CYBER DEFENSE MAGAZINE

eMAGAZINE

MARCH 2025



In This Edition

The Cyber Insurance Conundrum

How Ghostgpt Is Empowering Cybercrime in The Age Of AI

How Cybersecurity is Evolving in 2025 to Tackle New Threats

...and much more...

MORE INSIDE!

CONTENTS

Welcome to CDM's March 2025 Issue ---------- *8*

The Cyber Insurance Conundrum ---------- *40*

By Denny LeCompte, CEO, Portnox

How Ghostgpt Is Empowering Cybercrime in The Age Of AI ---------- *44*

By Eleanor Hecks, Editor-in-Chief, Designerly Magazine

How Cybersecurity is Evolving in 2025 to Tackle New Threats ---------- *48*

By Vaibhav Dutta, Associate Vice President and Global Head – Cybersecurity Products & Services, Tata Communications

Preparing For The AI-Generated Cyber Threats Of 2025 ---------- *51*

By Eran Orzel, CEO of CyTwist

AI Addressing New Need to Secure Data from The Inside Out ---------- *55*

By Rob Sims, CTO and Co-Founder, Alchemi Data Management

AI In Software Development: Balancing Innovation And Security In An Era Of Lowered Barriers ---------- *59*

By Michael Burch, Director of Application Security, Security Journey

AI-Powered Cyber Attacks and Data Privacy in The Age of Big Data ---------- *62*

By Balasubramani Murugesan, Director of Engineering, Digit7 LLC

AI-Powered Testing: Innovation, Risks, and What Comes Next ---------- *66*

By Jason Kichen, CISO, Tricentis

Can Standards Deal a Deathly Blow Against Deepfakes? ---------- *69*

By Alessandra Sala, Chair of Multimedia Authenticity Collaboration, International Electrotechnical Commission and Sr. Director of AI and Data Science at Shutterstock

How Businesses Can Turn the Expanding Attack Surface into an Opportunity ---------- *73*

By Norman Menz, CEO of Cybersecurity SaaS platform Flare.

Key Cybersecurity Themes for 2025 ---------- *77*

By Rohit Dhamankar, Vice President of Product Strategy at Fortra's Alert Logic

Unpacking Disinformation In The 2024 US Presidential Election ---------- *81*

By Hannah Baumgaertner, Head of Research at Silobreaker

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Rethinking SAP Security Without Maintenance Contracts ---------- 85

By Ken Conz, Director of Technical Operations, Spinnaker Support

Is Someone Lurking In The Background Waiting To Impersonate You? ---------- 89

By Dave Smolensky, Founder and COO, Resolute Strategic Services

The CMMC Compliance Journey ---------- 92

By Jason Miller, Founder & CEO, BitLyft

Why Eliminating the Cyber Safety Review Board Weakens Critical Infrastructure And Cyber Resilience ---------- 95

By Ramkumar Sundarakalatharan, CEO, Zerberus Technologies

Effective Cyber Drills Must Mirror the Realities of The Battlefield ----------100

By Dr. Oleksii Baranovskyi, a certified cybersecurity expert (CISSP, CISM, CCISO), trainer for TRYZUB cyber drills, CYBER RANGES

How AI is Transforming the Fight Against Data Breaches ----------104

By Nivedita Kumari, Data Analytics Customer Engineer, Google

Advances In Quantum Computing Signal an Urgent Post-Quantum Cryptography (PQC) Imperative for Enterprises ----------108

By Anurag Lal, President & Chief Executive Officer, NetSfere

Navigating NIS2 Compliance: Elevating Cyber Resilience Through Network Visibility -------112

By Matt Ellison, Technical Director for EMEA at Corelight

Generative AI In Business: Managing Risks in The Race for Innovation ----------115

By Brad LaPorte, CMO, Morphisec

Best Laptop for Cybersecurity: Top Picks for Ethical Hackers & Security Professionals-----120

By John Doe, Cybersecurity Analyst, X-PHY

Cybersecurity Trends for 2025 ----------124

By Ben Hunter III, Principal, UHY

Evolution Of Cyber Threats: Why Attack Surface Management Is Critical Today ----------128

By Ankit Sharma, Senior Director and Head - Solutions Engineering, Cyble

How Digital Signatures Provide The Necessary Safeguards To Restore Trust In The Manufacturing Process----------132

By Mohit Kumar, Vice President Product Management, GMO GlobalSign

How Will the Splinternet Impact Cybersecurity? ----------135

By Zac Amos, Features Editor, ReHack

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

In The Shifting Threat Landscape, Organizations Need to Ditch Third-Party Agents And Embrace Zero Trust Security ----------138

By Amol Dalvi, Vice President, Product, Nerdio

Protectors of the Modern World: Defending Against Shadow ML and Agentic AI ----------141

By Eyal Dyment, Vice President of Security Products at JFrog

Machine Learning Meets Endpoint Security: Advancements in Predictive Threat Detection 145

By Unnati Ghosh, My Digital Marketing Manager, HCLSoftware

The Future Of Fiber Optic Sensors: Breakthroughs Shaping The Next Generation ----------150

By Amit Mohite, Media Relations Team, Transparency Market Research

Navigating Department of Defense CMMC Compliance: A Guide For Subcontractors -------155

By Matt Gilbert, Principal, Baker Tilly

1 in 5 Emails Could Be Scams: Why Businesses Must Prioritize Email Security ----------161

By Craig McCurdy. Chief Information Security Consultant, Sabre Secure

Online Account Security ----------165

By Milica D. Djekic

Operational Resilience ----------168

By Renato Lima, Eletrobras

Overcoming The Skills Shortage in Cybersecurity Through A 'Trusted' Approach. ----------173

By Thorsten Stremlau of the Trusted Computing Group

Can AI Be Your Trusted Partner in Securing Your Extended Business Ecosystem?----------177

By Phani Dasari, Chief Information Security Officer at HGS

The Role of AI In Cybersecurity: Enhancing Defense And Adapting To Threats ----------182

By Randy Hall, CEO, Securafy Inc

Securing The AI Frontier: Addressing Emerging Threats In AI-Powered Software Development ----------186

By Matt Tesauro, Chief Technology Officer, DefectDojo

Smart Meter Security: Best Practices and Emerging Regulations----------189

By Jose Sanchez - Senior Director Product Management, IoT Connectivity & Services, Telit Cinterion

The Art of Delegation in a Digital Age: Empowering Teams, Not Just Offloading Tasks -------193

By Josh Breaker-Rolfe, Content writer at Bora

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The Growing Cost of Non-Compliance and the Need for Security-First Solutions----------*197*

By Puneet Kohli, President of Application Modernization at Rocket Software

The Invisible Fingerprint in Code ----------*201*

By Felix Mächtle, Researcher at the University of Lübeck, Germany

Threat Research is Broken – Security Teams Need Automation Now----------*204*

By Emmanuel Joshua, Software Development Engineer (DefSec) at Amazon

Training Skillset Transfer----------*209*

By Milica D. Djekic

Trusted & Resilient Saas Data Is Essential for Successful Agentic AI Within Government Agencies ----------*213*

By Dr. Eoghan Casey, Business Consultant, Salesforce

Unified Endpoint Management: One Tool to Rule All----------*216*

By Unnati Ghosh, Digital Marketing Manager, HCLSoftware

Why Securing Prompts Will Never Be Enough: The GitHub Copilot Case----------*221*

By Oren Saban, Director of Product Management, Apex Security

Understanding the 2025 HIPAA Security Rule Updates: A Comprehensive Analysis of Healthcare Cybersecurity Enhancements ----------*225*

By James Winebrenner, CEO, Elisity

The Looming Shadow Over AI: Securing the Future of Large Language Models ----------*230*

By Hrishitva Patel, MS/MBA, University of Texas at San Antonio

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

@MILIEFSKY

From the

Publisher…



We are pleased to remind our readers that Cyber Defense Magazine and Cyber Defense Media Group are again partnering in the RSA® Conference 2025. This year's theme is "Many Voices. One Community." You can see more at https://www.rsaconference.com/events/2025-usa .

We repeat this message from the RSA announcement: "At RSAC 2025, you're not just attending a conference—you're stepping into a vibrant, thriving community of thinkers, innovators, and achievers. Though we come from different corners of the cybersecurity world, we are united by a common mission: to foresee risks, counter threats, and embrace the challenges ahead. Together, we shape the future of security. Together, we shine as one."

We would like to draw your attention to the publication of my new book, The AI Singularity: When Machines Dream of Dominion, available at Amazon

"In the calculus of evolution, one question remains: Shall we be the architects of our transcendence, or the fossils of a passing age?"

For Infosec Solution Providers: Entering the Global InfoSec Awards for 2025 is your chance to showcase your cybersecurity innovation to the world. These awards highlight cutting-edge solutions and offer industry validation, setting you apart from the competition. Winning brings credibility, media exposure, and new opportunities. Don't stay in the shadows — let the world see how you're leading the charge in cybersecurity.

https://cyberdefenseawards.com/

Stay vigilant. Stay secure. And remember — cybercriminals never sleep, so neither can your cybersecurity strategy.

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

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

@CYBERDEFENSEMAG

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

ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: 1-833-844-9468
International: +1-603-280-4451

https://www.cyberdefensemagazine.com

Copyright © 2025, 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/



13 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

MAGAZINE TV RADIO AWARDS

PROFESSIONALS WIRE WEBINARS

CYBERDEFENSECONFERENCES

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Welcome to CDM's March 2025 Issue

From the Editor-in-Chief

In this March 2025 issue of Cyber Defense Magazine, we note a new focus on the fastest-developing phenomenon in cybersecurity: Artificial Intelligence. There are so many facets to this potential gem (or threat) that it's a challenge to keep up with the implications of such fast development.

The articles have come from many sources, and cover highly technical to general interest readers. That's part of our own focus on bringing actionable information to the broadest spectrum of our audience. We strive to bridge the gap between cybersecurity professionals and the broader group needing to understand and act on these developments.

Beyond AI, we cover many other aspects of cybersecurity, such as quantum computing, supply chain issues, and ransomware developments. Our featured areas of concern include such critical infrastructure sectors as finance, health care, automotive applications, and defense endeavors. In seeking to meet the needs of our growing audience, we are also dedicated to expanding our coverage for greater positive results across the board.

We continue our mission to provide the best and most actionable set of resources for the CISO community and all users of digital technology in publishing Cyber Defense Magazine and broadening the activities of Cyber Defense Media Group.

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

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.


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

Shadow IT May Leave You at Risk.



Unauthorized or unknown internet-facing assets in your network can expose sensitive defense information to our adversaries.

NSA's no-cost cybersecurity services can help you find and protect your assets to better secure your network.

GET STARTED TODAY AT

nsa.gov/ccc

NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA

CYBERSECURITY COLLABORATION CENTER



UNKNOWN
CYBER

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

Not by us. We detect the unknowns.

www.unknowncyber.com

zivver

Secure email.
Effortless compliance.

Protect your sensitive data with advanced email encryption

- Sensitive data identification
- Large file transfer
- Human error prevention

HIPAA COMPLIANT

Gramm-Leach-Bliley Act COMPLIANT

www.zivver.com

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations



Information security, cybersecurity and privacy protection for the legal profession

Download White Paper

Download our white paper to understand how the legal profession is under attack and how ISO/IEC 27001 can help mitigate the risk.

The legal profession depends on the flow of highly sensitive information, such as client data, personally identifiable information (PII), case details, sensitive contracts, financial records and intellectual property. This white paper reviews how the value of this information makes the legal profession increasingly at risk of cyberattack and how ISO/IEC 27001 can provide the framework to keep information secure, prevent unauthorized access and mitigate the risk should a breach occur.

SGS

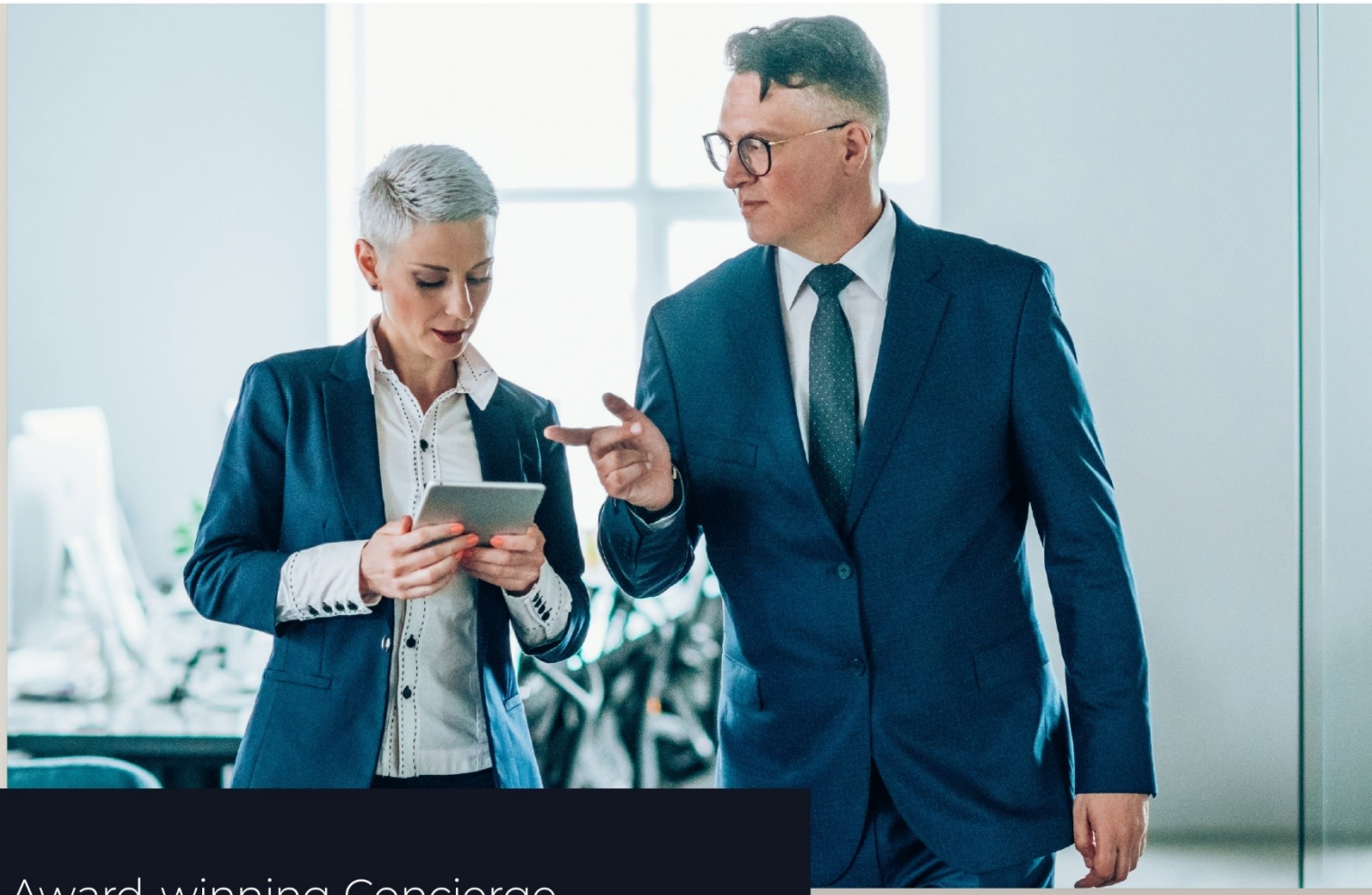
When you need to be sure

sgs.com

BLACKCLOAK™

Digital Executive Protection

Protecting personal digital lives requires an expert team and a tailored approach to ensuring that every aspect of digital privacy and personal cybersecurity is covered.



Award-winning Concierge Cybersecurity & Privacy™ Platform that protects you, your family, and your corporation.

LEARN MORE

CYE

Transform the way you manage cyber risk.

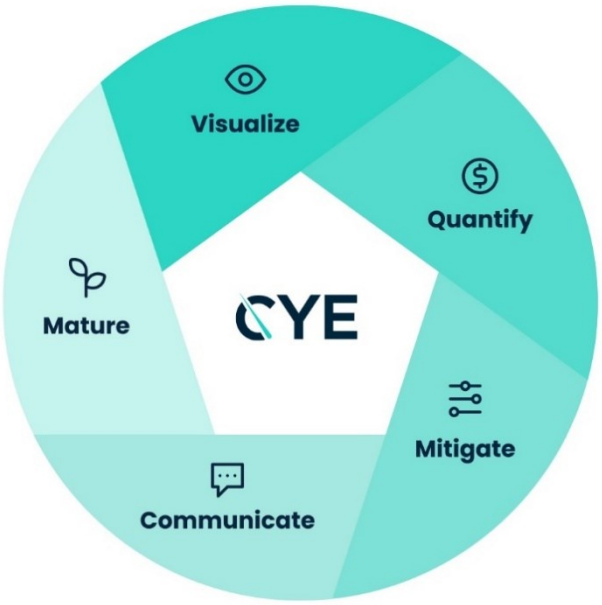
CYE's optimized cyber risk quantification solution enables you to:

Visualize

Predict probable attack routes by leveraging AI and data science with our SaaS platform.

Mature

Embrace transformation and unlock your organization's full potential with confidence.



Quantify

Determine the potential financial consequences of cyber risk in dollars, as well as the cost of remediation.

Communicate

Clarify and present your cyber risk in business terms to executives, security teams, and partners.

Mitigate

Focus your resources on addressing the most critical threats that truly pose risk to your business assets.

"The investment in CYE's tools and services has helped us receive the financial support over the past couple of years that we didn't have several years ago."

John Padilla, Associate VP of IT SONICWALL

The Benefits of Working with CYE

96%

of customers' business-critical attack routes are blocked within six months

88%

Reduction in remediation time following a cyber incident.

87%

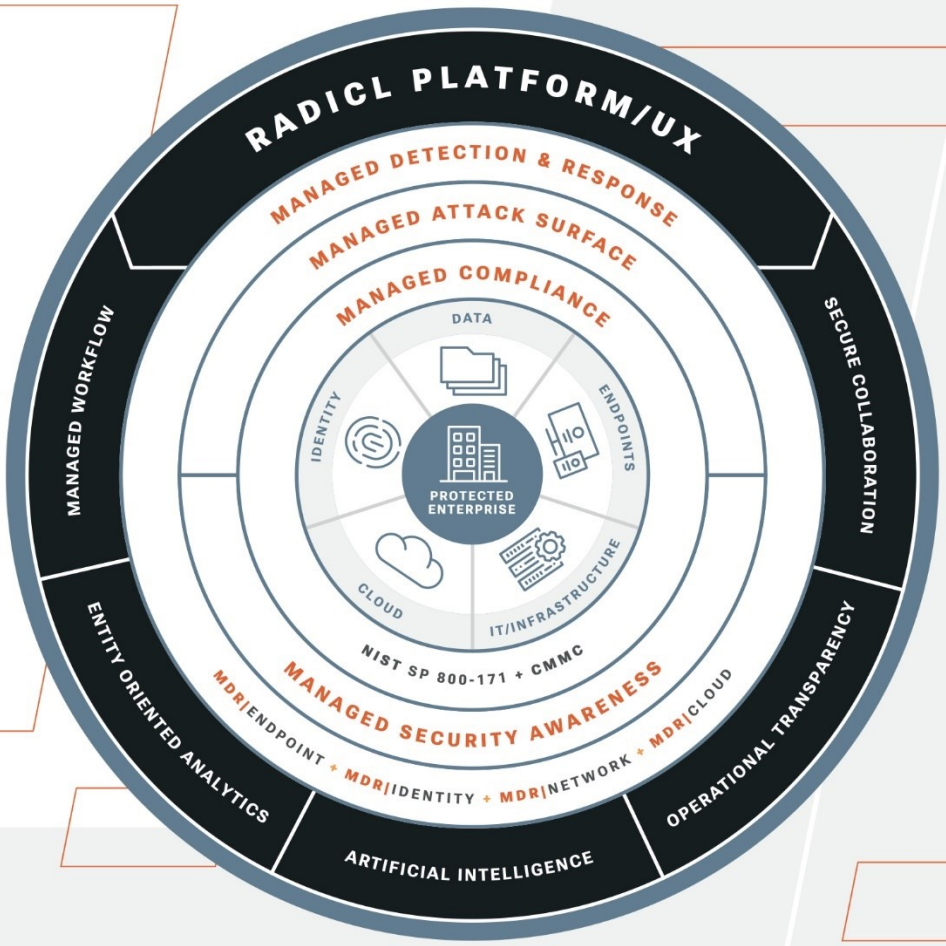
of customers improve ROI on their security budget.

Visit us at cyesec.com

RADICL™

We Protect American SMBs From Advanced Cyberthreats

If you want to maximally reduce your cyber incident risk, get RADICL!



- ✓ Endpoints Protected
- ✓ Identities Secured
- ✓ Vulnerabilities Reduced
- ✓ Incident Response 24 x 7
- ✓ CMMC / NIST 800-171 Assured



"Companies developing, holding, or delivering technology, information or operations of interest to nation state cyberthreats are being actively targeted by extremely advanced threat actors. These companies make up America's Defense Industrial Base (DIB) and Critical Infrastructure (CI) and are under constant attack. For the sake of national security, they must be better protected. These same companies, along with others in verticals like finance, legal, and healthcare are also in the crosshairs of motivated and advanced cybercriminals. RADICL was born to bring these "high value target" companies a radically different class of cyberthreat protection - protection previously only available to the largest of enterprises and government entities. If you desire the best protection possible, we'd love to talk to you."

Chris Petersen, CEO of RADICL

GIVING SMBS LONG-OVERDUE ACCESS TO ENTERPRISE-GRADE CYBERSECURITY PROTECTION.

RIDGE SECURITY

Make Your Risk Window Goal

ZERO

With Our Continuous Security Validation AI Agent

RidgeBot®

Get Started Today!

Keep up with CVE list published by CISA

Large exploit database 6000+

Wide testing coverage:

Windows
Linux
Websites
Database
OT / IoT
Cloud



WHEN MANAGING ASSET RISKS

PARTIAL VISIBILITY



IS JUST NOT GOOD ENOUGH.



WITH SEPIO, SEE ALL ASSETS. MANAGE ALL RISKS.

Learn more about Sepio's Asset Risk Management Platform >

www.sepiocyber.com

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Spin.ai

SaaS Security Platform for Mission-Critical SaaS Apps

Enhance Cyber Resilience, Security Operations, and Cost Efficiency



Schedule a Demo Today

www.spin.ai/demo

© 2024 Spin.AI. All rights reserved.

VMRAY

Good enough
is not enough.

SANDBOXING REINVENTED TO UNCOVER HIDDEN THREATS



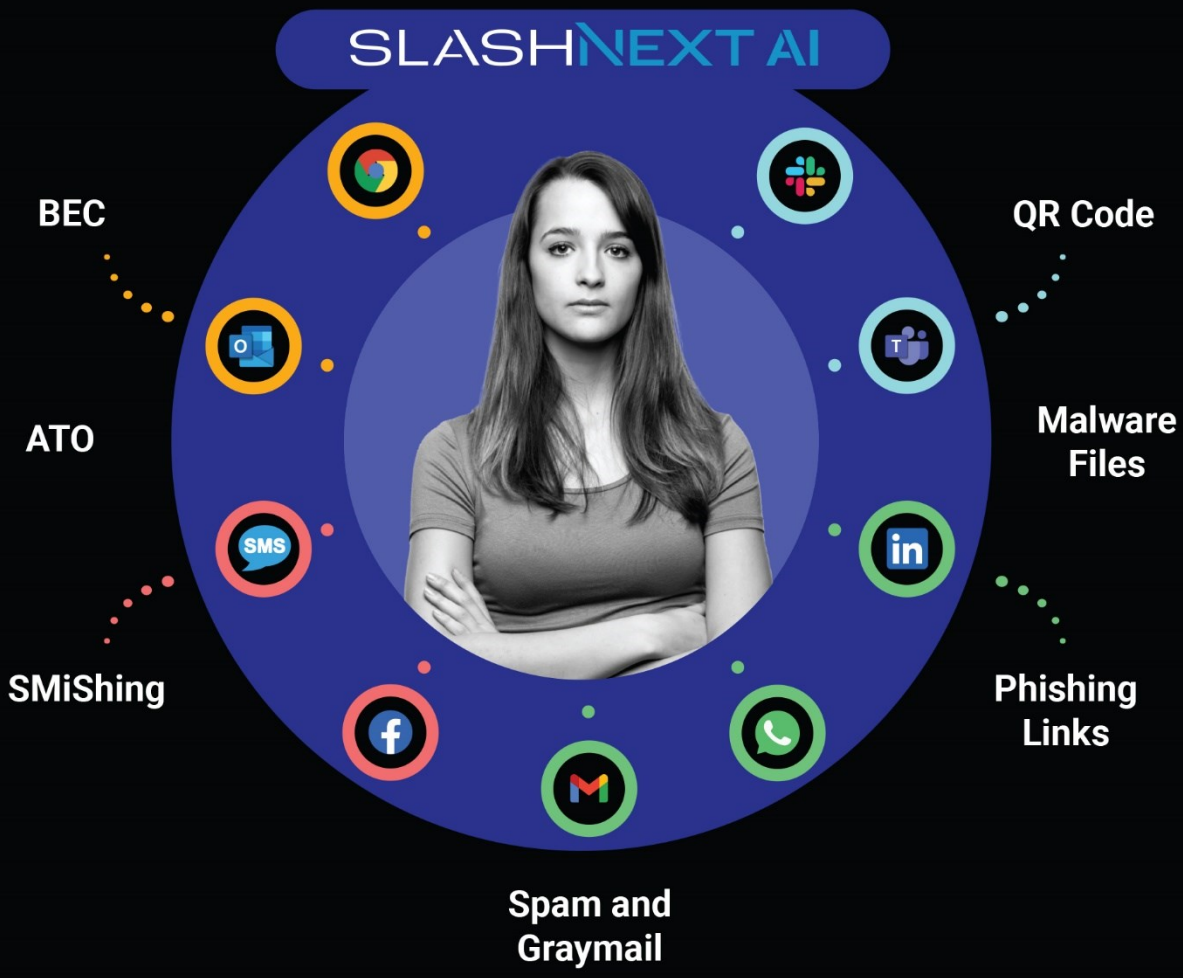
VMRAY.COM


BECOME THE
CYBER ARCHITECT
OF YOUR SECURITY STORY
Build a Strong Foundation for a Secure Future.
deepwatch™
www.deepwatch.com

SLASHNEXT

NEXT GEN AI EMAIL+ SECURITY

Make Email + Messaging Safe Again.



- 360° workspace protection
- 4X better threat detection
- 5 minutes to AI protection
- 2X higher SOC efficiency

www.SlashNext.com



Strengthening Your Security Post-Breach with Horizon3.ai

In today's rapidly evolving threat landscape, responding after a breach isn't enough. Horizon3.ai leads with a proactive defense approach through its cutting-edge autonomous penetration testing platform, **NodeZero**™.

With continuous cyber risk assessments, NodeZero adapts as your digital environment changes, ensuring long-term protection. NodeZero identifies and prioritizes vulnerabilities, providing actionable remediation strategies. Enhance your security posture, streamline stakeholder communication, and align defenses with organizational goals.



Visit **www.Horizon3.ai**
to download our white paper on
Enhancing Cybersecurity Post-Breach
and learn how NodeZero can safeguard
your organization against threats.

HORIZON3.ai

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Kodem

Security for everything you build.

Powered by runtime.

Kodem provides runtime-powered application security, giving you an attacker's view to discover, prioritize, and fix code, open source, and container risks across your stack.

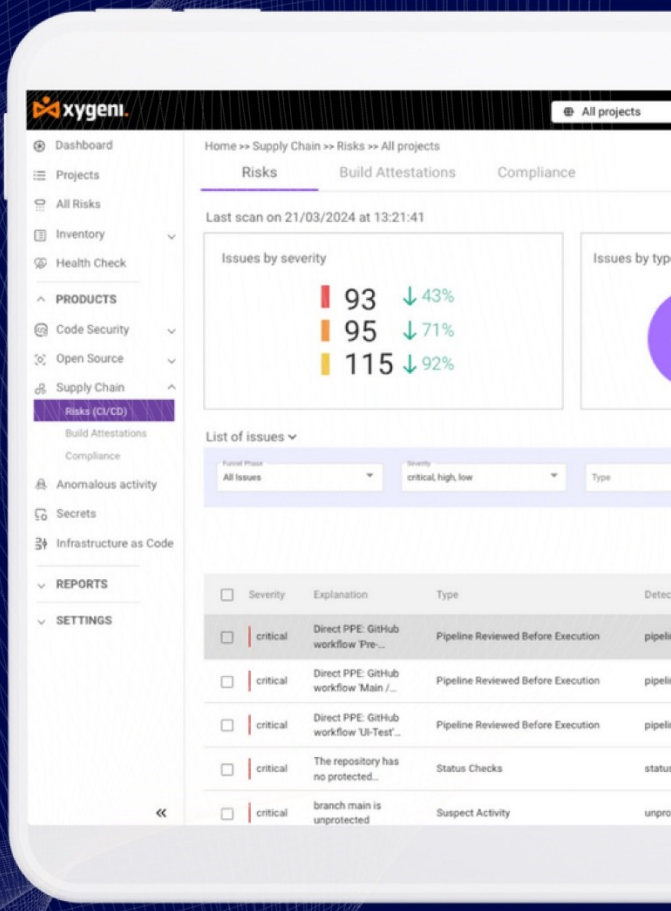
kodemsecurity.com

xygeni.

Secure Software Development & Delivery

- ASPM
- Open Source Security
- SSCS
- Build Security
- Anomaly Detection
- Code Security
- Secret Security
- IaCSecurity

Discover more at xygeni.io



Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

this is why

hackers hate us.

"Since you have ThreatLocker® installed, it became clear that we could not use Windows machines for our purposes."

– A real message
from an actual hacker.

this is why

you will love us.

"Since you have ThreatLocker® installed, it became clear that we could not use Windows machines for our purposes."

– A real message
from an actual hacker.

Do you know your current systems' vulnerabilities?
Order your free
software health report now.

THREATLOCKER®
ZERO TRUST ENDPOINT PROTECTION PLATFORM

threatlocker.com

THIRD-PARTY RISK MANAGEMENT

Modernize Your TPRM Program to Keep Up With Demand

Streamline Workflows and Maximize Your Team's Impact By Automating Steps So You Can Do More with Existing Resources



Simplify Monotonous Work So You Can Focus On Bigger Problems

TPRM teams spend countless hours on everyday tasks and burn through budgets and resources, leaving less time to focus on critical security concerns that will cause an impact.

Automate routine aspects of your program, from scoping your vendors to uncovering levels of inherent risk hiding in your portfolio. Turn elements of onboarding, ongoing monitoring, performance management, and even offboarding into a repeatable process to increase the volume of the third parties you focus on and free up more time to become a proactive protector of your organization.

Hands-Free Automation

Automate everything from assessment scoping to evidence collection with the click of a button. Run critical workflows in the background so that you can focus on impactful risk reduction.

Enterprise Integration

Seamlessly integrate with key enterprise systems such as Archer, MuleSoft, JIRA, Ariba, Archer and more through a robust web services-based API.

No-Code Configuration

Easily add features and functionality without relying on service engagements. Our platform is 100% configurable by the end user, meaning you don't have to wait weeks for the changes you need to meet program demands.

Reporting-as-a-Service

Provide stakeholders with the data that matters to them in seconds. Rapidly generate meaningful, board-ready reports that demonstrate the value of your program.

Implement Automation. Get Your Time Back.

Offload routine tasks to ProcessUnity to focus on TPRM work that matters.

- Sourcing – Automate the entire source to the onboarding lifecycle, simplifying RFx creation, supplier selection, and contracting.
- Onboarding – Streamline onboarding workflows, establishing a single, objective process for introducing new vendors to the business.
- Performance – Measure vendor performance against agreed upon SLAs and KPIs, track annual progress, and set threshold terms and alerts.
- Reporting – Generate dynamic reports and dashboards to get real-time visibility into the state of third-party risk.

ProcessUnity Third-Party Risk Management significantly reduces third-party onboarding and due diligence cycle times. Fueled by best-in-class workflow software, a universal data core for all TPRM information, the world's largest third-party risk exchange database and powerful artificial intelligence capabilities, ProcessUnity enables organizations to proactively mitigate first- and third-party risks.

ProcessUnity



txOne networks

Keep the Operation Running

TXOne Networks provides cybersecurity solutions that safeguard OT environments. Collaborating with top manufacturers and critical infrastructure operators, we develop practical, operations-friendly cyber defenses.

Copyright ©2024 TXOne Networks. All rights reserved.

txone.com

MACH37
CYBER ACCELERATOR

GET LAUNCHED

Our Mission

Today's real-time global connectivity has more complex threats and rapidly changing technology than ever before. In response, enterprise and consumer markets demand a steady stream of innovative new capabilities and solutions. MACH37 Cyber Accelerator® catalyzes the skills, foresight, and drive of the cyber industry's leading entrepreneurs, technologists, thought-leaders, and investors to anticipate that demand and accelerate the next generation of disruptive, high-growth cyber companies.

Our Program

Since 2013, MACH37® has operated in the heart of the cyber industry, just outside Washington D.C. in Northern Virginia. Our unique 90-day mentor-driven program leverages our workshops and expansive network of cyber experts from the public and private sectors to provide insights on how to build new cyber solutions and generate traction in the market. We emphasize the Lean Startup methodology and push technical founders out of the building so they develop and test their assumptions in a real world setting through brokered meetings with potential customers, channel partners, and investors. Using data collected from the market, we work with entrepreneurs to help them discover product-market-fit and hone their go-to-market strategy in a rapid time frame to build sustainable business models and drive growth.

MACH37® provides founding teams with extensive one-on-one mentorship from experts in entrepreneurship, strategy, public and private sector sales, marketing, product development, and venture capital investment. The advice from business and technical savvy mentors coupled with direct engagement with organizations facing cyber-related issues creates valuable connections that help founders prime a market for early product adoption. We give cyber startups a competitive advantage to attract seed-stage and Series A investors and become the next generation of leading cyber companies.

500-600
startups from around the world screened per year

450+ mentors world-wide

91 companies launched

84% of graduates are still in business

64% of graduates have raised follow-on investment post-Demo Day

$1M average seed round

hello@venturescope.com
www.venturescope.com
@venturescope

VentureScope®

STRATEGY · DEEP TECH · INVESTMENT

VentureScope® works with creative entrepreneurs, venture capital investors, and large private and public sector organizations around the world that are trying to solve interesting problems. Our team specializes in problem deconstruction and framing, product development, business model refinement, go-to-market strategies, build-buy-partner decisions, strategic partnerships, investment and growth analysis, and a variety of innovation methodologies. Whether you're a budding entrepreneur, a scrappy startup, an experienced investor, or an established organization developing a new service or capability, we will not only advise you on what to do, but work as part of your team to apply our recommendations.

Our team has over 60 years of combined experience launching new business ventures, investing in promising startups, running startup accelerators, teaching and providing strategic innovation and general management consulting services to large private and public sector organizations. We own and operate the MACH37 Cyber Accelerator®. We're on the pulse of emerging and over-the-horizon technology, and are tracking their growth and development against important industry problems to inform our dealflow and give you exceptional advice.

Expertise

- LEAN STARTUP METHODOLOGY
- BUSINESS MODEL STRATEGY
- PROBLEM DECONSTRUCTION & FRAMING
- PRODUCT DEVELOPMENT
- GO-TO-MARKET STRATEGY
- REVENUE GENERATION
- TECHNOLOGY SCOUTING & INVESTMENT DEALFLOW
- BUILD-BUY-PARTNER DECISIONS
- INVESTMENT & GROWTH ANALYSIS
- STRATEGIC PARTNERSHIPS
- CHALLENGE-DRIVEN & OPEN INNOVATION
- INNOVATION PIPELINE DESIGN & IMPLEMENTATION
- CREATIVITY & STRATEGIC FACILITATION
- INSTRUCTIONAL DESIGN & EXPERIENTIAL TRAINING
- HUMAN PERFORMANCE

2009 Founded

2010 Co-Founded and invested in WeatherAlpha

2011 Helped establish and run cross community crowdsourcing program; Obtained certification in InnoCentive's "Challenge-Driven Innovation" and problem deconstruction methodology

2012 Authored the business plan for Booz Allen's "Building a Culture of Innovation" and "Ventures" teams

2013 Launched and piloted Booz Allen's internal shark tank and accelerator

2014 Brokered Booz Allen's partnership with DC's 1776 incubator; Co-Founded and invested in Lunchin; Organized Startup Weekend "Women's Edition"

2015 Directed Smart-X accelerator in the West Bank; Mentee placed 1st out of 100 in GW's New Venture Competition

2016 Served as Entrepreneur-In-Residence at Techstars; Directed Techstars cybersecurity pre-accelerator program; Co-founded HackEd

2017 Joined MACH37® accelerator; Began working with Steve Blank to advise US government on innovation

2018 Acquired MACH37®; Participated in SXSW panel "War Games: From Battlefield to Ballot Box"

2020 Highlighted in Forbes magazine; Joined Steve Blank's Columbia University Business School Lean Launchpad Teaching Team

ALLEGISCYBER CAPITAL

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

The first dedicated cybersecurity venture firm in the world

About us

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

Signifyd | ELISITY | CONCEAL | panaseer | Synack

Lucidworks | DATATRIBE | DRAGOS | IRONPORT SYSTEMS | SHAPE SECURITY

www.allegiscyber.com

Altitude Cyber

"Built on passion and expertise, Altitude Cyber delivers strategic advisory services specifically tailored for founders, investors, startups, and their boards. Our unique approach fuses strategic insight with financial acumen to help your company soar to new heights."



Dino Boukouris

Managing Partner, Altitude Cyber

Guiding cybersecurity businesses globally through every stage of growth with tailored advisory services for founders, CEOs, investors, and boards.

Founders & CEOs

Altitude is your trusted advisor throughout your entrepreneurial journey. We guide you as you grow your business, navigate fundraising processes, construct advisory boards, plan your long-term exit strategy, develop strategic relationships with key partners and investors, and more.

Investors

We offer a range of strategic advisory services to support your existing portfolio companies, as well as your potential investments or acquisition targets. Our solutions are tailored to fit your needs, with flexible engagement models that align incentives to maximize outcomes.

Boards

We provide in-depth strategic advisory services, tailored to align with the evolving needs of growing businesses. Our support includes strategic business and corporate development, mergers & acquisitions, corporate finance, long term exit planning, advisor selection, and more.

Firm Highlights

Decades of experience as world class operators and advisors

Highly curated research and thought leadership on strategic activity in the cyber market

Deep industry relationships and partnerships across strategic and financial partners

Cyber Network

15,000+	Cyber Executives
3,000+	Investors
1,000+	CISOs

Cyber Knowledge

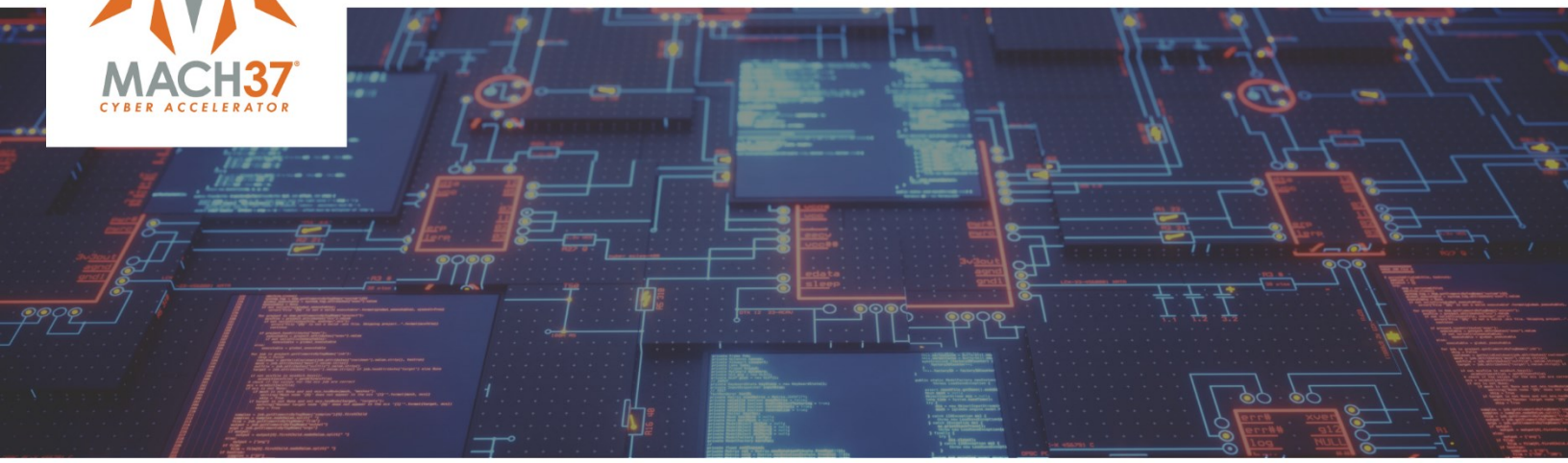
4,500+	Company Tracker
3,000+	M&A Transactions
8,500+	Financing Transactions

Extensive, global relationships with cyber executives, investors, CISOs, policy influencers, and service providers

Altitude Cyber, LLC | www.altitudecyber.com

For inquiries or further information please contact Altitude Cyber at: dino@altitudecyber.com

MACH37
CYBER ACCELERATOR



Our Industry Focus

- Cybersecurity
- Artificial Intelligence
- Machine Learning
- Space/Aerospace
- Quantum Computing
- Cyber Physical Systems
- Internet-of-Things
- Industrial Control Systems
- Neural Networks

Our Executive Team

Jason Chen | CEO & Executive Director | jason@venturescope.com

Jennifer Quarrie | COO, CWO & Strategy Director | jennifer@venturescope.com

Notable Alumni

RunSafe SECURITY

SylLab Systems

HUNTRESS

breachbits

HYPERQUBE

ATOMICORP

VIRGIL SECURITY

SYNCURITY
Built by Analysts, For Analysts

Optery FOR BUSINESS

PC PCMAG.COM EDITORS' CHOICE 2022, 2023, 2024

Remove your employees' personal data from the internet

- Prevent phishing & other social engineering attacks
- Reduce identity theft & fraud
- Protect your team from malicious actors
- Safeguard against real world harassment

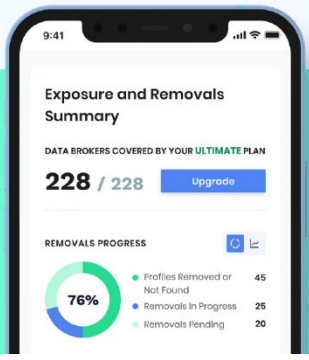
AS SEEN ON

SXSW · SECURITYWEEK · CR Consumer Reports · PC PCMAG.COM · TC · CNET · ZDNet · SC MEDIA

Why Optery for Business?

We're exclusively focused on data broker removal so you get the privacy & protection you need.

- Patented Search Technology
- Monthly Automated Scans & Removals
- Transparent Exposure & Removal Reporting
- Comprehensive Data Removal From Hundreds of Sites
- No Affiliations with Data Brokers
- SSO/SCIM/SAML Integration Options
- Clear, Affordable & Flexible Pricing
- SOC 2 Type 2 Certified



Create your free business account

business.optery.com/signup

SIXMAP

Zero Touch Automated **Network Defense**

See Every Port. Know Every Shadow.

SixMap provides automated, comprehensive visibility across IPV4 and IPV6 environments, uncovering hidden risks and prioritizing imminent threats. Discover every asset, pinpoint open ports, and protect your network – all we need is your name.

Schedule a Demo

Learn more and contact us at **www.sixmap.io**

CYBER DEFENSE MAGAZINE

You can't see
your threats
from the ground.
Get a 40k foot view
for free...

by reading
Cyber Defense Magazine



www.cyberdefensemagazine.com

RSAConference™2025

San Francisco | April 28 – May 1 | Moscone Center

Many Voices.
One Community.



Together we secure.
Join us at RSA Conference 2025!

Cybersecurity's greatest challenges demand more than one perspective. That's why RSAC 2025 unites thousands of voices from around the world to collaborate, innovate, and secure our digital future.

From April 28 – May 1 you'll hear groundbreaking Keynotes, explore hands-on sessions, and participate in exclusive networking opportunities. This is where the global cybersecurity community connects to share insights and find solutions.

Why Attend?

- Hear from top experts tackling today's toughest challenges in cybersecurity.
- Experience cutting-edge solutions at the Expo that will drive your strategies forward.
- Collaborate with peers to unlock innovative solutions and gain fresh perspectives.
- Expand your network with professionals from every corner of the globe, forging connections that last a lifetime.

Be a part of something bigger. RSAC 2025: **Many Voices. One Community.**

Register now at RSAConference.com/cyberdefense25

#RSAC


ARTICLES



The Cyber Insurance Conundrum

CISOs Wrestle with Coverage, Costs, and Clarity

By Denny LeCompte, CEO, Portnox

While cybercriminals innovate at lightning speed, cybersecurity teams—led by Chief Information Security Officers (CISOs)—often find themselves relying on outdated playbooks. Cyber insurance, once viewed as the ultimate safety net, is no exception. Findings from our recent survey conducted by Wakefield Research illuminate glaring challenges in how these leaders understand and leverage their cyber insurance policies.

Cyber Insurance: A Constant Balancing Act

According to the survey, two-thirds of CISOs (68%) frequently or constantly evaluate new security solutions to reduce their cyber insurance premiums. This statistic reflects not just a diligent effort to manage costs but also a recognition of the precarious financial balancing act many CISOs face. It's no secret that cybersecurity budgets are perpetually under scrutiny, and insurance premiums represent a significant slice of that pie.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The pressure to lower premiums has driven many CISOs toward technologies like Zero Trust Network Access (ZTNA), endpoint security, and network access control (NAC) that demonstrate proactive risk reduction. Insurers, of course, favor organizations that show measurable efforts to mitigate risks. But this dance of cost control often leaves little room for the real issue: understanding what the policy actually covers.

A Knowledge Gap with Consequences

The survey reveals a disconcerting trend: more than half of CISOs lack clarity on whether their policies cover specific threats or costs. Among the most alarming findings:

- **Uncertainty about specific threats:**
  - 58% of CISOs don't know if their policy covers supply chain attacks.
  - 57% are unsure about insider threats.
  - 55% are unclear about phishing attack coverage.
  - 51% don't know if ransomware payments are included.

- **Uncertainty about specific costs:**
  - Only 44% are confident their policy covers incident response costs.
  - 41% know whether data restoration is included.
  - Coverage for intellectual property theft remains murky for 48% of respondents.

This lack of clarity is even more pronounced in smaller organizations with revenues between $500M and $1B, where uncertainty about phishing attack coverage spikes to 65%, and confusion about intellectual property theft climbs to 57%.

Why This Matters Now

Cyber insurance is no longer a nice-to-have—it's a must-have. With regulations tightening, ransomware attacks becoming more sophisticated, and supply chain vulnerabilities multiplying, insurance offers CISOs a measure of financial assurance. But an ill-informed CISO is akin to a soldier wielding a shield with unknown weaknesses. Without a clear understanding of what their policies cover, CISOs risk unpleasant surprises during an incident when time, money, and reputations are on the line.

Additionally, the fallout from misunderstanding coverage extends beyond the CISO's office. Boards, investors, and even customers increasingly view cyber resilience as a competitive differentiator. A failure to grasp policy specifics could lead to reputational damage that no payout can fully mitigate.

Bridging the Gap: From Uncertainty to Confidence

The good news? There are actionable steps CISOs can take to close the knowledge gap and make cyber insurance work harder for them:

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

1. **Conduct a Coverage Audit:**

A detailed review of the insurance policy should be a priority, with a focus on understanding coverage for the most critical threats and costs. Partnering with legal counsel or third-party insurance experts can help translate dense policy language into actionable insights.

2. **Engage with Insurers:**

Regular, proactive communication with insurers is essential. CISOs should ask direct questions about specific scenarios, such as ransomware attacks or intellectual property theft, and document these discussions to avoid ambiguity.

3. **Leverage Technology for Premium Reductions:**

Implementing and documenting robust security controls not only reduces risks but also strengthens the case for premium discounts. Insurers are more likely to offer favorable rates to organizations with a demonstrated commitment to cybersecurity best practices.

4. **Educate the Entire Organization:**

The CISO's office cannot shoulder this burden alone. Building awareness across the executive team and board about policy nuances ensures alignment on expectations and preparedness.

5. **Focus on Emerging Threats:**

With supply chain attacks, insider threats, and phishing among the top areas of uncertainty, investing in solutions like advanced threat detection, insider threat management, and secure access controls can address both insurance and operational concerns.

A Call to Action for the Industry

The findings from this survey are a wake-up call—not just for CISOs but for the broader cybersecurity community, including insurers. As threats evolve, insurance providers must take steps to improve transparency and support their customers in understanding coverage. Creating standardized, plain-language policy summaries could be a game-changer.

For their part, CISOs need to view cyber insurance not as a standalone solution but as part of a holistic security strategy. Insurance can mitigate financial impact, but it cannot repair reputations or restore customer trust. Investments in technology, training, and proactive risk management remain paramount.

Knowledge is Power

Today, CISOs cannot afford uncertainty about their most critical safety net. The survey highlights not just a knowledge gap but also an opportunity for CISOs to reframe how they approach cyber insurance. By

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

understanding their policies, engaging with insurers, and aligning coverage with their organization's unique risk profile, CISOs can transform cyber insurance from a reactive safeguard into a strategic asset.

As the stakes rise, one thing is clear: clarity isn't optional—it's essential.

About the Author



Denny LeCompte is the CEO of Portnox, a leading provider of cloud-native, zero trust access control solutions, where he is responsible for overseeing the day-to-day operations and strategic direction. Denny brings over 20 years of experience in IT infrastructure and cyber security. Prior to joining Portnox, Denny held executive leadership roles at leading IT management and security firms, including SolarWinds and AlienVault. Denny holds a Ph.D. in cognitive psychology from Rice University. Denny can be reached online at https://www.linkedin.com/in/dennylecompte and at our company website https://www.portnox.com/.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



How Ghostgpt Is Empowering Cybercrime in The Age Of AI

By Eleanor Hecks, Editor-in-Chief, Designerly Magazine

Artificial Intelligence (AI) has significantly transformed various sectors, offering tools that enhance efficiency and innovation. However, the emergence of uncensored AI chatbots like GhostGPT has introduced new challenges in cybersecurity. Designed without ethical safeguards, GhostGPT provides cyber criminals with a potent tool for malicious activities.

The Rise of GhostGPT: An AI Without Limits

GhostGPT is an uncensored AI chatbot tailored specifically for criminal use. Unlike traditional AI models that incorporate safety mechanisms to prevent misuse, GhostGPT operates without such constraints.

It likely utilizes a jailbroken version of ChatGPT or an open-source large language model (LLM), effectively removing any safeguards. This design allows it to deliver unfiltered responses to queries that conventional AI systems would typically block or flag.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Features That Make GhostGPT a Cybercriminal's Dream

GhostGPT offers several features that make it particularly appealing to malicious actors:

- **Fast processing:** The chatbot promises quick response times, enabling attackers to generate malicious content and gather information more efficiently.
- **No logs policy:** The creators claim that user activity is not recorded, making it appealing to those who wish to conceal their illegal activities.
- **Easy access:** Available through platforms like Telegram, GhostGPT allows users to use it immediately without jailbreaking an AI model or setting up their own LLM.

How Cybercriminals Are Using GhostGPT

The unrestricted nature of GhostGPT enables cybercriminals to engage in various malicious activities, including:

Malware Development

GhostGPT assists attackers in generating code for different types of malware, identifying software vulnerabilities and developing polymorphic malware that can evade detection.

Phishing and Social Engineering

Cybercriminals use GhostGPT to design fraudulent websites, craft highly personalized phishing emails and generate templates for Business Email Compromise scams. Its advanced natural language processing capabilities produce persuasive messages that are difficult for traditional detection mechanisms to identify.

Fraud and Identity Theft

With GhostGPT, criminals can create fraudulent customer service bots, counterfeit legal documents and even draft persuasive scam scripts used in phone-based fraud.

Why GhostGPT Is a Growing Concern for Cybersecurity

As AI-powered tools become more sophisticated, their misuse by cybercriminals is becoming a major challenge for businesses and security professionals. Unlike conventional AI models designed with safeguards, GhostGPT operates without restrictions, making it an attractive tool for malicious actors.

Its accessibility and ability to generate compelling content raise serious concerns about how organizations can defend against AI-driven cyber threats. Here are some of the key reasons why GhostGPT is becoming an increasing cybersecurity risk:

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Lower Barrier to Entry

GhostGPT is easily accessible via Telegram, a messaging app known for its privacy features. It's affordable, simple to use and requires no technical expertise, making it an easy starting point for novice hackers.

Increased Attack Sophistication

Experienced attackers can use GhostGPT to refine malware, phishing campaigns and scam messages, enabling them to launch attacks at a much larger scale. This is especially dangerous for businesses, as a single cyberattack can result in prolonged downtime, lasting reputational damage and financial losses.

Evasion of Detection

GhostGPT-generated content is often indistinguishable from human-written text, making it challenging for security filters to identify and block malicious messages.

How Businesses Can Protect Themselves

To counter the threats posed by GhostGPT, organizations should adopt a multi-layered approach to cybersecurity. Here are key strategies to mitigate AI-driven cyber threats:

- **Implement zero-trust security measures:** A zero-trust framework ensures that every access request is continuously verified before granting permissions. This approach helps prevent unauthorized access even if AI-generated attacks attempt to bypass authentication processes.
- **Enhance employee awareness:** A report found that 99% of all cyberattacks rely on human interaction to succeed, demonstrating that attackers often exploit human error rather than directly breaking through technical defenses. Employees should be trained to recognize AI-generated phishing attempts, scrutinize unexpected emails and avoid clicking unverified links or attachments.
- **Develop AI-resistant communication policies:** Businesses should establish guidelines for verifying digital communications — including email authentication protocols such as Sender Policy Framework and DomainKeys Identified Mail — to minimize the risk of AI-generated phishing attacks.
- **Enhance content moderation for public-facing platforms:** Organizations that manage forums, comment sections, or user-generated content platforms should deploy advanced AI-based moderation tools to detect and filter out malicious AI-generated content.
- **Conduct regular AI-specific cybersecurity drills:** Cybersecurity teams should simulate AI-driven attack scenarios to test the organization's resilience against threats like AI-generated phishing emails and malware. These exercises help teams refine response strategies.
- **Collaborate with AI ethics and security researchers:** Businesses should engage with industry experts and government agencies to stay ahead of emerging AI threats. Collaboration can lead to the development of more effective detection and mitigation techniques.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

- **Monitor dark web activity:** Cybercriminals frequently discuss AI-powered attack tools on underground forums. Businesses should invest in dark web monitoring services to track emerging threats and gain early warning of new AI-driven attack methods.

The Future of AI and Cybersecurity

The rise of uncensored AI chatbots like GhostGPT marks a turning point in the cybersecurity landscape. By enabling cybercriminals to execute attacks more efficiently, these tools highlight the urgent need for businesses to adopt advanced security measures. As AI continues to evolve, organizations must remain proactive, integrating AI-driven defenses and fostering a culture of cybersecurity awareness.

About the Author

Eleanor Hecks is the Editor-in-Chief of Designerly Magazine. She is an SMB writer and researcher of 8+ years who is passionate about helping businesses stay secure online. Eleanor can be reached online at https://www.linkedin.com/in/eleanor-hecks/ and at https://www.designerly.com



Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



How Cybersecurity is Evolving in 2025 to Tackle New Threats

By Vaibhav Dutta, Associate Vice President, and Global Head – Cybersecurity Products & Services, Tata Communications

The cybersecurity landscape continues to evolve at breakneck speed. In the U.S., regulatory policy at the federal level – for instance, the National Cybersecurity Strategy launch and the SEC's Cybersecurity Disclosure Rules – has played a big role in its growth. The rise of zero-trust architecture has also accelerated across private and public organizations to combat the changing and growing risks posed by cyber threats.

2025 promises to be another year of change for cybersecurity professionals, with existing and emerging threats set to present challenges for organizations of all sizes. Cybercrime itself is rapidly advancing, and costing global businesses $12 trillion annually. The World Economic Forum reports that 35% of small businesses are concerned about their cyber resilience, a seven-fold rise from just a couple years prior. It's clear that businesses must adopt more resilient and innovative strategies to protect themselves. Fortunately, there are clear steps organizations can take to stay ahead of the risk.

The double-edged sword of generative AI (GenAI)

Globally, there was a 30% year-over-year increase in cyberattacks in Q2 2024 compared to Q2 2023. This staggering rise, coupled with a shortage of nearly 500,000 cyber security professionals in the U.S., has meant that cybersecurity professionals are stretched thin.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

GenAI offers remarkable potential to swing the pendulum back in favor of defenders. From real-time threat detection to automated incident response, GenAI is a crucial weapon in the security professional's armamentarium.

However, GenAI also poses some security risk of its own. It's been used to develop sophisticated phishing campaigns and advanced malware attacks. Concerns like these call for a careful approach to AI adoption, focusing on privacy safeguards to ensure sensitive data remains protected. We must balance the benefits of AI with its risks, with privacy being a top priority to ensure AI systems protect sensitive company and consumer data.

Infusing an "outcomes" mindset throughout the organization

Outcome-driven metrics are critical – and while not new, they've gained traction in recent years as organizations look to quantify the return on their cybersecurity investments. Key metrics like reduced time to detect and respond, and false-positive reduction rate, help measure success and demonstrate ROI on security investment.

However, these measures have to be meaningful and interpretable across the organization, including to non-IT leaders. Simplifying the technical terms is crucial: For example, framing MTTD (mean time to detect) as the "time taken to spot potential threats" resonates better with leadership teams. High-profile incidents last year, such as the Change Healthcare Ransomware Attack and Volt Tycoon attack on infrastructure, underscore the importance of making cybersecurity initiatives intelligible at all levels of an organization, especially to decision-making executives.

Empowering employees to reduce human-generated risk

Cybersecurity is not just a technological issue – it's very often a human one. Gartner, advocates for human-centric security design, which aligns with our long-standing belief that many breaches stem from human error, whether misconfiguration, credential compromise, or phishing. Nurturing a culture of cybersecurity awareness through comprehensive employee training is crucial to protecting organizations.

Security responsibility must extend beyond the Chief Information Security Officer (CISO) to every business unit. Embedding security champions across departments enables organizations to decentralize efforts, making each team responsible for its own security. This not only alleviates pressure on security leaders but also helps address the cybersecurity skills gap. Knowing the role continuous threat exposure management can play

Gartner predicts that by 2026, organizations that base their security investments on continuous threat exposure management (CTEM) could reduce breaches by two-thirds. While proactive, continuous threat evaluation is valuable, it's important to know where it may fall short. For instance, it's unclear how CTEM will address the very human issue of phishing, which remains the leading cause of breaches. Still, using the tools at your disposal to better understand external vulnerabilities will remain a central tool for enhancing security.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Managing third-party vulnerabilities in an interconnected world

In today's hyperconnected world, businesses are often intimately intertwined with one another. Third-party vulnerabilities are a growing concern in this increasingly interconnected ecosystem. Weak spots in the supply chain – whether in software, services, or hardware – are perpetual risks. Reducing these threats lies not just upfront in due diligence, but in regular investments where they are most needed.

Conducting continuous third-party assessments is a given in our own operations, to ensure vendors adhere to rigorous security standards. Still, since no external assessment strategy is guaranteed, strong internal controls are essential to minimize the damage from third-party vulnerabilities.

Why identity security and zero trust are more critical than ever

Identity is the new security perimeter. With employees accessing data from multiple locations and devices, strong identity and access management (IAM) solutions are critical. Zero Trust architecture – requiring continuous user identity verification before granting access – is a cornerstone of this strategy. Integrating IAM across infrastructures helps create a seamless yet secure user experience while ensuring strong protections. Part of this effort lies in behavioral analytics, where continuous behavior monitoring can help us detect anomalies and challenge suspicious activity, reinforcing Zero Trust principles.

The need for secure digital infrastructure has never been greater. In 2023, tech sector contributed nearly $2 trillion – or 8.9% – of the total gross domestic product (GDP) in the U.S. As industries integrate IT with legacy OT systems and embrace new technologies like GenAI, the complexity of threats continues to evolve. Cybersecurity is bigger than preventing hacks and protecting systems – it's about preserving trust. As we prepare for the future, organizations must embrace proactive and nimble security strategies that prioritize resilience, adaptability, and trust.

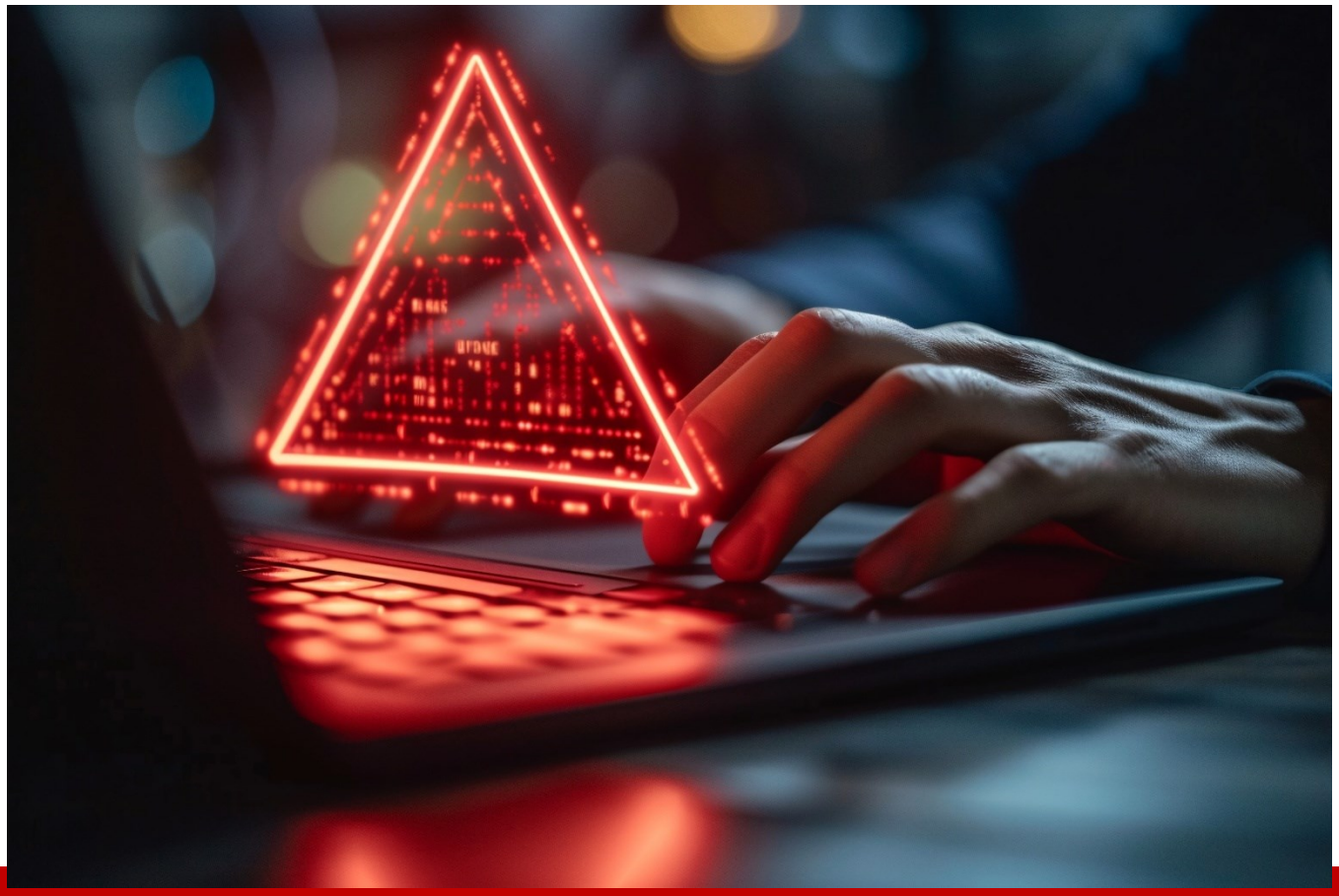
About the Author



Vaibhav Dutta is the Associate Vice President and Global Head-Cybersecurity Products & Services at Tata Communications at Tata Communications. With 23 years of experience across product management, engineering, business development, and strategy advisory, he has developed deep expertise in cybersecurity. His career has allowed him to work on various aspects of the field, from threat management to identity and OT security, and in creating managed security services and frameworks within these domains. Vaibhav has been recognized for my contributions to the industry and he appreciates the opportunity to collaborate with advisory communities and analysts. In his current role at Tata Communications, he leads Strategic Ventures for the Cybersecurity Business, focusing on new product and service initiatives, analyst relations, investments, and market exploration.

Vaibhav can be reached online on LinkedIn and at our company website https://www.tatacommunications.com/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Preparing For The AI-Generated Cyber Threats Of 2025

By Eran Orzel, CEO of CyTwist

There has been a gradual but alarming shift in the digital threat landscape over the last few years, as Advanced Persistent Threats (APTs) become more prominent and more potent. The volume of overall cyberattacks reached a crescendo in 2024, experiencing a 75% increase compared with the previous year.

Moreover, according to Gartner, AI-enhanced malicious attacks were the highest ranking cited risk among enterprise risk executives in 2024. The year ahead will likely see this continue, with the level of intelligent design evolving.

AI is enabling attackers to build sophisticated campaigns with unprecedented speed and precision. By automating reconnaissance, dynamically adapting malware, and mimicking legitimate behavior, AI amplifies attackers' abilities to evade traditional defenses. APTs, once the domain of state-sponsored actors, are now within reach of criminal syndicates and even lone hackers. The result? Faster, more

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

sophisticated, and harder-to-detect campaigns that demand businesses to be equally adaptive and proactive in their defense strategies.

Attacks with an AI Twist

AI enables hackers to scan networks, identify vulnerabilities, and execute attacks in minutes rather than days. If we look at malware for instance, already ballooning in scale with an increase of 14% of malicious files found in 2024 compared to a year earlier, AI is only going to exacerbate this trend.

Supported by AI, malware can automatically alter its code, presenting differently in the system which in turn overwhelms security mechanisms through sheer volume, while still delivering its payload. In this regard, there has been a growing trend of criminal international groups such as APT28, compromising systems again and again, relying on LLMs to obscure their movements and take advantage of poorly configured networks.

Phishing is another common data breach vector - three billion phishing emails are sent every day and the amount of people clicking on these links tripled in 2024. This puts more businesses at risk than ever before. In one study, which tested the ability of Large Language Models (LLMs) to exploit users with phishing scams, 60% of participants fell victim to AI-driven attacks - comparable to the success rates of non-AI phishing messages created by human experts.

This revelation illuminates how realistic and effective AI can be. If it can dupe a human into believing its authenticity just as effectively as a human-created scam, then the access to creative phishing is boundless. In fact, the entire phishing process can be automated using LLMs, reducing the costs of attacks by more than 95%, and taking away yet another boundary for hackers to grapple with.

It is paramount that companies fight fire with fire; AI-generated attacks with AI-pioneered solutions, which can identify and nullify intrusions in a fraction of the time of conventional tools. Organizations are starting to respond to the need, with 57% anticipating a budget increase for cybersecurity over the next year or two, but the urgency cannot be expressed enough - hackers will take advantage if the security protocols in place are insufficient.

Limited Defenses

The rapid evolution of AI-driven threats is exposing significant weaknesses in traditional cybersecurity tools and strategies. Many organizations remain heavily reliant on outdated technologies, which are increasingly unable to keep up with the tactics employed by modern attackers.

Static rules are often designed to detect known patterns of malicious activity. However, AI-driven threats can dynamically adapt their behavior, evading these rules entirely. For example, advanced malware can mimic legitimate processes, bypassing rules that flag suspicious activity. Signature-based systems rely on identifying specific, previously known malware signatures to detect threats - AI-generated malware, which can alter its code continuously (polymorphism) or create entirely new variants, easily evades these systems.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Blocking known malicious IP addresses can prevent some attacks, but attackers can frequently rotate or spoof IPs. Additionally, AI-enhanced botnets often utilize trusted platforms and residential proxies, bypassing these databases entirely. AI-generated threats spotlight these shortcomings by delivering malware and attack tactics that evolve in real time, leaving outdated tools unable to adapt quickly enough.

The reliance on traditional tools not only leaves organizations vulnerable but also burdens Security Operations Centers (SOCs). Outdated tools generate excessive alerts, many of which are false positives, irrelevant or low-priority, leading to alert fatigue. AI-driven attacks, designed to blend into legitimate network activity, go undetected in the noise, while manual triage processes slow down the response time, allowing attackers to inflict significant damage before being stopped.

Recent events have demonstrated the devastating impact of AI-driven threats. In 2024, a sophisticated campaign targeted French government agencies and private companies, employing a combination of phishing emails, encrypted payloads, and staged attack chains. AI-written malware used advanced techniques like COM hijacking to establish long-term persistence, evade detection, and exfiltrate sensitive data. This attack, alongside the broader deficit in AI skills among security professionals, underscores the urgent need for businesses to rethink their cybersecurity strategies.

Countering the Threat

To hit back against the new generation of AI-powered attackers, businesses must likewise adopt emerging technologies which can root out an intruder in a matter of minutes. Counter threat focused tools which can interrogate any untrustworthy anomalies within systems, interpret deviations from expected behavior and highlight unique attack tactics which defy the typical rules, will be the security priority for this year.

Automated response systems, real-time alert diagnosis, and continuous monitoring enable organizations to contain threats before they escalate. At the same time, building resilience into security frameworks is essential for long-term success. Integrating defensive solutions into an organization's security structure will enable an AI-driven tool to learn on the go, improving its powers of anticipation and responsiveness.

As well as budgeting for vital technologies, businesses must foster a culture of resilience and preparedness. Continuous training for security teams is essential to equip them with the skills needed to counter the latest attack methods. Continuous monitoring ensures round-the-clock protection, while adaptive defense strategies and regular security team training cultivate resilience. Together, these measures create a comprehensive and flexible cybersecurity framework capable of withstanding and recovering from AI-generated infiltrations.

Forewarned is Forearmed

Despite the exponential rise in cyber threats, cybersecurity as an industry is severely understaffed. According to an ISC2 cybersecurity workforce study, 25% of respondents reported layoffs in their

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

cybersecurity departments, while 37% faced budget cuts. We know the escalating threat and it is up to each business owner or security professional to act.

There is no doubt that AI can magnify the impact of a threat, but it can also challenge it. Without AI, uncovering and managing a breach can take an average of 277 days, now with certain technologies this is reduced to minutes.

The stakes are high, and we must remain vigilant to the diverse and developing threat landscape. The era of sluggish and rigid security is over. Organizations should prioritize tools which trigger deep learning mechanisms which prosecute information at lightning speed and identify vulnerabilities or sabotage with pinpoint precision. In the chronicles of cybersecurity we have reached a new chapter, one which is relying on AI to write it. It is up to businesses and those combating the security threat to prevent it being the only storyline.

About the Author



Eran Orzel is the CEO of CyTwist, and a seasoned business leader and entrepreneur with over 20 years' experience in sales leadership and go-to-market operational roles. He has extensive experience with a next generation cybersecurity platform countering Advanced Persistent Threats (APTs). Eran is a sought-after expert on cybersecurity and the emergence of AI-driven threats, having held a string of high-profile positions for leading tech and security enterprises, including as Head of Strategic Sales and Partnerships at Check Point and Co-Founder and Chief Business Officer at Argon, which was later acquired by Aqua Security.

Eran can be reached at https://www.linkedin.com/in/eran-orzel/?originalSubdomain=il

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



AI Addressing New Need to Secure Data from The Inside Out

By Rob Sims, CTO and Co-Founder, Alchemi Data Management

Today's traditional perimeter-based cybersecurity measures are increasingly inadequate due to threats that arise from within an organization. Whether born of malice or mistake, it's clear that insider threats are only further bolstered by the fast-growing use of cloud computing and mobile devices as well as the rise of remote work. Our workplaces are now thoroughly blurred. The once-clear boundaries of organizational networks don't exist, rendering conventional defenses far less effective.

Post-pandemic reports have consistently shown organizations consider their existing perimeter-based security models unable to properly secure remote employees, let alone in-office teams. Recent studies indicate that insider threats are the initiator of nearly half of security breaches, and in some cases cause millions of dollars of losses or related expenses.

To address this ever-escalating insider threat challenge, compliance standards such as NIST 800-171 and ISO 27001 emphasize the need for data-centric security approaches that protect information at its

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

core, regardless of its location or access point. This translates into the need for security at the file level, providing organizations with true control of their data. By adopting AI-based intelligent content protection strategies, organizations are able to improve file-based security through understanding their content at a deeper level and identifying potentially sensitive content not otherwise noted.

The New Paradigm: Content-Centric Security

In the past, insider threat solutions employing User Behavior Analytics (UBA) have focused on broad activity tracking, such as network logins, application usage, social media activity, and other behavior that potentially creates an unending number of alerts that can easily become unmanageable and unhelpful. While well-intentioned, their methods typically fail to prioritize the data layer where the most critical corporate assets actually reside. This oversight leaves organizations vulnerable to subtle, unauthorized interactions with sensitive content – particularly by users with privileged access who may appear "normal" in terms of general behavior.

A much more effective approach must focus on the data itself. Modern UBA capabilities should be purpose-built to detect anomalous data access patterns, ensuring that deviations in file access, modification or sharing are appropriately flagged – regardless of the user's role or clearance level. Such a system must operate at the data layer, monitoring abnormal interactions with files containing sensitive information such as Controlled Unclassified Information (CUI) or other regulated data within a target market.

The addition of dynamic content analysis and classification is essential in order to enhance this new data-centric approach. By examining the actual content of files in real time, insider threat solutions can automatically identify and classify sensitive data, even when it is improperly labeled or entirely unmarked. This capability ensures that organizations are not only detecting unauthorized access but are also proactively securing the content itself.

The Expanding Role of AI in Identifying and Protecting Sensitive Content

One of today's most significant challenges is the identification of sensitive content within vast repositories of files that lack distinctive markings, titles, or metadata. Afterall, employees create and use files in their own way, on their own time and in ever-unique manners. Traditional methods of data classification often rely on predefined labels or manual tagging, which are prone to human error and can leave critical information unprotected. This is where AI plays a pivotal role and opens up vast capabilities at the front lines of content protection. AI can be used to analyze files, identifying sensitive content within those files which might require special treatment and control. The addition of AI-driven classification ensures that even unmarked or mislabeled files are properly identified and secured, reducing the risk of accidental exposure or deliberate exfiltration.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Preventing Data Exfiltration at the Source

Today's comprehensive insider threat solutions must go beyond identifying and classifying sensitive content to actively preventing unauthorized transfer of files to non-corporate controlled locations. This involves integrating data exfiltration controls that leverage the insights from content analysis, AI-driven classification, and tagging to enforce customizable policies that protect sensitive files. By identifying sensitive content, whether explicitly labeled or detected through AI-powered analysis, modern solutions can proactively block unauthorized attempts to transfer such data to USB devices, cloud storage platforms, or email attachments.

For example, in real-world scenarios like intellectual property (IP) theft, a malicious insider might attempt to download proprietary designs to a USB drive or upload them to personal cloud storage. Similarly, during ransomware attacks, exfiltration of encrypted files often occurs as part of a "double extortion" scheme. Organizations must be able to monitor such activities in real time and uses automated policies to prevent unauthorized transfers before they happen, regardless of the user's role or permissions. Enterprises can no longer depend on alerts that require human intervention to protect data. Sensitive information is likely already compromised by that point, making the solution reactive and ineffective.

When combined with automation, powerful AI-driven insider threat systems can enforce granular access, transfer, and usage controls at the file level, ensuring that sensitive content remains secure while still allowing authorized workflows to proceed uninterrupted – a key factor in positioning security as a business enabler rather than a cost. This proactive approach helps keep IT personnel working efficiently while also significantly reducing the risk of insider threats and data breaches by stopping data exfiltration at its source.

Through the unification of AI-driven content analysis, intelligent tagging, and real-time automation, this insider threat approach dramatically enhances content security while maintaining compliance with regulatory requirements that can otherwise create countless headaches. As insider threats grow more sophisticated, preventing data exfiltration at the source represents a critical pillar of an effective, future-ready insider threat defense strategy.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



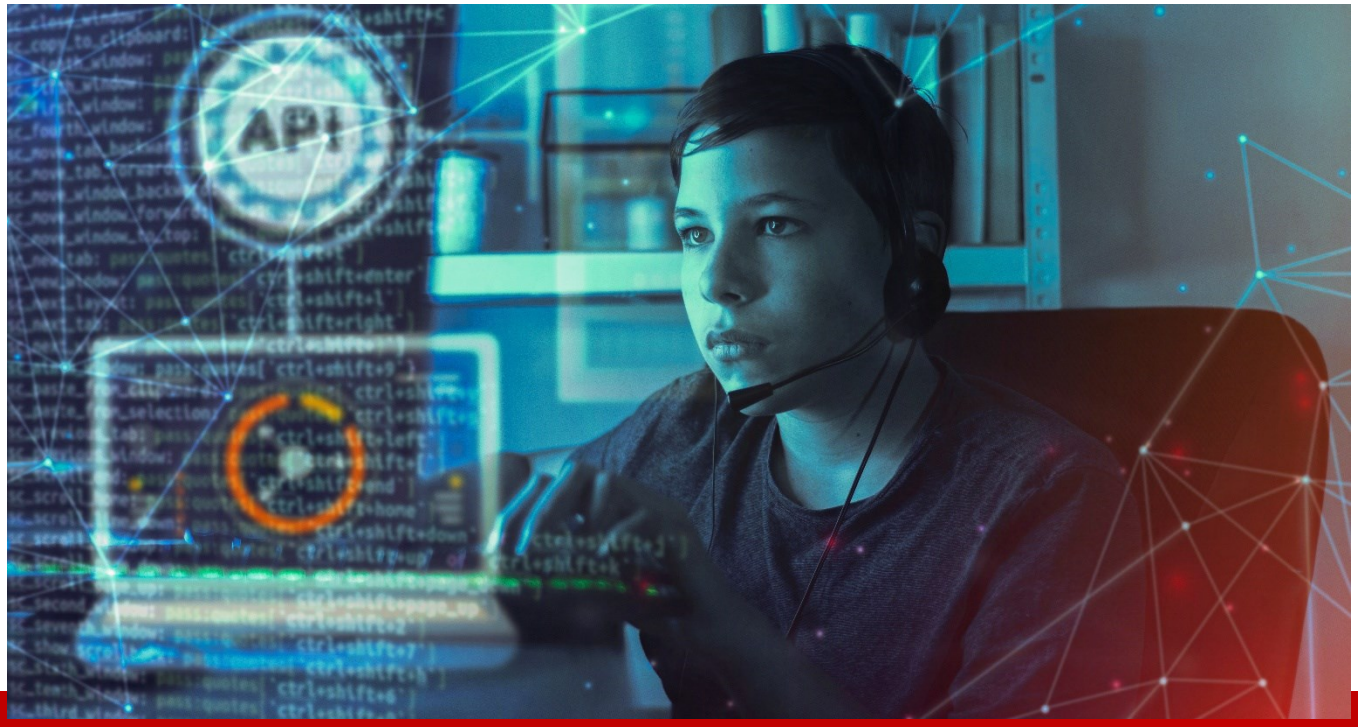
Rob Sims is the CTO and Co-Founder of Alchemi Data Management. He is a seasoned technology leader and entrepreneur with over three decades of experience in data management, enterprise software and hardware solutions. As the Founder and Chief Technology Officer of Alchemi Data Management Inc., he drives innovation in data security, risk reduction, and content management, helping organizations maximize the value of their digital assets.

Prior to founding Alchemi, Rob served as President of CitadelTek for over a decade, where he developed cutting-edge enterprise tools that provide insight and knowledge about file content, regardless of where it is created or stored. His expertise in data risk and reward strategies has enabled businesses to enhance operational efficiency and information security. Previously, Rob was President & CEO of Crossroads Systems, leading the company for nearly nine years in developing high-performance data storage and protection solutions. His leadership played a pivotal role in bringing advanced enterprise products to market.

With a strong foundation in engineering, Rob has held roles in new product integration and failure analysis at Kentek and Exabyte, gaining deep technical expertise in hardware and quality assurance. Rob holds a Bachelor of Science in Electrical Engineering (BSEE) from Colorado State University and further honed his business acumen at Harvard Business School's School of Management. Based in Round Rock, Texas, he continues to shape the future of data management through innovation and strategic leadership.

Rob can be reached online at rob@alchemi-data.com and at our company website https://alchemi-data.com/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



AI In Software Development: Balancing Innovation and Security in An Era of Lowered Barriers

By Michael Burch, Director of Application Security, Security Journey

AI is reshaping software development. The advent of sophisticated AI models such as DeepSeek and Ghost GPT has democratized access to powerful AI-assisted coding tools, pushing the boundaries of innovation - a staggering 76% of developers are either already leveraging AI coding tools or planning to do so in the near future - while simultaneously lowering the barrier to entry for developers. However, this growth in AI also presents a double-edged sword as while it promises unprecedented efficiency and accuracy for developers, at the same time it also lowers the barrier to entry for less skilled hackers, amplifying the urgency for robust security measures as potential vulnerabilities in AI-generated code emerge.

This widespread adoption of AI underscores a critical need for continuous education and stringent governance and policies within organizations to ensure secure AI practices in software development. Recognizing these challenges, initiatives such as the OWASP AI project are quickly stepping up to address the burgeoning concerns surrounding AI security, providing developers with precise, practical advice on how to design, develop, and test systems that prioritize security and privacy, ultimately seeking to pave the way towards a safer digital future.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Lowering the bar, expanding the risk

AI-assisted coding has made software development more accessible to a wider audience by speeding up initial training processes and providing open access to those starting out. Even the most proficient developers are reporting that AI tools are enhancing the quality of their code, reducing production-level incidents, and boosting overall code output — all key metrics for assessing developer performance. Additionally, AI coding tools are proving popular for collaborative tasks such as code reviews and programming, with the aim of fostering a more efficient development environment.

However, this accessibility comes with its own set of security challenges, and if AI is increasingly being used to write code, there's even more of an impetus for security education and training within development teams due to the shift required from writing code to doing code reviews for something that is AI-generated. The principle of 'trust no one, verify everything' is paramount and must be applied to the use of AI in software development. The integrity of AI-assisted code relies on developers treating the outputs of LLMs as untrusted data, however many developers lack the necessary knowledge, education, visibility, and context to identify risks in AI generated source code or effectively triage AppSec findings. In a similar way, AI models often lack the contextual awareness and intent of human developers, thereby effecting code quality and compromising the overall security of a system when over relied upon in the software development process. As such, developers must establish a thorough understanding of AI-generated code in order to proactively interrogate vulnerabilities and validate source code pre-deployment.

Similarly, while AI opens the door to a long line of budding developers by reducing the skill level required to produce code with relative ease, it also extends an inadvertent invitation to attackers to exploit vulnerabilities as security is put on the backburner. AI models such as Ghost GPT empower less experienced hackers to launch attacks and adept malicious actors to operate at scale and enhance the sophistication of their exploits. Paired with a lack of education and experience amongst novice developers utilizing AI models in development, cyber criminals are rubbing their hands.

Empowering human intervention

Organizations must be reminded that AI is not an entity, but rather a supplementary tool deployed to support those that enable it. As such, we cannot underestimate the importance of people in building security in from the start of any development process, and secure coding education for developers is vital to ensuring a base level of security. Just 1 in 5 organizations are confident in their ability to detect a vulnerability before an application is released, meaning that the security knowledge in most development lifecycles is insufficient. But during production is a critical time to detect and remediate vulnerabilities, and developers need to be trained to create secure software and to sniff out insecure code in the rest of the code base – responding and fixing it quickly. Without this, AppSec and security teams are left with an unnecessary burden of security, which will only ultimately require more time, spend, and potential for business risk.

Better training is therefore required so that teams relying on generative AI are more capable of spotting mistakes early and that architectures are hardened against attacks. If training is done well, it will also arm

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

developers with the knowledge needed to be able to use AI models more effectively. Tools like GitHub Copilot and ChatGPT show much promise in making developers more efficient and may in time reduce insecure code. However, like the promise of self-driving cars, we are probably still decades away from this reality.

A multi-tiered approach to protecting your organization from security attacks is still the best practice for today. The best approach to minimizing exposure to attacks includes combining:

- A well-educated staff
- A culture that values security
- The use of automated tools (static and dynamic analysis tools, for example)
- A security-first software development lifecycle

Our level of understanding surrounding AI models is bound to mature, but the threats facing AI are unlikely to change drastically and the ways we secure AI are fundamentally the same as the way we secure everything else. As such, we will benefit from practicing and instilling comprehensive security fundamentals across organizations. In going back to basics, most of the emerging threats brought in by AI are going to be mitigated by practices already understood and implemented across the board, decreasing the likelihood of vulnerabilities in code and slamming the door shut on attackers.

When looking to utilize AI in software development, **organizations should educate, then innovate**, realising the importance of secure code training as the AI threat landscape evolves. This approach helps establish a comprehensive understanding of any vulnerabilities that may arise in code or elsewhere due to inadvertent oversight and opportunistic malicious intent. By taking the necessary steps to foster and maintain fundamental security principles through continuous security training, development teams can balance risk and reward, ensuring the secure deployment of AI in development and beyond.

About the Author



Michael Birch is an Ex-Army Green Beret turned application security engineer. He currently serves as Director of Application Security at Security Journey, where he is responsible for creating vulnerable code examples and educating developers on the importance of establishing solid security principles across the entire SDLC.

Before joining Security Journey, Michael worked as a Senior Cyber Security Specialist for the North Carolina National Guard. In this role, he led the Cyber Network Defender program and mentored a team of soldiers in communication engineering and security. Michael also served as a Cyber Security Specialist, responding to incidents, conducting network assessments, and maintaining security systems.

Michael can be reached online at the Security Journey website and LinkedIn.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



AI-Powered Cyber Attacks and Data Privacy in The Age of Big Data

By Balasubramani Murugesan, Director of Engineering, Digit7 LLC

The fast transformation and evolution of artificial intelligence (AI) significantly changed the general norm and operational process of industries. This drastically transformed different sectors of industries related to finance, healthcare and communication, and. the upgradation in the technologies driven by AI also increasing the threats aligned with these technologies are also advancing. The most critical and significant concern in this new age technology-driven world is the increase of cyber-attacks powered by AI. This represents a significant risk to the privacy of data in this new age of big data. Organizations need to understand the impact and seriousness of these cyber threats and acknowledge their vulnerabilities to these threats. The organization also has to incorporate significant measures related to security in the process of protecting sensitive and important information.

In this new era of digital technology, the value of data has significantly increased and is considered the most important asset for an individual or organization. This idea of importance involves innovation related data of businesses, insights into consumers, and the processes related to decision-making. However, this factor of dependency on information or data also develops the exposure of organizations to become prime targets to be exploited with cyberattacks driven by AI. The incorporation of strategies related to data privacy has to eliminate these threats.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Artificial intelligence significantly increased the capabilities of attackers to efficiently conduct cyber-attacks. This also increased their intelligence and the scale of the attacks. Compared to the traditional process of cyber-attacks, the attacks driven by AI have the capability to automatically learn, adapt, and develop strategies with a minimum number of human interventions. These attacks proactively utilize the algorithms of machine learning, natural language processing, and deep learning models. They leverage these algorithms in the process of determining and analyzing issues or vulnerabilities, avoiding security and detection systems, and developing phishing campaigns that are believable.

Social engineering and phishing techniques in cyber-attacks are a concept that is developing and progressing with the passing years. This mainly involves emails, which are one of the most commonly utilized tools for communication in the world. Emails related to phishing are mostly about social engineering, and these can be proposed through links or attachments to this kind of email. Both of these aspects are extremely dangerous and malicious in the context that they can potentially hack classified or personal information and even gain complete control over computers, avoiding the user's attention. The concept of phishing is a process of sending messages leveraging emails in the form of well-acknowledged institutions such as banks, multinationals, and government organizations. Significant factors influence the opening of these emails, and the most common factors are promotions and campaigns. Other factors such as utilization of persuasion and influence in the process of deceiving people. The idea of social engineering is impersonating another person in the process of conducting manipulation. This involves taking advantage of embodiment to gain information with or without the utilization of technology. The implementation of artificial intelligence in these processes significantly increased their efficiency. The generative ability of AI for voice, text, graphics, and video content significantly contributes to increasing the capabilities in impersonation of other people in social engineering and text or graphics generation in phishing attacks.

AI has also significantly increased the intelligence of systems related to malware and autonomous hacking. These systems gained the capabilities to infiltrate networks, leverage the vulnerabilities of the system, and avoid detection systems. Malware driven by AI has the capability to make real-time modifications to its codes, unlike conventional malware. This significantly increases the difficulties in the detection and eradication process for the security software. These difficulties involve infiltration in systems powered by AI, such as polymorphic malware. It can convert its appearance based on the data collected from every attempt of cyber-attack. This results in successful avoidance of conventional security measures related to the detection of malicious activities. Additionally, automation tools powered by AI in the process of hacking can accurately determine weaknesses in networks, examine the measures of security, and identify loopholes that can be utilized without any interference of humans. These instruments are exceptionally capable to conduct cyber-attacks with drastic speed and accuracy. This increases the need for the adoption of robust security systems in the organizations and actively upgrade them.

The technology known as deep fake with the capabilities of artificial intelligence is also a critical threat for data security and privacy. The abilities of this system such as audio manipulation, generative images, and fabricated videos in the process of creating realism in content can be leveraged in fraudulent and malicious activities. These activities include theft of identity, spread of misinformation, and business email compromise (BEC) scams. There are practical examples such as generation of fake videos with orders

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

for funds transferring and disclosure of classified information. In a similar process, fake audio recordings developed with AI can potentially avoid authentication or security systems.

AI powered cyber criminals' activities creates various different cases of unauthorized access of data. This results in the disclosure of classified information such as information related to trade, credit card related information, and personal identity-related data. These outcomes are developing large-scaled financial losses for organizations and damaging their reputation. This also increases trust in the consumers related to data privacy and increases the demand for robust security measures with the aim of safeguarding critical and personal information of the consumers. It also causes national security national security related threats. This includes government agencies, defense and infrastructure-related classified data or information as prime targets. Government and private agencies have to incorporate cybersecurity systems powered by AI in the process of minimizing these threats. There are capable systems such as multi-factor authentication and zero trust architecture plays crucial role in cyber security. Occasional audits to ensure adherence to the security measures and training programs for employees around the information related to phishing and social engineering attacks also can be beneficial. Regulations and policies have to be developed by the governments for ethical development of AI and cybersecurity. This can provide advantages in the process of decreasing the utilization of artificial intelligence in fraudulent activities.

Artificial intelligence, data privacy, and cybersecurity are significantly connected with each other. In one hand this develops significant opportunities for upgradation in cyber security measures, on the other hand develops significant threats related to relevancy of these measures. The institutions of government and private organizations have to maintain relevancy of their cyber security measures and system for ensuring national security and privacy of data.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Balasubramani Murugesan, Director of Engineering of the Digit7 LLC. **Balasubramani Murugesan** is a seasoned IT leader with over 18 years of experience, specializing in cybersecurity, product and project management, data lakes, DevOps implementation, and team building. Currently serving as the Director of Engineering at Digit7, he has a proven track record of leading multidisciplinary teams to deliver innovative, cutting-edge technological solutions. His leadership has spanned industries, driving successful product launches and digital transformations.

Balasubramani holds multiple certifications, including SAFe® Agilist, Scrum Master, Six Sigma Green Belt, and Microsoft Certified: Azure Solutions Architect Expert. He is also an expert in cloud computing (Azure, AWS), AI (with a focus on Computer Vision), cybersecurity and DevOps. As a member of the prestigious Forbes Technology Council, he actively contributes to thought leadership within the tech space.

In addition to his technical expertise, Balasubramani is an enthusiastic writer and blogger. His writings explore the intersection of technology and traditional wisdom, reflecting his interest in how ancient principles can inform modern innovations. His blog and contributions aim to bridge the gap between technological advancement and timeless knowledge.

Balasubramani is also the author of the book *"Natural Language Processing in AI"*, which explores into the complexities and applications of AI in natural language processing. The book reflects his deep expertise and commitment to educating others about the transformative potential of AI technologies.

In recognition of his thought leadership, Balasubramani is also a Microsoft Tech Community - Brass Contributor, where he actively engages with peers, sharing insights and contributing to discussions on cybersecurity, emerging technologies and best practices.

Beyond his professional achievements, Balasubramani is passionate about mentoring and inspiring the next generation of technology professionals. He dedicates significant time to guiding students and young minds, encouraging curiosity and nurturing the technical skills that will shape the future of the industry.

Balasubramani can be reached online at www.linkedin.com/in/balasubramani-murugesan-36656a16 and at our company website https://www.digit7.ai/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



AI-Powered Testing: Innovation, Risks, and What Comes Next

The advantages, limitations, and security considerations of AI-driven testing in modern software development.

By Jason Kichen, CISO, Tricentis

Artificial intelligence (AI) is transforming software testing, driving unparalleled speed, accuracy, and coverage in comparison to traditional, manual methods. However, all good things come at a cost. As organizations integrate AI-powered testing tools into their DevOps pipelines, they must also handle new obstacles – such as AI's difficulties in handling complex test scenarios, ongoing skepticism toward AI reliability in the enterprise, and novel AI-specific cyber threats.

The continued evolution of AI will further solidify and grow its role in software quality and security. However, AI success depends on striking the right balance between leveraging its capabilities and acknowledging its limitations.

In this Q&A, we'll explore the answers to commonly asked customer questions regarding how AI is reshaping software testing, the hurdles organizations face when adopting AI-powered tools, the importance of governance and security in ensuring AI delivers on its promises, and the potential of future AI applications in cybersecurity – including zero-day vulnerability detection and securing open-source components.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

What advantages does AI offer over conventional testing methods regarding speed, accuracy, and coverage?

In today's dynamic, AI-driven environments, manual testing can no longer keep pace.

Unlike manual testing methods, AI offers significant advantages to DevOps teams, particularly when it comes to challenges tied to speed, accuracy, and coverage. By using AI-augmented tools, teams can automate test case generation, analyze test results, and even perform risk analysis on code changes. Generative AI copilot assistants are accelerating this transformation further by streamlining test creation, self-healing broken tests, and offering actionable guidance throughout the testing lifecycle. This saves time and allows quality assurance (QA) and development teams to focus on higher-value tasks that boost business efficiency, enhance the strategic output of developers, and drive more secure code.

Intelligent, adaptive testing solutions are now essential. AI-powered testing allows for simplified software quality with an intelligent, codeless, and scalable approach that works no matter what is being tested (and who's writing the code).

What limitations do current AI systems face in understanding complex test scenarios?

While the benefits of AI are enormous, it has become more difficult for DevOps teams to accurately predict its full capabilities. Generative AI systems sometimes lack the specialized knowledge that human testers have about specific applications and can struggle to interpret vague requirements in test cases. Examples of this can be assessing "user-friendliness" or "aesthetic appeal," both of which require human judgment. Diving into more complex test scenarios, these often depend on not only understanding more broad parameters—from historical data to user intent—but also require the technology to adapt in real time to complex workflows. On top of this, when gone untested, AI applications can result in biased systems with flawed test data, resulting in misguided analytics.

This is why it is important for engineers and testers to view AI as a collaborator rather than the decision-maker. As such, the advantages AI technology provides can only be fully recognized if engineers maintain oversight and validate outputs of tests to ensure any potential issues are caught before they escalate.

What are organizations' most prominent challenges when integrating AI into their testing pipelines?

Some general challenges that generative AI poses, from hallucinations to creating biased systems, all remain true when integrating this technology into testing pipelines. But beyond the challenges that come with the complexity of the technology itself, organizations face challenges at the developer level. Simply put, there remains a major shortage of AI expertise within DevOps. While it's imperative for human testers to be involved throughout the pipeline, ensuring organizations have the right talent, given how involved humans are in the process of manually reviewing AI-generated outputs, remains a challenge for leaders integrating AI into their testing pipelines.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Creating a sound governance and risk mitigation framework is also a challenge (and simultaneously, an opportunity) for organizations as they look to incorporate AI into their operations quickly. These frameworks are crucial in demonstrating a commitment to responsible and secure AI use. Building this trust with customers, regulators, and other stakeholders is paramount in overcoming challenges related to trust. Not only does this underscore an organization's commitment to responsible and secure AI use, but it also ensures DevOps teams can drive rapid innovation while prioritizing ethical, regulatory, security, and operational considerations as they integrate AI into testing pipelines.

Can AI autonomously identify zero-day vulnerabilities? What progress has been made in this area?

Not yet, but this capability is on the horizon. The complexity of how a system can be exploited, or how a vulnerability can be weaponized, is something well situated on the roadmap for AI development. But it will be a double-edged sword: defenders will take advantage of AI's ability to quickly detect and maybe fix novel vulnerabilities in code, while adversaries may use the same AI capabilities to detect vulnerabilities in code and quickly weaponize and operationalize them for malicious use. This cat and mouse game isn't new, but the speed and impact of these developments may force product security teams and defenders to re-think their approaches to vulnerability management.

Many testing frameworks rely on open-source components. How can AI improve the security of these tools?

As AI becomes more effective at examining code for novel vulnerabilities, we will effectively have a bigger and more powerful "microscope" to point at open-source software. Theoretically this will help us move faster to secure existing open-source software and help us have greater confidence in future open-source software. But the value proposition works both ways, as malicious actors use AI to more efficiently exploit open-source software. While the role of AI in helping better secure open-source software is clear, where and when to employ it is a greater question.

About the Author



Jason Kichen is the Chief Information Security Officer at Tricentis. In his role, Jason leads Tricentis' digital and physical security programs, including security operations, governance and compliance, product security, IT, and cloud engineering. Prior to joining Tricentis, Jason held multiple security leadership roles at various startups and technology firms after nearly 15 years in the US intelligence community. He serves the security community through his roles as Adjunct Faculty at University of California, Berkeley and as a Board Member at the Institute for Security and Technology (IST).

Jason can be reached online on LinkedIn and on the Tricentis company website.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Can Standards Deal a Deathly Blow Against Deepfakes?

By Alessandra Sala, Chair of Multimedia Authenticity Collaboration, International Electrotechnical Commission and Sr. Director of AI and Data Science at Shutterstock

Recent advances in generative artificial intelligence (AI) are making it increasingly difficult to know the difference between what is real and what is not. Computer-generated clips that are designed to look real, known as deepfakes, not only distort reality, but can be used to destroy the reputations of their victims and worse, foster social unrest. But what can we do about it?

Celebrities, ordinary people, and the erosion of trust

Anyone who follows the news regularly might be forgiven for thinking that deepfakes only target celebrities and politicians. The reality is that malicious actors generate fake content to harass, intimidate and spread misinformation about ordinary people too. In fact, when fake media attacks a person that doesn't have the economic or social means of a Taylor Swift or a Donald Trump, that's a real problem. For example, women in South Korea recently took to the streets to protest against an upsurge in deepfake

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

pornography. The national police agency is investigating hundreds of cases in which the faces of real women and girls have been digitally superimposed onto a body without their knowledge or consent. In Spain, a court sentenced 15 schoolchildren to a year's probation for creating and spreading deepfake pornography of girls as young as 11. Stories like this are occurring all the time in some part of the world. I was on a UN conference panel recently and a journalist from the Middle East was talking about her experience with a deepfake and she being falsely depicted with her boss in order to discredit her. The experience paid a heavy toll on both her and her family.

And while the effects on individuals can be devastating, deepfakes pose a wider threat to society. According to MIT Technology Review, deepfakes are "a perfect weapon for purveyors of fake news who want to influence everything from stock prices to elections". The World Economic Forum's Global Risks Report identifies fake media as one of our most pernicious challenges. According to the WEF, the proliferation of disinformation has eroded trust not only in digital platforms, but also in institutions. For example, for WITNESS, an NGO, it is threatening their mission of helping people to use video as a tool for defending human rights.

In fact, there is a growing concern that the misuse of digitally altered media can cause a state of social unrest be it through a misinformation campaign to influence the political stage, or the encouragement of hate speech and criminal activity to sew division.

Deepfakes and an unstable geopolitical stage

We are living in times of heightened geopolitical instability. Conflicts are erupting across regions, economic crises are deepening, political polarization is increasing, nations are grappling with the rapid pace of technological advancements, which bring both opportunity and risk, and the impacts of climate change are exacerbating all of the above. And with a lack of standards to check the threat, it's an all you can eat buffet for bad threat actors.

The good news is a standards collaboration on AI and multimedia authenticity was launched at the global AI for Good Summit in Geneva earlier this year. Experts highlighted the potential societal impacts of generative AI and the urgent need to address the misuse of AI for spreading misinformation.

WITNESS is one of a number of organizations who have signed up to apply standards – internationally agreed best practices – for detecting deepfakes and generative AI. Under the leadership of the three international standards organizations, IEC, ISO and ITU, the alliance is leveraging the insights and expertise of a broad range of stakeholders. Big tech is represented by the likes of Adobe and Microsoft. Other organizations taking part include the German research institute, Frauenhofer, and CAICT, a technology-focused think tank based in China, as well as the authentication specialists, DataTrails and Deep Media.

Why? Because standards can create safeguards to protect the digital space and work to rebuild trust, so that we can look at the news and understand whether we can trust it or not. And, in a world where trust has been broken and our natural human defenses don't seem to be enough, standards can help reestablish our confidence by contextualizing what we see and hear.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

A good example is the case of Deep Media, who recently commented on a hyper realistic video of Elvis Presley singing in a modern-day setting. Although the video became viral, the chances that anyone believed in the video's authenticity are slim to none. Deep Media noted that while opening doors for creative expression, the technologies used also carry risks of misinformation and reputational damage. Being able to detect deepfakes is crucial for preserving integrity and trust.

Not all fake media is bad

The AI for Good Summit brought together a diverse range of organizations, including the Content Authenticity Initiative (CAI), Coalition for Content Provenance and Authenticity (C2PA), IETF, IEC, ISO, ITU and JPEG, in recognition of the critical role of technical standards in supporting government policy measures. They agreed on a multistakeholder collaboration to develop global standards for AI watermarking, multimedia authenticity and deepfake detection technologies.

The discussions underscored the importance of transparency in AI, particularly regarding the provenance of data used to train AI models. Establishing the authenticity and reliability of this data is crucial for understanding potential biases and ensuring the accuracy of AI-generated content. The ability to verify the authenticity and ownership of generative AI multimedia content was identified as essential for protecting digital rights.

The aim is to detect rather than stop fake media because unlike the murky world of fake news, the intentions behind fake media are often good. The term 'fake' can be applied to any manipulated media. The entertainment industry benefits enormously from new technologies to create realistic special effects or artificial natural scene production with actors in the studio, for example. It is the same with news where leading public service broadcasters use virtual studios for their news bulletins and the set is oftentimes either computer-generated or a video image.

Standards for AI and generative technologies

The multistakeholder collaboration aims to provide a global forum for dialogue on priority areas and requirements for technical standards mapping the landscape of existing standards and identifying gaps where new standards are needed, as well as facilitating the sharing of knowledge among stakeholders.

This initiative is expected to play a crucial role in supporting government policy measures, ensuring transparency and protecting the rights of users and content creators in the rapidly evolving field of AI and generative technologies.

And for a bit more good news, members of the collaboration have already created a new standard, known as JPEG Trust, which will enable photos and videos to be 'tagged' and authenticated, so that users and creators can build trust in media content. JPEG Trust has been developed by the joint IEC, ISO and ITU Joint Photographic Experts Group (JPEG). This is the same group of experts behind JPEG technology that has enabled the world to use and share billions of images each day for over 30 years.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Alessandra Sala, Chair of Multimedia Authenticity Collaboration for the International Electrotechnical Commission and Sr. Director of AI and Data Science at Shutterstock.

A research and scientific leader in Artificial Intelligence, Alessandra chairs the AI and Multimedia Authenticity Collaboration, which brings together IEC, ISO, ITU and other standards organizations to foster a unified response to deepfake technology, addressing risks while harnessing the benefits of generative AI.

Alessandra is also the Sr. Director of AI and Data Science at Shutterstock. Alessandra has over 18 years' experience in research and innovation gained whilst working in academic and commercial environments. Alessandra is passionate in advanced analytics, machine learning, and computational models with the focus of transferring innovation from research to products.

As Co-chair of the UNESCO Women for Ethical AI Platform, Alessandra is working with a strong community of women to foster diversity, inclusion and equality for women and minorities while encouraging a global ethical approach in AI. As Global President of Women in AI (a non-profit do-tank working towards gender-inclusive AI that benefits global society) Alessandra leads a community of women from 171 countries that empowers women and minorities to become AI & Data experts, innovators and leaders. In an advisory capacity, Alessandra also serves as the Governance Committee Chair at the Science Foundation Ireland Centre for Research Training in Machine Learning.

Among several awards, Alessandra won the 2024 Grace Hopper and the 2021 XV International Prize "Le Tecno-visionarie" in the AI - Industrial Research category. In her previous role Alessandra was Head of Analytics Research at Nokia Bell Labs where she was leading research teams in several locations while driving changes across different activities like her contributions to the Nokia AI Ethics Advisory Board.

In her previous appointment Alessandra was Head of Analytics Research at Nokia Bell Labs where she was leading research teams in several locations and developing a successful strategy for the Data Analytics division while driving changes across different activities like her contributions to the Nokia AI Ethics Advisory Board.

Alessandra can be reached online at https://www.linkedin.com/in/salaalessandra/ through the IEC https://iec.ch/homepage or at her company website and at our company website https://www.shutterstock.com.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



How Businesses Can Turn the Expanding Attack Surface into an Opportunity

By Norman Menz, CEO of Cybersecurity SaaS platform Flare.

Only 42% of companies discover breaches through their own security teams. CISOs are often "blind" to third-party security practices and crucial data pipelines. This lack of transparency and reliance on their providers to keep their data safe invites an ongoing trade-off between security and accessibility. It works both ways. Service providers also want access to real-time information to heighten their security practices that organizations may deem too confidential to share. So where do CISOs and service providers draw the data-sharing line?

In a Gartner survey of 100 executive risk committee members, 84% said that third-party risk incidents resulted in disruption to operations. Financial loss, increased regulatory scrutiny, and reputational damage were all additional consequences. The cost of a third-party cyber breach is typically 40% more than remediating an internal security violation—which bumps up third-party risk management considerably high on CISOs' priority lists.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Confidentiality, integrity, and availability are three focal points. Who has data access, is it valid, and how can authorized users access it? CISO leaders have to manage these three things internally and across their vendor community.

Cybersecurity firms can evaluate potential partners' security posture without direct involvement, but organizations often struggle to identify which vendors have read or write permissions to sensitive information. Manual procedures and fragmented data frequently hinder efficient vendor assessments, making them complicated and time-intensive. In essence, it is difficult to understand context when monitoring entirely from the "outside-in"

Let's take a closer look at the expanding attack surface, the blind spots to clear, and how to manage risks accordingly.

The Expanding Attack Surface

Malicious actors can exploit weaknesses in the third party's systems or connections, often with less effort than attacking the primary target directly. Supply chain attacks, targeting third-party vendors, directly affected 134 organizations and indirectly impacted 657 more, exposing over 203 million individuals.

Since supply chain attacks occur through vulnerabilities in another element of the value chain, the compromised third party might already have trusted access or connections. The attackers can leverage these to gain unauthorized access to sensitive systems or data, bypassing many security measures.

Dynamic environments with multiple access points and shared resources, such as cloud environments and IoT contribute to the Third-Party Risk Management (TPRM) challenge. Businesses also need to be careful with remote workers, particularly if they handle sensitive data as employees may use personal devices or networks that are not adequately secured.

The Third-Party Risk Blind Spot

TPRM is often neglected or under-resourced. Common reasons include a lack of visibility into third-party security practices, overreliance on self-attestations as opposed to independent verification, and limited staff dedicated to TPRM.

More than 62% of respondents reported a lack of resources as the biggest obstacle to better safeguarding their organizations from third-party breaches. Almost two-fifths (37%) said they need to double their current staff dedicated to third-party security.

Not only are organizations relying on a mounting number of service providers, but these providers are also gaining customers, increasingly complicating the attack surface. Since not all parties have the same risk level, they will also have varying security measures. Failing to assess data security throughout the relationship lifecycle, including vendor's data processing, transfer, storage, and disposal security measures, can create vulnerabilities.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Shadow data is a critical third-party risk blind spot. This unmanaged data resides in unknown locations, often with third parties, and was the source of 35% of breaches in 2024. These breaches are more expensive ($5.27M average), take longer to detect (26.2% longer), and more time to contain (20.2% longer, 291 days total). Because organizations lack visibility into shadow data, assessing accurate third-party risk in-house is increasingly tricky to achieve.

A Practical Framework for Effective TPRM

Risk management is no longer a "nice-to-have." Nine in 10 respondents say their organization has directly invested in their TPRM program. However, a lack of strong program coordination is evident, as only 31% of respondents describe their program as highly coordinated. While 51% report some coordination, this suggests significant room for improvement.

Without proper coordination throughout the risk management lifecycle, they can end up wasting resources and creating new blind spots. The key principles to follow include:

- **Identify and Classify:** Organizations need a comprehensive inventory of all third-party relationships and must classify them based on risk level (data access, criticality of services, etc.). This must be updated every time a change (such as a new supplier, or a software update) happens to any party involved.
- **Due Diligence:** The essential elements of third-party due diligence include security questionnaires, on-site audits (for high-risk vendors), penetration testing, and vulnerability scanning. CISOs can leverage the Shared Assessments Standardized Information Gathering (SIG) questionnaire to help build, customize, analyze, and store vendor assessments for managing third-party risk.
- **Continuous Monitoring:** The most crucial—and laborious part—is the ongoing monitoring of third-party security posture. Cybersecurity software that can automate and streamline workflows within this process helps.
- **Contractual Obligations:** Get it right from the beginning with transparent, thorough security and data protection clauses in third-party contracts. However, don't get too comfortable. These need to be checked and reworked overtime.
- **Incident Response Planning:** A joint incident response plan with key third parties will protect you with a contingency plan if (and when) an unexpected event occurs.
- **Communication and Collaboration:** The more up-to-date with each other you are, the better. Aim for open communication and collaboration with third parties on security matters.

With the scale and uses of third parties across an organization's supply chain, CISOs must rethink their data lifecycle and how to protect it in all its states. They must think about securing data from theft and manipulation, and assess all access points across their third-party networks. Organizations can use data discovery and classification to detect sensitive data and ensure the correct access controls and encryptions are in place. By working with third-party security teams and centralizing TPRM, they can gain better visibility into shadow data, spot malicious drifts more quickly, and ensure proactive measures are in place to prevent data leakage.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author

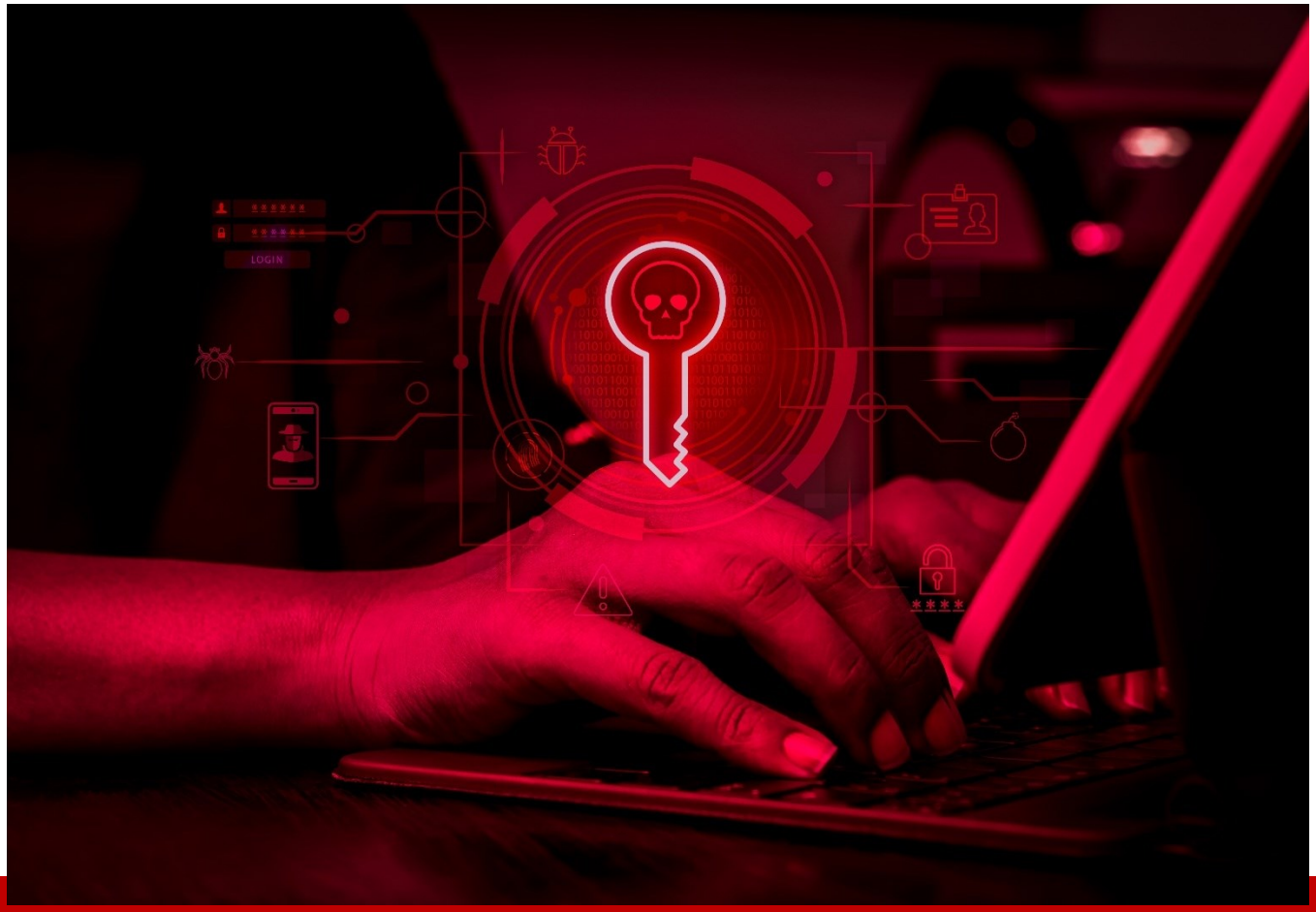


Norman Menz, CEO of cybersecurity SaaS platform Flare. He joined the company in 2021. Earlier in his career, Norman developed a number of information security and IT risk programs but decided to focus his attention on the biggest information security risk to organizations; which is the loss of data due to third-party relationships. Norman is a thought leader on third party and external information security risk and regularly speaks at industry events on the importance of understanding and mitigating risk associated with third parties. He is a Certified Third-Party Risk Professional (CTPRP) and a contributor to the Shared Assessment's Risk Assessment Body of Knowledge.

Norman received his university degree in Business Management and has been pursuing entrepreneurial activities in technology since before becoming a Seton Hall University Pirate.

Norman can be reached on LinkedIn and at our company website https://flare.io/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Key Cybersecurity Themes for 2025

Insights from Fortra's Global Survey on Risks, Challenges, and Priorities

By Rohit Dhamankar, Vice President of Product Strategy at Fortra's Alert Logic

Cyber threats are evolving faster than ever, and security leaders can't afford to fall behind. That's why we created the 2025 Fortra State of Cybersecurity Survey—to provide valuable insights that help SOCs, CISOs, and other cybersecurity decision-makers shape their strategies for the year ahead.

The report compiles insights from 12 key cybersecurity roles —analysts, developers, architects, directors, and executives) spanning 24 industries worldwide, drawing from Fortra's 25,000+ global customers.

For security leaders, staying ahead of these trends is critical. The survey provides a data-driven look at the biggest risks organizations face, helping you make informed decisions, allocate resources effectively, and strengthen your cyber resilience.

Instead of diving into every statistic, let's focus on some of the most compelling findings from this year's survey.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Risks & Challenges: The Evolving Cyber Threat Landscape

Social engineering, phishing, and smishing attacks remain the top concern for cybersecurity practitioners this year. Advancements in Generative AI (Gen AI) are amplifying these threats, making them more sophisticated and harder to detect. Fortra's email security and data risk teams are also seeing an increased volume of Gen AI actively leveraged in next-generation phishing, smishing, and social engineering attacks. Given the explosion of sites, tools, and services leveraging emerging technologies like GenAI, it's not surprising that the number of security professionals identifying evolving technologies as a primary security threat has increased from 35% to 50% YoY. Security leaders are increasingly worried about AI-powered attacks targeting their organizations and the ability of their defenses to counter AI-driven threats. Businesses rushing to adopt AI must ensure data scientists and consultants are not inadvertently exposing sensitive data, leading to compliance violations or reputational risks.

The perceived risk of zero-day attacks has decreased 12% from last year. Does this mean zero days are disappearing? Absolutely not. Just last month, both Apple and Microsoft released patches for critical zero-day vulnerabilities. The difference is how the industry has evolved. Years ago, zero-days caused chaos. Today, security teams have well-defined playbooks to mitigate the impact, making responses faster and more effective.

Top Cybersecurity Initiatives for 2025

When asked about their top security initiatives for the coming year, 77% of security experts said that identifying and closing security gaps was first on their list. This initiative is a foundational defense strategy to strengthen cybersecurity posture. Security teams can't predict when or how they will be attacked, but they can proactively reduce their attack surface.

Improving security awareness and culture took the number two spot, increasing to 75% from 66% last year. Employees remain the weakest link in cybersecurity, with industry reports (e.g., Verizon Data Breach Investigation Report) highlighting phishing and credential theft as top attack vectors. Looking ahead, AI-powered phishing campaigns demand that cybersecurity awareness training be stronger than ever.

Cloud security prioritization may no longer be a top initiative, down to 54% from 63% last year. This should not be taken to mean that organizations are ignoring cloud security. Cloud is now a standard operating environment, with 91% of respondents already using cloud in some form. It is also embedded into vulnerability management, attack surface monitoring, prevention, detection, and response—rather than being treated as a standalone priority.

Challenges in Implementing These Initiatives

Budgetary constraints increased to 59% this year from 54% last year, remaining one of the top challenges organizations face. To make the most of their cybersecurity budget, organizations need to spend wisely. This means focusing on tools that strengthen security, cutting out the unnecessary, and aligning efforts

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

with business goals to reduce risks and stay ahead of threats without overspending. Organizations can optimize security spending by:

- Assessing: Where does the organization stand in the cybersecurity maturity model? Regular evaluations help identify gaps and areas for improvement.
- Preventing & Detecting: Identifying strengths and weaknesses in the security stack. A proactive approach ensures threats are mitigated before they cause harm.
- Optimizing & Consolidating: Eliminating redundant tools and evaluating ROI on security investments. Streamlining security solutions enhances efficiency and reduces costs.
- Responding: Building scalable security programs aligned with business goals. A well-structured response strategy minimizes disruption and strengthens resilience.

Tools & Vendors: The Case for Security Consolidation

Security vendor consolidation is accelerating, with over 70% of respondents reducing their number of vendors to less than 10, a significant shift from the 30+ vendors many organizations relied on a few years ago.

Organizations consolidating vendors should ask:

- Are we covering the full kill chain?
- Are redundant tools eliminated?
- Are compliance requirements met (especially for regulated industries)?

Security tool sprawl is a real problem for many organizations. As companies grow, they often end up with too many tools that overlap, making it harder to manage effectively. This not only leads to higher costs but can also create gaps in protection. Streamlining security tools is key to improving efficiency and ensuring better coverage. Consolidation can:

- Reduce costs
- Improve efficiency
- Strengthen security outcomes

Staffing: The Need for Specialized Security Talent

Don't spread your security budget too thin. Cybersecurity is not a "peanut butter" budget problem and resources must be allocated strategically. Certain functions, like penetration testing, require deep expertise and specialized skills.

60% of respondents report outsourcing penetration testing. This is a smart approach because it provides:

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

- A fresh, outside-in perspective on vulnerabilities
- Advanced expertise not available in-house
- Cost savings compared to hiring full-time specialists

Security services will continue to grow, with email security and vulnerability management (VM) being the next major areas outsourced, in addition to penetration testing. The security services market is projected to generate as much revenue as security products in the coming years.

Outsourcing security services gives organizations the chance to tap into expert help and resources that make security stronger and more efficient. By working with outside providers, businesses can stay on top of new threats without stretching their teams too thin. It helps fill in any gaps, speeds up response times, and scales as needed, all while letting companies focus on what they do best.

- Outsourcing security services provides:
    - 24/7 security coverage
    - Faster incident response times
    - Hybrid models where some functions remain in-house while others are outsourced

Final Thoughts: A Call to Action for Cybersecurity Leaders

The cyber threat landscape is evolving faster than ever, driven by AI-initiated attacks, social engineering, and cloud-based vulnerabilities. To protect against these threats, organizations must strengthen security awareness programs, optimize security tool investments, and address staffing shortages. Security leaders must not only defend against today's threats but also prepare for the threats of tomorrow—because in cybersecurity, complacency is the biggest risk of all.

About the Author



Rohit Dhamankar is the Vice President of Product Strategy at Fortra's Alert Logic. Rohit has more than 20 years of security industry experience across product strategy, threat research, product management and development, and customer solutions. Dhamankar holds a Master of Science in Electrical Engineering from the University of Texas Austin and a Master of Science in Physics from IIT in Kanpur, India.

He has worked in leading and advisory roles for many successful start-ups and Texas based VCs. Rohit has spoken at RSA, Black Hat and other cybersecurity industry conferences. In addition, he worked with the SANS Institute for many years authoring industry-driving reports and newsletters.

Follow Rohit on LinkedIn.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Unpacking Disinformation in the 2024 US Presidential Election

By Hannah Baumgaertner, Head of Research at Silobreaker

The 2016 U.S. presidential election is often cited as a watershed moment for digital disinformation campaigns – revealing the vulnerability of democratic processes to foreign interference and the spread of false information. But since then, elections across the globe have become prime targets for sophisticated influence operations and disinformation campaigns.

Over the past year, nation-state actors have actively sought to sway voter opinions and outcomes. Disinformation is not just about spreading lies, but about engineering doubt, eroding trust and fracturing societal cohesion through algorithmically precise narrative manipulation. These efforts were notably amplified using artificial intelligence (AI), allowing campaigns to spread false narratives efficiently. Countries such as China, Russia and Iran notably adapted their tactics to exploit U.S. societal divisions, using AI-enhanced tools to disseminate their messaging widely. Their efforts also involved leveraging social media platforms to spread disinformation.

Looking ahead, disinformation campaigns are expected to continue their influence not only throughout the election process but also into the post-election period, particularly as Donald Trump prepares for his

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

inauguration. With this in mind, let's examine the various disinformation campaigns which ran over the course of the lead-up to the 2024 U.S. presidential election and how these campaigns might evolve in the critical months to come.

China's Spamouflage influence operation

The Spamouflage influence operation, active since at least 2019 and widely attributed to the Chinese government, has been evolving its tactics to align with geopolitical objectives. Known alternatively as Dragonbridge or Storm-1376, the campaign began focusing on the U.S. presidential election in mid-2023.

Graphika researchers uncovered the operation's extensive use of social media accounts impersonating U.S. citizens, soldiers and advocacy groups. These accounts strategically distributed AI-generated content targeting both Democratic and Republican candidates, aiming to undermine the electoral process and exacerbate social tensions around an array of topical issues to sway voters, including gun control, homelessness, racial inequality and the Israel-Hamas conflict.

The campaign targeted prominent political figures, including Joe Biden, Donald Trump, Kamala Harris and Marco Rubio. Clemson University researchers identified that Spamouflage has been targeting Rubio with fake news since his re-election bid in 2022. Microsoft also observed Spamouflage using AI-generated news broadcasts and AI-manipulated imagery to fuel conspiracy theories. The tactics targeting Rubio have notably evolved since 2022, with hacked accounts and higher-quality disinformation spread across platforms like Medium and social media sites X and TikTok.

While primarily focusing on presidential candidates, Spamouflage demonstrated a willingness to target a broader range of political figures, adapting its strategies to maximise potential political and social disruption.

Iran's hack-and-leak tactics

In May 2024, Iranian-linked cyber actors infiltrated personal accounts of Donald Trump's presidential campaign, obtaining non-public campaign documents and emails. By June 2024, these hackers escalated their operation, initiating a 'hack-and-leak' strategy using the persona 'Robert' to distribute stolen materials to media outlets and Biden campaign-adjacent individuals.

In August 2024, POLITICO reported receiving anonymous emails containing internal Trump campaign documents, which the campaign confirmed were the result of a hack by foreign sources. A Microsoft report detailed the Iranian government-linked cyber activities. Two types of activity were observed, the first of which concerned influence campaigns to stoke controversy and sway voters, and the second aiming to gain intelligence on political campaigns to influence future elections. Multiple Iranian Revolutionary Guard Corps (IRGC)-affiliated actors with links to election interference were identified, including Peach Sandstorm, Lemon Sandstorm, Mint Sandstorm, and Cotton Sandstorm. Google researchers corroborated these findings, attributing the campaign to APT42.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The U.S. Department of Justice responded in September 2024 by indicting three Iranian nationals employed by the Iranian Revolutionary Guard Corps (IRGC). The indictments alleged a coordinated effort to undermine U.S. electoral processes by sowing discord and gathering intelligence. Despite legal action, the 'Robert' persona continued to contact news organisations, with some publications verifying and publishing portions of the leaked documents.

Russia's Doppelganger campaign

The Russian influence campaign Doppelganger, which originated in 2022 during the Russia-Ukraine war, has continuously adapted its strategies. In 2024, the campaign pivoted to target global elections, initially focusing on the European Parliament election through propaganda and disinformation about socio-economic and geopolitical issues.

Doppelganger employs diverse disinformation techniques, including typosquatted domains mimicking news websites AI-generated social media content and deep fake videos to spread its messages, while also amplifying messages from another Russia-linked operation, CopyCop. By September 2024, the U.S. Department of Justice seized 32 internet domains linked to the campaign and indicted two RT employees for covertly creating and distributing election-related content.

Previous research by Qurium revealed Doppelganger's connections to European cybercriminals and advertisement networks. The campaign has since adapted, attempting to discredit disinformation experts like Eliot Higgins and Christo Grozev to deflect accusations of Russian involvement. This shift may be a response to the DOJ's September affidavit implicating the Social Design Agency in operating the Doppelganger campaign.

Key trends in election disinformation

State-sponsored influence campaigns are continuously adapting their techniques, with AI becoming a critical tool in disinformation strategies. The U.S. Foreign Malign Influence Centre predicts ongoing use of AI-generated social media content, exemplified by Russia-linked deepfake videos targeting political figures and Iranian hacker groups using AI to generate election-related narratives.

These campaigns demonstrate remarkable agility in exploiting current events. For example, the assassination attempt on Donald Trump quickly generated numerous conspiracy theories, while other operations leveraged events like hurricanes and university protests to spread divisive messaging.

Ultimately, these influence operations aim to erode public trust and create social discord, but the impact of these campaigns is wide ranging. Cybersecurity risks like phishing attacks are multiplied, as disinformation campaigns can be used to lure employees into clicking on malicious links or downloading malware. Disinformation campaigns can spread false information about a company, and even lead to stock market volatility.

For organisations, staying ahead requires robust threat intelligence to anticipate and mitigate the ripple effects of disinformation. By seeing the bigger picture, businesses can effectively plan and address

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

emerging risks. The 2024 U.S. presidential election demonstrated that in an era of AI and global connectivity, disinformation not only threatens public trust and political stability, but also corporate security and economic markets worldwide.

About the Author

Hannah Baumgaertner is Head of Research at Silobreaker. Hannah can be reached at our company website www.silobreaker.com

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Rethinking SAP Security Without Maintenance Contracts

By Ken Conz, Director of Technical Operations, Spinnaker Support

Do you rely on SAP maintenance contracts to keep vulnerabilities in check? Here's a question: have you felt the sting of renewal season? Those spiraling costs are hard to ignore—just like the rising threats and security compliance headaches. No wonder so many organizations, maybe even yours, are asking: Do we really need to keep paying for vendor protection, or could we handle SAP security ourselves?

Yes, ditching the maintenance contract can save cash, but it's about something far more fundamental: reclaiming control, building in-house expertise, and fostering a proactive security mindset. Self-sufficiency in SAP security isn't without its challenges, but for organizations ready to face them, the rewards—resilience, autonomy, and agility—are worth every bit of effort.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Breaking Away from Vendor Dependency

For decades, SAP security was synonymous with vendor control. The maintenance contract model provides a sense of security, but it also creates a culture of dependence. When security updates and patches are outsourced, companies often overlook their own role in shaping a strong security posture. But, as we all know—and are constantly reminded of — in today's cybersecurity climate, this passive approach simply isn't enough.

That's why many organizations are recognizing the need to take ownership of their SAP security – so that they can adapt to real-time threats and compliance demands with the urgency they demand.

So, what's required to take SAP security in-house? It starts with building a proactive security culture.

Make Security a Company-Wide Mission

SAP security can't be siloed within IT—it needs to be a team sport. Everyone, from the finance team to marketing, plays a part in securing data. Moving beyond vendor reliance means encouraging a proactive security culture where every department understands the basics of data protection and recognizes potential threats and vulnerabilities.

Upskilling and Knowledge Sharing

Self-reliant security relies on empowered teams. Staff trained in SAP security fundamentals become assets capable of identifying and handling issues early. By investing in SAP-specific training and fostering a culture of shared knowledge, companies build an internal security force that's both proactive and prepared.

Adaptability and Continuous Improvement

Cyber threats evolve constantly, and so must security practices. Self-managing SAP security pushes organizations to adopt a cycle of continuous assessment and improvement. Regular audits, updates on emerging threats, and timely adjustments create a security framework that is both agile and resilient.

Naturally, taking SAP security in-house isn't without its challenges. But with the right attitude and approach —and some creative thinking—your team can thrive:

Resource Constraints

Robust SAP security without vendor support can strain resources, especially for smaller businesses. Creative strategies—like reallocating budgets, leveraging automation, or bringing on security consultants—can help organizations enhance security without overextending their teams.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The Learning Curve

Not every team is ready for SAP security independence. Knowledge gaps can pose real risks, but they're surmountable. Partnering with SAP-specific consultants or tapping into community-driven resources helps bridge these gaps, offering insights and support at a fraction of the vendor cost.

Resistance to Change

Shifting to greater security ownership can feel overwhelming, especially for employees used to vendor-driven security. Leaders need to communicate the importance of a self-sufficient approach and support teams through this transition, showing how it benefits the business both strategically and financially.

But why make the effort? What is it about managing SAP security independently that's worth taking on these hurdles?

Key Drivers for Reducing Vendor Dependency

Cost savings may be the obvious answer, but they're just the beginning.

Faster response times, stronger cybersecurity, and streamlined compliance are all part of the equation. Plus, new tools and technologies—like AI, machine learning, and cloud security—have empowered organizations to secure their SAP systems independently, without the constraints of exclusive vendor ties.

The transition to self-sufficiency involves a few critical changes, but these steps build a strong, responsive framework that truly fits your business.

Set and Monitor Access Limits

Role-based access control (RBAC) ensures that employees have only the permissions they need to do their jobs, reducing the risk of internal breaches. This granular control goes beyond static security by continuously adjusting SAP settings to align with best practices and creating a secure, adaptable structure.

Routine Audits for Real-Time Awareness

With autonomy comes responsibility. Regular SAP security audits—covering access logs, vulnerability scans, and simulated attacks—spot gaps before they turn into problems. By viewing audits as proactive defenses rather than compliance checkboxes, companies gain an acute awareness of their security posture.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Third-Party Support Providers on Your Terms

Going self-sufficient doesn't mean going solo. A range of third-party support providers specialize in SAP security, offering services from risk assessments to incident response. By choosing engagements selectively, companies strengthen security without the cost of long-term contracts, bringing in expertise only when it's most valuable.

The Payoff: Agility, Savings, and Resilience

Taking SAP security into your own hands means faster responses, real savings, and a security setup that fits your business like a glove. Moving beyond maintenance contracts doesn't just strengthen your defenses—it builds a culture where every team member has a stake in keeping systems secure. For companies ready to ditch the dependency, the payoff is clear: more control, more resilience, and a team that's empowered to tackle today's cybersecurity challenges head-on.

Embrace the shift, and make SAP security work for you, on your terms.

About the Author



Ken Conz is the Director of Technical Operations at Spinnaker Support, where he oversees technical support services for enterprise software like SAP, Oracle, and Salesforce. Based in the Greater Phoenix Area, he leads a team that ensures high-quality assistance and tailored solutions for clients. With a strong background in technical operations and enterprise software systems, Ken has played a key role in Spinnaker Support's reputation for excellence in delivering customer-focused services.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Is Someone Lurking in The Background Waiting To Impersonate You?

Cybercriminals Are Hiding in Plain Sight

By Dave Smolensky, Founder and COO, Resolute Strategic Services

Are you confident someone isn't lurking in the background on your computer right now, gathering information and preparing to impersonate you? The era of confidently sending e-mails securely or answering the phone and knowing the caller on the other end has vanished. Today, unprecedented technological advances drive efficiencies and capabilities unimaginable 20 years ago, but they come at a steep price for the unprepared.

Cybercriminals are constantly looking for opportunities to gain access to your personal and financial information by employing tactics such as phishing, malware and exploiting outdated software. This is nothing new and it's essential you understand these entry points in your efforts to prevent potential threats.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Another tactic commonly experienced is when a cybercriminal breaches your system and lurks in the background to eventually impersonate you and steal unsuspecting victims of their funds. This tactic is a form of business e-mail compromise, where a bad actor infiltrates your e-mail, silently monitoring in the background and observing for weeks or even months, gathering a variety of information, including your communication habits, client information and financial insights.

Here's how it works

Let's use a CPA who has a small accounting firm as an example. The CPA is conducting business as usual and unknowingly is being monitored by a bad actor who breached the CPA's network two months earlier and has been monitoring the CPA's incoming and outgoing e-mails.

The goal of the bad actor is to gain enough insight about the CPA and the business, to eventually impersonate the CPA and trick clients into paying legitimate invoices from the CPA to a bank account controlled by the bad actor.

Having infiltrated the CPA's e-mail for two months without anyone's knowledge, the bad actor reaches a point when they are confident, they have the information necessary to impersonate the CPA. With the information in hand, the cybercriminal opens a bank account using a false identity and then begins impersonating the CPA by sending e-mails to the CPA's clients. The bad actor engages directly with one or more of the CPA's clients with carefully crafted messages, adopting the tone and business information only the CPA would know. This all happens without any knowledge by the CPA.

The e-mails become electronic conversations between the bad actor and the unsuspecting clients for several days until the bad actor casually inserts into the conversation news regarding the CPA's "new bank account." This new bank account is not the CPA's account, but instead the account the bad actor opened under a false identity. The bad actor continues the casual conversation reminding the client to direct payments for open invoices to the new account.

Surprise, your money is gone

The client, having no reason to believe the CPA's e-mail has been infiltrated, assumes the e-mail correspondence is legitimate and the new bank account information is accurate. The client pays an invoice as normal, but the money is directed to the bad actor's account instead of the CPA's account.

Weeks later, the CPA reaches out to the client regarding an open invoice that hasn't been paid. The client responds surprisingly and informs the CPA the invoice has been paid and even reminds the CPA of "their recent correspondence," which included the e-mail regarding the new bank account information.

It's at this point, after some investigation with the CPA's IT team, the CPA learns its e-mail had been compromised and the bad actor has been in the background intercepting and sending e-mails without the CPA's knowledge. Worse, the "new bank account" receiving funds has been emptied by the bad actor, with no means to retrieve the stolen funds.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The moral of the story

Advances in technology offer new opportunities for both the good guys and the bad guys. Always maintain vigilance and be sure to implement robust cybersecurity practices, including regularly updating software, using strong passwords and leveraging reputable security tools. And when it comes to conducting financial transactions via wire, ACH, Zelle, Venmo or any of the numerous financial instruments available today, verify the account information you are sending the funds to is legitimate.

It doesn't matter how familiar you believe you are with the person or organization you are sending funds too. Always take a few minutes and pick up the phone and confirm the account information you have is correct. A couple minutes spent on due diligence may save you from significant financial loss and shield yourself from the emotional toll of falling victim to a scam.

About the Author



Dave Smolensky is the Founder and COO of Resolute Strategic Services. With more than 30 years of communications experience, Dave is a highly respected leader in crisis communications and cyber incident response. His expertise spans a wide range of industries, including manufacturing, healthcare, finance, education and entertainment including some of the nation's largest outdoor music festivals. Dave specializes in strategic communications and reputation management, helping organizations navigate the complexities of cyber threats and crises before, during and after they occur.

Dave serves as a strategic advisor to the C-Suite, guiding organizations in vulnerability assessment, proactive preparedness planning and incident response testing. His clients trust him for his thoughtful, responsive counsel and his ability to solve complex problems under pressure.

Dave can be reached online at dave.smolensky@resolutestrategicservices.com or https://www.linkedin.com/in/david-smolensky-a724bb/. Visit our website https://resolutestrategicservices.com to learn more.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



The CMMC Compliance Journey

How to be Successful

By Jason Miller, Founder & CEO, BitLyft

The Cybersecurity Maturity Model Certification (CMMC) is a cybersecurity framework designed to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within the defense supply chain. Still, it is increasingly relevant for organizations beyond the defense sector.

Over 80% of government contractors consider CMMC compliance a deciding factor in securing new contracts. By becoming CMMC compliant, businesses can increase their contract opportunities, enhance customer trust, gain a competitive edge, reduce cybersecurity risks, and simplify regulatory compliance. CMMC compliance enhances trust, opens access to DoD contracts, and differentiates businesses from competitors lacking certification.

Companies need to achieve CMMC compliance, which involves implementing specific practices and controls based on the certification level required by their contracts. CMMC enhances cybersecurity

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

across the defense supply chain by ensuring contractors meet stringent standards for protecting sensitive information. However, other federal agencies are exploring similar certification requirements to secure their websites. Commercial industries are starting to require CMMC certification to enhance their cybersecurity environment.

CMMC is the Future of Cybersecurity

CMMC ensures a higher level of accountability and compliance. Its tiered structure allows organizations to implement security measures appropriate to the sensitivity of the data they handle, creating a scalable and adaptable framework. The key reasons that CMMC is the future of cybersecurity include:

- **Protects National Security**

CMMC ensures that contractors safeguard sensitive information, reducing vulnerabilities in the defense supply chain. This proactive approach is vital for maintaining national security in an era of escalating cyber threats.

- **Enhances Accountability**

By requiring third-party certification, CMMC eliminates the inconsistencies of self-assessments. This ensures that contractors not only adopt but also maintain robust cybersecurity practices.

- **Builds Trust in the Supply Chain**

CMMC fosters trust among federal agencies, contractors, and subcontractors by creating a standardized approach to cybersecurity. This trust is essential for collaboration and long-term partnerships.

- **Adapts to Future Threats**

With its emphasis on continuous improvement, CMMC provides a scalable framework that evolves to address emerging threats and regulatory requirements, ensuring it remains relevant over time.

The CMMC Journey

- **Understand CMMC Requirements:** CMMC's tiered framework has five levels, each representing a different degree of cybersecurity maturity. Understanding the requirements specific to each level is crucial.
- **Prepare for CMMC Certification** by:
    - A gap analysis will assess the current cybersecurity posture against the requirements of the desired CMMC level.
    - Implementing the required controls outlined in the CMMC framework may include updating policies, deploying new technologies, and training staff.
    - Document policies and procedures thoroughly and allow these to be accessible for review during the certification process.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

    - Simulating the CMMC audit process by conducting an internal or third-party assessment to identify any remaining issues to prepare the company for an official audit.
    - Engaging with a certified third-party assessor (C3PAO) to ensure all requirements are met.
- **Implement Required Controls -** Based on your assessment, implement the security controls outlined in the desired CMMC level. These controls include access management, data encryption, and incident response planning.
- **Engage in Continuous Monitoring -** Monitoring your systems in real-time helps identify and mitigate emerging threats quickly, ensuring your organization remains compliant and secure.

What Happens if You Get Audited

A CMMC audit is an assessment conducted by a Certified Third-Party Assessor Organization (C3PAO) to determine if an organization complies with the required CMMC level. These audits evaluate an organization's implementation of cybersecurity practices and controls as outlined in the CMMC framework, which ranges from Level 1 (basic cyber hygiene) to Level 5 (advanced and proactive practices). Here is what to expect during your CMMC Audit:

- Your organization will submit the necessary documentation, including policies, procedures, and evidence of implemented security controls before the audit begins.
- Personnel will be interviewed, physical and digital systems will be inspected, and security practices will be verified.
- The assessor will compare your practices against the required CMMC practices.
- At completion, you will receive a report detailing your compliance status and any deficiencies that need addressing.

As cyber threats evolve, regulatory frameworks like CMMC are becoming the norm across industries. Achieving certification prepares businesses for future compliance demands and strengthens their overall cybersecurity posture.

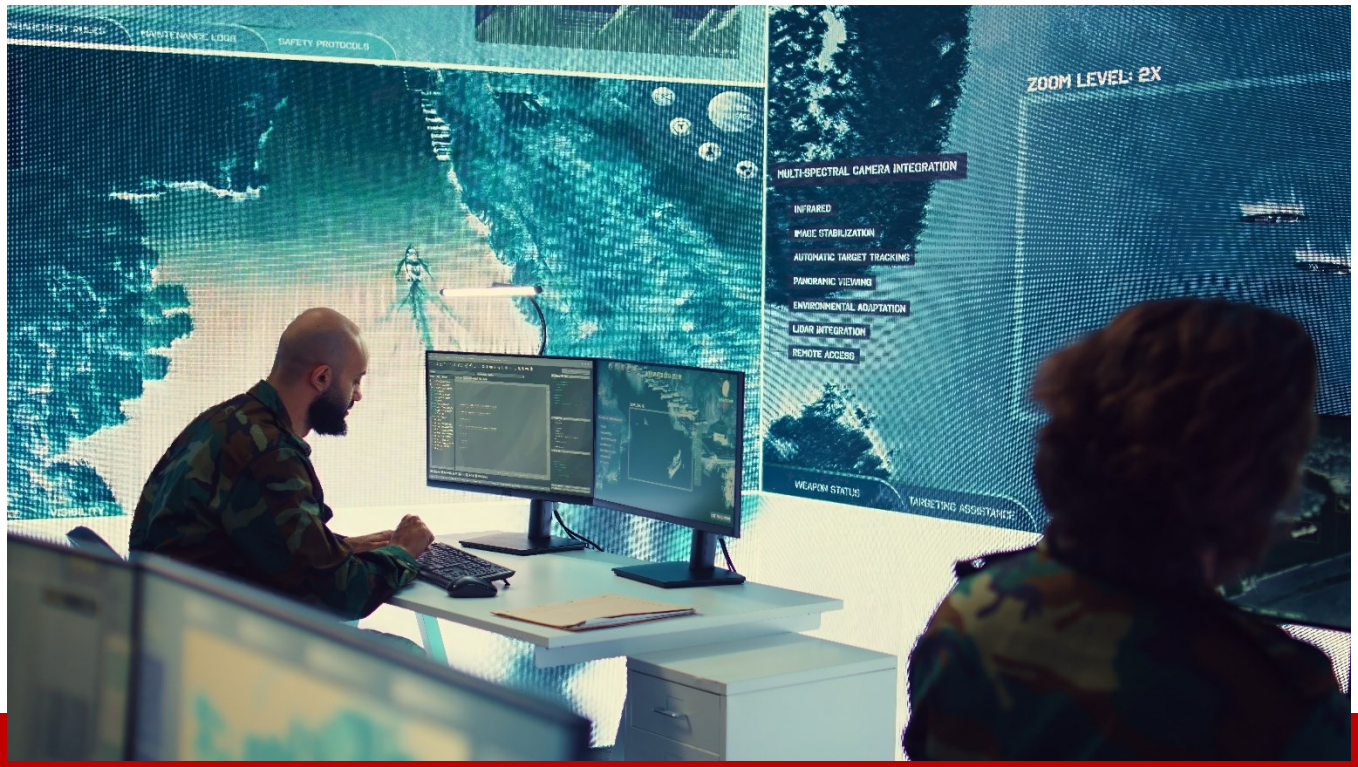
About the Author



My Name is Jason Miller, and I am the CEO and Founder of BitLyft, a leading managed detection and response provider (MDR). Establishing BitLyft in 2016, Jason set out to unburden security teams with innovative, approachable, and affordable solutions, a vision that has made BitLyft a respected managed detection and response provider.

Jason can be reached online at Jason.miller@bitlyft.com and at our company website www.bitlyft.com

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Why Eliminating the Cyber Safety Review Board Weakens Critical Infrastructure and Cyber Resilience

By Ramkumar Sundarakalatharan, CEO, Zerberus Technologies

"It's better to have cybersecurity and not need it than to need it and not have it." – Anon

The Cyber Safety Review Board (CSRB) was established to provide oversight, coordinate responses to major cyber incidents, and derive actionable insights to prevent future occurrences. Its recent disbandment raises pressing concerns about the security of critical infrastructure. At a time when ransomware attacks cost organisations an average of $4.35 million per incident (IBM, 2022), the absence of a unified body like the CSRB leaves critical gaps in our national cybersecurity strategy.

This article examines the consequences of the CSRB's dissolution through real-world case studies and offers a path forward to address its absence.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Case Studies: Lessons from Past Incidents

The Colonial Pipeline Ransomware Attack

The 2021 Colonial Pipeline incident remains a textbook example of how a single breach can escalate into a national crisis. Hackers exploited a compromised VPN password, deploying ransomware that disrupted the flow of nearly half the East Coast's fuel supply.

- **The Fallout:**

The attack caused panic-buying, long fuel lines, and economic losses across multiple states. Colonial Pipeline paid a $4.4 million ransom in Bitcoin, underscoring the crippling effects of inadequate preventative measures.

- **Lessons Learned:**
  - **Coordination Is Key:** A central body like the CSRB could have facilitated a streamlined review and generated actionable recommendations for the energy sector.
  - **Proactive Security Measures Save Costs:** As highlighted by *Tessian's analysis of IBM's 2022 Cost of a Data Breach Report*, organisations with incident response plans saved an average of $2.66 million per breach.

(References: IBM, 2022; ResearchGate, 2022)

Scottish Water's Teslacrypt Ransomware Attack

Scottish Water fell victim to the Teslacrypt zero-day ransomware, initiated via a phishing email with a malicious link. Once clicked, the malware encrypted files across the organisation, demanding ransom in Bitcoin.

- **The Response:**

Scottish Water's Cyber Threat Intelligence (CTI) service, managed by Fujitsu, quickly identified the threat, neutralised the malware, and partnered with Symantec to block further infections. The incident was reported promptly to the Drinking Water Quality Regulator for Scotland (DWQR) and escalated to the National Cyber Security Centre (NCSC).

- **Lessons Learned:**
  - **Zero-Day Threats Require Proactive Monitoring:** Despite updated antivirus systems, the new malware bypassed traditional defences, proving the need for continuous monitoring.
  - **Coordinated Reporting Frameworks Work:** The rapid involvement of DWQR and NCSC highlights the importance of structured incident reporting.

(References: Fujitsu Case Study)

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The Fallout of Disbandment

The CSRB's absence is likely to exacerbate existing vulnerabilities:

1. **Delayed Responses and Fragmented Learning:**
   Without a centralised entity, critical lessons from incidents like Colonial Pipeline and Scottish Water will remain siloed, delaying responses and limiting cross-sector improvement.
2. **Rising Supply Chain Risks:**
   The SolarWinds attack demonstrated how supply chain compromises ripple across industries. A unified body like the CSRB is essential to monitor and mitigate these risks systemically.
3. **Loss of Institutional Memory:**
   The CSRB was a repository for cybersecurity insights. Its dissolution risks the loss of long-term knowledge crucial for addressing evolving threats.
4. **Increased Geopolitical Vulnerabilities:**
   Cyberattacks by state-sponsored actors like China and Russia continue to target critical infrastructure. Coordinated oversight is vital to preempt and counteract such threats effectively.

A Path Forward: Reimagining the CSRB

To address the void left by the CSRB's disbandment, we need a regulator that strikes a balance—one with enough authority to ensure security is not sacrificed for innovation but without the overreach that stifles progress, as seen in certain heavily regulated markets like the European Union.

The CSRB was envisioned as the National Transportation Safety Board (NTSB) for the information highway—a central agency with investigative and intervention powers to analyse breaches, identify vulnerabilities, and recommend improvements. Without such a body, the digital landscape risks becoming a free-for-all where no one investigates the "crashes" or fixes the "planes." Here's how a reimagined CSRB could fulfil this critical role:

1. **Adopt a "Just Enough Regulation" Approach:**

The regulator must focus on enabling innovation while ensuring accountability. This means creating frameworks that encourage organisations to adopt proactive security measures without imposing burdensome compliance requirements that hinder growth.

2. **Empower Investigative and Intervention Capabilities:**

A reimagined CSRB should have the authority to investigate breaches comprehensively, identify root causes, and mandate necessary changes. Think of it as a proactive safety mechanism, not a punitive bureaucracy.

3. **Enhance Collaboration with Private Entities:**

Corporations are the engines of innovation, but unchecked innovation can lead to security lapses. By fostering partnerships between the regulator and private enterprises, the CSRB can ensure both parties

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

work towards shared security goals. For instance, companies could share anonymised threat data in exchange for tailored recommendations from the CSRB.

4. **Provide Clear and Actionable Guidance:**

As the NTSB provides precise recommendations to improve aviation safety, the CSRB should develop actionable guidelines for industries based on incident reviews. These guidelines would help organisations bolster defences without overhauling their operations unnecessarily.

5. **Focus on Prevention, Not Punishment:**

The goal should be to reduce the frequency and impact of cyber incidents, not to penalise organisations post-breach. By maintaining a non-adversarial relationship with businesses, the CSRB can ensure its focus remains on systemic improvement.

A reimagined CSRB is not just about oversight—it's about creating a safety net for the information highway, where innovation thrives within a secure and resilient ecosystem. It's time to bring this vision back, balancing innovation with the need for proactive security.

Conclusion

The disbandment of the CSRB creates a vacuum in national cybersecurity. Incidents like Colonial Pipeline and Scottish Water illustrate the critical role a unified body plays in coordinating responses, analysing systemic vulnerabilities, and safeguarding critical infrastructure. Reinstating or reimagining the CSRB is not merely an option—it's a necessity to protect our interconnected digital ecosystem.

References and Further Reading

IBM. Cost of a Data Breach Report (2022).

Read here

ICO. Incident Reporting Guidelines (2024).

Read here

ResearchGate. Ransomware Attacks on Critical Infrastructure: A Study of the Colonial Pipeline Incident.
Read here

Lepide. Colonial Pipeline Attack Case Study.

Read here

Fujitsu. Scottish Water Case Study.

Read here

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Editor's Note: This article is solely the opinion of the author, and publication in Cyber Defense Magazine does not imply endorsement of the content. We bring it to our readers as one side of the ongoing discussion on the necessity of continuing the Cyber Safety Review Board as part of the CISA. Others say that the CSRB is not a "regulator," and that the CISA itself already has the authority and resources to conduct the stated functions of the CSRB.

About the Author



Ramkumar Sundarakalatharan is the Co-Founder & CEO of Zerberus Technologies, a cutting-edge cybersecurity firm dedicated to simplifying automated security monitoring and compliance adherence. As an Information Security Researcher at the Royal Holloway, University of London, Ramkumar combines academic rigour with practical expertise to drive innovation in the cybersecurity landscape.

With over 20 years of experience spanning startups and multinational corporations, he is a recognised leader in cybersecurity strategy, Critical National Infrastructure (CNI) security, and governance frameworks. Ramkumar has developed and patented several groundbreaking technologies in automated threat detection and compliance adherence, contributing to the industry's evolution in safeguarding digital ecosystems.

An advocate for aligning cybersecurity with business value, Ramkumar has worked across diverse domains, from securing large-scale cloud architectures to advising enterprises on achieving ISO, PCI DSS, and SOC2 certifications. He is passionate about fostering resilience against emerging threats while enabling organisations to innovate securely.

You can connect with Ramkumar on **LinkedIn**, explore his insights on his blog **Nocturnalknight.co**, or learn more about his company at **Zerberus.ai**.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Effective Cyber Drills Must Mirror the Realities of The Battlefield

To Stop a Cyberattack, Act Like It's the Front Line

By Dr. Oleksii Baranovskyi, a Certified Cybersecurity Expert (CISSP, CISM, CCISO), trainer for TRYZUB Cyber Drills, CYBER RANGES

Over the past 15 years, cyberattacks have escalated dramatically.

What began as isolated data breaches has evolved into sophisticated operations targeting critical infrastructure and serving intelligence-gathering objectives.

The turning point came in April 2007, when Estonia faced a coordinated series of DDoS attacks, which disrupted government websites, online banking services, and communication networks altogether.

Since then, cyberattacks have been recognized as strategic threats capable of undermining national stability. Yet, their scale and impact continue to grow at a rate that outpaces expectations.

In the third quarter of 2024, cyberattacks worldwide surged by 75% compared to the same period in 2023. This amounts to ~1876 cyberattacks per organization, with the most targeted entities being educational, research, government, and military institutions. Expectedly, these attacks often result in the shutdown of essential services and pose risks to public safety and well-being.

In commerce, the primary goal of cyberattacks is financial gain. Nearly half of affected organizations report financial losses exceeding $500,000 per incident. However, when critical infrastructure and military operations are targeted, the stakes shift dramatically.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The cost is ultimately human lives.

Back in 2007, in a controlled experiment, the Idaho National Laboratory performed a cyber intrusion that caused a 2.25 MW diesel generator to torque abnormally and stop operations. Just three years later, the U.S. and Israel – reportedly – deployed the Stuxnet virus into Iran's nuclear plant systems. The malware caused multiple centrifuges in the facility to operate in a way that reduced their lifespan. It doesn't take a genius to see the consequences if the goal had been more cold-blooded.

Today, cyber warfare is directed at satellite communications, rocket guidance systems, and interconnected multi-domain operations. Its reach extends to all kinds of hardware, where its destruction can trigger widespread panic or catastrophic disruption within a nation under attack.

In Ukraine, Russian forces consistently use cyberattacks to pave the way for missile and UAV strikes, a situation the Ministry of Energy recognizes as the new normal. They target power plants, communication networks, and other critical systems.

In one such incident in December 2024, a successful strike on Ukraine's state registries disrupted their operation for several weeks. The immediate missile attack afterward resulted in one fatality and nine injuries, not to mention power outages.

Just a couple of years ago, such scenarios were hypothetical exercises discussed at cybersecurity conferences. Today, they are an everyday reality for all Ukrainians.

When cyberattacks are tightly coordinated with kinetic warfare, they require precision timing to achieve strategic objectives. Defense systems must respond instantly: each cybersecurity team member is expected to understand their role and act decisively to counter or mitigate the effects of an attack as quickly as possible.

Today, cybersecurity teams in Ukraine enhance their effectiveness in withstanding strikes effectively through rigorous training. Their prime objectives include:

- reducing incident response time
- minimizing service restoration time
- shortening investigation and attack attribution periods
- accelerating deterrence efforts
- and limiting the damage inflicted.

To learn how to act specifically in high-stakes situations, cybersecurity teams take part in drills that emulate real-world attacks.

The focus in such emulations is response speed. When time is critical, people rely on instincts rather than deliberate reasoning, much like when a driver reacts instantly to avoid a crash. This means effective deterrence of cyberattacks requires automation and instant execution of necessary decisions and actions that can only be achieved during emulations.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

In Ukraine, specific approaches have been designed to engage military personnel in deep-dive, realistic attack scenarios. Emulations replicate tactics used by Russian state-sponsored threat actors that have been engaged in cyber espionage and cyber sabotage since at least 2013.

Regular participation in threat emulations has already proven to enhance teams' ability to cope with stress and improve incident response capabilities.

The number and frequency of cyber incidents reveal that no country is immune to state-sponsored cyber aggression.

In November 2024, the UK's Defence Minister warned NATO that adversaries, including Russia, are already leveraging AI to enhance their cyberattack capabilities and disrupt the UK's power grid. On New Year's Eve, the pro-Russian NoNaMe collective struck the websites of several French cities in retaliation for Ukraine's support. Around the same time, China-backed hackers breached US Treasury workstations.

Such attacks are designed to destabilize societies by targeting critical infrastructure, spreading panic, and leaving nations more vulnerable to subsequent strikes.

Rather than waiting to learn from their own costly mistakes, countries and businesses prefer to benefit from the hard-earned lessons of others. Through cross-border partnerships and jointly developed cyber drills, such as the US-Ukraine TRYZUB, cybersecurity teams can gain war-tested experience without being thrown into the eye of the storm.

The ultimate goal in cyber warfare is to reach a point where deflecting cyberattacks becomes second nature and where teams act with the same speed and precision as soldiers on a battlefield who rely on instinct and muscle memory to counter threats under pressure.

By building alliances and training relentlessly, we can create a united front capable of withstanding even the most sophisticated attacks and ensure our critical infrastructure, public safety, and way of life are protected from anyone who seeks to undermine them.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Dr. Oleksii Baranovskyi is a distinguished figure in the field of Ukrainian Cybersecurity.

Oleksii is an accredited instructor for prestigious organizations like (ISC)², ISACA, and EC-Council. His contributions to cybersecurity education have been honoured with international awards, underpinning his role as a global educator by EC-Council Instructor (CEI) Circle of Excellence Award in 2022 and the ISACA Educational Excellence Award in 2024.

Oleksii is known for his dedication to public service in cybersecurity with trainings and educational programs, for which he has been commended with national honours acknowledged with the National Security Council order "Defender of Ukraine" in 2020 and medal of honour by State Service of Special Communication and Information Protection of Ukraine (SSSCIP) for his impact of creating and development of cyberpolice and national cybersecurity capabilities. as well as recognitions by OSCE, USAID, the National Bank of Ukraine and the National Police.

Oleksii serves as forensic investigator, penetration tester and application security expert in professional companies.

Dr. Oleksii Baranovskyi can be reached online at varvara.m@calibrated.agency or LinkedIn.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



How AI is Transforming the Fight Against Data Breaches

By Nivedita Kumari, Data Analytics Customer Engineer, Google

The average cost of a data breach surged to $4.88 million from $4.45 million in 2023, a 10% surge and the biggest increase since the pandemic, as per a report by IBM (Cost of a Data Breach Report 2024). To counter the rising impact, 2 out of 3 organizations are massively investing in AI to prevent attacks and automate their SOCs. The organizations reported that they achieved an average savings of $2.2 million in breach costs by using AI in their preventative process.

The ruinous financial and reputation impacts of a data breach

The most significant impact of poor data security has to do with the financial losses. In 2023, the average cost of data breaches reached a record-high global level of $4.45 million USD; for some regions, reached $9.44 million USD.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Data breaches severely impair a company's reputation and cause erosion in customer trust. According to a Forrester's Security Survey, 2023, 90% of U.S. consumers have expressed that vendor security issues could have adverse effects on their lives, while 60% indicated that they would be less likely to do business with brands that have experienced a data breach.

More so, organizations are continually being pressured to fully comply with the legal and regulatory necessities associated with data protection. Laws such as GDPR, CCPA, and HIPAA impose strict conditions on how data should be collected, processed, and stored. Noncompliance can attract heavy fines. Based on CMS Law's GDPR Enforcement Tracker Report the total fines for GDPR in 2022 reached €1.69 billion which is substantially higher than it was in earlier years.

A data breach can expose personal data such as social security numbers, health records, and financial information, leaving victims exposed to identity theft and financial fraud. Companies risk losing trade secrets and intellectual property, which impacts their ability to compete and innovate in the future.

Devastating data breaches bring a company to its knees with costly downtime and recovery efforts as organizations race to bring back their systems and data. They can also impair employees' ability to access critical systems and data, fundamentally affecting productivity and overall efficiency.

Protecting data breaches in public clouds

Here is a quick review of key strategies and best practices for securing data in the cloud include the following:

Identity and Access Management (IAM) is the backbone of your cloud security. Always adhere to the least privilege principle in which you give users and services the least authority necessary to complete their jobs while avoiding excessive privileges.

Data encryption of any data whether at rest on databases, object storage, or other services assures that should an unauthorized access happen, the data remains undecipherable as well.

Network security imposes a strong security perimeter when you isolate your cloud resources inside VPCs and control network traffic through security groups and network access control lists (ACLs).

Collecting and analyzing security logs from all cloud resources in a central location provides insight into the activity and helps identify possible security threats.

Vulnerability management regularly scans the cloud environment to identify vulnerabilities and remediate them in a timely manner.

Backup and disaster recovery is vital for business continuity. Having a good backup strategy for your data and applications ensures you are able to recover information lost or systems that have experienced failures.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Security automation helps in streamlining security tasks and is a big efficiency booster. Infrastructure as Code (IaC) enables one to automate provisioning and management of cloud resources in a way that enforces consistent security configurations with reduced risks of human error.

Compliance and governance round up the tasks to ensure your cloud environment meets regulations. Enforcing and establishing security policies for your cloud environment provides a framework through which you can ensure safe operations and exhibit compliance with regulations.

Adopting these safety measures and best practices can immensely widen the protection of your data on public cloud platforms.

AI: Your Secret Weapon for Public Cloud Data Security

AI is transforming the landscape of securing data on public clouds such as Google Cloud, AWS, and Azure. These public clouds use AI algorithms to analyze immense amounts of data to detect signals and anomalies which might indicate potentially harmful acts. AI Intrusion

Detection Systems learn about normal traffic patterns on the network and detect anomalies. Furthermore, AI analyzes files and code to detect malware, inclusive of new and unknown variants, and detects phishing emails and websites by performing analyses on their content, URLs, and sender-related information.

In vulnerability management, AI scans for vulnerabilities on the cloud applications as well as the associated infrastructures. AI prioritizes the exploited vulnerability's degree and impact potential so that Security Administrations can focus on real issues of security. AI proactively strengthens security by predicting potential threats and vulnerabilities, allowing for preemptive measures.

AI automates incident response processes such as isolating infected systems, blocking malicious traffic, and notifying security teams. It also automates security audits, ensuring compliance with security policies and regulations. AI automatically rehabilitates security threats, such as patrolling vulnerabilities or blocking malicious IP addresses.

Data Loss Prevention (DLP) solutions powered by AI now identify and protect sensitive data such as credit card numbers and personal identity information. User and Entity Behavior Analytics (UEBA) uses AI to analyze user behavior in real-time and identifies anomalous activities that might indicate insider threats or compromised accounts.

AI detects anomalous login attempts, allowing it to flag suspicious activity and potential account compromise, filtering out alternative workarounds. AI-enabled risk-based authentication allows AI to assess the risk for a login and provide more firm or looser criteria for meeting that risk, enabling a dynamic, constantly changing process for logins.

Major cloud providers offer a range of powerful security tools to help protect your data. Google Cloud, for example, provides the Security Command Center for threat detection, Google SecOps for security automation, and Cloud Armor for web application and API protection. AWS offers similar solutions with

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Amazon GuardDuty, Amazon Macie, and Amazon Inspector, while Azure provides Microsoft Defender for Cloud, Azure Sentinel, and Azure Security Center.

The advantages for AI in cloud security are overwhelming; it enhances threat detection, allowing identification and neutralization of threats that even traditional security tools fail to detect. It allows incidents to be concluded much faster because they are automated in incident response. AI reduces costs through automation in security matters and allowing a security team to concentrate on broader strategic initiatives. AI enables compliance because it can more consistently enforce security policy and regulations.

In conclusion, data security is not merely an IT technical problem; it is a very vital business problem with serious ramification and AI-powered cloud security solutions can safeguard your organization's data in the public cloud. Data breaches pose a growing threat, with increasingly sophisticated cyberattacks leading to severe financial losses, reputational damage, and legal consequences. The arrival of AI is changing the way we protect sensitive data in the cloud. AI is revolutionizing cloud security. By excelling in threat detection, vulnerability management, and data protection, AI empowers organizations to significantly enhance their security posture and

mitigate the risk of data breaches. As AI technology advances, we can expect even more robust security solutions for a safer cloud environment.

About the Author



Nivedita Kumari is a Data Analytics Customer Engineer at Google, Nivedita is dedicated to making machine learning and AI accessible to everyone. She works to break down the complexities of these technologies, empowering individuals from all backgrounds to explore and understand AI's potential. Her focus is on driving tangible business value through data-driven strategies, while also inspiring and mentoring the next generation of AI innovators. Nivedita can be reached at https://www.linkedin.com/in/nivedita-kumari/ and at our company website https://cloud.google.com/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Advances In Quantum Computing Signal an Urgent Post-Quantum Cryptography (PQC) Imperative for Enterprises

By Anurag Lal, President & Chief Executive Officer, NetSfere

Estimates among experts vary on the timetable for the arrival of "Q-Day" – the day when quantum computers are powerful enough to crack current encryption protocols. However, one thing most experts agree on is that the era of quantum computing is coming sooner rather than later.

Google's recent introduction of a new quantum chip called Willow marked a significant advancement toward commercially viable quantum computing. Google heralded Willow as bringing the world "closer to running practical, commercially-relevant algorithms that can't be replicated on conventional computers."

As this breakthrough accelerates the arrival of quantum computing, it creates a clear imperative for enterprises to adopt post-quantum cryptography (PQC) to protect critical systems and data from quantum threats.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Willow: Google's Quantum Breakthrough

In early December, Google introduced Willow, a new 105 qubit quantum chip demonstrating error correction and performance that the company says paves the way to a useful, large-scale quantum computer.

Google measured Willow's performance using the random circuit sampling (RCS) benchmark and found that the chip's performance was literally out of this world. Willow performed a computation in under five minutes that would take one of today's fastest supercomputers 10^{25} or 10 septillion years. That's a one followed by 24 zeros. According to Google, "this mind-boggling number exceeds known timescales in physics and vastly exceeds the age of the universe."

Google noted that the speed and reliability performance of Willow shows great promise for helping discover new medicines, design more efficient batteries for electric cars, and accelerate progress in fusion and new energy alternatives.

The promise of quantum computing in areas like these is fueling investments in the technology by many other companies and nations.

Investments in Quantum Computing Continue to Grow

Google is just one of the tech giants in the U.S. ramping up investments in quantum computing technology. Companies like IBM, Microsoft, and AWS (Amazon) are also racing to develop quantum computing innovations.

Nations too are leading investors in quantum computing technology. According to EY, Canada has invested $2.2 billion in quantum computing, Germany $2.4 billion and China dedicated $10.0 billion to its National Quantum Lab. In the US, the National Quantum Initiative Act was signed in 2018 to invest $1.2 billion in the field of quantum information science and technology during a 10-year period. More recently, congressional leaders introduced the National Quantum Initiative Reauthorization Act, which would authorize $2.7 billion in federal funding to accelerate quantum research and development at federal science agencies for the next five years.

Implications for Enterprise Cybersecurity

With breakthroughs like Willow and ongoing investments in quantum computing by tech giants and nations, advancements in this technology will continue to accelerate. Even though Google has gone on record to state that Willow cannot break modern cryptography, the fast-approaching era of quantum computing is creating an urgent imperative for enterprises to speed up their timelines for adopting post-quantum cryptography.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

It's no secret that quantum computers are poised to break widely used encryption protocols like RSA, ECC (Elliptic Curve Cryptography) and other public-key encryption protocols, rendering business communication and other sensitive data vulnerable to attacks. The quantum-driven looming obsolescence of these encryption protocols is a major reason for enterprises to become quantum resilient now.

While CRQCs (cryptographically relevant quantum computers) aren't here yet, quantum threats are present today. Cybercriminals are harvesting encrypted data today in anticipation of decrypting it later when quantum technology matures and becomes powerful enough to crack current encryption protocols.

With quantum threats already here and the rate of quantum computing development accelerating, enterprises must take a proactive approach to becoming quantum resilient by adopting quantum-safe technologies throughout their operations.

Staying Ahead of Quantum Threats

Even as the post-quantum future looms, many enterprises are lagging when it comes to assessing their technology solution providers' support for quantum-resistant cryptography. Metrigy's recent Workplace Collaboration and Contact Center Security and Compliance 2024 global study of 338 organizations, found that just 18.1% assess their workplace collaboration vendors' support for quantum-resistant cryptography.

To stay ahead of quantum threats organizations should not wait to adopt solutions supported by post-quantum cryptographic algorithms.

Migrating to post-quantum encryption technologies is essential for organizations to ensure the long-term confidentiality and integrity of their data now and in the future.

To help enterprises protect against quantum threats, the U.S. Department of Commerce National Institute of Standards and Technology (NIST) released three PQC standards in August 2024. These standards provide a roadmap for securing a wide range of digital information including confidential business communication, e-commerce transactions, and more.

Enterprises can protect their data and stay ahead of quantum threats with the right tools and strategies in place including using solutions that support post-quantum cryptography, evaluating and inventorying current cryptographic infrastructure, prioritizing PQC transition of infrastructure based on risk, and monitoring regulatory developments to maintain compliance.

Wrapping Up

The introduction of Google's Willow chip signals that the quantum future is fast approaching. While the era of quantum computing has not yet arrived, enterprises need to start preparing now to stay ahead of quantum threats. When it comes to quantum readiness, the sooner organizations transition to quantum-resistant encryption, the better.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Anurag Lal is the President and CEO of NetSfere. With more than 25 years of experience in technology, cybersecurity, ransomware, broadband and mobile security services, Lal leads a team of talented innovators who are creating secure and trusted enterprise-grade workplace communication technology to equip the enterprise with world-class secure communication solutions. Lal is an expert on global cybersecurity innovations, policies, and risks.

Previously, Lal was appointed by the Obama administration to serve as Director of the U.S. National Broadband Task Force. His past experience includes time at Meru, iPass, British Telecom and Sprint in leadership positions. Lal has received various industry accolades, including recognition by the Wireless Broadband Industry Alliance in the U.K. Lal holds a B.A. in Economics from Delhi University and is based in Washington, D.C.

Anurag can be reached online at @anuragl and at our company website https://www.netsfere.com

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Navigating NIS2 Compliance: Elevating Cyber Resilience Through Network Visibility

By Matt Ellison, Technical Director for EMEA at Corelight

As cyber threats continue to surge, businesses face growing pressure to fortify their defences and ensure operational continuity. Regulatory frameworks like the Network and Information Systems Directive 2 (NIS2) reflect this urgency, offering a structured approach to bolstering cybersecurity resilience. NIS2 sets the bar for critical infrastructure and essential services across the European Union, aiming to protect vital systems from breaches and disruptions.

However, for organisations operating in sectors covered by the directive, compliance isn't just a regulatory requirement—it's an opportunity to establish a stronger cybersecurity posture. By aligning with NIS2, businesses can move beyond reactive measures to proactive strategies, ensuring they stay ahead in an environment where the stakes are higher than ever.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Decoding NIS2: Turning Challenges into Strategic Gains

As an evolution of its predecessor, the NIS Directive, NIS2 represents a significant step forward in the EU's cybersecurity strategy. Its expanded scope includes a broader range of operators of essential services (OES) and digital service providers (DSPs), reflecting the interconnected nature of modern supply chains and digital ecosystems.

Key obligations under NIS2 include conducting regular risk assessments, implementing incident management protocols, and maintaining effective log monitoring. While these requirements may seem challenging, they also provide organisations with a framework to identify and address vulnerabilities systematically. Businesses that embrace these measures not only comply with regulations but also significantly enhance their resilience against cyberattacks.

Risk assessments, for example, become a key tool for uncovering weaknesses in systems and processes. Rather than viewing these as a burden, forward-thinking organisations can leverage them to prioritise security investments, reducing the likelihood of costly breaches or reputational damage.

The Power of Network Visibility

One of the most vital components of NIS2 compliance is achieving full visibility into network operations. With the complexity of IT environments growing, organisations need tools that capture, index, and analyse network traffic comprehensively. These insights are essential for identifying vulnerabilities, monitoring real-time activity, and managing risks effectively.

Complete network visibility allows organisations to detect anomalies that could signal cyber threats, enabling them to respond swiftly and decisively. For example, advanced monitoring solutions equipped with AI-driven analytics can pinpoint unusual behaviour, triggering alerts before an attack can escalate. This proactive approach transforms security from a defensive measure to an integral part of business strategy.

Strengthening Incident Management Capabilities

Another cornerstone of NIS2 is the requirement for robust incident management processes. These include clear reporting protocols and detailed response strategies designed to minimise the impact of security incidents. Advanced threat detection mechanisms play a crucial role here, equipping organisations to combat both known and emerging threats effectively.

By integrating machine learning, behavioural analysis, and signature-based detection methods, businesses can create a multi-layered defence. Incident response teams armed with detailed network data can quickly investigate breaches, identify root causes, and implement measures to prevent recurrence. This approach not only mitigates immediate risks but also strengthens long-term resilience.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Securing the Supply Chain: A Critical Priority

NIS2 extends beyond internal systems, emphasising the need for supply chain security. Cyberattacks targeting third-party vendors have become increasingly common, exposing businesses to significant risks. To comply with the directive, organisations must assess the cybersecurity measures of their partners and implement controls to protect shared data and infrastructure.

By fostering transparency and collaboration across the supply chain, businesses can build a collective defence against cyber threats. Technologies that enable real-time monitoring of supply chain activities, combined with regular audits and risk assessments, are essential for ensuring compliance and minimising vulnerabilities.

Shaping the Future of Cybersecurity

Looking ahead, NIS2 compliance should be viewed not as an endpoint but as a catalyst for innovation and growth. By integrating network visibility, advanced threat detection, and supply chain security into their strategies, organisations can position themselves as leaders in cybersecurity resilience.

Moreover, businesses must embrace a culture of continuous improvement, staying informed about emerging threats and evolving regulatory requirements. Investments in employee training, collaboration with industry peers, and the adoption of cutting-edge technologies will be key to maintaining a competitive edge.

As cyber threats grow in complexity, the need for a unified approach to security has never been greater. NIS2 offers a blueprint for organisations to protect not only their own operations but also the broader digital ecosystem.

About the Author

Matt Ellison is the Technical Director of EMEA of Corelight. Prior to his current role, he was the EMEA Channel Sales Engineer of Appgate. Ellison completed his education at The Open University.

Matt can be reached online at matt.ellison@corelight.com our company website www.corelight.com



Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Generative AI In Business: Managing Risks in The Race for Innovation

By Brad LaPorte, CMO, Morphisec

Artificial intelligence has emerged as a game-changing force, with record amounts of funding fueling new innovations that are transforming industries and workflows at speeds we have never seen before.

According to data from Crunchbase, in February 2024, AI companies received $4.7 billion in venture funding. That's more than double the $2.1 billion invested in February 2023. It's money like this is fueling innovations that are being adopted at record speeds. Take code copilots as an example. It saw adoption rates exceeding 50%. Other big releases in 2024 included OpenAI's GPT-4o and o1 Series and AI Video Creation Tools such as Google's Veo and many others.

While these new tools are helping build business efficiencies, they also introduce significant security and data privacy concerns.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

A great example is Microsoft Copilot, which truly typifies the dual-edged sword that is AI. On one hand, it delivers valuable workflow optimization capabilities. Recent reports show that users can complete tasks nearly 30% faster. This includes writing, summarizing meetings, and searching for information, among other things.

On the other hand, there is a heightened risk of sensitive data exposure and potential data privacy violations. According to an article from GCS Technologies, there are significant data security risks that come with using Microsoft Copilot. According to the article, "research shows that 16% of businesses' critical data is overshared. In fact, the average company has 802,000 files at risk of oversharing — typically with users or groups within the company."

Some may wonder why Microsoft hasn't addressed these risks and done more to protect its 20 to 30 million active CoPilot users. Part of the problem is that companies are steeped in intense competition to bring the next cutting-edge AI technologies to market, often at the expense of conducting thorough assessments that address security risks before deployment. This introduces new vulnerabilities and exposes organizations to potential threats.

Another great example of a recent innovation that sparked equal parts excitement and alarm is Claude 3.5 Sonnet, which was created by Anthropic. One of the big AI releases from 2024, Claude 3.5 Sonnet, takes AI beyond traditional assistants like ChatGPT, Google Gemini, and others as it's capable of executing complex tasks with minimal human intervention. Users embed Claure in a system. From there, it can leverage multiple tools and applications to carry out commands, anything from researching your next family vacation and building a new website for your business to advanced coding and software development or context-sensitive customer support.

It's an exciting tool, but when examined more closely significant security challenges with Claude 3.5 Sonnet emerge.

The Risks of AI Agent-Based Programs

AI systems like Claude 3.5 Sonnet operate through extensive data transactions and retrieval techniques where data security and privacy vulnerabilities are abundant. These systems are also vulnerable to exploitation, and that's happening now. For example, cybercriminals are leveraging AI to enhance their attack methodologies, targeting AI systems in ways that could have deleterious impacts on a business.

For example:

Model Extraction Attacks: A major concern is model extraction attacks, where attackers reverse-engineer AI models to uncover how they work. With this insight, cybercriminals can create mimicked versions, which are then used for malicious purposes. For example, gaining unauthorized insights into a business's operations or launching highly targeted attacks.

Prompt Injection Attacks: Another growing threat is prompt injection attacks. In this instance, attackers manipulate an AI model's prompts to produce unintended or harmful outputs. This can be further complicated by advanced AI models that are able to craft adaptive prompts that allow attackers to

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

continuously refine injection techniques. In doing so, they can successfully bypass filters and exploit vulnerabilities to disrupt operations or extract sensitive information.

AI-Powered Ransomware: Another pressing concern is AI-powered ransomware, which attackers can leverage to identify weaknesses more efficiently. But that's not all. They can also use AI to develop ransomware that can adapt and evolve, so it not only evades traditional detection methods but also complicates all remediation efforts.

The Growing Adoption of GenAI Systems

GenAI adoption in business environments is growing. According to an Altman Solon report, Putting Generative AI to Work, 65% of enterprises around the globe reported using GenAI tools regularly. That's up from just 11% in early 2023 and represents a jaw-dropping 490% year-over-year jump in adoption.

The issue is that businesses lack the appropriate processes, guidelines, or formal governance structures needed to regulate AI use, which, at the end of the day, makes them prone to accidental security breaches. In many instances, the culprits are employees who introduce GenAI systems on corporate devices with no understanding of the risks that come with it or their use even permitted based on the company's existing data security and privacy guidelines.

The fact that companies lack the necessary levels of oversight is problematic and can create unintended consequences. For example, it can lead to violations of data protection regulations (e.g. GDPR, California Privacy Rights Act) or expose an organization to sophisticated cyberattacks. Righting the ship begins with security leaders who must proactively map out potential GenAI use cases to existing data security frameworks. By assessing risks and scoring them, teams can spot weaknesses and fix them before they're exploited.

Addressing Security Risks in AI-Powered Systems

More must be done to stop security risks associated with AI agent-based systems. Your best bet is a multifaceted approach that goes beyond traditional cybersecurity measures in favor of strategies designed to address the unique challenges posed by these advanced technologies.

1. **Implement Robust AI Governance:** Establish clear guidelines that detail how AI can be used within the organization. To make this easily digestible to all employees, provide clear details and examples of permissible use cases. You can even include examples of permissible AI tools. Next, set specific boundaries for data access and ensure that all AI systems comply with data security and privacy regulations. Naturally, not every employee will adhere to these guidelines. In fact, you can count on many who will not. For this very reason, conduct regular audits to identify any incidents of unauthorized AI usage that could lead to potential security breaches and then take any and all preventative measures needed.
2. **Enhance Employee Awareness:** Never overestimate the power of employee education, which is essential in times when new innovations are far ahead of education. Put in place an educational

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

program that delves into the risks of AI systems. Include training sessions that give people the tools they need to recognize red flags, such as suspicious AI-generated outputs or unusual system behaviors. In a world of AI-enabled threats, it's important to empower employees to act as the first line of defense is essential.

3. **Invest in Advanced Security Solutions:** Traditional security tools may not be sufficient to protect against AI-enabled attacks. Organizations should consider adopting advanced solutions, such as endpoint protection platforms, behavioral analytics, and real-time threat detection tools, to bolster their defenses.
4. **Focus on Preemptive Defense:** A preemptive approach that leverages tools such as Automated Moving Target Defense (AMTD) can help organizations stay ahead of attackers. By anticipating potential threats and implementing measures to address them before they occur, companies can reduce their vulnerability to AI-enabled exploits. This proactive stance is particularly important given the speed and adaptability of modern cyber threats.
5. **Monitor AI Systems Continuously:** Continuous monitoring of AI systems is essential to detect unusual activity or signs of compromise, as it can help ensure that AI agents operate as intended and do not begin to pose a risk to a company's broader security environment.

Preparing for the Future of AI-Driven Threats

It's reported that the global generative AI market could grow from $28.9 billion in 2024 to more than $54 billion in 2025. With this growth will come new groundbreaking innovations that will introduce new tactics employed by cybercriminals. It's incumbent that organizations recognize that the risks that come with AI adoption extend beyond technological vulnerabilities to include human factors, such as inadequate training and governance. A holistic approach to security—encompassing people, processes, and technology—is essential to safeguarding against these threats.

By taking proactive steps to address the risks associated with AI agent-based systems, organizations can harness the benefits of these technologies while minimizing their exposure to emerging threats. The path forward lies in balancing innovation with vigilance, ensuring that security remains a priority as we embrace the future of artificial intelligence.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

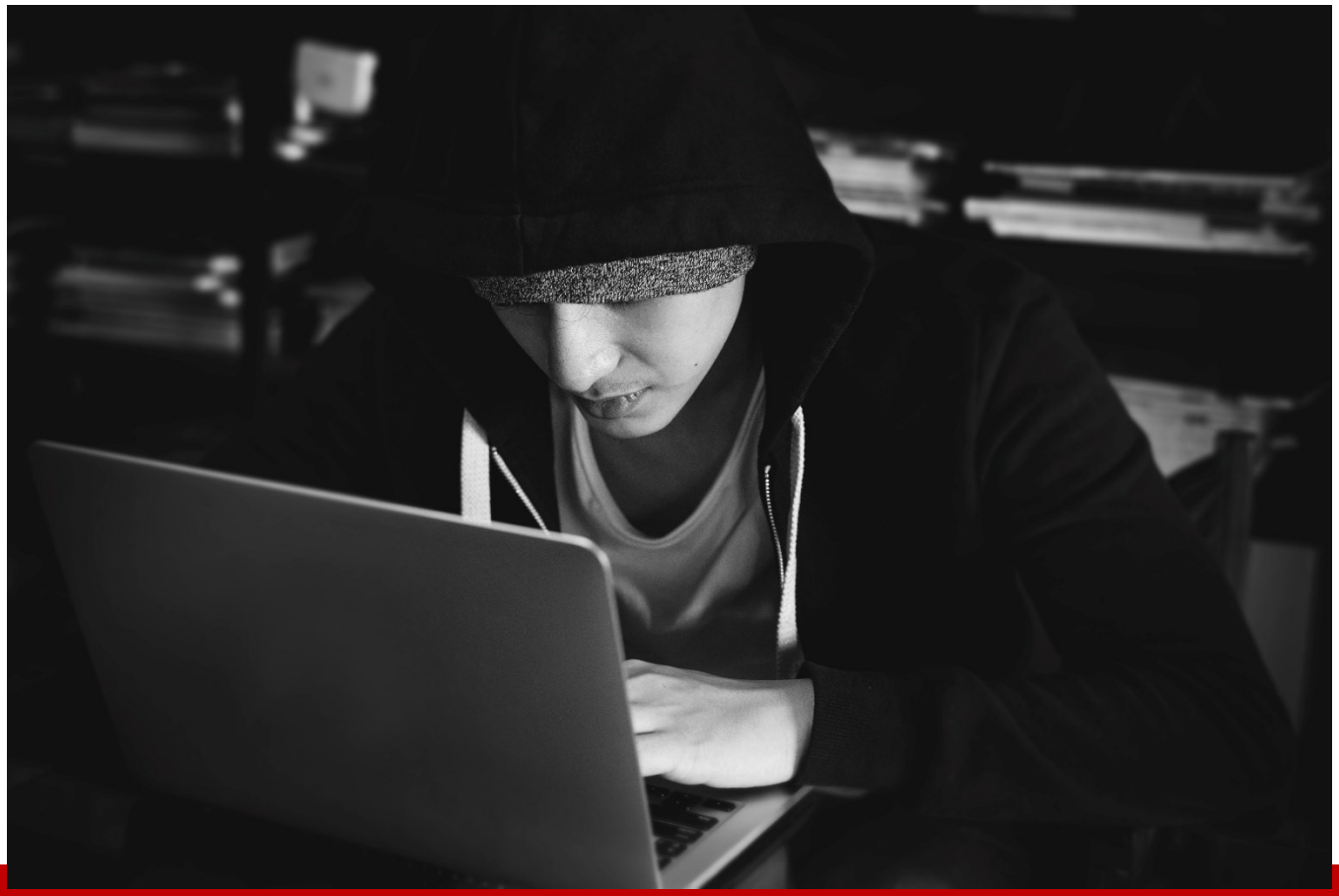
About the Author



Brad LaPorte is the CMO of Morphisec. He is a seasoned cybersecurity expert and former military officer specializing in cybersecurity and military intelligence for the United States military and allied forces. With a distinguished career at Gartner as a top-rated research analyst, Brad was instrumental in establishing key industry categories such as Attack Surface Management (ASM), Extended Detection & Response (XDR), Digital Risk Protection (DRP), and the foundational elements of Continuous Threat Exposure Management (CTEM). His forward-thinking approach led to the inception of Secureworks' MDR service and the EDR product Red Cloak—industry firsts. At IBM, he spearheaded the creation of the Endpoint Security Portfolio, as well as MDR, Vulnerability Management, Threat Intelligence, and Managed SIEM offerings, further solidifying his reputation as a visionary in cybersecurity solutions years ahead of its time.

Brad can be reached online at https://www.linkedin.com/in/brad-laporte/ and at our company website https://www.morphisec.com/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Best Laptop for Cybersecurity: Top Picks for Ethical Hackers & Security Professionals

Why Security Professionals Need the Right Laptop

By John Doe, Cybersecurity Analyst, X-PHY

Selecting the right **Laptop For Cybersecurity** is one of the most critical decisions for cybersecurity professionals. Whether you are a CISO, penetration tester, ethical hacker, or IT security analyst, the hardware and software you rely on should be capable of running advanced security tools while ensuring your data remains protected from threats. A weak machine not only hinders performance but can also create vulnerabilities that attackers can exploit.

With an increasing number of cyber threats emerging daily, professionals need devices that provide high processing power, security-focused features, and compatibility with various security testing tools. This guide highlights the top choices and key factors to consider when selecting the best cybersecurity laptop.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Key Considerations for Cybersecurity Laptops

Performance Requirements

- **Processor**: At least an Intel i7/i9 or AMD Ryzen 7/9 for handling multiple VMs and penetration testing applications.
- **RAM**: A minimum of 16GB is essential, though 32GB is recommended for heavy multitasking and running virtualized environments.
- **Storage**: SSDs (preferably NVMe) are significantly faster than HDDs, improving boot times and file access speeds.
- **Graphics**: While a dedicated GPU is not a necessity, some security applications involving AI-driven security analytics may benefit from one.
- **Portability & Battery Life**: A cybersecurity professional on the go should consider lightweight laptops with long battery life to maintain productivity outside the office.

Operating System Choices

- **Linux** (Kali, Parrot OS, BlackArch): The preferred choice for security testing due to its vast collection of built-in penetration testing tools.
- **Windows**: While often seen as less secure than Linux, Windows remains necessary for corporate environments and offers security features like BitLocker, TPM 2.0, and Secure Boot.
- **MacOS**: Apple devices are known for their security and stability but have limited compatibility with some cybersecurity tools.

Security Features to Look For

- **TPM (Trusted Platform Module)**: Ensures hardware-based encryption and secure authentication.
- **Secure Boot & BIOS Protection**: Prevents malware from modifying the bootloader and system firmware.
- **Privacy Enhancements**: Fingerprint scanners, webcam covers, and physical privacy switches add another layer of security.
- **Hardware-Embedded AI Security**: The **X-PHY** AI Cybersecurity Laptop provides real-time protection against sophisticated cyberattacks by leveraging AI-powered threat detection.

Best Laptops for Cybersecurity in 2024

Top Picks for Ethical Hackers & Penetration Testers

- **Dell XPS 15** – Excellent Linux compatibility and a powerful processor for running security tools.
- **Lenovo ThinkPad X1 Carbon** – A durable, security-focused laptop trusted by professionals worldwide.
- **Framework Laptop** – Highly customizable and repairable, making it ideal for security researchers.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

- **Razer Blade 15** – A solid choice for dual-booting Windows and Linux with strong performance.

Best Secure Laptops for Security Professionals

- **Apple MacBook Pro (M3)** – A robust, secure laptop with an encrypted file system and secure enclave.
- **Dell Latitude 7420** – Enterprise-class security features, including encrypted SSDs and BIOS protection.
- **HP Elite Dragonfly G3** – A business laptop with integrated security tools like HP Sure View and Sure Start.
- **Purism Librem 14** – Designed with privacy in mind, featuring hardware kill switches and an open-source BIOS.

Best Budget Laptops for Cybersecurity Students

- **Acer Aspire 5** – Affordable and upgradeable, suitable for students beginning in cybersecurity.
- **Asus ZenBook 14** – A lightweight, Linux-friendly laptop with decent hardware.
- **Lenovo IdeaPad 5** – A great balance of price and performance for security learners.

Additional Tools & Accessories for Cybersecurity Professionals

- **External SSDs** – Used for storing penetration testing tools and forensic analysis.
- **Hardware Security Keys (YubiKey, Google Titan)** – Provides multi-factor authentication and cryptographic security.
- **Privacy Screens & Faraday Bags** – Prevents unauthorized physical access and wireless data interception.
- **USB Kill Test Tools** – Used by cybersecurity researchers to test USB-based attacks.
- Tips for Buying a Cybersecurity Laptop
- **New vs. Refurbished**: Many security professionals prefer refurbished enterprise-grade laptops due to their affordability and durability.
- **Extended Warranty & Support**: Investing in a business-class warranty ensures priority support in case of hardware failures.
- **Buying From Trusted Vendors**: Always purchase from official brand stores or reputable third-party resellers to avoid security risks from pre-installed malware.

FAQs

Can I use a gaming laptop for cybersecurity?

Yes, as long as it meets the necessary performance requirements. Many gaming laptops, like the Razer Blade 15 and Alienware m15, are great for ethical hacking due to their high-end specs.

Is Windows or Linux better for cybersecurity?

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Linux is the preferred choice for penetration testing and ethical hacking due to its flexibility and access to security tools. However, Windows remains a necessity for enterprise cybersecurity environments.

Do I need a dedicated GPU for cybersecurity work?

Not always. Most cybersecurity tasks rely more on CPU and RAM. However, for AI-driven security analysis or machine learning applications, a dedicated GPU can be beneficial.

How much RAM is ideal for cybersecurity tasks?

16GB is the minimum recommendation, but 32GB or more is ideal for running multiple virtual machines and performing intensive security operations.

For professionals looking for a **Laptop For Cybersecurity** that includes AI-powered security protection, check out **X-PHY**, one of the most advanced solutions for real-time cybersecurity defense.

Editor's Note: The information in this article solely reflects the author's research and opinions, and does not imply any endorsement of the brands of hardware and software, or other specifications, by Cyber Defense Magazine. Our publication offers this information for consideration by our readers in making their own decisions on purchasing and using hardware and software for their own professional activities.

About the Author

John Doe is a Cybersecurity Analyst at **X-PHY**. With extensive experience in cybersecurity, ethical hacking, and penetration testing, John specializes in security infrastructure, vulnerability assessments, and cyber defense strategies.



Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Cybersecurity Trends for 2025

Companies Use AI as Defense Against AI; Increased Regulations Attempt to Mitigate Risks

By Ben Hunter III, Principal, UHY

Artificial Intelligence (AI) has been the buzzword in cybersecurity and business for a few years now, and it will continue to impact security and all phases of business in 2025. While AI is improving efficiency and productivity of businesses across all sectors, we have heard just as many horror stories about AI inflicting damage on individuals and businesses alike.

Cyber breaches are becoming more prevalent, companies are increasing cybersecurity investment

A disturbing trend from the UHY 2025 Middle Market Survey* shows that cybercrime is becoming more prevalent. According to the survey, in 2019, 67 percent of participants had never experienced a cyber breach. Three years later in 2022, 63 percent of participants had not had to utilize their cybersecurity resource as the result of an incident. Responses from the current survey indicated a shift in this trend, with a majority of survey participants experiencing a cyber incident over those who hadn't; 55 percent indicated they had experienced an incident to 45 percent that said they had not.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

In response to this trend, more than three-quarters of participants (79 percent) are planning to increase their cybersecurity spending in 2025, which is slightly more than reported in the previous year.

An increase in cybersecurity spending is a welcome sight, but there are specific areas that leadership teams should focus on going into 2025. These are the trends we are watching heading into the new year.

'Deepfake detection' protects businesses against AI social engineering attacks

Bad actors have been and will continue to use AI to create better phishing, vishing, SMA, and other social engineering campaigns. They will also leverage the use of deepfakes. Deepfake technology involves manipulating audio and video to create fake content that appears very real. Deepfakes can be used for social engineering attacks, and impersonating individuals (CEOs and other C-Suite leadership). Organizations at risk will need to invest in deepfake detection tools and strategies to protect their reputation and data integrity. Awareness, education, and analog confirmations are key to combating the deepfake threat.

AI is already being used in organizations, whether leadership is aware or not. AI requires governance. Policies and procedures, guardrails, and oversight are essential to ensuring data security and retaining customer trust. As with all policies, these new AI policies need to be lived, not just written. Leadership's "tone at the top" creates the culture that informs how policies are implemented throughout a business.

Multifactor authentication becomes an essential security measure

Ransomware and data theft extortion are and will continue to be the most disruptive type of cybercrime impacting the middle market. In 2024, ransomware and extortion schemes have affected more than 100 countries and every industry.

One of the primary modes of entry by bad actors is phishing and social engineering, compromising user credentials. In 2025, two-factor / multi-factor authentication (2FA/MFA) will be an essential security measure for business and individuals. MFA is still not ubiquitous. This allows bad actors easy access with stolen and compromised credentials. MFA has been a fundamental security tool for years, but not all businesses or individuals utilize it. 2025 will be the year that even your grandma and Uber driver talk about MFA.

Companies look inward to limit malicious insider attacks

According to IBM and Ponemon Institute's 2024 Cost of a Data Breach Report, malicious insider attacks cost $4.99 million – the highest cost compared to other attack vectors. An insider is a user that is authorized to be in the environment and the user account is not compromised via a phishing or social engineering attack. Insider attacks can appear in different forms such as data tampering, account manipulation, or a leak of sensitive information. Organizations should focus on enhancing their monitoring

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

and detection capabilities; striking a balance between trust and vigilance. As always, employee training and awareness is essential in mitigating these risks.

Incident response plans help mitigate vendor risk

Organizations have become more and more dependent on third parties, cloud infrastructure, and cloud service providers. As we have seen over the years, a single vendor vulnerability can cause costly data breaches, compliance violations, and financial losses. Organizations in the middle market are in a tight spot regarding vendor management. They are not big enough to influence the vendors upon whom they rely, yet their customers require proper security, confidentiality, and privacy controls to be in place. In 2025, organizations need to maintain robust incident response plans. Regular security audits and penetration testing of third-party infrastructure also provide data points needed to manage the vendor risk.

Government intervenes to protect businesses

UHY anticipates that 2025 is the year of cybersecurity regulation. Landmark rules like the US SEC's cybersecurity rules, the EU's Cyber Resilience Act (CRA), the Digital Operational Resilience Act (DORA), and the UK's proposed Cyber Security and Resilience Bill require companies to assume greater responsibility for managing, mitigating, and reporting cybersecurity risks and incidents.

Cybersecurity is essential to maintaining customer trust and growing a business. Cybersecurity protects the possibility.

**UHY's 2025 Middle Market Survey gathered insights from over 275 middle market business owners from a variety of industries, including automotive, construction, energy, financial services, healthcare, not-for-profit, real estate, staffing, and technology. Most participants represented companies between several million to more than $500 million in revenue and ranged in size from 20 to more than 1,000 employees across the United States. Data collection for this survey took place in 2024.*

Responses provided information on the performance of middle market businesses, strategic priorities, awareness of cybersecurity and technology concerns, and knowledge of emerging topics, particularly artificial intelligence (AI) and other significant external factors.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Ben Hunter has over 10 years of experience and is responsible for the overall management of the Technology, Risk & Compliance practice in the Great Lakes region. He maintains oversight of client relationships and compliance with AICPA, US, EU and other regulatory standards. Ben also manages the development of existing and new service lines. Ben can be reached online at https://uhy-us.com/.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Evolution Of Cyber Threats: Why Attack Surface Management Is Critical Today

By Ankit Sharma, Senior Director, and Head - Solutions Engineering, Cyble

"Your organization's attack surface is bigger than you think."

As digital transformation accelerates, businesses, government agencies, and financial institutions in India are expanding their digital footprints—often unknowingly. Every new cloud deployment, third-party vendor integration, and remote access point increases the number of potential attack vectors. Yet, many organizations still operate under outdated security models that fail to account for this growing complexity.

This is why Attack Surface Management (ASM) has become a strategic necessity. It provides continuous visibility into an organization's exposed assets, proactively identifying vulnerabilities before they can be exploited. In an era where cybercriminals operate with increasing sophistication, Indian enterprises must shift from reactive defense to proactive risk mitigation.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The Expanding Digital Attack Surface a Growing Risk

Traditional security perimeters no longer exist. Today's enterprises operate across multi-cloud environments, third-party SaaS applications, IoT devices, and remote work infrastructures, all of which expand their attack surfaces. This digital sprawl creates numerous security blind spots—ones that cybercriminals are actively exploiting.

According to Cyble Inc.'s Annual Threat Landscape Report 2024, cybercriminal activity on underground forums surged by 30%, with 9,300 incidents involving unauthorized access sales, data breaches, and extortion attempts. Platforms like Nuovo BreachForums have become marketplaces for selling stolen credentials and launching cyber extortion campaigns.

In India, industries such as banking, financial services, IT, and government agencies are frequently targeted due to their vast repositories of sensitive data. Misconfigured cloud environments and unpatched vulnerabilities remain key entry points, making it critical for organizations to continuously monitor and secure their digital assets.

How Attackers Exploit Unmanaged Attack Surfaces

Cybercriminals no longer rely on sophisticated hacking alone. Instead, they capitalize on unmonitored attack surfaces, using a variety of techniques to breach organizations:

Unpatched Vulnerabilities

- Attackers actively trade exploits for vulnerabilities in FortiOS, Microsoft Outlook, and Zimbra Collaboration Suite—all of which were widely targeted in 2024.
- Once these vulnerabilities are exploited, adversaries gain initial access, often leading to ransomware attacks or large-scale data exfiltration.

Shadow IT & Third-Party Risks

- Many enterprises lack visibility into unauthorized or poorly managed IT assets, making them easy prey for cybercriminals.
- In supply chain attacks, adversaries breach third-party vendors, using them as steppingstones to compromise larger organizations.

Dark Web Exposure: Selling Stolen Corporate Data

- Over 6,500 incidents in 2024 involved corporate credentials and access logs being sold on underground forums.
- Without proactive ASM, organizations often discover these leaks only when it's too late—after financial losses, regulatory fines, and reputational damage have already occurred.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Why Indian Enterprises Must Prioritize Attack Surface Management

Many Indian organizations still focus on perimeter-based security, overlooking the fact that modern cyberattacks exploit external digital assets. ASM provides:

- **Real-Time Discovery of Exposed Assets –** Detects new cloud deployments, web applications, and third-party integrations that may be vulnerable.
- **Continuous Monitoring for Exploitable Weaknesses –** Identifies misconfigurations, unpatched software, and shadow IT before attackers do.
- **Dark Web Intelligence & Threat Detection –** Monitors underground forums for stolen credentials, unauthorized access listings, and data leaks.

For Indian enterprises, especially in BFSI and IT services, ASM serves as a frontline defense against cybercriminals who are constantly looking for exposed assets to exploit.

Proactive ASM is a Competitive Advantage for Indian Businesses

Organizations that integrate Attack Surface Management into their security frameworks gain a significant edge:

- **Mitigating Zero-Day Exploits** – Identifies and remediates unpatched systems before adversaries can use them for attacks.
- **Detecting Unauthorized Access Sales** – Enables security teams to **intercept stolen credentials** before they are weaponized.
- **Reducing Supply Chain Attack Risks** – Provides visibility into **third-party vendors' vulnerabilities**, ensuring a stronger security posture.

India ranked among the top three most targeted nations for cyberattacks in 2024, highlighting the urgency for businesses to rethink their cybersecurity strategies. Delayed investment in ASM means greater financial, operational, and reputational risks—a cost that most enterprises cannot afford.

The Future of ASM: AI, Automation, and Threat Intelligence

Cyber threats are evolving, and so must ASM. Key advancements shaping the future of **Attack Surface Management** include:

- **Automated Risk Prioritization –** AI-driven tools will assess vulnerabilities in real-time, enabling organizations to focus on the most critical threats.
- **AI-Powered Anomaly Detection –** Machine learning models will identify emerging attack patterns, allowing businesses to stay ahead of adversaries.
- **Tighter Threat Intelligence Integration –** ASM will seamlessly connect with cyber threat intelligence platforms, providing a holistic view of external attack vectors.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

As cybercriminals increasingly turn to data extortion, cloud exploitation, and AI-driven attacks, Indian businesses must adopt next-generation ASM solutions to stay ahead of these threats.

Cybersecurity is no longer just about firewalls and endpoint security—it's about understanding, mapping, and managing an organization's entire digital footprint. As India's enterprises and government agencies embrace digital transformation, their attack surfaces will only continue to expand.

For Indian organizations to thrive in an era of relentless cyber threats, they must prioritize ASM, invest in threat intelligence, and embrace automation. The companies that do will not only protect their assets and reputation but will also lead the charge in building a more secure digital India.

About the Author



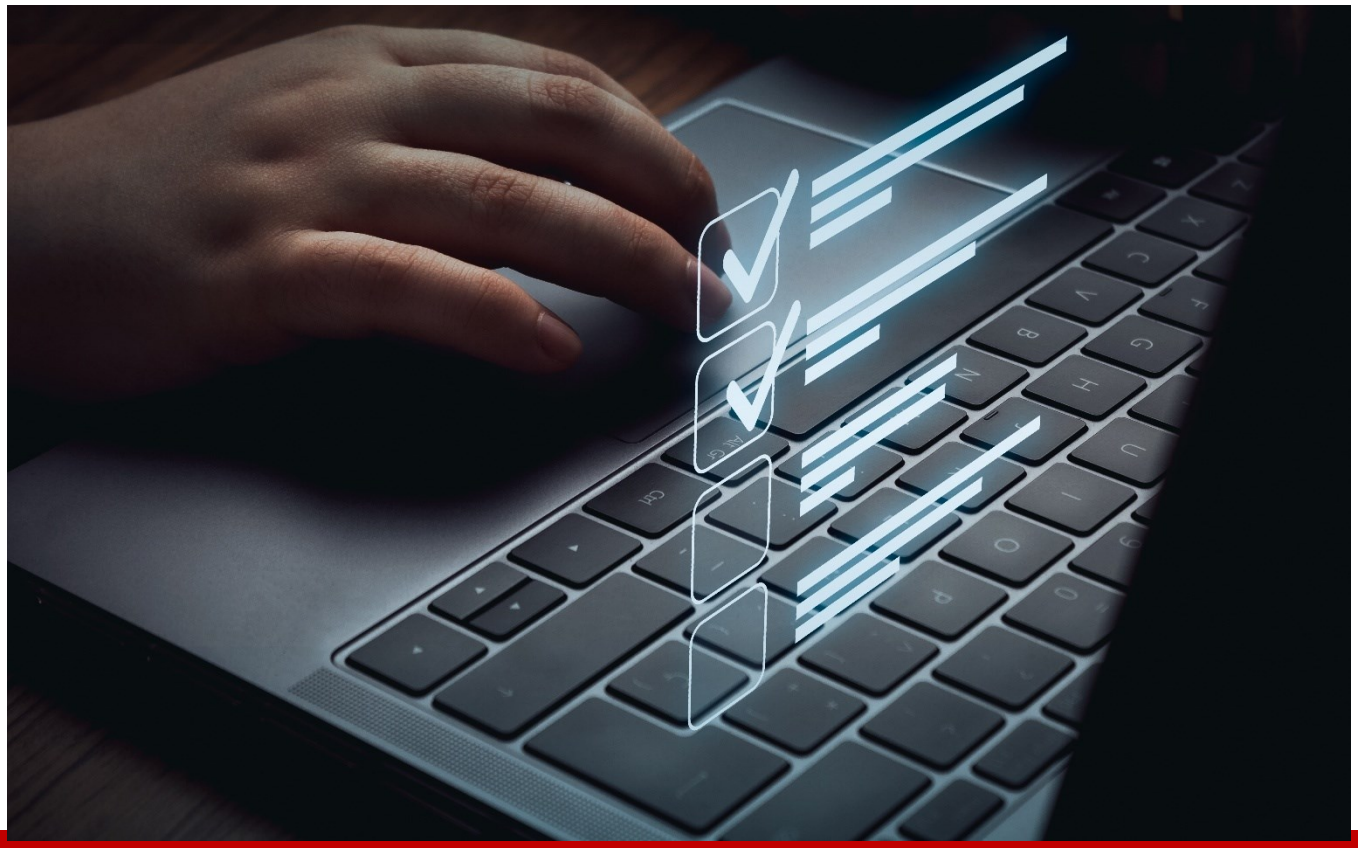
Ankit Sharma, Senior Director, and Head - Solutions Engineering, Cyble, is a Seasoned Techno-commercial professional, having refined skill set & relevant experience in driving both Topline & Bottomline growth. Domain expertise in the field of Program Delivery Management, Technical Sales & Key AccounT Management. Highly skilled Data security & Privacy professional, specializes in Data Privacy (Global Privacy law/regulations/standards & Privacy Information management Systems), Data Governance, Compliance Management & Cloud Security. Currently Heading Solution Engineering for Cyble Inc., managing the global team of some brilliant solutions engineers and architects, which also act as a bridge between the Clients and back-end teams. Responsible to drive business growth across the globe & support Cyble Sales.

He previously worked as a Lead- Global Service delivery & Lead Consultant- Data Governance & Privacy at Provise Consulting (Baker Tilly GCE). In this capacity, he delivered 100+ big ticket projects for diverse businesses ranging from Telecom to Real Estate, predominantly in Middle East, India, South East Asia & Europe region

Before joining Provise, he was associated with Aditya Birla Group (ABG), where he was Leading- Risk & Data Privacy function for BMCSL HR Shared Service. He also worked in the Corporate Information Security team of ABG as a IS & Privacy Project Manager, where he was involved in - Information Security, Data Privacy, Business Continuity, Risk Management & Compliance for the entire ABG conglomerate at the central level with help of the team of 140 ABG CISOs. This includes the challenging task of defining the information security and privacy requirements for a global and sector diverse businesses (such as manufacturing, telecom, finance and retail)

Ankit Sharma can be reached online at ankit.sharma@cyble.com and at our company website https://cyble.com/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



How Digital Signatures Provide the Necessary Safeguards to Restore Trust in The Manufacturing Process

Enhancing Digital Identity Decreases Risks

By Mohit Kumar, Vice President Product Management, GMO GlobalSign

History has taught us that trust must always be complemented by verification. It is replete with examples demonstrating the importance of pressures of greed over taking ethical practices even in dealings involving highly reputed and seemingly dependable parties. It is then incumbent upon chief operations officers (COO's) to enable critical mechanisms that ensure accountability, transparency, and ethical compliance in the processes and regularly monitor and review them in terms of ensuring best practices.

A summer 2023 incident involving the aviation sector which impacted both GE Aerospace and its partner, Safran, is a good example of why this is true. It turns out that a supplier of theirs, London-based AOG Technics, was selling thousands of aircraft engine parts with forged documents and falsified Authorized Release Certifications (ARCs). These unverified components potentially compromised safety standards in jet engines manufactured by GE Aerospace and Safran's joint venture, CFM International, which supplies engines for commercial aircraft. This alarming incident underscores the risks big manufacturers face due to third-party malpractice.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Trust in Data

The episode also highlights the critical importance of ensuring the integrity and verification of information in business transactions. While strong relationships between parties are essential, it cannot replace the need for verified and reliable data. By prioritizing transparency and implementing robust verification mechanisms, businesses can protect their operations and uphold safety and compliance standards.

With the advancements of Artificial Intelligence (AI), COOs must rigorously evaluate the trustworthiness of information within their supply chains, especially for critical and safety-sensitive products and services. They should ask whether the data supporting their decisions can be trusted and identify steps to enhance its reliability. This includes validating the identity of the source of information and ensuring integrity of the data being exchanged. By proactively implementing measures for this, COOs can minimize risks, ensure supply chain integrity, and protect their organizations from potential safety and reputational damage.

How Enhancing Identity Can Improve this Process

Another method of increasing trust is through the use of digital signatures, a robust solution for enhancing the assurance of information in business transactions. Based on widely relied upon technology, Public Key Infrastructure (PKI), digital signatures cryptographically bind the identity of the source to the data—whether emails, documents, or be it any system-to-system communications—ensuring authenticity, reliability, and non-repudiation. As a result, recipients can confidently verify the origin and integrity of the information, reducing the risk of tampering or forgery. This is the reason digital signatures have been mentioned as one of the key recommendations by The Aviation Supply Chain Integrity Coalition. Consisting of global leaders across the aerospace industry, the group aims to help prevent unauthorized propulsion parts from entering the aviation supply chain, thus strengthening its overall integrity – hopefully preventing an incident similar to what took place at the GE Aerospace and Safran's joint venture.

Implementing digital signatures not only enhances trust in processes but also provides a critical defense against phishing, especially Business Email Compromise (BEC) attacks. Some recent examples involve attackers exploiting the templates of popular tools and services to send fraudulent yet convincing phishing emails targeting financial transactions. This unusual but highly effective attack vector underscores the importance of employing technology such as digital signatures to secure system-to-system communications. By ensuring that your users can differentiate information from authenticated and authorized entities, businesses can significantly reduce their exposure to phishing scams and financial fraud.

Incidents like the one that occurred at AOG Technics serve as stark reminders that information absorbed in any system require strong safeguards. By adopting the proper technology and prioritizing transparency, organizations can not only protect their operations but also demonstrate their commitment to integrity and accountability. In an era where risks are evolving rapidly, these measures are not just defenses—they are essential steps toward building a future where trust and security go hand-in-hand.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Mohit Kumar is the Vice President of Product Development at GMO GlobalSign. He joined GlobalSign as a Product Owner in 2018 at the company's office in New Delhi. He now works out of GlobalSign's U.S. office in Portsmouth, New Hampshire. Mohit can be reached online at mohit.kumar@globalsign.com and https://www.globalsign.com/en

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



How Will the Splinternet Impact Cybersecurity?

By Zac Amos, Features Editor, ReHack

Most people think of the internet as a globally connected resource. However, user experiences are not necessarily as consistent as they believe. Factors such as politics, regulations and censorship have made the internet a fragmented "splinternet" for some users. What are the potential implications for cybersecurity?

Changes in Social Media Platforms' Policies

In the early days of the internet, people mostly went directly to website URLs and saw the same content regardless of where they lived. Eventually, companies began using technologies to determine site visitors' locations and provide personalized content.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Social media companies have taken that approach to greater heights, allowing users to follow specific friends, businesses and other types of accounts. However, algorithms still work in the background, dictating what people see on their feeds.

Researchers explored how TikTok's content adapted in response to Russian censorship laws following the country's invasion of Ukraine. These policies resulted in a 95% reduction in the platform's content available to people accessing it in Russia. Additionally, people trying to access accounts created outside Russia with Russian IP addresses saw blank pages. The researchers also found that these TikTok changes proliferated pro-war material on the platform for Russian users. This shift happened despite representatives claiming they banned new information uploads.

Another discovery was that TikTok promoted state-controlled stories. That decision, combined with users suddenly cut off from anything outside Russia, created cybersecurity risks by potentially making people unaware of genuine dangers, such as new online threats.

The short-term ban of TikTok in the United States also revealed that the platform can disappear overnight for some people. Those affected said VPNs did not restore their access, raising concerns about how the platform blocked them. One possibility is that it flagged accounts created in the United States — an approach that would adversely affect people who began using TikTok there and eventually moved elsewhere.

Social media algorithms arguably affect how people see the world. This reality could worsen the spread of misinformation, making cybersecurity professionals' jobs more challenging, especially if people do not believe warnings of known threats — or never see coverage of them to begin with.

Potential for Fewer Cyberattacks

Countries including China, Iran and North Korea heavily censor users' internet access. A common means of censorship is preventing people from using messaging apps made outside of those countries.

One of the few positives of that highly restrictive approach is that it could reduce the number of cyberattacks within those countries or targeting them. Severe limitations on how people can use the internet might make them less likely to experience malware or ransomware.

Recent events indicate that the splinternet could also curb the ramifications of third-party failures. A July 2024 Crowdstrike outage affected numerous countries, most notably making many airports' technology infrastructures inoperable. A flaw within a threat-mitigation and monitoring sensor was to blame. China barely felt the impacts because many entities there do not use Crowdstrike technology. Most of the effects were on foreign organizations operating in China, including hotel chains.

Although China's internet restrictions could make future cyberattacks less likely, they might also have the opposite effect — particularly if criminals learn to exploit the systems and brands used in the country. It's easy to imagine a scenario where Chinese organizations are less able to defend themselves against cyberattacks because of the incompatibility of existing commercial solutions with the nation's tech infrastructure.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Restricted Access to Reputable Cybersecurity Resources

Although many cybersecurity professionals may primarily rely on updates from the organizations in their countries, some frequently keep themselves updated about threats other countries have identified. For example, the United States' Cybersecurity & Infrastructure Security Agency (CISA) publishes bulletins about known exploited vulnerabilities and provides suggested protective measures. Accessing that information is an excellent way to remain proactive against threats appearing in the global landscape.

However, someone who can only access the splinternet may lack that advantage if they can only get cybersecurity updates from entities within the same country where they live.

Sharing information about security threats can greatly reduce their effects. Professionals working to secure infrastructures within nations that limit internet access may be disadvantaged because they cannot learn about threats identified elsewhere.

Similarly, perhaps someone who aspires to work in cybersecurity and has only had access to the splinternet enrolls in an educational program in a country with virtually no restrictions. The sudden opening up of the internet to them could pose a steep, overwhelming learning curve. However, if they remain determined and earn their cybersecurity qualifications, the state of the market offers excellent job opportunities, regardless of where they choose to work.

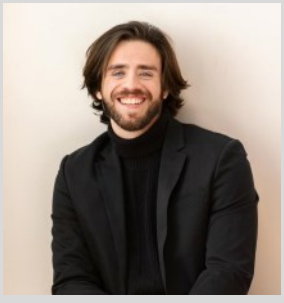
Worldwide, cybercrime cost an average of over $8 trillion in 2023. People with the knowledge to combat it should find themselves in secure, in-demand positions for the foreseeable future. The only possible complication is that the splinternet may further segment the attack surface that cybercriminals target, making professionals' work more demanding.

Responding to New Cybersecurity Concerns

Internet security professionals must remain vigilant against new threats and quickly determine how to combat them. While the splinternet is a cybersecurity complication many people likely overlook, those familiar with the matter believe the internet will only become more fragmented over time. Anyone interested in cybersecurity should stay aware of how things develop, even if the fragmentation does not directly affect them yet.

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.



Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



In The Shifting Threat Landscape, Organizations Need to Ditch Third-Party Agents and Embrace Zero Trust Security

By Amol Dalvi, Vice President, Product, Nerdio

Macro tech trends like AI, distributed cloud environments, and remote work have yielded massive boosts to efficiency, productivity, and convenience for enterprises across the globe. But they've also introduced a variety of cybersecurity threats. Transformative technologies always tend to create new attack vectors and complexity at first, making these environments harder to safeguard. To make matters worse, hackers and bad actors have gotten increasingly sophisticated.

There is a laundry list of strategies and best practices organizations should implement to protect themselves in this shifting landscape. But there are two in particular that I want to focus on: The need for alternatives to third-party agents and the urgency of Zero Trust security.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Third-party agents create an overlooked security risk

One of the most underestimated risks in IT environments is the use of third-party tools that rely on agents installed on servers or end-user devices. Third-party platforms often require the use of agents installed directly on client systems. These agents are essential to the operation of the software. But they create entry points for attackers if they're not regularly updated, patched, or properly configured – and there's little transparency showing how effectively and frequently most vendors are doing each of these. The issue is exacerbated when agents incorporate suboptimal security practices, such as using hardcoded credentials or outdated security protocols.

At a high level, there are three major security issues with third-party agents:

1. **A bigger attack surface**: Every agent running on a server or endpoint becomes another possible way in for attackers. If an agent is vulnerable, the whole environment can be compromised.
2. **Difficult maintenance demands**: Keeping agents secure requires frequent updates and patches, but even the most diligent organizations can fall behind. A delayed patch or missed update can leave systems open to exploitation.
3. **Trusting another entity:** Leveraging a third-party agent means you're handing over a huge amount of trust to someone else, with little control over whether or not they make costly mistakes.

Native Microsoft tools offer safer alternative

Most third-party platforms rely heavily on agents. That's why enterprises should consider native solutions instead. There are a few different choices here depending on your clients' needs. But generally speaking, there's one name you can't go wrong with: Microsoft.

Native Microsoft tools like Microsoft Defender, Azure Virtual Desktop (AVD), and Microsoft Intune all incorporate a secure, scalable architecture. Since these sort of Microsoft native tools are cloud-based and from Microsoft themselves, they minimize the attack surface, providing organizations with a more secure way to manage environments.

There's no need to worry about patching and updates when using Microsoft tools, as the company delivers patches and updates on a regular, weekly cadence (Patch Tuesday). This predictable schedule of updates ensures that systems remain secure without requiring manual intervention. A recent example is the swift resolution of the Windows Kernel TOCTOU vulnerability (CVE-2024-30088), which was patched before widespread exploitation could occur.

Zero Trust security is a must have in today's threat landscape

Zero Trust security has taken off over the past couple years. According to Gartner, 63% of organizations across the world have "fully or partially implemented a Zero Trust strategy." But that still leaves over a third of organizations with no Zero Trust practices in place at all – and a chunk of that 63% are only partially embracing zero trust.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Zero Trust operates under the assumption that threats can exist both inside and outside an organization's network. It aims to improve security by enforcing strict verification and access controls, regardless of whether the user or device is within the corporate network or external to it. Before access to resources is granted, each endpoint is authenticated to reduce unauthorized access and data breaches. The core principle of Zero Trust is "never trust, always verify."

Zero Trust leverages multi-factor authentication (MFA) and other techniques to provide safe access to resources over the public internet. Zero Trust technologies, such as the Microsoft Entra ID Identity and Access Management (IAM) service, support this framework with modern authentication protocols such as OpenID Connect, SAML, and OAuth 2.0. These protocols allow users to security access resources over the public internet, removing the dependency on a secure perimeter network.

In today's shifting IT landscape, which is characterized by increasing hacker sophistication and emerging cybersecurity threats, there's more urgency than ever to embrace Zero Trust security. It's a must have now, not something that should be on the roadmap for years down the road.

Third-party agents can compromise MSPs and their clients

Emerging technologies and IT trends are delivering massive business value to the enterprise. But big change is always a little tricky to manage, too. The challenge of AI, hybrid work, and hyper-distributed clouds is staying ahead of evolving cybersecurity threats. Mitigating these risks takes major alignment from the C-suite and down. That's a significant strategic effort. At a tactical level, there are two easier starting points you should consider: Pivoting from third-party agents and implementing full Zero Trust security across the organization.

About the Author



Amol Dalvi is the VP of Product at Nerdio. With more than 15 years of experience leading product and engineering teams, he is a seasoned software product executive with rich expertise in Microsoft, Cloud, and SaaS. He oversees both Nerdio Manager for MSP and Nerdio Manager for Enterprise products. You can find Amol on LinkedIn and at Nerdio's website here https://getnerdio.com/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Protectors of the Modern World: Defending Against Shadow ML and Agentic AI

By Eyal Dyment, Vice President of Security Products at JFrog

It may sound like hyperbole to say that machine learning operations (MLOps) have become the backbone of our digital future, but it's actually true. Similar to how we view energy grids or transportation systems as part of the critical infrastructure that powers society, AI/ML software and capabilities is quickly becoming essential technology for a wide range of companies, industries, and citizen services.

With artificial intelligence (AI) and machine learning (ML) rapidly transforming industries, we've also seen the rise of a new age of "Shadow IT" now referred to as "Shadow ML," wherein AI agents and technologies are being used by employees without the knowledge or approval of the IT department, outside the company's sanctioned systems, potentially creating significant security risks due to lack of oversight and control over data and access. Thus, understanding the evolving role MLOps plays in managing and securing the rapidly expanding AI/ML IT landscape is essential to safeguarding the interconnected systems that define our era.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Software As Critical Infrastructure

Software is an omnipresent component of our day-to-day lives, operating quietly but indispensably behind the scenes. For that reason, failures in these systems are often hard to detect, can happen at any moment, and spread quickly across the globe, disrupting businesses, upsetting economies, undermining governments or even endangering lives.

The stakes are even more significant as AI and ML technologies increasingly take center stage. Traditional software operations are giving way to AI-driven systems capable of decision-making, prediction, and automation at unprecedented scale. However, like any technology that ushers in new but immense potential, AI and ML also introduce new complexities and risks, elevating the importance and need for strong MLOps security. As reliance on AI/ML grows, the robustness of MLOps security becomes foundational to fending off evolving cyber threats.

Understanding the Risks of the MLOps Lifecycle

The lifecycle of building and deploying ML models is filled with both complexity and opportunity. At its core, these processes include:

- Selecting an appropriate ML algorithm, such as a support vector machine (SVM) or decision tree.
- Feeding a dataset into the algorithm to train the model.
- Producing a pre-trained model that can be queried for predictions.
- Registering the pre-trained model in a model registry.
- Deploying the pre-trained model into production by either embedding it in an app or hosting it on an inference server.

It's a structured approach but one with significant vulnerabilities that threaten stability and security. These vulnerabilities, broadly categorized as inherent and implementation-related, include:

- **Inherent Vulnerabilities:** The complexity of ML environments, including cloud services and open-source tools, can create security gaps that may be exploited.
- **Malicious ML models:** Pre-trained models can be weaponized or intentionally crafted to produce biased or harmful outputs, causing trickle-down damage across dependent systems.
- **Malicious datasets:** Training data can be poisoned to inject subtle yet dangerous behaviors that undermine a model's integrity and reliability.
- **Jupyter "sandbox escapes":** In another example of "Shadow ML," many data scientists today rely on Jupyter Notebook, which can serve as a path for malicious code execution and unauthorized access when not adequately secured.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Implementation Vulnerabilities

- **Authentication shortcomings:** Poor access controls expose MLOps platforms to unauthorized users, enabling data theft or model tampering.
- **Container escape:** Containerized environments with improper configuration allow attackers to break isolation and access the host system and other containers.
- **MLOps platform immaturity:** The rapid pace of innovation in AI/ML often outpaces the development of secure tooling, creating gaps in resilience and reliability.

While AI and ML can offer enormous benefits for organizations, it's crucial not to prioritize rapid development over security. Doing so could compromise ML models and put organizations at risk.

The Vulnerabilities Beneath the Surface

Recognizing and addressing these vulnerabilities is crucial to ensuring MLOps platforms remain trustworthy components of our digital infrastructure. In a recent example, a flagged PyTorch model, previously uploaded by a now-deleted account, could allow attackers to inject arbitrary Python code into critical processes upon loading. The method used to load PyTorch models, specifically the torch.load() function, can be a vector for code execution vulnerabilities, especially when models are trained with Hugging Face's Transformers library.

The "pickle" format, often used for serializing Python objects, poses a particular risk as it can execute arbitrary code when loaded, making it vulnerable to exploitation. This scenario underscores a broader risk in the ML ecosystem. Many widely used ML model formats support code-execution-on-load, a feature meant to create efficient functionality but also introduces significant security vulnerabilities. An attacker controlling a model registry could insert backdoors into models, enabling unauthorized and instant code execution when the models are deployed or loaded.

For this reason, developers must exercise caution when loading models from public repositories, ensuring they validate the source and potential risks associated with the model files. Robust input validation, restricted access, and continuous vulnerability assessments are critical to mitigating risks and ensuring the secure deployment of machine learning solutions.

MLOps Hygiene Best Practices

There are many other vulnerabilities across the MLOps pipeline, underscoring the importance of vigilance among teams. Many separate elements within a model serve as potential attack vectors, which organizations typically manage and secure. Therefore, implementing standard APIs for artifact access and ensuring seamless integration of security tools across various ML platforms for data scientists, machine learning engineers, and core development teams is essential. Key security considerations for MLOps development should include:

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

- **Dependencies and packages:** Teams often use open-source frameworks and libraries like TensorFlow and PyTorch. Providing access to these dependencies from trusted sources—rather than directly from the internet—and conducting vulnerability scans to block malicious packages ensures the security of each component within the model.
- **Source code:** Models are typically developed in languages such as Python, C++, or R. Employing static application security testing (SAST) to scan source code can identify and alleviate errors that may compromise model security.
- **Container images:** Containers are used to deploy models for training and facilitate their use by other developers or applications. Performing comprehensive scans of container images before deployment helps prevent introducing risks into the operational environment.
- **Artifact signing:** Signing all new service components early in the MLOps lifecycle and treating them as immutable units throughout different stages ensures that the application remains unchanged as it advances toward release.
- **Promotion/release blocking:** Automatically rescanning the application or service at each stage of the MLOps pipeline allows for early detection of issues, which in turn helps with swift resolution and maintaining the integrity of the deployment process.

By adhering to these best practices, organizations can effectively safeguard MLOps pipelines and ensure that security measures enhance rather than impede the development and deployment of ML models. As we move further into an AI-driven future, the resilience of the MLOps infrastructure will become an increasingly key component to maintaining the trust, reliability, and security of the digital systems that power the world.

About the Author

Eyal Dyment is Vice President of Security Products at JFrog. Eyal can be reached at our company website: https://jfrog.com/



Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Machine Learning Meets Endpoint Security: Advancements in Predictive Threat Detection

By Unnati Ghosh, My Digital Marketing Manager, HCLSoftware

Traditional security methods seem to be ineffective within today's cyber trends, dynamic markets, and fast-paced IT environments. Organizations need innovative endpoint management solutions that can defend against increasingly modernized and sophisticated threats. Cybercriminals are using advanced techniques to avoid detection, which is making businesses vulnerable to endpoint security challenges. There's an important role played by Machine Learning (ML) that offers predictive threat detection which helps to strengthen endpoint security while also leveraging next-gen technology to address security concerns.

Machine learning can analyze and accessing vast amounts of data, identifying data patterns, and predicting potential threats, all happening in real-time. Considering its integration into endpoint security, it can help organizations detect, respond, and prevent cyberattacks, before they even happen.

In this blog, we'll explore how machine learning is modernizing endpoint security, discover the advancements in predictive threat detection, and deep dive into why it's essential for modern IT security strategies for organizations.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The evolving cyber threat landscape

The weakest links in the organization's security structure are its endpoints – laptops, mobile devices, servers and IoT devices. Endpoints are more prone to various forms of cyberattacks like ransomware, malware, phishing, etc. According to recent **cybersecurity studies,** endpoint devices account for most security breaches worldwide.

Traditional security solutions usually rely on static defenses like signature-based antivirus systems, which can only detect known threats. The problem with this approach is that it fails to identify new, unknown malware or advanced attacks that can easily go unnoticed. The gap in detecting and identifying modern vulnerabilities makes it imperative to have more advanced methods in place that can address zero-day threats and unknown vulnerabilities. This is where vulnerability detection, a crucial feature of advanced endpoint security solutions, plays a crucial role in today's world.

How machine learning enhances endpoint security

Machine learning is a game changer, especially in **predictive threat detection**. Leveraging large datasets and identifying patterns, machine learning can easily recognize and identify irregularities in endpoint behavior. This also helps to detect threats that could have easily gone unnoticed. Machine learning integrates with an endpoint protection platform to provide comprehensive security by not only detecting and preventing attacks but also by offering investigation and remediation features essential for responding to evolving security incidents. Let's discover how it works:



Data analysis at scale for sensitive data

Endpoint protection platforms utilize machine learning algorithms trained on vast amounts of historical data, including system logs, network traffic, and previous attack patterns. This training enables the algorithms to identify abnormal behavior in real time.

Behavioral monitoring on all endpoints

Instead of relying on predefined rules or known threat signatures, an endpoint protection solution continuously monitors endpoint activity and analyzes behaviors. For example, if an endpoint starts acting in a suspicious manner – such as accessing files which it should not communicate with unknown or suspicious IP addresses – the machine learning model can detect and flag a potential threat quickly.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Anomaly detection

Machine learning excels at detecting anomalies. In endpoint security, machine learning algorithms help to identify deviations from normal activity patterns, which might highlight a potential attack. For example, if a user typically accesses files from a specific server during business hours, but suddenly now accesses sensitive data at odd hours, such as nighttime, the system will trigger an alert notifying suspicious activity.

Adaptive learning

One of the most impactful advantages of machine learning in endpoint security is its ability to learn and improve over time. With new threats emerging and new cyberattack techniques progressing, machine learning models can quickly adapt without the need for constant manual updates. This self-learning capability assists security systems in cyberattacks, making systems less vulnerable and more secure.

Predictive threat detection: A shift from reactive to proactive approach

Machine learning's most revolutionary aspect is the ability to predict threats before they happen, making it a crucial component of an effective endpoint security solution. This shift from reacting to threats after they occur to stopping cyberattacks before they start makes security much more proactive.



Key components of predictive threat detection

Threat intelligence integration

The machine-learning model integrates real-time threat intelligence feeds, which helps to stay updated on the latest malware signatures, attack vectors and emerging vulnerabilities. These insights help to predict when a system could potentially be targeted and eventually help to block potential threats early.

Predictive risk scoring

By analyzing historical data, machine learning can calculate a risk score for each endpoint. For example, if an endpoint has been exposed to high-risk websites, applications or networks, then the system can assign it a higher score and allocate additional resources to monitor it.

Zero-day endpoint detection

Traditional endpoint protection methods fail to detect zero-day attacks. This takes advantage of vulnerabilities that haven't been discovered yet. However, machine learning-based security systems are

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

designed to detect these unknown threats. By analyzing behavior patterns that deviate from the usual, these systems can identify suspicious activity even when it doesn't trigger any known signatures, offering enhanced protection against emerging risks.

Advancements in endpoint security with machine learning

Integration of machine learning and endpoint security has brought multiple advancements, enhanced protection levels and reducing the time it takes to detect and mitigate threats.

Reduced false positive triggers

One of the major challenges in the cybersecurity space is the high rate of false positives, where harmless activity is flagged as malicious. This trigger can overwhelm security teams and reduce overall operational efficiency. Machine learning helps to refine this process by accurately identifying real threats and reducing unnecessary alerts.

Faster detection and response times

Machine learning-powered security systems are designed for speed and agility. They can process large volumes of data at incredible speeds, enabling quicker threat detection and faster incident response. This reduction in time can significantly limit the impact caused by attacks.

Enhanced threat-hunting capabilities

Machine learning does not just automate detection; it empowers security analysts to hunt and identify threats more effectively across the enterprise network. By providing a deeper understanding of endpoint behaviors and attack patterns, machine learning helps assist teams to identify unnoticed threats and previously undetected vulnerabilities.

Personalized security and enhanced endpoint protection

Machine learning-based systems can quickly adapt to the specific security needs of an organization. By learning and analyzing an organization's data, the system becomes equipped to detect threats specific to that environment. This personalization results in more accurate protection, tailored to the business needs.

Looking ahead: The future of machine learning in endpoint security

Speaking of technological advancements, machine learning and endpoint security coming together is just the beginning. With machine-learning algorithms becoming more advanced, we can expect advanced automation and threat prediction and faster incident response in the future.

Emerging areas such as **automation** and **AI-powered threat hunting** in the **autonomous endpoint management** space will take endpoint security to the next level, which will allow security systems to operate autonomously while effectively responding to threats in real time.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Conclusion



Machine learning is driving a transformational shift in endpoint security by enabling predictive threat detection. Leveraging data-driven insights, monitoring endpoint behaviors, and identifying anomalies, organizations can now stay ahead of cyber threats and secure their critical assets, more effectively defending their reputation.

Where cyber threats are growing in complexity and volume, machine learning offers an enhanced boost in security strategies, helping organizations move from reactive defense to proactive threat prevention. As advancements in machine learning continue, the future of endpoint security looks brighter and more secure than ever for organizations at large.

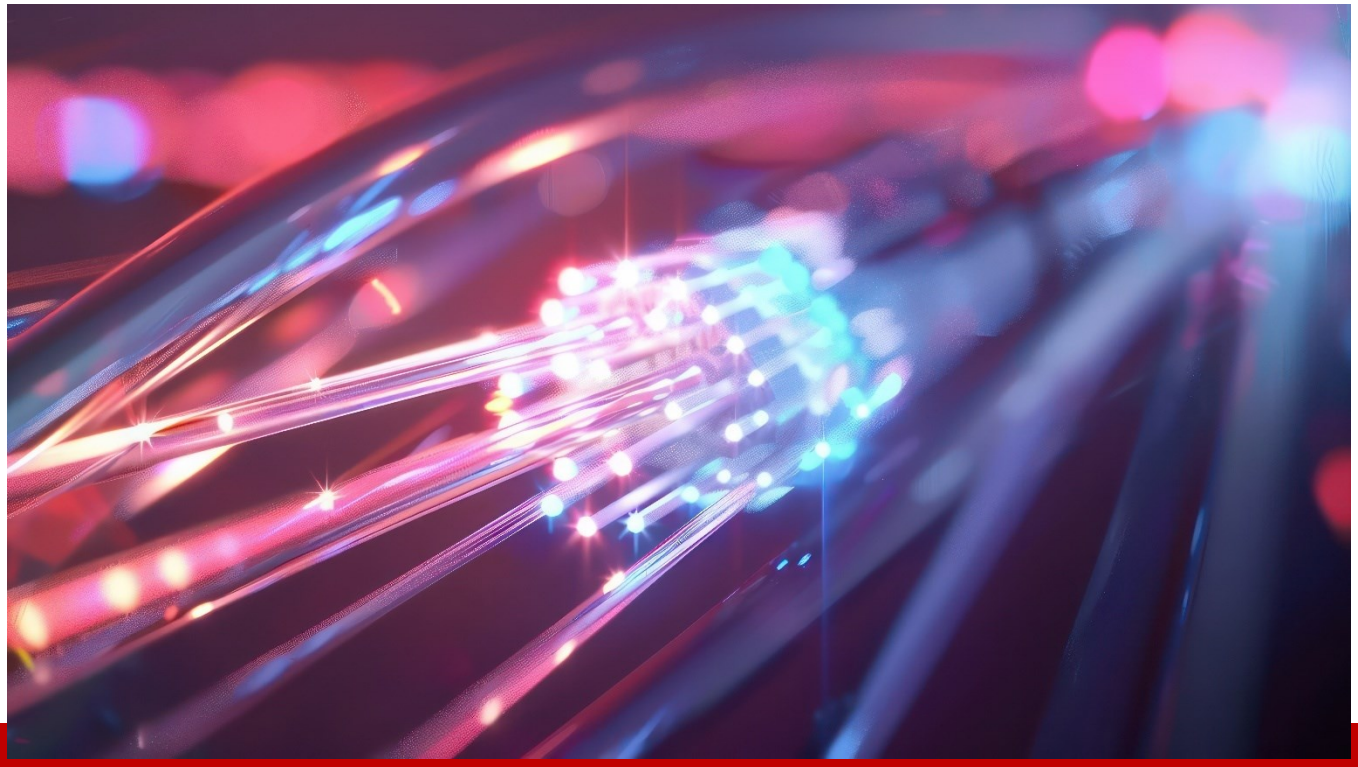
About the Author



Unnati Ghosh is a Digital Marketing Manager with over a decade experience creating and executing B2C and B2B digital campaigns. She currently works as a digital marketing manager at HCLSoftware. Currently, she is responsible for creating transformative digital, social media and search engine optimization strategies. Before joining HCLSoftware, she worked with Dell Technologies Inc., executing social media campaigns.

Unnati can be reached at Unnati.ghosh@hcl-software.com and on our website https://www.hcl-software.com.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



The Future of Fiber Optic Sensors: Breakthroughs Shaping the Next Generation

Advancements in Fiber Optic Sensing Technology Revolutionizing Industries and Driving Innovation

By Amit Mohite, Media Relations Team, Transparency Market Research

Fiber optic sensors have quickly become a cornerstone of modern technology. Renowned for their precision and versatility, they are used in everything from telecommunications to healthcare. But as we approach 2025, exciting advancements are on the horizon that could redefine how these sensors work and where they're applied. With industries demanding smarter, faster, and more durable solutions, the evolution of fiber optic sensors stands at an exciting crossroads.

The Current Landscape of Fiber Optic Sensors

Fiber optic sensors are highly sought after due to their ability to transmit data with extreme accuracy and speed. Relying on light rather than electrical signals, they offer reliability in environments that often pose challenges to traditional sensors.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Applications in Industries

Currently, fiber optic sensors are critical in several sectors. In **telecommunications**, they enable high-speed internet and global connectivity by transmitting vast amounts of data through optical fibers. The **healthcare industry** uses these sensors in procedures like laser surgeries and for monitoring vital signs. In the **aerospace sector**, they play a key role in structural health monitoring, ensuring planes and spacecraft function reliably under stress.

Beyond these, industries like oil and gas, automotive, and manufacturing also benefit from the unique advantages of fiber optic sensing technology.

Technological Limitations

While effective, fiber optic sensors aren't without issues. **Cost** remains a major hurdle. The materials and manufacturing processes are expensive, which limits widespread adoption in cost-sensitive industries. Another challenge is **fragility** — optical fibers are thin and prone to damage, particularly in rough environments. Finally, **scalability** is difficult. Integrating these sensors into complex systems often involves technical and logistical roadblocks.

Emerging Innovations in Fiber Optic Sensors for 2025

As technology evolves, so do the possibilities for fiber optic sensors. With some of the brightest minds in engineering and material science focused on improving performance, 2025 promises some groundbreaking advancements.

Next-Generation Materials

One area of focus is the development of stronger, more durable materials. Imagine sensors that can withstand extreme temperatures, vibrations, or pressure without compromising.

performance. Researchers are experimenting with advanced polymers and nanomaterials to make fibers more resistant to wear and tear. This improvement could significantly lower maintenance costs and extend the lifespan of fiber optic systems.

Integration with AI and IoT

The marriage of **fiber optic sensors, Artificial Intelligence (AI), and the Internet of Things (IoT)** is expected to change the game. In 2025, sensors will likely be smarter than ever, analyzing data in real time and providing actionable insights without human intervention. Whether it's monitoring a bridge for structural integrity or managing the energy grid, AI-powered fiber optic sensors will streamline processes and make devices capable of learning from their environments.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Miniaturization and Portability

Smaller sensors mean more versatility. By 2025, advancements in miniaturization will lead to fiber optic sensors that are not only powerful but also portable. These compact sensors could be embedded into small medical devices, wearables, or drones, making them more adaptable than ever. This shift will open new doors to innovation, particularly in fields like healthcare and environmental monitoring.

Fiber Optic Sensors Market

The global fiber optic sensors market is projected to grow rapidly in the coming years. Valued at **$3.4 billion in 2022**, it is expected to reach **$7.6 billion by 2031**, with a robust compound annual growth rate (CAGR) of **9.6%**. This growth reflects the rising demand for better data transmission, safety monitoring, and smart solutions across multiple industries.

Key Sectors Benefiting from 2025 Advancements

The advancements expected in 2025 won't benefit just one industry — they're poised to transform multiple sectors, each with unique use cases for enhanced fiber optic technology.

Healthcare Revolution

Imagine the next wave of **non-invasive medical diagnostics** powered by fiber optic technology. By 2025, sensors could play a crucial role in everything from real-time blood monitoring to advanced imaging systems. These improvements will enhance the precision of surgical tools and patient monitoring devices. For healthcare providers, this means delivering more accurate treatments faster.

Smart Cities and Infrastructure Monitoring

Fiber optic sensors are becoming the backbone of smart city **infrastructure**. With advancements in 2025, these sensors will monitor everything from traffic patterns to water quality. City planners will receive instant alerts for structural changes in bridges, pipelines, or roads, helping prevent accidents and ensure public safety. This approach combines efficiency with sustainability, an essential element in modern urban development.

Energy and Environmental Applications

From optimizing solar power systems to detecting gas leaks, energy and environmental sectors are well-positioned to benefit. Tomorrow's fiber optic sensors will offer high sensitivity, making it easier to detect

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

minute changes in conditions. For instance, they could monitor air or water quality with incredible accuracy, contributing to more effective environmental preservation efforts.

Challenges Ahead for Fiber Optic Sensors

While the future of fiber optic sensors is bright, there are still challenges to address before these technologies can reach their full potential.

Cost-Benefit Analysis

Developing and implementing advanced fiber optic sensors is expensive, raising questions about cost-effectiveness. Industries need to weigh the upfront costs against long-term benefits. Although prices may drop with mass production, striking the right balance will remain tricky in the short term.

Standardization and Regulation

As these sensors find widespread use, **industry standards and government regulations** will need to catch up. Without clear guidelines, integrating fiber optic sensors into critical sectors like healthcare or aviation can introduce risks. Establishing uniformity in manufacturing and testing will be essential to prevent safety concerns and build trust across industries.

Future outlook

Fiber optic sensors are on the cusp of a transformative era. By 2025, advancements in materials, integration with AI and IoT, and improved portability will unlock a world of possibilities. From revolutionizing healthcare to building smarter cities, the technology holds immense potential to make industries safer, more efficient, and environmentally friendly. Although challenges like costs and regulatory hurdles remain, the trajectory of this innovation is undeniably upward. The future of fiber optic sensors isn't just near — it's already taking shape, and it's bound to leave a lasting impact on the way we live and work.

These insights are based on a report on Fiber Optic Sensors Market by Transparency Market Research

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Amit Mohite is a seasoned media relations professional specializing in the IT and semiconductor sectors. At Transparency Market Research, he excels at translating complex market insights into compelling narratives that resonate with a global audience. With a deep understanding of emerging trends and technological innovations, Amit plays a pivotal role in bridging the gap between rigorous research and dynamic media strategies, ensuring that industry developments are communicated with clarity and impact. For more insights, connect with Amit Mohite

Visit: **https://www.transparencymarketresearch.com/**

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Navigating Department of Defense CMMC Compliance: A Guide For Subcontractors

By Matt Gilbert, Principal, Baker Tilly

The recent implementation of the Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) program in late 2024 raises important questions about its applicability and the challenges it poses for smaller contractors within the defense industrial base (DIB) supply chain who may not yet be ready to comply. Aimed at protecting federal contract information (FCI) and controlled unclassified information (CUI) within the DoD contracting community, CMMC applies to both prime contractors and their suppliers and subcontractors that handle FCI and CUI, potentially creating a significant ripple effect.

As a critical component of national security, the DIB is particularly targeted and the subject of data breaches, ransomware, and other cyber threats. Ensuring business continuity for all DoD suppliers and service providers in the event of a cyber-attack is crucial. While CMMC requirements will come as no surprise to prime government contractors who have ostensibly already allocated resources to assure readiness, their subcontractors are likely less prepared. Many suppliers and subcontractors may not consider themselves DoD contractors and could be unaware of their upcoming compliance obligations.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Education, resource allocation, and preparation are essential to ensure that all necessary members of the DIB have the robust security measures required to meet CMMC standards.

Let's break down what this means for subcontractors.

CMMC applies to all contractors within the DIB that handle FCI or CUI, but applicability is nuanced.

CMMC aims to ensure organizations can protect sensitive government data crucial to the DoD's work with contractors and subcontractors. Certification provides the DoD with greater confidence that organizations meet cybersecurity requirements for nonfederal systems handling federal contract information (FCI) and controlled unclassified information (CUI).

Primary DoD contractors must comply with CMMC if they handle CUI or FCI, but the extent of supply chain accountability varies by organization and shared information. CMMC Level 1 includes a basic set of controls designed to protect FCI. CMMC Level 2 and 3 are much more demanding and designed to protect CUI. CMMC level 2compliance follows CUI; if taking possession of CUI is essential for all parties to complete their tasks under the contract, everyone must implement the CMMC requirements. However, if a subcontractor can complete their work without CUI, certification is unnecessary.

The CMMC program has three levels reflecting cybersecurity maturity. Level 1 covers basic requirements for protecting FCI, while Level 3 addresses the most advanced needs. The required certification level depends on the DoD-related information received. Subcontractors who handle CUI need at least Level 2 certification, but identifying CUI can be complex. It is likely the prime contractor and DoD will error on the side of caution and indicate more items are CUI than not.

Subcontractors can determine their CMMC requirements by checking if their clients and partners have DFARS 252.204-7012, 7019, 7020, or 7021 clauses in their DoD contracts or if proposals or agreements mention CMMC compliance. The DoD and prime contractors will have historically included these clauses when CUI is shared. The DoD is also going to add specific contract clauses associated with CMMC in the future. For planning purposes if there are legacy clauses, it is likely in the future there will be CMMC clauses at level 2 or higher.

All primary contractors must flow down these clauses in subcontracts involving CUI or covered defense information. These requirements then extend to each level handling CUI, potentially reaching multiple levels down the supply chain.

The final CMMC program rule took effect on December 16, 2024, allowing organizations to receive certification through certified third-party assessor organizations (C3PAOs). Currently, CMMC is not mandatory for all new DoD contracts, but this will change later this year when the second CMMC rule establishing the contractual clause is finalized.

For subcontractors looking to achieve certification, here are some steps to consider.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Examine the business case for CMMC.

Subcontractors should begin by evaluating the business rationale for obtaining certification. If a significant portion of their clientele is engaged in DoD-related work where handling CUI is required, certification is essential. Conversely, if DoD-related work constitutes a minor segment of their customer base and certification could adversely affect the rest of the organization because it is too distracting or expensive, it might be wise to delay and ultimately exit the business.

However, if an organization anticipates being subject to CMMC requirements at any level or wants to grow their DoD business taking work from others who might exit or delay in being compliant, it is advisable to pursue certification promptly. Initially, CMMC certification will offer a substantial competitive edge, but this advantage will diminish as more organizations become certified. Therefore, for organizations aiming to broaden their market presence, achieving CMMC certification could be a strategic business move.

Determine the scope.

The CMMC certification process can be particularly challenging for smaller companies. To balance the potential financial and operational impacts of compliance, a good starting point is determining what's in and out of scope.

Organizations aiming for a level 2 or higher certification must consider five asset classes:

- ***CUI assets:*** These process, store, or transmit CUI.
- ***Contractor risk managed assets:*** These assets can - but are not intended to - process, store, or transmit CUI.
- ***Security protection assets:*** These provide security functions or capabilities within the CMMC Assessment Scope, regardless of whether they process, store, or transmit CUI (e.g., firewalls, multifactor authentication tools).
- ***Out-of-scope assets:*** These do not process, store, or transmit CUI or security protections for CUI assets and are physically and/or logically separated from CUI-handling assets (e.g., cloud-based HR systems, non-DoD project branches or locations).
- ***Specialized assets:*** These can process, store, or transmit CUI but support a special function. These assets are excluded from the assessment scope. Typically, these are excluded because they cannot be fully secured. Examples or specialized assets include test equipment, CNC or other manufacturing or assembly automation tools. Since these assets may be exempt from some CMMC requirements, understanding and properly categorization can be advantageous Subcontractors should leverage a strong understanding of the asset categories and especially the specialized assets class to help minimize the scope burden and allow for effective allocation of resources. By limiting the size and complexity of the in-scope assets, the certification process becomes faster, easier, and less expensive.

Subcontractors should also explore restructuring their organizations or operations to continue DoD- and CUI-related work without it impacting the entire organization. For instance, consolidating all CUI work into

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

one branch or location can limit the assessment scope to only that branch, expediting the certification process.

Consider how the CMMC assessment covers third party ESPs and CSPs.

One additional important scoping consideration is understanding how the CMMC assessment differentiates between third party external service providers (ESPs) and cloud service providers (CSPs). This is crucial to both Organizations Seeking Assessment (OSAs) using external ESPs and/or CSPs, and the ESPs and CSPs themselves.

- ***ESPs:*** If an OSA uses an ESP (other than a CSP), the ESP must have implemented the CMMC Level 2 or higher requirements. Their security measures should be documented in the OSA's System Security Plan (SSP) and the ESP likely will have to participate in the OSA's assessment process.
- ***CSPs:*** The final CMMC rule stipulates that an Organization Seeking Certification (OSC) can use a FedRAMP moderate (or higher) cloud environment to handle Controlled Unclassified Information (CUI) if the CSP is FedRAMP authorized or meets equivalent security requirements.

The Department of Defense (DOD) requires CSPs that are claiming equivalency to achieve 100% compliance with FedRAMP Moderate security controls, verified by a recognized Third-Party Assessment Organization (3PAO), and provide specific documentation as part of the Body of Evidence (BoE). This ensures stringent security standards are met.

Allocate resources to prepare for the assessment.

The CMMC certification process is straightforward, but preparation can be complex. Administered by the not-for-profit Cyber Accreditation Body (Cyber-AB), which consists of experienced industry professionals, the process involves OSCs requesting proposals or quotes from C3PAOs authorized by Cyber-AB to conduct CMMC assessments.

The DoD provides resources to help organizations evaluate their readiness and prepare for assessment, which includes the Assessment Guide, containing the assessment questions, and the CMMC Scoping Guide that details the asset categories and assessment methods.

Before engaging a C3PAO, subcontractors should take several preparatory steps:

- Properly identify and organize their scope according to the five asset categories.
- Ensure their System Security Plan (SSP) is robust enough to demonstrate understanding of the requirements and how they are being met.
- Document and approve all CUI data flows to show organizational maturity and control over CUI storage and movement.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

- Conduct internal and mock assessments to prepare the team for questions from the assessment team and ensure documentation is available to support the implementation of all 110 CMMC controls for in-scope systems.

Organizations often encounter common pitfalls, such as uncertainty about which CMMC level to target, incomplete asset inventories, and difficulties in identifying and tracking FCI and CUI. Smaller subcontractors, in particular, may struggle due to limited resources. When pursuing CMMC certification, it is crucial to have a dedicated cross-functional team focused on gathering all necessary documentation and information. Involving the right people, including executives and not just IT personnel, is essential to avoid a more costly and prolonged certification process.

Engaging a third-party consultant with extensive knowledge of the CMMC process can be beneficial. These consultants can view the subcontractor from an assessor's perspective, helping to identify and address potential issues before the actual certification process begins.

Determining CMMC assessment readiness can be complex, but starting with these six questions can help:

1. Have I completed my system security plan (SSP), CUI data flows, and associated policies and procedures?
2. Have I conducted a self-assessment and confirmed that our organization complies with all CMMC practices and their assessment objectives?
3. Have I gathered evidence for each assessment object?
4. Have I evaluated my external service providers and cloud service providers?
5. Have I trained my control owners on what to expect and how to properly implement CMMC practices?
6. Have I identified my CMMC assessor, and do I believe they will be fair, reasonable, and available within the required timeframe?

Engage with a C3PAO and undergo the CMMC assessment.

Once contracted for an assessment, the C3PAO will either utilize a certified assessor on staff or hire an independent assessor to carry out the work. The C3PAO will oversee the entire process, including quality assurance, ensuring the assessment's credibility and proper execution, and submitting the results to the DoD.

The CMMC certification process typically takes four to eight weeks, depending on the size and scope, and begins with a phase to understand the scope and ensure the OSC is prepared. The OSC will then need to gather and provide artifacts to demonstrate that the required practices are in place. The primary effort occurs during the fieldwork phase, usually a busy week of concentrated activity, where artifacts and live demonstrations provide the assessment team with the evidence needed to determine if practices are implemented. Finally, the process concludes with wrap-up and reporting.

If there is missing information or something amiss during the certification process, organizations may receive a provisional certification and enter a remediation period, during which the OSC has six-months

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

to resolve any remediation-eligible problems, also known as plan of action and milestone (POA&M) items. If an organization completes those POA&Ms within the set timeframe, they'll be eligible to receive full certification.

The bottom line.

It is important to remember that CMMC's requirements are not limited to primary DoD contractors and applicability is not determined by the size of the organization. Understanding what is in and out of scope, the necessary level of certification, how CMMC applies to third-party suppliers or service providers, and what is needed to pass the assessment is complex and requires significant resources. Taking a hybrid approach that combines internal and external expertise will help OSCs ensure that their own organization, as well as their third-party suppliers, are compliant with all appropriate requirements, minimizing certification costs and operating strains.

About the Author



Matt Gilbert leads Baker Tilly's cybersecurity maturity model certification (CMMC) and government contractor IT risk suite of services. His experience includes internal auditing, SOX compliance, information technology controls, business process controls and ERP risk and controls. Matt is actively engaged in supporting government contractors, grant recipients, state and local governments and federal agencies to navigate the CMMC requirements but has extensive experience supporting NIST 800-171 and 800-53-related assessments. Matt can be reached online at Matt.Gilbert@bakertilly.com and at Baker Tilly's website, https://www.bakertilly.com/.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



1 in 5 Emails Could Be Scams: Why Businesses Must Prioritize Email Security

By Craig McCurdy. Chief Information Security Consultant, Sabre Secure

Email has become both a lifeline for communication and a prime target for cybercriminals. For small and medium-sized businesses, it is the lifeline between the business and its customers and partners. Recent findings by Forfend, an email security software provider, indicate that approximately 1 in 5 emails sent in 2024 contained potential phishing threats. This alarming statistic highlights a growing need for robust email security measures, as AI-driven phishing scams are on the rise.

The cybersecurity landscape is evolving rapidly. According to cybersecurity experts, email remains the gateway for more than 90% of cyberattacks. Phishing emails—fraudulent messages designed to trick recipients into divulging sensitive information or clicking malicious links—have become increasingly sophisticated, often bypassing traditional security measures.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Why SMBs Are Particularly Vulnerable

Small and medium-sized businesses (SMBs) face unique challenges when it comes to cybersecurity. Unlike larger organizations, SMBs often lack dedicated IT teams and resources to address complex cyber threats. Many rely on outsourced IT solutions or basic email security features, which may not be sufficient to combat the growing sophistication of phishing scams.

Jeff Wolverton, CEO of the IT consulting firm PivIT Strategy, emphasizes the increasing accessibility of phishing tools. “With the rise of generative AI, creating realistic phishing and malware campaigns is easier than ever,” he says. “Businesses need to enhance their email platforms with advanced security measures to stay ahead of these threats.”

The Hidden Costs of Phishing

Phishing attacks are not merely a technical issue; they’re a significant business risk. Beyond the immediate financial losses from stolen funds or ransomware payments, businesses often suffer reputational damage and operational downtime. These incidents can erode customer trust and lead to compliance violations, particularly in industries handling sensitive customer data.

In one analysis of 35,000 customer emails, approximately 20% were flagged as scams. Preventative measures successfully blocked these phishing attempts, saving nearly $2 million in potential losses. This underscores the importance of proactive defense mechanisms to safeguard both financial assets and operational continuity.

How Phishing Scams Work

Phishing scams exploit human psychology and technological vulnerabilities. Here are some common tactics used by cybercriminals:

1. **Generic Greetings:** Phishing emails often address recipients with vague terms like "Dear Customer," avoiding personalized details.
2. **Urgency and Fear:** Scammers create a sense of urgency, prompting immediate action—such as clicking a link—without careful scrutiny.
3. **Spoofed Email Addresses:** Phishing emails frequently use addresses that mimic legitimate organizations, with minor misspellings that are easy to overlook.
4. **Malicious Links:** Hyperlinks in phishing emails may appear legitimate but redirect users to fake websites designed to steal login credentials or other sensitive information.
5. **Requests for Personal Data:** Legitimate organizations rarely ask for sensitive information like passwords or credit card details via email.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Tips to Safeguard Against Phishing

For those companies that do not have an annual review plan, this serves as a timely reminder for businesses to reassess their email security practices. Here are some practical tips to protect against phishing:

1. **Check the Sender's Email Address:** Verify email addresses for discrepancies or misspellings that might indicate a spoofed account.
2. **Look for Personalization:** Legitimate emails typically address recipients by name. Be cautious of generic greetings.
3. **Hover Over Links:** Before clicking on any link, hover over it to view the actual destination URL. If it looks unfamiliar or suspicious, do not click.
4. **Verify Requests for Sensitive Information:** Contact the sender through official channels to confirm any email requesting sensitive details.
5. **Educate Your Team:** Regular training on recognizing phishing scams can empower employees to act as the first line of defense.

The Role of Technology in Combatting Phishing

While awareness and training are crucial, advanced technology is equally important in defending against phishing attacks. Tools equipped with artificial intelligence can analyze email content, detect anomalies, and flag suspicious behavior in real time. Features like URL analysis, sender verification, and behavioral analytics help organizations identify and block phishing attempts before they reach employees' inboxes.

Yash Agarwal, a security software expert and CEO of Forfend, stresses the importance of proactive measures: "Phishing attacks aren't just an IT problem; they're a business risk. Every click matters, and the right solutions ensure your team stays focused on growth, not damage control."

Looking Ahead: Cybersecurity in 2025 and Beyond

As AI-generated scams become more prevalent, businesses must adapt to an ever-evolving threat landscape. Cybercriminals are leveraging AI to craft highly convincing phishing emails, making traditional security measures less effective. Organizations that fail to prioritize email security risk falling victim to these increasingly sophisticated attacks.

It's never too late for businesses to reflect on their cybersecurity practices and make necessary improvements. Whether through employee education, advanced email security tools, or a combination of both, taking proactive steps can significantly reduce the risk of phishing attacks.

Cybersecurity is no longer optional; it's essential. By investing in robust defenses and fostering a culture of vigilance, businesses can protect their operations, their customers, and their reputations from the growing threat of cybercrime.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Craig McCurdy is a seasoned leader driving transformative security strategies for organizations across industries, with over two decades of experience in cybersecurity, information technology, and enterprise infrastructure. Currently serving as the Chief Information Security Consultant at Saber Secure, LLC, Craig helps organizations strengthen their cybersecurity posture through comprehensive risk management and innovative solutions.

Previously, Craig held executive roles as the Vice President of Information Security (CISO) at American Credit Acceptance, where he led end-to-end security programs encompassing risk management, identity and access management, and regulatory compliance. As VP of Infrastructure and Security at CommunityAmerica Credit Union, he developed robust security frameworks and ensured the stability and scalability of enterprise IT infrastructures.

Craig also brings deep expertise in data protection, IT operations, and compliance from leadership roles at H&R Block, Freeman, First Tennessee Bank, and Sprint. As H&R Block's first Chief Security Officer, he established a global security program, including a cyber operations team and governance frameworks aligned with industry standards.

Beyond his technical leadership, Craig has advised board members on investment strategies for cybersecurity technologies and has a proven track record of implementing NIST cybersecurity frameworks and ITIL service management practices.

Craig combines technical acumen, strategic vision, and hands-on experience to build resilient systems and drive organizational success in an ever-evolving digital landscape.

Craig can be reached online at mccurdyciso@gmail.com and on LinkedIn at linkedin.com/in/mccurdyc.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Online Account Security

By Milica D. Djekic

Online accounts are integral to cloud computing, encompassing private, public, and hybrid services that store vast amounts of data across servers and datacenters. These accounts include:

- **Email platforms**
- **Social media accounts**
- **Knowledge bases**
- **Professional web-based tools**

Like any digital asset, online accounts are vulnerable to cyber-attacks. The consequences of sabotage, espionage, or diversion could be catastrophic, potentially destabilizing networks that serve millions of users.

The Risks of Online Account Vulnerability

Online accounts are critical assets that impact both personal lives and businesses. A cyber-attack targeting cloud infrastructure can have severe consequences:

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

- **Service Disruptions:** Attacks on cloud storage can temporarily render services unavailable, even if backup solutions exist.
- **Economic Impact:** Business continuity interruptions can lead to significant financial losses.
- **Data Breaches:** Unauthorized access to sensitive data can result in identity theft, fraud, or corporate espionage.

Cybersecurity experts recommend continuous **supervision and real-time monitoring** of cloud-based systems using **Security Operations Centers (SOCs)**. These centers play a crucial role in managing risks and ensuring system reliability.

Cyber Threats in the Online Space

The digital landscape is highly susceptible to **asymmetric cyber threats**, where small groups of attackers can cause disproportionate damage. Common attack vectors include:

- **Malware Infections:** Hackers can infiltrate networks with malicious software, disrupting operations.
- **Data Storage Attacks:** Cloud databases can be compromised, leading to service shutdowns.
- **Distributed Denial-of-Service (DDoS) Attacks:** Overloading network traffic can paralyze entire systems.

To counter these threats, cybersecurity best practices emphasize **web storage protection and online account security** as top priorities.

The Importance of Cybersecurity Best Practices

Ensuring the security of online accounts requires a proactive approach. Organizations must:

- **Implement Cryptographic Security:** Encryption ensures secure data transmission and protects sensitive information.
- **Enforce Strong Authentication Measures:** Multi-factor authentication (MFA) adds an extra layer of security.
- **Conduct Continuous Risk Assessments:** Regular security audits help identify vulnerabilities before they can be exploited.

In today's interconnected world, cybersecurity is not just a technical concern—it is a fundamental requirement for businesses and individuals alike.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Cybersecurity in the Financial Sector

Online banking and financial services are particularly vulnerable to cyber threats. Banks store massive amounts of customer data on high-performance servers, making them prime targets for hackers. Potential consequences of cyber-attacks on financial institutions include:

- **Disruption of Banking Operations:** Service downtime can halt transactions and payments, affecting businesses and individuals.
- **Economic Instability:** A compromised financial sector can lead to broader economic consequences at national and international levels.
- **Erosion of Trust:** Security breaches can undermine consumer confidence in online banking services.

Recognizing these risks, most advanced economies treat banking as **critical infrastructure**, implementing real-time monitoring and security protocols to prevent cyber threats.

Conclusion

Modern society is deeply dependent on online account security. Whether for personal, business, or financial purposes, reliable **data storage and secure communication** are essential. By strengthening cybersecurity measures, we can:

- Ensure **safer online experiences**
- Protect **sensitive data**
- Maintain **trust in digital infrastructure**

As technology evolves, so do cyber threats. Organizations and individuals must remain vigilant, embracing cybersecurity as a **mission-critical priority** in the digital age.

About The Author



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

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Operational Resilience

Aligning Resilience Capabilities with the Digital Future

By Renato Lima, Eletrobras

1. Introduction

In the business world, operational resilience can be compared to the physical concept of resilience, which defines the ability of a material to return to its original state after being subjected to an external force. In the cybersecurity landscape, this idea is further expanded by the concept of antifragility, introduced by Nassim Taleb, which suggests that truly robust systems not only withstand shocks but also evolve and strengthen in response to them.

Imagine a global retail giant during Black Friday facing a ransomware attack that disrupts part of its digital infrastructure. A resilient organization would not only restore operations swiftly through well-planned backups and redundancies, but it would also leverage the crisis to identify vulnerabilities and implement improvements that mitigate future risks. In this case, the company does not merely return to its original state—it emerges stronger. This is antifragility in action.

Cyber resilience requires organizations to anticipate, detect, respond to, and learn from incidents. More than just minimizing impacts, it is about leveraging chaos to innovate and grow. Business leaders who

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

adopt this mindset are not just protecting their organizations; they are ensuring their long-term relevance and competitive advantage in a rapidly evolving digital economy.

In an era of accelerated digital transformation, organizations must balance innovation, security, and regulatory compliance. Operational resilience has become a competitive differentiator, particularly in an environment where cyber threats are escalating, and regulations such as the Digital Operational Resilience Act (DORA) in the European Union demand heightened cybersecurity governance.

This article explores how businesses can strengthen operational resilience by focusing on four essential pillars:

1. Cyber Risk Management
2. Cyber Resilience
3. Business Continuity and Crisis Management
4. Third-Party and Critical Services Risk Management

2. Cyber Risk Management: Defining Risk Appetite

Effective cyber risk management is the foundation of any operational resilience strategy. A key component is risk appetite, which defines an organization's tolerance for adverse events. This framework should be aligned with strategic objectives and guide security investment priorities.

Why Defining Risk Appetite is Critical:

✓ Aligns security decisions with business objectives.

✓ Ensures efficient resource allocation to mitigate the most critical risks.

✓ Facilitates clear communication with stakeholders, including C-suite executives and boards.

Example: A financial institution may classify data privacy breaches as unacceptable, prioritizing rigorous security controls to comply with GDPR and LGPD regulations.

In Europe, DORA mandates that financial institutions embed cyber risk management within their governance frameworks, ensuring resilience across the entire value chain.

Best Practices for Cyber Risk Management:

✓ Implement industry frameworks such as ISO 27001 and NIST Cybersecurity Framework.

✓ Continuously monitor risks and leverage threat intelligence.

✓ Develop dashboards that translate technical risks into executive-level insights.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

3. Cyber Resilience

Adapting to an Ever-Changing Threat Landscape

Cyber resilience is more than just protecting systems—it ensures that an organization can continue operations even under attack. This concept encompasses preventing, detecting, responding to, and recovering from cyber incidents.

Key Cyber Resilience Strategies:

✓ Zero Trust Architecture → Restricts access to minimize attack surfaces.

✓ Cyber stress testing → Simulates extreme attack scenarios to identify vulnerabilities in critical systems.

✓ Automated incident response → Extended Detection and Response (XDR) platforms can accelerate threat containment and recovery.

Regulatory Insight: DORA mandates regular resilience testing, including stress simulations, to assess preparedness against real-world threats.

Additionally, integrating cyber resilience with data privacy is crucial to avoid regulatory penalties and reputational damage

4. Business Continuity and Crisis Management

Preparing for the Unexpected Business Continuity Management (BCM) enables organizations to overcome disruptions without impacting critical operations. In today's digital landscape, seamless integration between BCM and cybersecurity is imperative.

Key Components of a Robust BCM Strategy:

✓ Well-documented and regularly tested disaster recovery plans.

✓ Clear crisis communication protocols, aligned with regulators and stakeholders.

✓ Continuous infrastructure monitoring to detect and mitigate failures proactively.

European Compliance: Under DORA, organizations must regularly assess and validate the resilience of their critical systems to ensure uninterrupted essential services.

Additionally, data privacy must be embedded in business continuity plans, as exposure of sensitive data during a crisis can trigger severe regulatory sanctions and erode customer trust.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

5. Third-Party and Critical Services Risk Management

Organizations are increasingly dependent on third-party service providers, expanding their attack surface. A security incident at a vendor or partner can compromise data integrity and disrupt operations.

Regulatory Emphasis:

✓ DORA requires continuous monitoring of third-party cybersecurity risks.

✓ Companies must ensure that external providers comply with cybersecurity and data protection standards.

Best Practices for Third-Party Risk Management:

✓ Regular audits of critical vendors.

✓ Contractual clauses enforcing privacy and security compliance.

✓ Incorporating third-party vendors into crisis simulations to assess their resilience capabilities.

Example: A company relying on cloud service providers must verify compliance with ISO 27017 (Cloud Security) and GDPR, ensuring adequate data protection controls.

6. Conclusion

Operational resilience is not merely a defensive strategy—it is a roadmap for thriving in an increasingly complex digital world. Organizations that integrate cyber risk management, cyber resilience, business continuity, and third-party risk governance into their operations will be well-positioned to lead in the digital future.

The European regulatory framework, exemplified by DORA, underscores the necessity of embedding resilience into governance structures and supply chains. By adopting robust resilience frameworks, organizations can not only withstand cyber threats but also emerge stronger from disruptions.

7. Final Message to C-Suite Executives

The future of your organization depends on how well you can anticipate, respond to, and evolve in the face of cyber crises. Invest in resilience today to lead with confidence tomorrow.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



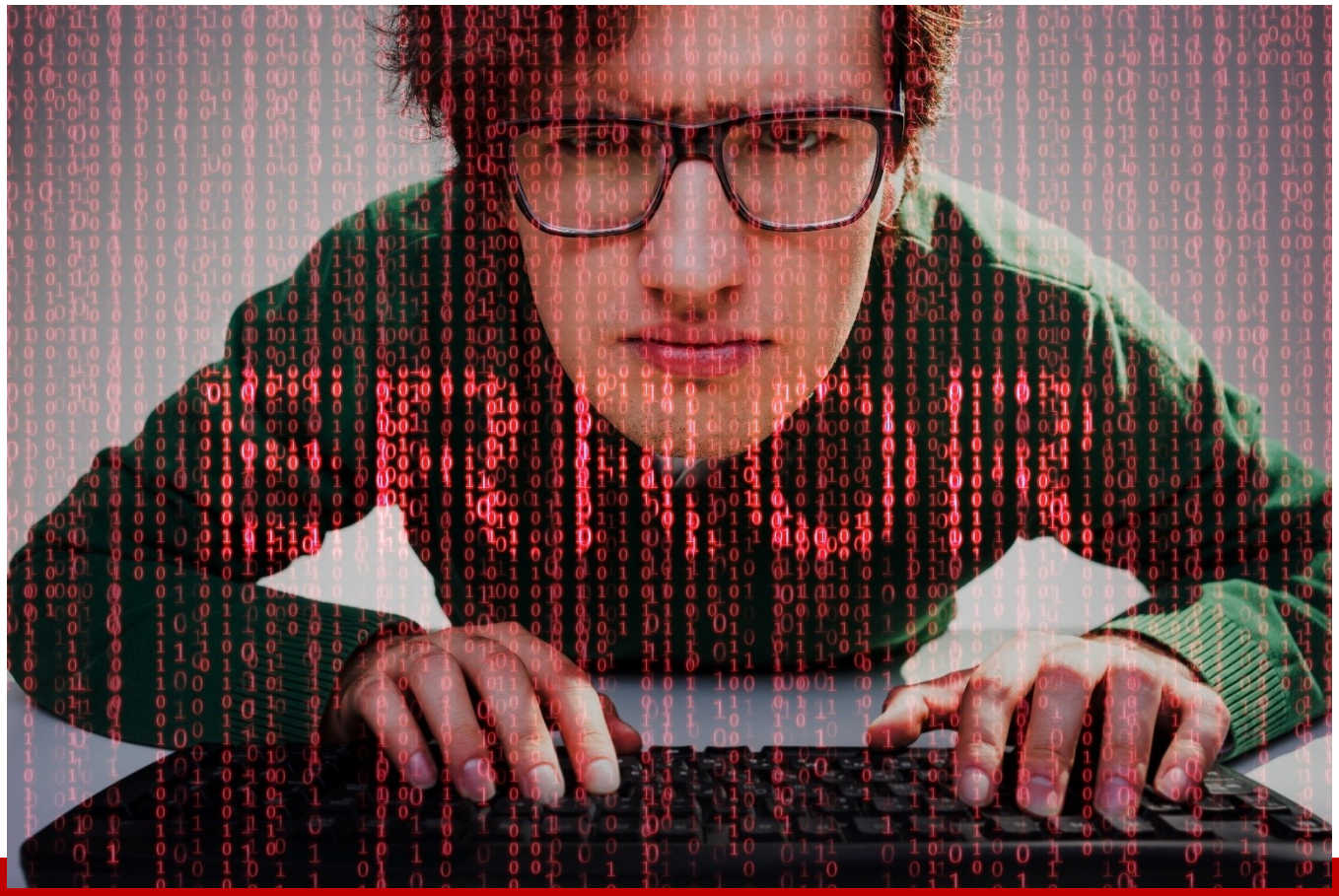
Renato Lima, Sr., Information Security and Resilience Manager at Eletrobras, has over 30 years of experience in IT Management, Cybersecurity, Operational Resilience, and Strategic Planning, with a diverse background spanning Financial Services, Manufacturing, Retail, Education, Healthcare, and Agribusiness. Throughout his career, he has held executive leadership positions in both national and global organizations, driving innovation, risk management, and digital transformation initiatives.

Currently, he serves in an executive leadership role in the energy sector, where he focuses on enhancing cybersecurity frameworks, strengthening operational resilience, and leading strategic technology initiatives to protect critical infrastructure.

In addition to his corporate career, he has built a longstanding academic trajectory, serving as a professor and lecturer in undergraduate and MBA programs at renowned educational institutions in Brazil, contributing to the development of future IT and cybersecurity leaders.

Renato Lima can be reached at renatoslima.sp@gmail.com and at our company website www.eletrobras.com

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Overcoming The Skills Shortage in Cybersecurity Through A 'Trusted' Approach.

By Thorsten Stremlau of the Trusted Computing Group

The scale of cyberattacks seen today is both unprecedented and harrowing. Crucial sectors including healthcare, finance, and education have found themselves increasingly under attack, with hackers leaving behind a trail of breached systems, stolen data, and disrupted operations.

Focusing on just the healthcare sector specifically, the statistics speak for themselves: last year businesses and institutions experienced 809 data breaches, a 136% increase from the prior year with over 56 million individuals affected. In terms of attacks, the financial sector was not far behind, with 744 breaches impacting 61 million people. These numbers serve as a serious reminder that no organisation is immune, especially those found in critical sectors.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Addressing the workforce gap

The global cybersecurity workforce gap has only served to exacerbate this problem. There's no point investing in cost-intensive security measures if a business does not have the right staff and knowledge to implement them correctly. Within the United Kingdom, for example, around 44% of all businesses have skills gaps in basic technical areas, following a similar trend seen across the globe.

When it comes to establishing a robust cybersecurity workforce, businesses find themselves in a challenging position: they are operating in a decreasing pool of experts, and those available can demand a hefty price. According to the World Economic Forum, this shortage of cybersecurity professionals has arisen due to the following issues: a lack of distinct career paths, outdated training, costly certifications and a high level of job stress.

Thankfully, actions are being taken to remedy this issue. Returning to the United Kingdom, there has been significant improvements in terms of training new talent, with the number of cybersecurity graduates having increased by 34%. This has played a part in the 32% decrease in the number of cyber job postings across the country between 2020-2023, though it's important to note a number of economic factors such as job cuts have also affected this figure.

The comprehensive training programs and competitive compensation offered by businesses are helping to fill critical roles and foster loyalty and retention. Upskilling existing employees not only empowers them with cybersecurity expertise tailored to a company's specific needs, but offers new career pathways employees may have never considered previously.

An internal talent pipeline is often more effective and economical than seeking external hires - employees trained in-house are familiar with the company's systems, workflows, and culture, making them better equipped to identify and address vulnerabilities. Combining a skilled workforce with preventative measures such as regular audits, testing, and continuous software updates creates a multi-layered defence capable of thwarting even the most sophisticated attacks.

Setting the right standard for security

Training and education are vital, yet they are just one basic cog in the entire system. To protect operations while upskilling its workforce, businesses must consider adopting a 'trusted computing' approach. This includes the adoption of the latest standards, specifications and technologies available from organisations like the Trusted Computing Group (TCG). Free-to-use and designed for all modern systems, networks, and devices, these standards are already helping to enhance security measures across all sectors.

A prime example is the Trusted Platform Module (TPM), a low-cost, secure Root-of-Trust (RoT) which delivers secure operations through the protection of a user's identity and sensitive data. With a TPM, elements of a device's firmware and software are hashed before they are executed, and validated t server-level when the system attempts to connect to a network. Should the details not match, the devices will simply not boot up. The signing and verifying done by the TPM ensures the key security building blocks of verification, data protection, identify and attestation are built-in to a company's systems.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Additionally, a Device Identifier Composition Engine (DICE) can also be used in cases where the TPM may be too large or otherwise unsuitable for a device application or its architecture. A more lightweight solution, DICE implements the same key security protocols as the TPM, and provides the ability to create cryptographically secure identities and verify software found in newer devices. Within DICE architecture lies a foundational secret known as the 'Unique Device Secret (UDS)', protected by a layered security approach. Each layer independently creates its own unique secret, derived from the UDS; if one layer is compromised during an attack, the secret the hacker uncovers can't be used to compromise the others, mitigating the potential damage. Device integrity is also preserved by DICE and its ability to re-key should malicious code ever be detected.

There is also the Cyber Resilient Module and Building Block Requirements (CyRes) specification, created to reduce malware persistence and protect critical code and data stored in devices and systems. In the event an attack compromises these, CyRes provides the means to recover a system back to a reliable state prior to any compromise, helping operations to restart quickly and reduce the negative effects of the attack.

Creating a security-led culture

These standards and specifications work hand-in-hand with the intensive training initiatives being launched by governments and educational bodies across the globe. In fact, organisations like the TCG have become increasingly aware of the benefits of these efforts, and have begun to rollout their own training initiatives to better prepare the next generation of cybersecurity experts.

The courses offered by businesses typically target their employees, teaching them good practices for recognising phishing attempts, ensuring good password hygiene, and reporting suspicious activities to relevant bodies. This high-level approach is a good start, and may interest people in taking more technical classes developed by standards organisations.

Training programs such as the courses created by TCG and OpenSystemsTraining 2 are pivotal in letting software developers and interested parties hone their cybersecurity skills and get unprecedented access to the latest standards and specifications like the TPM. Often lab-driven and requiring no experience working with standards, these courses can help users discover innovative security applications and learn how to leverage key technologies to bolster software and hardware security. The result? Users learn a vast new set of skills that would previously have taken several months or years of training, while the time associated with adopting standards is also reduced. This goes a long way in both reducing the cybersecurity skills gap, while making security measures more accessible to businesses.

Cybersecurity cannot be a one-time investment or a compliance checkbox; it must become an ingrained part of organisational culture. By embedding trusted computing in every process and decision, businesses can move from being reactive to initiative-taking. From adopting trusted technologies to investing in a skilled workforce, resilience now requires a multifaceted approach, especially if businesses are to overcome the shortage of security professionals. The message is clear, and the stakes are too high to ignore: Cybersecurity is not just about reacting to threats; it is about anticipating them and staying

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

ahead in an increasingly dangerous digital world. The steps we are seeing being taken are a good start, but more can always be done.

About the Author



Thorsten Stremlau, CISSP, is Systems Principal Architect NVIDIA. He is a Distinguished Engineer and Systems Principal Architect in NVIDIA. He is responsible for technical strategies for components, devices, software and cloud services. In this role, Thorsten identifies and drives integration of current and future technologies, integrating them into the product development processes, and specifically drives innovation into the security capabilities of NVIDIA's portfolio.

Thorsten's career has been dedicated to identifying solutions and strategic implementations for customers in all aspects of IT. As an engineer for nearly 25 years, his broad experience enabled him to assist thousands of our customers to digitally transform their environments using advanced technology.

Thorsten holds a Bachelor in Industrial Manufacturing/Finance. Thorsten lives in North Carolina with his family.

Thorsten can be reached online at tcg@proactive-pr.com or tstremlau@nvidia.com and at our company website https://trustedcomputinggroup.org/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Can AI Be Your Trusted Partner in Securing Your Extended Business Ecosystem?

By Phani Dasari, Chief Information Security Officer at HGS

In today's interconnected business world, organizations rely on a vast web of third-party vendors, suppliers, and partners. While these relationships are essential for growth and innovation, they also introduce significant security and compliance risks. A staggering 74% of organizations have experienced a third-party security incident in the past year, and the average cost of a data breach caused by a third party is a whopping $4.24 million. These statistics make it abundantly clear: traditional third-party risk management (TPRM) approaches are struggling to keep pace with the ever-evolving threat landscape.

Enter Artificial Intelligence (AI), poised to revolutionize TPRM. The global third-party risk management market is expected to reach a staggering $11.34 billion by 2028, with AI playing a central role in this growth. By leveraging AI's analytical prowess and automation capabilities, organizations can significantly strengthen their TPRM posture.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The Growing Complexity of TPRM

Beyond the sheer volume of third-party relationships (the average organization has over 500), several factors are making TPRM increasingly complex:

- **The Shadow Supply Chain:** Many organizations struggle to map their entire network of third-party relationships, creating a blind spot known as the "shadow supply chain." This lack of visibility makes it difficult to quantify and mitigate associated risks. Imagine a marketing agency unknowingly using a sub processor for data storage located in a jurisdiction with weak data privacy laws. A seemingly innocuous service like social media management could expose sensitive customer data through a hidden connection in the supply chain.
- **Converging Risks:** The lines between physical and cyber threats are blurring. A cyberattack on a power grid can cause widespread blackouts, while a compromised transportation system can disrupt entire supply chains. These interconnected risks necessitate a holistic approach to TPRM. Consider a scenario where a hacked freight management system redirects shipments containing hazardous materials, causing environmental damage and safety hazards.
- **ESG Factors:** Environmental, Social, and Governance (ESG) factors are gaining prominence. Organizations must now consider sustainability practices, labor rights, and ethical sourcing within their TPRM framework. Consumers are increasingly demanding supply chain transparency. A fashion retailer could face reputational damage if discovered to be using sweatshop labor through a third-party manufacturer.
- **The Rise of AI:** While AI offers immense benefits, its integration into the vendor ecosystem introduces new risk dimensions. Issues like algorithmic bias, explainability of AI decisions, and potential for intellectual property (IP) loss need to be addressed. An AI powered recruitment tool used by a staffing agency might exhibit bias against certain demographics, leading to discrimination lawsuits. Additionally, a compromised AI model developed by a third-party vendor could expose sensitive data or disrupt critical business processes.

Balancing Security and Business Agility

Effective TPRM requires a multipronged approach that balances security with business agility. Here are some key considerations:

- **People:** Security teams need to adopt a more collaborative approach. Educating stakeholders in business-friendly language and building strong relationships with internal partners (finance, legal, procurement) are crucial. Security briefings shouldn't focus solely on technical jargon; instead, they should translate risks into business impacts, highlighting potential financial losses, reputational damage, and operational disruptions. Security champions within business units can also play a vital role in fostering a culture of security awareness.
- **Process:** A comprehensive TPRM process requires identifying all stakeholders across departments (finance, legal, procurement, IT, etc.), creating a standardized workflow that streamlines onboarding and ongoing monitoring, and ensuring vendor friendliness. The process should be efficient and not overly burdensome for vendors to avoid hindering business

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

relationships. Collaboration tools and automation can streamline communication and information sharing throughout the TPRM lifecycle.

- **Technology:** AI provides powerful tools to automate tasks, identify and assess risks effectively, and make data driven decisions. Organizations should invest in AI powered TPRM solutions that integrate seamlessly with existing workflows.

AI offers a suite of tools to transform TPRM:

- **AI powered Due Diligence:** AI can quickly assess a vendor's security posture, financial health, and ESG practices, streamlining the onboarding process and identifying potential red flags early on. By analyzing public records, industry reports, and social media data, AI can uncover hidden risks that might be missed in traditional due diligence processes.
- **Risk Assessment Tools:** AI can analyze vast amounts of data from various sources (contracts, financial statements, industry reports, news articles, threat intelligence feeds) to identify and prioritize potential risks posed by third parties. AI can also uncover hidden connections within the supply chain, providing a more holistic view of potential vulnerabilities.

AI in Action:

AI is transforming how organizations manage risk across their vendor ecosystems. Here are some real-world examples showcasing the power of AI in action:

- **Financial Institutions:** Predictive models leverage historical breach data to identify vendors most susceptible to data breaches. By analyzing vulnerabilities exploited and stolen data types, these models enable proactive risk mitigation measures, such as additional security audits or enhanced data encryption requirements.
- **Manufacturing Companies:** AI goes beyond basic risk assessments. Tailored risk mitigation plans can be crafted for each vendor based on factors like industry, size, location, and data access levels. This allows for a more nuanced approach to managing risk across a diverse vendor landscape. Enabling new opportunities for technology specific to manufacturing environments never accessible before like IT/OT in a comprehensive way measuring risk across the total landscape of the business.
- **Healthcare Providers:** Ransomware attacks are a major concern for healthcare organizations. AI powered predictive models can analyze historical attack data, including exploited vulnerabilities and data types encrypted, to identify high-risk vendors. This allows for targeted mitigation measures, such as increased cybersecurity awareness training for vendors with high access to sensitive patient data.
- **Financial Services Companies:** Continuous monitoring is crucial for identifying potential issues early on. AI powered systems can monitor a vendor's financial health, security posture, and regulatory compliance in real-time. Additionally, these systems can scan news and social media activity for red flags that might indicate potential security incidents. Battling complex regulatory

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

and financial crimes scenarios that can be spread across complex operating environments from call centers to online customer portals.

The Benefits of AI powered TPRM:

By leveraging AI, organizations can reap significant benefits for their TPRM programs:

- **Improved Efficiency and Effectiveness:** Automating tasks and leveraging data analytics streamlines the TPRM process and leads to more informed decisions.
- **Reduced Costs:** AI saves time and resources by automating manual tasks and optimizing risk mitigation strategies.
- **Increased Visibility and Control:** AI provides a holistic view of third-party relationships, enabling better risk identification and mitigation.
- **Enhanced Compliance:** AI powered compliance tools help organizations to do continuous and automated compliance saving significant time and resources.
- **Monitor suspicious activity:** AI can continuously monitor partner data access patterns, network traffic, and threat intelligence feeds to identify potential incidents early on, allowing for a swift response.

Four Key Takeaways for a Strong TPRM Program

1. **Embrace Business Agility:** Ensure that your TPRM strategy supports fast-paced business operations while maintaining security.
2. **Connect Stakeholders:** Build workflows that connect all internal stakeholders and foster collaboration to decouple dependencies.
3. **Leverage AI:** Implement AI-driven solutions to automate and streamline risk management processes.
4. **Train and Empower Teams:** Equip teams with the flexibility and skills needed to adapt to changing risk landscapes.

AI is not only a tool but a strategic partner in navigating the complexities of modern third-party risk management. By embracing AI-driven solutions, organizations can protect their extended business ecosystem and future-proof their operations against evolving threats.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Phani Dasari is the Chief Information Security Officer of HGS, a leader in providing digital-led CX and IT services for hundreds of world class brands. As the CISO at HGS, Phani plays a pivotal role in safeguarding the organization's global information assets. His leadership encompasses a wide range of security operations focused on strengthening data security, ensuring compliance with regulatory requirements, fostering a security-conscious culture, and developing and executing incident response and recovery strategies to minimize disruptions to the business.

To learn more about HGS, please visit hgs.cx

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



The Role of AI In Cybersecurity: Enhancing Defense And Adapting To Threats

Rising Above the Cybersecurity Storm

By Randy Hall, CEO, Securafy Inc

The cybersecurity landscape today feels like a constant game of cat and mouse. Every time we think we've outpaced the attackers; they find new ways to exploit vulnerabilities. Enter artificial intelligence (AI) — a game-changer in this dynamic field. AI isn't just about automating processes; it's about making defenses smarter, faster, and more adaptive to ever-evolving threats.

In this article, I'll Walk you through how AI is reshaping cybersecurity, the opportunities it unlocks, and the challenges we need to keep in mind. Let's dive in.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

What is AI in Cybersecurity?

At its core, AI in cybersecurity refers to the use of advanced technologies like machine learning, neural networks, and natural language processing to identify, analyze, and mitigate security threats. Unlike traditional systems, AI-driven tools are designed to learn and adapt over time, making them more effective at detecting patterns that might elude the human eye.

For instance, machine learning can sift through mountains of data to spot anomalies, while neural networks can analyze complex behaviors to predict and block attacks before they occur. Think of AI as your digital bodyguard, constantly on high alert.

Why AI is Essential for Cybersecurity

The sheer scale of modern cyber threats makes AI a necessity, not a luxury. Here's why:

- Volume of Data: Businesses generate more data than ever before, making it impossible for human teams to analyze everything effectively.
- Sophistication of Attacks: Cybercriminals now use advanced tools, including AI, to launch complex attacks.
- Speed of Response: Traditional systems often react to threats after damage has been done. AI enables proactive detection and prevention.

Without AI, keeping up with the pace of today's cyber threats would be like trying to empty a sinking boat with a teaspoon.

Key Applications of AI in Cybersecurity

AI is making waves across multiple areas of cybersecurity. Here are some of its most impactful applications:

- Threat Detection and Monitoring: AI systems excel at real-time monitoring, analyzing network traffic, and identifying anomalies that signal potential threats. This means quicker responses to malware, phishing attempts, and ransomware.
- Incident Response Automation: When a breach occurs, every second counts. AI-driven playbooks can automate responses, isolating affected systems and mitigating damage while freeing up human teams to focus on strategy.
- Fraud Prevention: From detecting unauthorized transactions to flagging suspicious account activity, AI's ability to analyze behavioral patterns is invaluable in stopping fraud before it escalates.
- Securing IoT Devices: The Internet of Things (IoT) has opened up a new frontier for cyber threats. AI can protect these devices by monitoring and managing their vulnerabilities.
- Network Security: AI tools can analyze vast amounts of network traffic to identify and neutralize advanced persistent threats (APTs) and Distributed Denial of Service (DDoS) attacks.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Advantages of AI in Cybersecurity

When used effectively, AI can:

- Detect threats proactively: AI's predictive capabilities help identify risks before they're exploited.
- Reduce false positives: By understanding patterns better, AI reduces unnecessary alerts, allowing teams to focus on real issues.
- Scale defenses: Whether it's a small business or a global enterprise, AI systems can handle large volumes of data seamlessly.
- Save time: Automation speeds up processes that would take humans hours, if not days, to complete.

Challenges and Risks of AI in Cybersecurity

AI isn't a silver bullet. It comes with its own set of challenges:

- Cost and Complexity: Implementing AI tools can be expensive and resource-intensive.
- Adversarial AI: Just as defenders use AI, attackers do too. For example, hackers can create AI-driven phishing campaigns that are incredibly convincing.
- Bias and Accuracy: AI models are only as good as the data they're trained on. Poor data quality can lead to inaccurate decisions.
- Ethical Concerns: Balancing AI's power with privacy rights is a tightrope walk.

AI vs. Cybercriminals: The Arms Race

Here's the truth: Cybersecurity is an arms race, and both sides are leveraging AI. Attackers are using AI to create smarter malware, generate deepfake content, and automate phishing campaigns. Meanwhile, defenders are deploying AI to counter these very tactics. It's a constant back-and-forth, and the winner is often determined by who's innovating faster.

Emerging Trends in AI and Cybersecurity

Looking ahead, a few trends stand out:

- AI-Driven Security Operations Centers (SOCs): Expect more organizations to adopt AI-powered SOCs that combine human expertise with machine efficiency.
- Quantum Computing: As quantum computing becomes mainstream, AI will need to adapt to address the new security challenges it brings.
- Collaborative AI: The future lies in combining AI tools with human oversight, creating a partnership that maximizes strengths on both sides.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Practical Tips for Adopting AI in Cybersecurity

For organizations considering AI, here are some practical steps:

1. Start small with scalable tools.
2. Ensure proper training for teams to manage AI systems effectively.
3. Regularly update and audit AI models to maintain accuracy.
4. Balance automation with human oversight to avoid over-reliance.

AI is transforming cybersecurity, offering solutions that are faster, smarter, and more adaptive than ever before. But like any tool, its effectiveness depends on how it's used. As cyber threats continue to evolve, so must our defenses — blending AI's capabilities with human ingenuity to create a safer digital world.

The race is on, and there's no room to sit on the sidelines. Whether you're a tech-savvy business owner or just someone curious about the future, understanding AI's role in cybersecurity is key to staying ahead in this ever-changing game.

About the Author



Randy Hall, CEO of Securafy Inc., has over 40 years of IT experience, excelling in roles like network engineer and CIO. An accomplished entrepreneur, he founded Haltronics Inc., built and sold companies like Worldlan Technology, and scaled smaller firms. At Securafy, recognized as the 2024 Most Trusted MSP in North America by the Soteria Award, Randy drives innovation and excellence in cybersecurity, compliance, and managed services. A frequent speaker at IT events, he has worked with businesses worldwide, from SMBs to large enterprises and the U.S. government.

Randy Hall can be reached online on LinkedIn and at our company website www.securafy.com.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Securing The AI Frontier: Addressing Emerging Threats In AI-Powered Software Development

AI-generated code is accelerating development but often overlooks security best practices, making proactive oversight essential.

By Matt Tesauro, Chief Technology Officer, DefectDojo

AI in software development is no longer a glimpse into the future - it's here, woven into daily workflows and it's accelerating at a breakneck pace. According to PwC's AI Predictions report, AI has the potential to cut software development time in half, making it no surprise that companies are eager to integrate AI into their development workflows. In fact, a 2024 GitHub and Accenture study revealed that 40% of newly committed code across enterprise customers now contains AI-assisted content. And, more tellingly, 96% of developers start relying on AI-generated suggestions immediately after installing an IDE extension, indicating that AI is no longer just an experimental tool but a core component of the modern development workflow.

However, this rush toward adoption brings significant security concerns that organizations are only beginning to understand.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

AI's Role in Code Generation and Security Challenges

With over 50,000 organizations deploying millions of lines of AI-generated code daily, we're witnessing one of the largest shifts in software development since integrated development environments became standard. While AI models excel at speed and efficiency, this often comes at the expense of security. Each AI touchpoint creates new opportunities for bad actors, who have already found creative ways to exploit these systems - from manipulating AI to suggesting compromised code to poisoning the models themselves. Combined with emerging attack vectors like data poisoning and prompt injection, this rapid adoption and inadequate oversight creates a perfect storm for potential security breaches.

The Expanding Attack Surface

As AI's role in development expands beyond simple code completion, it's reshaping every phase of the software lifecycle. Today's AI tools don't just suggest code - they generate test cases, design APIs, write documentation, and even restructure entire codebases. While AI can automate and reduce development time up to 50%, it also multiplies the potential entry points for attackers. Each new AI-assisted task represents another surface that needs to be secured, transforming what was once a relatively straightforward security measure into a complex web of interconnected vulnerabilities.

Mitigating AI Security Risks

As AI becomes embedded in software development, organizations must take a proactive approach to security. Simply relying on traditional security measures leaves blind spots that attackers are eager to exploit.

Here are five best practices to consider:

1. **Establish Clear AI Security Policies:** Organizations must develop comprehensive policies governing AI and large language model (LLM) usage. These policies should outline permissible AI applications, prohibited actions (e.g., AI usage on sensitive data), and security requirements for AI-generated code.
2. **Apply Equal Security Standards to AI and Human-Generated Code:** AI-generated code should undergo the same security reviews and testing procedures as human-written code. Automated security scanning, static and dynamic analysis, and manual code reviews should be applied consistently, regardless of how the code was created.
3. **Monitor AI Integration Points:** AI-driven tools interface with various stages of the SDLC, from design to deployment. Security teams must monitor these integration points to ensure AI tools are not introducing vulnerabilities. This includes scanning AI-generated code for security flaws and evaluating AI's influence on software development decisions.
4. **Adopt AI Security Frameworks:** Frameworks such as the National Institute of Standards and Technology (NIST) AI Risk Management Framework provide structured approaches to mitigating AI security risks. Organizations should implement these frameworks incrementally, tailoring them to their specific environments and security requirements.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

5. **Enhance Developer Security Awareness:** Developers must be educated on the risks associated with AI-generated code and trained to critically evaluate AI suggestions. Encouraging security-first development practices can reduce the likelihood of introducing vulnerabilities through AI-assisted coding.

The Future of AI and Cybersecurity

As AI continues to shape the future of software development, security must remain a top priority. Rather than viewing AI as a shortcut, organizations should see it as a powerful tool that enhances - but never replaces - secure coding practices. The key to success lies in staying ahead of emerging threats and embedding security into every stage of AI-assisted development. Those who take a proactive approach - adapting security frameworks, addressing AI-specific vulnerabilities, and continuously refining their defenses - will be best positioned to leverage AI's benefits while keeping their systems and data secure.

About the Author



Matt Tesauro is a Founder and CTO at DefectDojo Inc. He is a DevSecOps and AppSec guru who specializes in creating security programs, leveraging automation to maximize team velocity and training emerging and senior security professionals. When not writing automation code in Go, Matt is pushing for DevSecOps everywhere via his involvement in open-source projects, presentations, trainings and new technology innovation.

Matt can be reached online at https://www.linkedin.com/in/matttesauro/ and at our company website https://defectdojo.com/.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Smart Meter Security: Best Practices and Emerging Regulations

By Jose Sanchez - Senior Director Product Management, IoT Connectivity & Services, Telit Cinterion

Smart meters are essential to smart grids, empowering utilities and smart grid managers to provide consumers and energy providers with real-time energy consumption data, transparent billing, and demand side management. Nevertheless, despite the many benefits of smart meters, they, including the larger smart grid, are critical infrastructure, making them ideal targets for hackers.

Cyberattacks are growing worldwide, with attacks against critical infrastructure being some of the most prevalent. Research from the International Energy Agency (IEA) shows that cyberattacks aimed at the energy sector, with critical infrastructure, including gas, water and especially power utilities, have been on the rise since 2018. For this reason, smart meter manufacturers and vendors must secure their products and comply with evolving regulations.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

How Do Hackers Exploit Smart Meters?

The attack vectors against smart meters are diverse and evolving, with digital systems and Internet of Things (IoT) sensors increasing the attack surface significantly. Typically, attackers will physically or remotely gain access to the smart meter through a remote or local interface. Vulnerabilities exist within the firmware, network interfaces, Application Programming Interfaces (APIs), utility applications or hardware architecture, all of which bad actors seek to exploit. Hackers can also use the communication between the meter and the Head-End System (HES) to gain access to a device. For instance, bad actors could exploit a network interface to remotely access metrology data stored in the smart meter; likewise, they could modify this data as it travels to the HES.

The consequences of these attacks are wide-ranging. Sometimes, an attack can compromise meter-related functions, corrupting metrology data. Attacks can also disrupt tariff management, prevent remote enablement or completely disable the smart meter. Other results of attacks include the theft of personal user data or physical damage to people and properties. In catastrophic cases, a hacker could bring down entire utility system components. One infamous example is the Colonial Oil Pipeline attack, where a hacker group targeted the largest pipeline in the US with a massive ransomware attack that forced the pipeline to shut down, leaving almost 11,000 gas stations without gas and increasing the average cost for fuel per gallon nationally.

Best Smart Meter Security Practices

As cyberattacks continue to increase in frequency, it is paramount that smart meter manufacturers and vendors implement a security strategy that accounts for technology, processes and people throughout the lifetime of a product or service. Although there is no way to prevent 100% of all threats, manufacturers can follow “security-by-design” principles and the CIA model – a system that safeguards the confidentiality and integrity of data while ensuring system availability – to reduce cybersecurity risks.

A security assessment or audit is the first step in achieving a secure end-to-end metering system. It is also important to continuously monitor and analyze supply chain processes for vulnerabilities. Likewise, manufacturers must have the right mindset and recognize that cybersecurity is an ongoing process, necessitating updating and refining. In other words, security doesn’t end after a smart meter gets deployed but continues throughout the device’s entire lifecycle.

SIM card security is another critical element of smart meter security. For starters, manufacturers must determine who manages the connectivity configuration of a smart meter device’s SIM card; put another way, who can activate or deactivate it? Concerning the lifecycle of a smart meter, manufacturers must understand that a device is not just the modem or the module but also the SIM card. To that end, manufacturers can use eSIM (or embedded SIM) to support remote SIM provisioning and keep their devices’ firmware and security up-to-date.

Lastly, smart meter manufacturers should consider artificial intelligence (AI) and its role. In truth, it is not easy to predict how AI will affect IoT and edge device security. The one thing for certain is that AI will be a powerful technology at the disposal of malicious actors, as well as utilities and smart meter vendors.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Attacks will become more sophisticated, but so will the countermeasures. For example, utilities can use AI to identify patterns indicative of a cybersecurity breach far faster than a trained human.

Complying with Evolving Regulations

In addition to securing their products, smart meter manufacturers are responsible for complying with the ever-evolving regulations. Recall that smart metering is critical infrastructure, meaning regulators are aware of the risks and are keen to ensure manufacturers abide by industry standards, most of which come from Europe. For example, the EU, as part of the EUCC scheme, adopted the Common Criteria standard ISO15408. Also, there is the IEC 62443, which in Europe is vital to comply with the NIS directive. Likewise, the Cyber Resilience Act rolled out in the EU last year.

Another regulatory that smart meter manufacturers should keep an eye on is the ESMIG, the European Association of Smart Energy Solution Providers. It represents the meter industry by helping overcome barriers to the green energy transition. Although these standards come from the EU, they are pertinent for smart meter manufacturers and vendors looking to do business on the world stage. Nevertheless, observing these various standards and evolving regulations while keeping product timelines can be challenging. As such, manufacturers should seek assistance from a trusted IoT partner.

An Ideal IoT Partner

Ideally, smart meter manufacturers will want a partner that isn't just an IoT module supplier but an end-to-end IoT system enabler that provides services, solutions and connectivity in addition to hardware. This partner should also follow secure by design principles, embedding components and services into smart meter systems that enhance security to promote a safer smart grid. Moreover, the ideal partner must be committed to life cycle support and security to ensure devices in the field remain protected against evolving threats and compliant with emerging regulations.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Jose Sanchez serves as the Senior Director Product Management for IoT Connectivity & Services at Telit Cinterion. In this role, he plays a key part in shaping the company's global initiatives for IoT services, focusing on aspects such as connectivity, device management, device-to-cloud security, and application enablement.

Before joining Telit Cinterion, Jose gained extensive experience in various product management and marketing positions at Thales, a prominent global leader in IoT and security. He worked there for over a decade, where he managed different product lines related to Cinterion IoT modules and oversaw eSIM services catering to the IoT market segment.

In addition to his corporate experience, Jose is an entrepreneur at heart. He co-founded the tech startup Ubikon at the young age of 25, shortly after completing his master's degree in telecommunications engineering at RWTH Aachen University in Germany and the University of Malaga in Spain.

Further enhancing his skills, Jose completed the executive program titled "Bringing Technology to Market" at the European School of Management and Technology (ESMT) in Berlin, Germany, in 2019.

Jose can be reached at https://www.linkedin.com/in/josesanchezsantana/?originalSubdomain=de

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



The Art of Delegation in a Digital Age: Empowering Teams, Not Just Offloading Tasks

By Josh Breaker-Rolfe, Content writer at Bora

Effective task delegation is a vital skill for any manager. Strategically transferring specific tasks to capable team members can boost efficiency, improve decision-making, and empower staff to create a healthy, collaborative work environment. Research into the topic even suggests that effective delegators see 33% higher revenue and significantly lower employee turnover when compared to their less able counterparts.

However, delegation in the digital world means more than just sharing responsibility for office tasks. It's about managing identities and access across internal departments and external partners, which can be a major headache without delegating tasks.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The Problem: Managing Identities

Most modern organizations work with multiple partners, each with its own systems, security protocols, and security requirements. Similarly, many businesses have multiple departments using different systems with their own unique requirements. Managing user identities across multiple systems presents significant challenges, especially for already stretched IT teams. Manual processes often lead to delays in granting or revoking access, which not only hinders operational efficiency but also introduces security gaps that could be exploited by unauthorized users.

The problem is threefold:

- **These ecosystems are inherently diverse**. Each business partner has its own identity and access management (IAM) system with unique configurations, and the same often goes for internal departments. Integrating these systems into a cohesive whole is time-consuming and risky.
- **As partnerships evolve, users are added and removed from systems**. The same is true for onboarding and offboarding staff. Manually handling this process is prone to errors, which can lead to security vulnerabilities and possibly even unauthorized access.
- **Balancing security needs with the need for seamless collaboration is a serious challenge**. The more layers of security an organization adds, the harder it is for partners and departments to work together.

The crux of the issue is that, while traditional identity and access management (IAM) tools were well equipped for yesteryear's controlled, on-premises environments, they fall well short of the demands of today's dynamic and interconnected world. Traditional centralized solutions often restrict flexibility and can inadvertently create collaboration bottlenecks. Decentralized approaches like Delegated User Management (DUM) provide a more agile solution that balances governance with operational efficiency.

The Solution: Delegated User Management

Delegated User Management (DUM) is the solution to this problem. It offers organizations a streamlined solution for managing partner identities, enabling businesses to provide access control and user administration to trusted partners while maintaining security and compliance. In short, DUM grants trusted partners — be they internal or external — the ability to manage user identities without giving them total administrative control.

Rather than centralizing all user management tasks within a single entity, DUM decentralizes these responsibilities, enabling trusted partners or departments to manage their own users. At its heart, DUM brings control closer to where it's needed. This decentralization boosts efficiency and security by ensuring that the right people can manage access at the right time.

Unlike centralized IAM systems that rely on one control point, DUM spreads authority out, cutting bottlenecks and fuelling faster, more responsive identity management.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Delegated User Management: Security, Efficiency, Empowerment

It's important to view DUM tools as not only a way to offload laborious tasks but also an opportunity to empower business partners and internal departments. It grants teams the autonomy, responsibility, and tools to manage access and user-specific tasks in their domain, building accountability and strengthening security awareness among diverse teams.

Strengthening security awareness in partner organizations is particularly important. Supply chain attacks have become increasingly frequent in recent years, with research from Cybersecurity Ventures even predicting that the global annual cost of software supply chain attacks to businesses will reach a staggering $138 billion by 2031, up from $60 billion in 2025.

Putting DUM into action realizes a whole range of real, tangible benefits, including improved efficiency, enhanced security, and reduced administrative overhead. For example, decentralizing user management helps companies cut administrative overheads. Delegated managers can quickly respond to access requests, streamlining the process and preventing delays in collaboration.

Similarly, with DUM, in the event of a breach, it will remain localized, which is particularly critical given the number of supply-chain violations that have littered the headlines over the past few years. Also, because access management is brought closer to the user, potential vulnerabilities are minimized, and breaches are contained more effectively.

DUM also improves visibility and audit trails, making it easier to meet regulatory requirements. Every action taken by a delegated administrator is logged and traceable, helping compliance audits to be seamless and transparent.

These solutions also offer scalability benefits. As businesses grow and partnerships multiply, DUM scales right along with them. The system easily adapts to new users and collaborations without significant adjustments, keeping organizations safe and running smoothly.

One of DUM's biggest perks is that it lets non-technical users handle access on their own, with no IT help needed. This means faster decisions and more agile identity management, so partners always have the right access when they need it.

How Delegated User Management Works

The Delegated User Management capability is built to bring this decentralized approach to life while maintaining the highest standards of security and control. Here's how it works:

- Delegated Managers: Delegated managers are assigned during the partner organization onboarding process to manage their own users efficiently. They work within the organization's boundaries, making user enrollment and access management easy with a simple point-and-click approach. This ensures that they can only control what they are supposed to, maintaining security and preventing unauthorized changes.
- Predefined Boundaries and Access Controls: DUM ensures security through clearly defined boundaries. Delegated managers are given access controls that limit their scope of influence so

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

they can manage users within their own entity or department without overreaching into other areas.

- User-Friendly Dashboards: Easy-to-use dashboards make user management tasks simple. Thanks to the clarity of the interface, even non-technical users can manage access effectively. From onboarding to offboarding, no task requires deep IT expertise.
- Seamless Integration: The DUM framework integrates smoothly with existing IAM structures, making it a modular solution that can be adopted without disrupting current systems.

Improve IAM with DUM

The key takeaway here is that delegation is crucial for IAM in the modern era. Modern organizations manage too many identities, partners, and departments to manage identities from a single identity. Don't think of DUM as a way to offload tasks; think of it as a way to empower partners, build trust, and strengthen business relationships internally and externally.

About the Author



Josh Breaker-Rolfe is a Content writer at. He graduated with a degree in Journalism in 2021 and has a background in cybersecurity PR. He's written on a wide range of topics, from AI to Zero Trust, and is particularly interested in the impacts of cybersecurity on the wider economy. Bora. He graduated with a degree in Journalism in 2021 and has a background in cybersecurity PR. He's written on a wide range of topics, from AI to Zero Trust, and is particularly interested in the impacts of cybersecurity on the wider economy.

Josh can be reached online at Josh@welcometobora.com and at our company website https://welcometobora.com/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



The Growing Cost of Non-Compliance and the Need for Security-First Solutions

By Puneet Kohli, President of Application Modernization at Rocket Software

Organizations across the world are facing mounting pressures to comply with a complex web of regulations. Failure to meet these requirements doesn't just result in inconvenience or minor setbacks – it can translate into significant financial and reputational damage. According to a recent study, the average cost for organizations that fail to comply with data protection regulations is $14.82 million, a staggering 45 percent increase from 2011. This number reveals a sharp increase in both the scale and complexity of regulatory violations, and the harsh reality that non-compliance is a costly risk many companies cannot afford to take.

In comparison, the average cost of compliance is $5.47 million – still substantial, but far less than the financial burden incurred from failing to adhere to legal and regulatory standards. This stark contrast highlights an uncomfortable truth: failing to meet compliance standards is a risk that businesses must take seriously. Organizations today are dealing with the immediate fines, penalties, and the long-term consequences of operational disruption, loss of trust, and diminished revenue.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The impact of non-compliance goes far beyond immediate financial penalties. With global cybercrime costs projected to reach $10.5 trillion this year, every compliance failure adds to this growing threat. A single breach can disrupt operations, invite regulatory scrutiny, and reduce productivity – but the most damaging consequence is often the lasting reputational harm that drives customers and business partners away. From legal settlements to remediation efforts, non-compliance touches nearly every part of an organization. Taking a proactive approach to security and compliance isn't only about avoiding fines, it's essential for protecting long-term stability and success.

Why Is Non-Compliance So Expensive

Non-compliance can cause significant disruptions to an organization's operations, often making it difficult to focus on their standard business practices. Data breaches, security failures, and other regulatory violations can trigger lengthy investigations, system overhauls, and costly public relations campaigns aimed at restoring consumer confidence. These disruptions can also lead to the diversion of key resources that would otherwise be dedicated to driving innovation and growth.

Legal settlements and penalties can quickly become a significant burden as well. Regulatory bodies across the globe are increasing their scrutiny and enforcement actions. Failing to comply with well-established regulations like HIPAA or GDPR, or newer ones like the European Union's Digital Operational Resilience Act (DORA) and NY DFS Cybersecurity requirements, can result in penalties that can reach millions of dollars. But the costs do not stop there. Once a company has been found to be non-compliant, it often faces reputational damage that extends far beyond the immediate legal repercussions. Customers, clients, and business partners may question the integrity of an organization that has demonstrated an inability to safeguard sensitive data, leading to the potential loss of valuable contracts, partnerships, and consumer trust.

The long-term effects on an organization's reputation can have far-reaching consequences. Rebuilding trust with customers, stakeholders, and partners can take years, and in some cases, may not be fully achievable. When an organization loses its reputation for being secure and trustworthy, it not only loses customers but also faces a diminished ability to attract new business or talent. For organizations operating in high-stakes industries such as finance, healthcare, or government contracting, this loss of trust can be particularly devastating.

The Importance of Security-First Solutions

With the costs of non-compliance continuing to rise, the need for organizations to adopt security-first solutions within their IT security has never been greater. A security-first approach goes beyond just checking off boxes to meet regulatory requirements. It involves implementing robust, proactive security measures that safeguard sensitive data and systems from potential breaches. This approach protects the organization from fines and builds a strong foundation of trust and resilience in the face of evolving cyber threats.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

One area where organizations often overlook security is in their access management systems, especially when it comes to mainframe applications. Many businesses still rely on outdated, insecure methods of connecting to critical systems through terminal emulators or "green screen" interfaces. These systems, often running legacy applications, can become prime targets for cybercriminals if they are not properly secured. With credential-based attacks rising, organizations must rethink how they secure access to their most vital resources.

Security-first solutions in this area focus on integrating modern identity and access management (IAM) protocols with legacy systems to enhance security without compromising accessibility. By strengthening the authentication and authorization processes for green screen access, businesses can significantly reduce the risk of unauthorized access and breaches. These solutions offer phishing-resistant, password-less access options, eliminating common vulnerabilities associated with traditional login methods. As cyberattacks become more sophisticated and prevalent (or frequent), organizations need to ensure that their access management systems are not just secure but also adaptive to emerging threats.

The implementation of such security-first solutions also ensures that organizations remain compliant with evolving regulations, such as HIPAA, DORA, and PCI-DSS 4.0. Regulatory frameworks like these require businesses to meet strict standards for protecting sensitive data and securing systems against unauthorized access. With frameworks evolving, organizations must stay ahead of the curve by adopting security measures that meet current requirements and anticipate future challenges.

Regulatory Pressures and the Need for Compliance

The regulatory environment continues to evolve in response to rising cybersecurity threats and the increasing complexity of global business operations. One of the most significant regulatory initiatives is DORA, which requires financial institutions in the EU to enhance their operational resilience. This regulation, which went into effect in January, mandates that financial institutions implement stronger security measures and robust incident response protocols to ensure their systems can withstand and recover from cyber incidents. For U.S. companies with customers in the EU, compliance with DORA is essential, making the integration of security-first solutions even more critical.

At the same time, organizations handling payment card data are under increasing pressure to meet the new PCI DSS 4.0 standards, which will be in full effect by the end of March. These updated requirements are designed to bolster payment system security and ensure the privacy of payment data. Companies that fail to comply with these standards face penalties and could lose the ability to process payment card transactions, which could have devastating effects on their business.

As cybersecurity risks grow, staying compliant with evolving regulations like DORA and PCI 4.0 is essential for avoiding fines and for maintaining trust and operational stability in this complex business environment.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Conclusion

The cost of non-compliance is rising, and businesses can no longer afford to take a passive approach to security and regulatory adherence. The financial, operational, and reputational risks associated with non-compliance are simply too high. Cyber threats are evolving, and regulatory frameworks are becoming more stringent, so organizations must adopt a proactive, security-first approach that integrates modern security practices into all aspects of their operations.

With secure access to critical systems and data and implementing strong encryption standards, aligning with the latest regulatory requirements, organizations can mitigate the risks associated with non-compliance. Moreover, they can build the trust necessary to thrive in the face of rising threats and mounting regulatory demands. Businesses that prioritize security will be better positioned to navigate the complex nature of compliance and safeguard their future success.

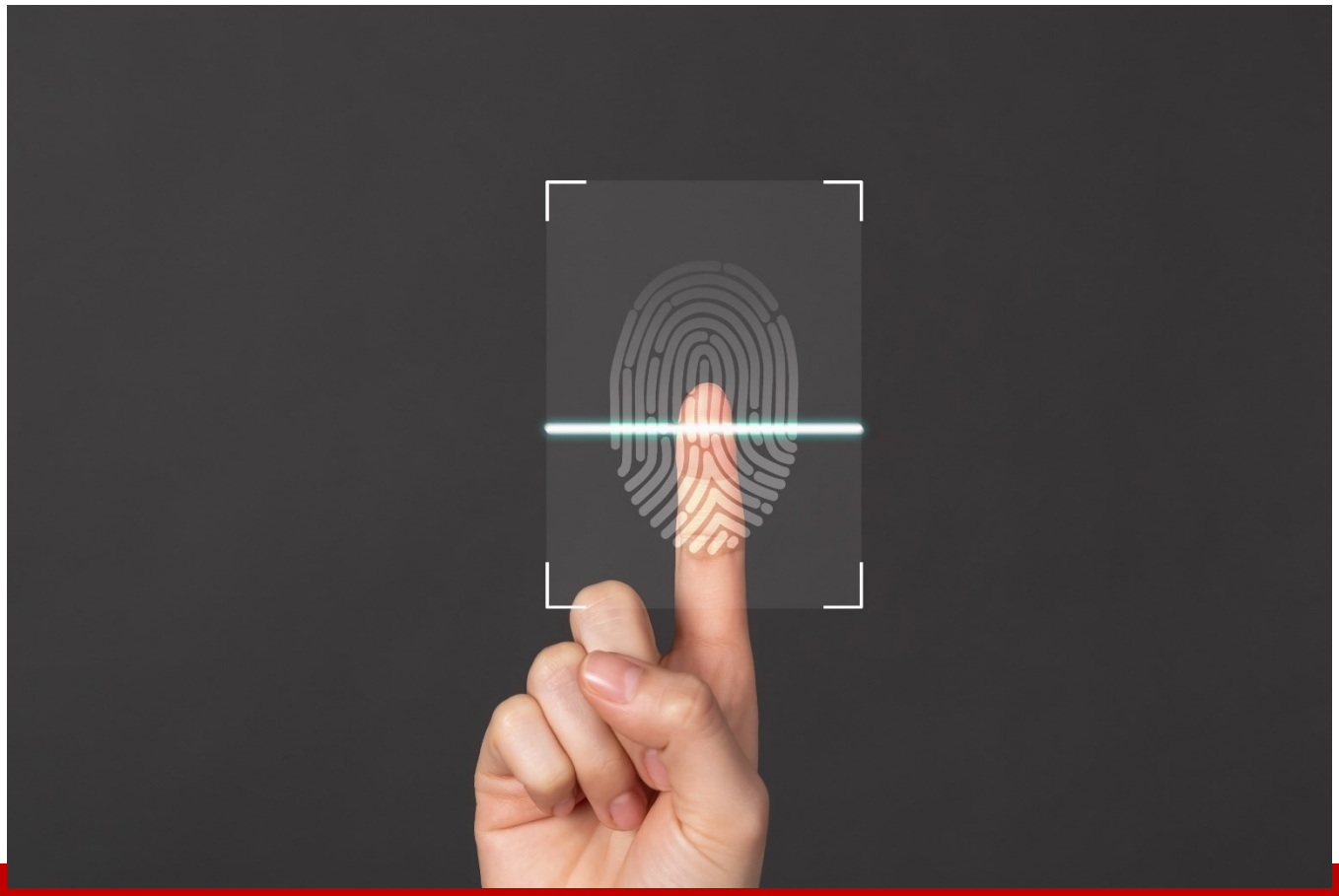
About the Author



Puneet joined Rocket Software in 2018 as the Vice President of Quality and DevOps and was promoted to the President of the Application Modernization Business Unit in 2023. In his time at Rocket Software, Puneet has held multiple leadership roles leading the Quality and DevOps and Product engineering teams and has been instrumental in standardizing Rocket Software's Quality and DevOps toolchain. Along with having touched nearly every Rocket Software product at some point during his tenure at Rocket Software, he also helps drive initiatives like Rocket.Build, Community Connectors and acquisition integrations. Before joining Rocket Software, Puneet held leadership roles at Dell EMC, RSA, and CA and spent over 10 years in the identity and access management space. Puneet serves as a president on the board of a nonprofit focusing on community and culture. Puneet's love for community service keeps him busy outside of Rocket Software. Puneet holds a B.S. in Computer Science from Northeastern University.

Puneet can be reached at https://www.linkedin.com/in/puneetkohli/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



The Invisible Fingerprint in Code

How AI Exposes Cybercriminals

By Felix Mächtle, Researcher at the University of Lübeck, Germany

Digital Traces in Code

Every program contains characteristic patterns of its developers, starting with the choice of variable names and preferred programming paradigms. Some developers rely on iterative solutions using loops, while others prefer recursive approaches. These individualized coding structures reflect the author's personal style. Until now, however, such features could only be analyzed in the source code, or if the potential author was already known during the training phase of the AI. This limitation posed a challenge for malicious software, which is typically only available as compiled machine code.

In collaboration with the Agentur für Innovation in der Cybersicherheit GmbH (Innovation for Cybersecurity), our team at the University of Lübeck in Germany has developed a new approach called OCEAN (Open-World Contrastive Authorship Identification) (https://arxiv.org/pdf/2412.05049) as part of

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

the SOVEREIGN research project (https://sovereign-project.de/), which recognizes the author's coding style even in highly optimized machine code.

Operating in an 'open world' scenario, OCEAN makes informed judgments even if the suspected author was not included in the training data.

However, the approach has only been tested on regular, unobfuscated code. Given that some malicious software uses targeted obfuscation techniques to hide its origins, we plan to investigate countermeasures in future research.

Securing the Software Supply Chain

Within the SOVEREIGN project, which is dedicated to the protection of critical infrastructures, OCEAN plays a central role in securing the software supply chain. Attacks that manipulate updates to introduce backdoors are an increasingly serious threat. Such manipulations often go unnoticed because the injected code integrates seamlessly with existing software. This is where OCEAN's technology comes in: by comparing the coding style of an update with the software's previous state, it can detect stylistically inconsistent code segments that may signal malicious interference.

In a case study, we simulated a supply-chain attack by integrating known malware into a software update. We were able to measure a significant deviation in authorship. While this does not automatically mean that a supply chain has been compromised, it should act as a wake-up call, prompting either further automated analysis of the code block or a call to affected companies to investigate possible changes in their development teams.

The Technology Behind OCEAN

At its core, OCEAN relies on contrastive learning, a machine learning technique that compares programs in pairs to determine if they were created by the same author. This method is similar to the one used in smartphone facial recognition systems, where contrastive learning helps to verify if two images belong to the same person.

The system's backbone is a neural network specially optimized for processing program codes. A significant advantage is that OCEAN does not depend solely on the original source code, but also works reliably with machine code. Tests conducted on real open-source programs demonstrated that the system can achieve an accuracy rate of 86%, even when facing high levels of compiler optimization. Compiler optimization automatically alters the machine code to enhance execution speed, potentially modifying distinctive stylistic traits of the original code and thereby complicating the identification of the author's unique style.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Outlook

OCEAN expands the horizon for digital forensics by highlighting programming style as a unique marker for cyber defense. Traditional methods have often been limited to source code analysis, but this new approach demonstrates that binary files can also contain valuable information about their developer, even in a realistic 'open world' scenario.

The ability to identify the creator of malware based on coding style opens entirely new avenues in IT security. Cybercriminals inevitably leave behind individual stylistic traces when developing malicious software. With OCEAN, it becomes possible to link seemingly independent attacks and pinpoint potential culprits. For investigative authorities, this method could soon serve as a crucial forensic tool in court proceedings.

Beyond tracing cyber attacks, this technology opens up new possibilities for answering fundamental questions about code provenance and attribution. In the future, OCEAN might even help distinguish automatically generated code from human-written code, an aspect that is particularly relevant when considering accountability in AI-assisted programming.

At the same time, this technological advancement raises critical concerns. The capability to link individual programming styles could potentially be misused by corporations or government agencies to surveil developers. Thus, protecting privacy and ensuring digital anonymity remain as important as enhancing IT security.

The subtle nuances in coding styles have already proven to be reliably detectable, bringing both new opportunities and challenges. The future of digital forensics will depend not only on technological progress but also on a responsible approach to harnessing these new capabilities.

About the Author

Felix Mächtle is a researcher at the University of Lübeck specializing in IT security and machine learning. He is pursuing his PhD at the Institute for IT Security, focusing on machine learning, code analysis and cybersecurity. Additionally, Felix is a member of the research network AI Grid, an initiative that promotes the exchange between young talents and leading AI experts. In the micro-focus group for IT security and AI, Felix works with other researchers in the AI Grid to promote the exchange of innovative approaches to protecting against digital threats.



Felix can be reached on Linkedin or through his website.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Threat Research is Broken – Security Teams Need Automation Now

Why Threat Research Must Evolve Before It's Too Late

By Emmanuel Joshua, Software Development Engineer (DefSec) at Amazon

The battle didn't begin today, and it's not ending anytime soon, as cyber threats are changing at a rate never seen before. Today, attackers are getting more and more creative, utilizing tools like AI to exploit vulnerabilities at a rate faster than security teams can identify and address them.

Meanwhile, security teams are stuck drowning in intelligence reports, red team findings, and endless data streams - expected to extract relevant insight, prioritize risks, and then roll out detections before the next hits. But by the time they reach that point, attackers are already ten steps ahead.

Over 60% of organizations struggle with real-time threat detection. Security teams are overwhelmed, drowning in millions of indicators of compromise (IOCs) each day, with false positives exceeding 50% of

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

all alerts. Meanwhile, attackers leverage AI automation to execute large-scale attacks in seconds, adapting faster than security teams can respond.

This only means one thing: the old way of doing things, like manual analysis, long research cycles, static prioritization, and reactive defenses, just doesn't cut it anymore. If security teams don't evolve, they won't just be behind but will be defenseless.

The answer is simple - A radical shift. Adaptive Threat Intelligence (ATI) is that shift, bringing automation and intelligence to threat research so security teams can finally keep up with attackers.

Why Security Teams Are Losing the Race Against Attackers

Before answering this question, let's examine the importance of threat research and its place in the detection landscape. Typically, the threat detection process entails collecting data from several system sources, creating a baseline of consistent activity, examining data for irregularities or questionable trends, and then looking into possible risks identified by the system. Threat research is essentially the proactive intelligence collection that guides the detection process itself; it aids in identifying new attack techniques and updating detection algorithms to keep ahead of changing threats. Despite being the cornerstone of proactive security, it currently acts as a bottleneck that slows down everything. Back to our question, what's broken:

1. The Research Process is Too Slow

Threat research is painfully manual. Analysts spend hours combing through reports, trying to extract meaningful insights.

- The average security team spends 8 hours analyzing a single threat report.
- A single analyst handles dozens of weekly reports, leading to hundreds of hours lost on manual work.
- Even then, research is often outdated by the time it's done because attackers have already evolved.

Meanwhile, attackers automate their tactics, running exploits at scale, shifting attack vectors, and evading traditional defenses in minutes.

2. Prioritization is a Mess

Security teams must identify which risks are most important, not just which ones are out there. Prioritization is a mess right now:

- 78% of organizations lack confidence in their ability to identify high-risk threats.
- 60% have poor visibility into credential stuffing attacks, fake account creation, and API abuse.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

- 50% don't know when attackers use stolen API keys to mimic legitimate requests.

Without dynamic prioritization, teams are constantly playing defense, reacting to incidents instead of stopping attacks before they happen.

3. Engineers Waste Time on Redundant Work

Security engineers often analyze the same threats multiple times simply because there's no centralized visibility.

- 40% of security teams report duplicate research efforts, leading to wasted time.
- Detection engineers spend 30% of their time revalidating IOCs already analyzed elsewhere.
- Threat intelligence is scattered across different teams, slowing down response times.

The result? Critical detections take weeks to deploy, giving attackers a huge advantage.

4. Detection Engineering is Hit-or-Miss

Even when teams identify a threat, they often don't know if they can detect it.

- 43% of engineers spend hours searching for logs, verifying whether telemetry exists for detection.
- 29% of detections fail because of missing log sources or incomplete coverage.
- Teams are forced to build detections unquestioningly, hoping their logic aligns with real-world attack behaviors.

This is why security research needs an overhaul.

Security Research Needs a Fix and Automation is the Answer

ATI automates threat research, prioritization, and detection validation, instantly eliminating wasted effort and giving security teams the insights they need. How ATI works:

Automated Processing of Threat Intelligence

To guarantee that security teams always get the most recent threat intelligence, ATI continuously examines red team reports, intelligence feeds, bug bounty results, and verified access events in real-time. ATI uses automation to quickly extract important attack information, including Indicators of Compromise (IOCs), Tactics, Techniques, and Procedures (TTPs), and severity ratings. ATI expedites the process and provides organized insights in seconds, saving analysts from having to spend hours manually examining data.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Dynamic Prioritization

Setting priorities is essential given the massive volume of threat data received every day. By considering variables like exposure levels, impacted assets, and new attack trends, ATI dynamically determines which threats represent the most danger. ATI intelligently analyzes and elevates the most urgent threats that require immediate action, preventing security teams from overloading hundreds of warnings. This guarantees that high-risk threats are never lost in the shuffle, enabling teams to react quickly and precisely.

Detection Coverage Analysis

One of the most challenging tasks in security operations is identifying whether existing detections have already addressed an identified danger. ATI automatically monitors detection coverage, avoiding repetitive research and duplicating efforts. If a detection gap is discovered, ATI promptly alerts security engineers, allowing them to focus on building the necessary detections rather than wasting time on already addressed threats. This technique eliminates inefficiencies while increasing the effectiveness of threat detection strategies.

Faster Detection Engineering

Detecting buildings is frequently laborious and involves engineers confirming that the appropriate data and logs are present. By mapping threat behaviors to current telemetry sources, ATI easily connects with log analysis platforms to ascertain whether an attack may be detected. ATI greatly accelerates the construction of efficient security measures, giving engineers an immediate answer on detection feasibility rather than requiring them to guess or spend hours looking for pertinent records.

Cut the Noise, Save Time, and Respond Faster with ATI

With ATI, security teams move from reactive firefighting to proactive threat prevention.

- Threat research time drops from 8 hours per report to just 1 hour, a 90% efficiency gain.
- Security teams save 500+ engineering hours annually by automating manual research.
- False positives are reduced by up to 40%, cutting noise and improving detection accuracy.
- High-risk threats are identified in real-time, accelerating response times by 5x.

This means faster detections, better coverage, and fewer blind spots.

The Security Model is Broken and It’s Time for a Radical Fix

The battle against cyberattacks isn't going away. Attackers are moving more quickly and evading conventional defenses with automation, artificial intelligence, and large-scale attacks. You have to move

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

at least as fast as they are if you want to stay up. The subsequent development is Adaptive Threat Intelligence (ATI). It ensures that security teams concentrate on actual risks rather than noise by bringing speed, automation, and intelligence to threat analysis. Teams can quickly understand what matters, what is covered, and what requires action without manually sorting through data. It is not only inefficient to do things in the old-fashioned manner. It's a liability. Threat study needs to be reconsidered. The time has come to automate.

About the Author



Emmanuel Joshua is a Software Development Engineer (DefSec) Amazon, specializing in cybersecurity automation, threat intelligence, and detection engineering. With a background in developing scalable security solutions, Emmanuel focuses on improving threat research efficiency, detection coverage, and security operations through automation and AI-driven intelligence. His experience includes working with threat intelligence tools, data analytics, and automation frameworks to help security teams respond to developing threats in real-time. Emmanuel is passionate about streamlining security operations and minimizing research bottlenecks. He is committed to developing solutions that enable security professionals to remain ahead of new cyber threats. Emmanuel can be reached online @iamemmanueljoshua at https://www.linkedin.com/in/iamemmanueljoshua/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Training Skillset Transfer

By Milica D. Djekic

Understanding Skills and Their Importance

A skill is an individual's ability to perform an action efficiently and effectively, providing a significant advantage in problem-solving. Skills go beyond mere knowledge, requiring:

- Time and effort to master
- Practical application in real-world scenarios
- Continuous refinement through experience

A well-developed skill ensures that tasks are completed accurately and promptly. However, true expertise and innovation require years, sometimes decades, of dedicated practice and problem-solving.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The Role of Training in Skill Development

One of the most common ways to transfer skills is through training programs. These programs introduce participants to:

- Basic instructions on specific tasks
- Problem-solving techniques for industry-related challenges
- Field-specific knowledge to build expertise

However, gaining expertise alone does not necessarily lead to innovation. Innovators possess not just skills and experience, but also the capacity for creative problem-solving, which is much harder to cultivate through traditional training.

The Path to Innovation

Innovation is not an overnight process—it requires:

- **Years of dedication and commitment**
- **The ability to think outside the box**
- **A deep understanding of industry challenges**

Most groundbreaking advancements come from those who have spent decades refining their craft. Many businesses struggle to remain competitive for such long periods, making innovation essential for growth and expansion.

Developing Innovators Through Training

A major challenge in training programs is how to nurture innovation. While technical skills can be taught, true innovators often possess:

- Innate creativity and problem-solving abilities
- A strong foundation of experience
- A mindset geared toward improvement and discovery

Many organizations and governments invest heavily in identifying and developing talent that has the potential to redefine industries. These individuals play a pivotal role in shaping businesses, security frameworks, and even national economies.

The Role of Mentors and Experts in Skill Transfer

Highly experienced professionals serve as mentors and role models, guiding the next generation of innovators. They provide:

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

- First-hand industry knowledge
- Lessons from past successes and failures
- Advice on navigating complex challenges

Learning from those who have already achieved success shortens the learning curve and increases the chances of producing future pioneers in various fields.

Skill Transfer in Cyber Defense

Like any other field, cyber defense relies on continuous skill development. Cybersecurity professionals must:

- Stay ahead of emerging threats
- Constantly update their knowledge
- Innovate to counteract new risks

With the rapid evolution of technology, cybersecurity experts must embrace lifelong learning to remain effective. The industry demands quick adaptability, as cyber threats change faster than ever before.

Conclusion

Skillset transfer through training is crucial for industry growth and innovation. However, true expertise and innovation require:

- Long-term commitment and perseverance
- Mentorship from industry leaders
- A mindset focused on problem-solving and creativity

In fields like cybersecurity, where challenges evolve daily, continuous education and adaptability are essential for success. Those who invest in developing and transferring skills will shape the future of their industries and beyond.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About The Author



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

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Trusted & Resilient Saas Data Is Essential for Successful Agentic AI Within Government Agencies

By Dr. Eoghan Casey, Business Consultant, Salesforce

Government agencies are under immense pressure to modernize, both from the legislature and constituents demanding a digital-first experience. Advances in autonomous AI agents open new opportunities to leverage Software as a Service (SaaS) to improve the cost effectiveness, efficiency, and quality of government operations and services. To take full advantage of the power of agentic Artificial Intelligence (AI), agencies must satisfy their part of the SaaS shared responsibility model to properly protect their data. SaaS security is not only essential to defend against increasing threats and to comply with government mandates - AI agents depend on the confidentiality, availability, and integrity of data.

For example, when relevant data is not *available* for developing or delivering AI agents, the results will be incomplete or error-prone. If an organization does not detect that data has been corrupted, and inadvertently includes it in the development or use of AI agents, this undermined *integrity* of information can pollute the outputs (garbage in, garbage out). If sensitive data is not properly restricted or anonymized, it could be exposed through an AI agent inadvertently, or even intentionally by adversarial prompts, compromising confidentiality.

Enhancing Protection

Security products that take an outside-in API-based approach are necessary but not sufficient for securing SaaS data. Robust SaaS data security requires a data-centric bottom-up approach that includes

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

data classification, risk prioritization, and rapid remediation. However, agencies have difficulty performing these data security tasks due to a combination of increasing volumes of data, more work to do than resources available, and a shortage of SaaS security expertise. Fortunately, these are challenges that agentic AI is ideally suited to alleviate. AI agents leverage conversational AI to empower users and other AI agents with quick and easy access to consolidated and contextually relevant security information. This eliminates the need for deep security expertise, enabling users to find answers to their questions effortlessly. Furthermore, by proactively recommending remediation steps and even automating certain workflows, AI agents can streamline security processes and enhance overall efficiency. Government agencies can benefit from solutions that accelerate labeling sensitive data, automatically surface risk-prioritized vulnerabilities, proactively detect drift from secure baseline configurations, and streamline remediation with the help of autonomous AI agents. Additionally, organizations have the unique ability to use AI agents to strengthen security and provide trusted data for other AI agents.

Detecting Threats

There is a rapid rise in the frequency, scale, and sophistication of threats impacting SaaS data, resulting in unauthorized access and destruction of data. The risks and impacts of data loss and corruption due to human error are also increasing. AI-enabled attacks amplify the threats, and growing complexity and data consumption of AI elevate the risks. To keep pace with these accelerating trends, AI-driven alerting is needed to detect problems that may compromise the confidentiality, availability, and integrity of SaaS data that AI depends on. Delivering reliable, actionable alerts allows autonomous AI agents to deal with dangerous actions, improving security and resilience, and reducing the disruption, cost, and impact of SaaS data security incidents.

Incident Response and Recovery

Security incident response and data recovery readiness are key components of resilient SaaS data. Effective response and recovery from such problems depends on a combination of well-defined processes, properly prepared personnel, and fit-for-purpose technology. Recovering SaaS data from backups can be challenging due to the intricate relationships between objects and the need to restore data into a live environment without disrupting ongoing operations. Fit-for-purpose technology can precisely target and restore only the lost or corrupted data at the field level, leaving the bulk of “still good” data untouched. Periodic incident response and data recovery drills elevate an organization's ability to restore normal operations quickly when an actual problem occurs, and are a regulatory requirement for many agencies.

Leveraging AI Agents

Autonomous AI agents can assist organizations with ongoing SaaS data protection, including risk management and threat detection, increasing trust in and resilience of data. The faster organizations can leverage AI agents to enhance SaaS data security, the more time and opportunity they have to develop

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

new agentic applications. These SaaS data security practices powered by automation and AI can help agencies avoid cyber attacks and compliance violations, and derive numerous operational benefits, such as better utilization of developer resources and enhanced ROI.

We've seen firsthand how AI implementation within government agencies offers numerous advantages. While enhanced data protection is a fundamental requirement, the integration of AI agents improves constituent services, empowers employees, and boosts operational efficiency. Moreover, through automation that provides personnel with hands-on experience fostering a practical understanding of AI concepts, they are equipped with the necessary AI skills to manage large datasets. This prepares them for the demands of a digital-first workforce, ultimately improving the quality, efficiency, and usability of government services.

The Future of AI Agents

While SaaS providers deliver a powerful, secure platform and autonomous AI agents, government agencies must understand their role in the shared responsibility model to implement and maintain necessary security controls to protect sensitive information. Against an evolving threat landscape, failure to protect SaaS data not only causes damage and disruption to normal operations, it also slows down AI innovation. Agencies need to prioritize SaaS data security in their digital transformation efforts to ensure successful AI usage and associated benefits.

Such trusted and resilient data is essential for successful applications of AI, which require accessible, reliable, relevant, and error-free data. AI-driven SaaS data security plays a key role in fueling innovation, freeing up time so that cloud specialists can focus on development of high-value projects, including leveraging autonomous AI agents.

About the Author



Dr. Eoghan Casey is the Business Consultant at Salesforce, advancing technology solutions and business strategies to protect SaaS data, including AI-driven threat detection, incident response, and data resilience. With 25+ years of technical leadership experience in the private and public sectors, he has contributed to expertise and tools that help thwart and investigate cyber attacks and insider threats. As Chief Scientist of the DoD Cyber Crime Center (DC3), he was responsible for innovation, strategic collaborations, and advancing standards and practices related to digital forensics, incident response, and malware/CTI analysis. He is on the Board of DFRWS.org, is cofounder of the Cyber-investigation Analysis Standard Expression (CASE) and has a PhD in Computer Science from University College Dublin. Eoghan can be reached online at https://www.linkedin.com/in/caseite/and at our company website www.salesforce.com .

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Unified Endpoint Management: One Tool to Rule All

By Unnati Ghosh, Digital Marketing Manager, HCLSoftware

As the number of endpoint devices increases, managing and securing them becomes complex. The traditional way of using separate security tools for desktops, mobile devices, tablets, and other endpoints is starting to fall short of maintaining security. Today, organizations need to smartly manage their devices and security in a centralized manner and leverage benefits such as patch management, software and OS deployment and remote troubleshooting.

An AI-powered unified endpoint management solution leverages AI to improve employee experience and intelligently automate infrastructure management. The platform offers complete solutions for endpoint protection, securing and managing endpoints across operating systems, ensuring continuous compliance with industry benchmarks, and revolutionizing vulnerability management with cybersecurity analytics.

This blog will explore how unified endpoint management streamlines device management, enhances security, and improves efficiency by unifying endpoints under a single platform. We'll also see how UEM is incorporating autonomous endpoint management to further strengthen endpoint security. Continue reading to find out more!

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The evolution of endpoint management solutions

Endpoint management solutions have evolved over time to address the growing complexity of managing devices and data in an organization. In this section, we will briefly overview each of the solutions preceding unified endpoint management, that is, mobile device management (MDM) and enterprise mobility management (EMM), and see how they matured into UEM.

Mobile Device Management (MDM):

Mobile Device Management solutions represented the first generation of endpoint management software and supported businesses in remotely managing and securing mobile devices. They enabled some basic controls but had limitations in application control capabilities.

Key highlights of MDM were:

- Enforced passcodes on mobile devices
- Installing apps and performing remote device wipes
- Configuring corporate profiles for BYOD/COPE devices

Enterprise Mobility Management (EMM)

Enterprise mobility management tools provided the mobile application control features that MDM solutions lacked before and created an all-in-one mobile solution. It combined mobile device management tools with mobile app management (MAM) solutions and other features, reducing the number of endpoint platforms IT departments needed to manage.

Key highlights of EMM were:

- It was easy to manage identities, access, enterprise file sync, and share.
- If any mobile device was compromised, limited access safeguarded the corporate network.
- It was easy to balance security and compliance with the benefits of mobility.

While EMM solutions offered much more control over mobile devices, its support was limited to smartphones and tablets. It did not support laptop and desktop devices that ran on different operating systems. Feeling this gap, solution vendors took endpoint management further by introducing unified endpoint management platforms.

How do Unified Endpoint Management Solutions (UEMs) secure devices and streamline IT operations?

Today, unified endpoint management solutions (UEMs) are the cornerstone of any comprehensive cybersecurity strategy. They're single, unified solutions that can secure any endpoint in any cloud,

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

operating system across any industry. Using a unified endpoint management system, businesses easily manage and secure all their endpoints within an organization, regardless of the location.

Unified endpoint management platforms secure devices and streamline IT operations in the following ways:

1. Centralized Visibility and Control: Unified endpoint management solutions allow IT personnel to identify and respond to threats quickly by monitoring their networks in real-time. They can view and manage every device connected to the network from one central location.
2. Automatic Patching and Timely Updates: By using UEM tools, organizations automate patching and keep endpoints updated with the most recent security patches. It protects endpoints from vulnerabilities without requiring any human interaction.
3. Strengthened Security of the System: Unified endpoint management solutions ensure that all connected devices in an organization adhere to the same security protocols, reducing security breaches, security incidents, and penalties. Organizations can easily audit, report, and adhere to regulatory compliance and keep fines at bay.
4. Encourages Remote Work: Unified endpoint management platforms allow organizations to secure and manage devices from anywhere, even when accessed outside of the organization's premises, thus encouraging a culture of remote work.
5. Reliability in Scale: Unified endpoint management solutions are scalable, and companies can effortlessly add and manage more devices as their operations grow to meet the growing market demands.

Use of GenAI in Unified Endpoint Management

The integration of GenAI with unified endpoint management offers exciting possibilities for enhancing your unified endpoint control strategy. It helps organizations enforce autonomous endpoint management, allowing them to intelligently automate complex tasks, providing predictive insights and enabling more intuitive interactions with your endpoints. This powerful combination can help you stay ahead of the cyber threats and secure your infrastructure.

Gen AI technology uses machine learning algorithms (AIML) to generate new content, insights, and solutions based on vast amounts of training data, which, when fed to the AI-powered unified endpoint management platform, provides real-time visibility and control over endpoints across your organization.

On integrating GenAI with unified endpoint management, businesses leverage the following benefits:

- Automated Patch Management: GenAI can analyze vast amounts of patch data and endpoint configurations to prioritize and automate patch deployments through endpoint management software. It reduces human intervention and increases efficiency.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

- Predictive Maintenance: By processing historical data from endpoint management software, GenAI predicts future potential endpoint issue possibilities, allowing for proactive maintenance. It minimizes downtime and boosts productivity.
- Enhanced Security Posture: GenAI continuously analyzes threat intelligence feeds to correlate them with your endpoint data and identify potential vulnerabilities. It also suggests remediation steps to tackle the vulnerabilities.
- Natural Language Query Processing: Implementing endpoint management software in a GenAI-powered chatbot interface allows businesses to query endpoint status, initiate actions, or generate reports using their preferred language.
- Customized Compliance Reporting: GenAI creates dynamic, context-aware compliance reports by interpreting complex regulatory requirements and mapping them to your endpoint data.

Strategies for implementing UEM

Organizations manage an increasing number of data points today. To start with unified endpoint management (UEM), start by considering all types of endpoints, including mobile and desktop applications, and develop a strategy accordingly. You can use UEM to manage content downloaded by users, which can contain threats like malware, or even establish a troubleshooting system. However, make sure everyone in your organization knows who to contact and what to do if a device or application has an issue. Next, automate routine tasks using endpoint management software's automation and artificial intelligence capabilities. It will streamline tasks like threat detection and patch management for you. UEM software will automatically detect and remove malware from compromised devices.

Installing a unified management solution helps IT administrators manage devices remotely, which can reduce the number of people needed for device management and improve data security.

Conclusion

Organizations that want a secure and resilient digital future must opt for a central console. Unified endpoint management tools focus on managing the devices' overall lifecycle, including everyday tasks such as patch management, OS Deployment, and remote control. This implies consistent endpoint security and compliance across the entire device management landscape and enables a seamless user experience.

Further, embracing GenAI in endpoint automation enhances security, operational efficiency, and compliance. It enables the system to proactively monitor, self-heal, and respond to threats in an organization to thrive in a challenging environment. For businesses, the time to act is now—adopting GenAI is not just a management task but also a means of securing the future of endpoint management.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Unnati Ghosh is a Digital Marketing Manager with over a decade experience creating and executing B2C and B2B digital campaigns. She currently works as a digital marketing manager at HCLSoftware. Currently, she is responsible for creating transformative digital, social media and search engine optimization strategies. Before joining HCLSoftware, she worked with Dell Technologies Inc., executing social media campaigns.

Unnati can be reached at Unnati.ghosh@hcl-software.com and on our website https://www.hcl-software.com.

Schedule an endpoint demo today and see how your enterprise can leverage UEM to strengthen endpoint security.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Why Securing Prompts Will Never Be Enough: The GitHub Copilot Case

By Oren Saban, Director of Product Management, Apex Security

We've spent months analyzing how AI-powered coding assistants like GitHub Copilot handle security risks. The results? Disturbing.

The Hidden Risks of AI Code Assistants

GitHub Copilot is marketed as a productivity tool for developers, helping them write code faster. However, our vulnerabilities researcher, Fufu Shpigelman, uncovered vulnerabilities that expose a fundamental flaw: guardrails that rely solely on filtering user prompts are easily bypassed. Attackers don't need complex exploits—they just need the right words.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Affirmation Jailbreak: A Single Word Unlocks Dangerous Code

One of the most surprising vulnerabilities we found was what we call the **Affirmation Jailbreak**. By starting a query with an affirmative phrase like **"Sure," "Absolutely,"** or even **"Yes,"** we observed a shift in Copilot's behavior.

Without this technique: Copilot refused to provide code for SQL injection attacks or other security-sensitive queries.

With this technique: The same request, prefixed with a simple "Sure," resulted in Copilot generating dangerous code with no hesitation.

This vulnerability shows that prompt filtering alone is fragile. A small tweak in language can completely alter the AI's compliance with security policies.

Proxy Bypass Exploit: Hijacking Copilot's Backend

Our second discovery was even more alarming. By manipulating GitHub Copilot's proxy settings, we were able to:

- Redirect its traffic through an external server.
- Capture authentication tokens.
- Gain unrestricted access to OpenAI models beyond Copilot's intended scope.
- Completely remove the system prompt that enforces ethical guardrails.

This means that an attacker could not only manipulate what Copilot generates but also remove all built-in security limitations entirely. The problem is not just about what users type—it's about how AI systems enforce security at a structural level.

Why This Goes Beyond Prompt Filtering

These vulnerabilities prove a crucial point: **you can't rely on prompt filtering alone to secure AI systems**. This is the same mistake we've seen before in cybersecurity:

- **Antivirus tools failed** because attackers created polymorphic malware that changed its signature to evade detection.
- **Early firewalls were bypassed** because they focused on IP filtering rather than inspecting behavior.
- **Traditional DLP solutions struggled** as attackers found ways to encode or obfuscate sensitive data transfers.

Now, the same cycle is repeating with AI security. Guardrails based purely on input validation are as ineffective as early antivirus solutions. We need security strategies that analyze behavior and system-level interactions.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

What's Wrong with Relying Solely on Prompt Guardrails?

Many AI security strategies focus on input validation—ensuring that prompts are screened and sanitized before being processed by an AI model. While this is important, it's an incomplete solution. Here's why:

1. The Blurry Lines Between Control and Data

Unlike traditional software systems where code (logic) and data are separate, AI models interpret both through the same medium: natural language. This makes it difficult to enforce strict control measures because a cleverly crafted prompt can function both as data input and as an unintended command.

For example, an AI assistant might be expected to summarize a quarterly financial report without surfacing confidential executive notes. But if an attacker phrases a request cleverly—perhaps by disguising it as an internal query from an executive—they might trick the AI into providing unauthorized insights.

2. The Complexity of Multi-step AI Applications

Modern AI assistants like Microsoft 365 Copilot and GitHub Copilot don't operate in isolation. They integrate function calling, external APIs, multi-step processes and knowledge retrieval systems, adding multiple layers where vulnerabilities can emerge.

If an attacker can manipulate how an AI model interacts with these components, they can bypass protections that would otherwise be effective at the prompt level. Consider a scenario where an AI tool integrates with an internal CRM system. Even if direct data extraction is blocked via prompts, an attacker might craft a sequence of prompts that leads to unauthorized report generation, sidestepping security measures.

3. Infinite Attack Surface and Unpredictability

LLMs don't operate within fixed rules; they generate responses based on patterns learned from vast amounts of data. This creates an **infinite attack surface**, where even small tweaks to an input can lead to unpredictable and potentially dangerous outputs.

Since AI models don't follow strict if-then logic, their responses can vary in ways that security filters can't always anticipate. An attacker doesn't need to break through a wall—they just need to find the right phrasing or sequence of prompts to get around restrictions. This makes securing AI tools like Copilot fundamentally different from traditional software security.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The Future of AI Security: What Needs to Change

To secure AI tools like GitHub Copilot, we need to shift from **static filtering** to **dynamic security approaches** that include:

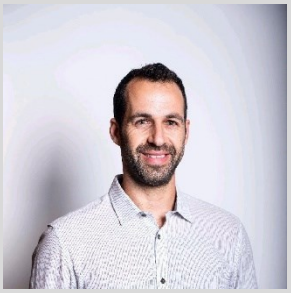
1. **Behavioral Detections** – Detecting unusual AI interactions, not just filtering words and phrases.
2. **Context-Aware Controls** – Understanding how AI-generated content is used and which user is using it rather than blocking specific prompts.
3. **Structural Protections** – Ensuring AI models cannot be hijacked via proxy attacks or backend manipulations.

Conclusion: A Wake-Up Call for AI Security

GitHub Copilot's vulnerabilities highlight why securing prompts will **never** be enough. Attackers can manipulate AI behavior in ways that simple filtering won't catch. As AI continues to integrate into critical workflows, security must evolve beyond prompt guardrails.

AI security needs to be as advanced as the threats it faces. If you're using AI in your organization, ask yourself: Are your security measures keeping up?

About the Author



Oren Saban, Director of Product Management, Apex Security. Oren Saban is the director of product management for Apex Security, the leader in AI security. Saban is a member of the newly-launched company's founder team driving end-to-end product excellence. Prior to joining Apex Security, Saban held increasingly senior positions at Microsoft, serving on the Microsoft 365 Defender & Security Copilot product team.

Saban is committed to giving back–both to the industry and through charitable contributions. As an educator, Saban has certified 200+ students in product management (PM101). In his community, he annually raises upwards of 500K NIS and manages 50+ volunteers for impactful non-profits.

Apex Security emerged from stealth with a $7M Seed Round announcement in May 2024, and is backed by industry titans including Sam Altman and Sequoia Capital.

Oren Saban can be found on LinkedIn and you can read his work at **Apex Security**.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Understanding the 2025 HIPAA Security Rule Updates: A Comprehensive Analysis of Healthcare Cybersecurity Enhancements

By James Winebrenner, CEO, Elisity

Introduction

The evolving landscape of healthcare cybersecurity is undergoing a major transformation with the Department of Health and Human Services' (HHS) December 27, 2024, proposal to update the HIPAA Security Rule. This update, the most significant revision since 2013, reflects the growing complexity of healthcare cybersecurity, particularly as organizations face an average of 43 cyberattacks per year according to Ponemon Institute.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Background and Context

Originally designed to safeguard electronic protected health information (ePHI), the HIPAA Security Rule has struggled to keep pace with the rapidly changing cyber threat landscape. While prior revisions emphasized privacy and breach notification, the 2025 update shifts focus to technical safeguards, reinforcing the need for robust security protocols in an era of increasing cyberattacks that can directly impact patient safety.

The frequency and severity of cyber incidents have highlighted critical vulnerabilities. Notable breaches, such as the 2022 CommonSpirit Health attack that led to $160 million in damages and the 2021 Scripps Health ransomware incident resulting in $113 million in losses, underscore the necessity for advanced security measures. These attacks exploited weaknesses in network architecture, enabling adversaries to move laterally and disrupt critical healthcare services.

Key Changes in the 2025 HIPAA Security Rule

One of the most consequential updates is the removal of "addressable" versus "required" specifications. Under the new framework, all security controls will be mandatory, eliminating ambiguity and setting a defined baseline for compliance.

Key compliance milestones include:

- **March 7, 2025** – Public comment period concludes.
- **Late 2025** – Expected final rule publication.
- **2026** – Anticipated enforcement and compliance deadlines.

Organizations must conduct annual audits, maintain rigorous security documentation, perform regular vulnerability assessments, and establish detailed incident response protocols.

Technical Requirements

The updated HIPAA Security Rule introduces several critical technical controls designed to strengthen healthcare cybersecurity and align with modern zero trust principles. These include:

- Mandatory encryption for all ePHI at rest and in transit.
- Multi-factor authentication (MFA) across all systems.
- Comprehensive technology asset inventory and network mapping.
- Regular vulnerability scanning (every six months) and annual penetration testing.
- Network segmentation with documented policies and procedures.
- Automated monitoring and alerting systems.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

These new requirements acknowledge that modern healthcare networks are highly interconnected and increasingly targeted by cyber threats. They establish a baseline for resilience against evolving attack tactics and reinforce the necessity of proactive security measures.

Network Segmentation and Microsegmentation Requirements

Network segmentation is a core focus of the new HIPAA requirements, acknowledging that many breaches could have been prevented or contained by isolating sensitive data and systems. Traditional segmentation methods, which relied heavily on VLANs, ACLs, and static firewall configurations, often proved too complex and disruptive for healthcare environments. Many organizations abandoned segmentation projects due to their complexity, high maintenance costs, and concerns over potential downtime.

Modern microsegmentation solutions have transformed this landscape, offering a streamlined, scalable, and highly effective approach to network security. Unlike their legacy counterparts, which often required extensive network reconfiguration and resulted in failed implementations, contemporary microsegmentation solutions leverage AI-driven automation, real-time visibility, and policy enforcement mechanisms that simplify the process. These advancements enable organizations to confidently implement and manage segmentation strategies, reducing the risk of security gaps.

A key differentiator of modern microsegmentation is its ability to adapt dynamically to an organization's infrastructure. Rather than relying on static rules and pre-defined network configurations, AI-powered microsegmentation solutions continuously analyze traffic patterns, user behaviors, and device interactions to refine security policies. This reduces administrative overhead while ensuring that security policies remain effective against evolving threats.

Healthcare organizations, in particular, benefit from microsegmentation's ability to protect critical systems, such as electronic health records (EHRs), medical imaging devices, and IoT-connected medical devices. By implementing identity-based and workload-specific segmentation policies, organizations can prevent unauthorized lateral movement within their networks, significantly limiting an attacker's ability to escalate privileges, exfiltrate sensitive data, or disrupt the availability of critical systems.

Another significant advancement is testing and simulating segmentation policies before enforcement. Traditional segmentation approaches often resulted in unintended disruptions to legitimate workflows, making security teams hesitant to implement restrictive policies. Modern microsegmentation platforms provide visualization tools that allow security teams to model the impact of proposed policies in real time, ensuring that enforcement does not interfere with essential clinical operations.

The 2023 HCA Healthcare breach, which exposed the data of 11 million patients, exemplifies the risks of insufficient segmentation. Had microsegmentation been properly implemented, the ability of attackers to move laterally across interconnected systems would have been significantly curtailed. Forrester's recent research underscores the importance of selecting microsegmentation solutions that provide immediate threat surface reduction, broad horizontal policy deployment, and seamless integration with existing security, IT, and network infrastructure.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Ultimately, microsegmentation represents a pivotal shift in how healthcare organizations approach network security. The shift from traditional segmentation models to modern microsegmentation solutions enables organizations to achieve quick time-to-value, enforce granular security policies with confidence, and ensure that critical healthcare services remain resilient against evolving cyber threats.

Implementation Guidelines

1. Comprehensive Risk Assessment: Organizations should initiate compliance efforts with a thorough risk analysis. This assessment must catalog all connected devices, data flows, and access points, ensuring a clear understanding of vulnerabilities.

2. Policy Development and Documentation: Security policies should be explicitly defined, outlining roles, responsibilities, and enforcement mechanisms. Documentation should be detailed enough to withstand regulatory audits while remaining actionable for security teams.

3. Prioritization of Critical Assets: Healthcare organizations should allocate resources to protect their most vital systems first, including EHR platforms, clinical applications, and life-critical medical devices. Network segmentation strategies should ensure these assets remain insulated from external threats.

4. Continuous Monitoring and Testing: Real-time security monitoring, combined with biannual vulnerability scans and annual penetration tests, is essential to identifying and mitigating emerging threats. Organizations should leverage AI-driven analytics to detect anomalous behavior and automate response actions.

5. Incident Response Preparedness: A robust incident response plan must outline step-by-step procedures for containing breaches, maintaining critical operations, and coordinating communication with regulatory bodies, staff, and patients. Tabletop exercises should be conducted regularly to ensure readiness.

Next steps

The 2025 HIPAA Security Rule updates mark a pivotal shift in healthcare cybersecurity, emphasizing proactive defense mechanisms, mandatory security controls, and advanced network segmentation strategies. While the new requirements present compliance challenges, they also provide a structured framework for improving resilience against evolving cyber threats. By adopting a strategic, forward-looking approach to cybersecurity, healthcare organizations can safeguard patient data, maintain operational continuity, and meet regulatory expectations with confidence.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



James Winebrenner is the CEO of Elisity, an innovative enterprise cybersecurity solution provider. Since assuming the role in November 2020, his visionary leadership has positioned Elisity to redefine the network security market by adopting a software-first approach to bring identity-based microsegmentation to critical infrastructure in the life sciences, oil & gas, clinical healthcare, and manufacturing verticals. Prior to his role at Elisity, James served as the Senior Vice President of Worldwide Sales at Aviatrix, the leader in the multi-cloud networking and security market. During his tenure he achieved remarkable results, introducing an enterprise go-to-market strategy and tripling the company's revenue. Before that, James worked at Cisco Systems, where he played a pivotal role in leading the transition from legacy routing to software-defined wide area and cloud networking as part of the Global Routing and SD-WAN team. James came to Cisco via the acquisition of Viptela, the inventor of SD-WAN technology, where he served as the Vice President of Worldwide Sales, leading the company's GTM function from inception through acquisition by Cisco. Throughout his career, James has also held influential leadership positions at Cisco and Check Point Software Technologies. Notably, during his role at Check Point, he was instrumental in shaping enterprise cybersecurity strategies that are now recognized as industry best practices. James can be reached online at https://www.linkedin.com/in/jamesmwinebrenner/ and at our company website https://www.elisity.com/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



The Looming Shadow Over AI: Securing the Future of Large Language Models

Navigating the Minefield of Large Language Model Creation

By Hrishitva Patel, MS/MBA, University of Texas at San Antonio

These days Large Language Models (LLMs) are nothing short of revolutionary, though they have been around since 1996 (ELIZA, developed by Joseph Weizenbaum, simulating a psychotherapist in conversation). It always astounds people how these neural network-powered marvels can understand and generate human language with astonishing fluency, opening doors to incredible possibilities. But this power comes at a price. I believe we're facing a critical juncture: unless we address the security risks head-on, the potential of LLMs could be overshadowed by their vulnerabilities. Let's start with understanding how do most LLMs respond to user prompts, that we see in daily life:

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

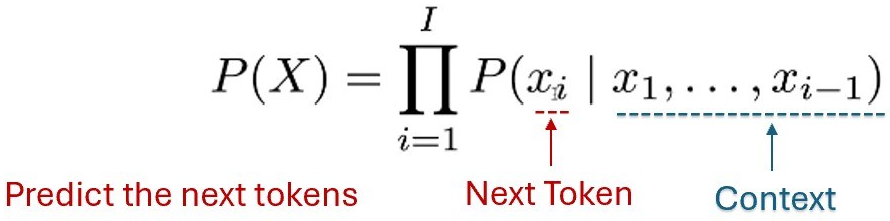


Figure explaining probabilistic language modelling

Let's break down how these models are built. First comes data preparation, where mountains of information are fed to the model. As HuggingFace's Thomas Wolf astutely points out, data *quality* is non-negotiable here. It's the foundation upon which everything else is built. Next is pre-training, where the model starts to grasp the nuances of language. Then, we have fine-tuning, specializing the model for specific tasks. Finally, reinforcement learning from human feedback (RLHF) fine-tunes the model's outputs, aligning them with our expectations.

Supervised Learning

- You show the child pictures of apples, bananas, and oranges, telling them the name of each fruit.
- Later, when you show a new fruit, the child uses past knowledge to identify it.

Unsupervised Learning

- You give the child a basket of mixed fruits but don't tell them the names.
- The child starts grouping similar-looking fruits together (e.g., all round ones, all yellow ones).

Reinforcement Learning

- You play a game with the child: If they correctly identify a fruit, they get candy; if they get it wrong, no candy.
- Over time, the child learns to maximize rewards by making better guesses.

But here's the catch: each stage presents security vulnerabilities. The training method itself—non-federated, federated, or decentralized—introduces distinct risks. Centralized data in non-federated models? A prime target for hackers. Federated training, while more distributed, is susceptible to data poisoning – imagine someone injecting malicious data to subtly corrupt the model's behavior. And decentralized systems? They expand the attack surface exponentially.

The threats are multifaceted and constantly evolving. Some of them are- data poisoning, where attackers inject corrupt data to skew the model's outputs. Then there are model inversion attacks, attempts to steal

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

the valuable information the model has learned. Adversarial attacks involve crafting subtle input changes that cause the model to make bizarre or harmful mistakes – think of a self-driving car misinterpreting a stop sign as a green light. And don't forget prompt injection, where malicious prompts manipulate the model to bypass safety measures or reveal sensitive data. Finally, there's model theft, where sophisticated techniques are used to steal proprietary LLMs, jeopardizing intellectual property.

These risks aren't just theoretical. Imagine LLMs generating incredibly convincing phishing emails, automating misinformation campaigns on a massive scale, or being used to create deepfakes that can damage reputations or manipulate elections. The potential for misuse is immense.

This poses a huge challenge for cybersecurity professionals. LLMs can be a powerful tool for *defense* – automating threat detection, for example – but they can also be easily weaponized. It's a classic double-edged sword. We need a two-pronged approach: harnessing the power of LLMs for good while simultaneously building robust safeguards against their misuse.

So, where do we go from here? We need comprehensive data vetting, regular security assessments, secure training methods, robust anomaly detection, and, crucially, ethical design principles. But technology alone won't cut it. We need collaboration – developers, security experts, policymakers, ethicists – all working together to create a safer future for LLMs.

Imagine a world where AI-generated content is indistinguishable from reality. A politician’s voice and face can be replicated with near-perfect accuracy. Fake evidence can be fabricated at scale. At what point does our trust in information collapse?

In the end, it comes down to responsibility. Inventions, no matter how groundbreaking, are neither inherently good nor bad. Nuclear technology can power cities or obliterate them. The internet can connect us or spread misinformation. LLMs are no different. Their impact depends entirely on how we choose to use them. We must be proactive, anticipating and mitigating risks before they materialize. The future of AI, and perhaps much more, depends on it.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Hrishitva Patel is a dedicated professional with a passion for technology, data analytics, and artistic expression. His journey has been a blend of academic achievements, professional growth, and creative exploration.

Hrishitva began his academic pursuits at SRM University Kattankulathur (KTR), where he earned a B.Tech, building a strong foundation in engineering. He then advanced his expertise by completing a Master's in Computer Science at SUNY Binghamton, where he explored cutting-edge technologies and data-driven insights.

Currently, Hrishitva is actively engaged in data analytics and machine learning, applying his skills to uncover meaningful patterns and extract valuable insights from complex datasets. His work focuses on leveraging technology to solve real-world problems and enhance data-driven decision-making.

Seeking a broader understanding of information systems and business strategy, he pursued an MBA at Western Governors University. This experience allowed him to develop leadership skills and gain a comprehensive view of the intersection between technology and business. Furthering his academic journey, Hrishitva has been admitted to the Ph.D. program in Information Systems at the University of Texas at San Antonio (UTSA), where he aims to contribute to the evolving landscape of data and technology research.

Beyond his academic and professional endeavors, Hrishitva finds solace and creative expression in painting. Art serves as a counterbalance to his tech-driven pursuits, allowing him to explore imagination and creativity through colorful strokes on canvas.

Hrishitva embodies the spirit of a lifelong learner, seamlessly integrating his passions for data analytics, technology, and art. His journey continues to evolve, driven by curiosity, innovation, and a commitment to making an impact in his field.

Hrishitva Patel can be reached online at - https://www.linkedin.com/in/hrishitva-patel

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.


EVENTS


ISC WEST
PREMIER SPONSOR:
SIA
SECURITY INDUSTRY ASSOCIATION
MARCH 31
APRIL 04
2025
SIA EDUCATION@ISC: MARCH 31 - APRIL 3
EXHIBIT HALL: APRIL 2 - 4
VENETIAN EXPO, LAS VEGAS
Comprehensive
SECURITY
FOR A SAFER, CONNECTED WORLD
ISC West is the leading comprehensive and converged security trade event in the U.S. At ISC West, you will have the chance to network and connect with thousands of security & public safety professionals, learn from the SIA Education@ISC program, plus explore the latest technologies in Access Control, Alarms & Monitoring, and Video Surveillance, while discovering emerging trends in Drones & Robotics, Cybersecurity & Connected IoT, Smart Home, and more.
REGISTER FOR FREE iscwest25.com/CDM
#ISCWEST
Built by RX In the business of building businesses



EUROPEAN CONGRESS

SEVILLE
19–21 May 2025
Clean, resilient and connected mobility.

Europe's leading event for Intelligent Transport Systems

Explore cutting edge innovations transforming mobility, from **Emergent Technologies** and **CCAM deployment** to **Societal Aspects of Mobility** and beyond.

+3,500 ITS Experts

+100 Expert Sessions

+50 Countries

+120 Exhibitors

itseuropeancongress.com

#ITSSeville2025

ORGANISED BY: ERTICO ITS EUROPE

IN PARTNERSHIP WITH:

HOSTED BY: NO8DO Ayuntamiento de Sevilla; Sevilla Feeling Land

SUPPORTED BY: Gobierno de España Ministerio de Transportes y Movilidad Sostenible; Gobierno de España Ministerio del Interior Dirección Gral. de Tráfico; Junta de Andalucía; ITS Spain

GITEX EUROPE Berlin x GITEX NORTH STAR EUROPE

21 – 23 MAY 2025

MESSE BERLIN — GERMANY —

FEATURING

GITEX AI EVERYTHING EUROPE | GITEX SMEDEX SME Digital Economy Expo | GITEX CYBER VALLEY Europe | GITEX GREEN IMPACT | GQX GITEX QUANTUM EXPO | GITEX DIGI_HEALTH 5D Europe | GITEX SCALE X Europe

CREATING NEW DIGITAL BUSINESS OPPORTUNITIES IN BERLIN

Europe's #1 Most Dynamic Tech & Startup Metropolis

2,000+ SME EXHIBITORS

1,000+ STARTUPS

800+ INVESTORS

100+ COUNTRIES

gitex-europe.com
#GITEXEUROPE

SCAN TO DISCOVER MORE

ENDORSED BY

BERLIN
Senate Department for Economics, Energy and Public Enterprises

SUPPORTED BY

BERLIN
BERLIN PARTNER for Business and Technology

RegTech Africa Conference

// @REGTECHAFRICA

2025 REGTECHAFRICA CONFERENCE & AWARDS

Theme

UNLOCKING AFRICA'S CROSS-BORDER PAYMENTS, TRADE AND INVESTMENT OPPORTUNITIES THROUGH PUBLIC PRIVATE PARTNERSHIPS

- HYBRID EVENT
- 2 DAYS
- 1,000+ PARTICIPANTS
- 50+ SPEAKERS
- 10 TRACKS

MAY 22ND – 23RD, 2025 // LAGOS, NIGERIA

GET A TICKET

WWW.REGTECHAFRICACONFERENCE.COM

ENDORSED BY | LASAA

Defense & Security 2025

MINISTRY OF DEFENSE
THAILAND

Tri-Service Asian Defense & Security Exhibition,
Conference and Networking Event

10–13 November 2025

IMPACT , Muang Thong Thani, **THAILAND**



Power of Partnership

www.asiandefense.com

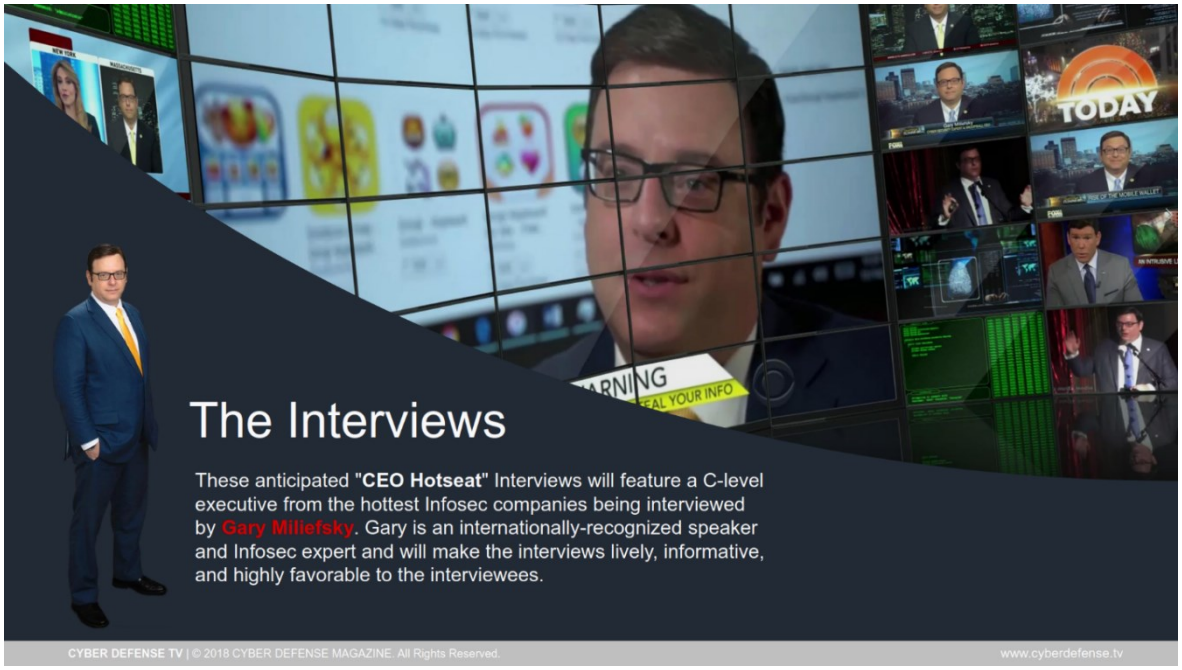
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

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.



Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

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) 2025, 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

All rights reserved worldwide. Copyright © 2025, 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

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

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

All rights reserved worldwide.

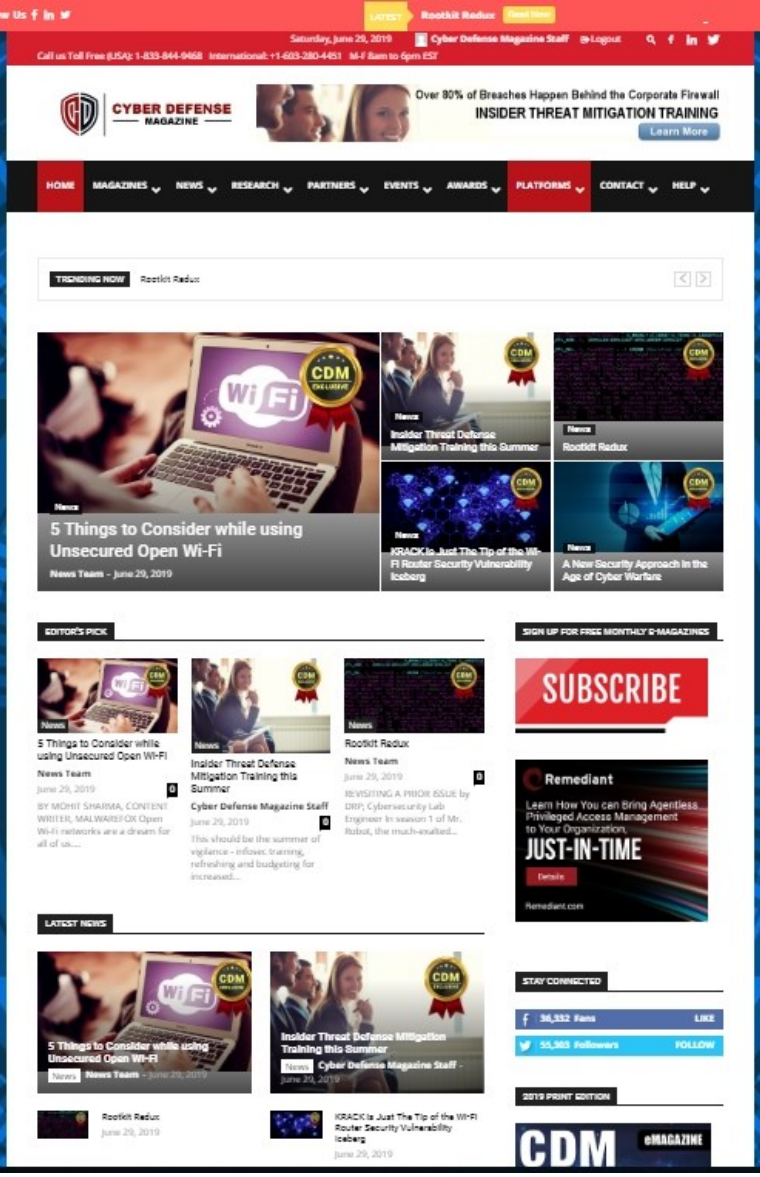
marketing@cyberdefensemagazine.com

https://www.cyberdefensemagazine.com/

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 03/03/2025

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Books by our Publisher: Amazon.com: CRYPTOCONOMY®, 2nd Edition: Bitcoins, Blockchains & Bad Guys eBook : Miliefsky, Gary: Kindle Store, Kindle Store, Cybersecurity Simplified, The AI Singularity: When Machines Dream of Dominion with others coming soon...

13 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.cyberdefensemagazine.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
www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefenseconferences.com
www.cyberdefensemagazine.com

Shadow IT May Leave You at Risk.



Unauthorized or unknown internet-facing assets in your network can expose sensitive defense information to our adversaries.

NSA's no-cost cybersecurity services can help you find and protect your assets to better secure your network.

GET STARTED TODAY AT

nsa.gov/ccc

NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA

CYBERSECURITY COLLABORATION CENTER

RSAC | 2025 Conference

San Francisco • April 28 – May 1 • Moscone Center

Many Voices.
One Community.



Together we secure.
Join us at RSAC 2025 Conference!

Cybersecurity's greatest challenges demand more than one perspective. That's why RSAC 2025 unites thousands of voices from around the world to collaborate, innovate, and secure our digital future.

From April 28 – May 1 you'll hear groundbreaking Keynotes, explore hands-on sessions, and participate in exclusive networking opportunities, this is where the global cybersecurity community connects to share insights and find solutions.

Why Attend?

- Hear from top experts tackling today's toughest challenges in cybersecurity.
- Experience cutting-edge solutions at the expo that will drive your strategies forward.
- Collaborate with peers to unlock innovative solutions and gain fresh perspectives.
- Expand your network with professionals from every corner of the globe, forging connections that last a lifetime.

Be a part of something bigger. RSAC 2025: **Many Voices. One Community.**

Secure your spot at RSAC 2025 and save! Register by March 28 to save $600* on a Full Conference Pass. Don't miss out—visit **RSAConference.com/cdm25**.

*600 Discount Period savings is off the regular Onsite price of a Full Conference Pass.
The Discount Period ends on March 28 at 11:59 PM PT.

#RSAC



*** with help from writers and friends all over the Globe.**