zscaler™

2023 VPN Risk Report

Cybersecurity INSIDERS

Overview

Traditionally, Virtual Private Networks (VPNs) have facilitated basic remote access. The rapid growth in the distributed workforce and increasing adoption of cloud technologies are challenging the basic connectivity that VPN offers. As the threat landscape rapidly evolves, VPNs cannot provide the secure, segmented access organizations need. Instead, VPNs often provide full access to the corporate network, increasing the chances of cyberattacks once bad actors gain access through login credentials. In addition, VPNs connect multiple sites, allow access to third parties, support unmanaged devices, and enable IoT device connectivity. However, these varied use cases stretch VPNs beyond their initial purpose and design, often creating security gaps in the face of an increasingly complex and changing threat landscape.

This comprehensive report, based on a survey of 382 IT professionals and cybersecurity experts, 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. The report also outlines more robust security models, with zero trust emerging as a viable option to secure and accelerate digital transformation.

KEY FINDINGS FROM THE SURVEY INCLUDE:

VPN Vulnerabilities and Cybersecurity Impacts: Despite their critical role, VPNs pose security risks, with 88% of organizations expressing a slight to extreme concern that VPNs may jeopardize their environment's security. Furthermore, 45% of organizations confirmed experiencing at least one attack that exploited VPN vulnerabilities in the last 12 months - one in three became victim of VPN-related ransomware attacks. The increasing threat of cyberattackers exploiting VPN vulnerabilities underscores the urgent need to address the security of current VPN architectures.

VPN Use and User Experience: VPNs have a broad spectrum of use, with 84% of respondents identifying remote employee access as their primary application. However, users reported a less than optimal experience, with a majority of users dissatisfied with their VPN experience (72%), highlighting the need for more user-friendly and reliable remote access solutions in the digital workplace.

Overview cont.

Primary Attack Vectors: One in two organizations have faced VPN-related attacks in the last year. VPN attack vectors need special attention due to their critical roles in business operations and communication. Additionally, third-party users such as contractors and vendors serve as potential backdoors for malicious access to networks, further complicating the job of network security teams. In the survey, 9 of 10 respondents expressed concern about third parties serving as potential backdoors into their networks through VPN access.

Embracing Zero Trust: The transition to a zero trust model is high on the agenda for a majority of organizations. About 9 of 10 respondents identified adopting zero trust as a focus area, and more than a quarter (27%) are already implementing Zero Trust. 37% of respondents are planning to replace their VPN with Zero Trust Network Access (ZTNA) solutions.

We are grateful to Zscaler for their contribution to this VPN risk survey. Their expertise in zero trust and secure access solutions has significantly enriched our findings.

We are confident that the insights from this report will be an essential resource for IT and cybersecurity professionals on your journey toward zero trust security.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

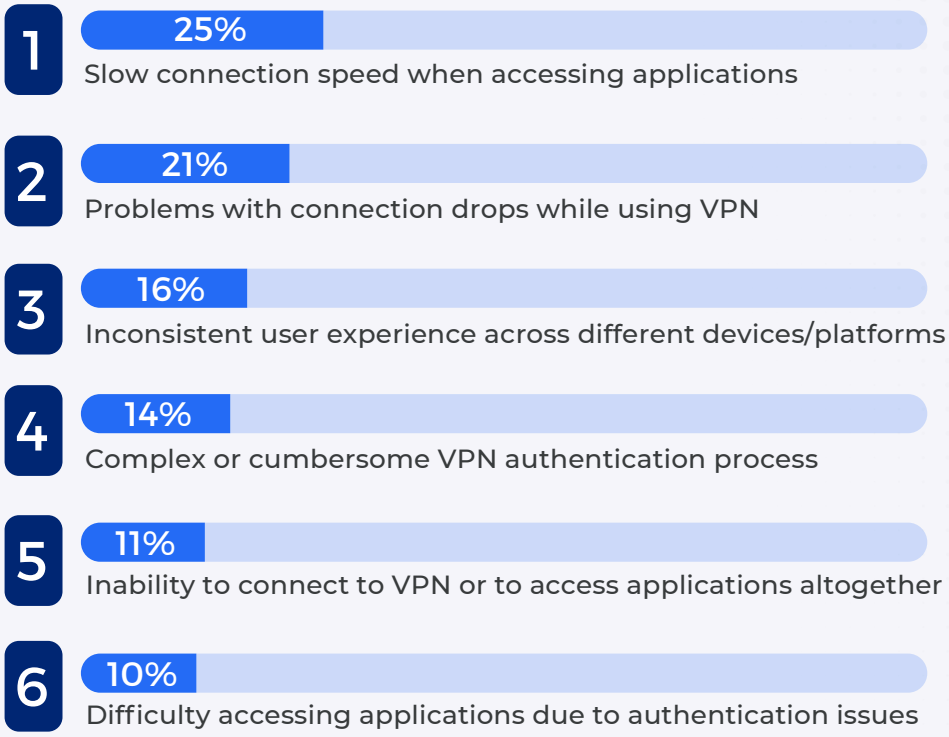
End Users Struggle with VPN

Among the VPN problems encountered, slow connection speed when accessing applications via VPN is the most prevalent, reported by 25% of respondents. Other notable issues include problems with connection drops while using VPN (21%) and an inconsistent user experience across different devices/platforms (16%).

Given these findings, it is evident that improving remote access user experience should be a priority for many organizations. A smooth and reliable access experience not only helps productivity but can also enhance security by encouraging compliance with security policies.

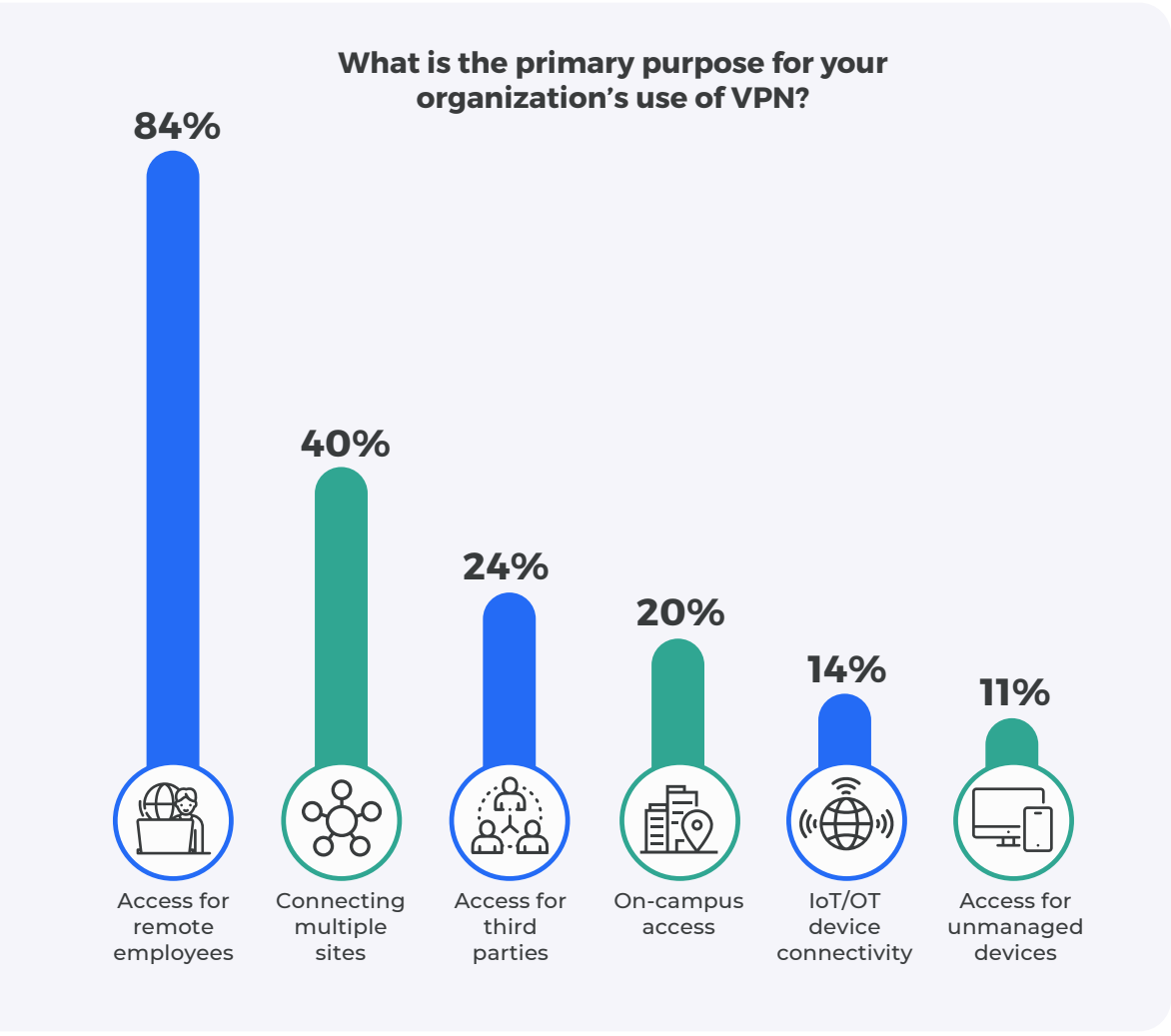
Improvements can range from optimizing network performance to minimizing slow connection speeds and connection drops, simplifying the VPN authentication process and ensuring a consistent user experience across different platforms. It is also critical to have robust support mechanisms in place to help users troubleshoot and resolve any difficulties they may encounter while using the VPN.

What is the most common complaint reported by your users when accessing applications via VPN?



Other 3%

Primary VPN Use Case: Remote Access for Employees



Other 3%

VPNs have a long history in connecting remote employees to the organization's network and facilitating a variety of use cases, such as remote work and third-party connections.

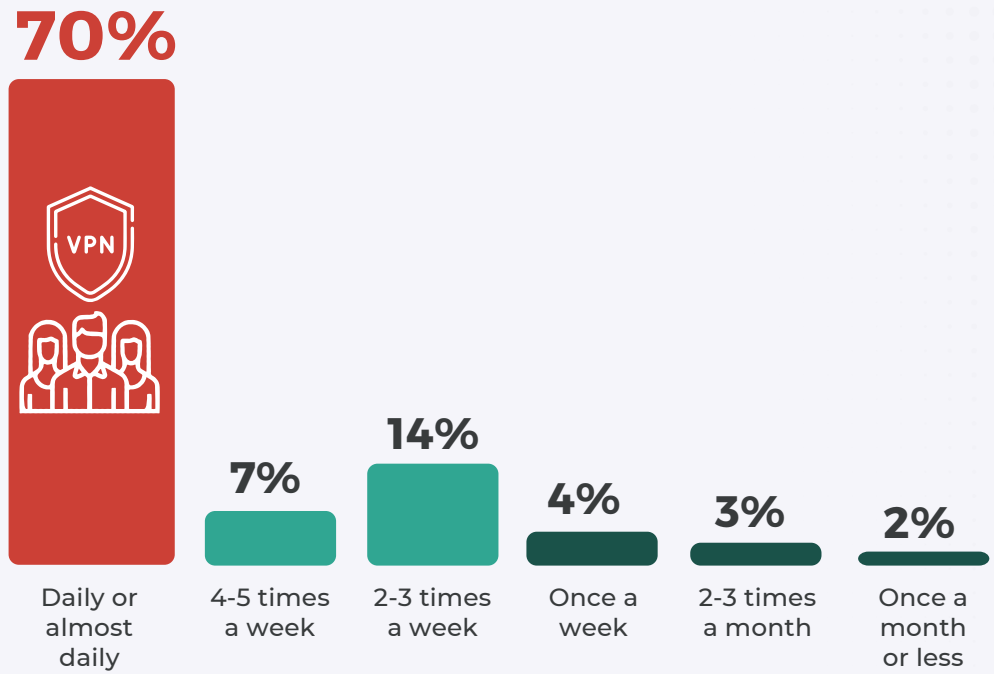
The primary purpose of VPNs in most organizations (84%) is to enable access for remote employees. This is a reflection of the remote work trend that has significantly increased in recent years. It's interesting, however, that only 11% use VPNs to manage access for unmanaged devices, pointing to an area of vulnerability that organizations may not be fully addressing.

High VPN Dependency

A significant number of end users (70%) utilize VPN daily or almost daily, showing high dependency on VPNs for daily, routine business operations. Combined with those using VPNs 4-5 times a week, 77% of all respondents use VPN for their work nearly every day. Interestingly, none of the respondents reported using VPN less often than once a month, confirming the widespread adoption of the technology.

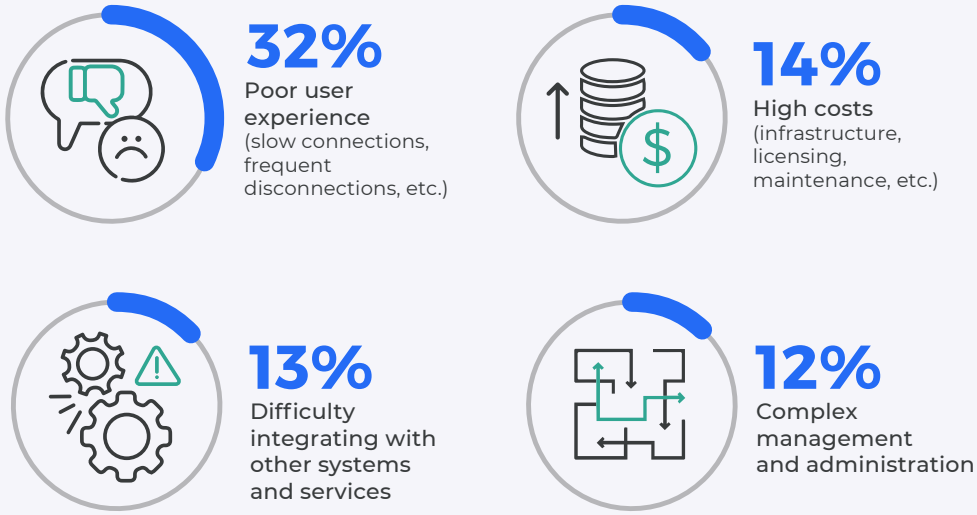
Given this high frequency of usage, it's vital to ensure the consistent availability and robust security of remote access/VPN services.

How often do your end users utilize VPN?



User Experience Issues

What is the most significant issue your organization encounters with its current VPN service?



Scalability and flexibility limitations 11% | Insufficient security and compliance 7% | Inadequate support for remote work and collaboration 4% | Other 7%

The performance and user experience of VPN services significantly impacts organizations' productivity and overall operational efficiency. A VPN that is slow or frequently disconnects can significantly disrupt business operations and frustrate users. Looking at the survey results, the most significant issue encountered with VPN services is poor user experience, with 32% of respondents citing slow connections and frequent disconnections.

Given these results, organizations should prioritize enhancing the user experience of their remote access services, which could involve increasing server capacity or choosing secure access solutions known for their speed and stability. Interestingly, organizations ranked security as a relatively low issue despite several cyberattacks on VPN in recent years.

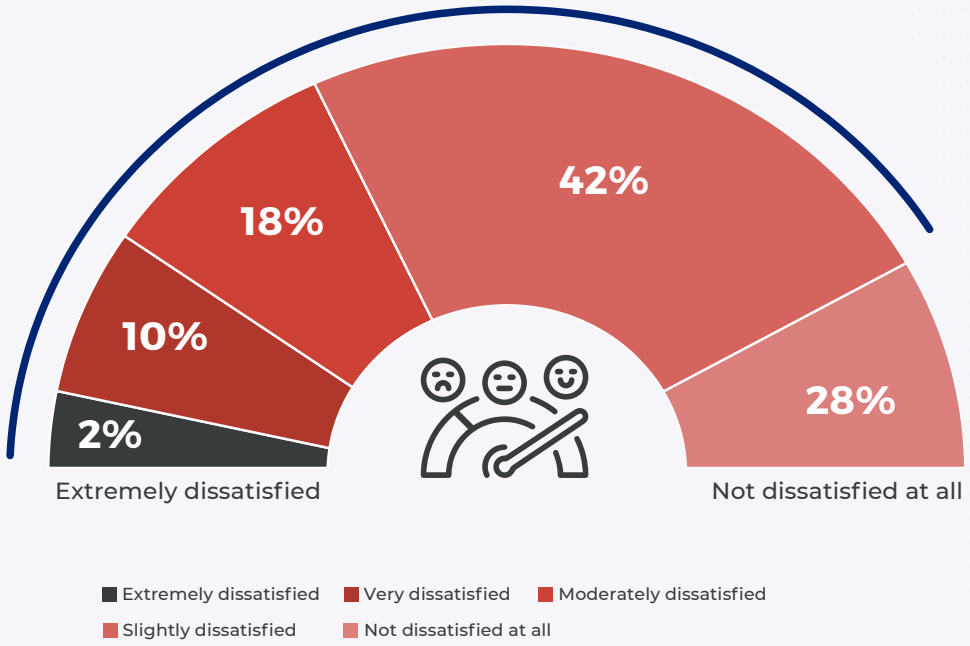
User Dissatisfaction with VPN

Assessing user satisfaction with VPN experience is critical, as dissatisfaction not only impacts productivity but can lead to non-compliance with security policies, which in turn could introduce security vulnerabilities.

A significant majority of users (72%) are dissatisfied with their VPN experience, highlighting the need for more user-friendly and reliable remote access solutions in the digital workplace.

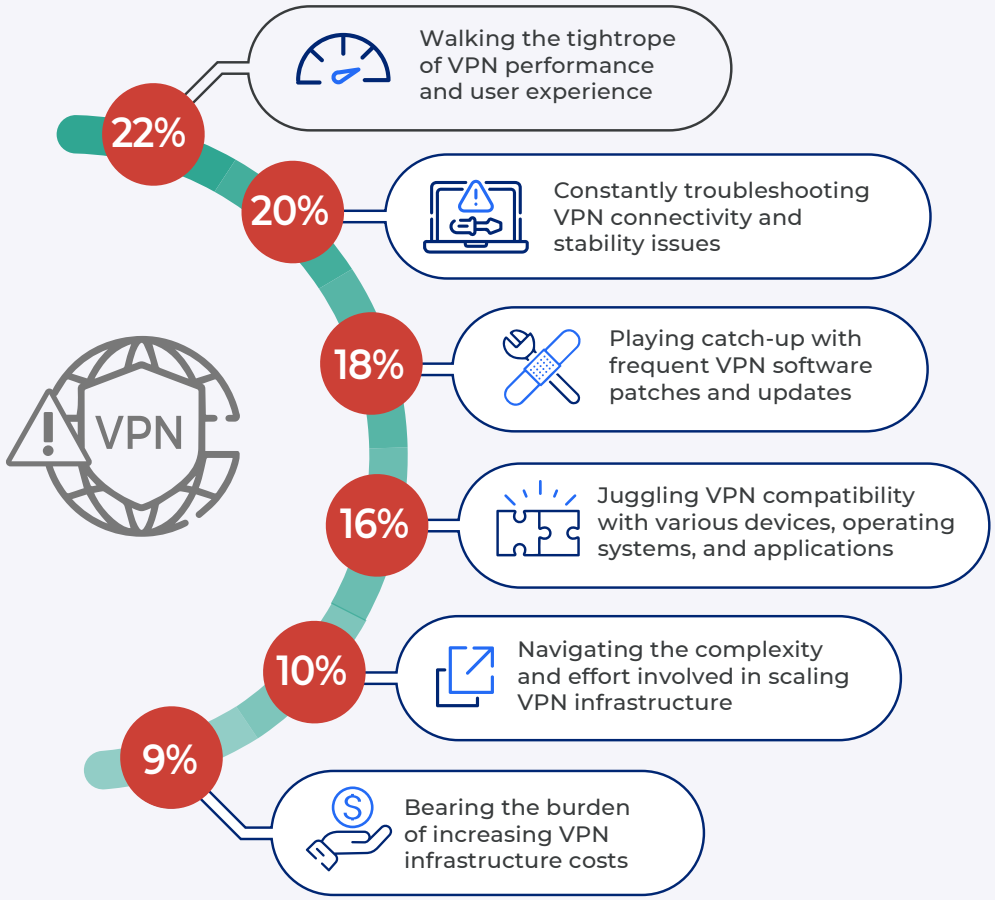
How dissatisfied are your users with their VPN experience?

72% of organizations are slightly to extremely dissatisfied with their VPN experience



VPN Management Challenges

What's the biggest headache in managing your VPN infrastructure?



Other 5%

The survey reveals that the biggest headache in managing VPN infrastructure, as indicated by 22% of the respondents, is balancing VPN performance with user experience.

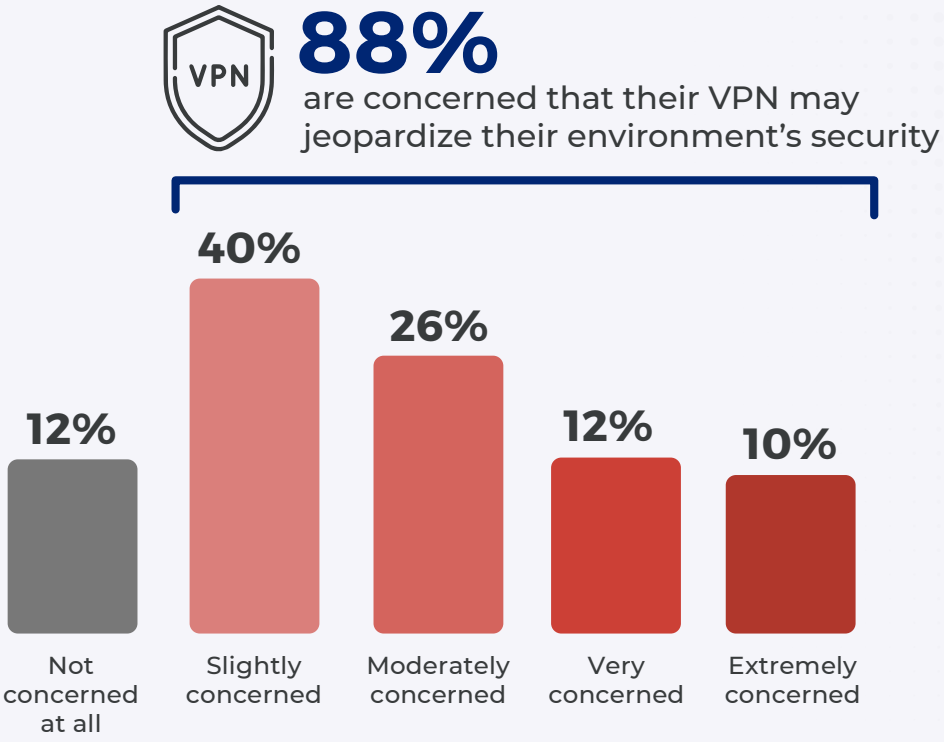
Troubleshooting VPN connectivity and stability issues is also a significant concern, impacting nearly 20% of respondents, closely followed by the effort required to keep up with frequent software patches and updates at 18%. Interestingly, only 9% of respondents cite increasing VPN infrastructure costs as their biggest headache.

VPN Security Concerns

The level of security a remote access solution provides is vital in protecting organizations' sensitive data and systems. Faced with increasingly advanced cyberthreats, VPNs can either fortify or compromise an organization's security posture, depending on their design and how well they are managed.

Reviewing the survey results, the vast majority of respondents (88%) are concerned that their VPN may jeopardize their environment's security. Particularly noteworthy is that a combined 22% of respondents report being "very" or "extremely" concerned, indicating a significant level of anxiety around VPNs as potential security weak points.

How concerned are you that VPN may jeopardize your ability to keep your environment secure?

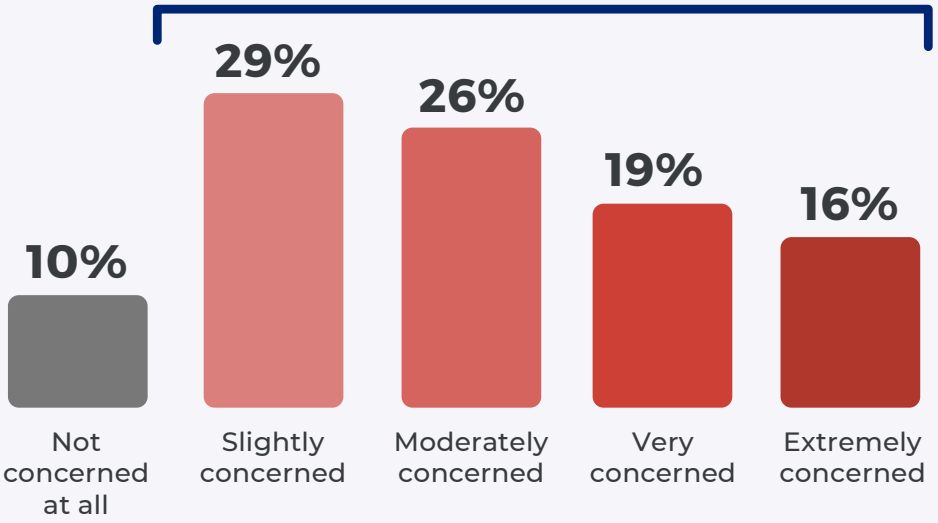


Third-Party Security Concerns

How concerned are you about third parties serving as a potential backdoor for attackers into your network through their VPN access?

90%

are concerned about third parties serving as potential backdoors into their networks through VPN access



Granting third parties access through a VPN is a necessary business practice, but it also raises serious security concerns. Given that third-party entities may not adhere to the same stringent cybersecurity standards, they can potentially provide a backdoor for cyberattackers to breach an organization's network.

In the survey, a vast majority of the respondents (90%) expressed concern about third parties serving as potential backdoors into their networks through VPN access. A combined total of 35% were "very" or "extremely" concerned, suggesting that third-party VPN access is a significant source of anxiety.

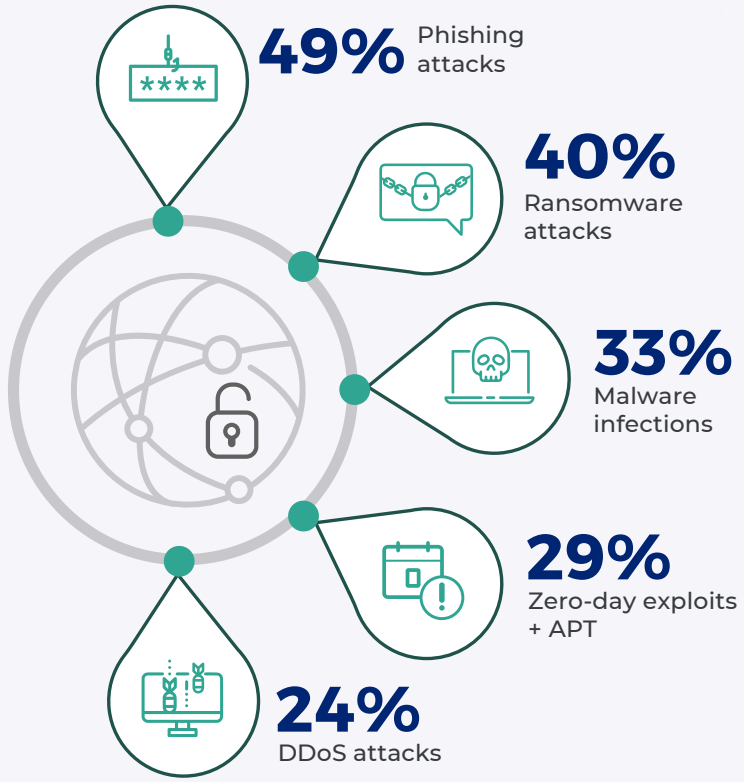
Organizations should enforce rigorous security measures when granting VPN access to third parties. This could involve regularly reviewing and updating access permissions, enforcing strong password policies, and monitoring network activity for anomalies. In addition, organizations should ensure that third parties comply with their cybersecurity policies and consider using advanced technologies such as zero trust architectures, which only grant access on a need-to-know basis.

Phishing Attacks Make Up Half of Cyberattacks

VPNs have a long history of vulnerabilities and require IT teams to constantly patch their VPN servers. This can potentially expose an organization to a variety of cyberattacks as threat actors continue to become more sophisticated and creative in their techniques.

Survey respondents see phishing attacks (49%) and ransomware attacks (40%) as the most likely types of attacks to exploit their organization's VPN vulnerabilities. These attacks often involve deceiving users into revealing sensitive information or deploying malicious software that locks down systems until a ransom is paid.

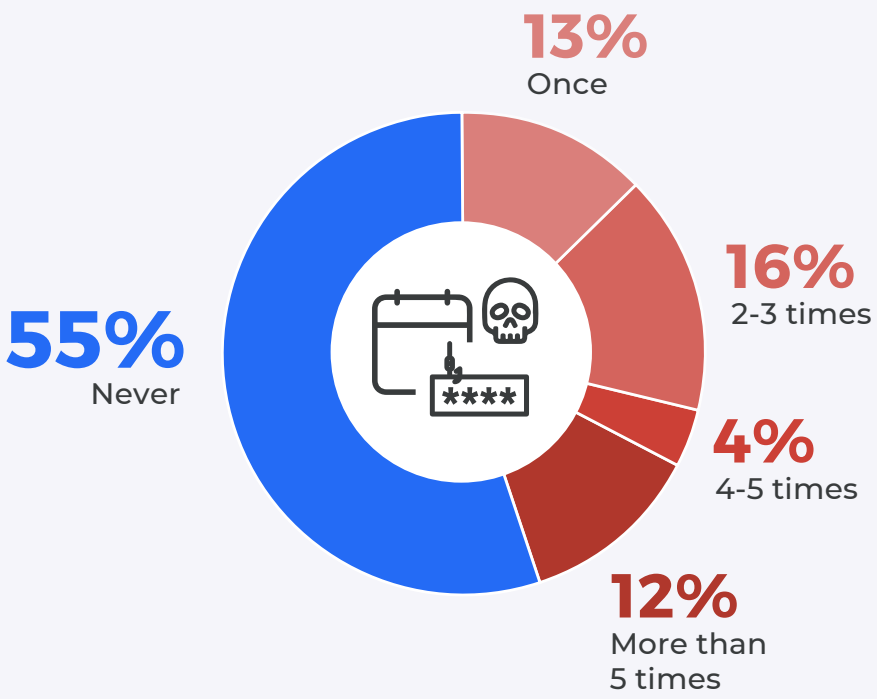
Which types of cyberattacks do you think are most likely to exploit your organization's VPN vulnerabilities?



Man-in-the-middle attacks 22% | Privilege escalation attacks 20% | Data exfiltration attacks 18% | Brute force attacks 11% | Cross-site scripting 11% | Remote code execution 9%

1 in 2 Organizations Have Experienced VPN-Related Attacks

In the last 12 months, has your organization experienced an attack that took advantage of security vulnerabilities in your VPN servers?



The security of a VPN server is crucial for maintaining the integrity and confidentiality of the data it handles. As organizations increasingly depend on VPNs for remote work, any vulnerabilities can become attractive targets for cyberattackers.

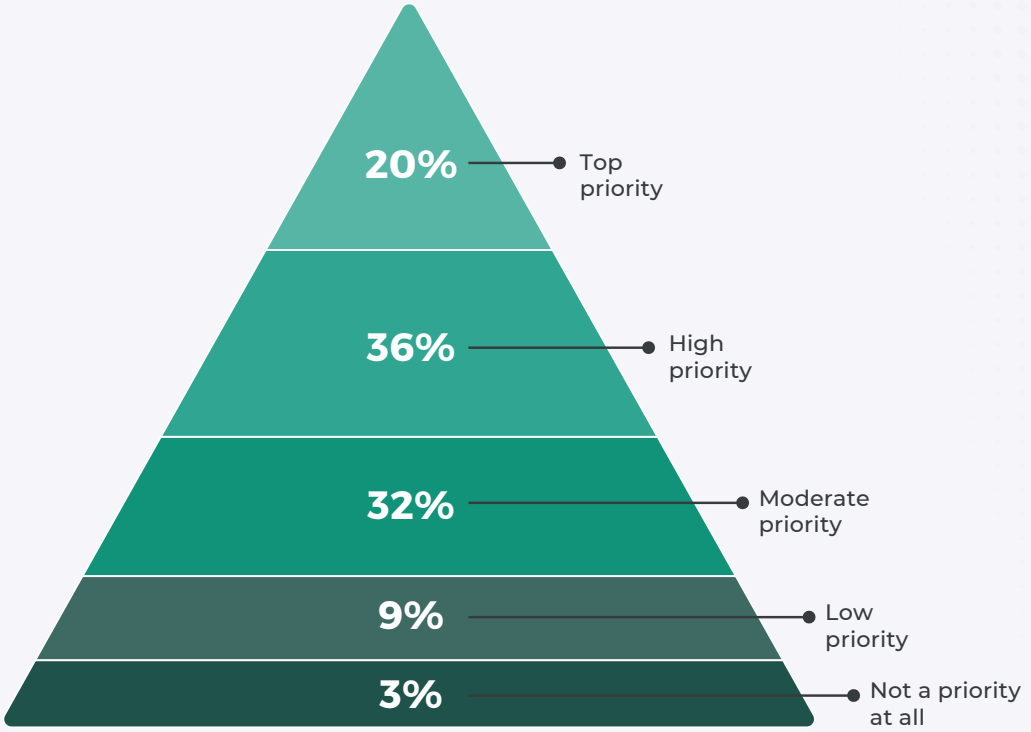
According to the survey, a sizable portion of organizations (45%) have experienced one or more attacks on their VPN servers in the past 12 months that exploited software vulnerabilities in VPN servers, highlighting the urgent need for more secure remote access solutions.

Zero Trust Strategy is a Big Priority

The adoption of zero trust, which is a security model that follows the maxim 'never trust, always verify,' is a priority for 9 of 10 organizations.

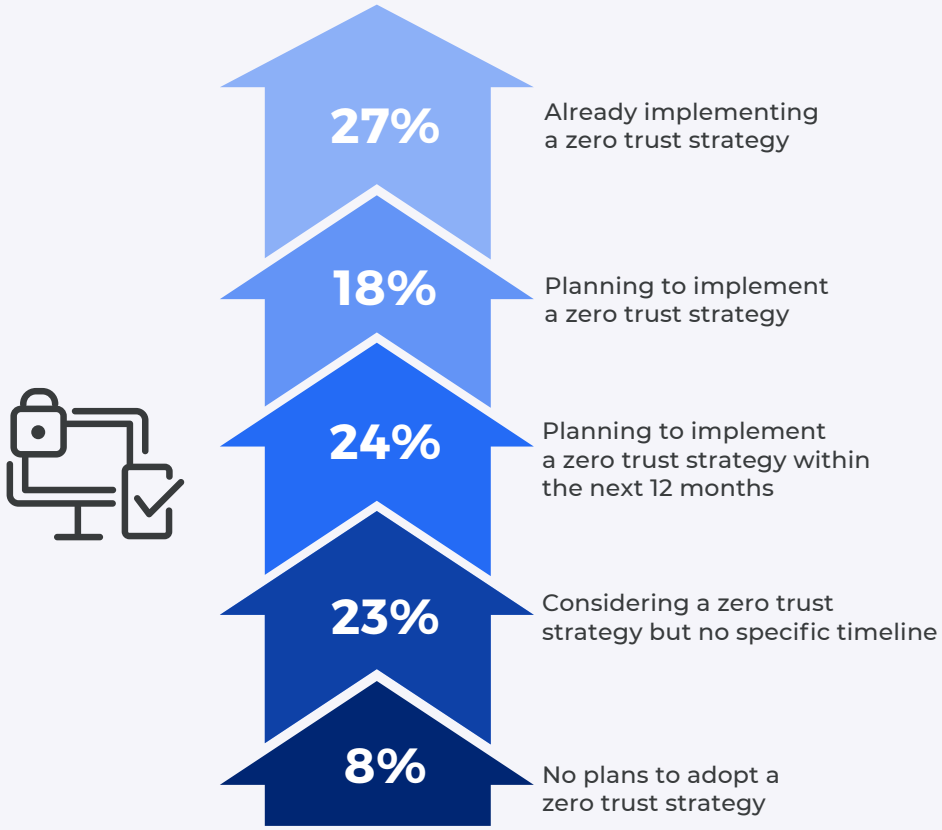
To fully leverage a zero trust architecture, organizations should prioritize key elements such as strong multi-factor authentication methods, continuous verification of traffic, network segmentation, least-privileged access, and continuous monitoring to strengthen their security posture.

How big of a priority is adopting a zero trust strategy for your organization?



Implementing Zero Trust is the Primary Focus

What are your plans for adopting a zero trust strategy for your organization?



92% of organizations are either already implementing (27%), planning to implement (42%) or considering a zero trust strategy, demonstrating an understanding of its importance and that zero trust is moving from a buzzword to a reality for most organizations.

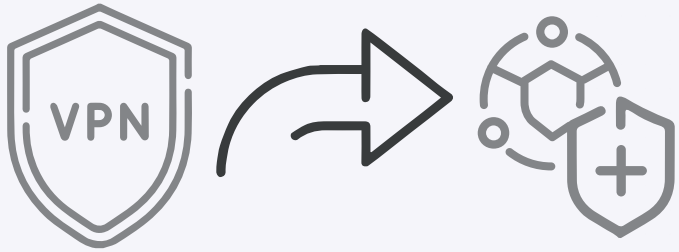
Those yet to define a timeline for implementation should consider accelerating their plans to remain competitive and secure. For those with no plans or who are unsure, they may risk falling behind in a rapidly evolving cybersecurity threat landscape.

VPN Transition Plans

The transition from VPN to Zero Trust Network Access (ZTNA) solutions marks a significant shift in modern cybersecurity strategies, given the heightened focus on least-privileged access and microsegmentation inherent in ZTNA. Four out of 10 organizations are transitioning to ZTNA, demonstrating an active response to evolving security requirements.

For organizations planning or considering a switch, it's crucial to evaluate and choose ZTNA solutions that meet their specific security requirements and business needs. Those who currently have no plans to adopt ZTNA should, at the very least, investigate the potential benefits of these solutions in enhancing their cybersecurity posture. For companies unable to switch completely, hybrid models can be a beneficial compromise, providing the advantages of ZTNA while leveraging existing VPN infrastructure.

Do you have plans to replace your current VPN solution with a Zero Trust Network Access (ZTNA) solution in the near future?



37%

have plans to replace VPN with a ZTNA solution in the near future

Best Practices for Your Journey to Zero Trust

We recommend the following best practices for successfully navigating the journey from traditional VPN infrastructure to a modern zero trust architecture.

Assess Your Current Infrastructure:
Start with a thorough review of your existing VPN infrastructure. With 32% reporting poor user experiences, and 14% high costs, it's crucial to understand your specific issues before moving forward.

Choose the Right Solution:
Look for a zero trust solution that aligns with your unique needs. A cloud-native, software-defined solution can simplify management, reduce costs, and improve user experience - issues frequently encountered with VPNs.

Implement Least-Privileged Access:
Grant users only the necessary access to specific resources based on their role's specific needs. This is a fundamental element of zero trust.

Plan for Scalability:
Opt for a solution that can scale as your business grows. Our survey indicated that about 11% of organizations face scalability issues with their VPNs. A cloud-based solution can effectively handle scalability needs.

Regularly Review and Update Your Security Policies:
Make it a practice to consistently review and update your security policies. This helps in maintaining a robust security posture.

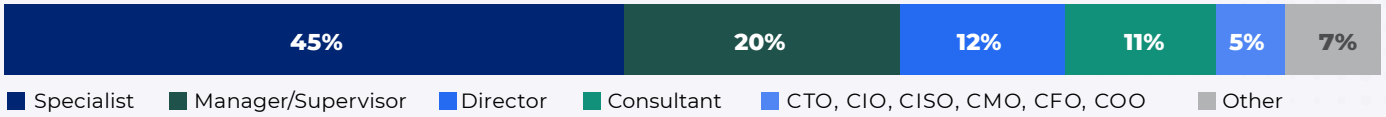
Enable Secure Access for All Users:
Adopt a solution that provides secure access for remote employees, third parties, and unmanaged devices. Choose a platform that supports any user, anywhere, on any device.

Continuously Monitor and Improve:
Adopt a continuous monitoring strategy to identify and respond to potential issues before they escalate. Proactive threat detection and response are key to a strong zero trust implementation.

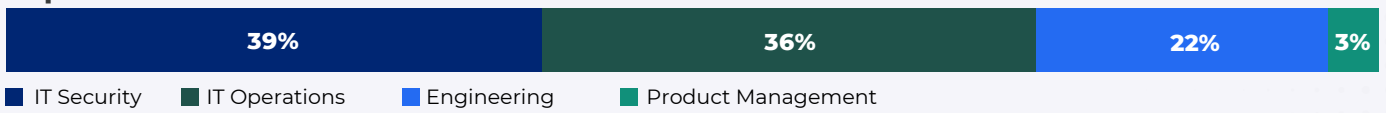
Methodology & Demographics

This report is based on the results of a comprehensive online survey of 382 IT and cybersecurity professionals, conducted in June 2023 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 multiple industries.

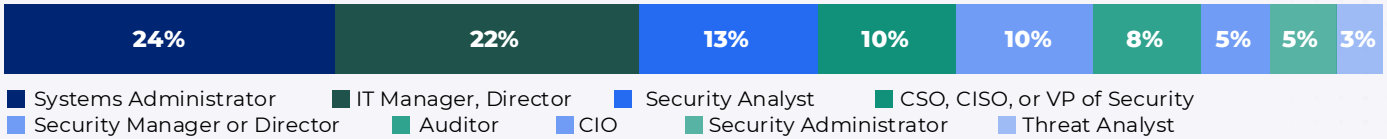
Career Level



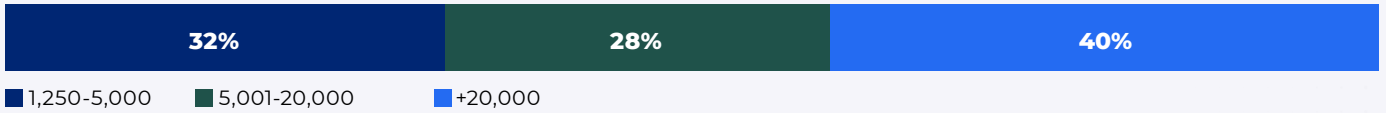
Department



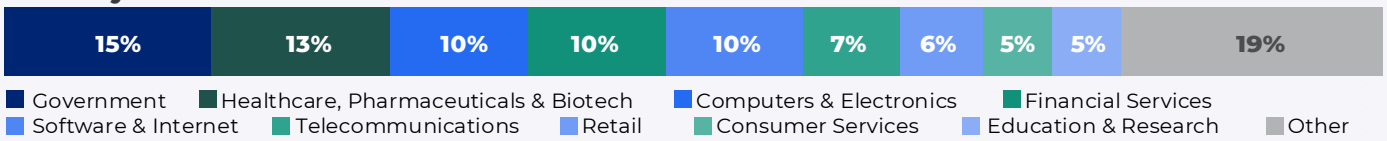
Primary Role



Company Size



Industry



About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that 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 inline cloud security platform.

Learn more at zscaler.com or follow us on Twitter @zscaler.

zscaler.com

Cybersecurity INSIDERS

Cybersecurity Insiders brings together 600,000+ IT security professionals and world-class technology vendors to facilitate smart problem-solving and collaboration in tackling today's most critical cybersecurity challenges.

Our approach focuses on creating and curating unique content that educates and informs cybersecurity professionals about the latest cybersecurity trends, solutions, and best practices. From comprehensive research studies and unbiased product reviews to practical e-guides, engaging webinars, and educational articles - we are committed to providing resources that provide evidence-based answers to today's complex cybersecurity challenges.

Contact us today to learn how Cybersecurity Insiders can help you stand out in a crowded market and boost demand, brand visibility, and thought leadership presence.

Email us at **info@cybersecurity-insiders.com** or visit **cybersecurity-insiders.com**