider.
- **Strong Authentication:** Dynamic authentication values in addition to passwords to grant authorized access to users.
- **Access Control:** Verify the authorization of entity to access the requested resource as well ensuring the entity is not compromised.
- **Least Privilege:** Users have restricted access limited to what they need to perform in their roles and responsibilities.
- **Limit Attack Surface:** Implement no implicit access to entire network with users, applications, and systems getting access to specific applications/systems. Micro-Segmentation is a good example of this principle.

## 3. Why organizations should embrace zero trust

With evolving threat landscape, IT environments going borderless, and users connecting to corporate environment from anywhere, zero-trust has become a security imperative. Zero Trust may not be a silver bullet to eliminate all cyber threats from an enterprise environment. However, it substantially reduces the risks and curb the impact of cyber-attacks. Zero trust principles are relevant for all organizations with digital footprint regardless of their size albeit the type and scale of zero trust implementation may vary with organization sector and size respectively. To enumerate, below mentioned are some compelling reasons for why organizations are increasingly adopting Zero Trust:

**Enhanced Security Posture:** significantly reduced risk levels with verification of all access requests with continuous monitoring, attack surface limitation, and minimizing the damage.

**Improved Remote Workforce Security:** Traditional network security is insufficient to secure proliferating remote work culture. Zero Trust can render advance level of security to access requirements irrespective of user location.

**Protection from Insider Threat:** As zero trust doesn't trust even internal users by default, it minimizes the potential of insiders to do malicious activities deliberately or inadvertently.

**Curtail Blast Radius:** Even with strong security defense breaches may occur, with zero trust the compromise can be significantly reduced by blocking lateral movement of attacker.

**Regulatory and Compliance Requirements:** Organizations may have several security obligations under regulations and compliances applicable to them, most of them mandate strong access controls and data protection. As Zero Trust implies no implicit trust and continuous verification, it can be a significant constituent in meeting the relevant security requirements.

## 4. Key Pillars of Zero Trust

There are 5 key pillars of zero trust as described by CISA (Cybersecurity and Infrastructure Agency) of USA in their publication, Zero Trust Maturity Model<sup>2</sup>, initially released in September 2021 and updated in version 2.0 of the publication released in April 2023.

**Identity:** The foundation pillar, ensuring only authorized users and devices can access corporate resources. Identity verification, multi-factor authentication (MFA), role-based access control (RBAC), and identity risk assessment are keys tools IAM tools.

**Device Security:** To achieve and maintain high degree of zero trust it is imperative for organizations to ensure the devices connecting to corporate resources are secured in parameters of compliance to security standards/policy, threat detection and prevention, management of devices, inventory control, posture assessment, and risk management.

**Networks:** Lesser the implicit trusted network segments higher the maturity of Zero Trust in networking parameter. The maturity level can be assessed progressing with ordered implementation of macro segmentation, network resiliency, data encryption, dynamic network configurations, risk-aware network access/network access control, and micro-segmentation.

**Application and Workloads:** This pillar entails Zero Trust in parameters of security integrated hosting and access of applications. Security methodologies like separate production and non-production environments, static and dynamic security testing, CI/CD pipelines for formal code deployment, integrated threat protection in application workflows, application availability in public networks with continuously authorized access, and immutable workloads determine the maturity of Zero Trust in the realm of applications and system workloads.

**Data:** Probably the most crucial asset of your organization. Implementation of key data security controls like minimal to full encryption of data, manual to automated inventory and categorization of data, redundant data stores, DLP implementation, data labelling, and dynamic access controls can determine the maturity of Zero Trust in the data security of organization.



## 5. Disadvantages of Zero Trust

After highlighting the key advantages of Zero Trust for an organization in section 3, let's look at some of its challenges and if it is worth the investment and resources.

**Implementation Complexity:** Implementing Zero Trust to an appropriate maturity level may be a challenging task as it requires comprehensive understanding of existing networks, applications, and user workflows. Besides, it may entail implementation of additional advanced security controls which may have compatibility issues with legacy systems.

**User Experience:** Additional or enhanced identity and access management controls employed as part of Zero Trust implementation may lead to user frustration if not implemented effectively. Consequently, this can lead to resistance in Zero Trust adoption and users might try to bypass security controls thereby adding additional threat exposure to the organization.

**Resource Strain:** Implementation and maintenance of Zero Trust may be resource intensive as it requires significant additional man hours to do the required job leading to strain on IT resources.

**False Positives:** Stringent security controls as part of Zero Trust can lead to false positive events of legitimate users denied access with their activities flagged as suspicious.

## 6. How to Overcome Zero Trust Challenges

The issues in adopting a Zero Trust security model can be mitigated with careful planning and organized implementation techniques; here are some measures:

**Staggered Implementation:** Adopt the zero trust model in phases instead of a big-bang approach to ensure agile implementation and smooth transition, significantly alleviating the risk of disruption.

**Optimize User Experience:** Adopt user-friendly and seamless authentication technologies like single sign-on (SSO), adaptive authentication, and context-based access controls to minimize friction while maintaining strong security.

**Training and Communication:** Build user awareness campaigns for the Zero Trust Model; impart trainings about new user authentication and access controls technologies and workflows.

**Capacity Planning:** Spend significant time in planning Zero Trust implementation. Carefully determine and plan for resources required to implement and maintain the Zero Trust model.

**Continuous Fine-Tuning:** Regularly review your Zero Trust model to meet your security goals. Optimize pertinent security technologies by regular fine-tuning to reduce false positives.

## 7. Zero Trust Adoption and Roadmap

Zero trust is a priority for most of the organizations as part their journey to mitigate security risks and improve security posture. Most of the mid-size to large organizations have some form of zero trust strategy in place. However, only a few of them have been able to implement effectively. Gartner has predicted that by 2026, 10% of large enterprises will have a mature and measurable zero-trust program in place.

As zero trust significantly contributes to alleviate risks and improving security posture, its adoption by organizations will prevail around world. With relevant security professionals gaining better understanding on zero trust and associated technology, security companies making advancements in their zero-trust offerings, its adoption is expected to grow significantly in future.

### References:

<sup>1</sup> <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>

<sup>2</sup> [https://www.cisa.gov/sites/default/files/2023-04/zero\\_trust\\_maturity\\_model\\_v2\\_508.pdf](https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf)

### About the Author

Ashish Arora is AVP - Network Security in Chubb. He has more than 18 years of experience in planning, design, consulting, and implementation of Cyber Security Solutions and Services.

He is experienced in building Multi-Tenant Cyber SaaS platforms in public clouds, bringing enhanced security, cost optimization, and performance efficiency to organizations' overall security. He has built curated security solutions for hybrid environments spanning across Private and Public Clouds as well.

Ashish has industry leading certifications in Security domain like CISSP and CCSP. He keeps himself abreast with evolving threat landscape and techniques to mitigate them. He enjoys participating in various security conferences and industry events.

Ashish can be reached via email at [ashish\\_arora22@hotmail.com](mailto:ashish_arora22@hotmail.com), LinkedIn at <https://www.linkedin.com/in/ashish-arora-856a231a/>, and at the company website <https://www.chubb.com/>.





## How AI Is Transforming Cyber Risk Quantification

By Jose Seara, Founder and CEO, DeNexus

Cyber risks differ from other more familiar risks in life, such as the dangers of a car crash for drivers, or a natural disaster for homeowners. These are well-defined, measurable risks with associated costs that insurers can estimate.

Yet despite the sophistication of modern IT cybersecurity protections, most large organizations still lack substantial empirical data about the risks facing their industrial control systems (ICS) and operational technology (OT) at utility plants, refineries, and factories. This shortcoming is due to the limited availability of data about OT cyber incidents, and an inability to apply traditional actuarial methods to estimate the potential financial consequences.

The lack of data at these facilities makes inherent uncertainty a key challenge for quantifying and prioritizing cyber risk. To get a better handle on this problem, a new field has emerged called Cyber Risk Quantification and Management, or CRQM, which relies on risk transfer practices. New CRQM platforms benefit from the use of artificial intelligence and data-driven tools to better manage, mitigate, and eventually transfer cyber risks to insurers.

To address the glaring gaps in publicly available data and thus account for so much uncertainty, AI-data-driven CRQM platforms use probabilistic models such as Bayesian networks, and probabilistic graphical models. All these approaches can be applied with AI to explicitly represent uncertainty, as they assign probabilities to different outcomes, which helps the AI system make informed decisions based on uncertain data.

## You Can't Quantify What You Don't Understand

The volume of information required to monitor the interdependencies between cyber physical systems, networks, and the cloud has become too enormous to be processed by mere human intelligence. AI-powered systems can be used to logically identify and automate the processing of data from interconnected systems and analyze the data to deliver continuous outputs that are always up-to-date.

To underwrite a risk, one first needs to understand it. That is why risk data is the lifeblood of the insurance industry. But in many cases, the datasets for operational technology remain incomplete. Or there might be duplicate sources of data from different inputs. Having a precise process to reconcile and normalize all that ingested information requires the creation of a data ontology for cybersecurity.

When AI is fed with enough dependable data about cyber risk, it can bring unprecedented accuracy and speed to help understand risk. The underlying concerns include vulnerability detection, prioritization of security tasks, and the cascading impact of cyber incidents on a network of interconnected critical infrastructure.

By enabling a better assessment and quantification of cyber risk, especially for OT environments and cyber-physical systems, AI also enhances risk transfer practices. On one end, companies get a more thorough understanding of their cyber risk to decide what risk to accept, avoid, transfer, or mitigate. On the other end, underwriters get more evidence-based data to align their cyber insurance parameters, including their policy coverage and limits.

## Taking Advantage of AI in the Cloud

AI can help us quantify cyber risk and define the best risk mitigation strategies. Cloud-based CRQM platforms use AI algorithms to normalize and categorize ingested data from dozens of sources, including internal data and raw signals from cybersecurity solutions for intrusion detection and vulnerability management. In addition, natural language processing (NLP) is applied to analyze text and process cyber incident information about victims and threat actors.

To show the scope of computing efforts this represents, CRQM platforms regularly perform millions of Monte Carlo simulations on monitored sites to model the probability of different outcomes for a range of processes that cannot be easily predicted. These simulations run what-if analyses on suggested mitigation projects to identify the ones with the greatest positive impact on risk reduction. Machine learning is also employed to model complex dependencies in the aggregation of risk based on impact and frequency.



This bottom-up approach to risk aggregation enables CRQM platforms to reliably predict where and how incidents are likely to occur in each client's unique context, and then translate that information into dollars at risk. The critical financial metrics that CRQM delivers to CISOs include value at risk, probability of loss, financial impact of cyber incidents, expected ROI, and risk reduction from evaluated risk mitigation projects. By applying these CRQM principles coupled with AI techniques, CISOs and CFOs can work together to craft the most appropriate risk mitigation strategies for their distinct facilities.

## About the Author

Jose M. Seara is the Founder and CEO of [DeNexus](https://www.denexus.io/), a leader in Cyber Risk Quantification and Management for Operational Technology (OT) and Industrial Control Systems (ICS). Jose was previously the President & CEO of NaturEner USA (now BHE Montana) & NaturEner Canada from November 2006 to January 2018. During his time at NaturEner, Seara led the company through a leadership transition, working to ensure a smooth transition for the new team.



Prior to his time at NaturEner, Seara was a founding partner and member of the board of directors at DeWind Co from June 1999 to September 2002. Jose was also a founding partner and principal at PROYDECO Ingenieria y Servicios SL from January 2003 to December 2006, and a partner and director at Proyectos de Cogeneración SL from January 1999 to December 2003.

He holds an Executive Program degree from Singularity University in the field of Exponential Technologies. Jose also holds a Master's of Science in Naval & Marine Engineering from Universidad Politécnica de Madrid.

Jose can be reached at the DeNexus website: <https://www.denexus.io/>



## Spotlight on Dashlane

By Dan K. Anderson vCISO and On-Call Roving Reporter, Cyber Defense Magazine

Dashlane is the leading enterprise credential manager that secures access and proactively protects against breaches. In an era where painfully simple password spraying and phishing attacks are still the primary cause of breaches, Dashlane is an essential part of company-wide credential management and security posture programs, making the simple path secure for end users.

Trusted globally by over 23,000 organizations, Dashlane's product suite includes credential management (passwords, passkeys and secrets), user onboarding and offboarding, phishing alert systems, and initiatives to proactively bolster overall password hygiene and security. Leveraging cutting-edge technologies such as Confidential SCIM + SSO and AWS Nitro Secure Enclaves, Dashlane empowers organizations of all sizes to efficiently and effectively protect their employees and customer data.

As the leader in password management, Dashlane is perfectly positioned to lead the shift into a new era of authentication – a passwordless future. Dashlane was the first credential manager to enable users to create, save, and log in with passkeys across desktop and mobile platforms, making phishing-resistant authentication accessible to its millions of users. The company was also the first to eliminate the Master Password via Passwordless Login for the Dashlane app, allowing users to seamlessly access their accounts across different platforms and devices without having to create or remember a single password, making the login experience faster and reducing phishing risk.

**Users** My account ▾ 🔔

**SUMMARY**

- 0 out of 100 seats left in your account [Buy seats](#)
- 100% employees have accepted the invite [Re-invite users](#)
- 90 is your Company Password Health Score [Check how to improve](#)

🔍 Search

Active users
  Revoked users
  Pending invites
 [Change rights to](#)
[Revoke](#)
[+ Add new](#)

EMAIL	PASSWORD HEALTH SCORE	LOGINS	SAFE	WEAK	REUSED	COMPROMISED	LAST ACTIVE	RIGHTS
camille.reynaud@upshift.com	🔴 54%	6	6	6	6	6	Yesterday	Member
isabelle.hawkins@upshift.c...	🟢 99%	73	71	2	0	0	1 hour ago	Admin
martha.dawson@upshift.com	🔴 24%	75	15	52	8	10	4 hours ago	Member
oscan.khan@upshift.com	🟢 99%	243	242	0	1	0	1 min ago	Admin
anna.scott@upshift.com	Unavailable ⓘ	<5	-	-	-	-	3 mins ago	Member

Items 1-15 (450 total) [1](#) [2](#) [3](#) [4](#) [5](#) [>](#) 15 items / page ▾

## Elevator pitch:

Among hard-to-use, narrowly focused security tools, Dashlane stands out as the universally loved, comprehensive credential manager that empowers admins with tools they can set and forget, providing proactive protection with minimal effort. The product provides employees with seamless and secure access they need to do their jobs, and can be easily deployed and is easy for employees to use. That means a massive reduction in IT tickets about credential management and sharing, saving time and money.

Dashlane leads the industry in security quality, using the strongest encryption available with patented technology to protect organizations from breaches. The product also seamlessly integrates with enterprise's infrastructure, security stack, and workflows for holistic credential security that admins can mass deploy in minutes. Our Confidential SSO & Provisioning is compatible with the most popular IdPs.

Through a simple and secure product suite that includes credential management, phishing alert systems, initiatives to bolster overall password hygiene and security, and more, Dashlane is an essential asset for any company looking to protect itself against credential-based attacks. Put Dashlane in the hands of every employee to ensure every point of access is secure across apps, tools, and devices.

**Cybercrime statistics on the problem you solve?** According to Dashlane's analysis of millions of end users, the average business end user has over 70 passwords, with 13% being compromised and 46% reused. Across its entire customer base, encompassing both consumers and business users, the average user has an overwhelming 227 passwords. Given that compromised credentials are the leading cause of data breaches, maintaining robust password hygiene practices and safeguarding credentials is more crucial than ever for both employees and average users.

Dashlane secures 2.5B credentials and administers more than 100M logins per month across its user base.

### CEO quote:

"Dashlane's mission is to deliver the credential security every business and employee needs to thrive. Our goal is to make users part of the security solution by designing security that promotes behavior change and empowers IT and security teams to proactively protect their businesses against the most prevalent threats they face today." – John Bennett, CEO, Dashlane

### Customer quote:

"We had a lot of advocates for Dashlane, including our CTO. Our employees have evaluated many solutions but Dashlane was the one they wanted to work with," says Kartheek S., Head of Information Technology, Consero. "We're proud to tell our clients that we're using Dashlane, and really, we think that every company handling client credentials should use Dashlane."

### What does Gartner say about you? Why?

While Gartner does not have a Magic Quadrant for password managers, they did recently publish their first report on workforce password management (WPM). While they did not analyze the effectiveness of specific vendors, they did detail a number of key benefits to deploying an enterprise password manager, including increased security, better UX, lower IT costs (they cite that the average password reset costs a company \$70 each time), and enforcement of password security policy compliance.

From the report, Gartner's recommendations to organizations include:

- Employ a workforce password management solution to help enforce and manage password security policies at scale, with minimum impact to users' experience.
- Select a WPM tool that addresses your specific requirements by mapping vendor capabilities against the organization's unique environment and user journeys.
- Implement a WPM tool to augment the coverage of single sign-on (SSO) deployments and facilitate access to apps that do not support federated standards.



This mirrors the conversations we're having with customers, who are realizing that there are limits to SSO in terms of overall credential management as SaaS sprawl and shadow IT proliferate. Dashlane is proud to deliver an SSO-like login experience to non-SSO applications. We provide seamless and secure access to all employees, keeping them protected whether they're using an app their admin doesn't know about (shadow IT) or simply using an app that doesn't integrate with SSO.

### Who are your competitors?

Dashlane's competitors are other third-party credential managers, such as 1Password and Bitwarden.

### Why is your solution better?

**Passwordless login across all devices:** Whereas some password managers are increasing minimum character requirements, Dashlane became the first to eliminate the Master Password. Unlike competitors, Dashlane's passwordless login works seamlessly across platforms due to the design of its passwordless system, delivering users the same experience regardless of their device hardware and software.

**Privacy-first, confidential computing-based protection:** Dashlane's "zero-knowledge" architecture ensures only the user has access to their credential vault by limiting sensitive data processing locally to the user's device, drastically raising the difficulty of accessing user vaults. Dashlane is the only password manager that incorporates confidential computing, leveraging AWS Nitro Secure Enclaves, to provide the enhanced security required to offer the highest level of security for enterprises through its Confidential SSO & Provisioning integrations.

**Added phishing protection:** Dashlane was the first among competitors to alert users and IT admins when credentials are copied and pasted into an untrusted site (and already prevents auto-filling in these cases).

### How does your solution fit into a company's Cyber stack? What does it pair well with?

We easily integrate with the existing security stack of enterprises, from Identity Providers for SSO and user provisioning, to SIEM solutions such as Splunk. Thanks to our use of Confidential Computing, we allow admins to very easily configure and integrate Dashlane while maintaining the highest level of security.

## How are you funded?

Dashlane has raised more than \$190M in total funding from FirstMark, Sequoia Capital, Bessemer Ventures, Rho Capital Partners and others. The company is cash-flow positive, with healthy growth that allows Dashlane to invest into scaling its platform and building an enduring business.

## What is your 3-year product roadmap?

While we don't discuss specifics, what we can say is that Dashlane will continue to innovate in the following areas:

- Enterprise support and offering increased protection for all employees. The key is to give the admin visibility and control over the company credential hygiene with low effort, while making the product delightful for employees to adopt and use every day.
- Passwordless and leading the industry into a world without passwords and phishing. We are very active in the FIDO Alliance, pushing new passwordless standards such as passkeys and WebAuthn.
- Keep raising the bar around credential security and cryptography. For instance, we have been exploring the implications of post-quantum cryptography for Dashlane.

## How do you keep your key devs around?

We provide them with an attractive mission - we solve a real pain point for consumers and organizations - and interesting technical challenges to solve, in the fascinating cybersecurity industry. Our engineers are passionate about the field and finding solutions to provide the best of security and convenience to our customers.

We share a lot about what we do in Engineering on the Dashlane Blog:

<https://www.dashlane.com/blog/category/engineering>

## Tell me about a customer who implemented your solution and what metrics show they are happy with the solution.

Financial Services firm Consero boasts a 90% Dashlane adoption rate with users across India, the U.S., and Canada. Because Consero takes security so seriously, new hires automatically receive Dashlane training, which gives every employee a strong foundation for secure password practices. From simplifying onboarding and offboarding processes to providing quick customer support, and more, using Dashlane has paid dividends.

"We've increased our security and helped clients increase theirs," shares Kartheek S. Head of Information Technology at Consero. And it's not just passwords that Consero employees can save in Dashlane. "We can now also safely store answers to follow-up security questions, which saves us a significant amount of time every day."

## About the Author

Dan K. Anderson Bio, Winner Top Global CISO of the year 2023

Dan currently serves as a vCISO and On-Call Roving reporter for Cyber Defense Magazine. BSEE, MS Computer Science, MBA Entrepreneurial focus, CISA, CRISC, CBCLA, C|EH, PCIP, and ITIL v3.

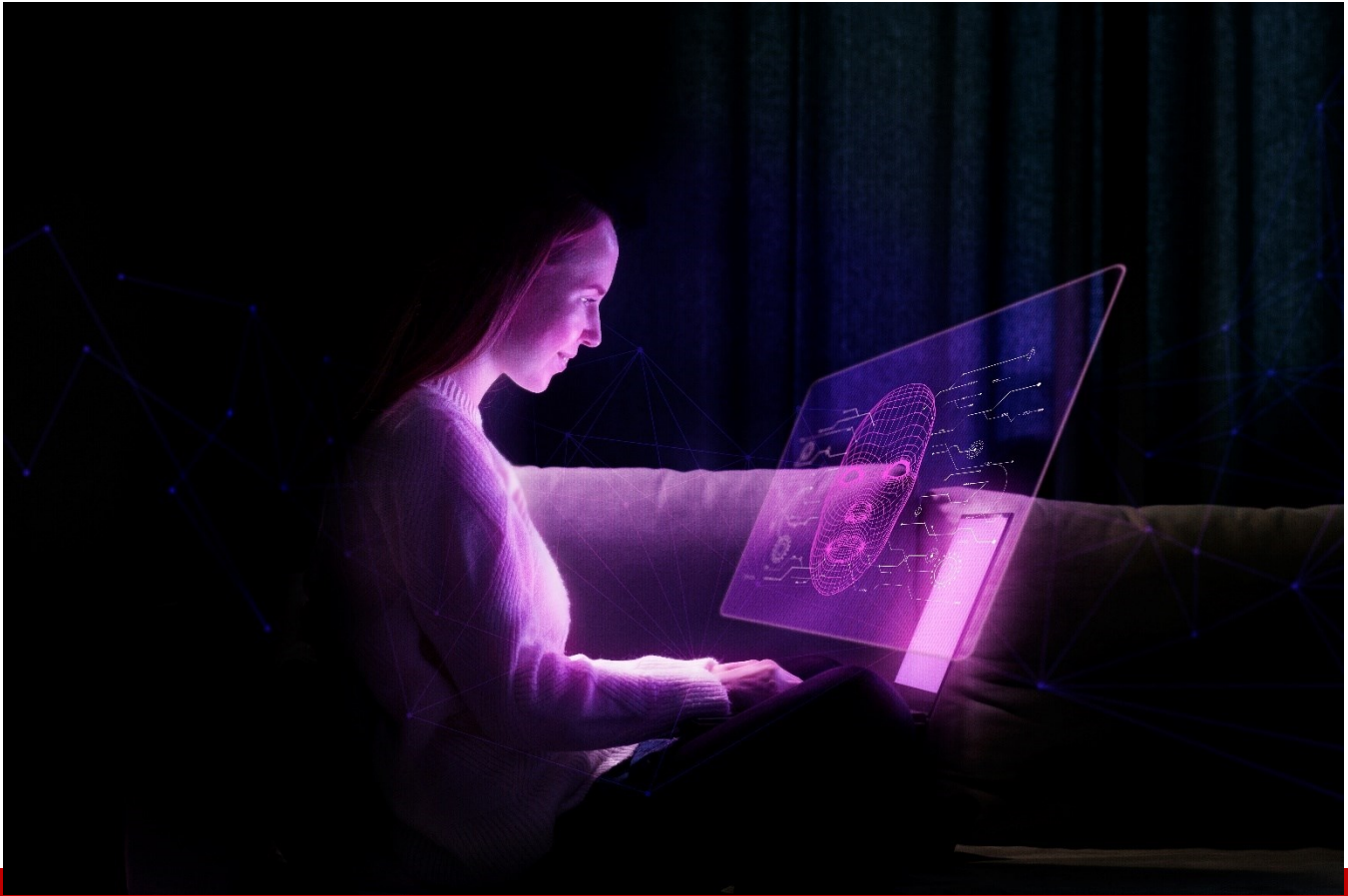
Dan's work includes consulting premier teaching hospitals such as Stanford Medical Center, Harvard's Boston Children's Hospital, University of Utah Hospital, and large Integrated Delivery Networks such as Sutter Health, Catholic Healthcare West, Kaiser Permanente, Veteran's Health Administration, Intermountain Healthcare and Banner Health.

Dan has served in positions as President, CEO, CIO, CISO, CTO, and Director, is currently CEO and Co-Founder of Mark V Security, and Cyber Advisor Board member for Graphite Health.

Dan is a USA Hockey level 5 Master Coach. Current volunteering by building the future of Cyber Security professionals through University Board work, the local hacking scene, and mentoring students, co-workers, and CISO's.

Dan lives in Littleton, Colorado and Salt Lake City, Utah [linkedin.com/in/dankanderson](https://www.linkedin.com/in/dankanderson)





## Spotlight on Onyxia

By Dan K. Anderson vCISO

Onyxia's Cybersecurity Management Platform delivers predictive insights and data intelligence that allow CISOs to gain a complete view of their cybersecurity program performance, achieve organizational compliance, increase security stack efficiency, and proactively optimize and communicate the business-level impact of their strategic security initiatives.

We collect and analyze data from the organization's entire security ecosystem. Based on the analysis, we provide the CISOs with continual program assessment and benchmarking as well as meaningful insights regarding their program performance.

Furthermore, with our OnyxAI predictive insights, we provide powerful suggestions for security program improvement (including resource and/or focus reallocation, security product replacement, etc.). Onyxia's Cybersecurity Management Platform enables CISOs to run 'What/If?' scenarios, receive relevant threat intelligence, and conduct business-level reporting.

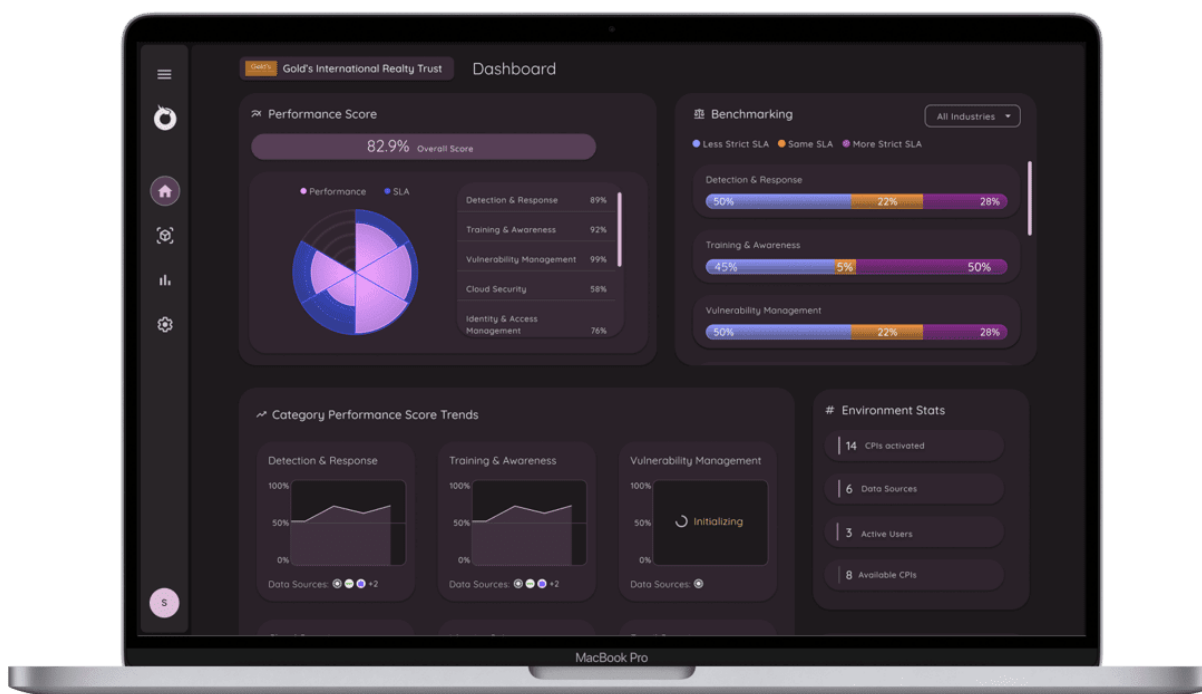


## Cybercrime statistics on the problem you solve

For 85% of CISOs and security leaders, managing and reporting on their security programs is a time-consuming process - done manually with numerous spreadsheets and/or by a team of analysts. In most cases, an organization operates with more than 50 security solutions, with CISOs needing to manage each one individually. And now, between the heightened demands of new risk management regulations and reporting rules and the need to stay ahead of ever-evolving threats, CISOs are truly facing an uphill battle.

## CEO quote

"We are seeing a real need in the market for security solutions that can simplify operations for CISOs, many of whom are still using spreadsheets to address challenges like measuring, reporting, and managing security programs," said Sivan Tehila, CEO and Founder of Onyxia. "New industry regulations such as those the SEC introduced last year place additional pressures on CISOs. Onyxia's Cybersecurity Management platform empowers CISOs to meet their growing responsibilities with a sophisticated, efficient, and accurate solution, delivering a predictive security platform created especially for them that leverages AI to fully harness insights, facilitate data-driven decisions, and maximize security efforts."



## Elevator pitch.

Onyxia's Cybersecurity Management Platform is the Salesforce for CISOs. We deliver powerful predictive insights and data intelligence so that security leaders can proactively improve risk management, ensure organizational compliance, and ultimately, bridge their security initiatives to the business.

## What does Gartner say about you? Why?

Most notably, Gartner recognized us as a Sample Provider in the Cyber Defense Planning and Optimization (CDPO) category. Gartner describes CDPO solutions as ones that can help CISOs "focus on reducing the attack surface without creating gaps in coverage of attacks" and keep their "focus on best-of-breed protection against major attack patterns."

## Who are your competitors?

For years, CISOs have relied on spreadsheets, teams of analysts and data visualization platforms to manage and report on their cybersecurity programs. We are disrupting the industry with a platform that enables CISOs to automate the measurement and management of their cybersecurity programs in a tailor-made way.

Gartner notes other players in the CDPO space as: CardinalOps, Enveedo, Posturity, Rivial Data Security, Veriti, XM Cyber and Zyston.

## Why is your solution better?

Onyxia is uniquely differentiated in three key areas:

1. **Utilization of AI to Improve the Security Program:** We are using AI to provide a deeper analysis of a user's data. Using this analysis, we share valuable insights into program performance and projected trends based on current SLAs. With the use of AI, we can quickly provide accurate and predictive analysis based on existing program data to help security leaders mitigate risks and prevent future crises.
2. **Customization and Personalization:** We give CISOs the ability to adjust what and how metrics are tracked, personalize the security stack map to add products outside of their program, and create detailed and visualized reports that align with the business-level message they want to present. With these customization abilities, we provide CISOs with a uniquely personal and relevant user experience.
3. **A Native Mobile Management Experience:** Onyxia is currently the only company that offers CISOs a dedicated Cybersecurity Management mobile app, enabling them to have complete visibility into their program anytime and anywhere. This is a drawing point for CISOs who appreciate constant access to the status of their programs.

## How does your solution fit into a company's Cyber stack? What does it pair well with?

The Onyxia Cybersecurity Management Platform sits above a company's cyber tech stack and is designed to pair seamlessly with those tools enabling an automated and real-time way for CISOs to manage, measure, and report on their entire security program. We integrate with many of the top security solutions like the Microsoft suite, CrowdStrike, CISCO and WIZ.

A core feature of our platform is our Security Stack Map, which enables CISOs to chart their cyber stack coverage to a NIST-aligned grid. This helps them to easily identify redundancies and gaps in their program tech stack and ensure organizational compliance.

## How are you funded?

We are a Seed-stage company with investments from WTV Ventures, Silvertech Ventures, and Angel Investors.

## What is your 3-year product roadmap?

As we move forward, we will also build out our offering for MSSPs with a multi-tenant platform, so that they can easily ensure that all of their clients have security programs that adhere to compliance frameworks and are cost-effective.

## Tell me about a customer who implemented your solution and what metrics show they are happy with the solution.

A client shared the time saving of at least 160 hours a month for an analyst. Instead of spending time on manual reporting of the program, the analyst can now apply this reclaimed time toward actual risk management strategy.

Another client is a publicly traded components manufacturer with over 40K employees globally and multiple subsidiaries. Before deploying Onyxia, their team spent hours pulling reports from dozens of disconnected security tools which proved vastly inefficient and inaccurate. With Onyxia, the client now has a central location to manage the performance of their entire security program, allowing them to focus more time on program optimization and risk reduction. Their security program now benefits from:

- Automated program measurement and benchmarking
- Streamlined Board reporting
- Full stack security and asset coverage visibility
- Achieves compliance more easily and aligns with security frameworks

## About the Author

Dan K. Anderson Bio, Winner Top Global CISO of the year 2023. Dan currently serves as a vCISO and On-Call Roving reporter for Cyber Defense Magazine. BSEE, MS Computer Science, MBA Entrepreneurial focus, CISA, CRISC, CBCLA, C|EH, PCIP, and ITIL v3.

Dan's work includes consulting premier teaching hospitals such as Stanford Medical Center, Harvard's Boston Children's Hospital, University of Utah Hospital, and large Integrated Delivery Networks such as Sutter Health, Catholic Healthcare West, Kaiser Permanente, Veteran's Health Administration, Intermountain Healthcare and Banner Health.

Dan has served in positions as President, CEO, CIO, CISO, CTO, and Director, is currently CEO and Co-Founder of Mark V Security, and Cyber Advisor Board member for Graphite Health.

Dan is a USA Hockey level 5 Master Coach. Current volunteering by building the future of Cyber Security professionals through University Board work, the local hacking scene, and mentoring students, co-workers, and CISO's.

Dan lives in Littleton, Colorado and Salt Lake City, Utah [linkedin.com/in/dankanderson](https://www.linkedin.com/in/dankanderson)







## Empowering Security Through Timely Nudges: Harnessing Behavioral Science for Real-Time Interventions

By Tim Ward, CEO of ThinkCyber Security

Picture this: your colleague's about to click a link that you know is dodgy. You see it happening from the corner of your eye and intervene just before it's too late, ready to offer a timely tap on the shoulder and guide them away from the risky action. Now imagine this happening every time they go to plug in a questionable USB stick, upload a sensitive file, or inadvertently reveal their credentials. Whilst it's almost impossible for humans to catch these risky behaviors in the act every time, this scenario takes nudge theory to its ultimate application—immediate, in-the-moment guidance that is even measurable.

But before diving into these real-time interventions, let's start at the beginning by addressing some fundamental questions:

- What is nudge theory?
- What is choice architecture?
- What constitutes a nudge and what does not?

- How to begin using nudges?
- What are the targets for implementing nudges?

## Nudge Theory and Choice Architecture

Nudge theory gained widespread recognition with the release of "[Nudge](#)" by Richard H. Thaler and Cass R. Sunstein, focusing on behavioral economics. They introduced the concept of "soft, paternalistic nudges," which aim to help people make beneficial decisions without restricting their choices.

Traditional methods of influencing behavior often involve 'forcing people,' which can be direct and require significant effort from individuals to change their actions. This approach is common in cybersecurity, where fear is often used as a motivator. However, poorly executed attempts can lead to resistance or disengagement.

In contrast, nudging employs a gentler strategy, allowing individuals to naturally make the right choices. Consider these examples:

When asking children to tidy their room, a directive approach would be instructing them, whereas a nudge might involve turning it into a game.

Signs that say "no littering" take a forceful approach, but simply providing and highlighting bins is a more nudge-based strategy.

In the context of healthy eating, counting calories and deliberately reducing portions can be a forcing approach that demands considerable effort, while using smaller plates serves as a nudge to encourage the behavior.

## The Role of Choice Architecture

In a later edition of "Nudge," Thaler and Sunstein emphasized the concept of Choice Architecture. They explained that all choices occur within a context, and that context greatly influences the decisions made. Choice Architecture involves designing this context in a way that steers choices in the desired direction. The authors point out that such an architecture always exists and will influence decisions, whether it is intentionally designed or not.

Moreover, our cognitive biases, shortcuts, and heuristics shape our decisions. By understanding the interaction between the environment and these biases, we can better guide people toward optimal choices.

## Decision-making and Cognitive Biases

To grasp this concept, we need to consider how we make decisions. While we like to believe that our decisions are deliberate and well-considered, only about 5% of them actually are. Around 95% of our

daily decisions are made more automatically. In these instances, the brain manages information overload by relying on shortcuts. Here are some real-life examples of choice architecture:

At a supermarket checkout, there will always be a shelf. The choice of what to place on it is an example of "architecting" the choice. Placing confectionery at the checkout promotes unhealthy choices, while placing water, vegetables, and fruit promotes healthier decisions.

Numerous studies on nudging have been conducted in school cafeterias, focusing on guiding children towards healthier choices. Researchers discovered that simple strategies, such as making fruits and vegetables more appealing with creative names or placing them at eye level for convenience, positively influenced children's choices. Additionally, normalizing the choice by having servers ask, "Would you like to try this?" also proved effective.

## Effective Nudges and Behavioral Models

Effective nudges leverage an understanding of cognitive biases and behavioral science to craft messages with maximum impact. This involves not just wording but also context and timing. Several models can help conceptualize how to apply nudges. The [MINDSPACE](#) acronym, developed by the UK government's Nudge Unit or Behavioral Insights Team, offers a framework. For the most straightforward applications of nudging, we focus on tweaking and refining messages we already send. If we're already communicating with our organization about security awareness, we should consider how to make those messages as effective as possible. Each letter in MINDSPACE represents a key element to consider for enhancing the impact of a nudge. For instance, M for Messenger emphasizes the influence of the information source, and P for Priming highlights the impact of subconscious cues.

A simpler alternative to MINDSPACE, developed by the Behavioural Insights Team, is the [EAST model](#). This model highlights the key characteristics of an effective nudge by suggesting that effective nudges target behaviors that are easy to perform, attractive, social, and timely.

Designing nudges goes beyond merely fine-tuning messages; it involves creating environments where desired behaviors are effortless, and messages are delivered at the right time. While nudge theory can refine communication wording, models like MINDSPACE and EAST underscore the critical role of timeliness and relevance. Messages in Slack, Teams, or emails are effective only if they address relevant risks or behaviors in those platforms. If not, they fail the timeliness and relevance test and may just come across as nagging.

## Challenges with Traditional Approaches to Cybersecurity Training

In the cybersecurity field, traditional methods often overlook how people learn and behave. Annual e-learning or PowerPoint presentations are untimely, lack context, and rarely facilitate ease of understanding. In fact, recent [research](#) revealed that 60% of cybersecurity professionals only receive training once a year (or even less frequently!) Given that cyber threats are constantly evolving, this sort of "snapshot" training doesn't go far enough to help keep your people up to date on the latest cybersecurity threats. Tools

like phishing simulations or SIEM-based behavioral analyses that follow up with training also fall short as they often come too late and may be perceived as punitive.

## Use Nudge Theory for More Effective Training

The ideal solution lies in timely, context-aware interventions, delivered at the moment the behavior occurs. Nudge-based approaches hold significant potential for enhancing security awareness by leveraging context and timeliness to embed desired behaviors. What does applying this to security awareness training look like?

- **Make it Timely** - Annual or even quarterly awareness efforts are insufficiently timely. Instead, we should consider drip-feeding content more frequently throughout the year, ensuring it is an ongoing effort. Additionally, making the content topical can leverage the availability heuristic; linking it to current news or making it personal by referring to individuals' personal lives and security can make it more impactful.
- **Make it contextual** – Providing nudges with pragmatic advice, at the moment of greatest risk, really helps people understand the impact their actions may have and make the safer choice.
- **Make your awareness easily accessible and user-friendly** - Keep it quick and simple to understand, offering advice that is easy to follow and actionable.
- **Motivate People** - Assist people with threat assessment by setting it in a personal context, which we found to be highly effective. Since we care deeply about protecting ourselves and our families, we are more likely to pay attention. Incorporating real examples, stories, and curiosity can significantly enhance the saliency and relevance.

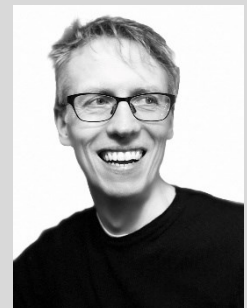
People don't always make rational decisions! Nudge theory explains that our brains often take shortcuts, influenced by cognitive biases and context. Our goal is to leverage this tendency to guide people towards actions that are in their best interest. Nudging involves designing the choice environment, recognizing that there will always be a choice architecture. Therefore, we should "architect it" to achieve the most positive outcomes.

By examining examples of effective nudges, the MINDSPACE model, other behavioral frameworks, and in-the-moment nudges, we can explore how to run campaigns to steer behaviors, what effective nudges look like, how to deliver them, and their potential impact.

### About the Author

Tim Ward is CEO and Co-Founder of Think Cyber Security Ltd. Tim has worked in IT for over 25 years with organisations including Logica, PA Consulting, Sepura and was previously Global Head of IT for the cyber division of BAE Systems (Detica).

Tim can be reached online at <https://www.linkedin.com/in/tim-ward-cyber/> and at our company website <https://thinkcyber.co.uk/>







## Unlocking the Right Encryption

**A Guide to Government System Protection**

**By Ben Warner, VP of Strategic Accounts, CRU Data Security Group**

The ever-evolving landscape of data security demands constant vigilance, especially for those handling Controlled Unclassified Information (CUI). A presentation by Greg Cooper, Cybersecurity SME & Security Engineer, at the USAF Cyber Monthly meeting shed light on common misconceptions surrounding data encryption and the critical role of obtaining the correct certifications for your specific data classification.

While encryption is widely understood as a crucial security measure, misconceptions abound. A common fallacy is that focusing solely on encrypting data-in-transit offers sufficient protection. The reality is far more nuanced. Technical data, for example, can also qualify as CUI, requiring robust encryption strategies.

Perhaps the most critical takeaway concerns the limitations of FIPS 140-3 compliance. While this standard offers a baseline for cryptographic modules, it doesn't guarantee CUI protection. For CUI

encryption, solutions must hold NIAP-CC certification, ensuring they meet rigorous security standards established by the National Information Assurance Partnership (NIAP).

NIAP plays a central role in evaluating cybersecurity products for use with CUI and Classified (CSfC) data. Overseen by the National Security Agency (NSA), NIAP validates FIPS-compliant modules against established Protection Profiles. This rigorous evaluation process typically takes 90-180 days.

For data classified as National Security Systems (NSS), cryptographic requirements are dictated by Commercial National Security Algorithms (CNSA). Crucially, CNSA 2.0 introduces new algorithms, with a 2025 deadline for transitioning to these updated standards.

## The Importance of Choosing the Right Encryption

According to the Defense Contract Management Agency (DCMA), failing to meet the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 security requirements has been the number one finding across the last three years of audits for Department of Defense (DoD) contractors [1]. This highlights the critical role that proper encryption plays in securing Controlled Unclassified Information (CUI) and Classified data.

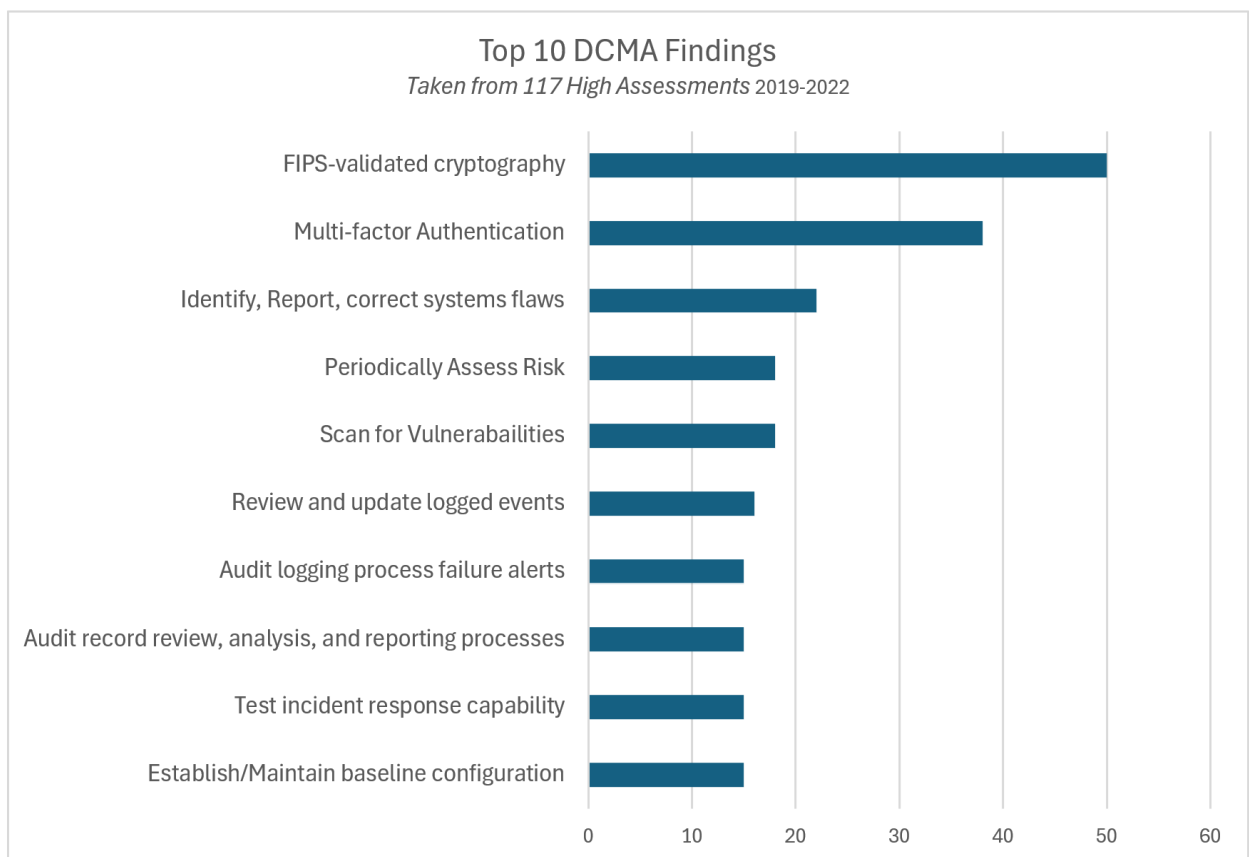


Image Data Source: Defense Contract Management Agency (DCMA) – Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) Powerpoint

Obtaining the right encryption solution hinges on understanding the classification of your data. Here's a breakdown of the encryption requirements for CUI and Classified data:

### **Controlled Unclassified Information (CUI):**

Encryption mandated by AFMAN 17-1301, paragraph 4.7 [2].

Cybersecurity products require NIAP-CC certification.

### **Classified Data at Rest (DAR):**

Must use NSA-approved cryptographic and key management systems [2].

Two approved options:

Government Off-the-Shelf (GOTS)/Type 1 hardware

Commercial Solutions for Classified (CSfC)

### **Understanding the Differences Between NIAP and CSfC**

While leveraging industry innovation through the CSfC strategy offers efficiency benefits, it's important to understand the key differences between CSfC and NIAP-certified products. CSfC solutions require two independent layers of encryption for adequate protection, differing significantly from the single layer approach employed by NIAP-certified products.

### **The Role of Authorizing Officials (AOs) and Path to NSA Approval**

Authorizing Officials (AOs) play a vital role in ensuring proper implementation of all security requirements outlined in the Capability Package (CP). This includes reviewing compliance matrices and signing off on the Registration Form.

The presentation concluded with a detailed overview of the process for obtaining NSA approval for both CUI and CSfC solutions. By understanding the nuances of data classification and the appropriate encryption solutions, organizations can ensure the confidentiality and integrity of their sensitive information.

Remember: Encryption is a powerful tool, but its effectiveness hinges on selecting the right solution for your specific data classification. Don't be fooled by common misconceptions – ensure you have the correct certifications in place to safeguard your valuable information.

## Glossary

CNSA: Commercial National Security Algorithms

CNSS: Committee on National Security Systems

CNSSI: CNSS Instruction

CNSSP: CNSS Policy

COTS: Commercial Off-the-Shelf

CSfC: Commercial Solutions for Classified

DAR: Data at Rest

CP: Capability Package

DCMA: Defense Contract Management Agency

DoD: Department of Defense

GOTS: Government Off-the-Shelf

IA: Information Assurance

NIST: National Institute of Standards and Technology

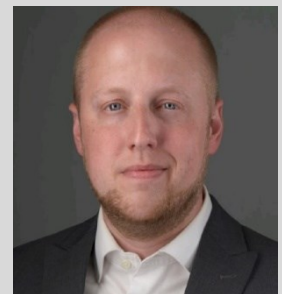
NIAP: National Information Assurance Partnership

NIAP-CC: National Information Assurance Partnership / Common Criteria

NSA: National Security Agency

### About the Author

Ben Warner, CRU Data Security Group | Throughout his career, Ben Warner honed his cybersecurity expertise working with the United States military. He worked on projects involving security and protection of networks holding some of the nation's most sensitive and classified information with Applied Research Solutions at Wright-Patterson Air Force Base. He has also worked with Booz Allen, a leading cyber defense contractor, and GE Aviation, and is a veteran of the U.S. Air Force. Ben can be reached online at [linkedin.com/in/davidbenwarner/](https://www.linkedin.com/in/davidbenwarner/)







## Cyber Threat Intelligence (CTI) for Supply Chain Monitoring

When companies outsource work to a third party, they do not outsource the security risks to the supplier. Instead, they inherit the security risks of the companies in their supply chain. CTI allows companies to identify these risks before these risks victimize them.

By Shawn Loveland, COO, Resecurity

### Executive summary

Many companies face various risks across their supply chain, which are increasing, especially cyber threats. Studies indicate that nearly all companies have at least one supplier that has recently, currently, or will soon be breached, and many more will be compromised in the next year. Further research shows that in nearly every company that suffers a breach, precursor signals of the breach could have been found on the dark web if the company was looking for them. Resecurity's research reveals that over 60% of all company breaches originate from a company within their supply chain, which increases to over 90% if technology providers are included. Although some companies assess the risk of potential suppliers during the evaluation phase, very few have the resources or mandate to monitor all their suppliers continuously. An organized CTI effort can provide companies with an economical and easy way to

monitor their suppliers and determine their risk profile and the likelihood of a breach by implementing CTI practices. This paper draws many parallels to Resecurity's previous paper, "[Active Dark Web Intelligence for M&A](#)." CTI research can answer critical questions that can help companies understand the risks associated with their supply chain, including:

- Standard suppliers, by evaluating the precursors of a breach:
- How does this supplier compare to the cybersecurity risk with its competitors and other suppliers?
- If the company is a technology supplier and has released a new security patch, is (or will) the N-day they have patched being actively exploited by threat actors?
- Has a data breach or loss been detected that could cause regulatory or privacy concerns and materially affect their company or pose a risk to their customers?
- If my customers monitor their supply chain, what are they observing about my company?
- Critical suppliers, identifying actual breaches:
- Is the supplier experiencing a data breach, or has it experienced an undisclosed one in the past?

What is the likelihood of the supplier being targeted, and will this result in a material data breach?

How does this breach impact my company as their customer? Has the supplier leaked strategic IP that affects my company, employees, or customers?

Has the company been involved in an unknown or undeclared material breach, as the recent SEC rule 7 defined? Did my company inherit these identified issues?

Is the supplier at risk of an insider threat from disgruntled employees offering data or services on the dark web that could impact my company or customers?

If my competitors monitor the dark web for breaches of their competitors, what are they observing about my company?

---

**In May 2023, a group of hackers, known as CL0P (TA505), started exploiting a zero-day vulnerability in MOVEit - a file transfer software managed by Progress Software. The breach by the numbers:**

**More than 62 million individuals were impacted.**

**Over 2,000 organizations were breached.**

**Approximately 84% of breached organizations are US-based.**

**Approximately 30% of breached organizations are from the financial sector.**

**The financial impact of the attack is over \$10 billion.**

---

Organizations inherit the cybersecurity risks of their suppliers. Unfortunately, many companies do not conduct adequate cyber risks to determine if a supplier has been breached or if there are precursors of a breach available to the threat actor to breach the company if they elect to. This lack of involvement can increase the risks of inheriting risks. Controlling cybersecurity risks can be increasingly more complex in the fast-paced business world. At the same time, information security departments need more personnel and resources to keep attackers at bay.

### **CTI can monitor for cyber risks in the company's supply chain**

Supply chain or third-party vendor disruptions can cause operational chaos. Specifically, if an organization experiences unauthorized access can lead to negligence claims, significant fines, contract disputes, potential lawsuits, loss of revenue, and even reputational harm. Therefore, companies must secure their data by having robust vendor agreements that address data security and outline their responsibilities in case of a breach. They also should monitor their suppliers for a potential breach that could impact their company or customers.

In January 2024, the US Department of Health and Human Services received reports of 24 healthcare data breaches, affecting 10,000+ records each. **Perry Johnson & Associates, Inc.** (PJ&A), a transcription service provider, reported two of the breaches. In November 2023, a cyberattack affected almost 9 million individuals. **Concentra Health Services** and **North Kansas City Hospital** added to the total of over 13.45 million affected individuals. [Source](#)

In April 2023, **Shopify** suffered a data breach that affected over 100,000 merchants who used their online store services. The breach occurred due to a malicious code injection in a third-party app called **Mailchimp**. Attackers accessed customers' names, email addresses, payment information, and order details. Shopify faced lawsuits, regulatory scrutiny, and potential fines. [Source](#)

In Jan. 2023, **Peloton** announced that **Strava's** third-party software caused a security flaw that exposed personal and health data of 3 million users. Names, emails, workout stats, and heart rate data were compromised. Peloton faced legal action and reputational damage as a result. [Source](#)

In 2021, **T-Mobile** disclosed a data breach that compromised the personal information of over 50 million customers. The breach was due to a compromised server rented from a third-party cloud provider, resulting in lawsuits, regulatory scrutiny, and potential fines. [Source](#)

In 2021, a ransomware attack on **Colonial Pipeline** caused operational disruption for several days. The cybercriminals exploited a leaked password from a third-party vendor, leading to gas shortages and price increases in the US. Despite paying \$4.4 million as ransom, Colonial Pipeline suffered significant losses from the attack and recovery efforts. [Source](#)

It is common for companies to do CTI analysis to protect themselves. Some companies use internal resources, and others use external resources to determine the supplier's cybersecurity posture, including a perimeter scan of the supplier's network, scans of low-end cybercrime data (TOR), and a review of the company's source code. CTI can enhance this vetting by focusing on threats based on access to the **Surface Web, Dark Web (TOR) / Deep Web**, and **Vetted / invite-only cybercrime communities**. This allows for the following questions to be answered with high confidence:

Is the supplier breached, and if so, by whom? What is their motivation? What data has been leaked?

Are there precursors of a breach that a threat actor could use to breach the supplier if they elected to do so?



---

**Resecurity's analysis has determined that only relying on data from the surface web and TOR will miss over 75% of the precursors of a breach and actual breaches.**

---

## One size does not fit all

Companies and their CTI vendors must understand that a single solution does not meet every company's needs. To address this, companies and their CTI vendors must collaborate to determine their needs and constraints. The CTI vendor must assist their customers in selecting the right combination of services to meet their requirements, including budget, timeframe, confidence, rules of engagement, and depth of insights.

This visibility is critical in providing accurate CTI. For example, Resecurity provides our customers insights based on:

- Continuously monitoring over 31k sources.
- Tracking over 38M threat actors
- Has collected, and continues to collect, billions of compromised credentials in the possession of threat actors.
- Has collected and continues to collect botnet records for billions of malware-infected devices.
- HUMINT researchers can dig deeper to answer questions that can't be answered by analyzing dark web data.
- Managed threat detection, including 0-day and N-day discovery and analysis.
- Industry-leading primary research, digital forensics, Red teaming, identity protection, and more.

## The type of information that is available

Through Resecurity and other analyses, it has been observed that there is a high correlation between the precursors of a security breach and an actual breach. Three common precursors: By analyzing dark web data, HUMINT researchers can dig deeper to answer questions that can't be answered. This data is traded among threat actors, sold in bulk, or sold by initial access brokers. In addition to these observable precursors, Resecurity **HUNTERS** provides additional intelligence about undetected breaches through traditional methods. Companies can use this data to prevent threat actors from using it as a beachhead in their company's or supplier's networks.

## Breach data

The trend of compromised accounts discovered on the dark web indicates the timing of breaches of services the company and its employees use.

For example, analysis of trends for a random Fortune 500 company, which is a supplier to nearly all customers in the US. Areas of concern:

6,273 compromised employee accounts were discovered on the dark web from 1/1/22 until 11/30/23. With a concerning trend of more compromised accounts of their employees leaking into the dark web.

Seven concerning spikes in the data indicate the company was breached or a significant company in their supply chain was breached.

### Botnet data

The trend is that the number of PCs used by this company's employees was compromised with malware. When the PC was compromised with malware, the employee's username, password, device fingerprint, and security tokens were also compromised. Threat actors typically buy the rights to push their malware to these devices, after which they have complete control over the victim's PC.

For example, an analysis of trends for the same random Fortune 500 company shows additional areas of concern:

- 5,406 PCs used by their employees were infected with malware from 1/1/22 until 11/30/23.
- A concerning trend of PCs being infected with malware since Q3 2022.

### Dark Web Data

**Monitoring data from the dark web can reveal threat actors planning to breach a company or how to monetize a breached or soon-to-be breached company.**

### Key takeaways:

CTI services can aid companies in understanding and reducing risks originating from their suppliers.

**One size does not fit all.** The scope and scale of these options are scaled up and down to meet the individual customer's and engagement's needs and budget:

Common offering	Summary	Timing	Used for
<b>Self-service evaluation of a potential supplier</b>	Companies can use Risk to determine the cyber-risks of a potential supplier	Can be done in as little as 15 minutes	Used to identify the relative risks of one supplier compared to other potential suppliers or their current suppliers.

<b>Ongoing supplier portfolio monitoring</b>	Ongoing monitoring of a portfolio of suppliers.	Ongoing	Used to identify the relative risks of all their suppliers.
	Ongoing reporting of alerts for emerging threats		

## Conclusion

When companies vet their suppliers, they often use third-party services with limited visibility, such as a simple perimeter scan of the supplier's network. Some companies delve deeper and rely on a CTI vendor for a more comprehensive scan. However, they usually depend on vendors who can only access TOR and the surface web, which gives their clients incomplete visibility and often results in missing essential issues they are concerned about. As a result, they usually miss more significant events than they discover.

### About the Author

Shawn Loveland is the COO of Resecurity. He is an experienced professional in the technology and cybersecurity field with over 35 years of industry expertise. He has worked for both small and large companies and has received 15 US patents and numerous international patents in computer security and telephony.

As the COO of Resecurity, Shawn aids Resecurity in providing practical solutions to our clients against the current threat landscape. He conducts proactive threat research and helps clients assess their Cyber Threat Intelligence (CTI) programs. He also provides customized intelligence services tailored to meet their unique needs. Before joining Resecurity, Shawn was responsible for dark web intelligence at Microsoft.



Shawn can be reached online at ([Shawn Loveland | LinkedIn](#)) and at our company website, <https://www.resecurity.com/>



## Cyber Risks for Government Agencies Are on the Rise. Why Security Is Still an Uphill Battle.

By Sarah Gray, Director of Product Marketing at Adaptiva

State and local government and education organizations (also known as SLED) were always at risk from cyberattacks, but the rise of [generative AI](#) has increased those risks significantly. Attackers are far more sophisticated than they've ever been, utilizing phony emails and even [deep faked phone calls](#) to trick unsuspecting employees into granting them access to systems.

During the first eight months of 2023, malware attacks on government organizations increased year over year by 148 percent, ransomware incidents by 51 percent and endpoint security services incidents—such as data breaches, unauthorized access and insider threats—by a staggering 313 percent, according to the [2022 Nationwide Cybersecurity Review](#). Schools were also heavily victimized by cyber attacks, with more than 1,300 publicly disclosed cyber incidents since 2016, reports [K12 Security Information Exchange](#) (K12 SIX). That “equates to a rate of more than one K-12 cyber incident per school day being experienced by the nation’s public schools.”



It is truly a scary environment, and it's never been easier for attackers to wreak havoc with remote workforces, BYOD and data in the cloud.

Government and education organizations are battling against these increased threats with limited budgets and competing for the best cybersecurity staffers against companies that can offer better pay. According to [data published in Axios](#), the average private sector cybersecurity role pays 14 percent more than public sector jobs. Another challenge in the public sector, especially with schools, is dealing with staff who are not technically the most savvy. Then there's the digital elephant in the room: resistance to change. Employees feel comfortable with their familiar processes and worry that new solutions could render their work—and them—less valuable.

So, what if a government or education organization doesn't have the budget or resources to get the cybersecurity talent and tools they need? Here are three other avenues they can take to be safe.

### 1. Pool resources at a state level

Licenses for cybersecurity products can be purchased at the state level, then rolled out to their "constituents." For this to work, state-level officials have to overcome any resistance to change. They need to make sure that every agency, from the Department of Corrections to the Department of Transportation, is on board with whatever tool they're using. That's a challenge because each of these departments might be doing something different for security. They have their own staff. Their email addresses are different. But this way, everyone can benefit while keeping costs down.

### 2. Push for continued grant money

In 2022, the Biden Administration [announced](#) \$1 billion in funding for a state and local cybersecurity grant program. The program was heralded by cash-strapped government and education organizations for allowing them to implement basic security protocols as well as gain access to state-level resources, as mentioned above. However, there are [concerns among state and city leaders](#) that the funding will not be fully dispersed, threatening ongoing cybersecurity efforts. It's vital for ongoing cybersecurity efforts that this grant program not only runs its course through its intended four years, but continues on in some form going forward.

### 3. Lobby for cybersecurity legislation

Around the country, leaders at the state, city and county level are working with their legislatures to pass laws that mandate certain cybersecurity protections. For example, Connecticut enacted legislation in 2023 that "establishes a cybersecurity task force" that will develop strategies and coordinate cybersecurity efforts among the state's agencies and other entities. This is a promising development for Connecticut, but much more cybersecurity legislation [failed than passed](#) last year. It behooves both public and private sector cybersecurity leaders to work with their elected officials on stronger cybersecurity programs.

## Reactive action is the most expensive path

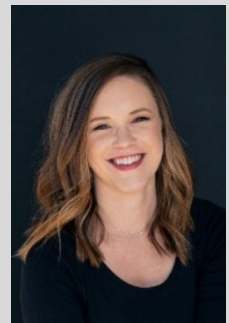
All three of these avenues insist on taking proactive action to stop cybersecurity threats before they become large problems. We don't need to look too far back to see the havoc that breaches cause to a city or state's population, and the subsequent expense of either paying a ransom or fixing the problems they caused. A ransomware attack on the City of Dallas last year led to [spending of \\$8.5 million](#) in taxpayer money on software, hardware, the hiring of forensics experts, in addition to two years of credit monitoring for people affected by the breach.

With the right cybersecurity resources, it's likely Dallas could have avoided the attack and not incurred such a large expense. Many tools on the market, including those that proactively manage software vulnerabilities, can ultimately save government and educational organizations money by stopping breaches before they happen.

The United States allocates a significant budget to physical security, but cybersecurity is overlooked and underfunded. To deal with this critical frontier, cybersecurity solution providers need to work with government and educational agencies to keep their data secure and protect the people they serve. The landscape is becoming more and more dangerous. Agencies need to ante up, or risk their organizations and constituents paying the consequences.

### About the author

Sarah Gray is the Director of Product Marketing at [Adaptiva](#), a Global Leader in Autonomous Endpoint Management.





## The AT&T Phone Records Stolen

### A Cautionary Tale of Cybersecurity Failures

By James Gorman, vCISO, Hard2Hack

In today's digital age, the importance of cybersecurity must be re-balanced. With increasing cyberattacks and data breaches, organizations must prioritize protecting their customers' sensitive information. Unfortunately, AT&T has recently fallen victim to a massive data breach, compromising the personal details of millions of its customers.

According to AT&T, the breach occurred between May 1, 2022, and October 31, 2022, as well as on January 2, 2023, and was discovered in April 2024. It affected millions of customers. The enormous phone company said they would notify approximately 110 million customers of the breach. The compromised data includes customer names, addresses, phone numbers, and account details but not the timestamps, the content of calls, texts, or Social Security numbers (SSNs). This sensitive information has been stolen from AT&T's databases, leaving customers vulnerable to potential identity theft and fraud.

The breach is thought to have occurred when an unauthorized individual or individuals accessed AT&T's systems. The company detected the incident in late June 2024 and immediately investigated. Law enforcement agencies are also involved in the probe to identify the perpetrator. While the exact details of the breach remain unclear, it is evident that AT&T's cybersecurity measures failed to prevent this massive intrusion.

Tech Crunch <https://techcrunch.com/2024/07/12/att-phone-records-stolen-data-breach/> reports that this is related to the recent vulnerability of Snowflake. Snowflake was implicated in several recent data breaches due to its customers not configuring access to the data they store on the Snowflake platform. Snowflake's advice to mitigate the risk of a similar breach, organizations using Snowflake should:

1. Implement multi-factor authentication (MFA) to enhance security and protect sensitive data.
2. Regularly monitor and audit Snowflake accounts for suspicious activity.
3. Ensure that all Snowflake users have strong, unique passwords and are not using default credentials.
4. Consider implementing additional security measures, such as data encryption and access controls.

The consequences of this breach are far-reaching and potentially harmful for affected customers. With compromised personal information, victims may be at increased risk of identity theft, fraud, and other forms of cybercrime. The impact on AT&T's reputation is also significant, as the company struggles to regain the trust of its customers and restore confidence in its ability to protect sensitive data.

The AT&T breach is a stark reminder of the importance of robust cybersecurity practices. The threat landscape constantly evolves in today's interconnected world, with new and sophisticated cyberattacks emerging daily. Organizations must take proactive measures to protect their customers' information and prevent breaches from occurring in the first place.

In response to the breach, AT&T offers affected customers free credit monitoring services for one year. The company is also implementing additional security measures, such as enhanced fraud detection and monitoring, to prevent similar incidents in the future. While these steps are welcome, they do little to mitigate the damage already done.

The breach has also raised questions about AT&T's compliance with industry standards and regulations. As a major telecommunications provider, AT&T is subject to strict data protection laws and guidelines. The company must meet its obligations under these laws and regulations, including the General Data Protection Regulation (GDPR) in Europe and the Gramm-Leach-Bliley Act (GLBA) in the United States. If the breach is as reported, AT&T must ensure that security and compliance programs, including outsourced service providers like Snowflake, protect all aspects of its infrastructure.

The AT&T phone records stolen data breach is a cautionary tale of cybersecurity failures. The incident highlights the need for organizations to prioritize protecting their customer's sensitive information and take proactive measures to prevent breaches. As customers, we must remain vigilant and proactive in protecting our personal information from potential threats.



## Recommendations:

1. Monitor your accounts closely: Keep a close eye on your account activity and report any suspicious transactions or login attempts.
2. Change passwords and enable 2FA: Update your passwords and enable two-factor authentication (2FA) to add an extra layer of security to your accounts.
3. Consider freezing your credit reports: If you're concerned about the potential impact of this breach on your financial information, consider freezing your credit reports or placing a freeze on your Social Security number.
4. Stay informed and stay safe: Stay up to date with the latest

cybersecurity news and best practices to minimize the risk of falling victim to cybercrime.

We must prioritize our online safety and security while navigating the ever-evolving digital landscape. Third-party risks will become more important as our data is stored online by what should be trusted enterprises. By protecting our personal information, we can reduce the risk of falling victim to cybercrime and restore confidence in our online activities.

AT&T customers should reference the webpage set up for this breach - <https://www.att.com/support/article/my-account/000102979>

### About the Author

James Gorman CISO, Founder and vCISO of Hard2Hack. James is a solutions-driven, results-focused technologist and entrepreneur with experience securing, designing, building, deploying and maintaining large-scale, mission-critical applications and networks. Over the last 15 years he has lead teams through multiple NIST, ISO, PCI, and HITRUST compliance audits. As a consultant, he has helped multiple companies formulate their strategy for compliance and infrastructure scalability. His previous leadership roles include CISO, VP of Network Operations & Engineering, CTO, VP of Operations, Founder & Principal Consultant, Vice President and CEO at companies such as GE, Epoch Internet, NETtel, Cable and Wireless, SecureNet, and Transaction Network Services.



James can be reached online at [@jgorman165 on X](https://twitter.com/jgorman165) and <https://www.linkedin.com/in/jamesgorman/> and at our company website <https://hard2hack.com>



## Uncovering the Gaps in Cyberthreat Detection & the Hidden Weaknesses of SIEM

Recent findings suggest that some tools may not be living up to their potential, raising concerns about their effectiveness.

By Garath Lauder, Director, Cyberseer

Cybersecurity tools and technologies are continuously being developed and refined to keep pace with the growing threat landscape. One tool we're all familiar with is the Security Information and Event Management (SIEM) system, designed to provide real-time analysis of security alerts generated by applications and network hardware. Despite their widespread adoption and pivotal role in many organisations' security postures, recent reports indicate that SIEM tools might not be performing as effectively as we think.

### The CardinalOps Revelation

A recent study by [CardinalOps](#) has unveiled some concerning insights into the performance of enterprise SIEM tools. The report suggests that many SIEM deployments are significantly

underperforming in their primary function: namely, cyberthreat detection. According to the study, a staggering 82% of enterprises believe their SIEM tools are not meeting expectations when it comes to identifying and responding to threats in a timely manner.

The underperformance of SIEM systems is not just a minor hiccup; it represents a substantial risk to enterprise security. SIEMs are expected to be the sentinels of an organisation's digital security, monitoring events from various sources to detect unusual activities and potential breaches. When these systems fail, it means threats can linger undetected, allowing adversaries ample time to inflict substantial damage.

## Understanding the Shortcomings

But why are such crucial tools are falling short?

There are several reasons behind the underperformance of SIEM systems:

**Complexity and Misconfiguration:** SIEM solutions are inherently complex, often requiring meticulous tuning and configuration to function optimally. Misconfigurations can lead to false positives and missed detections, as highlighted in the CardinalOps report, where over 70% of surveyed organisations admitted to facing configuration challenges.

**Data Overload:** SIEMs are bombarded with vast amounts of data from diverse sources. Without proper filtering and prioritisation, this data deluge can overwhelm the system, leading to missed alerts or delayed responses.

**Skill Gaps:** The effective operation of SIEM tools requires skilled personnel who can interpret the data and adjust the systems as needed. As the cybersecurity industry is currently facing a talent shortage, with an estimated 3.5 million unfilled positions globally, this exacerbates the problem.

**Integration Issues:** Many organisations struggle with integrating SIEM tools with their existing infrastructure and other security tools. Lack of seamless integration can obstruct the SIEM's ability to provide a comprehensive view of the threat landscape.

## Embracing Imperfections and a New Perspective on SIEM

In a thought-provoking piece by [security expert Anton Chuvakin](#) the inherent flaws of SIEM systems are examined and he argues for a different perspective. He suggests that rather than viewing SIEM flaws as failures, organisations should embrace these imperfections as opportunities for re-evaluation.

The importance of continuous improvement and iterative development in SIEM shouldn't be overlooked and requires a proactive approach where organisations regularly assess, align and

refine their SIEM configurations. This mindset shift can transform SIEM systems from static tools into dynamic components of a robust security strategy.

## Best Practices for Optimising SIEM Performance

Given the critical role of SIEM in modern cybersecurity, optimising its performance is vital. Here are some best practices to enhance the efficacy of your SIEM deployment:

**Regular Audits and Tuning:** Conduct frequent audits of your SIEM configurations to ensure they are aligned with your security policies and the current threat landscape. Regular tuning can help in minimising false positives and improving detection accuracy.

**Invest in Training:** Equip your security team with the necessary skills to manage and operate SIEM tools effectively. Continuous education and training programs can help bridge the skill gap and ensure your team stays updated with the latest threat detection techniques.

**Leverage Automation:** Utilise automation to handle routine tasks and data analysis within your SIEM. This can reduce the burden on your security team and enable faster response times to critical alerts.

**Enhance Data Management:** Implement robust data management practices to filter and prioritise the data collected by your SIEM. This can help in reducing noise and focusing on high-fidelity alerts that require immediate attention.

**Foster Integration:** Ensure seamless integration of your SIEM with other security tools and systems within your infrastructure. A well-integrated SIEM can provide a holistic view of your security posture and facilitate better threat correlation and analysis.

## Real-World Implications & How We Can Move Forward

The practical implications of underperforming SIEMs are significant. Consider a scenario in a financial institution, where a misconfigured SIEM fails to detect a sophisticated phishing attack. The unnoticed attackers can access sensitive financial data and customer information, leading to severe financial and reputational damage. By the time the breach is discovered, the cost of recovery and the impact on the institution's reputation can be immense.

Or take a healthcare organisation that deals with vast amounts of sensitive patient data. An underperforming SIEM might miss the initial attack activity that leads to a ransomware attack,



resulting in compromised patient records and disrupted services. This not only affects the organisation's operation but also erodes patient trust.

In both scenarios, regular audits and tuning of SIEM configurations, as well as investing in ongoing training for the security team, could have made a significant difference. The use of automation to streamline data analysis and reduce the volume of false positives would have enabled quicker and more accurate threat detection.

The insights from CardinalOps and experts like Anton Chuvakin highlight the need for a nuanced approach to SIEM management. While these tools are not perfect, understanding their limitations and working proactively to address them can significantly enhance their effectiveness.

I believe that continuous improvement and adaptation are the keys to staying ahead in cybersecurity. By embracing the imperfections and relentlessly refining our tools and strategies, we can build a more resilient defence against the increasing tide of cyber threats.

While SIEM systems may not be flawless, they remain a cornerstone of enterprise cybersecurity. The key lies in recognising their shortcomings and continuously working to optimise their performance. By adopting best practices and fostering a culture of continuous improvement, organisations can unlock the full potential of their SIEM tools and fortify their defences.

The path to enhanced SIEM performance involves a commitment to ongoing education, the strategic use of automation, and a proactive stance on configuration and integration. With these measures in place, organisations can transform their SIEM systems from a source of frustration to a robust component of their cybersecurity strategy.

Sources:

CardinalOps Report: [Fourth Annual Report on the State of SIEM Detection Risk](#)

Anton Chuvakin: [We Love What's Broken](#)

## About the Author

Garath Lauder is Director and Co-Founder of [Cyberseer](#). He, and Adrian Hunt, launched the company in 2014 to address sophisticated cyber threats that traditional methods were failing to catch. Garath and Adrian have assembled a team of specialists and experts dedicated to creating a secure digital society and helping organisations prepare for, rehearse, and respond to the growing threat of worldwide cybercrime.



Garath has over 30 years of extensive experience in the IT industry, beginning his career at BTN Internetworking. He has an impressive track record working with leading companies including Cable and Wireless, Juniper, Data Integration, and Xchanging PLC.

At Cyberseer, Garath oversees business development, marketing, and commercial relationships whilst ensuring every Cyberseer client has the benefit of their cutting-edge cybersecurity solutions.

Garath can be reached online at [garath.lauder@cyberseer.net](mailto:garath.lauder@cyberseer.net) or <https://www.linkedin.com/in/garathlauder/> and at our company website <https://www.cyberseer.net/>



## Data Breaches are a Dime a Dozen: It's Time for a New Cybersecurity Paradigm

By Ev Kontsevoy, Co-Founder and CEO, Teleport

Data breaches have accelerated quickly in 2024. Google 'data breach' and you're in for a whirlwind of high-profile names scattered across headlines of thousands, and sometimes millions, of customer and personal records exposed.

The headlines are reporting not only the compromise of sensitive data, but also the disruption of business operations as companies take systems offline to assess and contain the blast radius of compromised systems.

Not even Big Tech is safe from scrutiny. And it's because DevOps and cloud infrastructure have grown very complex. The fragmentation of identity and access silos has created an environment that enables bad actors to breach and pivot across infrastructure by identifying a misconfiguration, or forcing human error through techniques such as social engineering. Case in point: roughly 85% of data breaches in 2023 involved servers.

There's a way out of this breach nightmare, but it will require a new cybersecurity paradigm. This will require eliminating secrets, enforcing zero trust, enforcing the principle of least privilege, and hardening access with identity security and centralized policy governance.

## Modern infrastructure is a lot more complex than it used to be

But first, how did we get here? Well, engineering infrastructure evolved. A few decades ago, you might have had a handful of layers in a company's technology stack. It was easy enough to standardize the security model for each of those layers.

That's not the case in today's cloud-heavy environment of plentiful ephemeral resources. The modern-day 'stack' includes many disparate technology layers—from physical and virtual servers to containers, Kubernetes clusters, DevOps dashboards, IoT, mobile platforms, cloud provider accounts, and, more recently, large language models for GenAI.

This has created the perfect storm for threat actors, who are targeting the access and identity silos that significantly broaden the attack surface. The sheer volume of weekly breaches reported in the press underscores the importance of protecting the whole stack with Zero Trust principles. Too often, we see bad actors exploiting some long-lived, stale privilege that allows them to persist on a network and pivot to the part of a company's infrastructure that houses the most sensitive data.

## Zero Trust enforcement should now extend to applications and workloads

For a brief history lesson, the traditional security model before Zero Trust was about the perimeter – protecting internal applications and data with an external access point like a VPN. Authenticating via that VPN would grant access to whatever was inside, with no further authentication needed. From a malicious actor's perspective, breaching this perimeter by exploiting a static credential or stale privilege would grant access to other resources on the network.

Zero Trust was the answer to creating a 'perimeter-less' environment where 'everything requires authentication' (i.e. 'never trust, always verify'). Instead of authenticating to the network, you authenticate each time you access a resource.

Enter the pandemic, Zero Trust deployment heavily focused on solving network authentication. Most companies realized that VPNs weren't designed for large numbers of remote workers. The question was, 'How do we get our employees set up on the network if these VPNs only work within the office'? While plenty of companies have figured out how to authenticate users and enforce Zero Trust at the network level in the last few years, they haven't done so at the application and workload layer. They, therefore, haven't solved the more comprehensive challenge of enforcing a fully Zero Trust architecture for their cloud and data center operations.

To end rampant breaches, companies must now extend Zero Trust enforcement to applications and workloads. Companies need to transition to a mindset of constantly asking, "Does this person have



appropriate authorization to access this particular resource in the specific context in which they're to access it?"

The distinction between the corporate and public networks doesn't matter in a Zero Trust security model. Zero trust applied in this way makes all resources location-independent.

## The shift from role-based to attribute-based authentication

Companies can further harden their access control by ensuring that resource access is taking place in an appropriate context.

Attribute-based authentication is how we get there, effectively setting very granular requirements for when someone can access a resource.

For example, if you have a database table housing sensitive data, the first step might be to only grant access to employees with a specific job title – e.g., 'role-based authentication,' or RBAC. From here, companies can get more granular with attribute-based authentication, or ABAC. A few factors you might weigh for whether or not a user gains access include:

- **Where are you?** Are you in your 'workplace' (the office), or are you in Tahiti?
- **What device are you using?** Are you on a work laptop or something else, such as a personal phone or tablet?
- **What time is it?** i.e., do you want to permit access to a resource when it's being used in production?

You can create a rule that says, "All senior programmers trying to access database table XYZ have to be in Kansas between 2pm and 4pm." You've now shut access to anyone not meeting these conditions. If the employee is on vacation in Hawaii, if they're not senior enough, or if the database is in production use, it's locked by default.

Everyone should govern on attributes this way when granting access to users, as opposed to granting access to anyone inside 'the network'. These attributes are key to organizations reducing the attack surface exposed to bad actors with nefarious intent.

## Observability needs to be coupled with enforcement

Much investment is happening in the startup space across observability tools like identity security and policy governance. These are being layered on top of access technologies to add insight into how access is taking place. But they're being handled in isolated buckets, making associating the actual human user with each action hard.

Zero Trust access for modern infrastructure benefits from being coupled with a unified access mechanism that acts as a front-end to all the disparate infrastructure access protocols – a single control point for authentication and authorization. This provides visibility, auditing, enforcement of policies, and compliance with regulations, all in one place.

These solutions already exist on the market, deployed by security-minded organizations. However, adoption is still in early days. This means that a simple access rule like ‘developers should never have access to production data’ remains an unenforceable concept for many. We can see the consequences of organizations falling behind on unified access control for authentication and authorization, like the Change Healthcare, a UnitedHealth Group subsidiary, ransomware attack back in February which disrupted prescription and physician services across the company as systems were taken offline to assess and contain the blast radius.

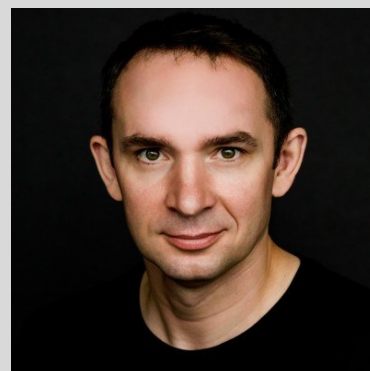
By unifying observability and enforcement, companies gain leverage in further hardening security, intervening in threat attacks, and reducing the blast radius. This means that if breaches occur, it may be possible to remediate efficiently without taking entire systems offline that disrupt operations and processes for companies and individuals.

## Complexity is not going away

Although Zero Trust solutions are broadly deployed in network security, it is time for engineering leaders to extend these principles to modern infrastructure, while making life easier for employees who manage the resources and data driving their business. Modern DevOps infrastructure will only get more complex, dynamic, and ephemeral as time goes on. By investing in access solutions that improve user experience for engineers while hardening security, companies can protect against the riskiest part of their infrastructure: the human element that attackers are exploiting.

### About the Author

Ev Kontsevoy is Co-Founder and CEO of Teleport. An engineer by training, Kontsevoy launched Teleport in 2015 to provide other engineers solutions that allow them to quickly access and run any computing resource anywhere on the planet without having to worry about security and compliance issues. A serial entrepreneur, Ev was CEO and co-founder of Mailgun, which he successfully sold to Rackspace. Prior to Mailgun, Ev had a variety of engineering roles. He holds a BS degree in Mathematics from Siberian Federal University, and has a passion for trains and vintage-film cameras. EV can be reached on [LinkedIn](#) and at <https://www.goteleport.com/>.





## DNS Security Strategies: Protecting Against Ransomware, Botnets, And Data Theft

Effective Ways to Fight Modern Cyber Threat

By Alexander Biushkin, Business Development Executive, SafeDNS

Protecting against the growing spectrum of cyber threats, including ransomware, botnets, and data theft, is fundamental for ensuring strong cybersecurity measures. DNS can be used within such a defense strategy efficiently to filter malicious traffic and block access to harmful websites that attackers use.

### Recent Cyber Events

In recent times, organizations have faced relentless attacks from sophisticated cyber threats exploiting DNS vulnerabilities. Concurrently, the projected cost of cybercrime in 2024 [is estimated](#) at \$9.5 trillion USD, reflecting a slight decrease from the anticipated growth rate. This underscores the substantial financial impact and emphasizes the urgent necessity for robust cybersecurity measures and the need for DNS security solutions' high effectiveness.

**Ransomware Attacks:** Ransomware is a cybersecurity threat that involves several vectors for use as an entry way into a network, such as email phishing, infected sites, and software or operating vulnerabilities. Soon after, a ransomware infection enters a network and encrypts documents on infected devices, thereby precluding access. Attackers go on to require ransom payment, mostly done through cryptocurrencies, to be able to give out keys for decryption that then allows access to data.

The effects of ransomware are devastating. They can paralyze operations to a much extent by making access to critical files almost impossible—with huge downtimes and operational paralysis. For example, in 2023, ransomware groups were very successful, making this the worst year on record. The number of victims had risen [55.5 percent to 5,070](#) from the 2022 figure. There were 2,903 victims in the second and third quarters combined, more than the total victims in 2022.

One very striking [example](#) is the Royal Mail, targeted by the LockBit ransomware group. It took out Royal Mail's ability to send international parcels, effectively halting a key portion of its operations. LockBit threatened to leak the stolen data unless a ransom was paid. What is more, ransomware attacks pose a very serious risk of sensitive information exposure in cases of attackers making a threat to leak data in order to coerce payment. The plain truth of the matter is that both operational disruption, and the potential exposure of data due to a cybersecurity incident, presents an organization with a dual jeopardy of risk.

**Botnet Exploitation:** Botnets pose a continuing threat and are used by cybercriminals to further disseminate malware, conduct DDoS attacks, and steal sensitive data from victim networks.

Historically, botnets were majorly referred to as viruses that infected computers and then propagated through networks, spreading havoc. However, botnets are now being manipulated by some sort of sophisticated bot masters or hacker groups who are propagating malware through various channels to exploit the vulnerabilities in the potentially compromised system. Once a system is infected, botnets continue to work subtly to remain undetected and communicate with their botmaster to follow the respective commands. Then, the attackers will monetize the successful breaches through video attacks, deployment of ransomware that encrypts data, or using a compromised system for cryptocurrency mining.

Usually, botnets take an average of approximately eight months before they are found. This is where one of the long-lived botnets goes, right at the top—to show the need for intrusion detection systems and proactive security measures. Without these defenses in place, the subtle indicators of botnet activities, such as sudden spikes in network traffic or performance degradation, can easily be overlooked and pose serious organizational security risks.

At our organization, we had a large-scale incident with our client, where botnet activity was detected against institutions. Such attacks were targeting institutions by the exploitation of network protocol vulnerabilities while scanning large ranges of IP addresses. The intrusion prevention systems in place were instrumental to the detection and mitigation of this malicious activity.

**Data Theft:** Cybercriminals leverage DNS exploits to exfiltrate data from the system, which essentially means the transmission of sensitive information out of the organizational perimeter. Such incidents can



prove very detrimental to any organization and may result in serious financial losses apart from the taint on the reputation factor associated with it.

## Protective Measures and DNS Filtering

Protection from the above-mentioned dangers can be enhanced through DNS filtering in the following ways:

**DNS Filtering Capabilities:** DNS filtering blocking access to known malicious domains ensures that unknowing users of a network are protected from visiting dangerous websites. It is possible to blacklist, at the DNS layer, access to known sites that host malware, phishing, or other such malicious content by maintaining an extensive database of categorized and flagged domains.

**IPS—Intrusion Prevention Systems:** Intrusion Prevention Systems (IPS) detect and block suspicious activities at the DNS level, effectively stopping potential threats from infiltrating the network. As part of IPS functionality, features like [SafeDNS](#) are employed to both detect and block these threats, providing an additional layer of security. Using predefined rules and behavioral analytics, IPS can thus very rapidly block DNS queries that point to known attack vectors or suspicious domains. This proactive defense mechanism helps to prevent potential threats from getting inside network infrastructure and hence fortify the security posture of any organization at large.

**Real-time Threat Intelligence:** Subscribing to real-time threat intelligence feeds allows for the very timely identification and blocking of emerging threats, therefore optimizing the security posture overall.

**Behavioral Analysis and Machine Learning:** Using machine learning algorithms, DNS security systems, such as those implemented by SafeDNS, analyzes patterns of DNS traffic to detect abnormal behavior indicative of potential threats, hence improving the detection and response capabilities.

Machine learning algorithms learn continuously from new data and adapt to evolving attack techniques, making threat detection and response more accurate and effective. This method, therefore, not only detects known threats but also detects otherwise unseen or zero-day attacks, thereby overall strengthening the resilience of organizations against sophisticated cyber threats.

Besides these strategies, it's important to recognize that depending on just one vendor's solution may not be enough. Relying on a single database doesn't ensure you're protected from all the latest threats. Each vendor has different ways of collecting threat information and how often they update it. So, having multiple sources provides a better and more complete defense against cyber threats.

The changing nature of these threats requires strong cybersecurity. An organization has no choice but to emphasize proactive defense, including all-around DNS security, to be always ready for the attack of a botnet. Companies are continuously innovating and adopting technologies to combat emerging threats and, in the process, assures organizations the capability to keep their businesses afloat and to ensure data protection in this ever-changing threat landscape. As you see, being prepared for the attack and staying vigilant are the utmost here to counteract effectively against the growing threats.

## About the Author

Alexander Biushkin is an accomplished Business Development Executive at SafeDNS, specializing in IT and Cybersecurity sales. Over 9 years, he has gained a deep understanding of the challenges in cybersecurity. At SafeDNS, he leverages his extensive experience to grow business and build strategic partnerships that ensure resilient and secure solutions for clients.

Alexander Biushkin can be reached online at [alex@safedns.com](mailto:alex@safedns.com) and at our company website <https://safedns.com/>.





## Embracing Proactive Fraud Management with Real-Time Orchestration

By Mario Dusaj, Senior Solutions Engineer - US, Callsign.com

With security breaches becoming more frequent, banks need to act swiftly to protect their users. The rapid advancement of technology, including real-time payments and AI, adds complexity to the tasks of security and fraud practitioners. With widespread compromise of passwords, the need for rapid response capabilities is highlighted.

Hackers are continuously evolving their methods and now even targeting password managers and users through sophisticated phishing campaigns. The challenges for security professionals such as Chief Information Security Officers (CISO), Chief Technology Officers (CTO) as well as authentication teams and fraud practitioners are becoming increasingly complex, especially within organizations that operate in siloed environments.

Traditional methods of addressing vulnerabilities are time-consuming, involving multiple stakeholders across authentication teams, application owners, fraud teams, and user experience teams who need to

work together to identify, assess, and resolve vulnerabilities. This process often takes weeks or months, leaving users vulnerable and eroding trust in the brand.

## Adaptability is Essential

Navigating the complexities of a robust fraud and security strategy can be a challenge. Are your team able to read the latest security briefs, devise strategies, and implement solutions within the same day?

Instead of focusing solely on individual breaches, the industry must embrace a broader perspective on adaptability and look to comprehensive solutions that combine proactive detection with the ability to apply rapid, confident changes.

Gartner\* advises that the orchestration of multiple Online Fraud Detection (OFD) solutions not only reduces this complexity but also provides a more dynamic and adaptive UX for the user.

Businesses not only need a 360 view of their users, but it also needs to be accessed and actioned upon by multiple business units.

## Holistic and Integrated Solutions

Integrated solutions offer a holistic view of user behavior and context, allowing organizations to dynamically adapt security measures in real-time. This not only mitigates risks but also enhances trust.

Today's solutions need to empower security teams to be able to:

- Review daily security updates.
- Identify threats targeting specific user groups, such as those affected by recent data breaches.
- Dynamically adjust authentication processes to enhance security without compromising the user experience.

Such a proactive, adaptive approach is crucial for addressing fraud and security in today's fast-paced environment.

## Proactive and Adaptive Fraud Management

Organizations can stay ahead of evolving threats while maintaining trust and reputation with their users by adopting integrated, adaptive solutions that prioritize real-time detection and response. Journey-time orchestration solutions such as Callsign gives organizations this flexibility, helping balance security and user experience.



The ability to react quickly and confidently to new threats is vital in our technology-driven world. It's time to rethink traditional approaches and embrace the agility required to navigate the complexities of modern security.

*\*Gartner, Market Guide for Online Fraud Detection, Akif Khan, Dan Ayoub, 12 December 2022. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.*

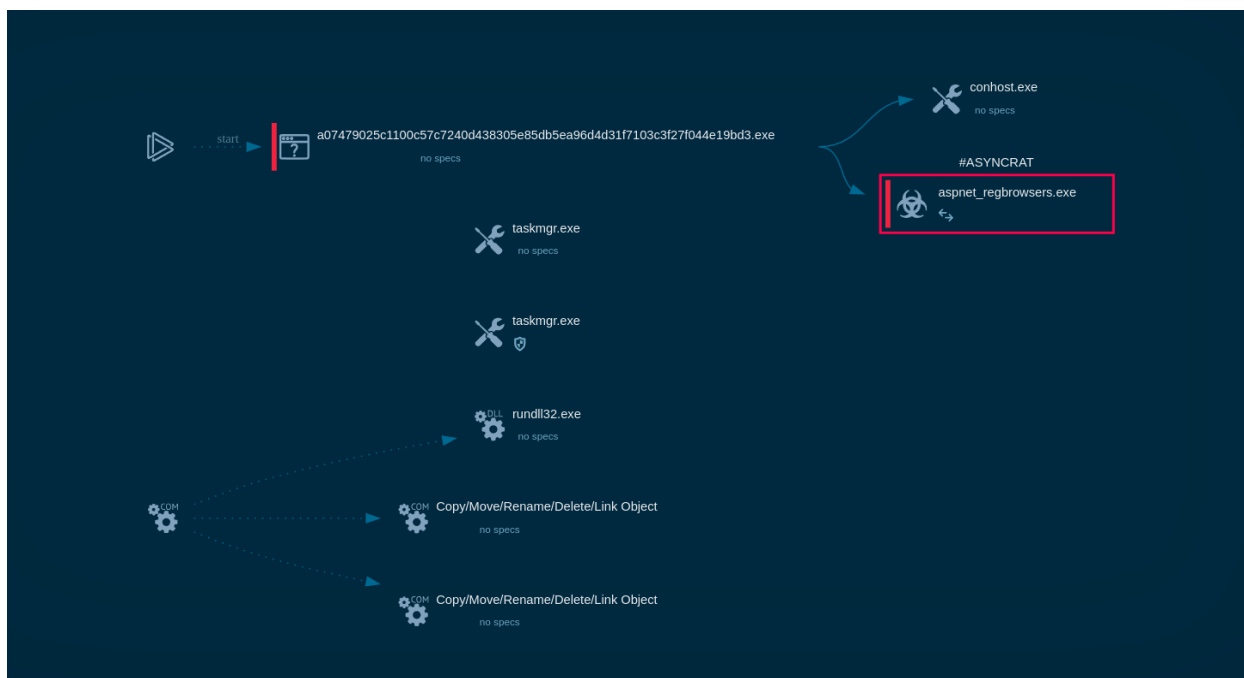
### **About the Author**

Mario Dusaj is a Senior Solutions Engineer - US at Callsign.

Mario can be reached online at [mario.dusaj@callsign.com](mailto:mario.dusaj@callsign.com) and at our company website <https://www.callsign.com/>







[AsynRAT's process graph](#) displayed by the ANY.RUN sandbox

- **Processes:** As malware often creates, injects, and terminates processes to carry out its malicious activities, tracking these changes and relaying them to the user in a digestible format is essential.
- **Registry:** Malware makes changes to the registry to achieve persistence, modify system settings, or disable security features. Detecting such activity proves useful in threat investigations.
- **File system:** Malware manipulates files and directories to store its components, steal data, or disrupt system functionality. A proper sandbox exposes all of these activities and reveals additional Indicators of Compromise (IOCs) that are not present in the code itself.

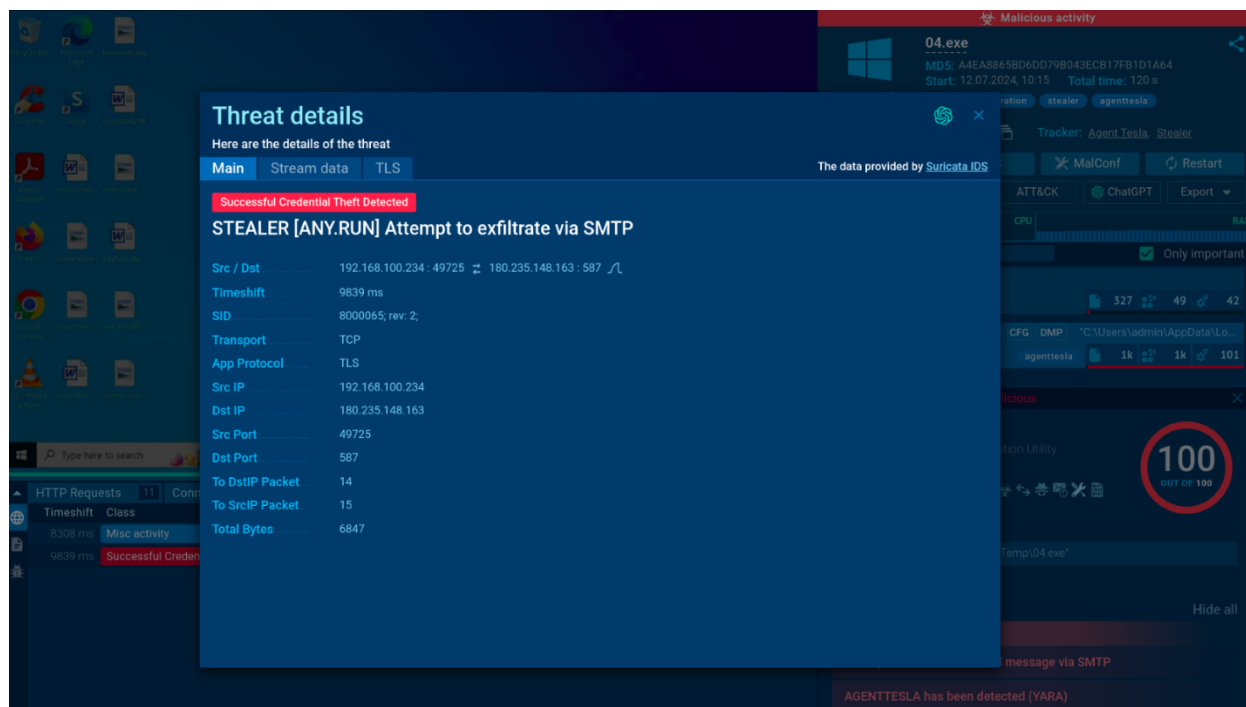
Additionally, advanced malware sandboxes should map the observed behaviors to the MITRE ATT&CK framework, a universal knowledge base of adversary tactics and techniques based on real-world observations.

This way, users can not only get a complete understanding of the threat's scale, but also receive actionable information for predicting the impact of the malware, creating effective countermeasures, and improving the overall security posture of the organization.

## 2. Network Analysis

Network analysis is another critical component of effective malware sandboxing, providing insights into the network-based activities. This process involves several key techniques:

- **Packet Capture and Inspection:** Logging network traffic and allowing the user to view its contents offers an in-depth view of the interactions between the malware and other systems. This includes information such as the source and destination IP addresses, the ports used, the protocols involved, and the timestamps of the communications. This can reveal if the malware is attempting to communicate with a command and control (C&C) server, scan for vulnerable systems, or perform other malicious activities.
- **Encrypted Traffic Analysis:** As more and more network traffic becomes encrypted, the ability to analyze it has become increasingly important. Sandboxes using built-in tools like MITM proxy make it possible to decrypt HTTPS traffic and thus identify malicious activity.



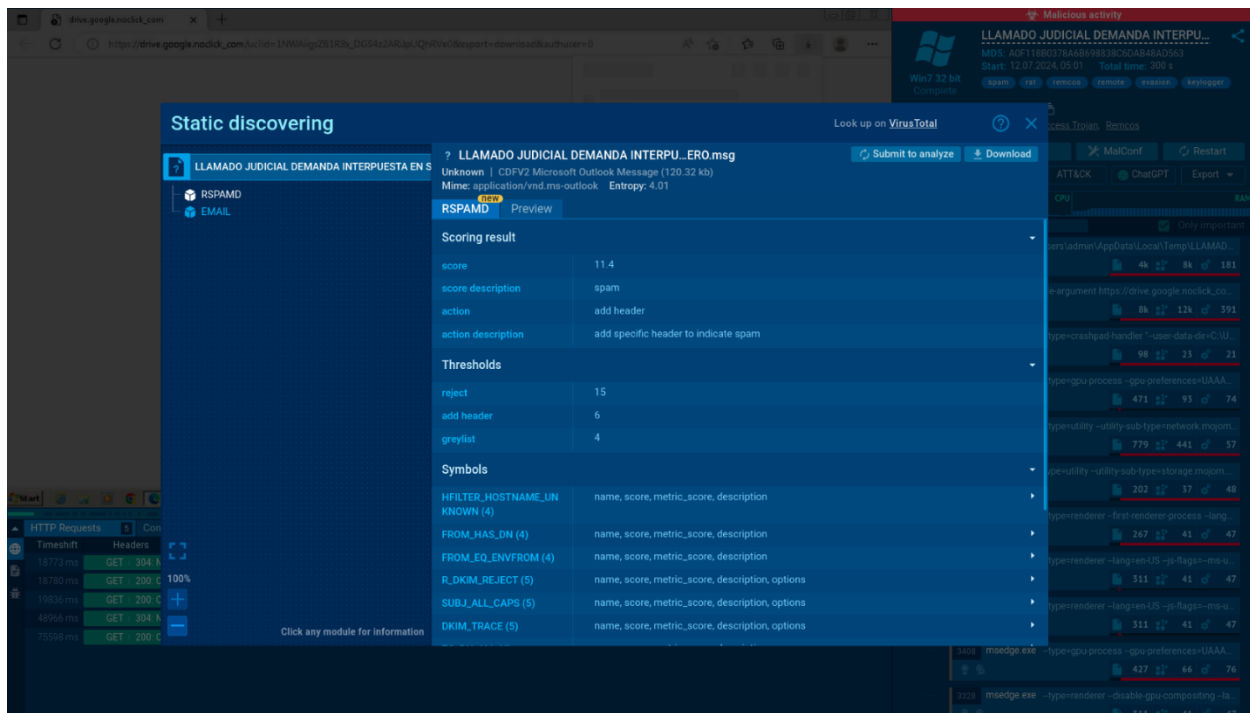
Suricata detection of AgentTesla's exfiltration activity [in ANY.RUN](#)

- **Network Threat Detection:** For sandboxes, it is also important to not only give access to the network traffic, but also automatically detect potential threats based on predefined signatures or anomalies. Solutions like Suricata IDS can be used to enhance the network analysis capabilities of a malware sandbox and flag suspicious network activities.

### 3. Static Analysis

Although sandboxes are usually used for dynamic analysis, they can be equally helpful in static analysis:

- **Analyzing Files:** Sandboxes can offer a static overview of various file types, such as PDFs, LNK files, and Microsoft Office documents. For instance, malicious PDFs can be analyzed to detect suspicious URLs, while LNK files can be inspected for embedded commands and scripts. Microsoft Office documents can be examined for malicious macros, images, QR codes, etc.



### Static analysis of a phishing email in ANY.RUN using the Rspamd spam-filtering module

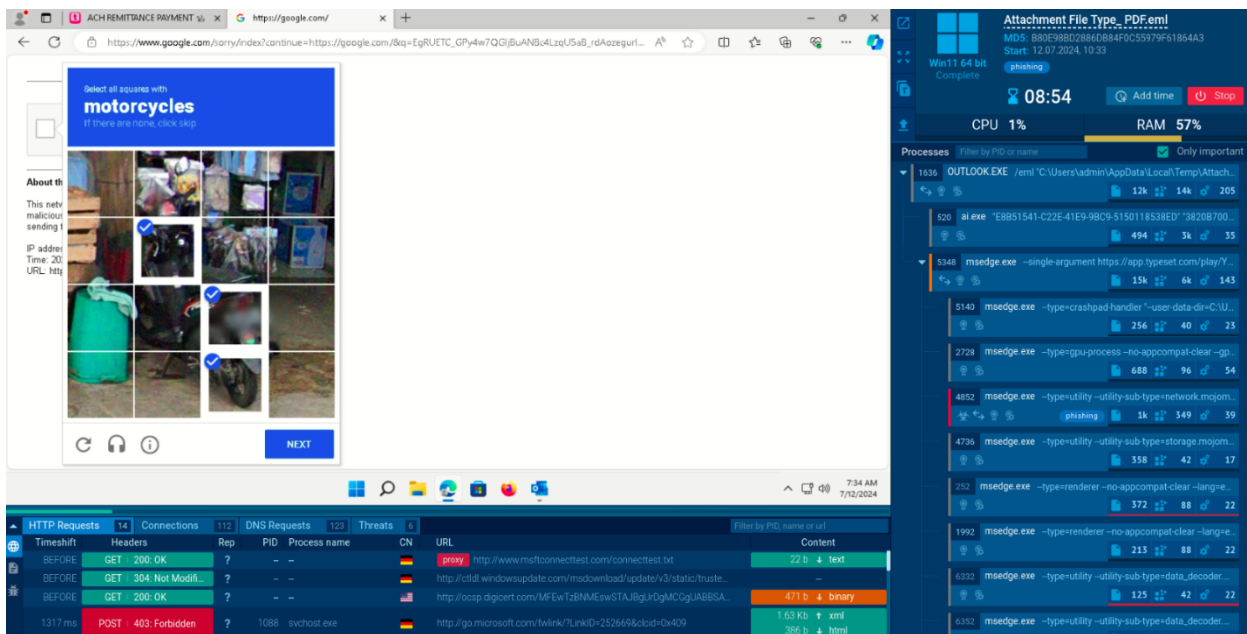
1. **Investigating Spam and Phishing Emails:** Sandboxes offer email previews, display metadata, and list Indicators of Compromise (IOCs), enabling you to examine email content and origin details without opening the email itself. Moreover, sandboxes can effectively handle malicious archive attachments, such as ZIP, tar.gz, .bz2, and RAR files, which are often used to evade basic detection.

While static analysis is a powerful technique, it is important to note that it is not always sufficient on its own. This is why sandboxes should also offer interactivity to manually engage with files and links when needed.

## 4. Interactivity and Flexibility

Interactivity is a key feature of advanced malware sandboxes that enables security teams to gain a more complete understanding of the behavior and capabilities of suspicious software.





### *Interactivity can help in cases like CAPTCHA-protected phishing pages*

With interactivity, security teams can manually perform various user interactions, such as clicking on links, entering data, or opening files within the sandbox. These actions can trigger additional behaviors or reveal hidden capabilities of the malware that might not be exposed through automated analysis alone. For instance, a piece of malware designed to steal credentials may only exhibit its true nature when a user attempts to log in to a specific website or application.

In addition to manual user interactions, advanced malware sandboxes must enable security teams to customize and emulate different system and network conditions. This can involve various operating systems, software configurations, or network environments. By emulating these conditions, security teams can analyze how the malware behaves in diverse scenarios.

## 5. Reporting

Since sandboxes are often the first tool for security analysts when addressing an incident or investigating a threat, they must offer detailed and easy-to-understand reports. Each report should provide a comprehensive summary of the malware's behavior, including any actions taken, changes made to the system or network, and any IOCs identified.

## General Info

Add for printing 

File name: NOTIFICA ACTUACION PROCESAL RAD 2024-0000099-00 BOLETA RAMA JUDICIAL COMUNICA DEMANDA REV

Full analysis: <https://app.any.run/tasks/9fcd85a5-3f0f-4373-aba5-6f459bc417ab>

Verdict: Malicious activity

Threats: **Remote Access Trojan** Remcos

Remote access trojans (RATs) are a type of malware that enables attackers to establish complete to partial control over infected computers. Such malicious programs often have a modular design, offering a wide range of functionalities for conducting illicit activities on compromised systems. Some of the most common features of RATs include access to the users' data, webcam, and keystrokes. This malware is often distributed through phishing emails and links.

Malware Trends Tracker >>>

Analysis date: July 12, 2024 at 06:34:20

OS: Windows 10 Professional (build: 19045, 64 bit)

Tags: rat remcos remote

Indicators: 

MIME: application/x-rar


File info: RAR archive data, flags: Locked EncryptedBlockHeader

MD5: BA6FF87BF396AACF3CB76184BF52068F

SHA1: 5663772F388D7045AA2E4751EFD37315909A2527

SHA256: 75C23BE4B4AB928350949D5C3829758748819515A756ADAE7A766AECF1DE5207

SSDEEP: 98304:OFyCKnUTYxRkoQXHvNSqdhiLEwowhtHL3kubyB7wcmMDtsTYbpuMIYcVbZPpVAer:UZ

 ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

### [Report on a Remcos sample in ANY.RUN](#)

By giving clear, detailed, and actionable reports on its findings, an effective malware sandbox can enable security teams to make informed decisions about how to respond to threats, improving the organization's overall security posture.

## ANY.RUN Sandbox

[ANY.RUN](#) provides an interactive cloud sandbox that incorporates all the features necessary for conducting advanced malware and phishing analysis with ease and speed. The free version offers unlimited submissions and analysis in Windows 7 (x32), 10 (x64) and Linux VMs, while the premium plans let you analyze your files and URLs privately and work with your entire team in your private space.

[Create your free ANY.RUN account to analyze cyber threats without limits.](#)

## Conclusion

A malware sandbox is a powerful tool in the arsenal of cybersecurity professionals, providing a safe space to analyze and understand potential threats. By incorporating behavioral analysis, network analysis, IOC extraction, interactivity, and comprehensive reporting, organizations can ensure their sandbox is not just a tool, but a robust and effective line of defense against cyber threats.

## About the Author

Vlad Ananin is a Technical Writer at ANY.RUN. With 5 years of experience in covering cybersecurity and technology, he has a passion for making complex concepts accessible to a wider audience and enjoys exploring the latest trends and developments. Vlad can be reached online at the company website <https://any.run/>





## Fortifying the Future: AI Security Is The Cornerstone Of The AI And GenAI Ecosystem

By Rony Ohayon, CEO and Founder, DeepKeep

The rapid proliferation of AI technologies is bringing about significant advancements, but it has also introduced a wide range of security challenges. Large language models (LLMs) and computer vision models, key components of generative AI (GenAI), are particularly susceptible to vulnerabilities that compromise security, trustworthiness, and privacy. New solutions are emerging to ensure the safe and ethical deployment of AI systems to address these challenges.

### Understanding the Risks

AI models are vulnerable to several types of attacks and mistakes:

- Adversarial attacks, for example when attackers mislead the LLM by adding adversarial content to prompts.
- Hallucination, when AI models generate incorrect or nonsensical information, reducing application accuracy and reliability.
- Data privacy breaches, when AI systems inadvertently leak private data.

- Bias and fairness issues, when AI models perpetuate or even exacerbate existing biases, leading to unfair or discriminatory outcomes and decisions.
- Toxicity, when models produce harmful or offensive content, which is particularly concerning in customer-facing applications.

## Evaluation and Risk Assessment

Comprehensive risk assessment solutions are deployed to mitigate AI and GenAI risks. These solutions evaluate AI models on various fronts, identifying vulnerabilities and providing actionable insights to improve security and trustworthiness. Key features of effective risk assessment include:

- Penetration Testing: systematic evaluation of AI models to uncover security weaknesses pre and post deployment.
- Hallucination: detecting and assessing the likelihood AI models will generate false or misleading information.
- Evaluating a model’s overall resilience.
- Privacy: assessing a model’s propensity to leak sensitive information.
- Content: detecting and mitigating the generation of toxic, offensive, harmful, unfair, unethical, or discriminatory language.
- Bias and Fairness: identifying and addressing biases within a model to ensure fair and ethical outcomes.
- Weak Spots: pinpointing specific vulnerabilities within AI applications.

## Case Studies and Practical Applications: English to French Translation

When DeepKeep evaluated Meta’s LlamaV2 7B LLM, we identified significant weaknesses in its ability to handle translation from English to French. The example below demonstrates the decline in performance DeepKeep found when applying its transformations, resulting in an over 90% drop in accuracy.

The table below showcases 5 test examples:

Original Prompt	LlamaV2 7B’s Translation	Correct Translation
It is the biggest acquisition in eBay's history.	C'est l'acquisition la plus importante de l'histoire d'eBay.	C'est la plus grande acquisition de l'histoire d'eBay.



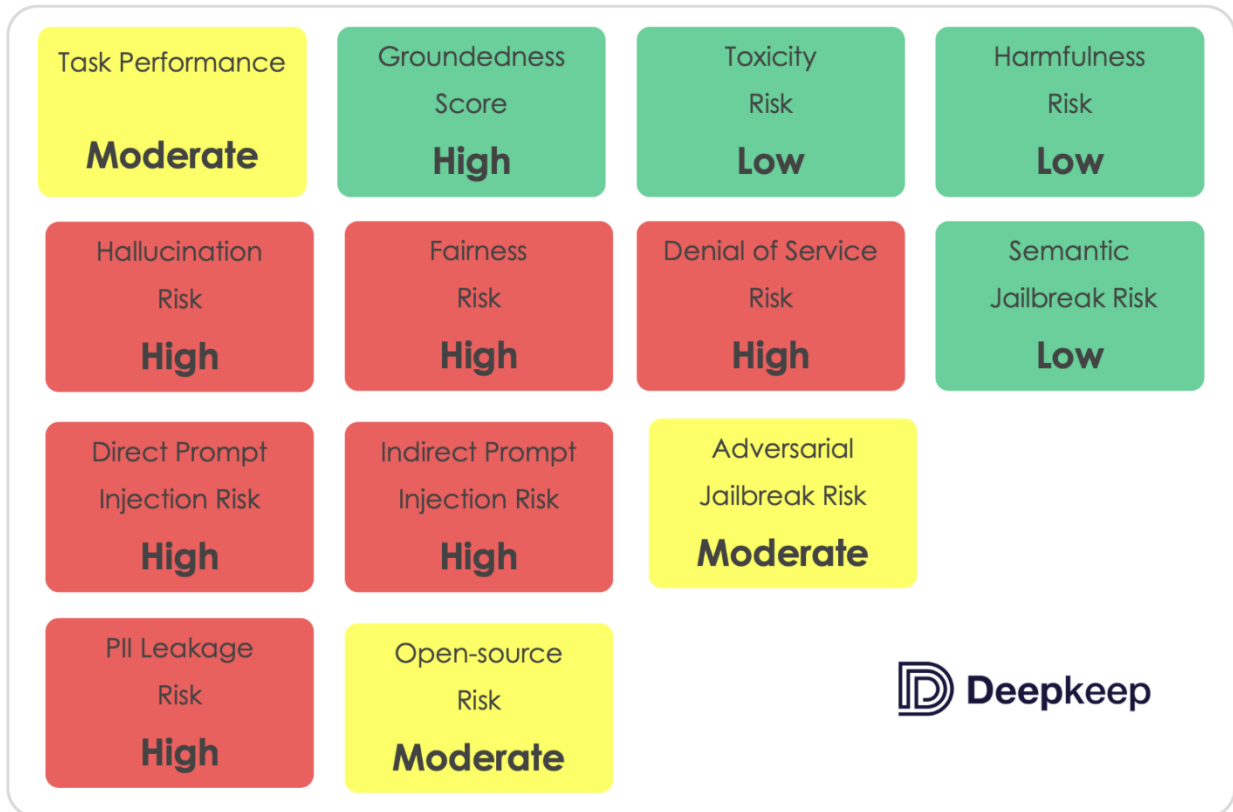
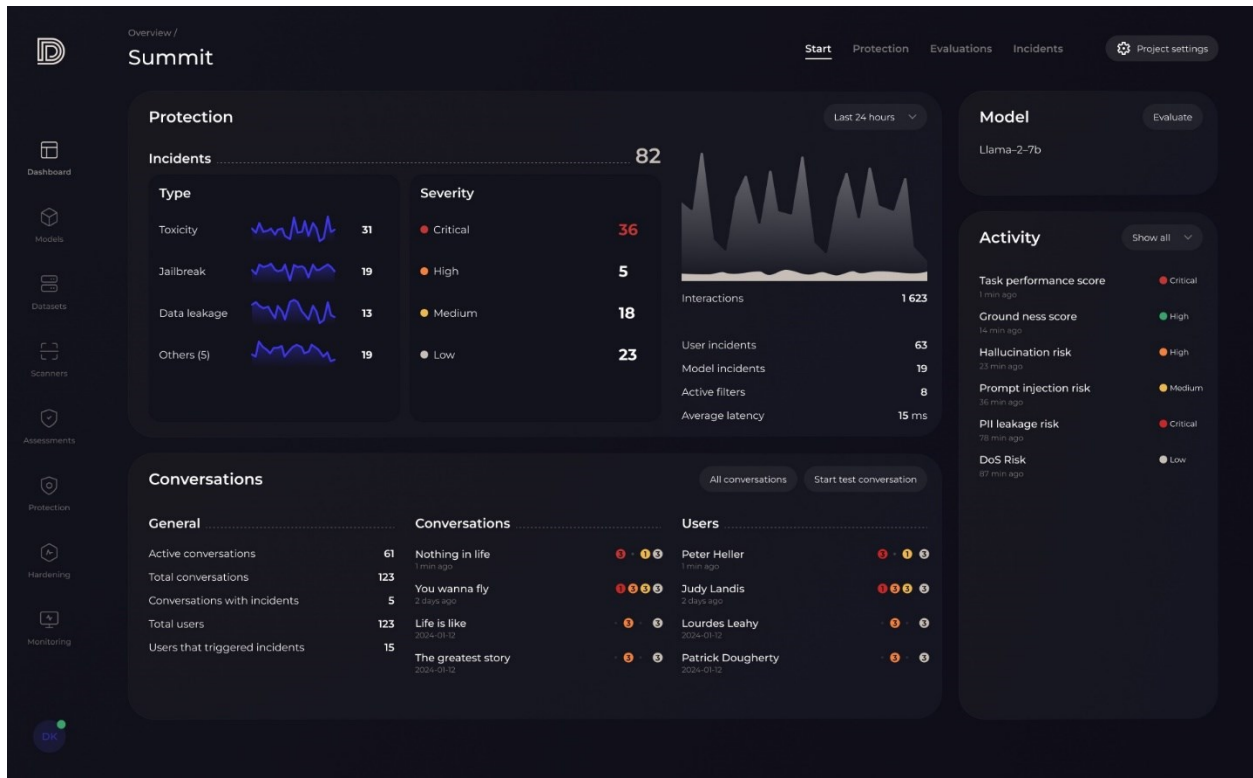
In Berlin, police estimated 6,500 protestors.	En Berlin, la police a estimé 6 500 manifestants.	À Berlin, la police estime qu'il y avait environ 6 500 manifestants.
An inquiry was established to investigate.	Une enquête a été créée pour mener une enquête.	Une enquête a été ouverte.
It has the same molecular structure whether it is a gas, liquid, or solid.	Il a la même structure moléculaire quelle que soit son état (gaz, liquide ou solide).	Il a la même structure moléculaire, qu'il s'agisse d'un gaz, d'un liquide ou d'un solide.
Since moving to the Catalan-capital, Vidal had played 49 games for the club.	Depuis son arrivée à la capitale catalane, Vidal avait joué 49 matchs pour le club.	Depuis son arrivée dans la capitale catalane, Vidal a joué 49 matchs pour le club.

## Broader Implications

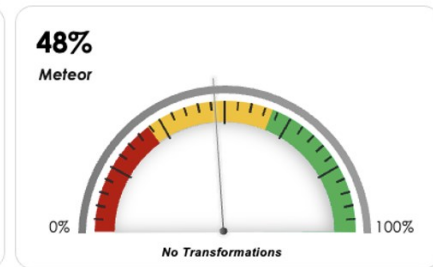
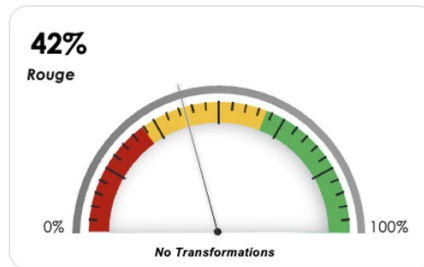
The importance of trust in AI cannot be overstated. The resilience and reliability of GenAI models is becoming critical as enterprises increasingly integrate GenAI into business processes. Evaluating AI models during their inference phase — when they are actively generating outputs — is essential for ensuring they are trustworthy, effective, private and secure.

## AI Security's Role is The Ecosystem's Foundation

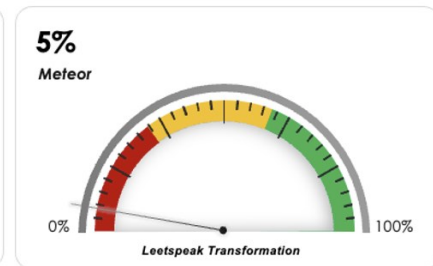
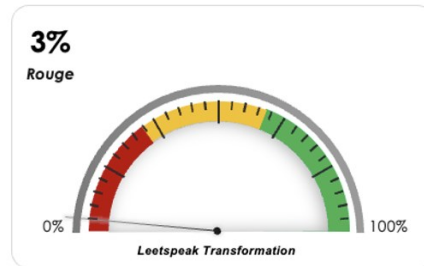
As AI technology evolves, so do the strategies and tools required to secure it. AI security is not just about protecting models from external threats, but also about ensuring they operate ethically and responsibly, providing insights into potential risks and vulnerabilities. This includes adhering to regulatory requirements, maintaining transparency, and safeguarding user privacy. Comprehensive AI security platforms are an essential foundation of the AI and GenAI ecosystem.



Baseline Translation Accuracy



Risk Assessment Translation Accuracy



### About the Author

Dr. Rony Ohayon is the CEO and Founder of [DeepKeep](https://www.deepkeep.ai), the leading provider of AI-Native Trust, Risk, and Security Management (TRiSM). He has 20 years of experience within the high-tech industry with a rich and diverse career spanning development, technology, academia, business, and management. He has a Ph.D. in Communication Systems Engineering from Ben-Gurion University, a Post-Doctorate from ENST France, an MBA, and more than 30 registered patents in his name. Rony was the CEO and Founder of DriveU, where he oversaw the inception, establishment, and management. Additionally, he founded LiveU, a leading technology solutions company for broadcasting, managing, and distributing IP-based video content, where he also served as CTO until the company was acquired. In the education realm, Rony was a senior faculty member at the Faculty of Engineering at Bar-Ilan University (BIU), where he founded the field of Computer Communication and taught courses about algorithms, distributed computing, and cybersecurity in networks.



Rony can be reached online at <https://www.linkedin.com/in/rony-ohayon-40232716a/?originalSubdomain=il> and at our company website <https://www.deepkeep.ai/>



## Guarding the Games: Cybersecurity and the 2024 Summer Olympics

By Desrah Kraft, Cyber Threat Intelligence Engineer, DefenseStorm

As Paris prepares to host the 2024 Summer Olympic Games, athletes from around the world converge to represent their country. But beyond the cheers and medals lies a digital underworld. The cyber threat landscape during major sporting events, including the Olympics, has become increasingly treacherous.

In the past decade, the number of cyberattacks has surged dramatically. During the London 2012 Games, there were approximately 212 million cyberattacks. Fast-forward to the Tokyo 2021 Olympics and that number skyrocketed to a staggering 4.4 billion. This year, experts anticipate an even greater onslaught of threats, including disruption attempts, disinformation campaigns, and cybercrime, making robust cybersecurity measures imperative for safeguarding this global spectacle. In a recent interview, Director General of ANSSI [The National Cybersecurity Agency of France], Vincent Strubel, stated, "We are getting ready for all types of attacks -- everything we see on a daily basis but in bigger, more numerous and more frequent." Additionally, Strubel commented, "We can't prevent all the attacks; there will not be games without attacks, but we have to limit their impact on the Olympics."

The games are scheduled to begin July 26, 2024, with cybercriminals lurking in the shadows, armed with malware, phishing tactics, and ransomware. Their target? The vital services of the games: retail, ticketing, travel, and hospitality. Organizations need to stand guard over their information technology and cybersecurity hygiene not just during the Olympic Games but daily.

The best way to stay safe in the face of these emerging threats is to remain vigilant and informed regarding the tactics and methods of threat actors. The following are some of the threats to watch for:

**1. Account Takeover and Credential Stuffing:**

- With increased financial transactions during events like the Olympics, the risk of account takeover and credential stuffing attacks escalates.
- Cybercriminals exploit weak or reused passwords to gain unauthorized access to user accounts.
- Vigilance in monitoring account activity and using strong, unique passwords is crucial.

**2. Social Engineering via Phishing Emails:**

- Expect a surge in phishing emails related to the Olympics. These deceptive messages often promise “promotional offers” or “special deals.”
- Unsuspecting recipients may click on malicious links, leading to compromised systems or stolen credentials.
- Users should verify the legitimacy of emails and avoid clicking on suspicious links.

**3. Ransomware and Malware Attacks:**

- Cybercriminals seize major events as opportunities to sow chaos. Ransomware attacks can disrupt critical systems, holding them hostage until a ransom is paid.
- Malware, disguised as legitimate files or software updates, can infiltrate networks and compromise sensitive data.
- Regular security updates, robust backups, and employee training are essential defenses.

**4. Ad Fraud (Including Click Fraud):**

- Ad fraud targets digital advertising networks for financial gain. One common method is click fraud, where bots artificially inflate ad clicks.
- During high-profile events, cybercriminals exploit increased ad traffic to perpetrate fraud.
- Advertisers and platforms must implement fraud detection mechanisms to safeguard ad budgets.

**5. Malvertising:**

- Malvertising injects harmful code into legitimate online ads. When users click on these compromised ads, they unwittingly expose themselves to risk.
- Vigilance while browsing and using ad blockers can mitigate exposure to malicious ads.
- Organizations should monitor their ad networks and promptly address any suspicious activity.

Consider how the threats mentioned earlier apply to your organization’s internal network. It’s crucial to recognize that not all end users prioritize security but whether it’s clicking on the wrong link or an end



user making a purchase from what they believe is a legitimate retail site within your network, these actions can lead to unauthorized access. During the Summer Olympics, all industries face heightened risks due to increased transaction volumes related to Olympic purchases (such as tickets, lodging, travel, and retail).

## Fortifying the Digital Arena

Organizations should not wait for a major event to fortify their defenses and protect against cyber threats. Instead, these practices should be a daily routine, further strengthened to address potential increases during events. Consider implementing the following methods:

### 1. Education and Training:

- Organizations should educate employees about cyber threats, emphasizing vigilance and safe practices.
- Regular training sessions keep staff informed about evolving tactics.

### 2. Incident Response Plans:

- Prepare for the worst. Have robust incident response plans in place.
- Timely detection and containment minimize damage.

### 3. Collaboration and Threat Intelligence:

- Share threat intelligence with industry peers. Collective defense is potent.
- Collaborate with law enforcement and cybersecurity agencies.

### 4. User Awareness Campaigns:

- Launch awareness campaigns during the Olympic season. Remind users of risks.
- Highlight the importance of reporting suspicious activity promptly.

Before the light is even ignited on the Olympic torch, the fight against cyber threats will begin and likely be relentless, but through strategic and proactive preparation and collective effort, organizations and consumers can proactively protect themselves.

## About the Author

Desrah Kraft is a Cyber Threat Intelligence Engineer at DefenseStorm. For the past three years, she has played a vital role in leading and contributing to various Incident Response efforts. Before transitioning into cybersecurity, Desrah obtained a bachelor's degree from Mitchell College and worked for 7 years in law enforcement. This experience helped her cultivate a comprehensive understanding of security principles and investigative practices. An accomplished cybersecurity professional with 4 years of hands-on experience in analyzing malware and extensive expertise in safeguarding digital landscapes against malicious threats, Desrah possesses an unparalleled ability to dissect complex cyber threats, identify their origins, and implement effective countermeasures. Additionally, she holds multiple MITRE certifications, which demonstrate her mastery of advanced threat detection and mitigation techniques as well as the GIAC Security Essentials (GSEC) certification. Recognized for her keen eye for anomalies and proactive approach, Desrah excels in Endpoint Detection and Response (EDR), enabling rapid identification, investigation, and containment of potential breaches. Committed to continuous growth and learning, Desrah remains at the forefront of cybersecurity, dedicated to fortifying digital infrastructures and inspiring others in the field. Desrah can be reached online at [Desrah.Kraft@defensestorm.com](mailto:Desrah.Kraft@defensestorm.com) and at our company website <https://defensestorm.com/>





## High Performance Software Defined Receivers

A Crucial Asset in Cybersecurity

By Brandon Malatest, COO, Per Vices Corporation

### Introduction

As cybersecurity challenges grow more complex, the tools we use to protect data and communications are also advancing. Among these tools, high-performance software defined receivers (SDRs) with tuning ranges up to 40GHz stand out as particularly critical. Their flexibility, precision, and adaptability make them essential for detecting, analyzing, and countering cyber threats.

### Understanding Software Defined Receivers

Software defined receivers (SDRs) mark a significant leap in radio technology. Unlike traditional receivers that rely on fixed hardware for signal processing, SDRs use software for this task. This allows for greater flexibility and adaptability, enabling them to handle a wide range of frequencies and protocols.

SDRs with tuning ranges up to 40GHz are especially notable. These receivers can capture signals across an extensive spectrum, from low-frequency communications to high-frequency microwave signals. This

broad tuning range is vital in cybersecurity, where threats can come from various sources operating at different frequencies.



SDR Operating Up to 40GHz

## The Role of SDRs in Cybersecurity

High-performance SDRs play multiple roles in cybersecurity. Their ability to monitor, analyze, and respond to a wide array of signals makes them invaluable in areas like network security, threat detection, and counterintelligence.

## Network Security and Monitoring

One key application of SDRs in cybersecurity is network security and monitoring. Traditional security tools typically focus on data packets and higher-layer protocols, but many sophisticated threats operate at the physical and link layers, where conventional tools may lack visibility.

SDRs bridge this gap by monitoring the electromagnetic spectrum for unusual signals. They can detect unauthorized wireless devices, rogue access points, and other malicious entities attempting to breach network security. By analyzing signal characteristics and behaviors, SDRs can identify and neutralize potential threats before they cause damage.

Moreover, SDRs are essential for securing wireless communication channels. In environments where wireless communication is prevalent, such as corporate offices, military bases, and critical infrastructure, SDRs can detect and mitigate attempts to intercept or disrupt communications. This is crucial for protecting sensitive information and maintaining the integrity of wireless networks.

## Threat Detection and Analysis

The ever-changing nature of cyber threats demands equally dynamic detection and analysis tools. High-performance SDRs excel here due to their ability to capture and analyze a wide range of signals in real

time. This is particularly important for detecting advanced persistent threats and other sophisticated cyber attacks that use diverse and evolving techniques.

SDRs can detect and analyze various signal types, including those used in covert communication channels, command and control (C2) servers, and data exfiltration methods. By continuously monitoring the spectrum, SDRs can spot unusual patterns and behaviors indicating cyber threats. This is all made possible through the use of dedicated DSP chips embedded within SDRs, most commonly field programmable gate arrays, which allow for parallel processing and the integration of 3<sup>rd</sup> party IP for a variety of techniques for detection using different processing strategies.

In addition to detection, SDRs are invaluable for forensic analysis after a cyber incident. By capturing and storing signal data, they provide critical information for reconstructing events, identifying attack methods, and developing prevention strategies.

## Counterintelligence and Electronic Warfare

In counterintelligence and electronic warfare, high-performance SDRs are indispensable. Governments and military organizations use SDRs to detect and counteract electronic threats like signal jamming, spoofing, and eavesdropping.

SDRs can detect and analyze signals from various sources, including radar systems, communication networks, and unmanned aerial vehicles (UAVs). By identifying signal characteristics, SDRs help determine their origin and intent, which is crucial for developing countermeasures and protecting against electronic threats.

## Technical Capabilities and Advancements

The effectiveness of high-performance SDRs in cybersecurity comes from their advanced technical capabilities. Several key features and advancements make these SDRs particularly suitable for cybersecurity applications.

### Wide Tuning Range and High Bandwidth

A tuning range of up to 40GHz allows SDRs to monitor a vast portion of the electromagnetic spectrum. This wide range is essential for detecting and analyzing signals across different frequency bands, including those used by new technologies like 5G and satellite communications.

High bandwidth is another critical feature, enabling SDRs to capture and process large amounts of data in real time, which is crucial for detecting fast and transient signals. High bandwidth also allows for simultaneous monitoring of multiple frequency bands, providing comprehensive spectrum coverage.



## Advanced Signal Processing

Advanced signal processing capabilities are at the heart of high-performance SDRs. These include techniques like digital filtering, modulation and demodulation, and spectral analysis. By using these techniques, SDRs can accurately identify and classify signals, even in complex and noisy environments.

Machine learning and artificial intelligence (AI) are increasingly being integrated into SDRs to enhance their signal processing capabilities. AI algorithms can recognize patterns and anomalies in signal data, improving the detection and analysis of cyber threats. These algorithms can also adapt to new threats and evolving attack techniques, providing a proactive defense mechanism.

## Reconfigurability and Flexibility

The software-based nature of SDRs allows for easy reconfiguration and updates. This flexibility is crucial in the dynamic field of cybersecurity, where new threats and technologies regularly emerge. SDRs can be quickly reprogrammed to support new frequency bands, protocols, and signal processing techniques, ensuring they remain effective against the latest threats.

Furthermore, the modular design of many SDRs allows for the integration of additional hardware components, such as frequency converters and signal amplifiers. This modularity enhances SDR performance and capabilities, enabling them to handle a wider range of applications and environments.

## Challenges and Future Directions

While high-performance SDRs offer significant advantages in cybersecurity, they also face several challenges. Addressing these challenges is essential for maximizing the effectiveness of SDRs and ensuring their continued relevance in the cybersecurity landscape.

## Signal Overload and Data Management

Capturing signals across a wide tuning range and high bandwidth generates large volumes of data. Managing and analyzing this data can be challenging, especially in real-time scenarios. Efficient data management and processing techniques are needed to handle the data overload and extract meaningful insights.

Advances in on-board processing capabilities, cloud computing, and edge computing are helping to address this challenge. By leveraging these technologies, SDRs can either process data at the source using high performance signal processors and only send post-processed data or offload data processing tasks to powerful servers or distributed edge devices. Either of these approaches are valid where the first reduces the processing and storage requirements of the interfacing equipment and the latter enables real-time analysis and reduces the burden on SDR hardware.

## Signal Interference and Noise

The electromagnetic spectrum is crowded and noisy. SDRs must distinguish between legitimate signals, interference, and noise. Advanced filtering and signal separation techniques are essential for improving SDR accuracy and reliability in detecting and analyzing cyber threats.

Ongoing research in signal processing and machine learning focuses on developing more effective methods for dealing with interference and noise. These methods include adaptive filtering, blind source separation, and AI-based noise reduction algorithms.

## Security and Resilience

As critical components in cybersecurity, SDRs themselves must be secure and resilient against attacks. Ensuring the integrity and security of SDR software and hardware is paramount. This includes protecting against firmware tampering, software vulnerabilities, and hardware-based attacks.

Implementing robust security measures, such as secure boot, encryption, and regular software updates, is essential for safeguarding SDRs. Additionally, ongoing monitoring and threat assessments are necessary to identify and mitigate potential vulnerabilities.

High-performance software defined receivers with tuning ranges up to 40GHz are crucial in cybersecurity. Their advanced capabilities in signal detection, analysis, and response make them indispensable for network security, threat detection, and counterintelligence. As cyber threats continue to evolve, the adaptability and flexibility of SDRs will be key to maintaining robust and proactive defenses.

The integration of advanced signal processing techniques, machine learning, and AI into SDRs is enhancing their effectiveness and enabling them to keep pace with emerging threats. However, challenges related to data management, signal interference, and security must be addressed to fully realize the potential of SDRs in cybersecurity.

Looking ahead, ongoing research and development in SDR technology, combined with advancements in computing and AI, will continue to drive the evolution of high-performance SDRs. These developments will ensure that SDRs remain at the forefront of cybersecurity, providing the necessary tools to protect against increasingly sophisticated and diverse cyber threats.

## About the Author

Brandon Malatest is the COO and Co-Founder of Per Vices Corporation, a leader in Software Defined Radio technology. Brandon has an honours degree in Physics with a specialization in Experimental Physics from the University of Waterloo in Ontario, Canada. On graduating, Brandon started his career as a research analyst and statistician at one of the largest market research firms in Canada and later joined Victor Wollesen to co-found Per Vices. Since starting Per Vices, Brandon has authored many thought leadership articles based on software defined radio technology. Brandon and Per Vices can be reached online by contacting [solutions@pervices.com](mailto:solutions@pervices.com) and at our company website <http://www.pervices.com>.





## How Ransomware Jeopardizes Healthcare Organizations

Ransomware is becoming a concern for healthcare organizations. Learn why healthcare is susceptible to it and what they can do to avoid its detrimental impact.

By Kartik Donga, Founder, PeoplActive

Security challenges in the healthcare sector continue to grow as connected assets and attack surfaces expand. Organizations in any sector face financial ramifications in the aftermath of a successful attack, but in healthcare the stakes are higher because patient outcomes are at stake. One of such threats that has been growing across worldwide for the healthcare sector is 'ransomware'. 41% healthcare organizations globally are concerned with this cyber threat as per 'The Global Healthcare Cybersecurity Study 2023'. And we can clearly see the reason why. The disruption caused by ransomware attacks on the continuity of care is huge leaving healthcare organizations in a state of chaos. In this blog, we will explore the reasons why healthcare is becoming a target, what impact these attacks have and how healthcare organizations can stay proactive against such threats. Let's dive in.

## Healthcare becoming a Ransomware Magnet. Why?

### 1. Sensitive Patient Information

The foremost reason healthcare organizations are becoming a ransomware magnet for malicious actors to exploit is the sensitive patient information. According to research by Rubrik, a typical healthcare organization has more than 42 million sensitive records – 50% more sensitive data than the global average of 28 million. This data is lucrative for cyber criminals and often the reason they target healthcare organizations. Once these malicious actors get access to such data, they can use it for various gains such as financial frauds, identity theft.

### 2. Legacy Software Systems

Ransomware attacks are also prevalent in healthcare due to their outdated systems. Healthcare organizations don't update their systems often because it disrupts operations. Updates protect these organizations by patching their security vulnerabilities. If these vulnerabilities aren't fixed in time, they can convert into data breaches. In fact, according to Sophos, in 29% of ransomware attacks, exploited vulnerabilities are the root cause of the attack. Hence, making them easy entry points for hackers to infiltrate and cause disruption. Want to secure your medical devices from such attacks? Learn more about our **medical device cybersecurity**.

### 3. Staff Unawareness

Healthcare staff remains to be a weak link against cybersecurity attacks like ransomware for hospitals. When it comes to ransomware attacks your staff can play a huge role in avoiding it. Credentials compromise (32%), Email based attacks (malicious links or phishing) in over one third of cases were the root cause of

ransomware attacks according to Sophos. All these attacks can be minimized if your healthcare staff is more aware of the cyber-threatening landscape like phishing attacks.

## The Impact of Ransomware on Healthcare Organizations

### 1. Financial Loss

The first point of impact that healthcare organizations face post a ransomware attack is the ransom they must pay to recover the data or the system. In 2023, as per The Global Healthcare Cybersecurity Study 2023, 26% of healthcare organizations had to pay money as ransomware payments. Data retrieval becomes an important aspect of healthcare as operations are impacted due to a ripple effect.

### 2. Data Loss

The second impact that a healthcare organization faces post a ransomware attack is the data loss. As per a Sophos report, in the year 2023, in more than one-third of the cases (37%) after the data was encrypted during a ransomware attack, the data was stolen as well. This “double-dip method” has also become quite common by cyber attackers over the years. This data is then used for financial frauds and



identity theft. Did you know According to Forbes, that a healthcare record can be worth as much as \$1000 on the dark web? You can make your data secure from such attacks with [PeoplActive's healthcare cybersecurity consulting](#).

### 3. Operational Downtime

Another area which is impacted by ransomware attacks is operations. When a ransomware attack hits a healthcare organization critical information is impacted like patient diagnosis and treatment history which is critical for carrying out the operations. When such information cannot be accessed, the healthcare institution must postpone appointments and care deliveries. Furthermore, healthcare organizations without regular backups as a security measure must pay recovery costs to overcome this bottleneck. 40% of healthcare organizations had to bear this cost in 2023 as per the 'The Global Healthcare Cybersecurity Study 2023'

### 4. Reputational Damage

Benjamin Franklin has quoted, "It takes many good deeds to build a good reputation and only one bad to lose it." A ransomware attack is the result of that one bad deed. Hospitals and healthcare institutions must bear with the attack's aftermath where the patient's trust is lost. Ultimately affecting the hospital's reputation and the bottom line. To recover from the reputational damage the hospitals must bear the recovery costs. Infact, 35% of healthcare organizations had to bear reputational costs in the year 2023 after a cyber incident.

## How can you stay proactive?

Staying proactive against ransomware requires healthcare organizations to take a multi-faceted approach towards cybersecurity. Here are some things businesses can do:

### 1. Continuous Threat Monitoring and Detection

One of the measures against ransomware attacks is implementing continuous threat monitoring and detection tools before they can inflict significant harm to your business. Insights from regular monitoring can help hospitals detect unusual patterns or abnormalities in the systems and eliminate them before they grow. One of the tools you can deploy is Security Information and Event Management (SIEM) systems.

The tool collects, correlates, and analyzes data on security from various sources, such as servers, applications, and network devices. SIEM solutions enable proactive threat detection, incident response, and regulatory compliance by centralizing security event logs and applying advanced analytics. These threat monitoring and detection measures can be carried out in-house or managed by a [cybersecurity consulting services](#) provider to reduce the risk.

### 2. Rock-solid Incident Response Plan

In most of the ransomware cases, the healthcare organizations are baffled as to how to process the attack. Healthcare organizations should have a rock-solid incident response plan to mitigate such threats.

These response plans establish clear procedures such as initial assessments to understand the scope and how to remove malware should be there. Furthermore, assigning responsibilities to the respective team members and a post-incident analysis to improve their security. One can also get advice from a healthcare cybersecurity consulting to gain a better understanding.

### **3. Regular Backups**

Backups are your #1 ally in such cases. A well-defined backup procedure which backups critical data at regular intervals and continuously ensures that your data and systems are intact. Automated backups without manual intervention ensure that your data is secured. Furthermore, these backups must be stored in secure, offsite locations which remain resilient to local system failures and attacks. Taking things a step further would be regular testing of such backups and recovery systems.

### **4. Employee Training**

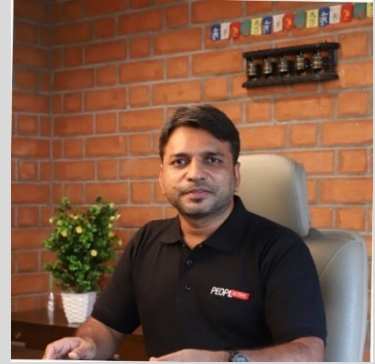
Creating a culture of cybersecurity is not easy unless your employees are involved in it. Providing your staff members with the knowledge against cyber threats and how to mitigate them reduces the likelihood of human error in such cases. If your employee knows someone is trying to gain sensitive information out of them, they would be the first to report it to the authorities. Furthermore, creating secure policies also strengthens the adherence part to the training. But how do you train them? You can consult a healthcare cybersecurity consulting service provider as they are experts when it comes to cybersecurity.

## **Final Thoughts:**

While it is easy to get overwhelmed looking at the growing threat landscape of cyber-attacks in healthcare. But, by learning from past cyber incidents, healthcare providers, cybersecurity experts and policy makers can create robust defenses against cyber-attacks. Remember your toughest case isn't on the operating table, but in your inbox trying to ruin your business. It's time to take a proactive stance against it. At PeoplActive, we help you solve such cyber problems with our healthcare cybersecurity consulting. Having extensive experience in healthcare, we know your vulnerabilities better than you do. The time to act is now. By taking a collaborative approach, you can safeguard your business from such emerging threats.

## About the Author

Kartik Donga is one of the thought-leaders in the technology space. With over 2 decades of experience in delivering impeccable technology solutions to businesses, he has transformed both digital and cybersecurity sectors. Healthcare cybersecurity being one of the areas he is passionate about, he loves to contribute every now and then regarding topics that involve cybersecurity strategies, tools and ever-evolving threat landscape. He loves staying up-to-date with the industry news that involve anything around cyber threats and enabling businesses develop resilience against cyber threats.



Kartik can be reached online at

LinkedIn (<https://www.linkedin.com/in/kartikdonga-peoplactive/>)

Email - [Digital@peoplactive.com](mailto:Digital@peoplactive.com)

Our company website - <https://peoplactive.com/contact/>



## Illegal Crypto Mining: How Businesses Can Prevent Themselves From Being ‘Cryptojacked’

By Andy Syrewicze, Security Evangelist at Hornetsecurity

The popularity of cryptocurrencies like Ethereum and Bitcoin surged during the pandemic era. What began as a niche, almost novelty form of payment in the 2010s, transformed into a legitimate financial asset. These currencies significantly contributed to the development of emerging technologies such as the metaverse and Web 3.0, a decentralized, blockchain-based version of the Internet open to everyone.

Although excitement around the metaverse and Web 3.0 has somewhat diminished, cryptocurrencies have maintained a strong presence in business and technology. Despite a [collective drop in 2022](#), Bitcoin has since reached record highs, with other popular coins also experiencing significant value increases.

The rising value of Bitcoin and other cryptocurrencies may lead to an increase in crypto mining operations by individuals and groups aiming to capture a share of these gains. However, if this trend continues, it

could spell trouble for organizations with vulnerable technical infrastructures, many of which do not realize they are at risk of exploitation from illegal crypto mining operations.

As such, business leaders should familiarize themselves with the tactics cyber criminals use to exploit tech infrastructure for crypto mining, and understand how they can prevent it.

## Legal vs. Illegal Crypto Mining

Cryptocurrencies were invented to establish a decentralized form of payment, meaning that banks or institutions had no control over their use and distribution. However, to protect against inflation, new crypto coins must be "mined," a process that involves solving complex mathematical problems. This process not only validates transactions and secures the blockchain but also controls the coin supply to prevent inflation, thereby adding security and integrity to the network. It's worth noting that newer guidelines exist for some cryptocurrency that doesn't require mining, but mining is, by-and-large, still a large part of the process today for many currencies.

That said, in the early days of Bitcoin, it was possible to mine crypto coins with a standard PC, but the increasing popularity of cryptocurrencies has decreased the number of generated units to prevent inflation. This means that crypto miners need much more computational power and resources, with many now renting hash services from a cloud mining provider to perform the same job.

While many crypto miners obtain their support through legitimate means, the high costs of legal mining operations have inspired some to seek support illegally with the help of botnets. This practice allows miners to make as many computers as possible part of one network, without the consent of the user.

## Forms of illegal crypto mining

Bad actors can engage in illegal crypto mining through two primary methods: the injection of JavaScript commands and crypto-jacking via malware.

The first method exploits popular crypto mining programs, such as the now-defunct Coinhive. Since most crypto mining programs run on JavaScript, bad actors deploy scripts across websites and browsers. When users visit these crypto mining websites, the script forces the users' devices to engage in crypto mining without their notice or consent, sometimes even utilizing the full processing power of the device.

The second method, crypto-jacking, is much more serious. Cybercriminals will often deploy malware specifically designed to exploit digital infrastructure, often through links to infected websites and pirated software. Users will unknowingly click links or download software, deploying malware that runs in the background. Due to the large amount of computing power needed to support the mining, criminals will throttle the software to avoid detection. Crypto mining malware can consume up to two-thirds of a victim's computer power, making detection even more challenging for users.



## The risks of illegal crypto mining for businesses

Business leaders might believe that illegal crypto mining programs pose no risks to their operations. Considering the number of resources most businesses dedicate to cybersecurity, it might seem like a low priority in comparison to other risks.

However, the successful deployment of malicious crypto mining software can lead to even more risks for businesses, putting their cybersecurity posture in jeopardy.

Malware and other forms of malicious software can drain computing resources, cutting the life expectancy of computer hardware. This can decrease the long-term performance and productivity of all infected computers and devices. Additionally, the large amount of energy required to support the high computing power of crypto mining can drain electricity across the organization.

But one of the most severe risks associated with malicious crypto mining software is that it can include other code that exploits existing vulnerabilities. Ransomware and viruses can spread across networks, impacting sensitive data and network infrastructure that can lead to severe financial and legal consequences for organizations.

## Safeguarding businesses against illegal crypto mining with employee training

While powerful cybersecurity tools are certainly important, there's no single solution to combat illegal crypto mining. But there are different strategies that business leaders can implement to reduce the likelihood of a breach, and mitigating human error is among the most important. In fact, the World Economic Forum [shows](#) that 95% of all cyber security incidents are caused by human error.

The most effective security awareness environment is one in which employees don't just know how to identify a possible threat – but one where they see cybersecurity as a necessity, rather than a nuisance. Cybersecurity has to feel like it's everyone's responsibility and a crucial part of every employee's job.

For this reason, it's important to build awareness on how cybercriminals engage in illegal crypto mining and the kind of tools they use. It is, of course, essential to supplement this with a powerful email security solution which leverages next generation features like advanced threat protection defensive tools powered by AI to spot evolving threats.

Moreover, [research](#) at Hornetsecurity revealed that phishing is still the most popular form of cyberattack, representing 43.3% of all identified threats. Spam or spoof emails may often contain links leading to websites contaminated with crypto mining droppers, and as it can be difficult to distinguish them from normal emails.

Business leaders therefore need to treat employees as the first line of defense against these types of cyberattacks, in order to create a "human firewall" to shield against threats. To do this, business leaders should consider these tips to help reduce the risks of illegal crypto mining operations.

Educate employees on cyber threats: Conduct training on the risks of illegal crypto mining, and

ransomware for all employees. This will heighten their awareness of strange activity and prevent them from falling for common tricks.

Implement cybersecurity policies for employees: Have a detailed cybersecurity policy so employees fully understand how to work safely and securely. This includes password management, using multi-factor authentication for logins, and policies for using company devices on unsecured networks.

Enable spam and web filters to block suspicious activity: Employ a managed spam filter service and web filters to block all such content in advance.

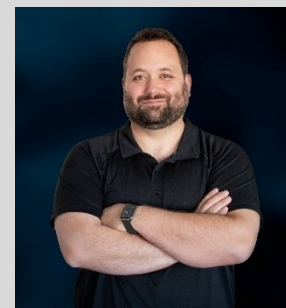
Encourage communication and transparency: Ensure employees report suspicious activity to IT or cybersecurity teams and their coworkers. This will help stop threats early, and prevent them from evolving into larger problems.

Have an incident response plan: Even with regular training, employees can still make mistakes. An incident response helps employees follow the best course of action if illegal crypto miners manage to compromise IT infrastructure.

Staying ahead of emerging threats and enabling protective measures before cybercriminals can identify potential gaps have never been more important for businesses. Through education and training, businesses can not only fend off the risks of illegal crypto mining, but also from all other types of harmful attacks such as ransomware, while creating a safe security culture across the entire organization.

### About the Author

Andy Syrewicze, Security Evangelist at Hornetsecurity, is a 20+ year IT Pro specializing in M365, cloud technologies, security, and infrastructure. By day, he's a Security Evangelist for Hornetsecurity, leading technical content. By night, he shares his IT knowledge online or over a cold beer. He holds the Microsoft MVP award in Cloud and Datacenter Management. Website: <https://www.hornetsecurity.com/en/>





## Maintaining File Security While Working Remotely

For remote workers in the knowledge economy, intellectual property (IP) is everything. And that's why defending it is so important.

By Majed Alhajry, CTO of MASV

These days remote workers in home offices using residential WiFi must maintain a similar security posture as a full-on corporation while working with other remote stakeholders, clients, and partners anywhere in the world.

Daunting? Yes. Impossible? Absolutely not. Read on to find out why.

### How to Maintain File Security in Remote Workflows

Keeping a strong cybersecurity posture isn't a luxury in 2024: it's a necessity. Especially if you don't want to lose client and stakeholder trust and end up on an embarrassing data breach list.

Here are six ways anyone working remotely can protect their data and systems from unwanted intrusions and the rapidly evolving threat landscape.

## Secure remote connections and hardware

All hardware and connection points among collaborators must be secure. If you use networked storage, configure your device to use an HTTPS connection, ensure you have a valid SSL/TSL certificate installed, and get your data backed up.

You should also ensure you and your collaborators keep all hardware and software up to date and fully patched, along with securing WiFi networks by logging into your router and disabling WPS and remote access, enabling HTTPS logins and WpA2 encryption, and updating the firmware.

Other best practices for keeping hardware and remote connections secure include using a virtual private network (VPN) or desktop-as-a-service (DaaS) platform, ensuring all endpoints have anti-virus and anti-malware protection, and educating stakeholders on the risks of human engineering attacks.

## Identity access management (IAM)

Speaking of educating stakeholders, we all know that humans are the weakest link in any cybersecurity posture.

And while security awareness training can help a ton, you also need to protect people from themselves with strong password enforcement and access management controls such as multi-factor authentication (MFA) or two-factor authentication (2FA). Enforcing the principle of least privilege—where stakeholders only have access to the data they need to do their jobs, and nothing more—is also highly encouraged.

Once you've developed a list of role-based access policies, enforce it with automated IAM software to keep your rules effective and enforced at scale.

## Strong encryption

Strong encryption such as Advanced Encryption Standard (AES) is a must when working remotely and transferring data to other remote workers and locations. That's because even if your other measures fail and your system is breached, strong encryption ensures hackers won't be able to read the data.

And although hackers can (and do) break cryptography using various methods such as cypher-text attacks, cracking those codes takes a lot of work and know-how. Unless the hacker is coming after you and your work specifically, it's likely they'll just move on to a softer target.

Always keep your files encrypted while at rest (and in flight during data transfers). Most data breaches come down to human error, not Enigma-style code breaking.

## Watermarking and chain of custody

For creatives who work with visual media, especially—but really for anyone who works with high-value data remotely—it’s also a good idea to use both visible and invisible watermarking, along with tracking all data movement through a recorded chain of custody.

Visible watermarks are useful in that they tell the world a piece of content or file is yours. But a savvy user can also remove or crop them out fairly easily.

That’s why forensic watermarking exists. Forensic watermarking embeds an imperceptible, metadata-infused mark that gives content owners valuable intel on who has viewed their content. This can help content owners track down the perpetrators in case of a data leak.

Forensic watermarks are imperceptible, robust—they should never break, even if the host file is dramatically altered—and are impossible to modify or alter.

## The Importance of Security for Remote Workflows

Remote workers who deal with sensitive and valuable data and files need to take security as seriously as any corporate IT team.

While the resources you have at your disposal aren’t quite the same as the head of IT for a Fortune 500 company, there are several simple steps you can take to lock down your workflow, including:

- Securing remote connections and hardware.
- Using identity access management and the principle of least privilege.
- Encrypting all files both in flight and at rest.
- Document watermarking and chain of custody.

By following these best practices and encouraging a culture of security among you and all your stakeholders, you can ensure your data stays secure—and avoid getting you, your company, or your partners placed on a data breach list.

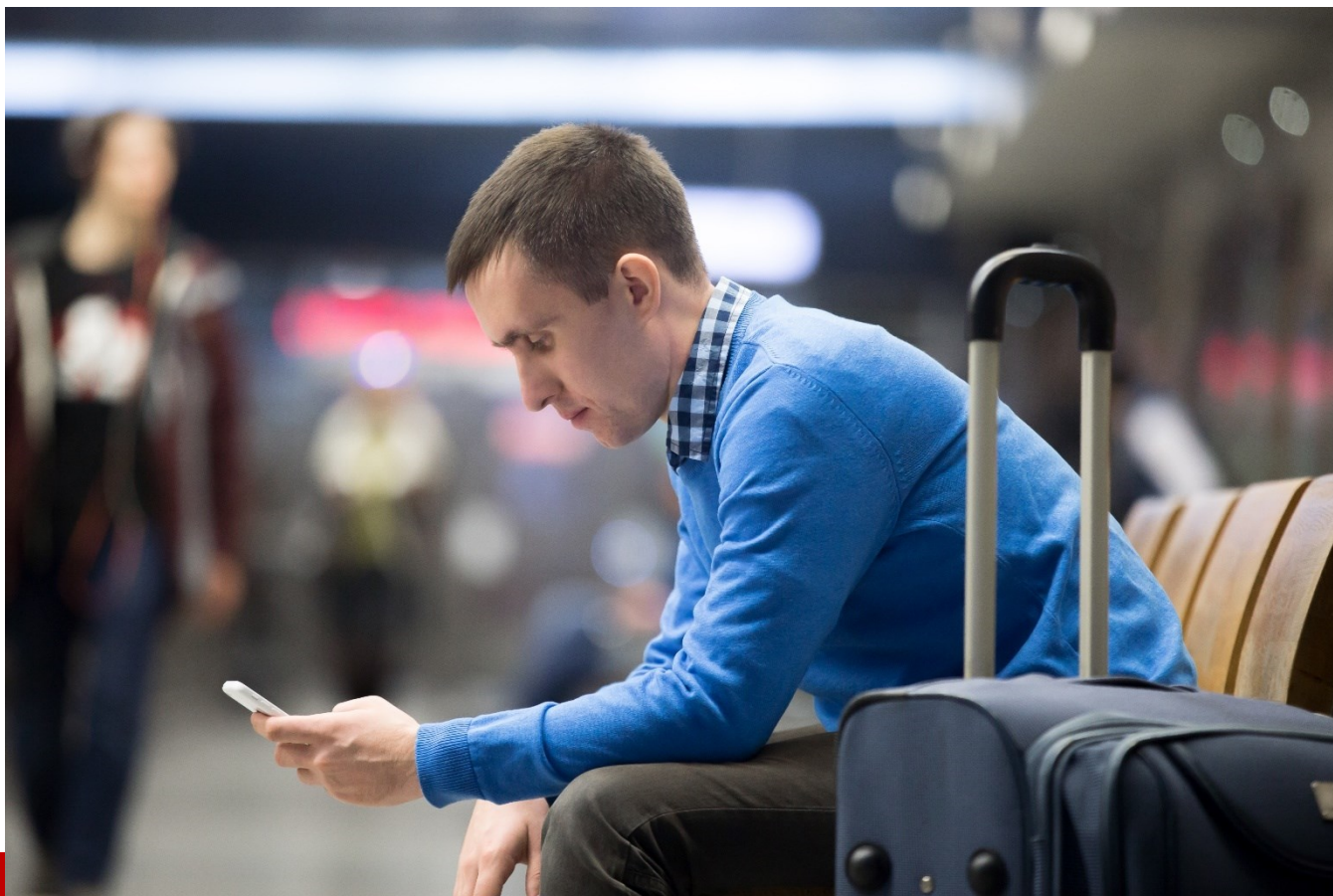
### About the Author

Majed Alhajry is the CTO of [MASV](#), the fastest large file transfer solution for media organizations. Majed’s passion lies in discovering novel solutions for complex technical problems, and he is an expert in the transfer of large files, both local and global, as well as in networking acceleration technology and application layer protocols.

Majed can be reached online at <https://www.linkedin.com/in/majed-alhajry-3a39a410/?originalSubdomain=ca> and at the company website: <https://massive.io/>







## Mitigating the Risk of Cybercrime While Traveling Abroad

How International Travelers Can Enhance Their Digital Safety Habits

By Dana Hummel, Senior Manager of Digital PR, All About Cookies

Global tourism is reaching pre-pandemic records and many people are eager to embark on a new adventure. Yet at the same time, incidents of cybercrimes are increasing at a staggering rate.

Reports indicate more than 340 million people were affected by cybercrimes in 2023 – a historical record. Breaking this down even further, the travel and tourism sector ranks #3 in cyberattack incidents alone.

This leads us to an unfortunate reality. International travelers just want to enjoy some time away from work. But they're becoming more vulnerable to cybertheft.

And while the statistics are concerning, cybercriminals aren't complaining. They can put their feet up and relax, as hijacking one's information is getting that much easier.

In fact, a new study by [All About Cookies](https://allaboutcookies.org/international-travelers-internet-safety-survey) (<https://allaboutcookies.org/international-travelers-internet-safety-survey>) shows more than 90% of Americans are engaging in risky tech practices while abroad.

The good news is that it doesn't have to be this way. There are several mitigation tips to follow in the long run and the majority of them can be accomplished within five minutes or less. But first, here's an overview of the big issues tourists and travelers are facing.

## The Most Common Mistakes Travelers Take with Their Digital Security

From accessing a checking account on an open Wi-Fi network to accepting unknown Bluetooth connections, cybercriminals are targeting those who aren't taking the necessary precautions.

The true challenge is battling the temptation to prioritize your personal tech over your personally identifiable information (PII). All About Cookies' study addresses how 60% of travelers are quick to connect their devices to a public charging station – a tourist trap that is directly linked to “juice jacking.” Separately, more than half of travelers either post their location on social media or check their financial information online.

Despite FBI warnings and government issued statements, many travelers aren't changing their ways. Yet these mishaps can result in compromised data and financial loss. Experts in the field recommend that travelers install a virtual private network (VPN) and sign up for an identity theft protection service.

## Unsafe Behaviors Can Lead to Dangerous Consequences

How many people are practicing safe tech habits? Not as many as you'd think.

It's understandable. One's digital security isn't top of mind when planning what activities to do on a trip or deciding which attractions are a must-see. This leaves a wide opening for cybercriminals to find their next victim.

Just over half (52%) of travelers alert their financial institutions before traveling abroad and 44% make sure to turn off their Bluetooth signal.

Since Bluetooth technology automatically creates a wireless connection, it grants instant access for cybercriminals to see the apps and websites you're already logged into. Travelers may want to turn off certain device sharing features and update their passwords.

Taking note of a couple basic practices will also allow tourists and their traveling peers to make the right decisions.

## Travel Safety Best Practices

Below are a few steps that can go a long way in preventing identity theft and more. A worthwhile tradeoff to consider when planning your next vacation.

- 1) Refrain from checking your personal banking apps or financial information over public Wi-Fi.

- 2) Enable a two-factor (2FA) authentication process on your gadgets and electronic devices.
- 3) Limit public posting about your location on social media and other forums.
- 4) Read up on travel advisories/restrictions specific to the region that you're visiting.
- 5) Adjust the screen settings on your devices to allow for a shorter automatic sleep feature.

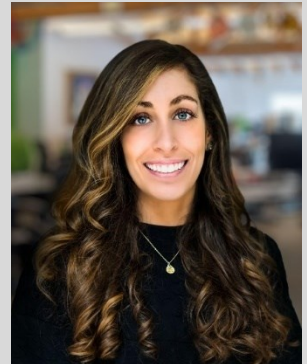
Not only do these digital safety habits create an added layer of protection for your online identity, they're even applicable for domestic travel in the U.S.

## Putting The Pieces Together

International travel is continuing to take off and while there's a lot that goes into packing and booking flights, one's digital safety should be included in the pre-planning process. By understanding how to avoid privacy issues and oversharing on the internet, travelers can stay better protected no matter their destination.

### About the Author

Dana Hummel is the Senior Manager of Digital PR at All About Cookies. She brings over 9 years of experience to the content marketing industry and has a specialized focus in cybersecurity, technology, and digital trends. Dana can be reached at LinkedIn (<https://www.linkedin.com/in/dana-hummel-goldberg/>) or [danahummel@allaboutcookies.org](mailto:danahummel@allaboutcookies.org).





## Modern Phishing Challenges and the Browser Security Strategies to Combat Them

By Kenneth Moras, Security GRC Lead, Plaid

In today's landscape of advanced phishing attacks, which leverage legitimate domains and sophisticated tactics to evade traditional security measures, it is imperative for organizations to bolster their digital defenses. Browser security solutions have emerged as a critical component in this effort, providing essential protection that complements existing strategies such as DNS security solutions. Here's why these solutions are indispensable in the fight against modern phishing threats.

### Understanding the Modern Phishing Landscape

Consider a scenario where an email directs the recipient to a Dropbox file. Upon clicking the link, the user is redirected to a Google Drawings page, ultimately landing on a fake login site designed to steal

credentials. This elaborate journey through trusted domains makes it nearly impossible for traditional security systems to detect the malicious intent.

Attackers have honed their techniques, exploiting the trust placed in well-known sites like Dropbox and Google. This sophisticated pathway easily slips through conventional defenses, highlighting the need for enhanced security measures.

## Limitations of Traditional Security Measures

Organizations typically deploy a comprehensive suite of security tools, including email security, firewalls, DNS filtering, web proxies, endpoint detection and response (EDR), and antivirus (AV) software. While these tools are foundational, they often depend on threat intelligence feeds listing known malicious domains. However, phishing attacks leveraging trusted domains can evade these defenses.

For example, while EDR and AV solutions excel at identifying malware, they often miss credential theft attempts that don't involve malware. Similarly, email security and DNS filtering might not flag links from reputable domains, allowing phishing emails to bypass these controls and reach users.

## Bridging the Browser Security Gap

Web browsers are the primary interface for internet access, making them a critical target for phishing attacks. Yet, they frequently represent a significant gap in many organizations' security strategies. Existing protections like EDR systems, firewalls, and Secure Access Service Edge (SASE) technologies offer some insight into browser processes and network-level activities but fall short in deciphering the nuances of in-browser user behavior. Zero-day phishing attacks, overlaps between personal and work accounts, and the intricacies of file-sharing and productivity applications in the browser remain elusive threats to legacy solutions, challenging to preempt and mitigate.

Modern browser security solutions analyze web activity directly within the browser, providing real-time visibility and control over user interactions with web pages. By scrutinizing the characteristics and behaviors of web pages—such as advanced analysis of site content, web scripts, and the DOM to understand context and activity risk—these solutions can detect and block malicious activities even if the domain hasn't been flagged as dangerous.

## Key Use Cases for Browser Security

- **Monitoring Domain Age:** Domains less than 30 days old might be considered malicious and automatically blocked or trigger a warning to employees to exercise caution before proceeding.
- **Controlling Excessive Permissions:** Sites requesting excessive permissions (such as clipboard access, location, camera, etc.) are automatically blocked to prevent potential abuse.
- **Blocking Typosquatting Links:** Links that use typosquatting (slight misspellings of legitimate domains) are identified and blocked to prevent phishing attacks.



- Preventing Browser-in-the-Browser Attacks: Advanced attacks that simulate legitimate browser windows within the browser are blocked using real-time analysis.
- Regulating Data Uploads: Uploads to personal Google Drive accounts versus corporate Google Drive accounts are monitored and blocked based on browser profile information to prevent data exfiltration.
- Detecting Malicious Browser Extensions: Malicious browser extensions are detected and blocked to safeguard against unauthorized access and data theft.

## Enhancing DNS Security with Browser Solutions

Integrating browser security solutions with DNS security measures creates a more comprehensive defense strategy. DNS security solutions play a critical role in filtering out harmful content before it reaches the user by preventing access to known malicious domains. However, phishing attacks that utilize trusted domains can bypass these filters. Browser security solutions add an additional layer of protection by analyzing web content and behavior in real-time, identifying threats that have slipped past DNS filters.

By combining these approaches, organizations achieve a layered defense strategy that addresses both known and emerging threats. While DNS security solutions handle the initial filtering of traffic, browser security solutions ensure that any threats reaching the user are promptly detected and mitigated.

## Key Takeaway: The Importance of Browser Security in Modern Defense

As phishing tactics evolve and become more sophisticated, leveraging trusted domains and multi-step processes, traditional security measures alone are no longer sufficient. Browser security solutions provide the necessary visibility and control at the point of attack—the web browser.

### About the Author

Kenneth Moras, Security GRC Lead at Plaid, is a cybersecurity leader with extensive experience in building strategic risk management programs at Plaid and scaling cybersecurity programs at notable organizations such as Meta and Adobe. His expertise also extends to cybersecurity consulting for Fortune 500 companies during his tenure at KPMG

Kenneth can be reached online at <https://www.linkedin.com/in/kennethmoras>





## Navigating the Complexities of AI in Content Creation and Cybersecurity

**Balancing Innovation and Security: How to Leverage AI in Content Creation while Mitigating Cyber Risks**

**By Rachel Stella, Founder & CEO, Stella Social Media**

As AI technology continues to evolve, its integration into various business sectors like content creation is expanding. AI's capabilities can significantly enhance marketing and business strategies but also present unique challenges. A misapplication of AI not only risks damaging your brand's reputation but can also expose your systems to cybersecurity threats.

### **A Case Study in AI Misuse and Cybersecurity Risks**

In March 2024, the fashion retailer TrendSet experienced a severe backlash due to inappropriate AI-generated social media content. This incident stemmed from an over-reliance on AI without adequate oversight, leading to public disapproval and damage to the brand's image. This case underlines the critical importance of managing AI tools wisely and implementing strict cybersecurity measures to mitigate such risks.

### Excessive Reliance on AI for Creativity

- 1) **Pitfall:** AI lacks the nuanced understanding and emotional depth that human creators offer, potentially leading to content that fails to connect with the audience.
- 2) **Strategy:** Use AI as a tool to augment, not replace, human creativity. Blend AI-generated ideas with personal insights to produce content that is both efficient and impactful. In the context of cybersecurity, ensure that these AI systems are continuously monitored and updated to guard against vulnerabilities that could be exploited by cyber threats. This vigilant approach not only protects your creative content but also reinforces the security of your entire digital infrastructure.

### Inadequate Detail in AI Prompts

1. **Pitfall:** Generic prompts may lead to irrelevant content, weakening audience engagement.
2. **Strategy:** Craft detailed prompts that specify the desired context, tone, audience, and key messages to ensure AI produces applicable and compelling content. For example, instead of simply asking AI to generate a blog post about cybersecurity, provide a detailed prompt like, "Create an informative and engaging blog post for small business owners on how to implement basic cybersecurity practices, with a friendly tone, aimed at non-tech savvy readers, highlighting strategies such as two-factor authentication and secure Wi-Fi usage."

### Ignoring Ethical and Bias Issues

1. **Pitfall:** AI may replicate existing biases in training data, leading to unfair or harmful content.
2. **Strategy:** Use diverse and unbiased data sets and regularly review AI outputs for fairness and accuracy and establish protocols to address any ethical concerns. Additionally, integrate a feedback loop where human reviewers consistently evaluate AI-generated content to identify and correct bias, ensuring the output aligns with ethical standards and company values.

### Neglecting Cybersecurity in AI Deployment

1. **Pitfall:** Integrated AI systems can become targets for cyber threats, risking data breaches and content manipulation.
2. **Strategy:** Enhance cybersecurity by isolating business IT from personal networks, deploying anti-malware solutions, utilizing two-factor authentication, and avoiding public Wi-Fi to secure your AI systems and data. Regularly conduct penetration testing and vulnerability assessments to identify and address potential security gaps, ensuring robust protection against emerging threats.

## Incorporating Cybersecurity Best Practices

Cybersecurity is a critical concern, especially with the increasing use of AI. Implementing best practices such as using anti-malware software, enabling two-factor authentication, and using secure connections can significantly reduce risks. Regular audits and updates of cybersecurity measures can also help ensure that your business remains protected. Moreover, educating your team about phishing scams and the importance of secure browsing practices is essential to safeguard against potential threats.

## Conclusion: Harmonizing AI with Human Insight and Cybersecurity

While AI can greatly improve content creation, it's vital to maintain a balance between technological assistance and human oversight. By sidestepping these common pitfalls and reinforcing cybersecurity protocols, you can leverage AI's potential safely and effectively. Remember, the goal is for AI to complement—not replace—your creative endeavors and maintaining vigilance in cybersecurity is paramount in the digital age.

### About the Author

Rachel Stella is the Founder and Owner of Stella Social Media. She is a regular contributor to Small Business Trends and has been featured in prominent publications such as Social Media Today, Forbes, PR Daily, SmallBizDaily, Business Insanity Radio, and CEOMOM Magazine. Stella Social Media is a digital marketing agency specializing in social media management, now in its 15th year.

With a degree in Communications and a background in journalism, Rachel leverages her expertise in storytelling across various platforms including her blog, social media channels, and syndicated content. Her dedication to entrepreneurship and small business growth extends beyond her professional endeavors, as she actively mentors and advises aspiring business owners. She identifies herself as a chronic multitasker, a master connector, and embraces her dichotomy as a high-D introvert!

Rachel can be reached online at [rachel@stellasocialmedia.com](mailto:rachel@stellasocialmedia.com), <https://x.com/RachelStella>, [Rachel Stella | LinkedIn](#), and at our company website <https://www.stellasocialmedia.com/>.







## New Levels, New Devils: The Multifaceted Extortion Tactics Keeping Ransomware Alive

By Jacques de la Riviere, CEO, Gatewatcher

Having evolved from a basic premise of locking down a victim's data with encryption, then demanding a ransom for its release, research now suggests that ransomware will cost around \$265 billion (USD) annually by 2031, with a new attack (on a consumer or business) every two seconds.

Against such a pervasive threat, businesses have sought to better prepare themselves against attacks. They have developed an array of tools: better backup management, incident recovery procedures, business continuity and recovery plans have all made the encryption of victims' data less profitable.

In addition, security researchers together with national bodies such as the Cybersecurity and Infrastructure Security Agency (CISA) have made substantial progress in identifying the weaknesses in the methods used by attackers, in order to develop decryption solutions. [No More Ransomware](#), promoted by Europol, the Dutch police, and other stakeholders lists approximately one hundred such tools.



In response to these developments, attacker groups are reconsidering their strategy. Rather than risk detection by encrypting as much data as possible, they now prefer to quickly extract as much information as possible and then threaten to divulge it. Ransomware has become extortion.

### **Re-energising the threat of publication**

The potential public disclosure of sensitive information is the core of leveraging fear to pressure victims into paying a ransom. The reputational damage and financial repercussions of a data breach can be devastating.

Ransomware gangs have recognised the potential for damage to a brand or group's reputation simply by being mentioned on the ransomware operators' sites. A study found that the stock market value of the companies named in a data leak falls by an average of 3.5% within the first 100 days following the incident and struggles to recover thereafter. On average, the companies surveyed can lose 8.6% over one year.

This threat of loss based on association, now quantified and in the hands of cybercriminals has become an effective tool.

### **Operational disruption and revenue loss**

Modern businesses rely heavily on digital systems for daily operations. A ransomware attack can grind operations to a halt, disrupting critical functions like sales, customer service, and production.

This disruption translates to lost revenue, employee downtime, and potential customer dissatisfaction. The longer the disruption lasts, the greater the financial impact becomes. Attackers exploit this vulnerability, pressuring victims to pay the ransom quickly to minimize their losses. And they do this most effectively by recognising key operational data.

This then evolves as a ransomware attack on one company can ripple through its entire supply chain. Suppliers and distributors may be unable to access essential data or fulfil orders, leading to delays and disruptions across the chain.

Knowledgeable attackers now target a single company as a gateway to extort multiple entities within the supply chain, maximizing their leverage and potential payout.

### **Brand damage at the regulatory level**

Brazen ransomware groups have already realised the value in making direct contact with end-users or companies that are the customers of their targets as it enables the operators to increase pressure.

However, one new avenue of this direct attack on brand reputation is for the gangs to connect with the authorities. In November 2023, the ALPHV/BlackCat ransomware gang filed a complaint with the United States Securities and Exchange Commission (SEC) regarding their victim, MeridianLink.

In mid-2023, the SEC adopted new requirements for notifying data leaks effective from September 2023. One of these rules requires notification within four business days of any data leak from the moment it is confirmed. Not only did ALPHV/BlackCat take control of the trajectory of the extortion, but they also even circulated the complaint form among specialist forums as part of a promotional campaign.

## Targeting the most vulnerable

Ransomware gangs are not above using sophisticated, customized extortion strategies on the most vulnerable sectors. Healthcare has long been a key target – there is a step change in urgency when critical medical procedures may be delayed if ransom is not paid.

Just a few months after the international Cronos Operation, the Lockbit group claimed a new victim in the healthcare sector. The Simone-Veil hospital in Cannes suffered a data compromise, adding to the extensive list of attacks conducted in recent months by other ransomware players against the university hospitals of Rennes, Brest and Lille.

Once the data had been extracted from the hospital on April 17, 2024, an announcement concerning their compromise was made on Lockbit's showcase site on April 29, 2024. According to the cybercriminals' terms, the hospital had until midnight on May 1, 2024, to pay the ransom.

The lesson here is that attackers exploit the vulnerabilities and pain points specific to each industry, making their extortion tactics more potent. And they do so with no consideration for the victims.

Ransomware attacks are now more than just data encryption schemes. They are sophisticated operations that exploit a range of vulnerabilities to extract maximum leverage from victims. By understanding the multifaceted nature of ransomware extortion, businesses and individuals can develop a more robust defence against this growing threat.

### About the Author

Jacques de la Riviere is the Founder and CEO of Gatewatcher, a cybersecurity provider based in France. Jacques has held positions throughout OpenCyber, Adneom and BK Consulting. He is also currently vice-president of Hexatrust - a cluster of 100 European software cybersecurity leaders and cloud providers.





## Perimeter Security Is at the Forefront of Industry 4.0 Revolution

**The emergence of smart cities across the emerging countries is stimulating the perimeter security market growth and development.**

**By Avinash Dhanwani, Research Director, The Brains Insights**

Perimeter security can be defined as the measures and systems which are deployed in order to protect a physical space from intrusion, unauthorized access or any kind of security breaches. Perimeter security involves a wide array of physical and technological methods which are utilized to secure a property of facility aiming to detect, deter and respond to the threats before those threats can even get/penetrate that particular secured area/space. The primary objective of perimeter security is to safeguard assets, information or people within that secured perimeter. Basically, perimeter security acts as the first line of defense from security breaches and unlawful activities. The global perimeter security market was valued around USD 76 billion in 2023. The global [perimeter security market](#) is expected to grow around USD 151 billion by 2033 growing at a CAGR of 7.1%.

The importance of the perimeter security can't be ignored in the current situation. Perimeter security is crucial for military, government organizations and other business enterprises alike to detect potential threats, deter the possible intruders, and delay the illegal attempts which the intruders make while breaching in a secured area/perimeter. Additionally, perimeter security maintains the operational continuity within these organizations. To prevent unauthorized entry to the premises, high-security associations, commercial centers, government facilities and other organizations can establish a physical barrier utilizing detection and deterrence techniques. Traditional perimeter security systems may encompass electrified fences along with other preventative measures such as CCTV security system and intruder alarms.

There are different types of perimeter security systems. The most common type of perimeter security system is CCTV security system. In this type, cameras are being deployed within interior and exterior part of a premise/building in order to get an overall coverage. There are several types of cameras deployed such as IP, conventional, thermal and others. Each of the camera types work better than the others in different working environments. For instance, a thermal camera can pick up heat signatures of any living being in low-light areas. Apart from CCTV, there are other types of perimeter security systems such as access control systems, fiber optic detection system, motion sensors, radar system, electrified fences, microwave barriers and others which are being utilized.

The installation of each type of perimeter security system varies from one end-user industry to the other. For instance, industrial facilities such as refineries, factories or quarries have larger operational area/space/perimeter. People working on industrial facilities may be from the in-house company or working as 3<sup>rd</sup> party on contractual basis. Apart from expensive machinery installed within the industrial facilities, there are other critical assets or some information/data which may interest the intruders/thieves while breaching. Along with the theft, the necessity to prevent access from the unauthorized personnel to avoid data theft or accidents; which is why, the security system within industrial facilities (mentioned above) is critical. It requires advanced technical equipment and technologies to prevent any kind of property loss or sabotage. Furthermore, the system should be installed and maintained by the group of qualified industry professionals/experts from the security system providing companies.

The effectiveness of the perimeter security system depends upon several factors such as design and implementation of the security measures, proper integration of physical and electronic devices and expertise of a well-trained personnel. A well-designed perimeter security system should provide a comprehensive coverage of any building/premise with multiple layers of security which can be effective against intruders/thieves in creating obstacles. Regular maintenance and testing of the perimeter security system is necessary to ensure their continued efficiency. It is critical to continuously assess and expand perimeter security measures in order to counter different types of threats and hazards.

One of the most prominent trends within the global perimeter security market is the integration of the advanced technologies. The ongoing technological advancement within this industry is anticipated to have a positive impact within the market growth and development. Artificial Intelligence (AI) is greatly revolutionizing the market place. These technologies can assess enormous amounts of data in real time, learning and thereby adapting the patterns of any living being. AI based perimeter security systems can identify irregularities, predict potential threats and improve the overall situational awareness. This dynamic approach provides aid in evolving the perimeter security systems in order to counter the emerging threats. Furthermore, video surveillance is considered to be the base of the perimeter security. AI-based video surveillance systems help in identification of abnormal behavior or any kind of suspicious activities within the perimeter. This approach in greatly enhances the security of the perimeter security systems by reducing the response time and minimizing the risk of false alarms. This factor is anticipated to provide lucrative opportunities in the upcoming years.

The emergence of smart cities across the emerging countries is stimulating the market growth and development. Smart cities represent the integration of the digital technologies in urban environments in order to make lives sustainable and environment friendly. The evolution of the smart cities is mainly driven the need to address the urban issues and challenges such as population growth, public safety and

sustainable growth. By incorporating perimeter security systems including the integration of Artificial Intelligence (AI), smart cities can easily monitor their infrastructure in real time. This integration facilitates optimization of city services effectively by analyzing the perimeter threats. Furthermore, as the smart cities heavily rely on digital technologies cybersecurity becomes an important aspect in maintaining the overall perimeter security. Cybersecurity measures include incorporation of firewall systems, encryption, intruder detection systems and others. So, it becomes crucial because protecting the city's digital asset and infrastructure is a part of maintaining the overall security. Thus, ensuring robust cybersecurity measures should be deployed within smart cities.

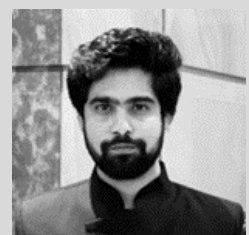
While the global perimeter security market is projected to grow at a substantial rate, the industry faces several challenges. High implementation costs, technical complexity in integrating several perimeter security components and lack of skilled workforce are some of the prominent challenges that the industry is facing. Additionally, the issues related to data privacy/data theft are emerging due to the emergence and integration of the digital technologies such as Artificial Intelligence (AI). These factors are restraining the market growth and development.

However, these challenges also present opportunities for the global perimeter security market to grow and flourish in near future. The demand for cost- effective solutions coupled with the growing concerns regarding data privacy provides prospects for the companies to differentiate themselves as innovative perimeter security solution provider in near future. This can help the companies in maintaining their competitive edge. Currently, the demand for customized solutions, user friendly interfaces and scalability is on rise. By leveraging this trend, the companies engaging in the industry can provide unique and customized solutions on the basis of their client's requirements. Additionally, the modern perimeter security solutions are designed with intuitive interfaces so that it would help the user to monitor and manage security systems easily. Scalability is an important aspect for consideration as it allows the security system to adapt to the changing needs of the customers. Thus, as the importance of the perimeter security solutions is gaining importance, the market is poised to have a significant growth in the upcoming years.

### About the Author

Avinash Dhanwani is the Research Director of Brainy Insights Private Limited. He is monitoring & engaging with latest innovations and market development in ICT industry.

Avinash can be reached online at ([sales@thebrainyinsights.com](mailto:sales@thebrainyinsights.com)) and at our company website <https://www.thebrainyinsights.com/>







## Greater Security for Small Businesses: Why Do SMEs Need a SIEM System?

By Sergio Bertoni, the Leading Analyst at SearchInform

**Recently, the number of cyber attacks has been increasing steadily. It's important to bear in mind that the more software and hardware the corporate infrastructure contains, the higher the chance of experiencing failures and problems within IT-infrastructure.**

In order to ensure control of external and internal information security risks, large companies have been implementing specific protective tools for a while. First of all, these are SIEM systems. Simultaneously, small companies often remain vulnerable in terms of the abovementioned risks, neglect protection of their own business and don't rush with ensuring protection. In this article I'll reveal, why implementation of SIEM systems is beneficial for SMEs and how to choose the system, that really suits your company's needs.

## Brief Description of SIEM Systems

Even small organizations use large number of technologies and various software, for example, firewalls, antiviruses, email, data base management systems etc. SIEM systems are developed for monitoring of complex IT-infrastructure, gathering and performing analysis of security events, revealing potential threats and targeted attacks in real life mode. The system notifies information security specialists about violations, failures and other problems. Data from SIEM system is also used for performing of corporate investigations. The system keeps archive with details on infrastructure operation for previous periods to ensure the availability of data if necessary.

## Why SMEs Need SIEM Systems

### 1. Ensure protection of IT-infrastructure

Each infrastructure object is a potential entrance point in the corporate infrastructure for malicious actors. Any infrastructure object may cause technical issues for the infrastructure or be exploited by malicious insiders for hacking, disabling IT system etc. SIEM systems gather and analyze data from various sources: employees' workstations, network scanners, servers, database management systems, programs etc. In fact, an organization remains under SIEM system's 24/7 supervision.

### 2. Automate routine processes

SMEs often don't have large IT and IS departments, thus, the task of automation of control over events in the IT infrastructure is an extremely actual one. Millions of security events are generated in the IT infrastructure of even small company on an everyday basis. It's too labor-intensive to analyze all of them manually. And it's even more difficult to detect dangerous activities and incidents in the overall event flows. SIEM systems optimize IS specialists work processes: software gathers events from various sources and thanks to the embedded analytical tools establish a correlation between them and notifies employees in charge about the threat.

### 3. Ensure control of network equipment

SIEM systems enable to ensure control of equipment condition and don't leave processes to chance. For example, a server equipment's change of temperature may indicate a serious failure, in some cases it may even alert that fire is about to begin. The system detects overheat, what enables to obtain the issue just in time and eliminate it. SIEM systems ensure protection against such situations as failure of equipment, due to which the organization may temporarily become inoperable.

### 4. Ensure compliance with regulatory requirements

Due to the increasing amount of cyber risks and ongoing sophistication of threats, SIEM systems are becoming more and more crucial components of ensuring corporate protection. SIEM class systems are crucial components of ensuring compliance with regulatory requirements, as they are capable of obtaining and analyzing data, related to security events within the whole corporate infrastructure and revelation of potential vulnerabilities and incidents. SIEM system should also provide the required functionality for performing full-scale work flow for performing incident investigations.

## How to choose the SIEM system, which really suits your organization's needs

Despite there are numerous SIEM systems available on the market, their functionality varies significantly. When choosing the solution, it's crucial to examine the conditions of implementation, usage and tasks, which the SIEM system is capable solving.

### Which aspects are recommended to consider:

#### 1. Speed of implementation and functionality, available "out-of-the-box"

14% of respondents, who took part in the survey by SearchInform stated potential labor costs for implementation, configuration and customization of a SIEM system as the prerequisites, why their companies didn't purchase a SIEM. However, there are solutions, which work out-of-the-box and don't require serious labor costs. The system should be deployed quickly, don't interrupt business processes or cause conflicts with IT infrastructure. Immediately upon the deployment SIEM should efficiently reveal software&hardware failures, targeted attacks, potentially dangerous users' actions.

#### 2. Simplicity of administration

Most part of respondents claim that it's a very complicated task for them to work with the SIEM system. That's why when choosing protective solution companies should assess the system's usability: IS and IT specialists with almost any experience should be able to work with the system. For example, to configure correlation rules in some SIEM class solutions, it's required to have some programming skills. In SearchInform SIEM this task was eased as much as possible: such rules can be configured in just a few clicks.

#### 3. Cost of SIEM system ownership and licensing model

SIEM system should offer the transparent system of licensing to make sure that customers can optimize budgets, allocated on protection of infrastructure. For example, if SIEM system licensing system is based on the number of hosts, customer will initially understand how much the deployment will cost.

It's also important to understand that implementation of SIEM system can be accompanied with some other ongoing expenditures, thus, it's also required to pay attention to the hardware requirements. In case the requirements are high, the server, for example, will be expensive and not any SME will be capable of purchasing such system.

## Why SIEM system is important for ensuring protection of small companies

Cyber threat landscapes evolve permanently and new risks occur regularly. These risks should be detected just in time. Detection of security events and timely response to them will reduce the threats, related to cyber attacks in small companies.

SIEM systems enable to combine functionality of a few tools: accumulate details on security events, ensure monitoring of infrastructure hardware, reveal incident in the link of events and notify IS officer.

The best way to ensure that the really solution suits your needs is to request a free trail. Thus, you'll obtain the first results before purchase of license, evaluate system's workability, reliability and capabilities.

### **About the Author**

Sergio Bertoni is the Leading Analyst at SearchInform which is the global risk management tools developer. Sergio has plenty of hands-on experience in the sphere of information security and has been contributing to the company's success for years. Sergio comments on different infosec topics, including information security trends and new methods of fraud (from simple phishing to deepfakes), provides advice on how to ensure security of communication channels and shares best practices for organizing information security protection of businesses. Sergio can be reached online at our company website <https://searchinform.com/>





## Securing AI Models - Risk and Best Practices

By Arun Mamgai, Cybersecurity and Data Science Specialist

Generative AI (Artificial Intelligence) has turned out to be a game changer after the introduction of ChatGPT, DALL-E, Bard, Gemini, GitHub Copilot etc. in 2022 and 2023 [1]. The majority of organizations are trying to figure out their AI strategy, but the LLM and its pipeline security, responsibility, and ethics can't be ignored. Artificial Intelligence has come a long way since its inception and now encompasses a broad spectrum of capabilities, ranging from natural language processing and computer vision to decision-making and problem-solving. It has become a powerful tool for user experience, business process development, and delivering a personalized solution. It's important that effective risk management strategies are implemented and evolved along with AI based solutions.

### A successful AI deployment requires 5 critical stages

1. Data Collection: The process of collecting and gathering raw data from multiple sources (this is done by integrating data sources with the target).



2. **Data Cleaning/Preparation:** The process of cleaning the data before using it for the AI pipeline (this is done by removing duplicates and excluding non-supported format, empty cells, or invalid entries that can lead to technical issues)
3. **Model Development:** The process of building data models by training a large set of data and analyzing certain patterns from the datasets and making predictions without additional human intervention. An iterative MDD (model driven development) is generally followed here.
4. **Model Serving:** The process of deploying machine learning (ML) models into the AI pipeline and integrating them into a business application. Mostly, these model functions, available as API, are deployed at a scale and can be used to perform tasks or make predictions based on real-time or batch data.
5. **Model Monitoring:** The process of assessing the performance and efficacy of the models against the live data and tracking metrics related to model quality (e.g., latency, memory, uptime, precision accuracy, etc.) along with data quality, model bias, prediction drift, and fairness.

While companies can use Gen AI solutions to expedite AI model development, it also poses enormous risks [3] to critical proprietary and business data. Data integrity and confidentiality are crucial and associated risk must be considered before approving new AI initiatives. The AI solutions can create a serious malware risk and impact if the right practices aren't followed. Following different types of attacks can compromise the integrity and reliability of the data models-

1. **Data Pipeline attack** - The entire pipeline of data collection to data training provides a large attack surface that can be easily exploited to obtain access, modify data, or introduce malicious inputs and cause privacy violations.
2. **Data Poisoning attack** - it involves inserting harmful or misleading data into the training datasets to intentionally influence or manipulate the model operation. It can also be done by modifying the existing dataset or deleting a portion of the dataset.
3. **Model Control attack** - Malware taking broader control of the decision-making process of the model resulting in erroneous outputs and significant impact to life and loss. This primarily occurs when externally accessible AI models are intentionally manipulated (like control of an automated vehicle).
4. **Model Evasion attack** - This attack results in a real-time data manipulation assault like changing the user inputs or device readings to modify the AI's responses or actions.
5. **Model Inversion attack** - It's a reverse engineering attack that can be used extensively to steal proprietary AI training data or personal information by exploiting the model output. Ex The inversion attack on a model predicting the cancer can be used to infer the person's medical history.
6. **Supply Chain attack** - Attackers hack third party software components (ex - open source third party libraries or assets) included in the model training, deployment or pipeline to insert malicious code and control the model behavior. Ex - Due to 1600 HuggingFace API leaked tokens [4], hackers were able to access 723 accounts of Organizations using HuggingFace API in their model development supply chain.
7. **Denial of Service attack (DoS)** - This kind of attack overloads AI systems with numerous requests or inputs, resulting in performance degradation or denial of service due to the resource downtime or exhaustion. Though it doesn't result in the theft or loss of critical information, it can cost the

victim a great deal of time and money to handle. Flooding services and Crashing services are two popular methods.

8. Prompt attack - These attacks include manipulative tactics where attackers deceive users into revealing confidential information by exploiting security weaknesses in language learning models used by AI-driven solutions like chatbots and virtual assistants. Ex - A security flaw found in Bing Chat [5] successfully tricked models into spilling its secrets.
9. Unfairness and Biased risks - AI systems may create unfair results or promote social prejudices, posing ethical, reputational, and legal issues. Given the fact AI solutions have potential to revolutionize many industries and improve people's lives in countless ways, this biases and unfairness may severely impact minorities, people of color, or users not well represented in the training dataset. Ex - A face detection solution may not recognize non-white faces if those users weren't added in the training set.

I would like to present the following recommendations to enhance the security of data models, MLOps Pipeline, and AI applications. The best practices will provide security guardrails and monitoring of assets while complying with regulations across respective geographies. AI models will be playing a critical role in delivering competitive advantage to organizations, therefore AI process integrity and confidentiality must be maintained by securing the most important assets and formulating the multi-prong approach to achieve AI security.

## Recommendations

1. Zero trust AI [6]: Access to model/data must be denied unless the user or application can prove their identity. Once identified, the user should be allowed to access only the required data for a limited period of time resulting in a least-privilege access, rigorous authentication, and continuous monitoring. "Trust, but verify" approach to AI results in models being continuously questioned and evaluated on a continuous basis - The Vault (secrets management), Identity and Access Management (IAM), and multi-factor authentication (MFA) plays a central role here.
2. Artificial Intelligence Bill of Material (AIBOM): It's similar to Software Bill of Material (SBOM) but prepared exclusively for the AI models, resulting in an enhanced transparency, reproducibility, accountability and Ethical AI considerations. The AIBOM [7] details the building components comprising an AI system's training data sources, pipelines, model development, training procedures, and operational performance to enable governance and assess dependencies. A suggested schema of AIBOM is referred [8] here.
3. Data Supply Chain - The access to clean, comprehensive, and enriched unstructured and structured data is the critical building block for AI models. The enterprise AI Pipeline and MLOps solutions supporting orchestration, CI/CD, ecosystem, monitoring, and observability are needed to automate and simplify machine learning (ML) workflows and deployments.
4. Regulations and Compliance - "Data is the new oil" and each country [9] is implementing its own rules to safeguard their interest. Organizations must adhere to AI data regulation and compliance enforced in the respective region. A "human centered design approach" Ex - H.R. 5628

(Algorithmic Accountability Act), H.R. 3220 Deep Fakes Accountability Act), European Union's Artificial Intelligence Act are few of the recent regulations.

5. Continuous Improvement and Enablement - With the continuous evolution of AI processes and models, the security of the AI ecosystem is a journey. A significant attempt must be made to frequently provide cybersecurity training to not only the data scientist and engineers but also developers and operations team building and supporting AI applications.
6. Balanced Scorecard based approach for CISOs - CISOs are now being invited to boardroom discussions to share their cybersecurity vision and align it with business priorities. A metrics driven based balanced scorecard solution ([How CISOs Can Take Advantage of the Balanced Scorecard Method](#)), provides a holistic approach to protect enterprise assets from malicious threats. A balanced scorecard-based cybersecurity strategy map can reduce business risks, increase productivity, enhance customer trust, and help enterprises grow without the fear of a data breach.

To summarize, it's critical to safeguard data and assets by compartmentalizing AI operations and adopting a metrics driven approach. A balance between harnessing AI's power and addressing its data security and ethical implications is crucial for a sustainable business solution.

#### References-

- [1] <https://blogs.nvidia.com/blog/ai-security-steps/>
- [2] <https://www.leewayhertz.com/ai-model-security/>
- [3] <https://www.hpe.com/in/en/what-is/ai-security.html>
- [4] <https://www.securityweek.com/major-organizations-using-hugging-face-ai-tools-put-at-risk-by-leaked-api-tokens/>
- [5] <https://www.wired.com/story/chatgpt-prompt-injection-attack-security/>
- [6] <https://www.computer.org/csdl/magazine/co/2022/02/09714079/1AZLiSNNvIk>
- [7] <https://snyk.io/series/ai-security/ai-bill-of-materials-aibom/>
- [8] <https://github.com/jasebell/ai-bill-of-materials>
- [9] <https://www.techtarget.com/searchenterpriseai/feature/AI-regulation-What-businesses-need-to-know>

## About the Author

Arun Mamgai has more than 18 years of experience in cloud-native cybersecurity, application modernization, open-source secure supply chains, AI/machine learning (ML), and digital transformation (including balanced scorecards, data management, and digital marketing) and has worked with Fortune 1000 customers across industries. He has published many articles highlighting the use of generative AI for cybersecurity and securely developing modern cloud applications. He has been invited to speak at leading schools on topics such as digital transformation and application-level attacks in connected vehicles and has been a judge for one of the most prestigious awards in the technology sector. He has also mentored multiple start-ups and actively engages with a nonprofit institution that enables middle school girls to become future technology leaders.



Arun can be reached online at [arun.m.eb1@gmail.com](mailto:arun.m.eb1@gmail.com) or <https://www.linkedin.com/in/arun-mamgai-10656a4/>



## Supply Chains Make Insider Threat Defense More Complex

By Zac Amos, Features Editor, ReHack

Regular insider threats are bad enough — conventional security tools don't detect them, they know where it'll hurt to hit, and management doesn't suspect them. Unfortunately, insider supply chain threats are often worse. What can business leaders do to protect their organizations?

### Why Companies Must Be Vigilant Against Insider Threats

Insider threats can be anyone with trust, access, knowledge or leverage. When people think of them, figures like a disgruntled former employee with a grudge or a spiteful colleague recently snubbed for a promotion often come to mind. However, more often than not, they are simply employees or contractors who make costly mistakes.

Malicious insiders act intentionally, often seeking to cause damage or gain something. They're often resentful or feel overlooked by their employer, prompting them to commit acts like espionage, sabotage or corruption. For them, working with a competitor or cybercriminal isn't out of the question



Negligent insiders generally act unintentionally, driven by carelessness or apathy. However, they are still responsible for their actions. Inadvertent insiders accidentally cause damage, whether by mistyping an email address, becoming a victim of phishing or using a device that behaves unexpectedly.

To be clear, an insider's intentions don't matter much when the result is the same. The distinction exists simply to guide disciplinary action and post-incident analysis. That may be why [30% of chief information security officers](#) agreed this threat was their organization's most significant cybersecurity risk in 2023, according to one global survey.

Unlike cybercriminals or disreputable competitors, internal threats don't stand out. Since they have legitimate access, conventional monitoring tools and security measures won't flag their activity. Moreover, since they personally know their colleagues, they often don't seem immediately suspicious — even if indicators suggest they are.

Crucially, insider supply chain threats pose an even more significant danger because they have disparate data systems, operate with less oversight and have different security protocols. Even under contract, these vendors may feel they can get away with taking shortcuts or being inattentive of cybersecurity — and businesses will likely be blissfully unaware until it's too late.

## Strategies to Defend Against Insider Supply Chain Threats

Several strategies to defend against insider supply chain threats exist.

### 1. Monitor Third-Party Vendors

Monitoring is critical to mitigating insider threats. After all, information technology (IT) teams can't address what they don't see. Recently, real-time visibility has become fundamental for developing a resilient supply chain. In fact, [most companies are seeking to invest](#) in such solutions within the next few years.

Decision-makers should consider this surge in interest a sign to begin monitoring their supply-chain vendors. Whether they decide on periodic audits, sentiment analysis software or radiofrequency identification tag tracking, increased oversight will help them identify and eliminate all but the most sophisticated insiders.

### 2. Develop a Mitigation Budget

Even though negligent insiders [cause 60% of data breaches](#), only 8% of a company's cybersecurity budget goes toward managing them. Developing a mitigation budget for this issue ensures the IT team has enough resources to address vendors in addition to their regular responsibilities.

### 3. Conduct Risk Assessments

How do senior executives know which third party to trust? Conducting risk assessments for supply-chain vendors removes the guesswork. It determines their likelihood of employing an individual who is a malicious, negligent or accidental internal threat. This method is simple and effective, making it ideal for time-sensitive situations or IT teams with large workloads.

Notably, many companies don't utilize this method. In one recent survey of over 2,500 companies, [29% of senior executives](#) reportedly don't assign a risk score to each vendor. An additional 13% admitted they don't use any third-party risk management system, highlighting the opportunity for widespread adoption.

Decision-makers should look to guidance like the International Organization for Standardization 28000 to learn how to reduce security risks or the National Institute for Standards and Technology SP 800-161 to manage supply chain threats. These standards can help them recognize what to prioritize and how to proceed.

## Best Practices for Handling Third-Party Insider Threats

A zero-trust architecture is quickly becoming fundamental to cybersecurity. Leveraging it can minimize companies' insider threat risk and reduce the scope of potential damage. Giving supply chain vendors the minimum amount of access needed to do their jobs prevents them from having opportunities to cause problems.

Another best practice is to leverage encryption. While typical techniques minimize the damage negligent and inadvertent insiders can do, format-preserving encryption (FPE) prevents malicious actions. Its ciphertext is the same form and length as the plaintext, allowing vendors to perform operations on data without reading it or possessing a decryption key.

Decision-makers should also consider developing an incident response strategy to address internal threats as soon as the IT team detects them, minimizing the scope of damage. Outlining the grounds, limitations and implications of such action in contracts would help them escalate as necessary while giving vendors a reason to comply.

## Insider Threat Mitigation Is an Ongoing Process

Human error and disgruntled employees are a natural part of doing business. In other words, insider threats will always exist, no matter how often the IT team addresses them. While this fact may seem discouraging, it is a reminder to stay vigilant — threat mitigation is an ongoing process that evolves with time.

### 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](#).





## Giving a Voice to Future Generations of Female Cybersecurity Leaders

**Bridging the Gap: Elevating Future Generations of Female Cybersecurity Leaders**

**By Nazy Fouladirad, COO of Tevora**

While most organizations today remain aware of the ongoing cybersecurity threats, there is a constant struggle to keep pace with them. Much of this has to do with a lack of resources and talent available in cybersecurity as a whole, with many organizations forced to take shortcuts in their security planning.

As alarming as this cybersecurity talent gap is, there is another noticeable gap when it comes to demographics in these types of roles. Today, women still only represent around 25% of all current roles in cybersecurity.

This imbalance of female and male workers in cybersecurity highlights the need for organizations to be more aware of their role in helping to avoid gender bias and play a part in right-sizing the differential.

## Why Diversity in Cybersecurity Needs More Attention

Diversity is an important topic of conversation in all industries, especially in highly technical areas like cybersecurity. Because despite increases in women educated in these technical areas, employment numbers are not changing over time. Below are some of the current challenges the industry is facing:

### Unapproachable Role Descriptions

Although hiring managers may have a specific type of person in mind when drafting their job descriptions, they may often underestimate the intimidation factor of the type of verbiage they use.

Many cybersecurity role descriptions today can be incredibly overwhelming, filled with a never-ending list of qualifications or next-to-impossible combinations of technical and soft skills. This can often discourage many people - especially women - from putting their hat in the ring. In fact, studies have shown that women are more likely than men to self-select themselves out of a job application based on the job description.

### Limited Access to Higher Caliber Positions

Another major challenge in cybersecurity is the apparent lack of advancement opportunities, especially for female employees. Regardless of qualifications, women can often find their career progression unintentionally throttled by factors such as a lack of diverse mentors and career champions.

This throttling - whether done consciously or not - has had major ripple effects on the number of women in higher-caliber positions. The lack of representation in this area could be another reason why females have found the cybersecurity industry as a whole to be outside of their best interests.

## How Women Are Contributing to Improved Cybersecurity Effectiveness

Even though the cybersecurity industry is still male-dominated, the current and ongoing positive impact that females are introducing to the sector is hard to ignore.

### Broader Perspectives and New Approaches to Problem Solving

The most impactful cybersecurity initiatives are born out of a blend of creativity and strategic planning. Having a more diverse workforce contributes to a wider range of perspectives and ideas to spark creative thinking.

Women bring a number of unique strengths to the table when it comes to offering innovative problem-solving and collaboration in group settings.

By encouraging and contributing individual experiences and acquired knowledge, women can help to facilitate a much more holistic security approach. This can be done by adopting more nuanced approaches to risk management, including penetration testing and security audits, as well as being an active voice when it comes to raising important questions and thinking outside of the box.

## Proven Leadership Capabilities

Successfully responding to security incidents requires leadership teams who can handle sustained pressure while making calculated decisions. Even though women as a group have proven to bring valuable leadership traits in professional settings, they still continue to be underrepresented in these critical security leadership roles

Various studies have demonstrated that female leaders are often viewed as more trustworthy in times of organizational crisis and when building more resilient teams. These skill sets can easily be applied to a number of important organizational objectives, including meeting rigorous compliance standards or certifications such as [HITRUST](#) or navigating various other industry regulations successfully.

## Wide Range of Skill Sets

Women often bring a valuable mix of both technical and soft skills when entering the cybersecurity field. This includes excellent listening skills, problem-solving, and the ability to manage various projects successfully. While these abilities are unfortunately underutilized in certain roles, this doesn't present an opportunity for organizations to start getting more out of the security roles they put in place.

Having a wide range of skills at your disposal can be a great asset when executing important initiatives like [vendor risk management](#) and ensuring security compliance. Having more employees who can clearly communicate critical gaps in security protocols and work with outside parties to stay in alignment with regulatory changes can be a huge asset for any organization.

### Giving Future Female Cybersecurity Leaders the Platform They Deserve

Despite long-standing biases, organizations must work together to help improve the diversity in cybersecurity leadership roles. By providing female professionals with more opportunities, resources, and support, we can create a more inclusive and equitable environment for everyone while furthering advancements in all areas of cybersecurity.



## About the Author

Nazy Fouladirad is President and COO of [Tevora](https://www.tevora.com/), a global leading cybersecurity consultancy. She has dedicated her career to creating a more secure business and online environment for organizations across the country and world. She is passionate about serving her community and acts as a board member for a local nonprofit organization. Nazy can be reached online at [LinkedIn](#), and at our company website: <https://www.tevora.com/>



Email: [info@tevora.com](mailto:info@tevora.com)

Web: <https://www.tevora.com/>

Phone# 833.292.1609



## The Evolution of Cloud Strategy: Beyond "Cloud First"

By Tanvir Khan, Executive Vice President of Cloud, Infrastructure, Digital Workplace Services and Platforms, NTT DATA

In the rapidly evolving digital landscape, the mantra "Cloud First" is becoming a relic of the past. Today, organizations are recognizing that mere digital transformation does not automatically translate into business value. The real challenge—and opportunity—lies in crafting a Comprehensive Modern Infrastructure and platform ecosystem that creates a journey to simplification and a seamless infrastructure ecosystem which enables a future proof and scalable approach to modern technologies while providing alignment and growth of the strategic business goals and desired outcomes. The key elements of this approach are: Hybrid Cloud and Infrastructure, multi-purpose adoption of AI, agile and proactive enterprise Security and the governance to manage open source solutions.

## The New Paradigm: Comprehensive Cloud Collective

Imagine the seamless, intuitive experience of using an iPhone. Now, envision that same level of simplicity and efficiency in enterprise IT systems. This is the goal of a successful hybrid cloud and infrastructure strategy. It's not just about moving to the cloud; it's about optimizing the hybrid cloud environment to achieve economic value and leveraging emerging cloud technologies to not just stay ahead of the curve but to enable growth, innovation and disruption of the business. These outcomes can easily be measurable and quantifiable.

Despite the rush to adopt cloud solutions, many companies have yet to unlock the true economic value of the cloud. This shortfall is often due to a lack of an agile, comprehensive strategy that goes beyond mere adoption.

**Five to Thrive:** A robust hybrid cloud strategy should encompass several key areas:

1. **Core Operations Digitization:** Transforming traditional business operations into digital, cloud-enabled solutions to enhance efficiency and scalability.
2. **IT Resilience Improvement:** Building robust systems that are not only secure but also resilient to changes and challenges in the business environment.
3. **IT Cost Optimization:** Leveraging cloud solutions to reduce IT and business operational costs while increasing overall efficiency and simplification of core IT
4. **Accelerated Product Development and Hyper scalability:** Using the cloud to speed up product development cycles and scale operations rapidly as needed.
5. **Innovation-Driven Growth:** Harnessing the cloud to foster innovation, thereby driving business growth and maintaining competitive advantage.

## Heavy Fuel of Innovation:

The business focus of a hybrid cloud and infrastructure strategy should be to fuel innovation, which impacts several critical areas as follows:

- **Digital Experience:** Enhancing customer and employee interactions through superior digital touchpoints.
- **Industry Cloud + Marketplace:** Developing specialized cloud solutions tailored to specific industry needs, complemented by a vibrant marketplace of services and applications.
- **Cloud Applications and Modernization:** Updating and modernizing existing applications to fully exploit cloud capabilities.
- **Cloud Data and AI:** Leveraging data analytics and artificial intelligence to extract actionable insights from large datasets stored in the cloud.

On the technology front, the focus shifts to driving optimization, agility, and security through enhanced platforms, networks, and infrastructure. This involves not only adopting cutting-edge technologies but also ensuring that they are seamlessly integrated and securely managed to support overall business objectives.

## Beyond Adoption: Strategic Implementation

Implementing a hybrid cloud and infrastructure strategy involves more than just technology deployment; it requires a holistic approach that encompasses process innovation and rejuvenation. This strategic implementation ensures that the move to the cloud is not just a checkbox exercise but a transformational process that aligns with long-term business goals.

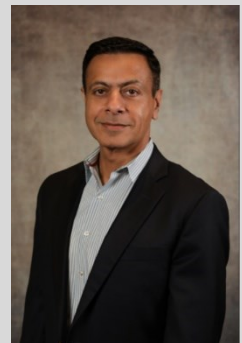
## Conclusion

As we move forward, the narrative is no longer about being "Cloud First" but about being "Cloud Smart." Organizations need to develop a nuanced understanding of how cloud technologies can be harnessed to drive not just operational efficiencies but also substantial business outcomes. The focus must be on building a resilient, optimized, and innovative IT infrastructure ecosystem that not only supports but also drives business growth in the digital age.

In conclusion, the shift from "Cloud First" to a more comprehensive, outcome-focused hybrid cloud and infrastructure strategy represents a mature approach to IT investment and business growth. It emphasizes the importance of strategic alignment between IT capabilities and business objectives, ensuring that enterprises not only survive but thrive in the competitive digital marketplace.

### About the Author

Tanvir Khan is the Executive Vice President of Cloud, Infrastructure, Digital Workplace Services and Platforms at NTT DATA. With over 25 years of experience in the IT industry, he is a recognized technology vanguard who specializes in the areas of digital transformation, associated core technologies and value realization. Aside from being a seasoned IT practitioner, he holds an impressive track record with five patents and four pending patents in AI and automation. Tanvir can be reached online on his [LinkedIn](#) and at our company website <https://www.nttdata.com/global/en/>







## The Last Stop: Protecting an NHL Franchise Against Cyberattacks

By Marc Laliberte, Director of Security Operations at WatchGuard

For the Seattle Kraken, the National Hockey League's 32nd franchise, maintaining a strong defense off the ice—one that keeps cyber attackers in the penalty box—is just as important as its defense on the ice.

Here's what it's like behind the scenes defending a widely recognized brand.

The Kraken IT and security team is charged with protecting the organization's digital assets – including sensitive team and fan data and proprietary information. The six-person team is responsible for managing and protecting more than 260 individuals and their devices at home and on the road as well as the servers and private networks that support the team's operations. In addition, the Kraken Community Iceplex, which houses the team's offices and IT equipment, is open to the public, offering a free Wi-Fi network for up to 1000 visitors per day. That traffic passes over the Kraken's firewalls.

The Kraken organization has built a reputation in the NHL for how it leverages cutting-edge technology across player, employee and fan experiences. The IT staff plays a key role in enabling technological innovation across the franchise, which includes supporting a software development team that builds and



maintains a fan-facing app with player stats and other team information and software for the team's coaching and player development.

From a cybersecurity standpoint, the Kraken have some unique challenges. Like any NHL franchise, team staff are on the road with players for half the season. Team scouts travel around the world year-round, including to places where the cybersecurity threat environment creates added risks. The daily threats faced by the team—from phishing, ransomware attempts and identity access management and more—create a need for strong network and endpoint security as well as correlated threat detection and response.

To secure this expansive attack surface, the Kraken IT team identified the need for a multilayered, unified security platform that significantly reduces complexity for users while still providing enterprise-grade protection. Most importantly, they needed a solution that would enable the team to quickly recognize and address potential security issues.

While the IT team normally holds off on major technology initiatives until the off-season, they decided to switch over to the WatchGuard Unified Security platform during the first half of the 2023-2024 campaign. That created a sense of urgency to make the transition happen as quickly and seamlessly as possible. With the clock ticking, the Kraken team were able to deploy the WatchGuard platform in less than 12 hours.

The first phase of the transition included the deployment of WatchGuard Firebox firewalls, anti-virus and patch management, followed by EPDR endpoint security and WatchGuard ThreatSync extended detection and response (XDR), which integrates data from firewalls and endpoints to surface potential threats. According to Ryan Willgues, cybersecurity engineer at the Seattle Kraken, WatchGuard's focus on providing a single, integrated management interface centered on ease of use has helped streamline the team's daily threat monitoring and cybersecurity workflow. "Now, we not only have comprehensive visibility across our network, but ThreatSync's AI filters out low-level threats so it's easy to see what I need to prioritize," said Willgues.

With the current season in the books, the Kraken IT team plans to integrate additional components of WatchGuard's Unified Security Platform, particularly around identity and access management. That includes single sign-on and AuthPoint Total Identity Security, which offers multi-factor authentication, password management, and dark web monitoring for compromised credentials.

For the Kraken, WatchGuard plays a critical role helping the team to maintain vigilance in monitoring for and defending against attacks amid a continually evolving and increasingly volatile threat landscape. With a comprehensive, multilayered security solution designed for ease-of-use, the Kraken IT team has the power to put cyberattackers in the penalty box and ice threats.

## About The Author

Marc Laliberte is the Director of Security Operations at WatchGuard Technologies. Marc joined the WatchGuard team in 2012 and has spent much of the last decade helping shape WatchGuard's internal security maturation from various roles and responsibilities. Marc's responsibilities include leading WatchGuard's security operations center as well as the WatchGuard Threat Lab, a research-focused thought leadership team that identifies and reports on modern information security trends. With regular speaking appearances and contributions to online IT publications, Marc is a leading thought leader providing security guidance to all levels of IT personnel.





# EVENTS





# **black hat**<sup>®</sup> USA 2024

**AUGUST 3-8, 2024**  
MANDALAY BAY/LAS VEGAS

5<sup>TH</sup> EDITION

 **MARRIOTT**  
ARAVALLI RESORT

**23-25** AUG 2024 



**ESCON**  

ENTERPRISE SECURITY CONNECT

RESEARCH REPORT | HANDBOOK | CONFERENCE | AWARDS

# A PREMIERE SOUTH ASIA CISO PROGRAM IN THE LAP OF ARAVALLI



Reach 500+ CISOs  
& Security Practitioners



Showcase  
Cutting-Edge Solutions



Enhance  
Brand Visibility



VIP Networking  
Opportunities



Engage with  
Industry Leaders

**KNOW MORE**



## CONTACT INFORMATION

Email: [msharma@strategink.com](mailto:msharma@strategink.com)

Visit: <https://www.strategink.com/escon/2024>

TELECAST PARTNER







# THE EMERGENCY TECH SHOW

18-19 SEPTEMBER 2024 | NEC BIRMINGHAM

**THE HOME OF  
TECHNOLOGY  
INNOVATION FOR  
THE EMERGENCY  
SERVICES**



**150+**  
EXHIBITORS



**8,000+**  
VISITORS



**10,000+**  
PRODUCTS AND SOLUTIONS



**CPD**  
ACCREDITED CONTENT

CO-LOCATED WITH

**THE EMERGENCY  
SERVICES SHOW**

Register for your FREE pass  
[www.emergencytechshow.com](http://www.emergencytechshow.com)





**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

Join us in shaping the future of ITS and Smart Mobility at the ITS World Congress in Dubai! 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





# ADAS 2024

Asian Defense and Security Exhibition



25-27 September 2024  
World Trade Center  
Metro Manila, Philippines  
adas.ph

# BUILDING ON A DECADE OF DEFENSE CAPABILITY

Register Your  
Interest to Exhibit  
or Visit at  
[www.adas.ph](http://www.adas.ph)



Officially Supported by:







# CYBER DEFENSE TV

## INFOSEC KNOWLEDGE IS POWER

[CyberDefense.TV](https://www.cyberdefense.tv) now has 200 hotseat interviews and growing...

Market leaders, innovators, CEO hot seat interviews and much more.

A division of Cyber Defense Media Group and sister to Cyber Defense Magazine.

### The Interviews

These anticipated **"CEO Hotseat"** Interviews will feature a C-level executive from the hottest Infosec companies being interviewed by **Gary Miliefsky**. Gary is an internationally-recognized speaker and Infosec expert and will make the interviews lively, informative, and highly favorable to the interviewees.

CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved. [www.cyberdefense.tv](http://www.cyberdefense.tv)

## Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. [Click here](#) to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

[By signing up, you'll always be in the loop with CDM.](#)

---

Copyright (C) 2024, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (STEVEN G. SAMUELS LLC. d/b/a) 276 Fifth Avenue, Suite 704, New York, NY 10001, Toll Free (USA): 1-833-844-9468 d/b/a CyberDefenseAwards.com, CyberDefenseConferences.com, CyberDefenseMagazine.com, CyberDefenseNewswire.com, CyberDefenseProfessionals.com, CyberDefenseRadio.com, and CyberDefenseTV.com, is a Limited Liability Corporation (LLC) originally incorporated in the United States of America. Our Tax ID (EIN) is: 45-4188465, Cyber Defense Magazine® is a registered trademark of Cyber Defense Media Group. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide. [marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)

All rights reserved worldwide. Copyright © 2024, Cyber Defense Magazine. All rights reserved. No part of this newsletter may be used or reproduced by any means, graphic, electronic, or mechanical, including photocopying, recording, taping or by any information storage retrieval system without the written permission of the publisher except in the case of brief quotations embodied in critical articles and reviews. Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them. Send us great content and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at [marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)

### **Cyber Defense Magazine**

276 Fifth Avenue, Suite 704, New York, NY 1000

EIN: 454-18-8465, DUNS# 078358935.

All rights reserved worldwide.

[marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)

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

### **NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)**

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 08/01/2024



Follow f in w Saturday, June 29, 2019 [Cyber Defense Magazine Staff](#) @Logout

Call us Toll Free (USA): 1-833-844-9468 International: +1-603-280-4451 M-F 9am to 6pm EST

**CYBER DEFENSE MAGAZINE** Over 90% of Breaches Happen Behind the Corporate Firewall  
**INSIDER THREAT MITIGATION TRAINING**  
[Learn More](#)

HOME MAGAZINES NEWS RESEARCH PARTNERS EVENTS AWARDS PLATFORMS CONTACT HELP

THINKING NOW Rootkit Redux

**5 Things to Consider while using Unsecured Open Wi-Fi**  
News Team - June 29, 2019

**Insider Threat Defense Mitigation Training this Summer**  
News Team - June 29, 2019

**Rootkit Redux**  
News Team - June 29, 2019

**KRACK is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg**  
News Team - June 29, 2019

**EDITOR'S PICK**

**5 Things to Consider while using Unsecured Open Wi-Fi**  
News Team - June 29, 2019

BY MOHIT SHARMA, CONTENT WRITER, MALWAREFOX Open Wi-Fi networks are a dream for all of us...

**Insider Threat Defense Mitigation Training this Summer**  
Cyber Defense Magazine Staff - June 29, 2019

This should be the summer of vigilance - involves training, refreshing and budgeting for increased...

**Rootkit Redux**  
News Team - June 29, 2019

REVISITING A PRIOR ISSUE by CDP, Cybersecurity Lab Engineer in honor of Mr. Robot, the mach-evalued...

**SIGN UP FOR FREE MONTHLY e-MAGAZINES**

**SUBSCRIBE**

**Remediant**  
Learn How You can Bring Agentless Privileged Access Management to Your Organization  
**JUST-IN-TIME**  
Details  
Remediant.com

**LATEST NEWS**

**5 Things to Consider while using Unsecured Open Wi-Fi**  
News Team - June 29, 2019

**Insider Threat Defense Mitigation Training this Summer**  
Cyber Defense Magazine Staff - June 29, 2019

**Rootkit Redux**  
June 29, 2019

**KRACK is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg**  
June 29, 2019

**2019 PRINT EDITION**

**CDM eMAGAZINE**

Books by our Publisher: [Amazon.com: CRYPTOCONOMY®, 2nd Edition: Bitcoins, Blockchains & Bad Guys eBook](https://www.amazon.com/dp/B078383838) : Miliefsky, Gary: [Kindle Store](https://www.amazon.com/dp/B078383838) (with others coming soon...)

*12 Years in The Making...*

*Thank You to our Loyal Subscribers!*

We've Completely Rebuilt 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 up and running as an array of live mirror sites. We successfully launched <https://cyberdefenseconferences.com/> and our new platform <https://cyberdefensewire.com/>



# 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**





# CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER



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

[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)





**\* with help from writers  
and friends all over the Globe.**