paloalto NETWORKS

The Convergence of Cybersecurity and AI

7 Game-Changing Predictions for 2025

A Message from Nir Zuk

The cybersecurity industry is on the cusp of tectonic shifts in 2025, demanding leaders to reimagine how they safeguard their organizations.

Make no mistake about it, we are at the intersection of human ingenuity and technological innovation, where the game of cybersecurity has evolved into a high-stakes match.

This isn't just an evolution – it's a redefinition of how we approach security in a world where threats are faster, smarter, and more adaptive than ever before.

Organizations can no longer afford to rely on fragmented systems or reactive strategies. To lead, they must take decisive, proactive measures: centralizing data, embracing AI-driven solutions, and unifying their security platforms.

True resilience will come from those who can anticipate challenges, adapt to the unknown, and leverage innovation to stay ahead. The predictions you'll find here are more than just forecasts – they are a guide to navigating the future with confidence.

The following predictions will provide the insights needed to navigate this new world. Once you've absorbed them, get in touch and we'll map out your innovative game plan.

Nir Zuk

Founder and CTO
Palo Alto Networks

Introduction

In 2025, businesses must adapt their strategies for operational resilience in the AI era, emphasizing the necessity of unified security platforms, transparent AI and cross-functional alliances for sustainability and trust.

The threat landscape is evolving rapidly. **Unit 42** highlights **early cybercriminal adoption of AI** to create highly personalized phishing and smishing schemes that exploit both public and private data. We'll see the continued escalation of adversarial AI targeting machine learning models to disable automated threat detection systems.

Critical infrastructure sectors like healthcare, energy, banking, transportation and data centers are expected to face heightened risks. These sectors are attractive targets due to their significant IP and critical data repositories, making them vulnerable to sophisticated disruptions.

By 2026, the majority of advanced cyberattacks will employ AI to execute dynamic, multilayered attacks that can adapt instantaneously to defensive measures. This escalation in AI usage by both attackers and defenders will transform the cybersecurity landscape into a continuous AI cyber arms race. Success in this New Year will depend on the convergence of security solutions and data into a unified platform, making strides in establishing governance frameworks and trust in AI, and putting AI at the helm of security operations.

Cybersecurity and AI: Predictions for 2025

PREDICTION
01
Cyber Infrastructure Will Be Centered Around a Single Unified Data Security Platform

PREDICTION
02
The Data Advantage: Larger Incumbent Organizations Will See Greater AI Success Than New AI Startups

PREDICTION
03
AI's Integrated Role: Establishing Trust, Adhering to Governance, and Reshaping Leadership in Security Operations

PREDICTION
04
Enterprises Will Widely Adopt a Secure Browser

PREDICTION
05
There Will Be More Focus on the Energy Impact of AI, Including AI Used for Security

PREDICTION
06
Debunking Quantum Security Hype: Managing Expectations and Taking Action

PREDICTION
07
The CIO and the CMO Are the Enterprise's New Dynamic Duo

PREDICTION

01

Cyber Infrastructure Will Be Centered Around a Single Unified Data Security Platform

In 2025, the cybersecurity landscape will undergo a transformative shift toward a unified data platform encompassing everything from code development to cloud environments and SOCs. Current fragmented systems, burdened with isolated workflows and manual processes, cannot match the speed and sophistication of modern cyberthreats. This is particularly evident in cloud security, where decentralized systems, inconsistent data flow and disjointed tools create blind spots, slowing the ability to detect, respond to and prevent breaches.

In the coming year, we can expect the convergence of code to cloud to SOCs in a unified infrastructure to enable AI-powered analysis from every point along the attack surface — from code vulnerabilities during development to real-time monitoring of cloud environments, down to the SOCs managing incident responses. For cloud security, this means organizations will have greater control over their multicloud environments, where AI can monitor for misconfigurations, anomalous behavior or unauthorized access at unprecedented speed and accuracy. The convergence of all security layers onto a unified platform will optimize resources, improve overall visibility and efficiency, and enable organizations to build more resilient, adaptive defenses against evolving threats.

Organizations projected to use fewer than 15 cybersecurity tools

13%
2023

45%
2028

Relying on multiple vendors for firewalls, cloud security and SOC tools could inhibit AI's full potential. The benefit of vendor and tool consolidation goes beyond the total cost of ownership (TCO) and becomes key to centralizing data streams to reduce the mean time to detect (MTTD) and mean time to respond (MTTR) to minutes. Already, 45% of organizations are projected to use fewer than 15 cybersecurity tools by 2028, compared to just 13% in 2023 — a trend toward streamlined, cohesive security solutions.

In turn, managed security service providers (MSSPs) and value-added resellers (VARs) will be at the forefront of a critical transformation in cybersecurity. As the industry pivots from fragmented, multivendor architectures to integrated, **AI-driven platforms**, these partners will be the catalysts, guiding clients to adopt cohesive solutions that unify security operations. By shifting to a single seamless platform, businesses will not only unlock powerful, AI-fueled insights but will also elevate their resilience in an era of unprecedented cyberthreats. Organizations embracing this unified approach will redefine industry standards, gaining agility, precision and a decisive competitive edge in cybersecurity.

PREDICTION

02

The Data Advantage: Larger Incumbent Organizations Will See Greater AI Success Than New AI Startups

In 2025, large incumbent organizations with vast datastores will take the lead in AI-driven innovation, gaining a powerful advantage over new entrants. Companies like Palo Alto Networks, which processes 9 petabytes of data daily across multiple platforms and serves a base of 72,000 active customers, are positioned to dominate in a data-centric AI landscape. AI's success hinges on data quality and volume, with the bulk of model performance relying on these elements. For incumbents with established customer bases, a wealth of data fuels continuous model improvement, creating a flywheel effect that's hard for startups to match.

In the coming year, however, we also anticipate these larger organizations partnering with emerging AI startups, granting them access to critical data in exchange for fresh ideas and agile innovations. This symbiotic relationship will accelerate AI advancements, with established companies leveraging innovative approaches while startups benefit from invaluable data access. Together, these partnerships will drive an accelerated pace of AI breakthroughs, setting a new standard for collaborative success in cybersecurity.

Organizations with Vast Datastores Will Take Lead In AI-Driven Innovation.

The wealth of data and established customer base of incumbents, like Palo Alto Networks, fuels continuous model improvement, creating a flywheel effect that startups can't match.

PROCESSES

9

Petabytes of data daily across multiple formats.

SERVES

72,000

Active customers.

PREDICTION

03

AI's Integrated Role: Establishing Trust, Adhering to Governance, and Reshaping Leadership in Security Operations

AI will become the driving force in the SOC, with human analysts playing a crucial but secondary role. Much like autonomous driving with human oversight, SOCs will increasingly rely on AI-driven processes, automating tasks such as vulnerability scanning and threat detection while reserving advanced analytics and response strategies for human experts. This AI-led evolution will **transform the SOC** into an agile, efficient powerhouse equipped to handle today's escalating threats.

Because of this, it will be crucial for organizations to prioritize transparency and proactive communication about AI model mechanics. This includes being transparent about aspects such as data collection, training datasets and decision-making processes. By providing employees and customers alike with clear information and insights into how AI systems operate, organizations can build credibility and foster deeper relationships. CISOs should build an AI council to help govern guardrails on what an autonomous system is allowed to action, while encouraging a culture for AI across the organization.

One of the key challenges in establishing trust in AI lies in the volume of data used to make AI decisions. With petabytes of data informing AI conclusions, it becomes increasingly difficult for humans to manually verify the accuracy of AI recommendations. Unlike the traditional needle-in-a-haystack analogy, where finding the needle is the goal, AI decisions are based on a haystack of needles. Therefore, organizations are facing the imperative to develop models that can accurately track and explain the decision-making process of AI systems. This transparency in decisioning will be particularly important in sectors such as finance, where the use of AI-powered security could raise concerns about blocking legitimate financial transactions.

This evolution does not suggest that AI analysts will replace human experts; rather, it highlights the vital partnership between the two.

As the number of threats continues to escalate, the need for AI speed and accuracy will be critical in the enablement of decision-making by the human counterparts. This shift will enable human analysts to concentrate on high-IQ tasks that require advanced analytics and strategic thinking.

PREDICTION

03

We can also expect further advancements in AI governance and regulations around the world. The European Union, building on the success of the General Data Protection Regulation (GDPR) and the AI Act, is likely to strengthen its digital sovereignty initiatives, tightening regulations around data privacy and implementing stricter rules for cross-border data transfers. Similarly, in the Middle East, increased digital transformation initiatives will likely prompt governments to establish more stringent cybersecurity laws focused on protecting critical infrastructure and expanding requirements for local data processing. Latin American countries, such as Brazil and Mexico, are also expected to enhance their national cybersecurity frameworks and engage in more collaboration on cross-border data flow agreements.

PREDICTION

04

Enterprises Will Widely Adopt a Secure Browser

The modern workplace is evolving. As more workers are on the go and organizations are embracing the modern workplace, it's fueling the growth of personal and unmanaged devices being used for work. By adopting secure browsers, organizations can implement stronger security measures to enable secure access to business apps from any device, and protect against malicious browser extensions, web attacks, user errors and more. With greater security, visibility and controls that secure browsers provide, companies of all sizes can enable secure access to business apps on any device and at any location, providing a more secure browsing experience for employees.

The rising concern over data breaches necessitates tighter control over corporate resources. Consumer web browsers are inherently insecure, with **95% of organizations** reporting security incidents originating from the browser across all devices, underscoring the lack of necessary security measures to protect organizations and their employees, no matter where they work. Secure browsers, on the other hand, allow organizations to extend security policies, such as masking sensitive PII (personally identifiable information) data and preventing attackers from accessing data inside the secure workspace of the browser. These security measures ensure that employees are able to access business applications safely and reduce the risk of data leaks.

This is why **Gartner** predicts that by 2030 browsers will be the key to delivering secure, digital workforce experiences on managed and unmanaged devices.

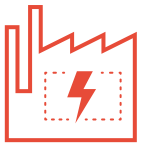
This proactive shift will extend security to the endpoint, empowering employees to work effectively while minimizing risk. By prioritizing secure access, organizations will not only protect sensitive data but also enable seamless collaboration in an increasingly mobile and distributed workforce. **Embracing this technology** will be essential for maintaining a robust security posture in today's dynamic business landscape.

Why are Secure Browser's Important?

Web browsers are inherently insecure. In fact, 95% of organizations report security incidents originating from the browser across all devices - no matter where people work.

PREDICTION

05



There Will Be More Focus on the Energy Impact of AI, Including AI Used for Security

As AI continues its trajectory, concerns over its energy impact will also grow—particularly in cybersecurity. Large-scale models deployed for tasks such as threat detection, anomaly detection and vulnerability assessment require constant updates and complex computations, all of which contribute to greater compute at faster speeds, increasing today's energy demands.

Data centers consume approximately 4% of U.S. electricity generation today. Looking forward, the Electric Power Research Institute **estimates** that consumption to reach upwards of ~9% of U.S. electricity generation annually. Similar numbers are projected at global scale. While efficiency gains in model innovation are likely, we see the necessity for public private partnerships for grid modernization and clean energy generation.

Simultaneously, all industries will need to consider energy-smart strategies, that could include:

Energy efficient AI models:

According to **ITI**, organizations should enhance resource efficiency through integrating new cooling technologies and optimize data center design. Cooling systems account for roughly **40%** of a data center's electricity bill. AI-driven cooling technologies, including multi-layer neural networks for optimized temperature control, has the potential to enhance efficiency and reduce emissions.

Quantum-based AI frameworks:

Advancements in **quantum-based AI frameworks** also hold promise as they can cut energy consumption and carbon emissions by enabling robust, uncertainty-aware control strategies for managing energy-intensive AI workloads.

Platformization

As organizations move towards vendor consolidation to achieve lower total cost of ownership and unify data security platforms, AI's efficiency could also reduce redundant processes and help to minimize energy demands and related environmental impact.

PREDICTION

05

Companies that deliver cloud-based services powered by renewable energy will provide additional benefits to customers. As such, tech made up **62%** of contracted renewable capacity from February 2023 to February 2024. In 2025, cloud providers will continue to invest in renewable and clean energy capacity to fuel the surge in AI.

Data centers are not just energy-intensive but also are a security risk for the volume of sensitive information they house. In 2025, there will be even more focus on the cybersecurity that protects data centers and the energy that powers AI,I, ensuring that technology's rapid growth remains sustainable for the long term.

PREDICTION

06

Debunking Quantum Security Hype: Managing Expectations and Taking Action

As quantum computing, quantum risk and the technology necessary to protect, encrypt and secure it move into the mainstream tech discussion, practical quantum attacks on widely used encryption methods are not yet feasible but are likely to become possible within the next decade. However, that doesn't mean you shouldn't plan ahead. In 2025, nation-state-backed threat actors will intensify their "harvest now, decrypt later" tactics, targeting highly classified government data or highly valuable intellectual property with the intent to access it as quantum technology advances. The reality is that this poses a risk to today's protected data as quantum computing has the potential to jeopardize civilian and military communications, undermine critical infrastructure and defeat security protocols for most internet-based financial transactions.

To counteract these threats effectively, organizations will need to begin to prepare by a short-term **quantum-resistant roadmap**, and act and adopt quantum-resistant defenses, including quantum-resistant tunneling, comprehensive crypto data libraries and other technologies with enhanced crypto-agility. The National Institute of Standards and Technology (NIST) recently released final standards for post-quantum cryptography. Transitioning to these algorithms will help secure data against future quantum threats. Organizations that require high security should explore quantum key distribution (QKD) as a means of ensuring secure communications. As quantum computing continues to become more of a reality and potential threats loom, it will be essential to adopt these measures to keep pace with the rapidly evolving cyber landscape, prevent data theft,and ensure the integrity of their critical systems.

For now, CIOs can debunk any hype around this topic to the board. Although significant progress with quantum annealing has been made, military-grade encryption has still not been broken.

Harvest Now, Decrypt Later

In 2025, nation-state-backed threat actors will intensify their "harvest now, decrypt later" tactics, targeting highly classified government data or highly valuable intellectual property with the intent to access it as quantum technology advances.

PREDICTION

07

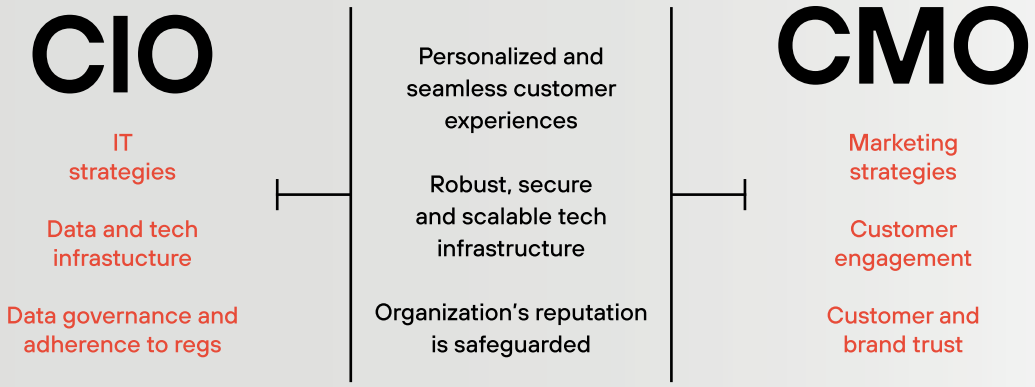
The CIO and the CMO are the Enterprise's New Dynamic Duo

In the next year, the alignment between the chief information officer (CIO) and chief marketing officer (CMO) will become increasingly critical as organizations continue to leverage advanced technologies such as AI, machine learning and big data to drive personalized customer experiences and digital transformation. The rapid evolution of customer expectations will demand seamless integration of marketing and IT strategies, with a focus on using data-driven insights to deliver personalized, real-time engagement across multiple channels. This will necessitate close collaboration between the CIO and CMO to ensure that marketing initiatives are supported by robust, secure and scalable technology infrastructure.

For this partnership to succeed, early alignment on security and regulatory compliance is essential. As customer data becomes increasingly integral to marketing efforts, the CIO's role in ensuring robust data governance and adherence to regulations such as GDPR or CCPA is critical.

CIO + CMO = Enterprise's New Dynamic Duo

The alignment of the CIO and CMO will create competitive advantage and will become increasingly critical as organizations continue to leverage advanced technologies such as AI, machine learning and big data.



PREDICTION

07

In addition to safeguarding customer data, organizations must stay vigilant in keeping track of new AI governance regulations, specifically around AI-content labeling. These regulations are aimed at ensuring the ethical use of AI and protecting user privacy. By staying up to date with AI governance, organizations can demonstrate their commitment to responsible AI practices and build trust with customers. Failure to align early on could lead to security breaches, compliance violations or inefficient marketing efforts, harming both customer trust and business performance.

This holistic approach will not only enhance cybersecurity but also enable organizations to leverage the power of data and AI for meaningful and personalized customer experiences, while safeguarding the company's reputation and avoiding legal pitfalls. This new "dynamic duo" will be perceived by organizations as a key driver of competitive advantage. Their collaboration will position them as indispensable contributors to a company's future, ensuring a strong market presence and maintaining customer trust amid rapid technological advancements.

About Us

At Palo Alto Networks, we are committed to making each day safer than the one before with industry-leading, AI-powered solutions in network security, cloud security and security operations. Powered by Precision AI™, our technologies deliver precise threat detection and swift response, minimizing false positives and enhancing security effectiveness. Our Platformization approach integrates diverse security solutions into a unified, scalable platform, streamlining management and providing operational efficiencies with comprehensive protection.

Learn more about our innovative solutions at **www.paloaltonetworks.com**.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com