zscaler™

Principle networks

Zscaler ThreatLabz 2024 VPN Risk Report

Cybersecurity INSIDERS

Explore key VPN security, risk, and user experience trends as zero trust adoption reaches critical momentum.

Contents

Overview

Today's distributed and cloud-centric work environment has triggered a shift in access methods from traditional virtual private networks (VPNs) to more robust security frameworks like zero trust. Traditionally, VPNs provided essential remote access capabilities to connect users or entire office sites. However, the growing sophistication of cyberthreats alongside the expansion of remote workforces and cloud technologies have exposed significant vulnerabilities in VPNs. Due to their legacy architecture, VPNs grant overly broad network access once credentials are verified, significantly increasing the risk of cyberattacks if those credentials are compromised.

Recent high-profile exploits of VPN appliances have highlighted critical vulnerabilities (notably CVE-2023-46805, CVE-2024-21887, and CVE-2024-21893) affecting essential sectors, including US defense. These vulnerabilities enable attackers to bypass authentication, execute commands with elevated privileges, and maintain persistence after device resets. In response, the US Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive to federal agencies to immediately disconnect affected VPN devices due to substantial security risks.

Through Executive Order 14028, the US government now mandates the adoption of zero trust architectures to enhance cybersecurity, moving away from traditional VPNs. This directive, part of a comprehensive strategy to fortify national cybersecurity, instructs federal agencies to implement zero trust, which verifies every access request irrespective of origin. The Office of Management and Budget (OMB) further supports this initiative with a detailed Federal Zero Trust Strategy, underscoring the shift from VPN-based implicit trust within network perimeters to continuous verification of any and all access requests. These directives and recommendations reflect a consensus within the cybersecurity community that zero trust provides a more robust defense against complex and evolving cyberthreats, a necessity underscored by the recent vulnerabilities and exploits related to traditional VPNs.

As a result, organizations are rapidly adopting zero trust models, which do not inherently trust any user or device inside or outside the network perimeter and require granular verification for every access request. This model is particularly effective in preventing lateral movement within networks—an exploit that attackers often use to deepen their intrusion after gaining initial access.

Based on a survey of 647 IT professionals and cybersecurity experts, this report explores the multifaceted security and user experience challenges of VPNs to reveal the complexity of today's access management, vulnerabilities to various cyberattacks, and their potential to impair organizations' broader security posture. The report also outlines more advanced security models, particularly zero trust, which has firmly established itself as a robust and future-proof framework to secure and accelerate digital transformation.

We are grateful to Zscaler for contributing 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, Founder, Cybersecurity Insiders

"Over the past year, numerous critical VPN vulnerabilities have served as successful entry points for attacks on large enterprises and federal entities. Considering these repeated outcomes, it's crucial for enterprises to anticipate that threat actors will increasingly exploit these legacy, internet-exposed assets—appliances and virtual—that enable them to easily navigate laterally across traditional flat networks. It is essential to transition to Zero Trust architecture, which significantly reduces the attack surface by eliminating legacy technologies like VPNs and firewalls, enforces consistent security controls with TLS inspection, and limits the blast radius with segmentation and deception, preventing damaging breaches."

—DEEPEN DESAI, CHIEF SECURITY OFFICER, ZSCALER

Key Findings

VPN attacks are on the rise.

56% of organizations experienced one or more VPN-related cyberattacks in the last year—up from 45% the year before—highlighting the growing frequency and sophistication of attacks targeting VPNs.

The vast majority are shifting to zero trust.

78% of organizations plan to implement zero trust strategies in the next 12 months. Meanwhile, 62% of enterprises agree that VPNs are anti-zero trust.

Most have doubts about VPN security.

91% of respondents expressed concerns about VPNs compromising their IT security environment, with recent breaches illustrating the risks of maintaining outdated or unpatched VPN infrastructures.

VPNs are no match for ransomware, malware, and DDoS.

Respondents identified ransomware (42%), malware (35%), and DDoS attacks (30%) as the top threats exploiting VPN vulnerabilities, underscoring the breadth of risks organizations face due to inherent weaknesses in traditional VPN architectures.

The risk of lateral movement can't be ignored.

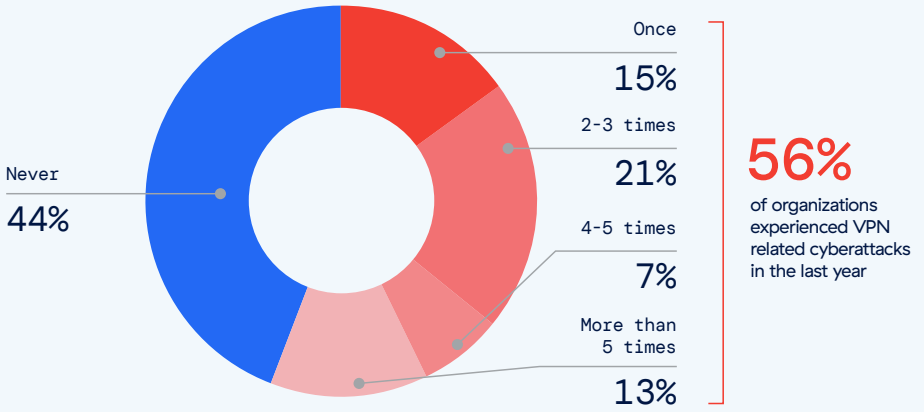
54% of enterprises breached via VPN vulnerabilities say threat actors moved laterally, demonstrating containment failures at the initial point of compromise that underscore the risks of traditional, flat networks.

Security Concerns with VPN

VPN Attacks on the Rise

The frequency and severity of attacks exploiting VPN vulnerabilities highlight the ineffectiveness of conventional cybersecurity measures and underscore the persistent risks posed by network exposure. Our survey reveals that 56% of organizations experienced cyberattacks in the last year that took advantage of VPN vulnerabilities, a significant increase from 45% the year before. Alarmingly, 41% of organizations reported suffering two or more VPN–related attacks, indicating severe security gaps.

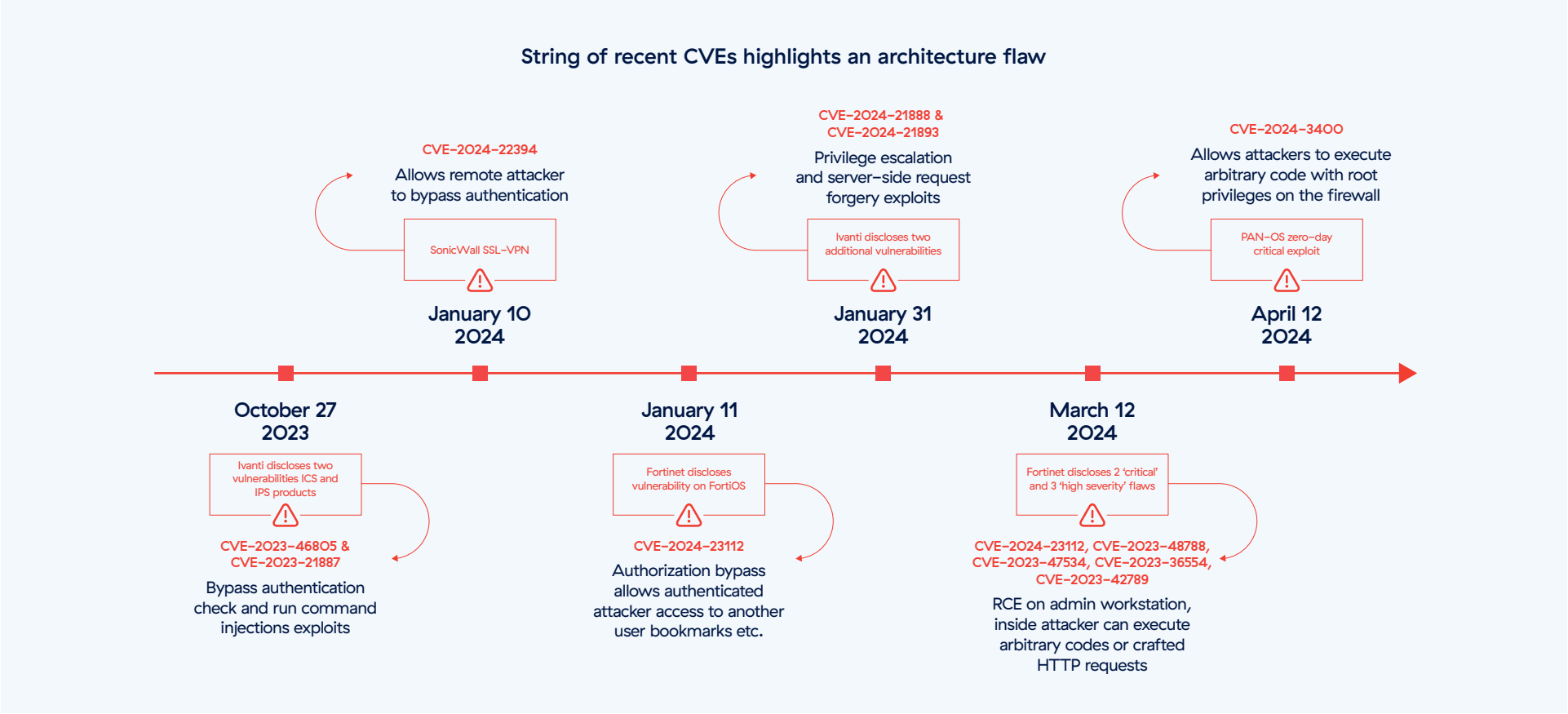
In the last 12 months, how often has your organization experienced an attack that took advantage of security vulnerabilities in your VPN servers?



Recent trends confirm that attacks on VPNs are becoming not only more frequent, but also more sophisticated. For instance, more cases of ransomware exploiting VPN flaws—particularly in the aftermath of publicly disclosed vulnerabilities—highlight the critical weaknesses inherent in traditional VPNs. Such vulnerabilities give attackers easy entry points to infiltrate networks and facilitate lateral movement, leading to substantial data breaches and operational disruption.

Major VPN Vulnerabilities in the Past Year

Amid the recent string of high-severity CVEs impacting VPN products, it's no surprise that enterprises are reporting more attacks that exploit these kinds of vulnerabilities. Of course, no single vendor or any particular technology can be immune from software vulnerabilities. In the case of VPN, the challenge for enterprises is that each CVE can represent a single security point of failure for the enterprise: a beachhead that allows attackers to compromise a VPN asset, establish persistence, move laterally across the network, and steal data. As VPN CVEs continue to be disclosed at this pace, they will be a persistent risk for enterprises that use VPNs for remote connectivity.



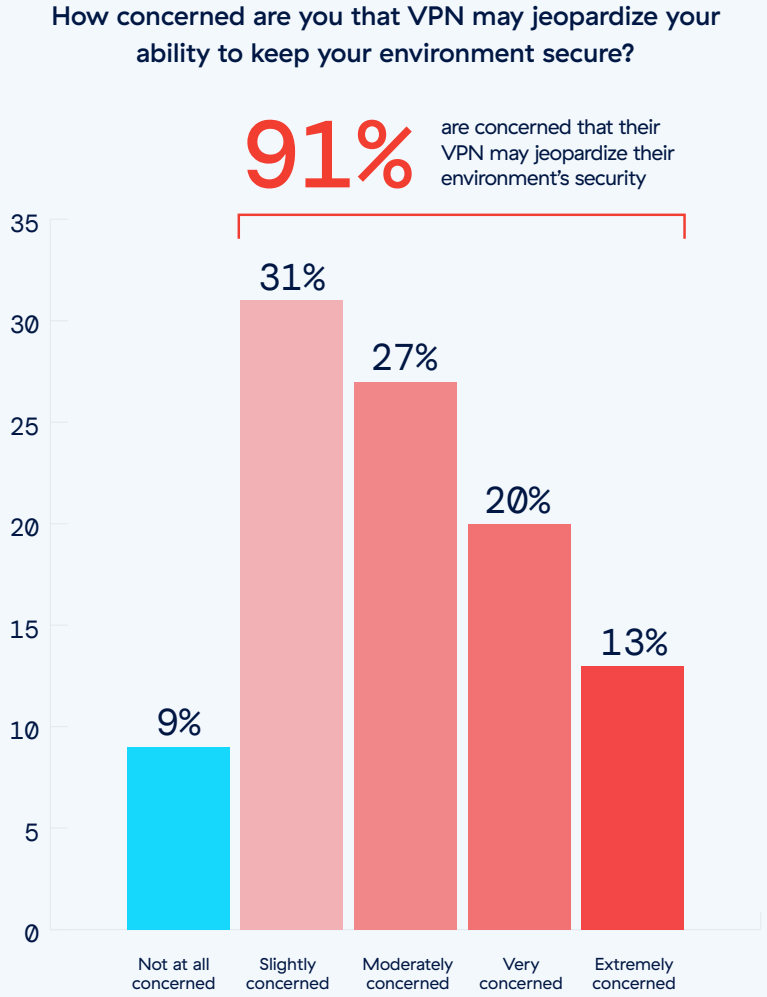
Navigating VPN Security Concerns

The survey results reflect deep-seated concerns about VPNs compromising security environments, echoing ongoing trends and increasing vulnerabilities in VPN technologies. An overwhelming majority of respondents (91%, up from 88% in 2023) express concerns about VPNs jeopardizing their IT security, underscoring heightened awareness of VPN-related risks among organizations.

This concern is justified by recent exploits targeting Ivanti VPNs, where attackers leveraged severe vulnerabilities to infiltrate networks and exfiltrate sensitive data. These incidents, involving vulnerabilities like CVE-2024-21888 and CVE-2024-21893, highlight the risks of maintaining and securing outdated or unpatched VPN infrastructures. Moreover, the inherent architecture of VPNs poses significant security risks in today's perimeter-less digital landscape. As businesses increasingly adopt cloud services and as remote work models evolve, VPNs face new security challenges, including managing broad access rights and securing an expanding attack surface.

These vulnerabilities and architectural limitations underscore a pivotal shift in perceptions toward VPN security, aligning with broader cybersecurity trends that advocate for more dynamic and resilient frameworks such as zero trust.

Forward-looking organizations transition toward zero trust architectures to gain more granular control and significantly reduce the attack surface by never conferring implicit trust, whether inside or outside a network perimeter. Adopting such a strategy addresses the immediate vulnerabilities of traditional VPNs and aligns with a proactive cybersecurity approach, essential for adapting to the evolving threat landscape.



Key Scenarios for Secure Access

Understanding why organizations use VPNs is essential as it highlights how they prioritize secure access across various business scenarios. It also reveals which networking use cases are most exposed to security risks, indicating areas that require more robust and innovative access security strategies.

A significant 70% of organizations use VPNs primarily to secure access for remote employees. This widespread use makes remote access a prime target for cyberattacks. Following this, 33% use VPNs to connect multiple sites, presenting substantial risks as these connections can serve as vectors for cyberattacks if not properly secured. Next, 26% of organizations noted access for third parties, which further complicates security due to the varying security postures of different external stakeholders and lack of control over security policies. Additionally, 20% of organizations use VPNs for on-campus access, and 19% use them for IoT/OT device connectivity.

VPNs no longer provide adequate security for critical access use cases in today's evolving cyberthreat landscape because they operate on outdated trust models that grant extensive network access upon simple user authentication. This broad access exposes organizations to significant risks by allowing potential attackers to exploit a single point of entry to navigate and extract sensitive data across the network.

VPN Management, Performance, and User Experience

Challenges in VPN Management

In addition to inherent security risks, managing VPN infrastructures presents significant challenges for IT teams as the requirements for robust access solutions intensify in dispersed, cloud-centric work environments. The primary management challenge for IT professionals is the balancing act between VPN performance and user experience (19%). This issue is crucial because it directly impacts productivity: if the VPN slows down the network or proves too cumbersome to use, it can lead to lower employee satisfaction and slow, inefficient business processes.

The next most common concern, cited by 17% of respondents, is constant troubleshooting of VPN connectivity and stability issues. These problems are not only time-consuming for IT staff, but also cause frustrating disruptions for users. Other notable challenges include VPNs' lack of compatibility with a diverse range of devices, operating systems, and applications, which about 16% of IT professionals find burdensome. Additionally, 13% of respondents struggle with the complexity and labor-intensive nature of scaling VPN infrastructure, a critical issue as organizations grow and their needs increase amid a severe shortage of skilled cybersecurity professionals.

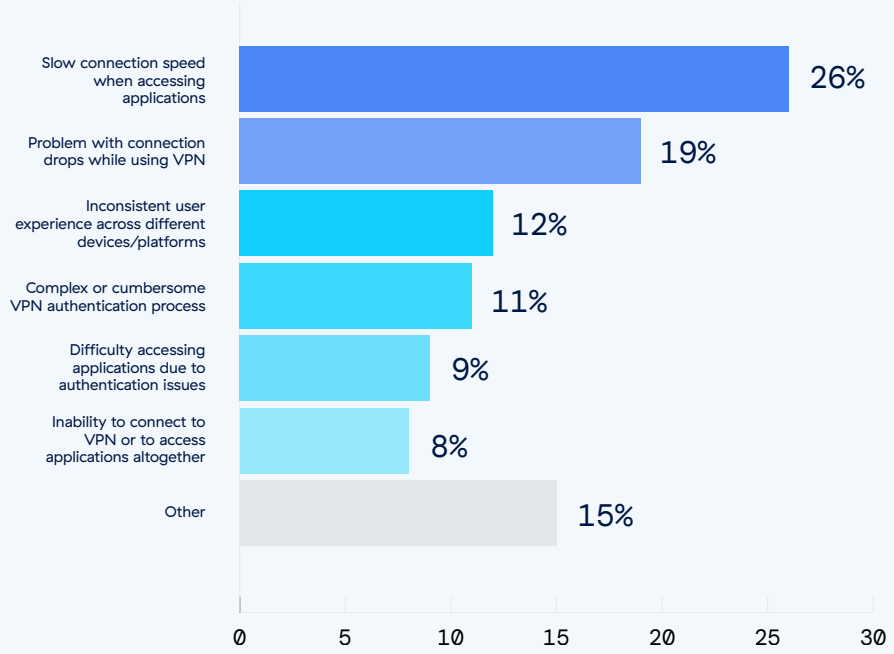
These insights underscore the need for organizations to explore more agile, user-friendly, and less resource-intensive alternatives, such as zero trust network access (ZTNA) models. ZTNA provides more granular control, enhanced scalability, and reduced management overhead, making it a superior choice to traditional VPN in today's dynamic cybersecurity landscape.

Common VPN User Challenges

The most frequent user complaint about VPN use, as noted by 26% of respondents, is slow connection speeds. This highlights a critical user productivity and satisfaction issue as slow speeds can significantly reduce the efficiency of routine tasks and access to cloud-based resources, especially in work-from-home environments.

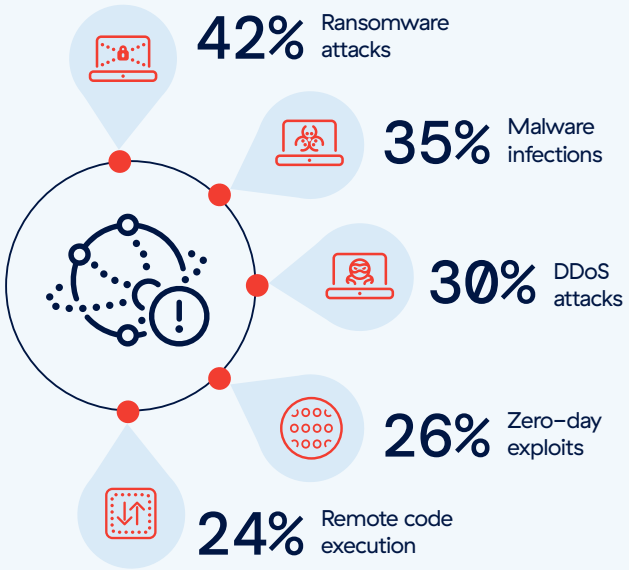
VPN connection drops represent the second-most common issue, cited by 19% of respondents. This problem can disrupt ongoing tasks and communications, significantly affecting user experience and operational continuity. Inconsistent user experiences across different devices and platforms, reported by 12% of users, points to a need for more uniform access performance.

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



To address these concerns, organizations should consider adopting network access solutions that offer more stability and consistency across various platforms. Implementing a zero trust architecture can be particularly effective, as it enhances security without introducing performance bottlenecks. Zero trust networks ensure that connection issues do not compromise security and that access control is both strict and adaptable to different user environments.

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



To counter these vulnerabilities, organizations should adopt proactive security measures like a zero trust model. Zero trust enforces stringent access controls and continuous verification of all network connections, regardless of their origin. This strategy effectively mitigates the risks posed by a wide array of attacks that exploit VPN weaknesses, limiting lateral movement and reinforcing robust access controls.

VPN Vulnerability Exploits

The variety of cyberattacks that exploit VPN weaknesses highlights the breadth of risks organizations face. The survey reveals that 42% of respondents identify ransomware attacks as most likely to exploit VPN vulnerabilities, highlighting significant impact and frequent occurrences. This is followed by malware infections, reported by 35% of respondents, and DDoS attacks—noted by 30%—which compromise availability as well as the confidentiality and integrity of systems.

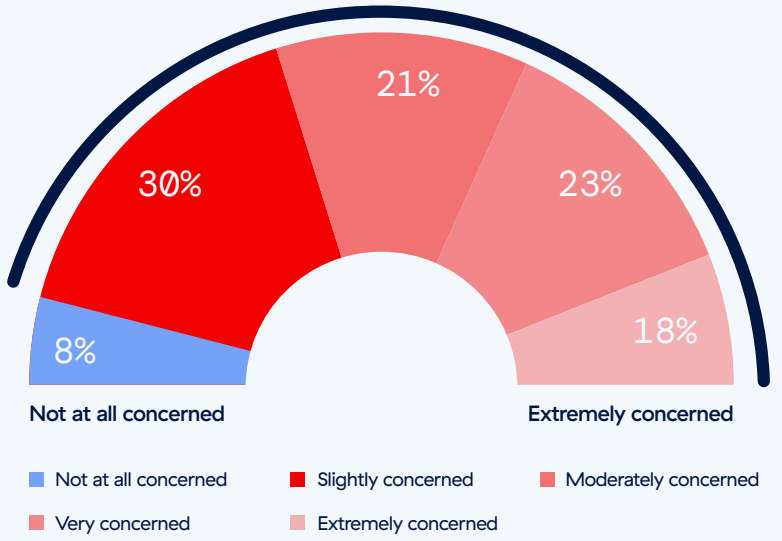
Third-Party VPN Risk

The survey underscores significant concern around third-party VPN access as a network security vulnerability. A notable 92% of respondents express apprehension about this risk, marking a slight increase from 90% in 2023. This growing recognition highlights the potential for third-party access to serve as an entry point for cyberthreats.

New insights into VPN vulnerabilities and breaches have further validated these concerns. Traditional VPNs typically provide extensive network access post-credential validation, posing risks if third-party vendors' security measures are compromised.

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

92% are concerned about third parties serving as a potential backdoor into their network through VPN access



Organizations should expedite their transition from traditional VPNs to zero trust architectures. This shift involves implementing systems that rigorously verify access requests based on identity and context, limiting third-party vendors to specific resources essential for their tasks.

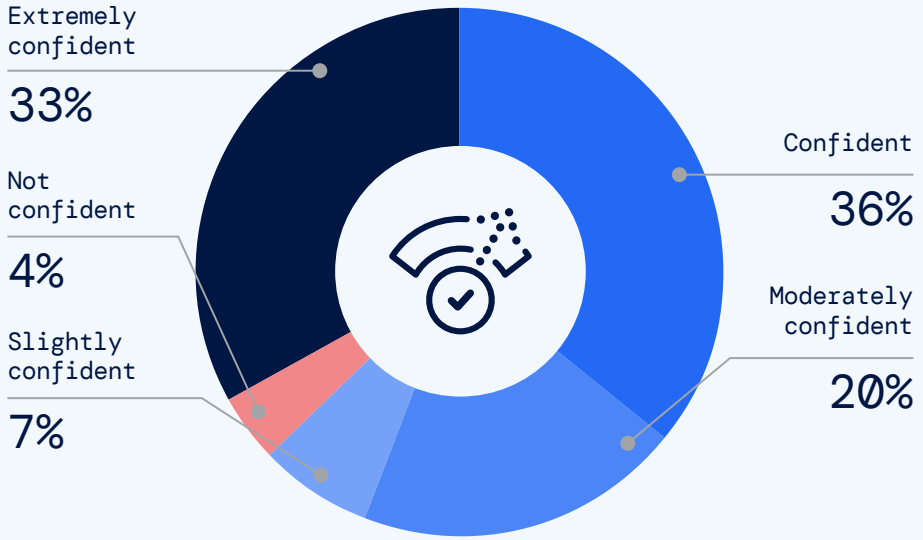
Security Issues with VPN Infrastructure

Overconfidence in VPN Security

The recent surge in VPN breaches highlights a disconnect between perceived security and actual risk. Recent high-severity exploits in VPN products underscore that even well-prepared organizations might be underestimating the capabilities of cyber adversaries exploiting vulnerabilities inherent in VPN technology. A significant 69% of survey respondents cited high confidence in their organization's ability to handle VPN vulnerabilities, which may not fully align with the escalating threat landscape where sophisticated actors exploit even minor weaknesses very quickly. Overconfidence can be particularly risky given the complexity and persistence of recent VPN exploits, as shown by incidents involving state-sponsored groups and cybercriminal gangs targeting unpatched systems for prolonged periods.

Organizations must recalibrate their security stance by incorporating rigorous vulnerability assessments, frequent updates, and comprehensive security awareness training. Adopting a layered security approach that does not overly rely on VPNs for comprehensive protection is advisable. This approach should include advanced monitoring, anomaly detection, and the integration of zero trust principles.

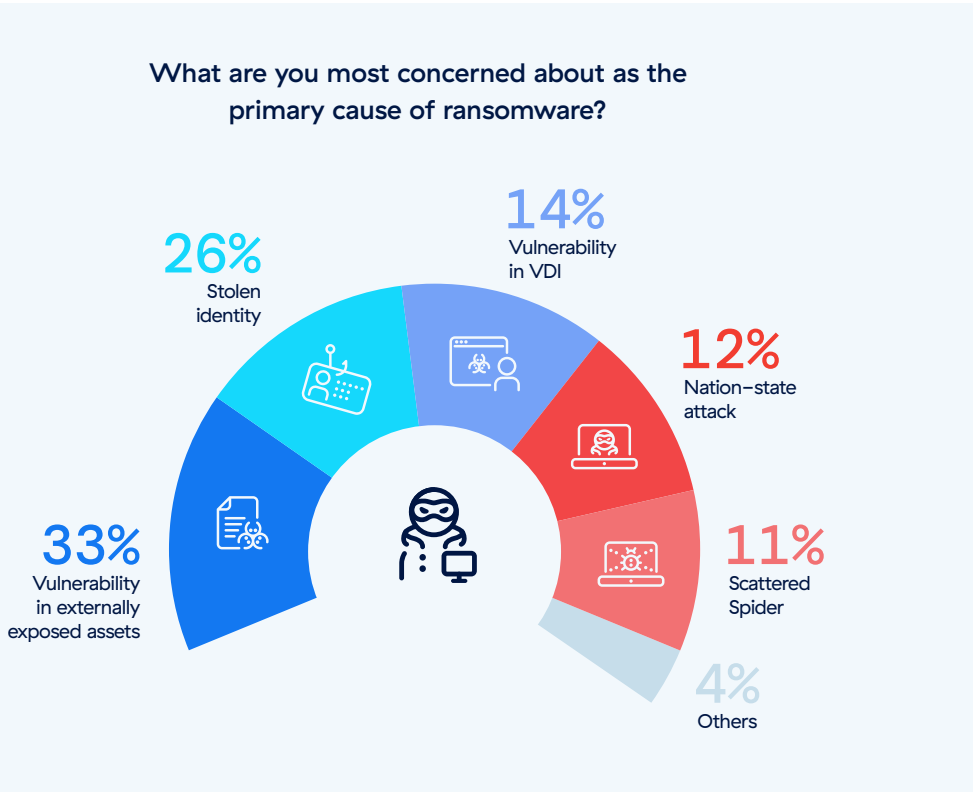
How confident are you in your organization's ability to detect and mitigate VPN vulnerabilities exposing it to cybersecurity attacks?



Ransomware Attack Vectors

The survey clearly identifies vulnerabilities in externally exposed assets as the most concerning potential attack vector of ransomware, noted by 33% of respondents. This points to widespread recognition of the risks associated with exposed network services or web applications, which are often the first point of entry for ransomware attacks.

Stolen identities follow closely at 26%, underscoring the role compromised credentials play in enabling attackers to bypass security measures and gain access to deliver ransomware payloads. Concerns about vulnerabilities in virtual desktop infrastructures (VDI) and nation-state attacks, at 14% and 12% respectively, highlight the diverse origins of ransomware threats that organizations must defend against. Scattered Spider (a cybercriminal group that uses sophisticated social engineering tactics, including phishing, multifactor authentication fatigue attacks, and SIM swapping), concerns 11% of participants.



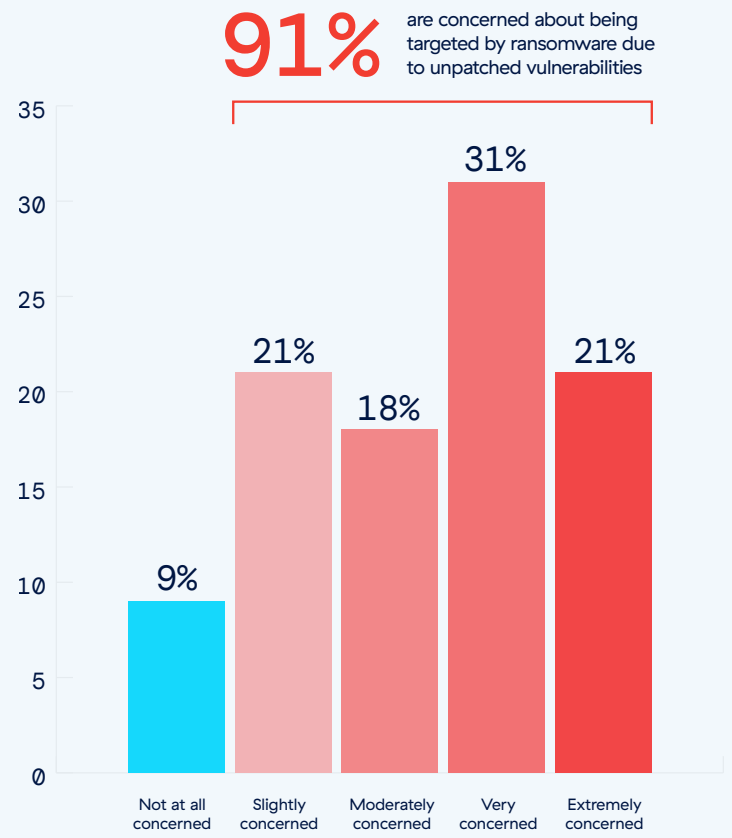
Organizations should enhance their defenses and identity management protocols. Implementing comprehensive vulnerability management processes and adopting a zero trust security model can effectively reduce the risk of ransomware attacks by denying access to network resources and lateral spread.

Ransomware Concerns

The survey results show 52% of respondents are very or extremely concerned about the threat of ransomware due to unpatched vulnerabilities. This is justified since unpatched vulnerabilities remain a primary attack vector for ransomware. Recent analyses show that a substantial portion of ransomware attacks exploit these vulnerabilities, with notably severe impact compared to other types of cyberattacks.

Ransomware groups are growing more sophisticated, with many now using advanced tactics that can quickly exploit newly discovered vulnerabilities before organizations can patch them. This rapid exploitation cycle greatly shortens the window for responding to critical vulnerabilities, highlighting the urgent need for advanced security measures that reduce the attack surface.

How concerned are you about being targeted by ransomware due to unpatched vulnerabilities?



Lateral Movement in VPN Attacks

Most respondents (54%) report that more than 25% of VPN-related attacks involved lateral movement, demonstrating significant containment failures at the initial point of compromise. Nearly one-third (32%) experienced lateral movements in more than half of attacks, indicating major challenges in controlling threat spread once adversaries breach network defenses.

Lateral movement is a significant risk with VPNs, as attackers can obtain broad network access similar to that of an authenticated user. This enables them to stealthily move across the network and target sensitive areas.

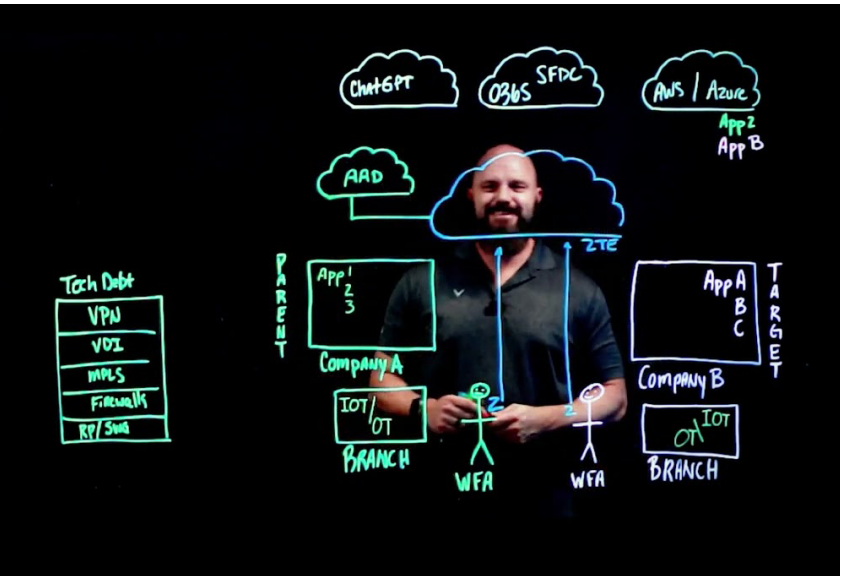
In this way, VPNs can compound risks and expand the scope of an attack beyond its initial entry point. Resolving this necessitates stringent segmentation, ideally with user-to-application traffic via a zero trust architecture, and continuous monitoring. This substantially reduces the blast radius of lateral movement by enabling granular access to a smaller set of applications for each individual user, while the rest are rendered invisible.

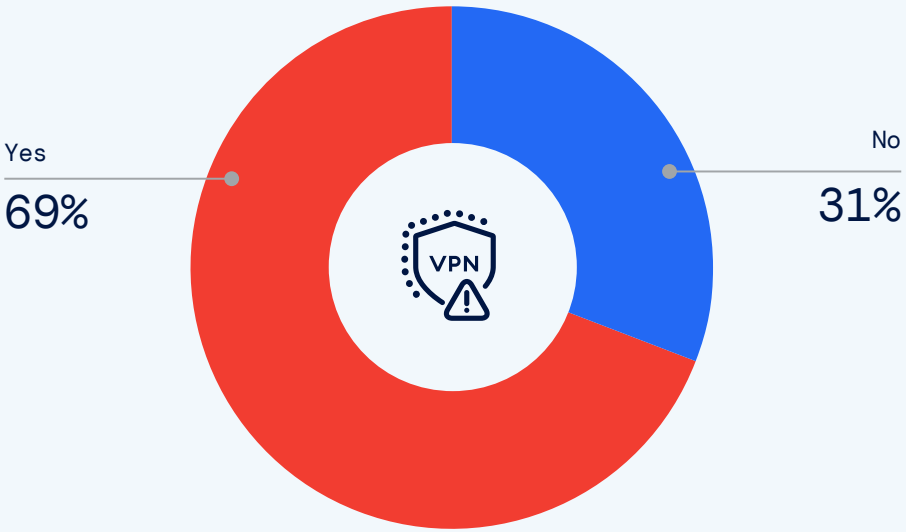
The rising sophistication of attacks exploiting VPN vulnerabilities underscores the need for a shift toward a zero trust framework. By enforcing strict access controls and continuous verification, zero trust limits unauthorized lateral movements and enhances security across expanding digital landscapes.

VPN Security Concerns After M&A

Concerns around the impact of mergers and acquisitions (M&A) on existing VPN infrastructure spotlight the potential vulnerabilities that arise from organizational changes and the integration of disparate networks.

A substantial 69% of respondents express apprehension about cyberattacks post–M&A, highlighting widespread concern over the security risks associated with these corporate transformations. This sentiment reflects a clear understanding that M&A activities can destabilize existing security frameworks, heightening exposure to cyberthreats.





Transition periods during M&A present unique opportunities for organizations to phase out antiquated, vulnerable VPN technologies in favor of zero trust frameworks. Specifically, zero trust architectures enhance security by providing comprehensive segmentation of the environment between users and applications, between workloads, branch locations, and devices, whether managed devices, unmanaged devices, IoT, or OT systems. This approach significantly bolsters security during and after a transition through rigorous verification of all users and devices, comprehensive segmentation, and strict enforcement of least–privileged access controls.

Enterprise Adoption of Zero Trust

Progress in Zero Trust Adoption

The survey reflects a strong trend toward adopting zero trust security frameworks, underscoring the growing recognition of their importance in enhancing organizational cybersecurity. A significant 31% of respondents are already implementing zero trust (up from 27% in 2023), indicating a growing proactive effort to better protect network resources.

Additionally, 27% of organizations plan to implement a zero trust strategy within the next six months (up from 18% in 2023), and another 20% of organizations plan to make the shift within the next 12 months, demonstrating a widespread commitment to transitioning to zero trust in the near future. This confirms that more than three-quarters of survey respondents (78%) recognize the urgency and benefits of zero trust.

However, 17% of respondents are still considering a zero trust strategy without a specific timeline (down from 23% in 2023), highlighting some hesitancy or potential challenges in planning or initiating the transition. Only a small fraction (5%) report no plans to adopt zero trust (down from 8% in 2023), possibly due to a lack of resources.

An analysis by company size indicates that larger organizations in our survey, particularly those with over 20,000 employees, are more likely and faster to adopt zero trust strategies, with 33% already implementing them. In contrast, smaller companies with 1,000–5,000 employees show a slightly lower adoption rate at 29%, suggesting that scale and resource availability may influence the pace and scope of zero trust integration.

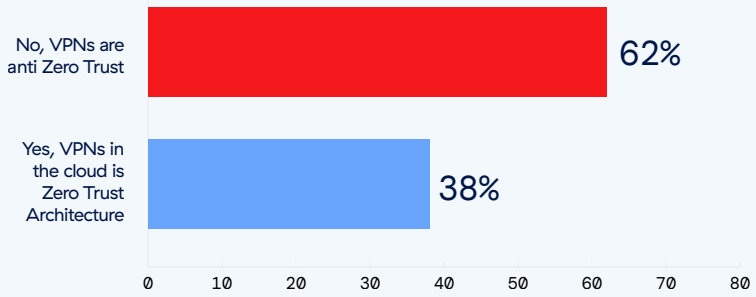
Organizations still on the fence or planning to adopt zero trust should start by assessing their current security posture and network architecture to identify specific needs and potential challenges.

No Zero Trust Security Through VPN

The survey results reflect a significant divide in beliefs about the compatibility of VPNs with zero trust security frameworks. Most (62%) believe that VPNs are fundamentally "anti-zero trust," confirming that traditional VPN architectures do not align with the principles of zero trust. Conversely, 38% of respondents view VPNs, especially cloud-based platforms, as compatible with zero trust architectures.

While this perspective may stem from VPN vendors claiming that their cloud-based solutions align with zero trust principles, it's important to scrutinize these assertions critically. Simply hosting a VPN service in the cloud, for example, does not automatically confer zero trust attributes. Zero trust security requires more than just a secure hosting environment; it mandates a fundamental shift from perimeter-based defenses to a model where security is dynamic, granular, and context-based.

Do you believe you can achieve Zero Trust security with VPNs?



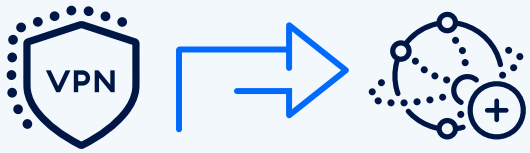
True zero trust security involves continuously validating all users and devices, applying least-privileged access, and segmenting traffic to prevent lateral movement—features that traditional VPNs, even cloud-based ones, do not provide. Therefore, organizations must confirm that any claimed "zero trust" VPN actually incorporates these core principles, rather than relying solely on marketing promises.

Advancing from VPN to Zero Trust Network Access

The survey results show that most organizations are making a strategic shift, with 53% of respondents citing plans to replace their existing VPN solutions with ZTNA solutions in the near future. ZTNA offers a more flexible and secure approach by enforcing policies based on user context, location, and device security, without assuming trust based on network location. This contrasts with traditional VPNs, which generally grant broad access to a network, creating security vulnerabilities.

For the 53% of organizations moving toward ZTNA, it is crucial to ensure a smooth transition by planning comprehensive risk assessments, updating access policies, and educating users about new protocols. Meanwhile, the 47% not yet planning to switch should evaluate their current security challenges and consider whether ZTNA could address these more effectively than VPN.

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



53%

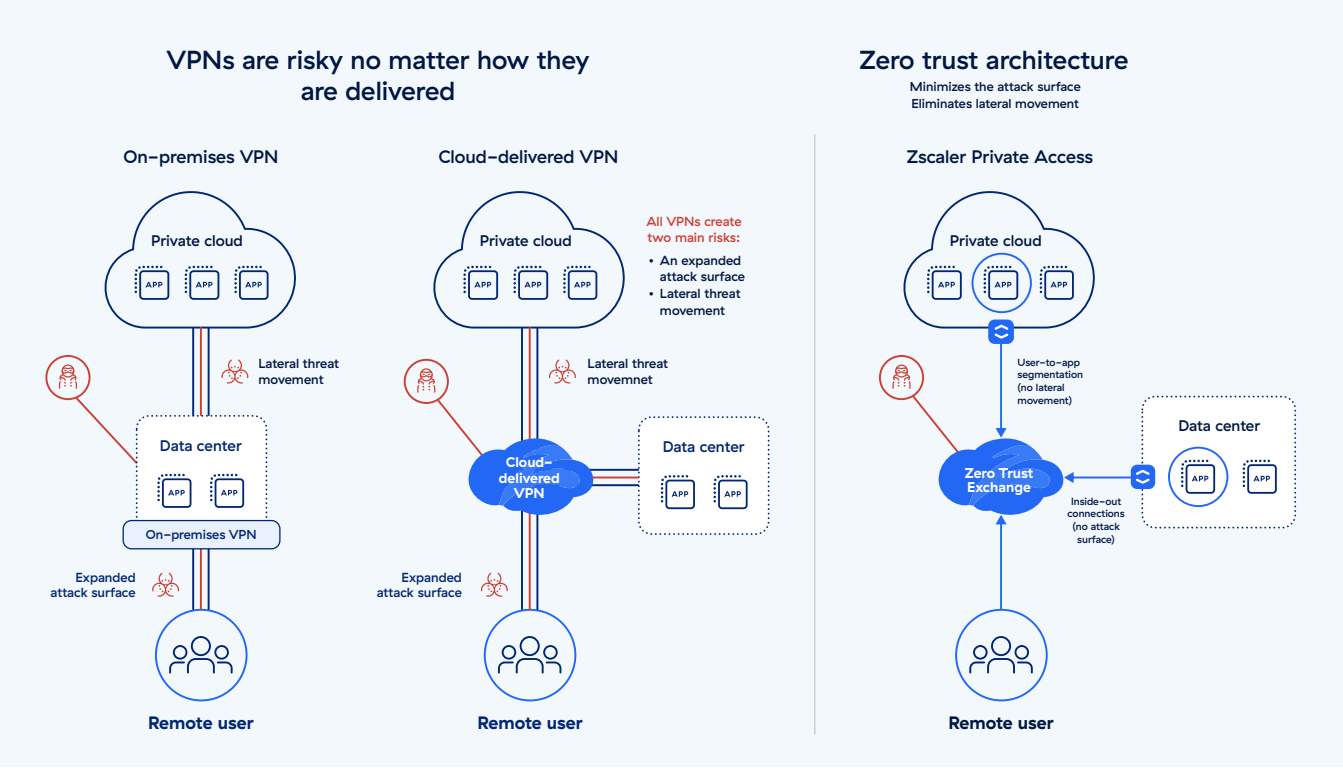
have plans to replace VPN with a ZTNA solution in the near future

Why Zero Trust is More Secure Than VPN

Architecturally, zero trust and ZTNA are more secure than traditional VPNs for several reasons, primarily due to a robust security framework that never inherently places trust in any single connection. Traditional VPN-based architectures are susceptible to a single point of failure. When a VPN or device is compromised (such as through a new CVE), threat actors can exploit the trust inherent in a flat network to gain access to the entire network, move laterally, steal data, and deploy ransomware. This is why security practitioners are increasingly concerned about the security risks of VPN.

On-premises and cloud-delivered VPNs present similar security vulnerabilities. Additionally, VPNs introduce complexity, resulting in unnecessary overhead and time-consuming tasks like user provisioning, routing table management, connectivity troubleshooting, patching, monitoring, and performance optimization.

In a zero trust architecture, no single connection is ever trusted. Users connect directly to applications—never to the underlying network. Moreover, every connection is automatically terminated, regardless of origin, before being verified by seven layers of zero trust security controls. Zero trust architecture allows organizations to comprehensively segment their environments with granular access—from users to applications, between workloads, between branch locations, and between devices, including IoT and OT devices.



Key Differences and Advantages

Significantly Reduced Attack Surface
A zero trust architecture enables inside-out connectivity that hides critical assets, applications, servers, and more from the public internet, while removing the need for vulnerable assets like VPNs and firewalls. This allows enterprises to provide hybrid connectivity for their workforces while greatly shrinking their attack surface. In contrast, VPN- and firewall-based architectures require enterprises to expand the attack surface to accommodate increased connectivity.

Continuous Verification
Zero trust models enforce continuous security verification of credentials and security posture before granting access to resources, making it much more difficult for unauthorized entities to gain and maintain access to sensitive information and systems. Meanwhile, with VPNs, the user or device often has extensive access to network resources once access is granted.

Least-Privileged Access
Zero trust principles enforce least-privileged access policies, ensuring that users and devices only have access to the resources necessary for their specific roles. This minimizes the risk of internal threats and lateral movement within a network, which are common vulnerabilities in VPN setups.

Granular Access and Segmentation
By dividing network resources into separate segments—between users and apps, between workloads, between devices—zero trust isolates potential breaches to smaller zones, greatly reducing the impact of an attack. While organizations often try to segment their network environments, it's an operationally complex and costly process that, in practice, often remains incomplete, requires hundreds of discrete firewall rules, and exposes broader network areas to authenticated users.

Empowering Today's Hybrid Workforce
Zero trust makes it possible to easily extend lightning-fast access to private applications across remote users in addition to HQ, branch offices, and third-party partners.

Improved User Experience and Reduced Complexity
Zero trust enhances user experiences by eliminating the need for all remote traffic to route through a central network point, a common performance bottleneck with VPN. This architecture is better able to handle the scaling requirements of modern networks that include IoT and BYOD policies. Additionally, zero trust reduces management overhead by automating security controls and simplifying the enforcement of security policies across the network.

These architectural advantages make zero trust a compelling alternative to traditional VPNs, particularly in today's increasingly sophisticated and distributed threat landscape. For organizations looking to bolster their cybersecurity defenses, adopting a zero trust approach provides a more robust, flexible, and scalable security infrastructure.

VPN Predictions for 2024 and Beyond

1 Severe VPN vulnerabilities and exploits will increase

Given the frequency, severity, and scale of VPN vulnerabilities disclosed in the past year, enterprises should expect this trend to continue. Threat actors and security researchers are aware of the heightened risk of high-severity vulnerabilities in VPN products. In turn, they are actively hunting for more, making it likely that additional CVEs will be found in the coming months and years.

2 High-profile attacks caused by VPN will take the spotlight

Closely related to our first prediction, we will see more large organizations disclose breaches that result from exploited VPN vulnerabilities. In part due to the new SEC regulation guidelines which require public companies to disclose details around breaches with a material impact. As we have seen, threat actors consistently create backdoors in target environments when VPN vulnerabilities occur, only to exploit them at later dates, even after these vulnerabilities have been patched. As the year progresses, more of these will start to be disclosed in public SEC filings and hit the news.

3 A surge in AI-powered VPN offerings will raise security and privacy concerns

Amid ongoing advancements in AI, AI-powered VPN solutions will flood the market. However, enterprises should evaluate these offerings with caution. Although they will promise enhanced performance, the integration of AI will amplify security risks and increase opportunities for attackers to exploit VPN vulnerabilities. In addition, privacy concerns will arise from extensive data analysis that increases the risk of sensitive information being exposed.

4 Password-spraying attacks on VPNs will continue to grow

Attackers will increasingly find ways to exploit weak password management practices and unused default VPN connection profiles through password-spraying attacks. In these attacks, threat actors try the same password across many VPN accounts until they successfully log in, gaining unauthorized access. With numerous recent high-profile VPN breaches effectively leveraging this technique, enterprises should expect similar attacks to persist.

5 Enterprise spend will shift away from VPN toward zero trust connectivity

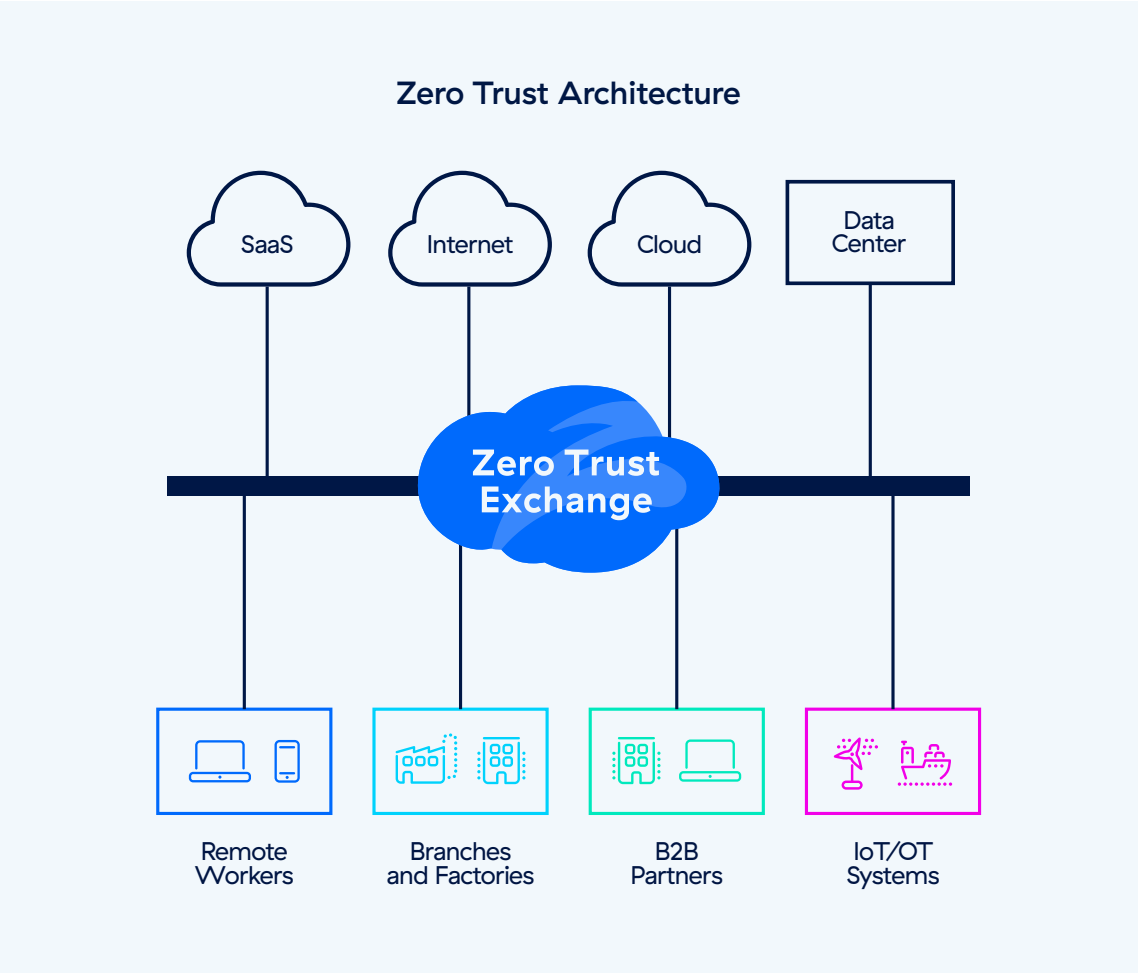
While VPN has long enabled remote connectivity for enterprises, the technology's consistent and growing security challenges will make it more challenging to justify long-term spending. As enterprises cement a consensus around zero trust as the preferred architecture for security and connectivity, enterprise budgets will continue to shift toward zero trust initiatives to secure the remote workforce.

How Zscaler Enables VPN Replacement and Zero Trust Transformation

Traditional firewalls and VPNs create a massive attack surface that lets attackers see and exploit exposed resources. By putting users on the network and letting them access any application it hosts, these legacy approaches give attackers easy access to sensitive data. They make it challenging and time-consuming to safely provide access or share resources with third-party vendors, contractors, and agencies. Beyond that, they drive up costs and complexity, and are too slow to serve today's hybrid workforce.

The Zscaler Zero Trust Exchange™ platform, the world's largest inline security cloud, securely connects users, workloads, IoT/OT, and B2B partners without extending network access.

Zscaler Private Access™ (ZPA™), an essential part of the Zero Trust Exchange, provides direct access to private applications hidden behind the Zero Trust Exchange, minimizing the attack surface, enabling granular 1:1 user-to-app segmentation, eliminating lateral movement, and delivering private app protection and inline traffic inspection while stopping zero-day threats—elevating your security posture. A cloud native service, ZPA can be deployed in just hours to replace legacy remote access tools like VPNs and VDIs.



Zero Trust Networking

ZPA enables granular, segmented access with inside-out connectivity to private applications and workloads. Moreover, ZPA includes a comprehensive set of access control services, including AI-powered user-to-app segmentation—with automated recommendations for user access policies and application segments—workload-to-workload segmentation, privileged remote access, private service edge, browser access, and more.

Cyberthreat Protection

ZPA delivers advanced cyber protection capabilities to secure your organization. These include app protection capabilities that use inline security inspection to stop the most prevalent application attacks and zero-day vulnerabilities, as well as deception technology that lures attackers with decoy apps and makes it easy to detect sophisticated threats.

Data Protection

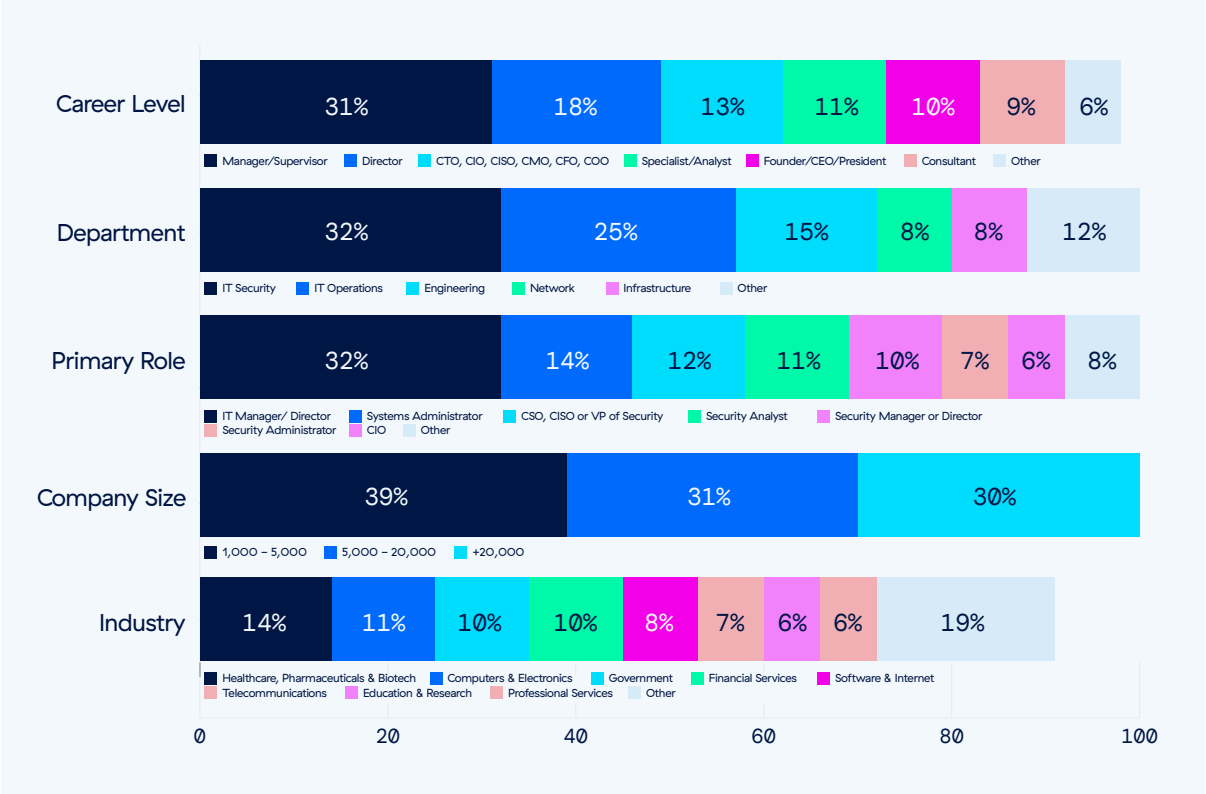
ZPA provides holistic data protection and stops data loss across all channels with web Data Loss Prevention (DLP), endpoint DLP, and browser isolation that prevents data leakage for vulnerable users and BYOD endpoints.

Best Practices to Counter VPN Risks

- **Minimize the attack surface:** Provide direct access to applications, ensuring that both apps and users are invisible to the internet, effectively preventing attackers from discovering and exploiting them for initial access.
- **Prevent initial compromise:** Inspect all traffic inline to automatically stop zero-day exploits, malware, and other sophisticated threats.
- **Block unauthorized access:** Use strong multifactor authentication (MFA) such as one-time passwords or tokens, biometrics, or FIDO2 credentials to validate user access requests. Conversely, weak MFA often uses approaches such as password reset questions.
- **Enforce least-privileged access:** Restrict permissions for users, traffic, systems, and applications based on identity and context, ensuring only authorized users can access approved resources (providing additional security in cases of MFA compromise or credential theft).
- **Eliminate lateral movement:** Connect users directly to apps, not the network, to limit the blast radius of a potential incident and mitigate the risk of lateral threat movement.
- **Shut down compromised users and insider threats:** Enable inline inspection and monitoring to detect compromised users with access to your network, private applications, and data.
- **Stop data loss:** Inspect data in motion and data at rest to stop active data theft during an attack.
- **Deploy active defenses:** Leverage deception technology with decoys and perform daily threat hunting to derail and capture attacks in real time.
- **Test your security posture:** Get regular third-party risk assessments and conduct purple team activities to identify and harden the gaps in your security program. Request that your service providers and technology partners do the same and share the results of these reports with your security team.

Methodology and Demographics

This report is based on the results of a comprehensive online survey of 647 IT and cybersecurity professionals, conducted in April 2024, to identify the latest enterprise adoption trends, challenges, gaps, and solution preferences related to VPN risk. Respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.



About Zscaler

Zscaler 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. To learn more, visit www.zscaler.com.

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 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.

Experience your world, secured.

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. To learn more, visit **www.zscaler.com**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com