New VPN Risk Report by Zscaler Uncovers Hidden Security Risks Impacting Enterprises and Offers Alternatives for Secure Remote Access

February 16, 2021

2021 Research Highlights Growing Security Vulnerabilities Around Targeted Social Engineering, Ransomware and Malware Attacks

SAN JOSE, Calif., Feb. 16, 2021 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today announced a new study that examines hidden vulnerabilities found in enterprise virtual private networks (VPNs) and spotlights the need for a zero-trust security approach to mitigate threats. Published in collaboration with the Cybersecurity Insiders, the report includes findings from a global survey of more than 350 cybersecurity professionals on the current state of remote access environments, the rise in VPN vulnerabilities, and the role zero-trust security models play in providing access to enterprise applications. To download the full study, see the Zscaler 2021 VPN Risk Report.

For the last three decades, VPNs have been deployed to provide remote users with access to resources on corporate networks. However, the increased demand for remote work solutions, a shift to the cloud, and advancements in digital transformation have uncovered increased incompatibility between VPNs and true zero-trust security architectures. These incompatibilities, largely due to VPNs inherent need for access to the network, and need to be exposed to the Internet, have increased the enterprise attack surface allowing threat actors to exploit these legacy models based on their inherent trust of users.

The 2021 Zscaler VPN Risk Report highlights the current VPN usage by enterprises and uncovered the list of top challenges faced by IT administrators who manage VPNs. It recommends security alternatives that exist for network and security leaders wanting to provide fast, seamless and secure access to business apps without compromising their existing zero trust security strategies, and includes data that provides a glimpse into the role that zero trust will play in the future of remote access. The survey findings show:

- 93 percent of companies surveyed have deployed VPN services, despite 94% of those surveyed admitting that they are aware that cybercriminals are exploiting VPNs to access network resources.
- Respondents indicated that social engineering (75%), ransomware (74%), and malware (60%) are the most concerning attack vectors and are often used to exploit users accessing VPNs.
- With nearly three out of four businesses concerned with VPN security, 67% of organizations are considering remote access alternatives to the traditional VPN.
- As a result of growing VPN security risks, 72% of companies are prioritizing the adoption of a zero-trust security model, while 59% have accelerated their efforts due to the focus on remote work.
- Looking at the future need for zero trust services, the report states that 77% of respondents indicated that their workforce will be hybrid, with greater flexibility for users to work remotely or in the office.

“It’s encouraging to see that enterprises understand that zero-trust architectures present one of the most effective ways of providing secure access to business resources,” said Chris Hines, Director, Zero Trust Solutions, Zscaler. “As organizations continue on their journey to cloud and look to support a new hybrid workforce, they should rethink their security strategy and evaluate the rising cybersecurity threats that are actively exploiting legacy remote access solutions, like VPN. The more secure approach is to completely leave network access out of the equation by taking the users securely and directly to the applications by brokering all user to app connections using a cloud-delivered zero trust access service instead.”

The full findings of the Zscaler VPN Risk Report are now available to the public. Please see the 2021 VPN Risk Report for more information.

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 SASE-based Zero Trust Exchange is the world’s largest in-line cloud security platform.

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