Written Testimony of:

Wendi Whitmore
Chief Security Intelligence Officer
Palo Alto Networks

Before the:

Committee on Homeland Security
United States House of Representatives

Titled

“Innovation Nation: Leveraging Technology to Secure Cyberspace and Streamline Compliance”

May 28, 2025
2:00 PM

Chairman Green, Ranking Member Thompson, and distinguished members of the committee: thank you for the opportunity to participate in today's hearing. I appreciate this committee's commitment to understanding cybersecurity threats facing our nation and how to best equip the defenders on the digital front lines. My name is Wendi Whitmore, and I am the Chief Security Intelligence Officer for Palo Alto Networks.

For those not familiar with Palo Alto Networks, we are an American cybersecurity company founded in 2005 that has since become the global cybersecurity leader – protecting over 70,000 enterprises across more than 150 countries. We support 97 of the Fortune 100, critical infrastructure operators of all shapes and sizes, the U.S. Federal Government, universities and other educational institutions, and a wide range of state and local partners.

My testimony outlines the increasing sophistication of cyber adversaries and sheer volume of cyber attacks our customers defend against daily. In fact, every day we block up to 31 billion cyber attacks. Of this total – up to nine million of those daily attacks – represent novel attack methods *never previously seen*.

To stay a step ahead, we must be relentless in our commitment to cyber defense innovation. To that end, Palo Alto Networks is proud to have invested $1.8 billion in R&D just last year. We are confident that this innovation – with AI at its core – can disrupt the status quo of the cybersecurity industry and simultaneously: 1) deliver transformative cybersecurity outcomes, 2) drive much-needed cost rationalization for network defenders, and 3) eliminate inefficient, manual processes. This innovative spirit will be critical to combatting not just the threats of today, but also the emerging risks – like encryption-breaking quantum computing – of tomorrow.

Palo Alto Networks supports this committee's desire to pivot away from a stale, point-in-time, compliance-first mindset for cyber resilience – and instead radically rethink how AI and automation can turbocharge cyber defense. While policymakers appropriately cultivate a robust and ongoing debate about the right combination of carrots and sticks to incentivize desired outcomes, one thing is clear: "business as usual" in the cybersecurity ecosystem is failing to translate cybersecurity investments into cybersecurity outcomes. We look forward to working with all interested parties to chart out a more resilient path forward.

The Evolving Cyber Threat Landscape

At Palo Alto Networks, we have a unique vantage point into the cyber threat landscape. What we are seeing should concern us all. Our cyber adversaries – China, Russia, Iran, North Korea and beyond – certainly aren't sitting on their hands.

In May of 2023, we contributed to the first U.S. Government advisory on the China-attributed Volt Typhoon campaign against a range of critical infrastructure entities. Since then, another China-linked campaign, called Salt Typhoon, rightfully garnered substantial attention from cyber practitioners and policymakers for its successful targeting of communications infrastructure.

These campaigns, and others, highlight a sobering reality – adversaries can also be innovative. They are actively leveraging emerging technologies, like AI, to amplify the scale and speed of their attacks and to find new vectors to compromise systems. Attackers are leveraging AI for deepfake-enabled social engineering, enhancing ransomware negotiations, and identifying sensitive credentials. The emergence of Agentic AI, autonomous systems capable of making decisions and adapting tactics without human intervention, poses a significant escalation of this threat. In the future, Agentic AI will be able to independently execute multi-step operations, leading to faster, more adaptive, and difficult-to-contain cyberattacks.

Meanwhile, the pace of AI adoption across companies and industries vastly increases the total size of the digital attack surface that can be exploited by adversaries, even further complicating the cyber defense picture.

Palo Alto Networks distills these cyber threat landscape trends in our annual incident response report, informed by our work assisting victims of over 500 major cyberattacks. These incidents involved large organizations grappling with extortion, network intrusions, data theft, advanced persistent threats, and more. The targets of these attacks spanned all major industry verticals across 38 countries. Our analysis of these engagements highlights several important trends:

- Increasing Business Disruption. Threat actors are augmenting traditional ransomware and extortion with attacks designed to intentionally disrupt victim operations. In 2024, 86% of incidents that we responded to involved business disruption – spanning operational downtime, reputational damage, or both. Attackers are using this disruption to force victims into negotiating and paying a ransom.

- Cyberattacks Are Moving Faster than Ever. Attackers exfiltrated data in under five hours in 25% of incidents in 2024, which is three times faster than in 2021. What's even more alarming is that in one in five cases, data theft occurred in under one hour.

- AI Is Accelerating the Attack Lifecycle. AI has the potential to significantly reduce the cost of creating customized malware, creating conditions for a significant surge in malware variants that will be more difficult to defend against with traditional cyber capabilities. In a controlled experiment, our researchers found that AI-assisted attacks could reduce the time to exfiltration to just 25 minutes, a 100x increase in speed.

- Phishing Makes A Comeback. After vulnerabilities took the top spot in 2023, phishing resurged as the most common entry point for cyberattacks, responsible for 23% of all initial access. Fueled by generative AI, phishing campaigns are now more sophisticated, convincing, and scalable. Inclusive of phishing, 44% of the attacks we investigated in 2024 involved a web browser – heightening the importance of browser security.

- Complexity Is Killing Security Effectiveness. In 75% of incidents, logs existed that should have indicated potentially malicious activity. But, data silos prevented detection before it was too late.

- Multipronged Attacks Are the New Norm. In 70% of incidents, attackers exploited three or more attack surfaces, forcing security teams to defend endpoints, networks, cloud environments, and the human factor in tandem.

- Elevated Insider Threat Risk. Organizations face an elevated risk of insider threats, as nation-states like North Korea target organizations to steal information and extort victims for funding which they then use to support national initiatives. Insider threat cases tied to North Korea tripled in 2024.

- Increasing Cloud Attacks. Nearly 29% of cyber incidents involved cloud environments, with 21% causing operational damage to cloud environments or assets as threat actors embedded within misconfigured environments to scan vast networks for valuable data. In one campaign that compromised a cloud environment, attackers scanned more than 230 million unique targets for sensitive information.

Meeting the Moment: Leveraging AI for Cyber *Defense*

Despite the evolving threat landscape, we remain confident that we are well-equipped to combat the cyber incursions of today and tomorrow. AI is, and will continue to be, a game changer, not only for the bad guys, but also for the cyber defenders who ward off the crooks, criminals, and nation states that threaten our digital way of life. Our product suite, which spans network security, cloud security, endpoint security, and Security Operations Center (SOC) automation, leverages AI to stay a step ahead of attackers.

Palo Alto Networks first introduced machine learning (ML) capabilities as part of our malware protection offering 10 years ago. We now deploy over 30 products that leverage AI, with many more in development. Our Precision AI combines the best of ML, deep learning, and generative AI to drive real-time and automated security.

Looking forward, these benefits will continue to increase as cyber professionals incorporate more Agentic AI capabilities into their defense portfolio. Here, AI-powered cyber capabilities will help automate remedial, often human-driven operations, to allow the platform to automate certain response actions and decrease the time it takes for an organization to respond to an incident.

Empowering Cyber Professionals:

For too long, our community's most precious cyber resources – people – have been inundated with security alerts that require manual triage, forcing them to play an inefficient game of "whack-a-mole," while vulnerabilities remain exposed and critical alerts are missed. Making matters more difficult, this legacy approach often requires defenders to stitch together security data from across dozens of disparate cybersecurity products at the same time. Organizations find themselves drowning in their own data, struggling to operationalize it. Industry research shows that over 90% of SOCs are still dependent on manual processes, a sure-fire way to give adversaries the upper hand and increase analyst burn-out.

This inefficient, manual posture results in suboptimal performance against metrics like Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to incoming incidents. Metrics like these serve as basic cyber vital signs for an enterprise's security posture. They provide quantifiable data points for network defenders about how quickly they discover potential security incidents and how quickly they contain those incidents. Historically, organizations have struggled to execute against these metrics. In fact, a report by Unit 42 found that security teams average nearly six days to resolve an alert in cloud breach incident response cases.

AI-Driven Security Operations Centers:

AI-driven SOCs can flip this paradigm and give defenders the upper hand. This technology acts as a force multiplier for cybersecurity professionals to substantially reduce detection and response times. The results from deploying this technology on our own company networks are significant:

- On average, we ingest 90 billion events daily.
- Using AI-driven data analysis, this is distilled down to 26 thousand raw alerts.
- This is further triaged to just *one* incident that requires manual SOC investigation.

We then deployed this AI-powered SOC to our customers where we are seeing similarly transformative outcomes:

- Reduction of MTTR from 2-3 days to under two hours, *with ~60% of customers under 10 minutes*.
- Fivefold increase in incident close out rate.
- Fourfold increase in the amount of security data ingested and analyzed each day.

These dramatic improvements are critical to stopping threat actors before they can encrypt systems or steal sensitive information – which is now frequently happening in mere hours. None of this would be possible without the power of AI.

Commitment to Cybersecurity Innovation – Protecting Against Emerging Risks

Securing AI by Design:

AI is taking enterprise IT by storm, and it is here to stay. On the commercial side, 42% of enterprises are already leveraging AI tools. This is expected to grow to 96% within the next 12 months, with over 12,000 AI apps projected to be in use by 2030. AI use is also surging in the U.S. federal government, where 41 government agencies reported a total of 2,133 AI use cases for the Consolidated 2024 Federal AI Use Case Inventory, up from just 710 use cases reported for 2023. The typical large enterprise will use hundreds of AI apps internally, leverage thousands of AI models, and produce many petabytes of training and vector embedding data annually.

This expanded AI attack surface brings evolved data security and network security challenges. Research indicates that 50% of employees currently use AI apps without permission in their enterprise, 80% of public models can be "jailbroken" (bypassing restrictions installed by model creators), and there are already hundreds of malicious models available in the wild.

In sum, AI app proliferation is changing how enterprises operate. This change demands an evolved security approach. We like to think of this approach as Secure AI by Design. This approach requires the ability to:

1. ***Discover*** – gain a clear understanding of AI assets being developed across the enterprise.
2. ***Assess*** – continuously assess security, safety, and compliance risks of AI apps, agents, models and datasets, across the supply chain and runtime.
3. ***Protect*** – detect and prevent risks detected in the supply chain and runtime.

These principles are aligned with, and based on, the security concepts already included in the NIST AI Risk Management Framework (RMF).

Fully harnessing the enormous potential of AI requires deploying it securely. Furthering our commitment to lead this important AI security conversation, we recently announced our intention to acquire ProtectAI, an early innovator in this space.

Ensuring Quantum Readiness Today:

AI is also accelerating quantum R&D, bringing the era of encryption-breaking quantum computers closer than previously anticipated. This forthcoming moment of quantum reckoning is likely to render existing public key encryption, the foundational underpinning of data security for the last several decades, obsolete and insecure. Accordingly, we must move aggressively to harden our systems for the inevitable post-quantum cryptographic reality.

While the U.S. Government has commendably established a 2035 timeline for federal agencies to transition to quantum-safe cryptography, the reality of "harvest now, decrypt later" attacks demands a far more aggressive posture. Adversaries are actively collecting our sensitive encrypted data today, fully intending to decrypt it within the coming years. Waiting until 2035 to achieve comprehensive quantum readiness will leave a significant window of vulnerability, jeopardizing classified information and the personal data of American citizens.

To effectively counter this risk, the United States must adopt a more proactive and accelerated approach to quantum readiness. We urge Congress to prioritize quantum readiness in all federal IT modernization initiatives, ensuring that new systems are built and procured with post-quantum cryptographic compatibility from the outset. Further, we must incentivize the adoption of quantum-safe technologies across the critical infrastructure sectors that underpin our national security and public safety. Central to this imperative will be leveraging solutions that empower organizations to continuously inventory their cryptographic vulnerabilities, visualize and prioritize risks, and implement quantum-safe remediations through automated workflows.

Bottom line: we believe 2035 may be too late. Quantum readiness requires decisive action now.

Policy Recommendations to Drive Federal Cyber Resilience

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 developed a set of recommendations for policymakers to consider at this pivotal moment for our nation's cyber defense:

1. Focus on measurable cybersecurity *outcomes*. Are cybersecurity investments actually making networks safer? Two of the most telling indicators of cyber resilience are MTTD and MTTR. The president should be able to walk into the White House Situation Room and see the real-time cyber vital signs, like real-time MTTD and MTTR metrics, for all agencies.

2. Forcefully respond to Salt Typhoon by promoting Zero Trust. 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 security. Cloud is becoming the dominant attack surface – in a Unit 42 report, 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 empower cyber defense. 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 SOCs, and Palo Alto Networks applauds the recently signed EO on Removing Barriers to American Leadership in Artificial Intelligence as an important validation of AI's enormous national security potential.

5. Promote 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, and it is under constant attack by adversaries. In response, we should further expand the scope and scale of DIB cybersecurity services offered by the NSA Cybersecurity Collaboration Center.

7. Modernize federal procurement. Current procurement cycles do not 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 cybersecurity regulatory harmonization. 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.

10. Leverage cyber shared services to increase efficiency and reduce waste. Shared service offerings for federal agencies can provision cybersecurity capabilities at scale – improving cybersecurity outcomes while being prudent stewards of taxpayer dollars.

People and Partnerships

To stay ahead of cyber threats, we need people, processes, and technology working in concert. To that end, Palo Alto Networks applauds Chairman Green on the reintroduction of the *Cyber PIVOTT Act*. The bill's recognition of the importance of collaboration between the government, community colleges, and industry, and the power of hands-on, skills-based exercises, will help build a pipeline of skilled professionals capable of protecting our digital way of life.

We are also working to broaden access to cybersecurity education. The Palo Alto Networks Cybersecurity Academy offers free and accessible curricula, aligned to the NIST National Initiative for Cybersecurity Education (NICE) Framework, to academic institutions from middle school through college. Hands-on experiences with cyber and AI benefit the entire ecosystem as they help to upskill our own workforce as well as that of our customers.

Palo Alto Networks also offers several accelerated onboarding programs to help broaden our workforce, including the *Unit 42 Academy*. As full-time members of our incident response and cyber risk management teams, early-career professionals with both university and military backgrounds spend 15 months developing skills through specialized, instructor-led courses, on-the-job training, and mentorship.

Partnership is in our DNA at Palo Alto Networks, and our collective defense depends upon deepening collaboration between industry and government. We are active members of the Information Technology Sector Coordinating Council (IT-SCC), and participate in several projects – including zero trust network architecture, quantum security, and 5G security – at the National Cybersecurity Center of Excellence (NCCoE).

We continue to see productive collaboration across a range of cybersecurity-focused convening bodies, including CISA's Joint Cyber Defense Collaborative (JCDC). With that in mind, we support Rep. Swalwell's efforts to further put wind in the sails of the JCDC, which has been a great partner for those in industry.

Maintaining the ability to share cyber threat intelligence across the public and private sectors remains vital, and we fully support reauthorizing the *Cyber Information Sharing Act of 2015*. We appreciate the thoughtful hearing Rep. Garbarino convened on this issue earlier this month.

We take our partnership with lawmakers – and this committee – seriously. Please consider Palo Alto Networks a standing resource as you continue to consider cybersecurity and AI issues. Thank you for the opportunity to testify. I look forward to your questions.