Zscaler ThreatLabz 2025 VPN Risk Report: Over Half of Organizations Say Security and Compliance Risks Make VPNs Obsolete

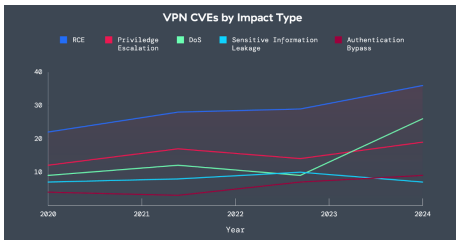
April 10, 2025

Annual Report Highlights How Unpatched VPNs Fuel Ransomware Attacks, Underscoring the Urgency for Zero Trust Security

Key Findings:

- 92% of organizations are concerned about ransomware attacks due to VPN vulnerabilities
- 93% of organizations fear backdoor vulnerabilities from third-party VPN connections
- 81% of organizations are adopting or planning to adopt zero trust within the next year

Zscaler 2025 VPN Risk Report



VPN CVEs by Impact Type

SAN JOSE, Calif., April 10, 2025 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today published the Zscaler ThreatLabz 2025 VPN Risk Report, commissioned by Cybersecurity Insiders, which highlights the widespread security, user experience and operational challenges posed by VPN services. The findings are based on insights from a survey of 600+ IT and security professionals. The results are stark: maintaining security and compliance is the single largest challenge (56%) facing enterprises using VPNs today. Meanwhile, the risks of supply chain attacks and ransomware are top of mind for these companies with 92% of respondents concerned that persistent VPN vulnerabilities will lead to ransomware attacks. These combined risks have culminated in a profound shift in thinking around enterprise VPNs with 65% of organizations planning to replace their VPNs within the year — while 81% plan to implement a zero trust everywhere strategy.

Initially built for remote access, VPNs have become a liability for corporate networks, exposing IT assets and sensitive data due to over-privileged access, vulnerabilities, and an ever-growing attack surface. VPN, both physical and virtual, is opposite of Zero Trust as by architecture it brings the remote users as well as attackers on the network. Additionally, VPNs hinder operational efficiency with slow performance, frequent connection issues, and complex maintenance, burdening IT teams and disrupting employee productivity. The report aims to shed light on these concerns with trusted insights from industry peers, while arming enterprises with guidance to enable secure access across today's hybrid work environments.

Security and usability concerns

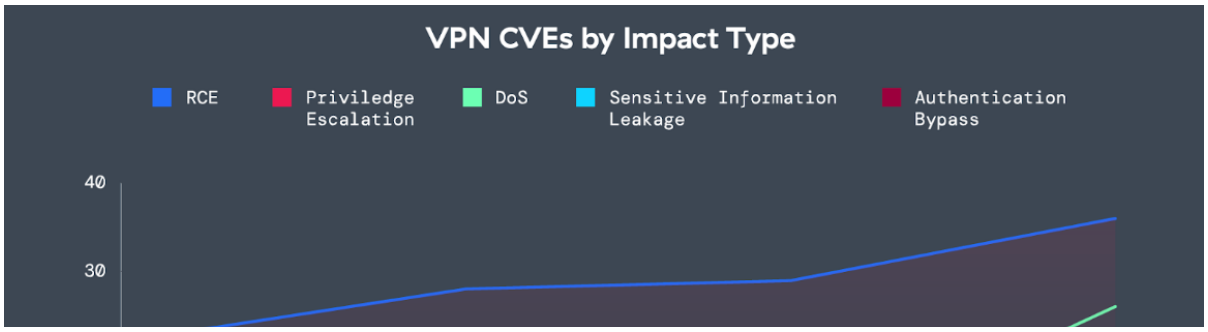
Security and compliance risks ranked as the top VPN challenges at 54%, highlighting growing concerns that VPNs are inadequate and obsolete for defending against today’s evolving cyber threats. Cybercriminals are now leveraging AI to pinpoint vulnerabilities by using GPT models to run queries focused on identifying weaknesses in VPNs — for instance, performing reconnaissance by simply asking a generative AI chatbot to return all current CVEs for VPN products in use by an enterprise. Tasks that once required weeks or even months can now be accomplished in just minutes.

Recently, a foreign cyberespionage group exploited vulnerabilities in a popular VPN, gaining unauthorized access to corporate networks. This incident, one of several in recent months, reinforces how VPN vulnerabilities continue to be a key target in cyberattacks, underscoring the urgent need to transition from legacy security models to a Zero Trust architecture. A staggering 92% of survey respondents said they are concerned about being targeted by ransomware attacks due to unpatched VPN vulnerabilities.

"Attackers will increasingly leverage AI for automated reconnaissance, intelligent password spraying, and rapid exploit development, allowing them to compromise VPNs at scale," said Deepen Desai, CSO at Zscaler. "To address these risks, organizations should shift to a Zero Trust everywhere approach. This approach eliminates the need for internet-exposed assets like VPNs (physical and virtual), while drastically reducing the attack surface and potential impact of breaches. It’s encouraging to see that 81% of organizations are planning to implement Zero Trust within the next year—a critical step in mitigating the security risks posed by legacy technologies like VPNs."

The rise of critical, scannable VPN vulnerabilities

To understand how attackers exploit vulnerabilities in internet-connected VPN infrastructure, ThreatLabz also analyzed VPN Common Vulnerabilities and Exposures (CVEs) from 2020-2025, based on data from the MITRE CVE Program. In general, vulnerability reporting is a good thing, as rapid vulnerability disclosure and patching helps the entire ecosystem improve cyber hygiene, foster community collaboration, and quickly respond to new vectors of attack. No type of software is immune from vulnerabilities, nor should it be expected to be.



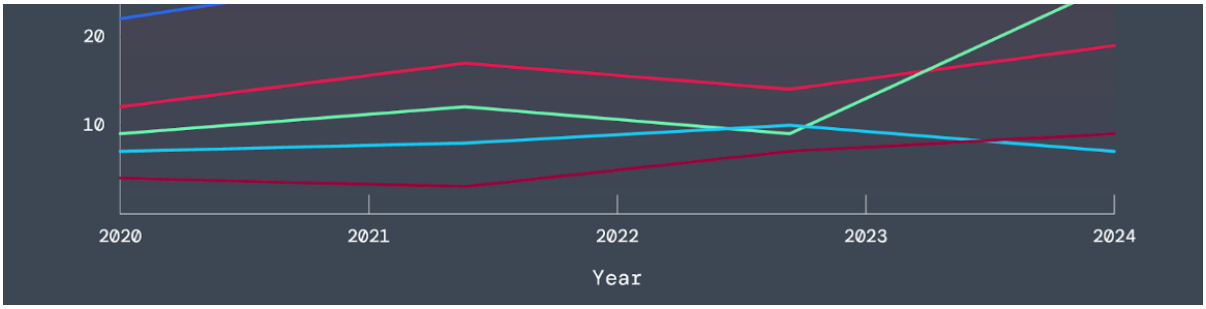


Figure 1: The impact type of VPN CVEs from 2020-2024, covering remote code execution (RCE), privilege escalation, DoS, sensitive information leakage, and authentication bypass.

Over the sample period, VPN CVEs grew by 82.5% (note that early 2025 data has been removed for this portion of the analysis). In the past year, roughly 60% of the vulnerabilities indicated a high or critical CVSS score — indicating a potentially serious risk to impacted organizations. Moreover, ThreatLabz found that vulnerabilities enabling remote code execution (RCE) were the most prevalent kind, in terms of the impact or capabilities they can grant to attackers. These types of vulnerabilities are typically serious, as they can grant attackers the ability to execute arbitrary code on the system. Put another way, far from being innocuous, the bulk of VPN CVEs are leaving their customers vulnerable to critical exploits that attackers can, and often do, exploit.

Unwelcome party guests
VPNs provide broad access following authentication, extending user access to contractors, external partners and vendors. While great in theory connectivity tools, attackers can easily exploit weak or stolen credentials, misconfigurations, and unpatched vulnerabilities to compromise these trusted connections. The report shows, 93% of organizations now worry about backdoor vulnerabilities stemming from third-party access. In February 2024, a financial services company suffered a data breach exposing nearly 20,000 clients' personal information, caused by vulnerabilities in their VPN. This incident highlights how VPNs create exploitable entry points into corporate networks.

Out with the old, in with the new - Zero Trust Everywhere
Legacy or traditional vendors are attempting to adapt to the evolving landscape by deploying virtual machines in the cloud and labeling them as Zero Trust solutions. Unfortunately, a VPN hosted in the cloud remains, at its core, a VPN and does not adhere to true Zero Trust principles. Illustrating this point, the industry has recently witnessed massive spikes in scanning activity targeting tens of thousands of publicly searchable VPN IP addresses hosted by at least one of the largest security vendors. Historically, this kind of activity has indicated some likelihood that attackers may be preparing to exploit yet-to-be-disclosed vulnerabilities in targeted VPN assets. Case in point: if you are reachable, you are breachable — which is why, from an architectural perspective, cloud-based VPN technology can never achieve true zero trust principles, no matter the branding.

The switch to a holistic Zero Trust architecture is rapidly gaining momentum and replacing outdated legacy security tools due to the proven security benefits and efficiency gains for adopting organizations. The report found 81% of organizations are adopting, or planning to adopt, a Zero Trust architecture within the next year and by extending this architecture to users, applications and workloads, enterprises are ensuring that Zero Trust is truly everywhere enabling VPN-free resilient security that:

1. **Minimizes the Attack Surface**: Replaces network-based access with Zero Trust policies and identity-based controls to secure users and third parties.
2. **Blocks Threats**: Prevents initial compromise through robust authentication, identity security, and least-privileged Zero Trust Access.
3. **Prevents Lateral Movement**: Uses Zero Trust segmentation to contain threats and stop unauthorized spread within networks.
4. **Enhances Data Security**: Enforces context-aware, integrated Zero Trust policies to protect sensitive information.
5. **Simplifies Operations**: Replaces VPNs with AI-driven security, continuous monitoring, and automated policy enforcement, in addition to uninterrupted access with business continuity.

By adopting these best practices, organizations can replace VPN security risks with a robust Zero Trust framework, enabling continuous verification, least-privileged access, and proactive threat prevention.

The Zscaler ThreatLabz 2025 VPN Risk Report provides additional insights and best practices to help organizations effectively prevent attacks and ransomware. Download your copy here.

Research Methodology
This report is based on a comprehensive survey of 632 IT and cybersecurity professionals conducted by Cybersecurity Insiders. The study examines VPN security risks, enterprise access trends, and the adoption of zero trust architectures. Respondents include executives, IT security practitioners, and network infrastructure leaders across various industries. The findings provide a data-driven perspective on the decline of VPNs and the shift to zero trust, offering critical insights for organizations modernizing their access security strategies.

About ThreatLabz
ThreatLabz is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabz regularly publishes in-depth analyses of new and emerging threats on its portal, research.zscaler.com.

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

Media Contact
Natalia Wodecki
press@zscaler.com

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/6c9af7e7-b67b-46d5-bfeb-c62a453b507a