Palo Alto Networks Introduces Frontier AI Critical Defense Program

August 19, 2026

A collaboration of leading technology providers to protect critical infrastructure against the rapid rise of AI-discovered vulnerabilities

SANTA CLARA, Calif., Aug. 19, 2026 /PRNewswire/ -- Palo Alto Networks (NASDAQ: PANW) today announced the Frontier AI Critical Defense Program, a first-of-its-kind initiative to protect critical infrastructure from AI-driven exploits. Through the program, leaders across operational technology (OT), healthcare, commercial software and open-source communities coordinate with Palo Alto Networks to deploy proactive "virtual patches," neutralizing vulnerabilities at the network-level before attackers can exploit them.

Palo Alto Networks recently used Frontier AI models to uncover more than 14,000 previously unknown vulnerabilities in open source software, underscoring how AI could enable threat actors to automate cyberattacks and shrink attack timelines. Yet, critical infrastructure operators, constrained by strict uptime and safety testing, cannot patch at AI speed. This mismatch creates a significant exposure gap, leaving essential systems vulnerable long before software fixes can be safely deployed.

True defense at AI speed requires joint action. This program builds on our existing collaborations with IBM and Red Hat (as part of Lightwell), Microsoft (as part of MAPP) and OT leaders like Siemens and the Idaho National Laboratory (as part of the OT Threat Research Lab).

Today, the collaboration is expanding to include Anthropic, OpenAI, OT leaders like Mitsubishi and Axis Communications, industry consortiums for sharing risk information like Analysis and Resilience Center for Systemic Risk and Health-ISAC, OT research organizations like the independent, non-profit Energy R&D Institute (EPRI) and OSS initiatives like Akrites (an initiative from the Linux Foundation).

Palo Alto Networks Frontier Virtual Patching puts these insights into action to deliver proactive protection for joint customers. By combining Frontier AI threat discovery with trusted vulnerability intelligence, it delivers rapid network-level patches while safeguarding sensitive vulnerability details from attackers.

Lee Klarich, Chief Product Officer, Palo Alto Networks
"In the age of Frontier AI, the traditional, reactive race to build and deploy software patches before adversaries exploit a flaw is a losing battle. Protecting critical infrastructure requires a structural shift from isolated patching to collective, proactive intelligence. Through initiatives like our Frontier AI Critical Defense Program, we can neutralize threats at the network layer before they are weaponized."

Help safeguard critical infrastructure by joining the expanding Frontier AI Critical Defense Program, today. Visit the website to learn more on how to get involved, or explore Palo Alto Networks broader Frontier AI Defense Initiative.

About Palo Alto Networks
Palo Alto Networks (NASDAQ: PANW), the global AI cybersecurity leader, protects our digital way of life with a comprehensive portfolio of cybersecurity solutions and platforms across Network, Cloud, Security Operations, AI and Identity. Trusted by 70,000+ customers and powered by Unit 42 threat intelligence, our AI-driven platforms eliminate complexity, empowering enterprises to modernize with confidence and securing the speed of innovation. Explore the future of security at www.paloaltonetworks.com.

Forward-Looking Statements
This release contains forward-looking statements with respect to Palo Alto Networks that involve risks, uncertainties and assumptions, including, without limitation, statements regarding the benefits, impact, or performance or potential benefits, impact or performance of Palo Alto Networks products, technologies, and integrations or future products, technologies, and integrations. 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 release. Palo Alto Networks identifies certain important risks and uncertainties that could affect its results and performance in its most recent Annual Report on Form 10-K, its most recent Quarterly Report on Form 10-Q, and its other filings with the Securities and Exchange Commission from time-to-time, each of which are available on Palo Alto Networks' website at investors.paloaltonetworks.com and on the SEC's website at www.sec.gov. All forward-looking statements in this release regarding Palo Alto Networks are based on information available to Palo Alto Networks as of the date hereof, and Palo Alto Networks does 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-introduces-frontier-ai-critical-defense-program-302855274.html

SOURCE Palo Alto Networks, Inc.

press@paloaltonetworks.com