Zscaler's 2022 VPN Report: As VPN Exploits Grow, 80 Percent of Organizations Shift Towards Zero Trust Security

September 26, 2022

Organizations should be mindful of Firewall/VPN solutions marketed as Zero Trust Cloud Security

Key Findings:

- 68% of executives surveyed say their focus on remote work accelerated the priority of Zero Trust Security projects, up from 59% in 2021
- Nearly half of all IT professionals surveyed witnessed an increase in exploits targeting their VPNs since adopting remote work
- 65% of companies are considering adopting VPN alternatives; organizations should be warned of misleading legacy cloud-based VPN offerings masqueraded as Zero Trust security

SAN JOSE, Calif., Sept. 26, 2022 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today released the findings of its annual VPN Risk Report, conducted by Cybersecurity Insiders, which shows a growing number of VPN-specific security threats and a need for Zero Trust security architecture in enterprise-level organizations. The 2022 report surveyed over 350 IT professionals in North America at organizations with global workforces. Despite high awareness of VPN risks, remote work forced many companies to rely more heavily on legacy access methods during the pandemic. At the same time, cybercriminals continue to take advantage of long-standing security vulnerabilities and increased attacks on VPNs. This year's Zscaler VPN Risk Report includes analysis of the state of the remote access environment, the most prevalent VPN risks, and the growth in adoption of Zero Trust.

"As evident in several high-profile breaches and ransomware attacks, VPNs continue to be one of the weakest links in cybersecurity. Their architecture deficiencies provide an entry point to threat actors and offer them an opportunity to move laterally and steal data," said Deepen Desai, Global CISO of Zscaler. "To safeguard against the evolving threat landscape, organizations must use a Zero Trust architecture that, unlike VPN, does not bring the users on the same network as business-critical information, prevents lateral movement with user-app segmentation, minimizes the attack surface, and delivers full TLS inspection to prevent compromise and data loss."

Zero Trust Secures Remote Access
While more and more companies have employees returning to the office, 95 percent of surveyed workplaces still rely on VPNs to support a combination of hybrid and distributed work environments that often span multiple geographies. In addition to remote employees, large organizations often extend network access to other external stakeholders, including customers, partners, and contractors. In many cases these users are connecting from untrusted devices on insecure networks, are granted far more freedom than necessary, and result in additional security risks. Unlike cumbersome, insecure VPNs, Zero Trust architecture improves organizational security posture without sacrificing the user experience. In addition, Zero Trust allows IT teams to keep the location of their network and applications secret, reducing the attack surface and threat of internet-based attacks.

Status Quo Falls Behind as VPN Risks Continue To Grow
The increase in the number of remote workers across industries has resulted in a sharp spike in cyberattacks that are tailor-made to target VPN users. As VPNs grant a greater degree of trust to users when compared to Zero Trust architecture, cybercriminals are more active in seeking to gain unauthorized access to network resources through exposed attack surfaces. According to the report, 44 percent of cybersecurity professionals have witnessed an increase in exploits targeting their business VPNs in the last year, demonstrating the risks associated with this technology when deployed to support remote users.

Legacy network security architectures are pervasive and deeply entrenched in corporate data centers, making it difficult to challenge the status quo and adopt new architectures. So it should come as no great surprise that nearly all of the organizations surveyed continue to use VPNs despite knowing they are being targeted by ransomware and malware. Meanwhile, incumbent network security vendors have a vested interest in maintaining the remote access status quo. Organizations should be wary of legacy network access approaches that rely on cloud-based VPN, and examine vendors' architectures to understand whether they will bring significant benefits in risk reduction and user experience. VPN technology carries the same fundamental shortcomings and risks in cloud virtual machines as it does on appliances, and should be avoided in favor of more modern approaches.

VPN Alternatives Gain Traction
Ongoing risks from legacy VPNs have created a gradual shift towards Zero Trust Security, which provides greater control and flexibility for effective remote access management. 78 percent of organizations surveyed for the VPN Risk Report indicated that their future workforce will be hybrid, creating an ongoing need for this type of security infrastructure in the enterprise.

Since the shift to remote and hybrid work environments, 68 percent of surveyed companies have indicated that they are accelerating their Zero Trust projects. Unlike VPNs, Zero Trust architecture treats all network communications as potentially hostile and requires tightening access using identity-based validation policies. This ensures IT and security teams can restrict users from off-limits applications and prevent malicious intruders from taking advantage of granted access to move laterally within the network. Zero Trust security architecture also reduces network risk by eliminating the attack surface, masking activity from internet-based threats and connecting them directly to the applications and resources they need.

Click here to download and read the 2022 VPN Risk Report. Click here to download the Zero Trust for Architects Book.

Methodology

The 2022 Zscaler VPN report is based on the results of a comprehensive online survey of 351 IT and cybersecurity professionals. The survey was conducted in June 2022 to identify the latest enterprise adoption trends, challenges, gaps, and solution preferences related to VPN risk. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across North America with global workforces.

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest in-line cloud security platform.

Media Contacts
Natalia Wodecki
Global PR Director
press@zscaler.com

Zscaler, Inc.