Zscaler VPN Report Finds Nearly Half of Organizations Are Concerned About Enterprise Security Due to Unsafe VPNs

August 1, 2023

Insecure VPNs, Email, and End User Devices Identified as Primary Attack Vectors, Stressing the Need for a Zero Trust Architecture

- 88% of companies report being concerned that VPNs jeopardize their ability to maintain a secure environment
- 90% of organizations are apprehensive that attackers will target them through third-party-owned VPNs
- User satisfaction is also low, with 72% of users expressing frustration due to slow and unreliable VPN connections

SAN JOSE, Calif., Aug. 01, 2023 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today revealed the findings of its annual VPN Risk Report, produced by Cybersecurity Insiders, which shows that a resounding number of organizations are expressing deep concerns about their network security due to the risks from VPNs. The report includes a survey of 382 IT and cybersecurity professionals in multiple industries and explores their security and user experience challenges. The report stresses the need for organizations to reevaluate their security posture and migrate to a Zero Trust Architecture due to the increasing threat of cybercriminals exploiting VPN vulnerabilities.

“The report shows 92% of survey respondents recognize the importance of adopting a Zero Trust architecture; however, it is concerning to see many organizations are still using a VPN for remote employee and third-party access, inadvertently providing a juicy attack surface for threat actors,” said Deepen Desai, Global CISO and Head of Security Research, Zscaler. “Legacy firewall and VPN vendors are spinning virtual VPNs in the cloud and claiming that it is Zero Trust, and they go the extra length to hide the word "VPN". Customers need to ask the right questions to make sure that they are not getting a false sense of security with these virtualized legacy offerings in the cloud. To safeguard against evolving ransomware attacks, it is critical for organizations to eliminate the use of VPNs, prioritize user-to-app segmentation, and implement an in-line contextual data loss prevention engine with full TLS inspection.”

VPN Vulnerabilities Underscore the Need for a Zero Trust Architecture
88% of organizations express deep concern over potential breaches due to VPN vulnerabilities. More specifically, organizations are most concerned with possible phishing attacks (49%) and ransomware attacks (40%) as a result of regular VPN usage.

Nearly half of the organizations reported they have been targeted by cyber attackers who were able to exploit a VPN vulnerability like outdated protocols or data leaks, with one in five experiencing an attack in the past year. Ransomware, in particular, has emerged as a significant adversary for organizations, with 33% falling victim to ransomware attacks on VPNs within the past year.

Third-Party Users Are a Top Concern
Despite diligent security measures, research shows that 90% of organizations are still highly concerned about third-party vendors being exploited by attackers to gain indirect backdoor access into their networks. Outside users like contractors and vendors serve as potential risks to the organization due to varied security standards, a lack of visibility into their network security practices, and the complexity of managing external third-party access.

Legacy networking and security architectures manage access to internal applications by providing users direct access to the network - inherently trusting users that can confirm their credentials at the access point, which is problematic if those credentials are stolen. With a Zero Trust approach, users connect directly to the apps and resources they need, never to networks. User-to-application and application-to-application connections eliminate the risk of lateral movement and prevent compromised devices from infecting other resources. Additionally, users and apps are invisible to the internet, so they can’t be discovered or attacked.

Poor User Experience Can Lead to Security Challenges
In addition to security concerns, 72% of users are dissatisfied with their current VPN experience due to slow and unreliable connections. Most notably, 25% are frustrated by sluggish application speeds, while 21% face frequent connection disruptions.

Unreliable internet connectivity contributes to poor user experiences, leading to frustration and lower user engagement. In addition, authentication complexity and friction can lead to lost productivity, reduced revenue, and increased risk of data loss from users that find ways to bypass inefficient VPN services.

Shifting to Zero Trust
Organizations that recognize the role outdated VPNs play in creating these security and user experience concerns are starting to move towards Zero Trust architecture. In fact, a resounding 92% recognize the importance of adopting a Zero Trust approach to safeguard their assets and data - an increase of 12% year-over-year, and 69% are already in the planning stages of replacing their current VPN solutions with Zero Trust Network Access (ZTNA).

Mitigating VPN Risk with Zero Trust
The report strongly recommends organizations implement a Zero Trust-based architecture to effectively mitigate the risks associated with VPN vulnerabilities and protect their sensitive data and applications from cyber attacks.

- For more information about best practices for moving away from VPNs, see *New VPN Risk Report: Third-Party Access Identified as a Huge Risk to Organizations* blog
- To download the Zscaler 2023 VPN Risk Report, visit https://info.zscaler.com/2023-vpn-risk-report
- If you are considering replacing your VPN and seeking guidance, download Zscaler’s *Securing Your Hybrid Workforce with ZTNA* eBook.

Methodology
The 2023 Zscaler VPN Report is based on a survey of 382 IT professionals and cybersecurity experts and explores these multifaceted security and user experience challenges. The 2023 VPN Risk Report reveals the complexity of today's VPN management, user experience issues, vulnerabilities to diverse cyberattacks, and their potential to impair organizations' broader security posture.

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform 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
Nick Gonzalez
press@zscaler.com