



NEWS RELEASE

Cisco CEO Addresses World's Largest Cybersecurity Conference: "Security Must Be Simple, Intelligent and Everywhere"

2021-05-17

SAN JOSE, Calif., May 17, 2021 /PRNewswire/ -- RSA Conference 2021 --

News Summary:

- Cisco unveils innovations that radically simplify security across devices, networks, applications and data with expanded Extended Detection & Response (XDR) capabilities in the SecureX platform.
- Cisco delivers on Secure Access Service Edge (SASE) vision with enhanced threat protection in the cloud.
- Cisco redefines network security, introduces the industry's first integrated firewall and application workload protection for dynamic environments.

"Security has to be at the heart of everything in the new world we live in," said Cisco Chairman and CEO Chuck Robbins

Cisco, the leader in enterprise security, today unveiled innovations to further its journey to radically simplify and deliver end-to-end security, across users, devices, networks, applications and data. Announcements today improve Extended Detection and Response (XDR) with greater visibility across network, endpoint and cloud. New innovations expand Cisco's vision for Secure Access Service Edge

(SASE) with enhanced threat detection in the cloud and redefine and simplify network security. Cisco continues to simplify customers' security, network and IT operations - empowering organizations to embark securely on digital transformation.

The world has shifted towards a more distributed workforce, and with recent global events, hybrid work is here to stay. Users now expect to connect from anywhere and on any device, while security teams have the same complex, piecemeal and time-consuming solutions. It is time to rethink security.

"Security has to be at the heart of everything in the new world we live in. We believe it needs to be done with a platform approach that is simple, comprehensive and based on intelligence," said Cisco Chairman and CEO Chuck Robbins, addressing the virtual RSA Conference audience. "There is really no perimeter in the enterprise to defend anymore. We need visibility across endpoints, users and applications as well as securing critical control points with continuous passwordless authentication."

Improving Visibility and Simplifying Extended Detection and Response (XDR)

The erosion of the network perimeter and transition to work-from-anywhere have conspired to expose endpoint devices, users and applications to threats more so than ever before. Organizations continue to struggle with extending visibility and protection to endpoints, with more than 40 percent globally reporting a major security incident in the last two years, according to the new **Cisco Security Outcomes Study: Endpoint Edition**. Organizations that do not prioritize integrated solutions were almost twice as likely to have suffered a major security event. In response, Cisco continues to expand its XDR capabilities, integrating multiple security control points and applying analytics and automation to reduce customers' time to detection and response. Cisco today announced:

- **Industry-leading Vulnerability Management with Kenna Security:** Cisco will combine threat and risk-based vulnerability management as part of the SecureX platform with its announcement of [intent to acquire Kenna Security](#). This integration will help customers prioritize vulnerabilities, speed and automate decision making with tailored information, and accelerate response time for cyber readiness.
- **SecureX Device Insights:** Customers can quickly consolidate their device inventory from multiple sources within the SecureX platform to provide unsurpassed visibility and context for IT operations (ITOps) and security operations (SecOps) as well as automated threat enrichment and response.
- **Simplified Transition to XDR from EDR:** As the only endpoint security solution with a built-in platform, SecureX continues to help customers simplify the move from Endpoint Detection and Response (EDR) to XDR with more than 30 pre-built workflows, 40 turnkey integrations and new orchestration capabilities. In addition, Cisco Secure Client, our single agent across user, cloud and endpoint protection, enables faster XDR while reducing agent fatigue.
- **Expanded Investigation and Quicker Response:** Cisco Secure Endpoint's advanced search technology now bolsters XDR value, offering more than 200 endpoint queries out-of-the-box to get real-time answers to support investigations, threat hunting, and IT Ops use cases such as tracking artifacts about endpoints.

"Organizations are increasingly looking to adopt end-to-end security architectures to support this new way of working, and we think it's critical to take a platform approach to simplify security, network, and IT operations as customers embark on digital transformation," said Gee Rittenhouse, SVP and General Manager, Cisco Secure. "Since it was launched last year at RSA, more than 7,000 customers are using Cisco's SecureX platform to unlock value from existing security solutions and accelerate their migration to XDR."

"SecureX device insights provides an instant view of all the endpoints and devices with details needed to assess compliance and health of all assets in my environment," said John DePalma, Cybersecurity Engineer, Sentara Healthcare. "SecureX device insights delivers welcome help to gain momentum on our Zero Trust journey at Sentara."

Delivering on a SASE Vision with Enhanced Cloud Security

Today's distributed and hybrid workforce necessitates delivering protection and performance wherever employees access the internet or cloud applications. Cisco's SASE architecture integrates

multiple security and networking functions into a single, secure connectivity offer. This significantly simplifies security and reduces the cost, time, and resources previously required for deployment, configuration, and integration. Continuing to deliver on its **SASE vision**, Cisco today announced:

- **Rapid Deployment of Cloud Security across SD-WAN:** New integration between Cisco Umbrella and Cisco SD-WAN powered by Meraki extends the SD-WAN fabric to the cloud with the click of a button and includes intelligent path selection to enable customers with secure access and the best user experiences when connecting to cloud applications.
- **Intrusion Prevention System (IPS) in cloud-delivered firewall:** Umbrella's cloud-delivered firewall now includes an additional layer of protection with Snort 3 IPS, backed by Cisco Talos, one of the largest commercial threat intelligence teams in the world.
- **New Packages for Best Protection and Value:** Umbrella's new Secure Internet Gateway (SIG) Advantage package reduces the complexities of purchasing and unifying point solutions by offering a complete set of security capabilities in a single subscription.

Redefining and Simplifying Network Security

Constantly changing application environments make network security more complex. Modern continuous integration and continuous delivery (CI/CD) applications necessitate tighter coordination among developers, security, and network teams to ensure application environments and workloads are secure, firewalls are appropriately configured, and policies are integrated. Otherwise, vulnerabilities and misconfigurations in these constantly changing environments leave doors open for potential threat actors. Redefining and simplifying **network security**, Cisco today announced:

- **Industry-first Integrated Network and Workload Security:** Cisco Secure Workload dynamically informs Cisco Secure Firewall of required policy changes and provides comprehensive visibility and control, no matter where applications are located.
- **Upgraded Threat Defense:** Secure Firewall Threat Defense 7.0, delivers better efficacy with Snort 3 IPS, the world-leading threat protection platform which defined next generation intrusion prevention systems (NGIPS). Snort is now deployed across 800K+ Cisco devices, and the open-sourced Snort engine has seen over 8M+ downloads with 750K+ active users. It includes the flexibility to create robust policies in dynamic environments where fixed IP addresses don't exist, and performance gains up to 30 percent on most appliances. (Snort 3 is also now featured in Cisco SD-WAN powered by Meraki and Umbrella.) The addition of the SecureX ribbon to Secure Firewall Management Center also further simplifies detection and response.
- **Introducing Cisco Secure Firewall Cloud Native:** Purpose-built for Kubernetes environments, Cisco Secure Firewall Cloud Native is developer-friendly, and the most elastic firewall Cisco has ever built.

"At ePlus we strive to deliver effective, integrated cybersecurity centered on mitigating business risk," said Lee Waskevich, Vice President of Security at ePlus Technology, Inc. "Cisco is building on a strong portfolio and continues to innovate how they deliver a holistic platform approach focused on reducing complexity, and integrating security across the network, endpoints, users, apps and cloud through SecureX. As a Gold Master Certified Security Partner, ePlus is excited to partner with Cisco and help our customers recognize the advantages SecureX brings to their security operations."

To learn more about Cisco's solutions to simplify security, visit cisco.com/go/security.

Additional resources:

- Blog: [Reflecting on a Year of Simplify Security with Cisco SecureX](#)
- Blog: [Cisco Empowers the Endpoint to be More Efficient and Effective](#)
- Blog: [Rapidly Executing on SASE Vision with New Cloud Security Enhancements](#)

- Blog: [NetWORK: Redefining Network Security](#)
- Report: [2021 Security Outcomes Study: Endpoint Edition](#)
- News Release: [Cisco Announces Passwordless Authentication by Duo](#)

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 Network 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.

View original content to download multimedia: <http://www.prnewswire.com/news-releases/cisco-ceo-addresses-worlds-largest-cybersecurity-conference-security-must-be-simple-intelligent-and-everywhere-301292603.html>

SOURCE Cisco Systems, Inc.