NEWS RELEASE

Cisco Unveils New Solution to Rapidly Detect Advanced Cyber Threats and Automate Response

2023-04-24

News Summary:

- With unmatched visibility across the network and endpoint, Cisco Extended Detection and Response (XDR) simplifies security operations in today's hybrid, multi-vendor, multi-threat landscape.
- Cisco XDR prioritizes and remediates security incidents more efficiently using evidence-backed automation.
- To protect against multi-factor authentication (MFA) attacks, Cisco is now offering advanced features in all editions of Duo, the most secure, cost-effective, and user-friendly access management solution on the market.

SAN FRANCISCO, April 24, 2023 /PRNewswire/ -- **RSA CONFERENCE 2023 --** Cisco (NASDAQ: CSCO), the leader in enterprise networking and security, unveiled the latest progress towards its vision of the Cisco Security Cloud, a unified, AI-driven, cross-domain security platform. Cisco's new XDR solution and the release of advanced features for Duo MFA will help organizations better protect the integrity of their entire IT ecosystem.

Threat Detection and Response

Cisco's XDR strategy converges its deep expertise and visibility across the network and endpoints into one turnkey, risk-based solution. Now in Beta with General Availability coming in July 2023, Cisco XDR simplifies investigating incidents and enables security operations centers (SOCs) to immediately remediate threats. The cloud-first solution applies analytics to prioritize detections and moves the focus from endless investigations to remediating the highest priority incidents with evidence-backed automation.

"The threat landscape is complex and evolving. Detection without response is insufficient, while response without detection is impossible. With Cisco XDR, security operations teams can respond and remediate threats before they have a chance to cause significant damage," said **Jeetu Patel, Executive Vice President and General Manager of Security and Collaboration at Cisco.** "Cisco continues to ensure that 'if it's connected, you're also protected.' We are uniquely positioned to deliver integrated solutions that simplify securing today's increasingly complex, hybrid multi-cloud environments without compromising user experience."

While traditional Security Information and Event Management (SIEM) technology provides management for log-centric data and measures outcomes in days, Cisco XDR focuses on telemetry-centric data and delivers outcomes in minutes. It natively analyzes and correlates the six telemetry sources that Security Operations Center (SOC) operators say are critical for an XDR solution: endpoint, network, firewall, email, identity, and DNS. On the endpoint specifically, Cisco XDR leverages insight from 200 million endpoints with Cisco Secure Client, formerly AnyConnect, to provide process-level visibility of where the endpoint meets the network.

"The true measure of XDR is its ability to deliver actual security outcomes, real and measurable benefit to organizations — early detection, impact prioritization, and effective and efficient response," said **Frank Dickson, Group Vice President, Security & Trust, IDC.** "True results need to be quantifiable numerically and not just qualitatively described with words. Cisco XDR delivers a clear framework for enabling organizations to achieve such tangible outcomes."

In addition to Cisco's native telemetry, Cisco XDR integrates with leading third-party vendors to share telemetry, increase interoperability, and deliver consistent outcomes regardless of vendor or technology. The initial set of out-of-the-box integrations at general availability include:

- **Endpoint Detection and Response (EDR)**: CrowdStrike Falcon Insight XDR, Cybereason Endpoint Detection and Response, Microsoft Defender for Endpoint, Palo Alto Networks Cortex XDR, SentinelOne Singularity, Trend Vision One
- **Email Threat Defense:** Microsoft Defender for Office, Proofpoint Email Protection
- **Next-Generation Firewall (NGFW):** Check Point Quantum, Palo Alto Networks Next-Generation Firewall
- **Network Detection and Response (NDR):** Darktrace DETECT™ and Darktrace RESPOND™, ExtraHop Reveal(x)
- **Security Information and Event Management (SIEM):** Microsoft Sentinel

"Throughout Logicalis' decades-long pursuit to becoming a world class integrator; we have recognized the impact extensibility can have on the viability and efficacy of any solution," said **Brad Davenport, Vice President of Technical Architecture, Logicalis**. "With the launch of Cisco XDR, we can finally provide our customers with XDR outcomes as a solution or managed offering. We see this as a natural progression for us along the security maturity journey. Logicalis is very excited to put our combined expertise to work for our clients and offer Cisco XDR to help them achieve their business outcomes."

Zero Trust and Access Management

As attackers increasingly target gaps in weaker multi-factor authentication (MFA) implementations, Cisco is redefining what is essential for access management. Every business needs three key pillars for its access management strategy: enforcing strong authentication, verifying devices, and reducing the number of passwords in use. This is why, beginning on May 1st, Cisco is adding Trusted Endpoints to all its paid Duo Editions. Previously just available in Duo's highest tier, Trusted Endpoints allows only registered or managed devices to access resources. By delivering Trusted Endpoints alongside Single Sign On, MFA, Passwordless, and Verified Push within the entry-level Duo Essentials edition, Cisco is delivering the most secure, cost-effective, and user-friendly access management solution on the market.

To learn more, visit Cisco.com/go/security.

Supporting Quotes

"Darktrace DETECT and RESPOND, parts of the Darktrace Cyber AI Loop, can quickly contain and disarm threats, whether known or unknown, and with a high degree of fidelity. Our collaboration with Cisco will provide our mutual customers with added visibility into security incidents and actions across cloud, network and OT," said **Mattheus Bovbjerg, Vice President of Integrations, Darktrace.** We look forward to expanding this collaboration to additional coverage areas including email and SaaS applications in the future."

"As organizations embrace the network as the essential source for cybertruth, our partnership with Cisco offers enterprises the ability to integrate ExtraHop with best-of-breed products for a more comprehensive view of their IT environments," said **Jesse Rothstein, Chief Technology Officer and Co-Founder, ExtraHop**. "Joint customers will benefit from ExtraHop's enterprise-grade, high–fidelity detections with network decryption and support for more than 80+ protocols, while also seamlessly integrating with log and endpoint solutions to achieve more streamlined investigations."

"SentinelOne is excited to team with Cisco to deliver market-leading solutions that allow our joint customers to push the boundaries of security," said **Akhil Kapoor, Vice President of Technology Partnerships and Business Development, SentinelOne**. "We look forward to integrating our EDR and Cloud Workload Protection (CWPP) solutions with Cisco to help organizations of all sizes secure tomorrow today."

"Our vision for XDR is to provide customers with a comprehensive, consolidated view of their security posture, enabling them to respond to threats quickly and effectively," said **Mike Gibson, Senior Vice President of Global Services and Customer Success, Trend Micro**. "The integration with Cisco XDR is a significant step forward in the evolution of cybersecurity. By leveraging the strength of both solutions, we are able to offer our customers a unified solution that expands telemetry insights to gain a greater perspective of their security environment enabling them to detect threats faster and respond more effectively."

Additional Resources

- **Blog**: XDR and the Importance of Cross-Domain Correlated Telemetry
- **Blog**: Simplify Your Security Operations with Cisco XDR, Launching at RSAC
- **Blog**: Raising the Bar: Duo Redefines What is Essential for Access Management

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide leader in technology that powers the Internet. Cisco inspires new possibilities by reimagining your applications, securing your data, transforming your infrastructure, and empowering your teams for a global and inclusive future. Discover more on The Newsroom and follow us on Twitter at @Cisco.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

View original content to download multimedia:https://www.prnewswire.com/news-releases/cisco-unveils-new-solution-to-rapidly-detect-advanced-cyber-threats-and-automate-response-301805174.html

SOURCE Cisco Systems, Inc.