Two-Thirds of Businesses Are Exploring SASE to Address Hybrid Work Security Challenges

January 14, 2025

Employees named number one risk to network security, Hughes and Cybersecurity Insiders found

GERMANTOWN, Md., Jan. 14, 2025 /PRNewswire/ -- Hughes Network Systems, LLC, an EchoStar company (Nasdaq: SATS), today released the 2025 State of Secure Network Access Report, exploring how businesses are adapting cybersecurity strategies to combat emerging cyber threats and ensure ubiquitous connectivity in a hybrid world. Critically, employees were highlighted as the No. 1 user group posing the greatest threat to network security—demonstrating the importance of evolving cyber strategies alongside the modern workforce.

In partnership with Cybersecurity Insiders, Hughes surveyed over 400 IT leaders and cybersecurity professionals, examining the use of Hughes offerings like Secure Access Service Edge (SASE), Security Service Edge (SSE), and Zero Trust frameworks to strengthen hybrid security. The survey also considers the value of tapping Managed Security Service Providers (MSSPs) like Hughes to fill gaps and elevate security, with 47% of respondents citing a lack of in-house expertise to successfully implement innovative security solutions.

"Traditional IT models are struggling to keep up with the complexity of today's distributed enterprises," said Dan Rasmussen, senior vice president and general manager, Enterprise Division, Hughes. "As organizations expand across geographies and manage a mix of on-site, hybrid, and remote operations, ensuring secure and seamless connectivity has become a top priority. Hughes is committed to supporting business performance through solutions and actionable insights that guide IT teams through the challenges of securing a dispersed network landscape."

Adapting IT strategies for a hybrid world

The average workforce is becoming more complex. Employees need to be able to connect to the network from anywhere, anytime, and on different devices. Meeting these needs requires a new approach to IT networks and, by extension, their MSSPs.

Sixty-three percent of respondents said they use a hybrid work model, with an additional 19% operating fully remote. This shift in workforce distribution has brought new challenges in ensuring safe connectivity organization-wide, including increased latency, reduced network performance, and increased complexity that reduces the overall user experience. These are the issues that distributed enterprises are looking to SASE to help resolve.

With a distributed workforce, organizations have turned to Zero Trust—a core tenet of SASE—to implement strategies to secure the expanse of their network. A Zero Trust framework that emphasizes continuous verification of identities and devices. Zero Trust is already being implemented by 38% of respondents with an additional 42% planning to implement within the next 12 months. This growth is indicative of key strategic shifts happening in a world where networks and devices exist beyond four walls.

A growing commitment to security solutions

At this time, only 8% of respondents have fully implemented SASE solutions, creating a cohesive security model. While 32% are in the process of implementing and 31% are evaluating the potential, organizations must act swiftly to adopt these solutions to safeguard their network throughout the distributed workforce.

Notably, respondents highlighted remote work as the top driver (45%) for adopting SASE solutions. This was followed closely by enhancing cloud security and visibility (42%) and implementing a Zero Trust security model (40%). As traditional Virtual Private Networks (VPNs) struggle to keep pace with emerging technologies and threats, SASE solutions not only secure access but ensure seamless connectivity for hybrid and remote employees.

Successful implementation, however, can be challenging. Organizations point to key challenges integrating with existing infrastructure and systems (48%), as well as complexity in policy management across environments (44%). This has led organizations to consider MSSPs to help streamline implementation and operations—noting a lack of in-house expertise (47%) and access to specialized skills or expertise (46%) to fully realize the potential of innovative security solutions. As an MSSP, Hughes offers a hands-on, tailored approach to meet organizations' needs and streamline the integration of newer technologies with legacy VPNs.

"Connectivity today is the lifeblood of successful business," said Holger Schulze, founder of Cybersecurity Insiders. "Sophisticated cyber threats, coupled with a distributed workforce, demand that businesses embrace innovation and collaboration to fortify their defenses and safeguard their future. This analysis isn't simply informative—it's a crucial weapon for IT organizations committed to pioneering the future of robust, uninterrupted security."

For more information, download the 2025 State of Security Network Access Report: https://www.hughes.com/securenetwork

Hughes delivers enterprise-grade cybersecurity solutions to businesses everywhere. This survey reveals how employing technologies—like Hughes Managed Secure Access Service Edge (SASE) and Security Service Edge (SSE), as well as additional security controls, such as Managed Detection and Response (MDR), Network Detection and Response (NDR), and Ransomware & Zero-Day Prevention—will bolster businesses' cybersecurity and provide the robust protection their workforces now require.

To learn more about Hughes cybersecurity solutions for enterprise, please visit: https://www.hughes.com/what-we-offer/managed-cybersecurity

About Hughes
Hughes Network Systems, LLC, an EchoStar company (Nasdaq: SATS), provides broadband equipment and services; managed services featuring smart, software-defined networking; and end-to-end network operation for millions of consumers, businesses, governments, airlines, and communities worldwide. The Hughes flagship internet service, Hughesnet®, connects millions of people across the Americas, and the Hughes JUPITER™ System powers internet access for tens of millions more worldwide. Hughes supplies more than half the global satellite terminal market to leading satellite operators, mobile network operators and military customers. Hughes products and services have helped bring in-flight video and broadband to thousands of aircraft for over twenty years. A managed network services provider, Hughes supports approximately half a million enterprise sites with its portfolio of wired and wireless solutions including 5G Open RAN and Low Earth Orbit (LEO) satellites. To learn more, visit www.hughes.com/ or follow HughesConnects on X (Twitter) and LinkedIn.

About Cybersecurity Insiders
Cybersecurity Insiders connects security vendors with a global network of over 600,000 IT security professionals, providing content-driven marketing solutions that elevate brand visibility, establish thought leadership, and generate qualified leads.

Through data-rich research reports, practical CISO guides, unbiased product reviews, engaging webinars, and educational articles on the popular Cybersecurity Insiders news site, we deliver actionable insights that empower cybersecurity professionals to stay ahead of emerging threats, evaluate solutions, and adopt best practices with confidence.

Trusted by industry leaders like Hughes Network Systems, Cybersecurity Insiders is a strategic partner for cost-effective marketing that delivers results.

Learn more at www.cybersecurity-insiders.com.

View original content to download multimedia:https://www.prnewswire.com/news-releases/two-thirds-of-businesses-are-exploring-sase-to-address-hybrid-work-security-challenges-302350195.html

SOURCE Hughes Network Systems, LLC

Kylie Bezpa, MikeWorldWide, (732) 439-8918, kbezpa@mww.com