Palo Alto Networks Delivers Anthropic's Mythos and OpenAI's GPT-5.6 to Customers with Unit 42 Continuous Frontier AI Defense

September 22, 2026

New service enables enterprises to continuously find and fix exposures before attackers weaponize them

SANTA CLARA, Calif., Sept. 22, 2026 /PRNewswire/ -- Palo Alto Networks (NASDAQ: PANW) today announced Unit 42® Continuous Frontier AI Defense, an agentic offensive security service designed for enterprises that want to leverage gated capability models, including Anthropic's Claude Mythos and OpenAI's GPT, to perpetually find, validate, and remediate enterprise exposures before attackers can weaponize them.

Threat actors today are deploying AI to find and exploit vulnerabilities, compressing breach cycles by almost 97% in some cases, from weeks to hours. To help defenders answer the critical question of whether they are prepared for this step-change in cybersecurity, Unit 42 is now offering continuous offensive testing to identify and validate vulnerabilities, pinpoint exposures and attack paths, and then accelerate remediation.

This builds on Unit 42's Frontier AI Defense, which launched in April and introduced a point-in-time exposure analysis and a subsequent security blueprint that benchmarks current capabilities to help organizations modernize their cybersecurity systems. In August, Unit 42 announced it would expand its Frontier AI Exposure Analysis with OpenAI's GPT-5.6-Cyber and Anthropic's Claude Mythos 5, giving organizations access to its advanced cyber capabilities.

Key Capabilities of Unit 42 Continuous Frontier AI Defense
Powered by a proprietary multi-model harness that integrates cyber-specialized frontier AI models with Unit 42 threat intelligence and offensive security expertise, the new service delivers always-on threat exposure management to eliminate critical security blind spots. Key capabilities include:

- **Continuous Testing Engine:** Provides a full-estate baseline scan followed by always-on testing as an organization's environment changes.
- **Multi-Model AI Harness:** Unit 42 deploys a proprietary multi-model harness, the software architecture to route work to the model best suited for the task, improving efficacy and coverage while managing the cost of frontier AI at scale.
- **Leading Cyber Models:** The harness is built around gated capability models, including Anthropic Claude Mythos 5 and OpenAI GPT-5.6-Cyber, as well as open weight models.
- **Advanced Adversary Simulation:** Proves real-world exploitability by validating end-to-end attack paths across first- and third-party web apps, APIs, cloud infrastructure, source code repositories, and network assets.
- **Accelerated Remediation:** Delivers actionable and prioritized fixes, code-level guidance, and virtual patch recommendations. To implement virtual patches before vulnerabilities are publicly disclosed or official patches exist, organizations can pair this with Frontier Virtual Patching.

Proven Efficacy
Palo Alto Networks developed and validated this approach over six months of in-house testing and across more than 100 Unit 42 customer engagements, backed by a $17 million investment in R&D and methodology optimization. During internal deployment within Palo Alto Networks, the company found a year's worth of exposures in three weeks. In customer assessments, the Frontier AI Exposure Analysis found exposures in 100% of customers. Of those, 37% rated high or critical in severity. Overall, most exposures stemmed from first-party apps and more than two in three exposures in third-party apps had no known CVE.

Sam Rubin, Senior Vice President of Unit 42 at Palo Alto Networks
"AI has created an asymmetric advantage for threat actors against organizations trying to defend at human speed. Modern cybersecurity requires machine-speed defense. We're combining Unit 42's offensive testing and threat intelligence expertise with industry-leading AI harnesses and exclusive access to gated capability models to give defenders back the upper hand."

McCall McIntyre, Head of Global Cyber Partnerships, OpenAI
"Frontier AI is compressing the time it takes to find and exploit vulnerabilities, and defenders need frontier AI capabilities within the tools, workflows, and services they already trust. Through Daybreak and our work with Palo Alto Networks's Unit 42, we are pairing OpenAI GPT Cyber Models with deep security expertise, strong governance, and human judgment to help organizations validate the attack paths that matter and move from discovery to remediation at machine speed."

Michael Moore, Cybersecurity Lead, Anthropic
"Claude Mythos found flaws that survived decades of human review, and more than ten thousand high-severity vulnerabilities across the software the world runs on. That kind of visibility is only useful if someone can act on it, and Palo Alto Networks is built for exactly that. Unit 42 takes what Claude Mythos finds, tests whether it can actually be exploited, maps what an attacker could reach from there, and gets the fix in front of the right team first."

Availability
Continuous Frontier AI Defense is available worldwide on an annual subscription with options that vary based on the specific OpenAI, Anthropic and open-source models that are used. All subscriptions leverage a multi-model harness to match the optimal AI model to each security task.

To learn more about Unit 42 Continuous Frontier AI Defense, register for the upcoming Virtual Threat Briefing here.

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 75,000+ 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.

View original content to download multimedia:https://www.prnewswire.com/news-releases/palo-alto-networks-delivers-anthropics-mythos-and-openais-gpt-5-6-to-customers-with-unit-42-continuous-frontier-ai-defense-302885013.html

SOURCE Palo Alto Networks, Inc.

press@paloaltonetworks.com