Cisco is Delivering on Platform Strategy with Rapid Innovation Across Cisco Security Cloud

2024-05-06

Building on the momentum of Cisco Hypershield and the acquisition of Splunk, Cisco is reimagining security at AI-scale

News Summary:

- Cisco and Splunk are helping customers accelerate their journey toward the Security Operations Center (SOC) of the future with a powerful integration just two months after Cisco's acquisition of Splunk.
- With the industry's first AI-native security architecture, customers will be able to protect against both known and unknown attacks using Cisco Hypershield.
- Cisco Identity Intelligence is now available in Cisco Duo to enable Continuous Identity Security to protect organizations against the sharp rise in identity-based attacks.

SAN FRANCISCO, May 6, 2024 /PRNewswire/ -- **RSA CONFERENCE 2024 --** Cisco (NASDAQ: CSCO), the leader in enterprise networking and security, today announced new industry-shaping innovations across the Cisco Security Cloud to both power and protect the AI revolution. The new capabilities across Cisco's unified, AI-driven, cross-domain security platform help companies better protect their applications, devices, users and data as well as detect, respond and recover faster from incidents.

Securing today's complex, hyper-distributed digital landscape can no longer be done at human scale, as attacks become more sophisticated and nearly 90 percent of companies around the world say shortage of cybersecurity talent is a real issue, according to the [2024 Cisco Cybersecurity Readiness Index](). Organizations need to rethink security by building natively with AI and challenging long held conventions to tip the advantage in favor of the defenders.

"At the RSA Conference last year, we delivered enhanced customer efficacy and economics through a true platform approach to security with the Cisco Security Cloud. By minimizing point-solutions, customers have realized better end-to-end visibility, uncovered actionable intelligence and automation

with AI and simplified management with Cisco's unified security infrastructure," said **Jeetu Patel, Executive Vice President and General Manager for Security and Collaboration at Cisco.** "Since then, our security momentum continues to accelerate. With 'zero to one' innovation like Cisco Hypershield and strategic acquisitions like Splunk and Isovalent, the power of Cisco's security platform is supercharged and unmatched."

Cisco is helping customers defend against the entire attack chain – from detecting and blocking not just known, but also unknown vulnerabilities with Cisco Hypershield, to stopping the increasing barrage of identity attacks with Cisco Duo, and reimagining the security operations center (SOC) with Splunk for security analysts to move faster and make more informed decisions with contextual insights and automated workflows.

Advancing the Vision of the SOC of the Future

To thrive in the new digital era, organizations need to connect and protect all that they do. The combination of Cisco and Splunk is the most comprehensive security solution for threat prevention, detection, investigation and response for organizations of any size, utilizing cloud, endpoint traffic - along with Cisco's unmatched network footprint - for unparalleled visibility. As Cisco and Splunk converge these platforms, there are many opportunities to advance security operations including:

- **Integrating Cisco Extended Detection & Response (XDR) with Splunk Enterprise Security (ES):** Seamlessly feed high-fidelity alerts and detections from Cisco XDR, purpose-built to detect today's most common attacks such as ransomware and lateral movement, into Splunk ES to accelerate investigation and remediation. The integration allows organizations to utilize the strength of each solution to create a more comprehensive defense strategy that will improve digital resilience.
- **Splunk Asset and Risk Intelligence:** A critical solution for the SOC of the future, designed to revolutionize proactive risk mitigation through continuous asset discovery and compliance monitoring. This addresses a pressing need for security teams, as they can't protect what they can't see.
- **Cisco AI Assistant for Security in XDR**: Cisco's unified AI Assistant for Security is now available in Cisco XDR – one year after Cisco shared its vision for reimagining the security analyst experience with AI on-stage at RSAC 2023. The AI Assistant in XDR empowers security analysts of all skill levels to make faster, more informed decisions about evolving threats by offering contextual insights, guided responses, recommended actions and automated workflows.
- **New Cloud Detection and Response Capabilities:** Cisco's Panoptica cloud native application protection platform (CNAPP) now harnesses AI and ML to detect and alert security teams to emerging threats within cloud applications in real-time, while GenAI Dynamic Remediation allows teams to resolve issues quickly by providing prescriptive guidance. The new Search Graph Query feature enables granular query and graph visualizations across multi-cloud environments to allow for deeper investigation into cloud security posture to reduce exposure.

"The XDR market is broad, one that includes many companies that promise to deliver a more complete view of the security stack beyond the endpoint. In doing so, XDR aims to detect cybersecurity threats across multiple domains," said **Will Townsend, VP & Principal Analyst, Moor Insights**. "Observability is key, and with its successful acquisition of Splunk, Cisco is poised to enhance its XDR solution launched one year ago, now adding AI, unified threat detection, investigation, response and transformation capabilities aimed at enhancing security operations."

"At Optiv, we provide our clients the essential security expertise and solutions they need with an integrated approach that spans the entirety of their cybersecurity journey, all with a focus on accelerating their business outcomes," said **John Hurley, Chief Revenue Officer, Optiv**. "Cisco's integrated AI-driven platform, the Cisco Security Cloud, is a solution that helps reduce complexity. The

integration of Cisco XDR and Splunk Enterprise Security will enable our clients to operate efficiently while making informed decisions on how to bolster their cyber resiliency in today's evolving threat landscape."

Protections From Unknown Vulnerabilities with Cisco Hypershield for the AI-Scale Data Center

In today's attack landscape, the time from vulnerability to exploit is shrinking - and defending against the increasingly sophisticated, complex threats in data centers is beyond human scale. Unfortunately, not all vulnerabilities are known.

Building on last month's launch of [Cisco Hypershield](#) with Distributed Exploit Protection protecting against known vulnerabilities (e.g. CVEs), Cisco is now introducing capabilities to detect and block attacks stemming from **unknown vulnerabilities** within runtime workload environments. In addition, suspected workloads can be isolated to limit the vulnerability's blast radius.

Cisco Hypershield is a radically new approach to securing data centers and clouds in response to the increasing demands the AI revolution has put on IT infrastructure. Cisco Hypershield protects applications, devices and data across public and private data centers, clouds and physical locations - anywhere customers need it. Designed and built with AI in mind from the start, Hypershield enables organizations to achieve security outcomes beyond what has been possible with humans alone.

Frictionless User Protection with Continuous Identity Security

With the rise in identity-based attacks, security solutions must evolve from just asking 'can' a user access an application. Instead, they need to continuously assess whether a user 'should' be able to do what they are doing – and do so without creating friction for the user. Continuing momentum since the recent launch of [Cisco Identity Intelligence,](#) Cisco is bringing together phishing-resistant capabilities in Duo to realize its vision for Continuous Identity Security – stopping identity attacks while simultaneously delivering a simpler, more seamless user experience.

- **Eliminate Authentication Fatigue with Duo Passport:** Minimize repeated authentication requests to provide interruption-free access to everything a workforce needs without compromising security using Duo Passport, a major leap forward in user experience.
- **Cisco Identity Intelligence in Duo**: Leverage powerful AI-driven analytics to strengthen posture across your workforce identity infrastructure and to assess and respond to identity risk before, during and after login. Now in limited availability, this addition enables customers to implement Continuous Identity Security that reduces security gaps and addresses today's most common cyber threat.

"Cisco Duo is advancing past its core access management functions, incorporating identity enrichment from Cisco Identity Intelligence and introducing a streamlined access experience with Duo Passport," said **Todd Thiemann, Senior Analyst, Enterprise Strategy Group.** "This evolution leads to Continuous Identity Security, where access adapts in real-time to the associated risk, crucial in today's threat landscape where identity-based attacks are on the rise Cisco Duo's commitment to dynamic response to risk, coupled with an emphasis on seamless user experience, is not just timely-it's groundbreaking."

Cisco protects 100% percent of the Fortune 100. To learn more, visit [cisco.com/go/security](#).

Additional Resources

- News Release: [Splunk Unveils Asset and Risk Intelligence to Revolutionize Proactive Risk Mitigation](#)
- Blog: [Cisco & Splunk: A Complete SOC Platform Purpose-Built for the AI-Driven Future](#)
- Blog: [Cisco Hypershield - Our Vision to Combat Unknown Vulnerabilities](#)
- Blog: [Authentication Alone is Failing: Introducing Continuous Identity Security](#)
- Blog: [Outshift Leads the Way with AI at RSA Conference 2024](#)

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide technology leader that securely connects everything to make anything possible. Our purpose is to power an inclusive future for all by helping our customers reimagine their applications, power hybrid work, secure their enterprise, transform their infrastructure, and meet their sustainability goals. 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-is-delivering-on-platform-strategy-with-rapid-innovation-across-cisco-security-cloud-302136571.html

SOURCE Cisco Systems, Inc.