NEWS RELEASE

Cisco Redefines Security for the Agentic Era with AI Defense Expansion and AI-Aware SASE

2026-02-10

News Summary:

- Cisco is announcing a suite of capabilities to help enterprises securely adopt AI technology while maintaining agent integrity and control of agentic interactions.
- Biggest-ever updates to Cisco's AI Defense solution bring AI supply chain governance and runtime protections to agentic tool use, reducing the risk of compromise or manipulation.
- Industry-first, AI-aware security advancements to Cisco's Secure Access Service Edge (SASE) pair with AI traffic detection and optimization to keep agentic workflows safe, fast, and reliable.
- Cisco's latest secure routing and smart switching solutions add full-stack, post-quantum cryptography and operational improvements designed to support resilient, encrypted communications for AI-driven workflows.

AMSTERDAM, Feb.10, 2026 /PRNewswire/ **-- CISCO LIVE EMEA** -- Cisco (NASDAQ: CSCO) today announced a sweeping evolution of its security portfolio to help enterprises adopt agentic AI with confidence, combining agent protection, interaction governance, and resilient connectivity for AI-driven workflows.

As organizations move from AI assistants to autonomous agents that use tools and data across hybrid environments, security teams need to strengthen agentic defenses, govern agent interactions with enterprise systems and external services, and maintain reliable, cryptographically protected connectivity at scale.

"In the age of AI, safety and security are pre-requisites for adoption, and AI agents bring a whole new set of challenges," said **Jeetu Patel, Cisco's President and Chief Product Officer.** "As agents take on critical enterprise roles, we're developing protections that work both ways: preventing agents from being compromised and controlling what they can access and do on our behalf."

Protect agents from compromise, manipulation, and poisoned tooling

Agentic AI innovations have expanded the attack surface across AI supply chains and the tool ecosystem. Enterprises need protections that reduce the risk of agents being manipulated, or hijacked, including during tool interactions.

In the biggest expansion since its January 2025 launch, Cisco AI Defense delivers new features to better secure agents and the AI supply chain. These features include:

- **AI BOM (Bill of Materials):** Provides centralized visibility and governance for AI software assets, including model context protocol (MCP) servers and third-party dependencies, to secure the AI supply chain
- **MCP Catalog:** Discovers, inventories, and helps manage risk across MCP servers and registries spanning public and private platforms, strengthening AI governance
- **Advanced algorithmic red teaming:** Expands the scope of AI security assessments with adaptive single and multi-turn testing for models and agents in multiple languages
- **Real-time agentic guardrails to keep agents and applications safe:** Continuously monitor and inspect agentic interactions to detect manipulation or unsafe behavior—such as poisoned tools or prompts designed to trigger unauthorized tool use—helping teams enforce policy and reduce compromise risk

Together, these updates help teams inventory and govern AI assets, understand provenance, and surface vulnerabilities earlier in the AI development lifecycle.

Since launch, AI Defense has mapped to leading AI frameworks from organizations like NIST, OWASP, and MITRE. The latest updates add mapping to Cisco's new Integrated AI Security and Safety Framework to help teams better understand adversary objectives and measure risk exposure.

In addition, AI Defense's runtime protections now feature a developer-ready integration with NVIDIA NeMo Guardrails' open source framework, offering organizations a modular, interoperable architecture to protect AI systems in real time in production. AI Defense is a key component of the Cisco Secure AI Factory with NVIDIA, a validated reference architecture to securely power AI workloads in customer environments.

"AI security teams are now being asked three questions at once: what AI assets do we have, where did they come from, and how will they behave in production as agents interact with tools and third-party services," said **Chirag Mehta, Vice President and Principal Analyst at Constellation Research**. "With AI BOM and MCP governance plus multi-turn red teaming and real-time guardrails, Cisco AI Defense is targeting the full risk path from the AI supply chain to agentic runtime."

Govern agent interactions and ensure AI workflows

AI agents rely on continuous interaction with LLMs, SaaS applications, data stores, and tool endpoints that are often remote. When responses are slow or unreliable, people and machines must wait—delaying decisions, disrupting operations, or halting processes altogether.

From a security perspective, these AI workflows involve semantically complex messages that evade analysis by conventional defensive tools unable to interpret the "why" and "how" of agentic actions.

To meet these needs, Cisco SASE is unveiling new capabilities designed to both govern agent interactions and keep AI traffic reliable:

- **AI traffic optimization for predictable performance during surges:** Detects AI traffic and

applies optimization techniques like packet duplication to maintain reliable, low-latency AI interactions during bursts of load
- **MCP visibility, logging, and policy control:** Discovers and governs MCP communications with in-path controls and inspection outcomes to manage agent-to-tool connectivity
- **Intent-aware inspection of interactions and tool requests:** Combines rapid detection techniques with cloud-based analysis to evaluate the intent behind agentic messages and actions to detect and stop threats
- **Unified policy enforcement across SD-WAN and SSE:** Coordinates controls in a single framework to simplify governance as agent adoption accelerates and regulatory expectations evolve

"For today's CIOs and CISOs, the explosive growth of AI-driven workloads creates both opportunity and risk," said **Mauricio Sanchez, Senior Director at Dell'Oro Group. "**As enterprises adapt SASE architectures to support AI-driven workflows, Cisco has steadily increased its market share—up roughly 20% since 2023. Vendors that align networking, security, and policy enforcement are increasingly well-positioned as SASE deployments scale."

Deliver reliable, cryptographically protected connectivity at scale

As more businesses embed agentic AI into their operations, mission-critical workflows will traverse campus and branch environments. Organizations need networking that keeps AI-driven communications responsive today while preparing encryption for long-lived confidentiality and evolving regulatory expectations.

To meet this challenge, Cisco is announcing IOS XE 26, the latest version of the operating system that powers millions of networks globally. The new release powers its recently announced Cisco 8000 Series Secure Routers and Cisco C9000 Series Smart Switches, as well as two new variants of the 8100 Series Secure Routers for small and mid-size businesses, also available today. IOS XE 26 delivers industry-first full-stack post-quantum cryptography (PQC) protections for the enterprise, defending organizations against device tampering and data compromise designed to align with evolving European and global regulatory guidance.

Together, these advancements help organizations maintain predictable performance for AI-driven traffic across distributed environments and protect encrypted communications as they prepare for PQC. They also extend security, visibility, and operational simplicity from the core to campus and branch locations where AI-enabled workflows increasingly originate.

Also announced today:

- **Active Directory Defense:** Cisco Duo is rolling out new capabilities to add visibility, insights, and protection for on-premises identity infrastructure, helping close the legacy gap where modern controls and MFA can be difficult to apply to older protocols and applications. In partnership with SpecterOps BloodHound Enterprise, Cisco helps teams identify and reduce real-world identity attack paths.
- **AgenticOps for Security:** New agentic capabilities in Cisco Security Cloud Control will proactively analyze firewall traffic, capacity, health, and configuration data to surface prioritized recommendations and autonomously remediate issues while maintaining security and compliance.

For more information, visit cisco.com/go/security.

Additional Resources:

- Blog: One platform for the Agentic AI era by Jeetu Patel, President and Chief Product Officer, Cisco
- Blog: Redefining Security for the Agentic Era
- Blog: Security for the Agentic Era: Cisco AI Defense Breaks New Ground
- Blog: SASE for the AI Era: See the Intent. Secure the Agent. Scale the AI.
- Blog: How to Protect Your Active Directory with Duo's New MFA and Visibility Solutions
- Blog: Reinventing Branch Networking: How Cisco Empowers Small Businesses and Beyond
- Blog: Protection, Policy and Power at the Foundation of Future-Ready Campus Networks
- For more information about announcements from Cisco Live Amsterdam, visit the Cisco Newsroom

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.

Disclaimer: Some of the products and features mentioned are still in development and will be made generally available as they are finalized, subject to ongoing evolution in development and innovation. The timeline for their release is subject to change.

View original content to download multimedia:https://www.prnewswire.com/news-releases/cisco-redefines-security-for-the-agentic-era-with-ai-defense-expansion-and-ai-aware-sase-302683205.html

SOURCE Cisco Systems, Inc.