NEWS RELEASE

Cisco Transforms Security for the Agentic AI Era, Further Fusing Security into the Network

2025-06-10

Latest innovations safeguard AI workloads and agents, give security teams cutting-edge tools to protect against increasingly sophisticated threats

News Summary:

- Cisco is building secure infrastructure for the AI era, further embedding zero trust and observability into the fabric of the network, from silicon to security operations centers (SOCs).
- Cisco's market-leading Hybrid Mesh Firewall portfolio adds a new generation of firewalls, expands segmentation, and enhances security visibility and policy management to further fuse security into the network.
- Cisco is redefining Zero Trust for the AI era with its Universal Zero Trust Network Access (ZTNA) offering that ensures seamless, identity-driven access for users, devices and AI agents, simplifying secure connectivity and providing visibility across hybrid environments.
- Cisco and Splunk deliver powerful integrations across Cisco's network, firewall and threat detection capabilities to enhance visibility, accelerate detection, and streamline response across infrastructure and applications.

SAN DIEGO, June 10, 2025 /PRNewswire/ -- **CISCO LIVE --** Cisco (NASDAQ: CSCO) today announced innovations to help enterprises reimagine security for the AI era. Security teams are racing to securely adopt AI throughout their enterprises, while threat actors are using AI to increase the frequency and reduce the cost of launching sophisticated cyber attacks. To overcome this unprecedented challenge, Cisco is fusing security capabilities deeper into its networking infrastructure, helping companies implement zero trust architectures, innovating on security for AI apps and models, and delivering breakthrough AI tools that improve threat detection and remediation.

Key advancements announced at Cisco Live include solutions for Hybrid Mesh Firewall and Universal Zero Trust Network Access (ZTNA) that simplify policy management, enhance visibility, and enable enterprises to scale securely without adding complexity to their security stack. In addition, Cisco

announced further Splunk integrations that unify data across platforms, helping security teams automate tasks and respond faster to threats.

"Safety and security are the defining challenges of the AI era—and agentic AI multiplies the risk, as every new agent is both a force multiplier and a fresh attack surface," said Jeetu Patel, President and Chief Product Officer, Cisco. "At the same time, threat actors are already leveraging AI tools to launch more sophisticated attacks than ever. To help IT and security teams fight back, Cisco is reimagining how we secure networks, protect AI apps and models, manage identity, and equip security teams with the AI tools they need to meet the moment."

Reimagining Zero Trust: Fusing AI-Powered Security into the Network
Robust network security has never been more critical, as enterprises navigate increasingly complex environments characterized by a growing number of applications, a highly-distributed and mobile workforce, and sophisticated AI-driven threats. Adopting a zero-trust security approach – including continuously verifying users, applications, and soon AI agents – is critical to preventing the lateral movement of threats across hybrid environments. Cisco is addressing these challenges with innovative solutions for AI-ready data centers and campus networks, centered on the Cisco Hybrid Mesh Firewall and Universal ZTNA.

Cisco Hybrid Mesh Firewall and Universal ZTNA work together to deliver a robust zero-trust security framework that seamlessly integrates into the network. For zero-trust segmentation, AI application protection and advanced threat protection across diverse environments, including data centers and IoT, Cisco Hybrid Mesh Firewall offers a distributed security fabric. This fabric includes Cisco and third-party firewalls, Cisco Hypershield and Cisco Secure Workload. For secure, identity-driven access for users and devices, regardless of location, Universal ZTNA unifies policy management and extends zero trust principles even to unmanaged devices and IoT.

Together, these solutions secure user-to-application connections and back-end interactions, simplify management through Cisco's Security Cloud Control, and enhance observability with AI-driven insights, empowering organizations to scale securely and protect their digital assets in a complex threat landscape.

Cisco's Hybrid Mesh Firewall is adding hardware as well as new enforcement points and policy management capabilities in Security Cloud Control with its latest innovations:

- **Cisco Secure Firewall 6100 Series:** Addresses complexity, cost, and scalability challenges in AI-ready data centers with the highest performance density for data center firewalling — 200 Gbps per rack unit — and modular scalability**.**
- **Cisco Secure Firewall 200 Series:** Delivers advanced on-box threat inspection and integrated software-defined wide area network (SD-WAN) for distributed branches, at up to 3x price-performance compared to competition.
- **Expanded Enforcement Points:** Cisco Security Cloud Control will extend unified policy management to next generation firewall (NGFW) on Cisco Catalyst SD-WAN (including on the new Cisco 8000 Secure Router Series), Cisco Hypershield-ready C9000 Smart Switches, and Cisco's Application Centric Infrastructure (ACI) data center fabrics.
- **Multi-Vendor Segmentation Policy:** Cisco Security Cloud Control introduces Mesh Policy Engine, enabling teams to define a single intent-based policy that is enforced across Cisco and third-party firewalls. Not only does this simplify day-to-day operations, it also enables organizations to change enforcement points without re-writing policy.

Cisco's Universal ZTNA will also bring customers new innovations that simplify secure connectivity and enhance visibility across hybrid environments and AI agents.

- **Secure Access Service Edge (SASE) Simplified:** All Cisco SD-WAN offerings, including Meraki, now integrate with Cisco Secure Access. This enables customers to choose the optimal branch connectivity while still enjoying a unified security service edge (SSE) policy and consistent enforcement.
- **Frictionless Phishing Resistance:** With the launch of Duo Identity and Access Management (IAM), Duo now acts as an identity broker. With a new complete passwordless option and unique proximity verification capability, Duo layers end-to-end phishing resistance—without clunky hardware tokens—on top of existing identity infrastructure.

Enabling Agentic AI Securely: The emergence of agentic AI is revolutionizing workplaces while introducing critical security and safety challenges. These AI agents autonomously access enterprise resources, make decisions, and act on behalf of users, necessitating robust safeguards. To tackle these pressing issues, Cisco is advancing its Universal Zero Trust architecture to:

- **Secure agentic identities**
- **Enable seamless zero-trust access** to enterprise resources
- **Provide comprehensive tracking** of agent actions

Cisco's vision integrates cutting-edge capabilities, including automated agent discovery, delegated authorization, secure zero trust agentic access, and native support for the Model Context Protocol (MCP).

This approach is powered by Cisco Duo IAM, Cisco Identity Intelligence, Cisco Secure Access, and Cisco AI Defense, unified under a single policy framework in Security Cloud Control. By leveraging these innovations, enterprises can confidently adopt agentic AI, ensuring unparalleled safety and security while maximizing their Cisco Security investments.

"The AI era demands a transformative approach to security. Organizations need distributed, identity-based, zero trust protection for applications, users, AI models and agents, supported by a unified policy framework," said John Grady, Principal Analyst, Enterprise Strategy Group. "Cisco is in a very unique position to support this with its ability to embed advanced protections directly into the network through innovations like Hybrid Mesh Firewall and Universal Zero Trust Network Access, which safeguard AI models and applications, manage identity, and simplify policy management across distributed environments."

"As AI continues to evolve at an unprecedented pace and new cybersecurity challenges emerge, it's even more important to fuse security into the very fabric of the network," said Chris Konrad, Vice President, Global Cyber, World Wide Technology. "Cisco is redefining security for the AI era with its latest innovations from Hybrid Mesh Firewall to Universal Zero Trust Network Access. This integrated approach will help our customers to prepare for an AI-driven future and achieve better outcomes, by protecting AI models and applications, managing identity, and providing essential tools to combat increasingly complex threats."

Splunk Integrations Unlock New Threat Detection, Investigation, and Response Capabilities
As security challenges become more complex, organizations need integrated solutions that enhance visibility, accelerate detection, and streamline response. Advancements between Cisco and Splunk strengthen interoperability across key security workflows. By unifying and enriching data across platforms, these enhancements help security teams respond faster, reduce manual effort, and extract greater value from their security operations. This expanded functionality includes:

- **Surface Insights from Cisco Secure Firewall integrated with Splunk:** Customers using Cisco Secure Firewall will be able to unlock deeper threat insights within Splunk by ingesting firewall log

data. This enables advanced detections and helps security teams maximize the value of their Cisco and Splunk investments.
- **Expanded Threat Detection, Investigation and Response (TDIR) Coverage with Enhanced Detection Integration with Cisco Secure Firewall Threat Defense:** The Cisco Security Cloud App for Splunk now delivers deeper support for Cisco Secure Firewall Threat Defense (FTD), enabling enriched correlation and detection content aligned to TDIR workflows. Combined with telemetry from Cisco AI Defense, Cisco XDR, Cisco Multicloud Defense, Cisco Talos, and other sources, Splunk accelerates detection use cases across hybrid environments.
- **Streamlined TDIR with Security Orchestration, Automation and Response (SOAR) integrations for Cisco Secure Firewall:** Expanded SOAR integrations now include Cisco Secure Firewall-specific actions to support containment and response within TDIR workflows. This is in addition to the currently available Cisco Talos Threat Intel integration. Playbooks can automatically isolate hosts, block outbound connections, and apply policy controls, reducing manual effort and accelerating resolution.
- **Connected Application Risk Signals from Splunk AppDynamics:** By forwarding Secure Application events into Splunk, security teams gain visibility into application-layer vulnerabilities and threats, helping to contextualize findings within broader business risk.

For more information on Cisco's security solutions, visit cisco.com/go/security.

Additional Resources:

- Blog: Making Agentic AI Work in the Real World
- Blog: Cisco Hybrid Mesh Firewall: Better Enforcement Points, Smarter Segmentation, and Multi-Vendor Policy
- Visit the Cisco Newsroom for all Cisco Live 2025 announcements.
- Cisco Customer Experience helps customers get more from their technology investments.
- Cisco Capital payment solutions provide choices – ways to pay for your technology in more than 100 countries.
- Support AI-ready outcomes with new skills training in Cisco U.

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.

Futures Disclaimer: Many of the products and features mentioned are still in development and will be made 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-transforms-security-for-the-agentic-ai-era-further-fusing-security-into-the-network-302477451.html

SOURCE Cisco Systems, Inc.