Palo Alto Networks Forecasts 6 Predictions on Securing the New AI Economy for 2026

November 18, 2025

2026 will be the "Year of the Defender," where autonomous AI defense is the only way to combat AI-driven identity attacks, data poisoning and quantum risks

SANTA CLARA, Calif., Nov. 18, 2025 /PRNewswire/ -- Palo Alto Networks (NASDAQ: PANW), the global cybersecurity leader, today released "6 Predictions for the AI Economy: 2026's New Rules of Cybersecurity," forecasting a transformative leap to the AI economy. This new AI-native global economic model, where AI drives productivity and operations, also introduces a seismic shift in risk. In 2026, autonomous AI agents will fundamentally redefine enterprise operations, setting the stage for major changes in identity, the security operations center (SOC), quantum computing, data security and the browser.

Palo Alto Networks forecasted 2025 as the Year of Disruption based on the rise in mega breaches that take entire enterprise networks offline — driven by supply chain vulnerabilities and attackers reaching new levels of speed and sophistication. This has since been proven true, as 84% of the major cyber incidents that Unit 42® investigated this year have resulted in operational downtime, reputational damage or financial loss. In 2026, we will enter into the Year of the Defender, where AI-driven defenses tip the scale in the defense's favor, driving down response times, reducing complexity and increasing visibility to quickly respond to cyberattacks.

Wendi Whitmore, Chief Security Intelligence Officer at Palo Alto Networks
"AI adoption is redefining cybersecurity risk, yet the ultimate opportunity is for defenders. While attackers utilize AI to scale and accelerate threats across a hybrid workforce, where autonomous agents outnumber humans by 82:1, defenders must counter that speed with intelligent defense. This necessitates a fundamental shift from a reactive blocker to a proactive enabler that actively manages AI-driven risk while fueling enterprise innovation."

From the anticipated surge in AI-driven identity attacks to the new wave of executive liability for rogue AI, these predictions for 2026 serve as essential guidelines for organizations to shape their cybersecurity strategies and confidently navigate the new autonomous economy.

Palo Alto Networks 2026 AI and Cybersecurity Predictions:

1. **The New Age of Deception: The Threat of AI Identity:** In 2026, identity will become the primary battleground as flawless, real-time AI deepfakes — or CEO doppelgängers — make forgery indistinguishable from reality. This threat is magnified by autonomous agents and a staggering 82:1 machine-to-human identity ratio, creating a crisis of authenticity where a single forged command triggers a cascade of automated actions. As trust breaks down, identity security must transform from a reactive safeguard into a proactive enabler for the enterprise, securing every human, machine and AI agent.

2. **The New Insider Threat: Securing the AI Agent:** Enterprise adoption of autonomous AI agents will finally provide the force multiplier needed to solve the 4.8 million-person cyber skills gap and end alert fatigue. This is also an inherent risk, creating a potent new insider threat. These always-on, implicitly trusted agents are given privileged access and the keys to the kingdom, instantly becoming the most valuable target. Adversaries will no longer make humans their primary target; they will look to compromise these powerful agents, turning them into an "autonomous insider." This forces a shift to autonomy with control, requiring AI firewall governance tools at runtime to stop machine-speed attacks and ensure the AI workforce isn't turned against its owners.

3. **The New Opportunity: Solving the Data Trust Problem**: Next year, the new frontier of attack will be data poisoning — invisibly corrupting AI training data at its source. This attack exploits a critical organizational silo between data scientists and security teams to create hidden backdoors and untrustworthy models, igniting a fundamental "crisis of data trust." As traditional perimeters become irrelevant, the solution must be a unified platform that closes this blind spot, using data security posture management (DSPM) and AI security posture management (AI-SPM) for observability and runtime agents for firewall as code to secure the entire AI data pipeline.

4. **The New Gavel: AI Risk and Executive Accountability:** The enterprise race for an AI advantage will collide with a new wall of legal reality. By 2026, the massive gap between rapid adoption and mature AI security (with only 6% of organizations having an advanced strategy) will lead to the first major lawsuits holding executives personally liable for rogue AI actions. This "New Gavel" elevates AI from an IT issue to a critical liability issue for the board. The CIO's role must evolve to that of a strategic enabler — or partner with a new Chief AI Risk Officer — using a unified platform to provide verifiable governance that enables innovation safely.

5. **The New Countdown: The Quantum Imperative:** The "harvest now, decrypt later" threat, accelerated by AI, creates a crisis of retroactive insecurity, as data stolen today becomes a future liability. With the quantum timeline shrinking from a ten-year problem to a three-year one, governments' mandates will soon force a massive, complex migration to post-quantum cryptography (PQC). This immense operational challenge requires organizations to shift from a one-time upgrade to building long-term crypto agility — the ability to adapt cryptographic standards as a new, non-negotiable security foundation.

6. **The New Connection: The Browser as the Novel Workspace:** As the browser evolves from a tool for information synthesis into an agentic platform that executes tasks, it is becoming the new OS for the enterprise. This trend creates the single largest, unsecured attack surface — an AI front door operating with a unique visibility gap. With GenAI traffic up over 890%, organizations will be forced to adopt a unified, cloud-native security model capable of enforcing consistent zero trust security and data protection at the last possible millisecond — inside the browser itself.

To discover what Palo Alto Networks expect for AI and cybersecurity in 2026, learn more about our predictions.

Follow Palo Alto Networks on **X (formerly Twitter)**, **LinkedIn**, **Facebook** and **Instagram**.

About Palo Alto Networks
As the global AI and cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.

This press release contains forward-looking statements that involve risks, uncertainties and assumptions, including, without limitation, statements regarding the benefits, impact, or performance or potential benefits, impact or performance of our products and technologies or future products and technologies. These forward-looking statements are not guarantees of future performance, and there are a significant number of factors that could cause actual results to differ materially from statements made in this press release, including, without limitation: developments and changes in general market, political, economic, and business conditions; risks associated with managing our growth; risks associated with new products and subscription and support offerings; shifts in priorities or delays in the development or release of new offerings, or the failure to timely develop, release and achieve market acceptance of new products and subscriptions as well as existing products and subscription and support offerings; failure of our business strategies; rapidly evolving technological developments in the market for security products and subscription and support offerings; our customers' purchasing decisions and the length of sales cycles; our competition; our ability to attract and retain new customers; and our ability to acquire and integrate other companies, products, or technologies. We identify certain important risks and uncertainties that could affect our results and performance in our most recent Annual Report on Form 10-K, our most recent Quarterly Report on Form 10-Q, and our other filings with the U.S. Securities and Exchange Commission from time-to-time, each of which are available on our website at investors.paloaltonetworks.com and on the SEC's website at www.sec.gov. All forward-looking statements in this press release are based on information available to us as of the date hereof, and we do not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made.

View original content to download multimedia:https://www.prnewswire.com/news-releases/palo-alto-networks-forecasts-6-predictions-on-securing-the-new-ai-economy-for-2026-302617959.html

SOURCE Palo Alto Networks, Inc.

Caren Auchman, cauchman@paloaltonetworks.com