NEWS RELEASE

Global Cisco Study Identifies Top Security Practices to Detect Threats and Ensure Business Resiliency

2021-12-07

News Summary:

- Organizations that proactively test their security capabilities are 2.5 times more likely to maintain business resiliency
- Integrated technology with high levels of automation increases productivity and improves threat detection capabilities by more than 40 percent
- The Asia Pacific, Japan and China (APJC) region leads in both zero trust and secure access service edge (SASE) adoption globally

SAN JOSE, Calif., Dec. 7, 2021 /PRNewswire/ -- Today, Cisco released its latest cybersecurity report, Security Outcomes Study Volume 2, surveying more than 5,100 security and privacy professionals across 27 markets to determine the most impactful measures teams can take to defend their organizations against the evolving threat landscape. Respondents shared their approaches to updating and integrating their security architecture, detecting and responding to threats and staying resilient when disaster strikes.

Cisco's Security Outcomes Study, Volume 2 takes the guesswork out of prioritizing security strategies and technologies

Last year's study revealed that five practices had an outsized influence on the overall health of an organization's security program. These include proactively refreshing outdated technology; well-integrated security technologies; timely incident response; prompt disaster recovery; and investing in accurate threat detection capabilities. This year's study analyzed those top five practices more closely to identify success factors. Highlights of these findings include:

Updating and Integrating Architecture

- Investing in a proactive technology refresh strategy is more important than ever, as on average 39 percent of security technologies used by organizations are considered outdated.

Unsurprisingly, organizations with cloud-based architectures are more than twice as likely to refresh than those with more outdated, on-premises technologies.
- Organizations with integrated technologies are seven times more likely to achieve high levels of process automation. Additionally, these organizations boast more than 40 percent stronger threat detection capabilities.
- More than 75 percent of security operations programs that do not have strong staffing resources are still able to achieve robust capabilities through high levels of automation. Automation more than doubles the performance of less experienced staff, supporting organizations through skills and labor shortages.

Detecting and Responding to Threats

- The value of cloud-based security architectures cannot be understated. Organizations that claim to have mature implementations of Zero Trust or Secure Access Service Edge (SASE) architectures are 35 percent more likely to report strong security operations than those with nascent implementations.
- Organizations that leverage threat intelligence move twice as fast to repair damage caused by security threats, than organizations that do not use threat intelligence.

Staying Resilient When Disaster Strikes

- As the threat landscape continues to evolve, testing business continuity and disaster recovery capabilities regularly and in multiple ways is paramount, with proactive organizations 2.5 times more likely to maintain business resiliency.
- Organizations with board-level oversight of business continuity and disaster recovery efforts that have operations residing within cybersecurity teams perform best.

"With the shift to hybrid work, organizations are grappling with the increased complexity of securing a distributed workforce," said Shailaja Shankar, SVP and GM of Cisco's Security Business Group. "At the same time, they are also dealing with limited staff and budget constraints, so it's critical for organizations to invest in innovative technologies and security practices. Cisco's Security Outcomes Study, Volume 2 takes the guesswork out of prioritizing security strategies and technologies. By investing in cloud-based, integrated security architectures with high automation, practitioners can respond to threats faster, so they can focus on enabling the business and keeping users safe."

To learn more, visit cisco.com/go/SecurityOutcomes2. Join the conversation using #SecurityOutcomes.

Additional Resources:

- Report: Cisco's Security Outcomes Study, Volume 2
- Blog: Presenting the Security Outcomes Study, Volume 2
- Newsroom: The Fab Five: A practical guide to what works in security

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 Network and follow us on Twitter.

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/global-cisco-study-identifies-top-security-practices-to-detect-threats-and-ensure-business-resiliency-301438434.html

SOURCE Cisco Systems, Inc.