NEWS RELEASE

Cisco Unveils AI Defense to Secure the AI Transformation of Enterprises

2025-01-15

News Summary:

- Cisco's end-to-end solution protects both the development and use of AI applications so enterprises can advance their AI initiatives with confidence.
- AI Defense safeguards against the misuse of AI tools, data leakage, and increasingly sophisticated threats, which existing security solutions are not equipped to handle.
- The innovative solution leverages Cisco's unmatched network visibility and control to stay ahead of ever-evolving AI safety and security concerns.

SAN JOSE, Calif., Jan. 15, 2025 /PRNewswire/ -- Cisco (NASDAQ: CSCO), the leader in security and networking, today announced Cisco AI Defense, a pioneering solution to enable and safeguard AI transformation within enterprises. As AI technology advances, new safety concerns and security threats are emerging at an unprecedented speed which existing security solutions are unprepared to protect against. Cisco AI Defense is purpose-built for enterprises to develop, deploy and secure AI applications with confidence.

"Business and technology leaders can't afford to sacrifice safety for speed when embracing AI," said **Jeetu Patel, Executive Vice President and Chief Product Officer, Cisco**. "In a dynamic landscape where competition is fierce, speed decides the winners. Fused into the fabric of the network, Cisco AI Defense combines the unique ability to detect and protect against threats when developing and accessing AI applications without tradeoffs."

The stakes of something going wrong with AI are incredibly high. According to Cisco's 2024 AI Readiness Index, only 29% of those surveyed feel fully equipped to detect and prevent unauthorized tampering with AI. The security challenges are also new and complex, with AI applications being multi-model and multi-cloud. Vulnerabilities can occur at model or app level, while responsibility lies with different owners including developers, end users and vendors. As enterprises move beyond public data and begin training models on proprietary data, the risks only grow.

To unlock AI innovation and adoption, enterprises need a common layer of safety and security that protects every user and every application. AI Defense enables enterprises' AI transformations by addressing two urgent risks:

Developing and Deploying Secure AI Applications: As AI becomes ubiquitous, enterprises will use and develop hundreds if not thousands of AI applications. Developers need one set of AI security and safety guardrails that work for every application. AI Defense helps developers move fast and unlock greater value by protecting AI systems from attacks and safeguarding model behavior, across platforms. The capabilities of AI Defense include:

- **Discovering AI**: Security teams need to understand who is building applications and the training sources they use. AI Defense detects shadow and sanctioned AI applications across public and private clouds.
- **Model Validation**: Model tuning can lead to toxic and unexpected outcomes. Automated testing checks AI models for hundreds of potential safety and security issues. This AI-driven algorithmic red team identifies potential vulnerabilities and recommends guardrails in AI Defense for security teams to use.
- **Runtime Security**: Continuous validation safeguards against potential safety and security threats such as prompt injection, denial of service and sensitive data leakage on an ongoing basis**.**

Securing Access to AI Applications: As end users rush to adopt AI applications like summarization tools to improve their productivity, security teams need to prevent data leakage and the poisoning of proprietary data. AI Defense enables security teams with:

- **Visibility:** Provides a comprehensive view of shadow and sanctioned AI-enabled apps used by employees.
- **Access Control**: Implements policies that restrict employee access to unsanctioned AI tools.
- **Data and Threat Protection**: Continuously safeguards against threats and confidential data loss while ensuring compliance.

Unlike safety guardrails built into individual AI models, Cisco delivers consistent controls for a multi-model world. AI Defense is self-optimizing, leveraging Cisco's proprietary machine learning models to detect ever-evolving AI safety and security concerns based on threat intelligence data from Cisco Talos. Splunk customers that are using AI Defense will receive enriched alerts with additional context from across the entire ecosystem. AI Defense integrates seamlessly with existing data flows for unparalleled visibility and control and is built into the Security Cloud, Cisco's unified, AI-driven, cross-domain security platform. It leverages Cisco's extensive mesh of enforcement points to perform AI security at the network level in a way only Cisco is optimized to deliver. Accuracy and trustworthiness are essential for protecting enterprise AI applications, and Cisco has been actively involved in developing AI security industry standards, including those from MITRE, OWASP, and NIST.

"The adoption of AI exposes companies to new risks that traditional cybersecurity solutions don't address," said Kent Noyes, Global Head of AI & Cyber Innovation at World Wide Technology. "Cisco AI Defense represents a significant leap forward in AI security, providing full visibility of an enterprise's AI assets and protection against evolving threats."

AI Defense is the latest in a series of AI-driven security innovations from Cisco, including Cisco Hypershield. Cisco AI Defense will be available in March for enterprises to safeguard their AI transformations. For more information, visit cisco.com/go/ai-defense.

Additional Resources:

- Blog: Protecting AI So AI Can Improve the World, Safely
- Blog: Cisco AI Defense: Comprehensive Security for Enterprise AI Adoption
- Animation: Cisco AI Defense

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide technology leader that is revolutionizing the way organizations connect and protect in the AI era. For more than 40 years, Cisco has securely connected the world. With its industry leading AI-powered solutions and services, Cisco enables its customers, partners and communities to unlock innovation, enhance productivity and strengthen digital resilience. With purpose at its core, Cisco remains committed to creating a more connected and inclusive future for all. Discover more on The Newsroom and follow us on X at @Cisco.

View original content to download multimedia:https://www.prnewswire.com/news-releases/cisco-unveils-ai-defense-to-secure-the-ai-transformation-of-enterprises-302351307.html

SOURCE Cisco Systems, Inc.