



NEWS RELEASE

Cisco Security Cloud Vision Comes to Life, Transforming Enterprise Defenses

2024-06-04

With unified solutions across its security portfolio, Cisco brings enhanced security posture to customers fueled by AI and industry partnerships

News Summary

- Industry-first Cisco Hypershield bolsters hardware acceleration to analyze and respond to anomalies in application and network behavior, now supporting AMD Pensando Data Processing Units (DPUs) to be available from Cisco's Unified Computing System (UCS) servers and other leading vendors, and in future service-accelerated switching platforms.
- Best-in-class Cisco Secure Firewall introduces the new Firewall 1200 Series, delivering up to three times the performance of comparable firewalls and eliminating the need to have multiple appliances for switches, routers and firewalls at enterprise branch locations.
- New, AI-native management architecture, Security Cloud Control, will configure, manage and monitor the entire Cisco Security Cloud, beginning now with Cisco's network security solutions.
- New sources of Cisco telemetry through technical add-ons for Splunk will deliver unparalleled visibility to power the SOC of the Future.

LAS VEGAS, June 4, 2024 /PRNewswire/ -- **CISCO LIVE US 2024** -- Cisco (NASDAQ: CSCO), the leader in enterprise networking and security, today announced new capabilities across the Cisco Security Cloud that extend its security architecture in the age of AI. With Cisco's unified, AI-driven, cross-domain security platform, customers will experience the balance of power tipping in favor of the defenders.

"Cisco Security has delivered more innovation in the past year than in the previous decade combined, and this year will be multiples of what we delivered last year," said **Jeetu Patel, Executive Vice President and General Manager for Security and Collaboration at Cisco**. Our announcements today are helping us realize the vision of Cisco Security Cloud, bringing our customers a true security platform for an increasingly complex and hyper distributed world. Bolstered by our partnerships with other titans in the industry, strategic acquisitions and a commitment to an open ecosystem, we are reimaging security for our customers."

Cisco Delivers on Its Vision to Melt Security into the Network

In April 2024, Cisco announced Cisco Hypershield, a brand new security architecture designed to defend modern, AI-scale data centers. Architected to seamlessly incorporate new enforcement points into its fabric, Hypershield embeds security enforcement in virtual machines or Kubernetes clusters in public clouds using an open-source technology called eBPF. It is also architected to insert security enforcement into advanced silicon in servers and networking devices such as switches. Today, Cisco is taking a big step forward towards realizing its vision by announcing Cisco Hypershield support for AMD Pensando DPUs, with targeted availability in Cisco Unified Computing System (UCS) servers and from other leading server vendors by the end of 2024.

"We are thrilled to collaborate with Cisco to integrate AMD Pensando DPUs with Cisco Hypershield. This partnership brings together AMD's cutting-edge hardware acceleration technology and Cisco's advanced security solutions, enabling enterprises to achieve unparalleled network security performance and flexibility," said **Soni Jiandani, General Manager, Networking Technology and Solutions Group, AMD**. "By leveraging our DPUs in customer servers or in future Cisco networking platforms, Hypershield users can enjoy high-capacity throughput and intelligent policy enforcement without compromising on workload performance. This collaboration represents a significant step forward in delivering robust, scalable, and efficient security solutions for private cloud environments."

Building on this momentum, Cisco is also announcing support for Intel infrastructure processing units (IPUs) with availability to be announced in the future.

"We are pleased with the advancement of our collaboration with Cisco that combines the cutting-edge infrastructure acceleration of Intel IPUs with the breakthrough Cisco Hypershield architecture," said **Pere Monclus, Chief Technology Officer, Network and Edge Group at Intel**. "This powerful combination marks a significant leap forward, helping to enable enterprises to realize an AI-driven, distributed security architecture that seamlessly goes from the cloud, to datacenters, to the edge with high performance and energy efficiency."

The Best Next Generation Firewall is Now Even Better

For the second year running, SE Labs [named](#) the Cisco Secure Firewall the best next generation firewall. Today, Cisco is advancing its market leadership with the introduction of the **Cisco Firewall 1200 Series**, delivering up to three times the performance of comparable competitive firewalls. The 1200 Series is a new family of SD-WAN enabled, high-performing, compact firewall security appliances that eliminate the need to have multiple appliances for switches, routers and firewalls at enterprise branch locations. The first models in the series are targeted for availability in October 2024.

Cisco is also announcing the new **software 7.6 version of Firewall Threat Defense (FTD)**, available for all of Cisco's physical and virtual firewalls. FTD 7.6 not only enhances security by using AI to prevent zero-day threats and extends application control to over 70 generative AI apps to secure sensitive information but also streamlines branch network rollouts with pre-built SD-WAN and firewall templates and supports zero-touch provisioning.

Taking another giant leap, Cisco is introducing **Cisco Security Cloud Control** to unify management for the Cisco Security Cloud, beginning with its network security fabric including Cisco Secure Firewall. Going beyond AI assistants, Security Cloud Control delivers an AI-native approach to proactively surface actionable insights and automate resolution across hybrid environments. Customers benefit from simpler, more streamlined policies while getting the most out of their Cisco Security investment with optimal configuration. Unified management with Security Cloud Control is targeted for initial availability in September 2024 with support for Secure Firewall Threat Defense, Secure Firewall ASA, Multicloud Defense, and Hypershield.

"We are very excited about the platform level innovation Cisco is bringing to market with the Security Cloud. Where security meets the network is a massive opportunity for our customers," said **Chris Konrad, Vice President, Global Cyber, World Wide Technology**. "The promise of what Cisco Hypershield will deliver is a game-changer for how our customers will be able to close the exploit gap and achieve segmentation that adapts and learns. Along with new AI-powered management through Security Cloud Control and the quality innovation we continue to see in Cisco's firewall portfolio, we are able to deliver an unparalleled customer outcome coupled with our services capabilities and expertise."

Better Telemetry Means a Better Security Operations Center (SOC) of the Future

Security companies today also need to be AI companies, and that requires data. As the creator of the network, Cisco has unmatched visibility across its customer's IT environments. Embracing that notion and building on the recently [announced](#) integration of Cisco Extended Detection and Response (XDR) and Splunk Enterprise Security, Cisco continues to unify its portfolio of solutions to deliver the promise of the SOC of the Future, powered by Cisco's unparalleled telemetry to better detect lateral movement.

- **Splunk + Cisco Security Cloud:** Security Operations teams can fully leverage the telemetry and alerts from the Cisco Security Cloud as part of a unified threat detection, investigation, and response workflow in Splunk. The new Cisco Security Cloud Technology Add-on (TA) for Splunk is a simple, reliable way to get a broad range of Cisco Security Cloud telemetry and analytics outcomes into Splunk. Cisco Duo and Secure Malware Analytics are available now, with additional sources to be added in the coming months.
- **Cisco XDR + Cisco Meraki MX:** Customers will be able to quickly and easily see and stop network-based attacks with a new, native integration coming soon to deliver network telemetry from Meraki MX appliances directly to Cisco XDR. With just a few clicks, Cisco XDR can begin analyzing network telemetry across even highly distributed organizations and correlating it with other telemetry to prioritize active threats.

"Organizations of all sizes continue to be challenged on the security front. Generative AI is enabling bad actors with new capabilities to launch widescale automated attacks, compose grammatically correct and realistic phishing emails and orchestrate deep fakes that challenge identity access management platforms. The combined power of Splunk and Cisco Security Cloud could serve as a transformative leap for defenders in mitigating collateral damage," said **Will Townsend, Vice President and Principal Analyst, Moor Insights & Strategy**. "Cisco is already demonstrating early integrations of Splunk that weave advanced analytics and AI into a cloud-delivered security architecture that has the potential to level the cybersecurity playing field."

"Network telemetry is consistently ranked in the top three most valuable security signals," said **Dave Gruber, Principal Analyst, Enterprise Strategy Group**. "Native integration between Cisco XDR and Meraki MX strengthens detection and investigation capabilities, while simplifying deployment and management. This will be especially helpful for lean IT and distributed organizations. The convergence of network and security operations sets the stage for the SNOC of the Future."

Integrated and Open Security Ecosystem

In today's world where the threat landscape is rapidly evolving, the call from organizations for an integrated and open security ecosystem is louder than ever. Cisco Security Cloud was built to deliver better security outcomes for customers by avoiding dependence on a single vendor, optimizing instead to partner with other industry titans against a common adversary: the malicious actor.

Furthering this mission and differentiation with a robust technology ecosystem, today Cisco announced its latest collaboration with Google. Cisco is working with Google to bring browser-based

threat and data protection from **Chrome Enterprise to web apps secured by Cisco Secure Access**. As more modern work happens on the web, a secure enterprise browser strengthens and simplifies endpoint security as part of broader zero trust initiatives.

"Cisco shares our vision for a more holistic zero trust architecture that is better for users and easier for the IT team to deploy and manage," said **Sunil Potti, General Manager and Vice President of Cloud Security at Google Cloud**. "We are excited to work together to deliver a combination of browser-based and cloud-based protection that results in a secure and frictionless user experience."

This work builds on the successful [integration](#) between Chrome Enterprise and Cisco Duo to enable end-to-end zero trust access, including device trust, strong authorization, and secure access for applications on both managed and unmanaged devices. Together, the companies are committed to delivering innovative security solutions that address today's evolving landscape.

Cisco protects 100% percent of the Fortune 100. To learn more, visit cisco.com/go/security.

Additional Resources

- [Blog: Cisco Security at Cisco Live 2024: Innovating at Scale](#)

View original content to download multimedia: <https://www.prnewswire.com/news-releases/cisco-security-cloud-vision-comes-to-life-transforming-enterprise-defenses-302163429.html>

SOURCE Cisco Systems, Inc.