NEWS RELEASE

Cisco Secure AI Factory with NVIDIA Makes AI Easier to Deploy and Secure, Anywhere Organizations Need It

2026-03-16

Expanded architecture lets businesses run AI at scale, from central data centers to the factory floor, without sacrificing performance or security

NEWS SUMMARY:

- Cisco expands its Secure AI Factory with NVIDIA to work not just in large data centers, but at local edge sites where real-time decisions can't wait, from hospitals and warehouses to moving vehicles.
- Cisco is the premier partner to deliver partner-developed systems featuring NVIDIA Spectrum-X switch silicon paired with a Cisco operating system, providing customers the flexibility of leveraging both NVIDIA Cloud Partner-compliant reference architectures and Cisco Silicon One-based architectures.
- Cisco adds deeper security capabilities to its reference architecture by extending Hybrid Mesh Firewall policy enforcement to NVIDIA BlueField DPUs and integrating Cisco AI Defense to secure multi-agent systems.
- Cisco AI Defense will support and secure NVIDIA's new open agent development platform, OpenShell, adding controls and guardrails to govern agent and claw actions.

SAN JOSE, Calif., March 16, 2026 /PRNewswire/ -- Cisco (NASDAQ: CSCO) today announced a major expansion of its Secure AI Factory with NVIDIA, giving customers a framework for deploying AI across their entire infrastructure – from central data center to local sites where data is created and decisions are made. Enterprises, neoclouds, sovereign clouds, and service providers can now move AI from pilot to full-scale production without stitching together disconnected systems, compressing deployment timelines from months to weeks and embedding security from the start.

"Most organizations understand the potential for AI to transform their businesses, but they're navigating how to deploy the technology safely and at scale," said Chuck Robbins, Chair and CEO, Cisco. "In partnership with NVIDIA, we're solving that challenge with an architecture that sets a new standard for performance – making it simpler to deploy, operate, and secure AI infrastructure."

"AI factories are transforming every industry, and security must be built into every layer—from silicon to software—to protect data, applications, and infrastructure," said Jensen Huang, founder and CEO of NVIDIA. "Together, NVIDIA and Cisco are building the secure foundation for AI infrastructure—core to edge—so companies can scale intelligence with confidence."

AI That Runs Everywhere, Not Just in the Data Center

AI inference happens where data lives and decisions can't wait, whether on the hospital floor or for analyzing video of a factory floor in real-time to keep workers safe. This reality fundamentally reshapes infrastructure by requiring inference workloads to operate locally — closer to the data, the devices, and the moment a decision must be made. Cisco and NVIDIA are enabling organizations to support edge inferencing use cases by:

- **Transforming the Enterprise Edge:** Now supporting NVIDIA RTX PRO™ 4500 Blackwell Server Edition GPUs across the Cisco UCS and Cisco Unified Edge portfolios, Cisco enables enterprises to run mission-critical AI workloads at the edge without the energy cost and footprint of data center-scale hardware.
- **Transforming the Service Provider Edge:** Today Cisco announces the Cisco AI Grid with NVIDIA reference design that combines the power of Cisco's Mobility Services Platform with NVIDIA RTX PRO Blackwell Series GPUs. This enables service providers to leverage their existing networks to offer managed services for edge AI applications with carrier-grade reliability and sovereignty.

Driving Performance and Efficiency for Massive-Scale AI Factories

Building on the momentum of the recently launched systems powered by Cisco Silicon One G300 for scale-out and P200 for scale-across, Cisco continues to raise the performance ceiling while making the whole process faster and simpler.

- **Next-Generation Performance:** Cisco's latest high-speed switches power the most demanding AI workloads, including a new 102.4Tbps Cisco N9100 powered by NVIDIA Spectrum-6 Ethernet switch silicon. This joins the now generally available 800G N9100 powered by NVIDIA Spectrum-4 Ethernet switch silicon.
- **Rapid Deployment:** Cisco Nexus Hyperfabric, now a part of Cisco Nexus One, will support Cisco N9000 Series switches, including the N9100 Series powered by NVIDIA Spectrum-X Ethernet silicon. Now organizations can transform a complex, multi-vendor integration puzzle into a simple, full-stack solution to cut deployment times and reduce the burden on IT.

Customers building large AI factories now have two validated paths to choose from: an AI factory based on a reference architecture compliant with the NVIDIA Cloud Partner (NCP) program, and a Cisco Cloud Reference Architecture built on Cisco Silicon One that adheres to the same design tenets.

Security Fused into Every Layer

In an era where AI models are high-value assets and agents are more autonomous, taking actions, making decisions and interacting with other agents - security can't be an afterthought. Cisco is embedding protection into the fabric of the Secure AI Factory with NVIDIA to safeguard against both external threats and rogue agent behavior, including:

- **Securing AI infrastructure:** AI is only as safe as the hardware running it - and attackers know it.

Cisco Hybrid Mesh Firewall delivers consistent security policies across a diverse set of enforcement points: network switches, workload agents, and more. Greater coverage means fewer gaps for attackers to exploit. Today, Cisco is extending the Cisco Hybrid Mesh Firewall solution to enable policy enforcement on NVIDIA BlueField data processing units (DPUs) embedded in NVIDIA GPU servers connected to Cisco Nexus One fabrics. Threats are blocked at the server level before they ever reach an organization's data. The result: AI workloads that can be protected from the inside out, with zero performance trade-off.

- **Securing AI agents:** Cisco AI Defense delivers model security, automated vulnerability testing, and now purpose-built guardrails for AI agents at the edge through integration with NVIDIA NeMo Guardrails, a part of NVIDIA AI Enterprise software. This helps AI developers and security teams stay ahead of emerging threats and maintain trust in AI. AI deployments are becoming increasingly distributed, with agents at edge locations often interacting with those at the core to accomplish tasks and execute workflows. AI Defense, as a part of the Cisco Secure AI Factory with NVIDIA, now extends to securing those agent-to-agent interactions.

Cisco Secures Enterprise AI Agent Development

Building on Cisco's commitment to fuse security into all layers of AI infrastructure, as well as the agentic workforce, Cisco also announced today that Cisco AI Defense will support and secure NVIDIA's OpenShell runtimes – part of the NVIDIA Agent Toolkit - adding controls and guardrails to govern agent and claw actions. By continuously monitoring and validating every tool and action an agent performs, Cisco AI Defense ensures that enterprises can confidently deploy AI agents to manage critical workflows without compromising security. This integration bridges the gap between innovation and risk, allowing organizations to trust their autonomous systems to operate reliably and securely.

Industry Reactions:

"As a leader in high-performance computing solutions, Cirrascale is thrilled by the introduction of new NVIDIA Spectrum-6 based Cisco's N9100 series switches, extending Cisco's NCP reference architecture-compliant portfolio with an impressive 102.4T capacity and a unified management plane through Nexus One. These innovations, combined with the flexibility of NX-OS and SONiC, enable us to scale our AI infrastructure seamlessly while maintaining operational simplicity. The availability of the 51.2T Spectrum-4 switch further enhances our ability to deliver cutting-edge AI solutions to our clients with unmatched performance and reliability."
– Alex Nataros, CTO, Cirrascale Cloud Services

"Sharon AI looks forward to the Cisco's N9100 series switches, offering 102.4T capacity with Nexus One's cloud-managed Nexus Hyperfabric. With NCP RA compliance and the 51.2T Spectrum-4 based N9100 switch availability, we will be scaling our AI infrastructure with robust performance and efficiency. The G300 Silicon One-based N9300 switches provide the flexibility to meet evolving customer needs. Turnkey AI infrastructure deployment through Nexus One significantly simplifies operations and accelerates time-to-value for our initiatives."
– Andrew Leece, COO and founder, Sharon AI

"World Wide Technology's clients trust Cisco for enterprise networking. Their robust AI networking portfolio extends that trust to AI workloads. Cisco's portfolio offers choice and flexibility to clients to build tailored AI infrastructure using Cisco Silicon One and NVIDIA Spectrum-X Ethernet switch silicon based switches with stellar performance up to 102.4Tbps running NX-OS or SONiC and unified by the Nexus One management plane. We're excited about these advancements to deliver the scalability and performance required for the agentic era."
– Jeff Fonke, Practice Director - Global Solutions & Architecture, World Wide Technology

"As organizations move beyond the experimentation phase of AI, the primary challenge has shifted from 'what can AI do' to 'how do we operationalize it securely at scale.' The industry is at a critical inflection point

where AI workloads — specifically real-time inferencing —must move closer to the data at the edge without creating new security or infrastructure silos. The partnership between Cisco and NVIDIA is designed to offer customers the flexibility and choice they need to scale while helping them overcome complex integration challenges."
– Mary Johnston Turner, Global Lead, Digital and Datacenter Infrastructure and Services, IDC

Additional Resources

- For more information on the Cisco Secure AI Factory with NVIDIA, click here
- Executive Blog Post: Cisco Secure AI Factory: Powering Agentic AI at Scale
- Blog Post: Cisco Gives its Secure AI Factory with NVIDIA a Secure Multi-Agent Edge Up
- Blog Post: Securing Enterprise Agents with NVIDIA OpenShell and Cisco AI Defense

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide technology leader 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. Discover more on The Newsroom and follow us on X at @Cisco.

Disclaimer: Many of the products and features described herein remain in varying stages of development and will be offered on a when-and-if-available basis. The delivery timeline of these products and features is subject to change at the sole discretion of Cisco, and Cisco will have no liability for delay in the delivery or failure to deliver any of the products or features set forth herein.

View original content to download multimedia:https://www.prnewswire.com/news-releases/cisco-secure-ai-factory-with-nvidia-makes-ai-easier-to-deploy-and-secure-anywhere-organizations-need-it-302715129.html

SOURCE Cisco Systems, Inc.