Palo Alto Networks Cortex XSIAM Delivers Industry's First AI-Driven SecOps Platform to Span Proactive and Reactive Security

April 28, 2025

Evolves industry-leading capabilities with AI-driven Cortex Exposure management and Advanced Email Security

SANTA CLARA, Calif., April 28, 2025 /PRNewswire/ -- Palo Alto Networks® (NASDAQ: PANW), the global cybersecurity leader, today unveiled Cortex XSIAM® 3.0, the next evolution of its industry-leading SecOps platform, bolstered with proactive exposure management and advanced email security, enabling customers to further consolidate on Cortex for significantly better, faster and more cost-effective security operations.

Three years ago, Palo Alto Networks anticipated the future of security operations by introducing Cortex XSIAM, which consolidates and normalizes all cybersecurity data to fuel advanced, real-time analytics and automation, making disjointed point products obsolete. The best-selling platform surged past $1 billion cumulative bookings in FY25 Q2, making it our fastest offering to reach this milestone. Earlier this year, Palo Alto Networks doubled down on cloud security with the introduction of Cortex Cloud, converging its industry-leading CNAPP and CDR capabilities on the unified Cortex platform.

Cortex XSIAM 3.0 continues its relentless disruption of the security operations market by upending decades-old approaches to vulnerability management and email security. It further expands the scope of the SOC from reactive to proactive security to prevent breaches before they happen, in addition to its current powerful incident response capabilities. These new XSIAM innovations will help customers modernize legacy offerings across a total TAM of $37 billion.

Gonen Fink, SVP of Products, Cortex at Palo Alto Networks:
"Cortex XSIAM harnesses the power of the world's largest and most comprehensive set of security data to transform our customers' ability to rapidly counter evolving attacks with advanced AI and automation. This expansion of our groundbreaking SecOps platform merges best-in-class reactive with proactive security measures, allowing customers to achieve unprecedented risk reduction across their entire enterprise, from code to cloud to SOC."

Cortex XSIAM 3.0 will enable customers to stop attacks at scale using AI-driven threat defense with Cortex Exposure Management and Advanced Email Security.

Cortex Exposure Management: Cut vulnerability noise by up to 99% with AI-driven prioritization and automated remediation spanning the entire enterprise:

- **See every exposure:** Uncover risks with a unified solution spanning native network, endpoint and cloud scanners — extended with integration from any third-party source.
- **Cut alert noise based on actual risk, not compliance:** Use AI to prioritize high-risk, exploitable vulnerabilities with no compensating controls, eliminating false alarms.
- **Close the loop with industry-leading automation to prevent future attacks:** Seamlessly create new protections for critical risks in native network, endpoint and cloud security solutions. Automate remediation across first- and third-party tools with playbook automation.

Cortex Advanced Email Security: Stop sophisticated email-based attacks missed by other solutions, with advanced AI and automation:

- **Outsmart GenAI-powered threats:** Detect advanced phishing and email-based threats based on attacker intent with LLM-powered analytics that continuously learn from emerging threats.
- **Stop attacks in real time with built-in automation:** Automatically remove malicious emails, disable compromised accounts, and isolate affected endpoints with best-in-class workflow automation.
- **Extend industry-leading detection and response with complete email context:** Correlate email, identity, endpoint and cloud data for unparalleled visibility into the full attack path for effective incident response.

Chris DeBrunner, VP of Security Operations, CBTS:
"The transition to Cortex XSIAM has transformed our SOC operations at CBTS. Previously, we struggled with alert fatigue due to multi-console complexity, multiple data sources, disparate vendors, and labor-intensive tasks. With the consolidation of major security capabilities into one platform, we have achieved remarkable efficiencies. Our incident close-out rate has reached 100%, and we have significantly reduced our median time to resolution (MTTR) from days to, in some cases, seconds. The automation provided by XSIAM has been crucial in managing the alert overwhelm we faced, making our team more effective and less error-prone."

Chase Hymel, CISO, State of Louisiana:
"Discovering the capabilities of Cortex XSIAM was a game-changer for the State of Louisiana. It's helped us to modernize our security infrastructure and set an example for other states to follow. By adopting XSIAM, we have significantly improved threat visibility and response effectiveness. Cortex XSIAM has allowed us to consolidate our security tools into one integrated platform, enhancing our security operations and protecting citizen data effectively. We have reduced MTTR from over 24 hours to under two minutes and automated the resolution of 86% of incidents."

Availability: Exposure Management and Advanced Email Security are expected to be generally available to customers globally in FY25 Q4. For more details on Cortex XSIAM 3.0, read our blog here.

Register to attend: On Tuesday, April 29, 2025, from 2:30-4:30 p.m. PDT, join Palo Alto Networks Chairman and CEO Nikesh Arora for a virtual event: Hello Tomorrow, and dive into how innovations in AI-driven SecOps are redefining security from the inside out.

Don't miss the launch event: Register for a one-hour virtual event June 4-5, 2025, to be among the first to see Cortex XSIAM 3.0 in action.

About Palo Alto Networks
As the global cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by 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. Discover 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-cortex-xsiam-delivers-industrys-first-ai-driven-secops-platform-to-span-proactive-and-reactive-security-302439335.html

SOURCE Palo Alto Networks, Inc.

Matt Manturi, mmanturi@paloaltonetworks.com