

# Palo Alto Networks Secures the AI Agent Revolution with the Launch of Prisma AIRS 2.0

October 28, 2025

*Securing every layer of enterprise AI, from autonomous agents to the models that power them*

SANTA CLARA, Calif., Oct. 28, 2025 /PRNewswire/ -- Palo Alto Networks (NASDAQ: PANW), the global cybersecurity leader, today announced [Prisma@AIRS™ 2.0](#) a major platform upgrade that completes the native integration of the recently acquired [Protect AI](#) to deliver the industry's most comprehensive AI security platform. This release directly confronts a critical enterprise challenge: **78%** of organizations are transforming with AI, but only a staggering **6%** have the guardrails to do so securely. Prisma AIRS 2.0 meets this urgent demand by providing customers with end-to-end protection across the entire AI application lifecycle, securing everything from autonomous agents to the models themselves.

## **Anand Oswal, Executive Vice President of Network Security, Palo Alto Networks**

"AI is transforming every enterprise, creating extraordinary opportunities and new risks. Prisma AIRS 2.0 bridges that gap, uniting deep model inspection, real-time agent defense, and continuous red teaming in a single platform. We're redefining what it means to secure AI at scale by turning security into an accelerator for innovation, not an obstacle. This marks the continuation of our rapid innovation in AI security as we advance new capabilities to defend against the threats of tomorrow."

Prisma AIRS 2.0 delivers comprehensive end-to-end AI security, seamlessly connecting deep AI agent and model inspection in development with real-time agent defense at production runtime. The platform, continuously validated by autonomous AI red teaming, secures all interactions between AI models, agents, data, and users. This gives enterprises the confidence to discover, assess, and protect their entire AI ecosystem, accelerating secure innovation. Already trusted by global leaders in finance, healthcare, and government, Prisma AIRS 2.0 provides visibility, control, and confidence at scale through three enhanced security modules:

- **AI Agent Security: Securing the Autonomous Workforce.** Provides real-time, in-line defense against prompt injections, tool misuse, and malicious agent behavior. Prisma AIRS discovers and inventories every AI agent in use – sanctioned or unsanctioned ("Shadow AI") giving the visibility and control needed to secure the explosion of AI agents.
- **AI Red Teaming: Continuous, Autonomous Vulnerability Hunting.** Addresses the new, dynamic attack surface of Generative AI applications. Uses an autonomous, continuous, and context-aware agentic approach and over 500 specialized attacks to proactively find vulnerabilities in enterprise AI systems before they can be exploited. While others offer periodic testing, Prisma AIRS delivers a persistent, automated red team that thinks like a real adversary.
- **AI Model Security: Shielding Open-Source Deployment.** Performs a deep architectural analysis of the model itself to find threats traditional scanners can't see. It can detect sophisticated, AI-native threats like architectural backdoors, data poisoning, and malicious code hidden within the model layers. AI Model Security provides a complete "list of ingredients" for enterprise AI, including the model's architecture, training datasets, open-source licenses, and all software dependencies. This provides unparalleled visibility for AI model governance, risk, and compliance.

## **Harshul Joshi, Principal, Cyber, Data & Tech Risk, PwC US**

"The rapid adoption of generative AI is creating a new, complex threat surface for every enterprise. Our strategic alliance with Palo Alto Networks is designed to address this head-on. By fusing PwC's deep AI risk expertise, governance frameworks, and security advisory services with the technological power of their platforms, particularly Prisma AIRS, we offer our customers a unified platform approach to secure their AI deployments. This is no longer about point solutions; it's about providing the full-lifecycle, 'secure-by-design' assurance and managed defense required for our clients to innovate with AI, confidently and at scale."

## **Securing the Future: Defending Against Threats of Tomorrow**

With Prisma AIRS 2.0 setting the standard for AI security today, Palo Alto Networks is already looking ahead to the challenges of tomorrow. The company continues to drive AI innovation at an accelerated pace, strategically engineering its solutions to protect against tomorrow's threats. This vision stretches from securing new application modalities like [Cortex® AgentiX™](#) for the autonomous workforce, to ensuring safety at the endpoint with [secure browsers](#), and looking ahead to computational risks like [quantum readiness](#). By delivering the most complete, natively integrated platforms, Palo Alto Networks is setting the new benchmark for AI defense, enabling enterprises to accelerate adoption with confidence and ensuring their digital future is secure.

Prisma AIRS 2.0 is available today. To learn more, read the [blog](#) and register for [Ignite: What's Next](#) on Tuesday, October 28, at 9 a.m. PT. Visit our official [news center](#) for the latest announcements, news and developments from Ignite: What's Next.

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](http://www.paloaltonetworks.com).

*Palo Alto Networks, Prisma, Prisma AIRS, and the Palo Alto Networks logo are trademarks of Palo Alto Networks, Inc. in the United States and in jurisdictions throughout the world. All other trademarks, trade names, or service marks used or mentioned herein belong to their respective owners.*



View original content to download multimedia: <https://www.prnewswire.com/news-releases/palo-alto-networks-secures-the-ai-agent-revolution-with-the-launch-of-prisma-airs-2-0--302596820.html>

SOURCE Palo Alto Networks, Inc.

Hannah Seeman, hseeman@paloaltonetworks.com, 1-630-777-0261