PALO ALTO NETWORKS

perspectives

MARCH 2025

THE FUTURE SECURED

Insights from the Frontlines of Innovation

Better Security Outcomes Start in the Boardroom:
Why Platformization Is Essential

Understanding and Leveraging the Role of Platformization in AI-First Cybersecurity

C-Suite Leaders Embrace Platformization for Security Success

Contributors

RICH CAMPAGNA is the SVP of Product Management at Palo Alto Networks.

SHERYL CHAMBERLAIN is the Managing Director of Global Alliances at Palo Alto Networks.

DAN FORD is the CISO at Jovia Financial Credit Union.

SAM KAPLAN is the Assistant General Counsel for Public Policy at Palo Alto Networks.

DANIEL KROESE is the VP of Public Policy & Government Affairs at Palo Alto Networks.

ANAND OSWAL is the SVP and GM of Network Security at Palo Alto Networks.

HAIDER PASHA is the CSO of EMEA & LATAM at Palo Alto Networks.

MEERAH RAJAVEL is the CIO at Palo Alto Networks.

NAVNEET SINGH is the VP of Network Security Marketing at Palo Alto Networks.

KARIM TEMSAMANI is the President of Next-Generation Security at Palo Alto Networks.

NIR ZUK is the CTO and Founder of Palo Alto Networks.

Security at Scale: Why Leaders Are Betting on Platformization

Leading the Charge: AI, Innovation, and Cyber Resilience

Cybersecurity at Every Level: From Fundamentals to Public Policy

Better Security Outcomes Start in the Boardroom: Why Platformization Is Essential

BY KARIM TEMSAMANI

We've reached a critical juncture in cybersecurity. Artificial intelligence is evolving with unprecedented speed, making threats more frequent and sophisticated, and enterprises are struggling under the weight of fragmented security ecosystems.

A new IBM Institute for Business Value study,[1] conducted in collaboration with Palo Alto Networks, lays bare a reality that many security leaders already know too well: complexity has morphed from a costly operational challenge to the "biggest impediment to their security operations." Layer upon layer of disconnected tools have created a patchwork defense, leaving organizations exposed. Platformization is the solution that transforms security into a unified, intelligent system.

Still, today, dozens of organizations respond to new threats and changing needs by layering on additional security tools. The study found that the average enterprise now manages 83 security solutions from 29 vendors.[2] As a result, security operations centers (SOCs) have become inundated with alerts, unable to separate the signal from the noise. This sprawl has created an untenable situation where visibility is fragmented, integration is haphazard, and response times are unacceptably slow.

The research does, however, highlight an urgent shift is underway: 75% of organizations that have embraced security platformization agree that better integration across security, hybrid cloud, AI, and other technology platforms is crucial,[3] with 80% of platformization adopters already reporting they have full visibility into potential vulnerabilities and threats.[4] The time for incremental solutions has passed, and the answer is clear: The future of cybersecurity demands platformization. ››

Platformization as a Business Strategy

At its core, platformization integrates multiple security functions into a unified system where AI, automation, and real-time analytics work together seamlessly. Platformization not only reduces tool fatigue and streamlines IT operations but also serves as a fundamental reimagining of how organizations secure their digital environments.

According to the study, organizations that have embraced security platformization identify threats 72 days faster and contain them 84 days sooner than their nonplatformized counterparts.[5] They also achieve an average ROI of 101% on their cybersecurity investments — nearly four times the return seen by nonadopters. But this isn't just about cost savings; it's about enabling growth, protecting revenue, and ensuring that cybersecurity is a strategic enabler rather than a barrier to innovation.

In a recent podcast, I talked with Mark Hughes, IBM's Global Managing Partner for Cybersecurity Services, who astutely pointed out that complexity itself is the enemy. The more fragmented an organization's security infrastructure, the harder it becomes to articulate risk to the board, let alone manage it effectively. This is why cybersecurity must shift from being viewed as an operational necessity to a boardroom priority. The question executives should be asking is not whether platformization is necessary but how soon they can implement a comprehensive strategy.

AI and the Evolution of Security Operations

One of the most striking takeaways from the study is the way AI is transforming security operations. Palo Alto Networks alone blocks up to 30.9 billion attacks daily, with nearly 9 million of those being new and unique threats that didn't exist the day before. Traditional, siloed security approaches cannot keep pace with this level of dynamism — nor can humans. Organizations that leverage AI-driven security platforms can move 60 times faster in preventing attacks compared to those relying on disjointed systems.

But adding AI isn't enough — security for AI must be built by design. This means ensuring that AI models are trained on high-quality, diverse threat intelligence, that automation is used to orchestrate real-time responses, and that security teams are equipped with the tools to operationalize AI insights effectively.

This is where platformization delivers true value. Unifying security functions — threat detection, incident response, compliance management — under a single AI-powered system allows organizations to shift from reactive security postures to proactive threat prevention. Instead of SOC analysts manually stitching together insights from multiple tools, a platformized approach provides a singular, real-time view of an organization's security landscape.

The Board's Role in Driving Security Transformation

Too many boardroom discussions on cybersecurity have historically been reactive — focused on compliance, risk mitigation, and breach response. But in today's environment, security must be embedded in business strategy from the outset. As Hughes pointed out, one of the biggest obstacles organizations face is not just the sophistication of attackers but their own inability to articulate risk clearly to executives.

Security leaders must bridge this gap by reframing cybersecurity as a business imperative. The study found that 95% of executives in platformized organizations now view security as a source of value rather than a cost center. This shift in mindset is critical, but, oftentimes, unprecedented. Security should not be viewed as a sunk cost. It is an investment that enhances resilience, accelerates digital transformation, and ultimately fuels revenue growth.

Security for the Future

The future of security belongs to those who embrace transformation – not just in technology but in mindset. Organizations that continue to navigate a labyrinth of disconnected tools will find themselves too slow, too reactive, and ultimately too exposed. Platformization isn't about consolidating for the sake of efficiency; it's about better security outcomes and enabling security teams to operate ahead of the speed of threats. ◆

[1] *Capturing the cybersecurity dividend: How security platforms generate business value*. IBM Institute for Business Value and Palo Alto Networks, 28 January 2025.

[2] Ibid.

[3] Ibid.

[4] "Top 10 Critical Findings for Considering Security Platformization in 2025." Palo Alto Networks, 28 January 2025.

[5] Chamberlain, Sheryl. "C-Suite Leaders Embrace Platformization for Security Success." Palo Alto Networks, 28 January 2025.

C-Suite Leaders Embrace Platformization for Security Success

BY SHERYL CHAMBERLAIN

Businesses are facing a significant challenge – security fragmentation and complexity are getting in the way of results. The IBM Institute for Business Value in collaboration with Palo Alto Networks conducted the study, *Capturing the cybersecurity dividend: how security platforms generate business value*.[1] The research found 52% of surveyed executives identified complexity as the biggest impediment to their security operations. With the average organization managing 83 different security solutions from 29 vendors, the struggle to keep security operations streamlined and effective is real.

The Cost of Complexity

Security fragmentation is not just an operational headache; it's a productivity and financial drain. As threats grow, many organizations add more security tools, but this approach often leads to inefficiencies and skyrocketing costs. With cybersecurity spending expected to grow over 50% from 2023 to 2025, according to the study, organizations are under immense pressure to reduce costs while improving security outcomes.

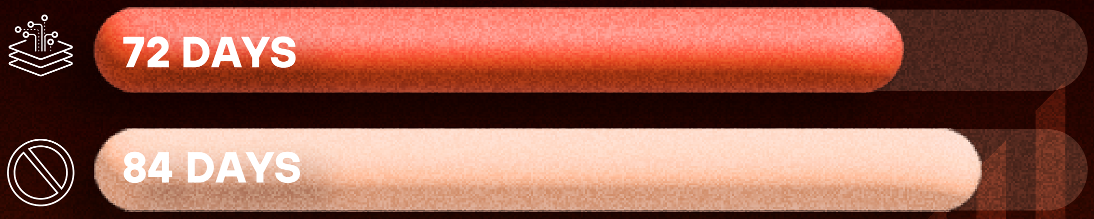
Debunking the Myth, More Solutions Equals More Security

It's not that most organizations believe that adding more solutions will enhance their security posture, but that along the way they have selected various "best of breed" solutions to solve the security challenge of the moment. However, research shows that this approach compounds complexity and dilutes the benefits of individual tools, ultimately reducing overall effectiveness.

Platformization — the Key to Faster, More Efficient Security Operations

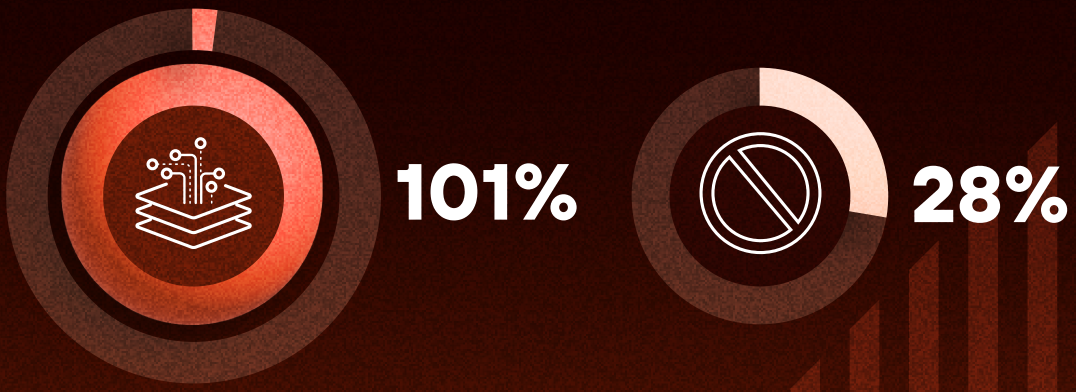
A clear solution to this complexity is platformization – the consolidation of security solutions into integrated platforms. Organizations that adopt platform-based approaches report significant benefits:

- Faster Incident Response – On average, platformized organizations identify security incidents 72 days faster and contain them 84 days sooner than their non-platformized peers.
- Better ROI – Platformized companies achieve an average 101% ROI, compared to 28% for organizations that have not yet embraced platformization. ››



Speed as Organization Savior

Platformized organizations identify security incidents **72 days faster** and contain them **84 days more quickly** than their nonplatformized counterparts.



Maximizing ROI in Tight Markets

Platformized organizations achieve an average **ROI of 101%** on cybersecurity investments, while nonadopters achieve only a **28%** ROI.

Cybersecurity as a Bottom-Line Driver

The transformation driven by platformization extends beyond operational efficiency. 96% of executives who have adopted platformization now view security as a value generator, compared to only 8% of those who haven't embraced this approach. Integrated security platforms not only reduce costs but also unlock opportunities for innovation and growth, turning cybersecurity from a necessary expense into a strategic asset in their current digital transformation initiatives.

Read Capturing the cybersecurity dividend: How security platforms generate business value[2] for more insights and actionable steps to help you take a platform-enabled approach to security this year. ◆

> Security fragmentation is not just an operational headache; it's a productivity and financial drain.

[1] *Capturing the cybersecurity dividend: How security platforms generate business value.* IBM Institute for Business Value and Palo Alto Networks, 28 January 2025.

[2] Ibid.

Understanding and Leveraging the Role of Platformization in AI-First Cybersecurity

BY RICH CAMPAGNA

It seems inevitable that the worlds of cybersecurity and artificial intelligence (AI) should intersect, collide, and transform each other. Each is rapidly changing due to a combination of significant technical advances and the revolution in how, when, where, and why technology is used—for both better and worse.

This isn't just a matter of tracking the amount of financial and human resources that go into both cybersecurity and AI—although those trends are undeniable and top of mind for technical leaders, business executives, line-of-business stakeholders, and board members. The convergence of cybersecurity and AI has changed the rules of the game when it comes to both how organizations leverage this trend for more robust and flexible cybersecurity defenses and how attackers take advantage of the same trend to make their attacks more frequent and potentially more successful.

Take generative AI (GenAI), for instance. GenAI leaped to the front of the pack of AI iterations reshaping the role and impact of the technology, including machine learning, predictive AI, causal AI, and deep learning.

Industry analyst firm Enterprise Strategy Group recently issued a report on how generative AI impacts organizations' cybersecurity efforts. This report points out that 76% of organizations feel cyberattackers will gain the biggest advantage from generative AI, compared with just 24% who believe security defenders will have the upper hand.[1] Still, despite organizations' concerns about hackers initially gaining an edge with the technology, the ESG analysts wrote: "Generative AI could help improve security team productivity, accelerate threat detection, automate remediation actions, and guide incident response."[2] ››

Cybersecurity Pressure Mounts: New Solutions and Mindsets Are Essential

You don't need to be a chief information security officer to understand that cybersecurity is more challenging than ever, even without the impact of AI. There are two major reasons why: First, the massive influx of new threats presses organizations to detect, respond to, and remediate attacks faster and more completely. Second, managing an ever-expanding portfolio of tools, services, and solutions continues to be more complex, which can lead to mistakes and security coverage gaps.

The cybersecurity tools sprawl also brings other real-world challenges. Each tool has a different console, data logging convention, and context. This can make it significantly more difficult for security teams to fill in those coverage gaps while minimizing errors. Worst of all, it means security teams may spend a lot of time integrating versus doing actual security.

For years, the typical answer for this growing array of threats and challenges has been new tools—lots of them. But having dozens and dozens of best-of-breed tools and services to pick through when determining how to prevent and respond to attacks takes time, money, and skills. Since those resources are in short supply and getting tighter, organizations are pressed to find a new way to overcome this complexity and reduce risk, especially in an era when artificial intelligence is a powerful weapon being leveraged by attackers.

More and more often, organizations opt for a platformization approach to managing the cybersecurity puzzle to reduce complexity, identify and mitigate risk, and ensure a more digitally secure environment. In fact, Gartner cited "consolidation" as a key CISO trend in 2023.[3]

Introducing Platformization

Platformization combines numerous products and services into a unified architecture with a single datastore, streamlined management and operations, and native integrations to reduce the time required to have different products speak to each other.

In order for platformization to meet its expectations, several critical requirements must be fulfilled. First, every product or service consolidated into the platform must be as good or better than the corresponding point products available in that space. Adopting a platform should never mean sacrificing security efficacy for simplified management or vendor consolidation.

Next, the platform must be modular, allowing your organization to grow into the use of the platform over time. Wholesale replacements of many different security products at the same time can be more complicated than most organizations would want to take on. Adding the challenge of different replacement cycles of incumbent offerings makes it even more difficult. A platform must be adoptable in whole or in parts, without losing its ability to meet the complete need of the use cases being considered.

Finally, the platform must also enable native platform integrations that make each component even stronger than it would be on its own. All too often, vendors develop platforms as "ships in the night," building a single user interface but with each product operating entirely independently beneath that UI. Everything from policy management to reporting must be consolidated and tightly integrated. As an example, if you're evaluating a platform for network security and that platform offers numerous services to protect against different types of advanced threats, visibility into where and how you're stopping each threat should be consolidated and reported centrally. It should not be in separate reports that pull from entirely separate datastores.

Why Is Platformization So Important?

Most importantly, an integrated, consolidated, coordinated platform can help bring better security. Pulling together multiple solutions into a single platform can all but eliminate the security coverage gaps that naturally occur when multiple individual point products are deployed to solve narrow, specific problems. This is especially important as cyberattacks leverage multiple vulnerabilities simultaneously, thanks to attackers' opportunistic use of AI. ››

One of the key elements of platformization is the ability to have a unified dataset pulled from a myriad of sources to create a richer telemetry of cybersecurity-specific data.

But there's more. By consolidating a number of related products, services, and tools into a single platform designed within a common architecture, with single-pane-of-glass orchestration, organizations can:

- Unify data to uncover the source and impact of emerging threats and zero-days.
- Achieve seamless consistency and traceability, helping ensure consistency at every point and integration across the lifecycle.
- Dramatically ease the management of cybersecurity solutions.
- Improve visibility across threat vectors, geographies, and technology platforms.
- Reduce cybersecurity risk by helping to detect and block attacks much faster and more reliably.
- Reduce procurement costs, such as purchasing, licensing, integrating, and maintaining a multitude of solutions.
- Stop double-paying for overlapping functionality among different product sets.
- Trim the training and education burden for cybersecurity and IT professionals since the consolidated solutions under a platform are designed to "collaborate."

Platforms also are an efficient way to use the power and utility of AI/ML not only to remediate the impact of attacks but also to spot and block attacks before they hit. AI-powered platforms provide SecOps teams dramatically improved visibility and enhanced intelligence to deliver the proper response to the growing range of attacks. AI also drives platforms' value by surfacing high-fidelity data to inform decisions made by and for tools consolidated within the platform. The result is better security outcomes, especially when APIs and plugins enable the platform to ingest data from trusted third-party sources.

Why Cybersecurity Platformization Matters More than Ever in an AI-Centric Environment, Thanks to Precision AI by Palo Alto Networks

The development of cybersecurity platforms in an AI-centric era was hardly an act of luck and serendipity. Palo Alto Networks engineers and security professionals anticipated the growing significance and impact of AI as a force multiplier for more effective cybersecurity. They also understand the technology's potential to be leveraged by hackers for faster, easier, and wider-impact threats.

Platforms are critical to taking advantage of all AI has to offer (in cybersecurity and in other use cases) for several reasons. For example, they can:

- Identify and prevent AI-specific threats, such as malicious use of AI-generated code for identity theft or inappropriate access controls.
- Prevent corrupt code from being generated and integrated into application development lifecycles or in the creation of organization-specific large language models.
- Spot and block attempts to plant malicious AI-generated code during the deployment of production systems.
- Provide more comprehensive and efficient data protection and privacy.

By making cybersecurity frameworks and architectures simpler to design and deploy, platforms promote improved cybersecurity posture and offset the growing problem area of the cybersecurity skills gap with widespread automation and improved orchestration.

Another vital part of the growing role of platformization in an AI-centric era is Precision AI® by Palo Alto Networks. One of the key elements of ›› platformization is the ability to have a unified dataset pulled from a myriad of sources to create a richer telemetry of cybersecurity-specific data. At the heart of this focus on unified data is Precision AI, the Palo Alto Networks proprietary AI system. Precision AI incorporates best-of-breed AI capabilities, including machine learning, deep learning, and GenAI to create security-specific data models that automate detection, prevention, and remediation.

Powered by Precision AI, Palo Alto Networks products are a great fit for cybersecurity platformization because they leverage the security dataset created, curated, and organized at the platform level. Our platform is an apt set of solutions for many organizations because the products powered by Precision AI are engineered to work in hybrid environments, collecting and leveraging relevant data from on-premises, edge, and multicloud settings.

This allows the cybersecurity platform to capture and contextualize security-related data to identify and prevent attacks in real time. Precision AI helps to drive trust and confidence in platform-driven recommendations by using the right information, in the right context, in the right manner, helping to obviate the impact of alert fatigue, false positives, and human error that contribute to cybersecurity problems.

Platformization is an essential part of optimizing the use of products powered by Precision AI because it consolidates and integrates a wide range of features and capabilities in a simplified, contextually aware framework built heavily upon the concepts of data accessibility, improved visibility, and automated response.

How Palo Alto Networks Helps Organizations Get the Most from AI and Platformization

Over the past several years, Palo Alto Networks has been on a mission to simplify cybersecurity while at the same time improving outcomes. This has driven the development of three platforms powered by Precision AI, collectively providing a holistic approach to cybersecurity throughout the enterprise. Strata™ is our network security platform that simplifies operations, consistently enforces security policies, and protects against advanced threats with one unified platform. Prisma® Cloud is our Code to Cloud™ platform that secures apps from design to runtime. Cortex® is our AI-driven SecOps platform that accelerates detection and remediation of security threats. These deliver purpose-engineered solutions that help customers radically simplify their cybersecurity operations and increase their cybersecurity outcomes.

In each area, Palo Alto Networks has consolidated numerous standalone security tools with a single tightly integrated architecture that is built to automate, streamline, and improve cybersecurity operations. And since we know not everything happens at once, the platforms are built modularly, allowing you to adopt components over time, instead of all at once; and you have a wide range of integrations with other products you may be using in your security infrastructure. This commitment to platformization follows more than a decade of work with AI and machine learning to make cybersecurity more intelligent, more automated, and more contextually aware. This lets you have it all without compromise.

Getting to platformization fast is both an operational and a commercial challenge. Palo Alto Networks brings to bear its deep bench of technical talent and customer consultants to help orchestrate platformization in real-world settings while also creating the right economic package to turn platformization into fast ROI and low total cost of ownership. Now, powered by Precision AI, the Palo Alto Networks platform approach to cybersecurity helps organizations thwart attackers' use of AI while mitigating the impacts of architectural complexity and the yawning skills gap.

A wide range of Palo Alto Networks customers has reaped the security, operational, financial, and management benefits of a platform approach, often enjoying many financial benefits in the process, such as rapid return on investment, substantially reduced total cost of ownership, and lower procurement costs.

Palo Alto Networks professionals are ready and able to help any organization—including those working with other cybersecurity technology vendors—find tangible ways to benefit from platformization and the power of Precision AI. ◆

[1] Gruber, Dave and Bill Lundell. *Generative AI for Cybersecurity: An Optimistic but Uncertain Future*, Enterprise Strategy Group, April 2024.

[2] Ibid.

[3] "Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022," Gartner, September 13, 2022.

2025 Predictions — How One Year Will Redefine the Cybersecurity Industry

BY NIR ZUK

The cybersecurity industry will experience tectonic shifts in 2025, unlike any we've seen in years past. These historic transformations will see the convergence of AI, data and platform unification, altogether changing how both cybersecurity defenders and attackers will operate and innovate. Shifts such as these won't just be a series of isolated advances. They will be a reimagining of what security means in an increasingly digital world and will assuredly call for businesses to rethink fundamental strategies. Organizations must be diligent and deliberate when preparing for these changes. These predictions act as a harbinger for a future where unified security platforms, transparent AI and cross-functional alliances are not only advantageous but essential for long-term resilience and trust.

Traditional, siloed cybersecurity systems can no longer keep pace with the sophistication and frequency of modern threats. In response, businesses must move toward a single unified data security platform. This shift toward platformization will be about more than efficiency; it will establish a comprehensive security posture that adapts to evolving threats and supports business growth.

In the race for AI superiority, data is the fuel that powers effective, adaptive models. Larger, established organizations already positioned with massive datasets hold a significant advantage — they can train AI models at scale, creating a feedback loop that continuously strengthens defenses. This advantage will only widen as data-centric models outpace competitors, especially new entrants. However, we can also expect industry incumbents to collaborate with emerging startups, combining extensive datasets with innovative techniques. With this in mind, for AI to garner user trust, especially in the absence of global AI frameworks, organizations ›› will need to demonstrate transparency in how AI models make decisions and manage data. This will undoubtedly set a new standard for accountability and brand loyalty across the industry.

Consequently, with these AI workloads expanding, the industry will face another pressing challenge — energy consumption. Currently, data centers consume around 4% of U.S. electricity,[1] with projections estimating that the figure could more than double by 2030. To meet these rising demands sustainably, businesses must adopt energy-smart strategies, including AI-driven cooling technologies, quantum-based AI frameworks, and unified security platforms that eliminate redundant processes. Ensuring AI's growth aligns with a resilient future will not only require securing data centers but also prioritizing energy grid modernization, paving the way for a sustainable AI-driven world.

The shift toward AI-led SOC operations introduces another vital dimension — trust. While AI will manage core tasks, like vulnerability scanning and threat detection, human analysts will shift their focus to high-level strategy and decision-making. This approach emphasizes the need for transparency around AI models, data collection and decision-making processes. As regulatory frameworks tighten worldwide, establishing robust governance structures (including AI councils) will be crucial for aligning with compliance standards and fostering trust among customers and stakeholders.

Quantum computing's future holds both transformative potential and profound risks. Although quantum attacks on current encryption systems aren't yet viable, the push for quantum supremacy is accelerating. State-backed adversaries are employing a "harvest now, decrypt later" strategy — capturing encrypted data now to decrypt it once quantum technology matures. This looming risk to government secrets, intellectual property and military communications raises the stakes for today's organizations. A proactive, quantum-resistant roadmap is crucial, starting with adopting quantum-safe algorithms, advanced cryptographic libraries and quantum key distribution (QKD). As the National Institute of Standards and Technology (NIST) finalizes post-quantum cryptography standards, leaders must act strategically, balancing the possibilities of quantum advancements with robust defenses that protect sensitive data, ensuring they are prepared for a quantum-enabled world.

The adoption of dedicated, enterprise-grade web browsers will be another forward-thinking step for organizations in 2025. Traditional consumer browsers are often vulnerable to phishing, malware and data breaches. With over 95% of organizations reporting security incidents that originate from the browser across all devices,[2] companies must provide employees with secure, purpose-built browsing environments. Gartner predicts that, by 2030, enterprise browsers will be foundational for delivering secure, digital work experiences,[3] which is essential to building resilient, frontline defenses that support seamless collaboration across distributed workforces.

As data increasingly drives both security and customer engagement, the roles of the CIO and CMO will become more interdependent, with the CIO and CMO aligning efforts to leverage data and AI for secure, personalized customer experiences. The CIO's focus on data governance and AI transparency, coupled with the CMO's commitment to ethical AI in customer interactions, will be crucial for safeguarding trust and ensuring compliance. This collaboration positions companies not only as leaders in security but also as innovators in delivering data-driven customer experiences responsibly.

Ultimately, these shifts signal a future where organizations that lead with a unified, transparent and collaborative approach will set the pace in cybersecurity. For businesses, embracing this transformation isn't just about staying secure; it's about building resilience, fostering customer trust and gaining an edge in a rapidly evolving digital world. Together, these predictions underscore the new pillars of cybersecurity — platform unity, data transparency and strategic partnerships — that will define success in 2025 and beyond. ◆

Discover what Palo Alto Networks leaders had to say about AI and cybersecurity in 2025.

[1] *Powering Intelligence: Analyzing Artificial Intelligence and Data Center Energy Consumption*, EPRI, 28 May 2024.

[2] "Embrace the Browser-Driven Workspace." Palo Alto Networks, 9 February 2025.

[3] Ayoub, Dan, et al. "Emerging Tech: Security — The Future of Enterprise Browsers." Palo Alto Networks, Gartner, 14 April 2023.

Staying Ahead of Evolving Cyberthreats: A CIO's Perspective

BY MEERAH RAJAVEL

Cybersecurity defense has become the new, modern-day battlefield. What once were isolated attacks by hobbyist hackers have evolved into sophisticated operations, often backed by nation-states or organized crime syndicates. For CIOs, the challenge is no longer just about defending against a singular cyberthreat — it's about protecting an increasingly interconnected, digital-first world where everything from customer data to intellectual property is at constant risk.

Consequently, the urgency for robust cybersecurity strategies has never been greater. By 2025, cybercrime is expected to cost the global economy $10.5 trillion annually,[1] and we're already seeing ransomware, phishing, and AI-driven attacks growing at exponential rates. With threats this diverse, businesses can no longer rely on legacy defense systems and reactive security practices. Two emerging strategies — Precision AI and platformization — will have to lead the charge when redefining the way businesses protect themselves.

The Evolution of Cyberthreats: New Challenges for CIOs

In the early days, cyberattacks were often limited to viruses or simple malware delivered via email attachments or downloads. But as digital transformation accelerated and the attack surface expanded, so too did the complexity of these threats. Yes, attackers are increasingly leveraging AI to automate threats and identify vulnerabilities faster — but defenders have the same tools at their disposal. With the right strategy, security leaders can turn AI from a challenge into a powerful force multiplier, strengthening resilience and staying ahead of emerging threats.

AI's integration into cybercrime dates back to the early 2010s, when basic AI models were first used for automating phishing campaigns. These attacks have since grown in sophistication. Attackers now deploy AI-generated deepfakes, automated credential stuffing, and even AI-designed malware to outmaneuver traditional defenses. Cybercriminals have become particularly adept at using AI to amplify the scale and speed of their efforts, often extracting vast amounts of data in record time. A recent example is the Muddled Libra group, which deployed AI-generated deepfakes to deceive internal systems and infiltrate sensitive networks.

For CIOs, these developments have resulted in a host of new pain points:

- **Growing attack surfaces**: With the rise of cloud, edge computing, and IoT, organizations now face an exponentially larger digital footprint to protect. Every new device or cloud service becomes a potential target for attackers using AI to search for vulnerabilities.
- **Talent shortages**: The cybersecurity skills gap is well documented. Over 4 million cybersecurity positions remain unfilled worldwide, creating a shortage of expertise that makes defending against increasingly sophisticated AI-driven threats even harder.
- **Operational overload**: Today's security operations centers (SOCs) are bombarded by thousands of alerts daily, many of which are false positives. AI can increase both the volume and complexity of these threats, overwhelming traditional systems and causing alert fatigue within security teams.
- **Fragmented security systems**: Many organizations rely on disparate security tools that do not integrate well with one another, creating dangerous blind spots where AI-driven attacks can slip through unnoticed.

Harnessing the Next Frontier in Cybersecurity

To combat these challenges, Precision AI is rapidly becoming a vital component in modern cybersecurity defenses. AI isn't just a threat — it's also a critical tool for defense. By using machine learning and advanced analytics, Precision AI can identify and neutralize emerging threats faster and more accurately than traditional methods.

In our Cortex XSIAM platform, for instance, AI-driven threat detection allows organizations to process millions of security events in real time, filtering out noise and focusing on the true anomalies that pose the greatest risk. AI has also revolutionized threat hunting, enabling SOC teams to shift from reactive defense to proactive threat detection. ››

The future of cybersecurity is being shaped by AI.

One of the most important advantages of Precision AI is its ability to significantly reduce false positives. A common pain point for SOC teams is the deluge of low-priority alerts, which drain resources and can lead to critical threats being missed. Precision AI helps streamline this process by learning from the data and optimizing alert prioritization, allowing teams to focus on what truly matters.

Moreover, AI's ability to predict potential attack scenarios adds a powerful layer of foresight to cybersecurity strategies. This is essential in a world where attacks are becoming increasingly AI-driven. By adopting AI-powered defense strategies, organizations can counter attackers with the same tools being used against them.

Breaking Down the Silos

A major challenge for CIOs is the fragmentation of their security tools. Too often, security systems operate in silos, with little communication between various layers of defense. This not only creates inefficiencies but also leaves organizations vulnerable to multivector attacks, where cybercriminals exploit the gaps between systems.

Platformization solves this by consolidating multiple security tools into a unified platform. At Palo Alto Networks, we've seen significant success with our own platforms — Strata Network Security, Prisma Cloud, and Cortex XDR — which integrate security across cloud, on-premises, and edge environments. By providing end-to-end visibility, platformization enables real-time threat detection and response, eliminating the gaps attackers frequently exploit.

For example, one particular global retailer that implemented an AI-driven platform approach reduced their incident response times by 60%. This reduction allowed them to quickly neutralize threats before they escalated into larger problems. Similarly, a healthcare organization saw a 35% decrease in false positives, freeing up SOC analysts to focus on critical issues rather than sifting through low-priority alerts.

Cross-Functional Collaboration: The Key to Success

In past discussions, we've often emphasized the fight against AI-driven threats isn't just a technology issue — it requires cross-functional collaboration between security, technology, and business teams. For CIOs, aligning these groups is essential for ensuring security strategies not only protect the organization but also enable innovation.

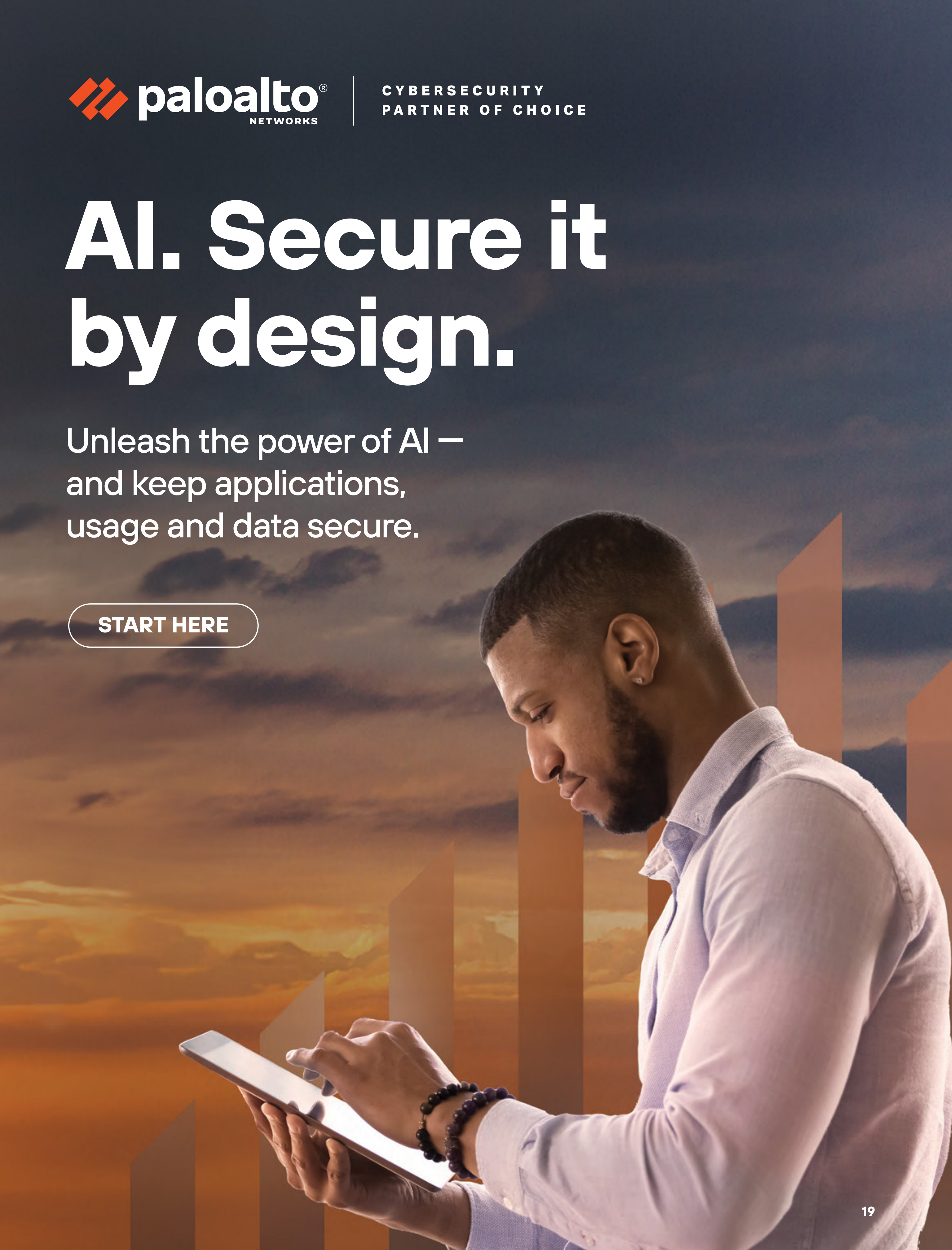
One lesson we've learned is integrating AI into the broader enterprise security framework must be a team effort. By bringing together IT, security, and business stakeholders, organizations can better balance innovation and security — allowing AI to serve both as a defense mechanism and a tool for driving business outcomes.

The Path Forward for CIOs

The future of cybersecurity is being shaped by AI. The question for CIOs isn't whether to adopt AI-driven solutions but how to do so in a way that balances innovation and security. With Precision AI and platformization, CIOs have powerful tools at their disposal to combat increasingly sophisticated threats, improve operational efficiency, and enhance overall resilience.

However, success will also depend on cross-functional collaboration and the ability to stay ahead of both attackers and technological advancements. As AI continues to evolve, so too must our defense strategies — allowing us not just to react to threats but to anticipate them. ◆

1. "Cybercrime to Cost the World $10.5 Trillion Annually by 2025," *Cybercrime Magazine*, Cybersecurity Ventures, 13 November 2020.



Your Cybersecurity Strategies Need to Change: How Can AI Play a Role?

BY ANAND OSWAL

Artificial intelligence has become a defining force in reshaping industries, from healthcare to finance to logistics. But perhaps nowhere is AI's transformative potential — and its inherent peril — more apparent than in the field of cybersecurity. It is here that AI has emerged as both a shield and a sword in the silent but unrelenting war against cyber adversaries.

Yet, as organizations rush to embrace AI as the cornerstone of their cybersecurity strategies, a critical question looms: Are we truly ready to harness its power effectively, or are we inadvertently creating vulnerabilities as quickly as we close them?

A New Arsenal for Defenders

AI's capabilities are breathtaking in their speed and precision. Generative AI (GenAI) models, once praised for their ability to create human-like text, are now integral to threat detection, quickly analyzing oceans of data to flag suspicious behavior.[1] Predictive AI, with its knack for identifying patterns, scans the horizon for potential vulnerabilities, while causal AI examines the interplay of factors that might indicate a brewing threat.

At Palo Alto Networks, we've developed Precision AI, a sophisticated proprietary system that blends multiple forms of GenAI, machine learning, and deep learning. Precision AI predicts and blocks attacks in real time, evolving alongside adversaries. It is a solution that promises not just to defend but to preempt — an essential capability in a world where the velocity of threats is matched only by their variety.

For CISOs and cybersecurity teams, these tools are a lifeline. Faced with growing attack surfaces and limited resources, AI offers a way to extend their reach, automate repetitive tasks, and focus on

››

high-priority threats. It's a force multiplier for overtaxed teams, capable of addressing the challenges of alert fatigue and integrating seamlessly into broader cybersecurity platforms.

But even as defenders celebrate these advances, adversaries are not sitting idle. They, too, have access to many of these same technologies — often at shockingly low costs.

AI in the Hands of Adversaries

On the dark web, the democratization of AI has given cybercriminals a new arsenal. It is now routine for attackers to deploy AI to probe defenses, exploit vulnerabilities, and embed sophisticated exploits that evade detection for weeks. The tools once reserved for innovators and well-funded nation-state actors are now being wielded by even novice bad actors, who use GenAI to craft convincing phishing campaigns or create deepfakes that mimic corporate executives.

The numbers are sobering. According to Gartner, AI-driven malicious attacks ranked as the top emerging risk for three consecutive quarters in 2024.[2] Meanwhile, 57% of cybersecurity professionals believe adversaries already have an edge in leveraging AI to their advantage.[3]

This stark reality raises an uncomfortable truth: The same technology that fortifies defenses also accelerates attacks. The race is no longer about who can build the better firewall, but who can outthink and outpace their opponent in an escalating game of digital chess.

Strategic Implications for Organizations

For organizations, the implications are clear. AI cannot remain an isolated tool or a standalone product; it must become a foundational element of cybersecurity strategy. And that strategy must shift from responsive to proactive — a change in mindset as much as in methodology.

To achieve this, organizations need to confront several challenges:

1. **Targeted Investment over Spending Sprees**

   The solution isn't simply to throw money at AI tools. Instead, organizations must focus on investments that directly counter adversaries' tactics, such as adopting Zero Trust models, fortifying infrastructure, and bolstering security with cloud-delivered security services.

2. **Integration, Not Isolation**

   AI's potential is maximized when integrated into broader cybersecurity platforms that simplify and unify defenses. As cybersecurity grows more complex, platformization becomes essential to reduce risk, improve efficiency, and achieve better security outcomes.

3. **Operationalizing AI for Real-Time Resilience**

   AI must move beyond theoretical potential and become an operationalized component of daily cybersecurity workflows. This includes automating threat detection, response, and remediation while aligning AI-driven insights with business continuity plans.

How Do We Win?

The future of cybersecurity will not be won by those who simply adopt AI, but by those who embed it into their core strategy. And the urgency to do this has never been greater. In a world where adversaries evolve at the speed of innovation, complacency is not an option.

AI's greatest strength lies in its duality. It is capable of uncovering vulnerabilities and preempting threats with unprecedented precision. As defenders race to integrate AI into their strategies, adversaries are wielding it just as effectively. The organizations that succeed in this digital arms race will be those that view AI not as a tool but as a unifying force across their security platforms, business practices, and leadership priorities.

Therefore, this action calls for more than investment; it demands a bold and provocative vision. Boards and executives must champion AI as a cornerstone of their cybersecurity strategies, ensuring it is seamlessly integrated into the fabric of the organization. The goal is not just to mitigate risk but to ensure adaptability as the ultimate defense. ◆

[1] *Generative AI in Cybersecurity: An Optimistic but Uncertain Future*," Enterprise Strategy Group, April 2024.

[2] "Gartner Survey Shows AI-Enhanced Malicious Attacks as Top Emerging Risk for Enterprises for Third Consecutive Quarter," Gartner, November 2024.

[3] *The Life and Times of Cybersecurity Professionals Volume VII*, Enterprise Strategy Group, November 2024.

The Future of AI in Cybersecurity in a Word: Optimistic

BY RICH CAMPAGNA

When we assess the state of artificial intelligence (AI) in cybersecurity, it's a dynamic mix of opportunity and challenge. Most of us can agree, AI is undeniably reshaping cybersecurity — offering transformative potential for both defenders and attackers. On the one hand, AI empowers cybersecurity teams to automate threat detection, accelerate responses, and deploy adaptive security frameworks at unprecedented speeds. On the other hand, adversaries are leveraging AI, creating a continuous tug-of-war between innovation and exploitation.

Despite the challenges, though, the future of AI in cybersecurity remains optimistic. As organizations (and vendors) become more adept at integrating AI into their security strategies, they are poised to outpace emerging threats and protect critical infrastructure more effectively than ever before. The progress being made is not only promising but will be a key factor in securing the digital landscape of tomorrow.

What's Been Done?

While generative AI (GenAI) and tools like ChatGPT ushered AI into the mainstream, AI has been in widespread use in cybersecurity for over a decade. While AI isn't a new phenomenon, its application in cybersecurity has advanced significantly in recent years. It has become a critical element in both proactive defenses and reactive strategies against attackers who also use AI. Today's cybersecurity frameworks are designed with AI at their core, helping organizations detect, respond to, and mitigate threats more effectively and more efficiently. This technology is already having a profound impact on threat detection, making it more contextually aware and precise.

A key development has been the global recognition that AI requires substantial resource commitments. Projections show global spending on AI-driven cybersecurity solutions will surge to $135 ›› billion by 2030.[1] This illustrates a growing consensus that AI is no longer optional; it's essential for defending digital infrastructure across industries and geographies. The increase in global spending signals a broader shift in the cybersecurity landscape, where AI's goal is no longer about catching up to attackers — it's about outpacing them.

GenAI, specifically, has become a game changer in cybersecurity. Its ability to automate previously manual tasks as well as make it simple and easy to both gain targeted visibility and administer security platforms are allowing experts much-needed time to focus on other high-value activities. The proactive nature of GenAI underscores how cybersecurity is shifting from reactive measures to preparing for threats before they fully emerge.

Moreover, AI has significantly enhanced cybersecurity workflows by automating repetitive tasks like threat monitoring, alert triage, and malware analysis. This automation is especially valuable in an era when the demand for cybersecurity talent exceeds supply, enabling AI to handle routine operations while freeing human professionals to focus on more strategic efforts.

In threat intelligence, AI has made it harder for hackers to mask their actions, detecting patterns and signals far more quickly than traditional methods. This shift to real-time, data-driven intelligence is essential to staying ahead of adversaries who continually innovate new ways to breach systems.

Organizations are also leveraging AI to secure operational technology (OT) environments — critical infrastructure such as power grids and healthcare systems. Research from Palo Alto Networks shows that 3 out of 4 organizations have experienced cyberattacks targeting OT environments,[2] underscoring the need for advanced AI protections. The integration of AI across critical systems highlights the growing recognition of its necessity, especially in high-risk sectors.

As AI continues to evolve, its role in cybersecurity will only grow. The challenge moving forward is how to best pair AI's capabilities with human expertise, allowing organizations to stay agile in the face of increasingly sophisticated threats.

What's Likely to Be Done Soon?

The most exciting aspect of AI in cybersecurity isn't just what it has already achieved — it's what's coming next. As AI continues to evolve, it will enable organizations to bolster their defenses even further, empowering them to stay ahead of attackers. And with the rise of agentic AI, the role of humans in cybersecurity will become more and more strategic, with tactical everyday administration becoming increasingly automated. While adversaries will no doubt try to exploit new AI capabilities, defenders are already investing heavily in optimizing AI's role in cybersecurity.

One area where AI will become increasingly pivotal is **edge computing**, particularly in environments where the internet of things (IoT) plays a central role. With more devices and data sources contributing to edge environments, securing these distributed systems presents unique challenges. AI's ability to process and analyze data in real time will be critical to detecting and mitigating threats in these scenarios. As the National Institutes of Health has noted, "AI-efficient machine learning and deep learning solutions are necessary for next-generation IoT systems to maintain up-to-date and adaptive security systems."[3] This underscores AI's essential role in evolving IoT security.

Another key use case for AI in the near future is **data privacy**. As regulatory frameworks grow stricter, AI will be vital in balancing data access with privacy protection. Technologies like **differential privacy** and **federated learning** will allow AI to analyze massive datasets while safeguarding personally identifiable information (PII). These AI-driven privacy solutions will be crucial as organizations navigate the challenge of working with larger, more diverse datasets without compromising data security.

AI is also expected to revolutionize several other areas of cybersecurity:

- **AI-First Security Operations Centers (SOCs)**: With a shortage of skilled security engineers, AI will step in to automate threat detection and response, enabling SOCs to become more intelligent and contextually aware. The future "SOC of the Future" will rely heavily on AI to manage the growing volume of threats while maintaining agility. ››

- **Phishing and Business Email Compromise (BEC) Defense**: Given that email remains a primary attack vector, AI will enhance defenses against phishing and BEC attacks. AI's ability to analyze communication patterns in real time will help organizations stay ahead of increasingly sophisticated email-based threats.
- **Enhanced Data Insights**: AI will take analytics to the next level. As the conversation around big data evolves, AI-driven analytics will provide more actionable insights, allowing organizations to make data-driven decisions with greater precision.
- **Simplification of IT and SecOps Architecture**: As cybersecurity infrastructures grow more complex, AI will help simplify workflows by creating a more platform-centric approach to cybersecurity. This integration will reduce operational complexity and improve security effectiveness.
- **Network Security**: As networks become even more interconnected and mission-critical, AI will play a key role in securing any user, on any device, no matter where they may be accessing the network. AI-driven solutions will detect vulnerabilities, prevent lateral movement, and respond to infiltration attempts in real time.

These advancements reflect a paradigm shift in cybersecurity — from reactive to predictive, from manual to automated, and from fragmented to integrated. The real opportunity lies in how organizations will pair AI's capabilities with human expertise to not only defend against emerging threats but also transform how cybersecurity is executed.

Things to Watch Out For

As AI advances in cybersecurity, one of the biggest risks organizations face is complacency. While it's easy for CIOs, CISOs, and other C-suite and board leaders to be reassured by AI's incredible results, they must remember cyber adversaries are constantly evolving. A recent report revealed many organizations experienced breaches after believing their AI-powered defenses were impenetrable. The bad actors only need to succeed once; they are smart, resourceful, and increasingly collaborative through dark web forums and other underground channels.

> As AI advances in cybersecurity, one of the biggest risks organizations face is complacency.

Organizations must stay on guard, continuously refining their AI strategies to stay ahead. Additionally, governance, risk, and compliance (GRC) concerns should remain top of mind as AI continues to be integrated into security operations. Regulatory pressures from consumer groups and legislators are increasing, especially as AI's role in handling personal and private data grows. Technologies such as differential privacy and federated learning help mitigate these risks, but companies must remain vigilant about legal and ethical issues. With new regulations emerging, such as expanded privacy laws under GDPR and CCPA, and case law continuing to evolve, organizations must ensure their AI deployment is compliant and future-proofed.

What You Can Do Right Now

To make the most of AI in cybersecurity, here are a few actionable steps organizations should consider:

1. **Integrate AI Across the Cybersecurity Ecosystem**: AI shouldn't exist in a silo within the cybersecurity function. Instead, it needs to be embedded in networks, security infrastructure, workflows, and policies. Appointing a singular "AI cybersecurity czar" limits AI's potential. Instead, every member of the cybersecurity team should treat AI as a core competency, fostering a collective understanding and engagement with the technology. ››

2. **Training AI with Comprehensive Threat Data**: The effectiveness of AI in cybersecurity hinges on the quality and breadth of data used to train its models. Generic or narrowly scoped datasets fail to capture the dynamic complexity of today's threat landscape, limiting AI's ability to anticipate and neutralize evolving attacks. By leveraging vast, real-world datasets that reflect diverse attack vectors and adversary behaviors, organizations can arm their AI systems with sharper predictive and defensive capabilities. Precision AI exemplifies this approach, integrating global threat intelligence to not only detect but preemptively block advanced threats — setting a new benchmark for adaptive and comprehensive cybersecurity solutions.
3. **Stay Informed and Proactive About AI Developments**: The AI landscape is evolving at a rapid pace, with new developments emerging in best practices, responsible use, regulatory frameworks, and threat detection techniques. Staying up to date on these trends is essential. Regularly engage with industry reports, attend webinars, and participate in AI-driven cybersecurity communities to ensure your team is continuously learning and adapting.

Ultimately, the future of AI in cybersecurity is one of optimism. As this powerful technology continues to evolve, it offers organizations the tools to stay ahead of emerging threats and fortify their defenses. However, with this potential comes responsibility. By embedding AI into every layer of security, and staying informed about the latest developments, organizations can fully unlock AI's potential to transform how we defend against an ever-evolving threat landscape.

The fight isn't over, but with AI in the mix, the outlook is certainly brighter. ◆

1. "AI and Cybersecurity: A New Era." Morgan Stanley, Sept. 11, 2024.
2. *The State of OT Security: A Comprehensive Guide to Trends, Risks, and Cyber Resilience*. ABI Research and Palo Alto Networks, March 21, 2024.
3. Mazhar, Tehseen et al., "Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence," *Brain Sciences*, 13, no. 4: 683.

Deliver Innovation to Fight AI with AI

How to Radically Simplify Cybersecurity

BY NAVNEET SINGH

Cybersecurity has always been a game of chess: strategic, layered, and endlessly complex. But, in recent years, the board has seemingly changed: defenders now have the opportunity to shift from playing defense to setting the pace. Artificial intelligence (AI) is one tool reshaping the landscape, a powerful force for transformation. With the right approach, AI can do more than counter threats — it can simplify security, accelerate response times, and unlock new levels of resilience.

AI is the key to a future where cybersecurity is proactive, precise, and intuitive. The challenges ahead are significant, yes, but so is the potential to reinvent how we defend businesses, data, and digital ecosystems. Embracing AI as a strategic imperative will enable organizations to stay ahead of evolving threats while simultaneously redefining what's possible in cybersecurity.

The Tyranny of Complexity

Ask any cybersecurity professional about their biggest challenge, and one answer comes up time and again: complexity. And there are no two ways about it, complexity kills. It doesn't just kill productivity or budgets; it kills security itself. The average enterprise, for example, manages an average of 83 security products,[1] sourced from countless vendors, layered atop multicloud infrastructures. Each tool solves a specific problem, but together they create a fragmented, inefficient defense system. This patchwork approach breeds blind spots — exactly what attackers love to exploit. Attackers thrive in environments where defenders can't connect the dots fast enough. They exploit the gaps created by siloed tools and overwhelmed teams, launching coordinated assaults that outpace detection and response. And in a world where threats move at machine speed, every second counts.

To understand the stakes, consider the infamous Log4J vulnerability. When it was discovered, security teams worldwide scrambled to assess their exposure. The traditional response? Weeks of manual investigation, countless Slack messages, and phone calls to product teams. The result? Frustration, delays, and missed opportunities to prevent exploitation.

This is the old model of cybersecurity — reactive, fragmented, and slow. It's also unsustainable. If complexity is the enemy, simplification is the solution.

Rewriting the Rules with AI

But the question remains: How? Yes, AI represents a seismic shift in how we approach cybersecurity. It doesn't just detect threats; it anticipates them. But that's only half the battle. There needs to be a symbiotic relationship between AI and the analysts.

AI-powered solutions like Palo Alto Networks Copilots transform security operations by analyzing vast datasets in real time, uncovering patterns invisible to human analysts.

Let's look at the Log4J example again. With AI, the process of identifying affected systems and taking corrective action wouldn't have been a weeks-long ordeal. Now, security teams can query an AI-powered platform using natural language: "Show me all instances of Log4J running in our environment." The response is immediate, precise, and actionable.

Speed, though, is only part of the equation. The true power of AI lies in its ability to simplify complexity. Instead of writing intricate SQL queries or navigating countless dashboards, analysts can interact conversationally with their systems. Follow-up questions, enriched data, and automated actions become part of a seamless workflow. It's a transformation that turns a daunting haystack into a manageable thread.

AI also enables organizations to preempt attacks by identifying vulnerabilities before adversaries can exploit them. This proactive capability is crucial in a world where the next breach could emerge from anywhere.

The Cold War of Our Time — but with a Twist

The rise of AI has ignited a new arms race, one that recalls the geopolitical tensions of the Cold War, but with a digital battlefield where lines are blurred and adversaries are unseen. And while the geopolitical arms race of the mid-20th century was defined by physical weapons and territory, today's adversaries ›› fight for dominance in the digital realm, where disruption can ripple across borders in seconds.

In every era of innovation, from the space race to the rise of the internet, progress has belonged to those who harnessed technology to drive new possibilities. Cybersecurity today is no different. The future belongs to defenders who don't just react but anticipate — leveraging AI to stay ahead of the curve. Intelligent, by-design security solutions have the power to outpace adversaries, safeguard innovation, and build a digital world where organizations thrive with confidence. History, time and time again, reminds us that those who embrace technological advancements don't just survive — they lead the charge.

This digital arms race, though, has its own unique twist: AI has obliterated traditional constraints on resources and scale. Attackers no longer need massive teams or endless hours. AI enables them to launch simultaneous phishing campaigns, weaponize deepfakes, and tailor malware to specific environments — all at speeds humans simply can't match. A single actor can now target hundreds of organizations simultaneously with precision and persistence that would've been unthinkable just a decade ago.

For defenders, this is a wake-up call. To stand still is to surrender. And yet, unlike the attackers who operate without ethical boundaries, defenders must innovate responsibly, adhering to principles of accountability, fairness, and transparency. The challenge is not merely to react but to anticipate, to build systems that evolve and adapt as threats emerge.

Imagine a cascade of breaches orchestrated with precision, shielded by deepfake communications and AI-generated disinformation. The response cannot be manual or delayed. It must be instantaneous, cohesive, and intelligent — an orchestra of AI-powered tools acting in harmony to detect, neutralize, and prevent further escalation.

This is the defining tension of our era: the dual role of AI as both a weapon and a shield. To succeed, defenders must adopt a wartime mentality — not just deploying technology but fostering the collaborative spirit that defined Cold War innovation. Industries, governments, and organizations must unite, sharing intelligence and aligning strategies to create a unified front against adversaries who thrive on division.

> The fight against AI-driven cyberthreats is a defining challenge of our era. It demands urgency, collaboration, and above all, innovation.

Another lesson history teaches us is that moments of technological upheaval are also moments of opportunity. Just as the Cold War spurred advancements that reshaped the modern world, the AI arms race offers the chance to revolutionize cybersecurity. But the clock is ticking, and the digital battlefield waits for no one. Will defenders rise to the challenge, or will innovation remain a weapon wielded only by those with malicious intent?

The Human Element in AI Defense

Even the most sophisticated AI tools cannot replace the human element. Phishing attacks, social engineering, and identity theft still prey on human error, often exploiting gaps in training and awareness. Organizations must invest in education that extends beyond the security operations center (SOC) to all employees, including those in the C-suite.

AI-driven training platforms can fundamentally reshape how organizations build their first line of defense. These tools generate dynamic simulations tailored to the specific threat landscape of the organization. Instead of static training modules,

››

employees engage in evolving scenarios that mimic real-world attacks. For instance, a phishing simulation can adjust its complexity based on an employee's performance, identifying knowledge gaps and offering targeted feedback in real time.

Beyond simulations, AI can help track and analyze training effectiveness at scale. By evaluating how employees respond to simulated threats, organizations can pinpoint systemic vulnerabilities and tailor training programs to address them. This feedback loop ensures continuous improvement, moving security training from a reactive to a proactive approach.

Importantly, this isn't about replacing human intuition. It's about sharpening it. AI acts as a coach, preparing employees to recognize anomalies and respond with confidence. From junior staff to senior executives, tailored training programs ensure that every individual — regardless of role or technical expertise — is equipped to spot and respond to evolving threats. Alternatively, if organizations treat training as a one-time exercise, they put themselves at risk. Training must be a continuous, adaptive process, evolving as quickly as the threats it seeks to combat.

A Vision for the Future

The fight against AI-driven cyberthreats is a defining challenge of our era. It demands urgency, collaboration, and above all, innovation. By leveraging AI to fight AI, we can simplify the complex, stay ahead of adversaries, and build a secure digital future. ◆

[1] "IBM IBV Study on Platforms." *Palo Alto Networks and IBM Institute for Business Value*, 28 January 2025.

Mastering the Basics Cyber Hygiene and Risk Management

BY DAN FORD

Cybersecurity is a journey, not a destination. This mantra has defined much of my career and guides how I approach the challenges of protecting people and organizations in an increasingly digital world. Cybersecurity continues to evolve — I've watched the immense transformation over the years — and there has always remained one constant: the basics matter.

When I first entered this field, the threats seemed more localized. Early on, I was captivated by the technical intricacies of securing systems and understanding how they could be broken. But during my time with Homeland Security, my perspective shifted. Cybersecurity became more than a technical challenge, and the stakes were no longer hypothetical or small in scale. Threats became global, and the risks became devastating. It was clear to me then, as it is now, that a solid foundation in cyber hygiene is critical for building resilience.

What Cyber Hygiene Means to Me

Think of cyber hygiene the way you think of personal hygiene. Each day, you follow a routine: brushing your teeth, taking a shower, using deodorant — basic but essential tasks to ensure your health and well-being. Cyber hygiene is no different. It's about the routine practices and habits that protect your digital assets and identity. For individuals, this might mean using strong passwords or enabling multifactor authentication (MFA). For organizations, it's about maintaining system updates, managing access controls, and having clear protocols in place.

At Jovia, we've embraced the idea that financial literacy and cyber literacy are two sides of the same coin. In today's world, your assets aren't just in a wallet; they're in digital transactions, Venmo payments, and Zelle transfers. Unfortunately, these conveniences come with risks, and I've seen far too many people lose their life savings because they didn't understand the basics of protecting themselves online. Educating our members — and the communities we serve — on cyber hygiene is one of the most impactful ways we can make a difference.

Building Resilience Through Cyber Hygiene

When it comes to organizations, effective cyber hygiene boils down to a few key principles:

1. **Adopt Multifactor Authentication Everywhere**

   MFA is one of the simplest and most effective defenses against unauthorized access. Yet, I'm constantly amazed by how often it's overlooked. If MFA is available, use it — whether for personal accounts like Facebook or for critical systems at your organization.

2. **Use Password Managers**

   Strong, unique passwords for every account are non-negotiable in today's threat landscape. A password manager not only simplifies this task but ensures you're not reusing credentials — a common vulnerability that attackers exploit.

3. **Tighten Email Security**

   Emails remain one of the primary entry points for attackers. Web gateways and link-checking tools can help, but the goal should be to eliminate risky links from ever reaching users. Teaching employees to avoid clicking on email links isn't enough; organizations need systems that proactively mitigate these risks.

4. **Emphasize Routine Maintenance**

   Just as you wouldn't skip a doctor's appointment, you shouldn't ignore regular system updates. Vulnerabilities are patched constantly, and staying up to date is essential for keeping adversaries at bay. ››

Facing the Inevitable

Despite our best efforts, breaches happen. I've said for years the question isn't whether your organization will be attacked but how quickly you can detect and contain it. It can take several days to detect and respond to an intrusion, sometimes weeks. That's unacceptable. At Jovia, we aim to identify threats in hours — not weeks or months — and contain them before they escalate.

This proactive mindset stems from what I call "changing the rules" of cybersecurity. In the same way Captain Kirk refused to accept the unwinnable Kobayashi Maru scenario, cybersecurity teams must redefine success. It's not about preventing every attack — that's impossible. It's about minimizing the impact, reducing the time to detection, and responding decisively.

A Call for Greater Transparency

One of my biggest frustrations in this field is the lack of transparency when breaches occur. Too often, organizations handle incidents quietly, under the shadow of legal concerns, which means we, as an industry, fail to learn from these events. Imagine if every breach were treated like an airline crash, with thorough investigations and published findings. The lessons we'd gain could help prevent future incidents. Instead, the same mistakes are repeated because we're too hesitant to share what went wrong.

Cybersecurity as a Shared Responsibility

Ultimately, cybersecurity is about collaboration. It's about organizations, vendors, and even customers working together to create a safer digital ecosystem. At Jovia, we integrate third-party risk monitoring and threat intelligence to ensure our vendors meet our security standards. But it's more than that; it's about partnerships. When we hear through our intelligence channels that a vendor is being targeted, we act immediately. We reach out to understand the risks and to support mitigation efforts. That's the kind of proactive, collaborative approach we need across the board.

The battle against cyberthreats can feel overwhelming, but we're not powerless. By mastering the basics of cyber hygiene and adopting a proactive mindset, we can turn the tide. It starts with curiosity — asking questions, challenging assumptions, and staying ahead of adversaries. It grows through collaboration — within organizations, with partners, and across industries. And it's sustained by a commitment to resilience to being better tomorrow than we are today. Cybersecurity may be a journey without a final destination, but it's a journey worth taking. ◆

Everyone's Data Is at Risk: Protecting It Is Much More Than a Compliance Issue

BY HAIDER PASHA

Protecting sensitive, personal, and proprietary data should be at the forefront of every cybersecurity strategy. The consequences of failing to do so can range from damaging to catastrophic — leading to massive fines for regulatory violations and, more importantly, the erosion of customer trust. The lineup of data privacy regulations is long and complex, and it seems to expand every time a new breach occurs.

However, while compliance with regulations like the General Data Protection Regulation (GDPR), Network and Information Systems Directive 2 (NIS2), or California Consumer Privacy Act (CCPA) is crucial, protecting data is not just about avoiding fines. It's about safeguarding the lifeblood of an organization – its trust, its reputation, and its long-term survival. The real question isn't, "What regulations do we need to comply with?" but rather, "Why should data protection be a core strategic priority beyond compliance?"

Today's Big Issues in Data Privacy and Cybersecurity

It's true, when evaluating the state of data privacy and cybersecurity today, regulatory compliance often dominates the conversation. Across countries, states, and industries, organizations must navigate an ever-growing array of regulatory mandates to protect data.

For many, compliance starts with regulations like the European Union's GDPR,[1] which has acted as a global blueprint since its implementation in 2018. In the U.S., nearly two dozen states have followed suit with their own regulations, with the CCPA[2] leading the charge. The CCPA's stringent guidelines — paired with hefty fines for violations — highlight how failing to meet compliance can result in brand-damaging publicity. ››

Industry-specific mandates, such as HIPAA for healthcare, add another layer of complexity. To meet these diverse regulations, organizations are spending billions of dollars on cybersecurity tools and services. In fact, research projects the global data privacy software market will skyrocket from $3.8 billion in 2024 to more than $48 billion by 2032, driven by a compound annual growth rate of more than 37%.[3]

While compliance is essential, it's just one piece of the puzzle. Organizations must admit true data protection is about more than avoiding fines and meeting regulatory requirements. It's about safeguarding the core of a business and ensuring long-term success. Several critical factors demonstrate why protecting data is much more than a compliance issue:

- **Operational Resilience**: When personal or sensitive information is compromised, it can halt entire business operations. Whether it's identifying the source of an attack or mitigating its impact, compromised data means downtime — disrupting services for employees, partners, and customers. Protecting data is essential to keeping systems operational and avoiding costly disruptions.
- **Financial Loss**: The financial fallout of a data breach extends far beyond regulatory fines. Organizations face lost revenue from downtime, hefty penalties, and massive costs in addressing the breach. For global businesses operating across multiple jurisdictions, the financial hit from a data privacy breach can be exponentially larger.
- **Reputational Loss**: A data breach can irreparably damage an organization's reputation. As the Federal Trade Commission (FTC) warns, companies that fail to live up to their promises of protecting personal information can face public scrutiny and enforcement actions. No organization wants to make headlines for losing millions of sensitive records — it's a hit to their brand that's hard to recover from.
- **Erosion of Trust**: Trust is one of the most valuable assets an organization has. Whether it's employees whose personally identifiable information (PII) has been exposed or customers whose data has been mishandled, trust can be shattered in an instant. Restoring that confidence can take years and carries significant reputational and financial costs.

While **compliance** is a vital driver of data privacy initiatives, organizations must recognize the true stakes are much higher. Data privacy is about safeguarding business continuity, financial stability, and the trust that underpins an organization's relationship with its customers and employees.

Risks and Vulnerabilities in Data Privacy

Cybercriminals are motivated by a range of factors — financial gain, geopolitical disruption, or simply the thrill of competing with other hackers. Regardless of the reason, they consistently target several familiar vulnerabilities, and each one underscores why protecting data is about more than just adhering to regulations:

- **Weak or Inconsistent Access Controls**: Poorly managed access controls are one of the easiest ways for hackers to gain unauthorized access to sensitive information, such as PII. Stolen or compromised credentials allow attackers to bypass security systems, and even multifactor authentication (MFA) — long considered a security staple — can now be creatively side-stepped. Compliance measures may mandate access controls, but true protection requires continuous monitoring, frequent updates, and a deeper commitment to keeping up with evolving threats. It's not enough to implement controls for the sake of compliance — they must be robust and actively managed to adapt to new attack methods.
- **Ransomware**: Ransomware attacks have become the go-to weapon for cybercriminals, especially in sectors like healthcare, education, and government, where the exposure of sensitive data can lead to significant operational disruptions. These attacks can cripple services, potentially leading to long-term downtime and damage to public trust. While compliance frameworks may dictate baseline defenses, the real risk here is operational resilience. Ransomware attacks remind us that protecting data is about safeguarding the continuity of services and maintaining the trust of stakeholders — two critical factors regulations alone cannot guarantee. ››

- **Phishing and Social Engineering**: Phishing attacks, which often involve highly sophisticated social engineering tactics, are increasingly difficult to detect. Hackers craft emails or messages that mimic trusted brands, tricking users into sharing credentials or clicking malicious links. With business email compromise (BEC) on the rise, organizations must monitor the enormous volumes of email traffic passing through their systems daily. Phishing goes beyond compliance checklists; organizations must implement behavioral analytics and user education to stay ahead of these evolving threats. The human element, often the weakest link, is not something that regulations alone can fix — vigilance and continuous training are essential.
- **Insider Threats**: Insider threats are becoming more frequent as disgruntled employees and contractors retain access to sensitive databases, even after leaving an organization. These actors often exploit their knowledge of a company's systems to steal data or disrupt operations. Compliance might require logging access to systems, but insider threats highlight the need for continuous access audits and stricter policies around data retention. Protecting data means going beyond regulatory measures to ensure people no longer affiliated with the organization can't retain harmful access.
- **Third-Party Vendor Compromise**: As organizations increasingly rely on external vendors, third-party data breaches are on the rise. These vendors often have privileged access to sensitive information, but may not always have strong security practices in place. Protecting data privacy isn't just about what happens inside your organization — it's about the entire ecosystem. Organizations must look beyond their own compliance and assess the security practices of their partners, vendors, and service providers to prevent breaches from occurring outside their direct control. Beyond these common threats, the rise of personal mobile devices used by remote and hybrid workforces presents another significant risk.

> Organizations must prioritize data privacy in cybersecurity for more than just compliance reasons.

Hackers can exploit unsecured devices and home networks, often posing as legitimate users to gain access to organizational systems. Why this matters: With the widespread shift to remote work, relying on compliance regulations isn't enough. Organizations must implement comprehensive mobile device management (MDM) solutions and educate employees on securing their home networks.

Edge computing and the internet of things (IoT) are also expanding the attack surface, as many IoT devices lack strong security measures due to their small size and limited computing power. As IoT adoption accelerates, these devices offer hackers a vulnerable entry point into larger systems. Why this matters: Compliance may address the broader IT infrastructure, but IoT and edge devices demand dedicated security protocols to close the gaps that regulations often overlook. Protecting these endpoints is vital to ensuring overall data security.

Finally, artificial intelligence (AI) is being used by hackers to automate and scale their attacks. From phishing to identity theft, AI-driven attacks are faster, more frequent, and more damaging than ever before. Why this matters: While compliance mandates data protection, they rarely account for the speed and complexity that AI brings to the table. Organizations need to adopt AI-driven defensive measures to counter the rapidly evolving techniques used by attackers. ››

Strategies and Steps All Organizations Need to Ensure Data Privacy in Cybersecurity

Organizations must prioritize data privacy in cybersecurity for more than just compliance reasons — operational resilience, legal obligations, trust, reputation, and employee/customer experience all depend on it. The following steps can help establish a strong foundation for immediate action:

1. **Test, Test, Test**

   Regular data privacy audits and vulnerability assessments should be core to any cybersecurity strategy. While compliance audits are often mandatory, internal audits that assess real-time vulnerabilities and organizational readiness are equally important. Testing ensures systems remain resilient and adaptable to evolving threats.

2. **Encrypt Everything**

   Data — whether in motion or at rest — should always be encrypted, whether it resides in the cloud, on the edge, or in a data center. Backup data must also be encrypted, with encryption key management being precise and consistently applied. Encryption serves as a last line of defense, ensuring data remains secure even if breached.

3. **Establish Robust Policies**

   A strong data privacy framework is essential. Fortunately, you don't have to reinvent the wheel — GDPR, HIPAA, and PCI DSS offer excellent standards. Adopt policies that only collect and store personal data essential for business operations, such as payroll or customer data. Every expansion of access policies increases the risk of a data breach, so maintaining minimal necessary access is critical.

4. **Leverage AI as a Force for Good**

   With the increasing volume and sophistication of attacks, AI should be employed to bolster data privacy defenses. While organizations may struggle to hire enough skilled cybersecurity engineers and SOC analysts, AI is an efficient force multiplier that can automate the identification and mitigation of threats.

Going Beyond the Basics: Additional Steps for Enhanced Data Privacy

In addition to the critical steps above, consider implementing these measures to further strengthen your data privacy strategy:

- **End-User Training**: Human error is the leading cause of data breaches, with employees often unknowingly undermining their own data security. Continuous education and training can help mitigate this risk by raising awareness of phishing, social engineering, and best practices for data handling.
- **Reduce Complexity**: Modernizing aging infrastructure and embracing platformization can help eliminate vulnerabilities caused by overly complex security environments. Simplifying the security stack reduces the attack surface and improves data privacy controls.
- **Identify Rogue IT**: "Rogue IT" occurs when employees or departments introduce unauthorized technology into the organization. This is particularly dangerous when large language models (LLMs) or AI tools are developed and trained using personal or private data without oversight. Conducting audits to locate and address rogue IT initiatives is essential for maintaining control over data privacy.
- **Assign a Data Privacy Officer**: Keeping track of new data privacy threats, regulations, and emerging case law requires constant vigilance. Make data privacy someone's full-time job — appoint a dedicated officer to stay on top of new developments and ensure compliance with evolving regulations.

Finally, keep in mind a key requirement for any organization taking data privacy seriously is to team with a cybersecurity partner that demonstrates a commitment to data privacy beyond the boundaries of regulatory compliance. This must be exemplified in its products, its practices, and its strategic approach to data privacy on all levels. ◆

[1] "What is GDPR, the EU's new data protection law?" GDPR.EU, 2024.

[2] US Data Privacy Guide, *White & Case*, 2024.

[3] "*Data Privacy Software Market Size, Share & Industry Analysis*." Forbes Business Insights, 2024.

10 Cyber Recommendations for the Trump Administration

BY DANIEL KROESE AND SAM KAPLAN

Having served our country in the cyberranks of the first Trump Administration, we know how important it is for the second Trump Administration to hit the ground running in its cyber defense mission. As recent events have reinforced, our cyber adversaries — China, Russia, Iran, North Korea and beyond — aren't sitting on their hands.

We are confident that the incoming national security and cybersecurity team is ready to forcefully counter adversarial cyber activity from foreign nation-states; fight the proliferation of ransomware attacks on critical infrastructure and other U.S. businesses; protect American intellectual property; and embrace AI innovation as a critical enabler of cyber resilience. These are all goals the entire nation can rally around.

Palo Alto Networks is proud to be an integrated national security partner with the Federal Government and stands ready to help. To that end, we have developed 10 recommendations for the incoming team to consider as they take the reins:

1 Focus on cybersecurity *outcomes.*

Are cybersecurity investments actually making networks safer? We've found that two of the most telling indicators of cyber resilience are Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). The President should be able to walk into the White House Situation Room and see real-time MTTD and MTTR metrics for federal agencies.

2 Forcefully respond to Salt Typhoon by promoting a Zero Trust approach to telecommunications security.

This is an evolved security approach with a layered, continuous reverification posture that does not implicitly grant access. It requires end-to-end visibility and an enhanced focus on mobile core and management plane security.

3

Embrace the multicloud reality, but don’t forget about security.

Cloud is becoming the dominant attack surface — in a Unit 42 report,[1] over 80 percent of vulnerabilities observed by our team were cloud-based. The increasing trend of multicloud adoption further challenges the legacy-shared responsibility model for security. In response, we must aggressively promote cross-cutting cloud security tools that provide both visibility and operational control.

4

Leverage AI to avoid an inefficient game of cyber defense whack-a-mole.

Cyber professionals are drowning in alerts that they must manually triage. They need AI-powered tools to flip this paradigm and stay ahead of adversaries, like China. There is a particular opportunity to leverage AI to modernize security operations centers (SOCs), and Palo Alto Networks applauds the recently signed EO on ***Removing Barriers to American Leadership in Artificial Intelligence***[2] as an important validation of AI’s enormous national security potential.

5

Further drive confidence in the extraordinary power of AI by promoting Secure AI by Design.

To fully harness the incredible power of AI, enterprises (including federal agencies) need to enforce access controls, harden deployment environment configurations, and ensure data integrity across AI supply chains.

6

Promote Defense Industrial Base (DIB) resilience.

The DIB is a natural extension of our national security apparatus but is under constant attack by adversaries. In response, we should further expand the scope and scale of the cybersecurity services offered by the NSA Cybersecurity Collaboration Center.

7

Modernize the federal procurement process.

Current procurement cycles don’t operate at the speed of technological innovation, giving adversaries the upper hand. For example, there is far too much reliance on legacy VPN tools (increasingly targeted by adversaries) instead of modern Zero Trust solutions.

8

Make meaningful progress on regulatory harmonization for cybersecurity.

The Federal Government can lead by example by consolidating and streamlining federal government software compliance certifications. For example, there should be logical reciprocity between FedRAMP High and DoD IL-5 certifications.

9 Operationalize the Federal Acquisition Security Council (FASC).

Established during the first Trump Administration, this can be a critical tool to ensure the technology in our federal enterprise is trustworthy with appropriate supply chain integrity.

Protecting our digital way of life is a bipartisan mission that requires all of us working together. As the Trump Administration enters office at this pivotal moment for America's cyber resilience, we look forward to doing our part to help the cause. ◆

[1] *Unit 42 Attack Surface Threat Report 2023*, Palo Alto Networks, 14 September 2023.

[2] "Removing Barriers to American Leadership in Artificial Intelligence." The White House, 23 January 2025.

10 Leverage cyber shared services to increase efficiency and reduce waste.

Shared services offerings for federal agencies can provision cybersecurity capabilities at scale — improving federal cybersecurity outcomes while being prudent stewards of taxpayer dollars.

paloalto® NETWORKS | UNIT 42®

Threat insights that matter.

Trusted expertise from leaders in incident response.

EXPLORE FINDINGS >

paloalto® NETWORKS | UNIT 42®

Global Incident Response Report

2025