netskope

REPORT

VPNs Under Siege

Why you need zero trust access in 2025

Research by

Cybersecurity

INSIDERS

Overview

Organizations are rapidly rethinking remote access as security threats escalate, performance issues persist, and hybrid workforces demand more flexible access. Legacy virtual private network (VPN) and network access control (NAC) systems, once the backbones of enterprise connectivity, are now struggling to keep pace with evolving security and usability demands. Attackers continue to exploit VPN vulnerabilities, users grapple with slow connections and complex authentication, and IT teams face growing challenges in managing access across an increasingly hybrid and cloud-first landscape.

To understand how businesses are responding, Cybersecurity Insiders surveyed 683 cybersecurity and IT professionals, capturing the key priorities, challenges, and strategies driving the shift from VPN to modern access models like zero trust network access (ZTNA) in 2025. The findings make one thing clear: organizations are actively taking steps to transition away from legacy VPNs and NAC solutions, adopting identity-aware, adaptive access models that enhance security, performance, and operational efficiency.

The survey reveals five key trends shaping the future of remote access security:

VPNs and NAC solutions are security liabilities: VPNs continue to be a major attack vector, with 56% of organizations experiencing a VPN-related security incident in the past year. These risks, combined with NAC's inability to enforce zero trust principles, are pushing organizations to rethink their access security strategies.

Organizations face persistent VPN performance and user experience challenges: VPN slowdowns and authentication struggles are frustrating end users, with 22% citing slow connections as their biggest complaint and 19% frustrated with complex authentication. These usability challenges reduce productivity and increase IT support burdens.

ZTNA adoption is accelerating: With 26% of organizations already deployed and another 37% planning implementation within the next year, ZTNA—once seen as a long-term strategy—is now viewed as an immediate priority to modernize remote access and replace legacy VPNs.

Security, infrastructure simplification and performance are the main drivers for ZTNA: 78% of organizations cite enhanced security as their primary reason for adopting ZTNA, reinforcing that risk reduction is the top motivator. Additionally, simplified infrastructure management (63%) and better application performance (51%) highlight that organizations see ZTNA as a way to both strengthen security and eliminate VPN complexity—making it a foundational step toward broader zero trust strategies.

Real-time visibility and hybrid access are becoming critical priorities: Organizations need ZTNA to go beyond VPN replacement by providing real-time monitoring, adaptive security policies, and seamless hybrid access. 86% of organizations consider real-time visibility critical, reinforcing its role in detecting threats and enforcing least-privilege access. With 75% prioritizing seamless policy enforcement across hybrid environments and 60% favoring ZTNA integration into SSE, organizations require deep visibility and continuous monitoring to maintain security consistency, detect anomalies, and optimize performance—making them essential rather than optional.

The findings in this report confirm an accelerating shift away from legacy VPN and NAC models toward ZTNA. Organizations need secure, seamless, and scalable access solutions that not only eliminate VPN security vulnerabilities but also resolve the performance and usability challenges that impact productivity. ZTNA delivers by enforcing least-privilege access, continuously verifying context that might require adapting trust levels, and providing real-time visibility across hybrid environments.

As organizations move forward, the transition to ZTNA is not just about replacing VPNs—it is about adopting a fundamentally more secure, adaptive, and efficient approach to access security that aligns with the realities of modern workforces and cloud-first IT strategies.

We thank Netskope for supporting this research and helping to highlight the evolving challenges shaping the future of remote access security. We hope this report serves as a practical guide for security professionals as they navigate ZTNA adoption and the transition away from legacy VPNs and NACs.

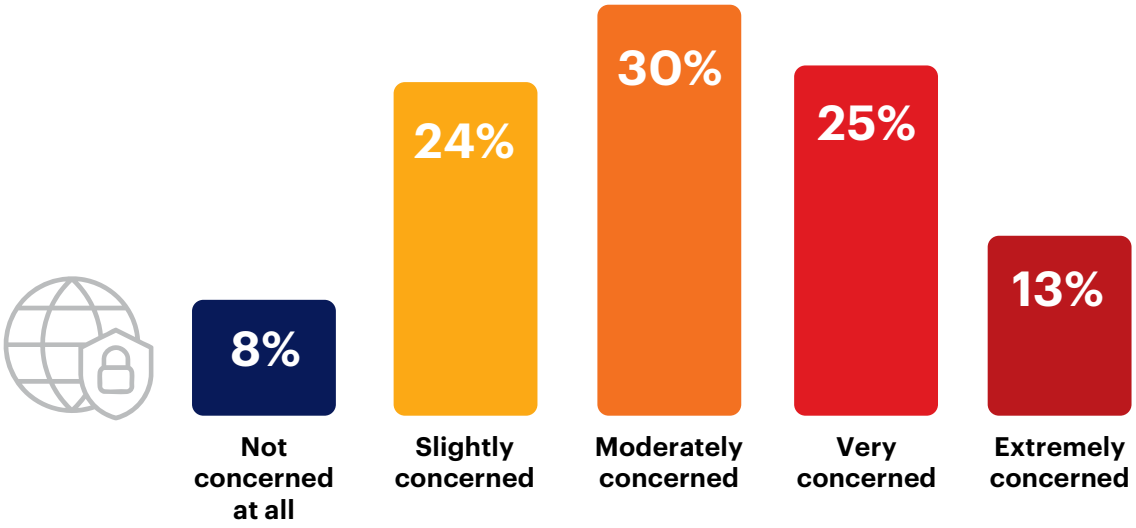
Holger Schulze
Founder, Cybersecurity Insiders

Why VPNs and NAC Are Security Liabilities

Rising Concerns Over VPN Security

Organizations relying on VPNs for secure remote access are facing mounting security risks as credential theft, lateral movement attacks, and unpatched vulnerabilities continue to be exploited. VPNs were not designed for today's highly distributed, cloud-first environments, and their reliance on implicit trust leaves organizations exposed. These risks are no longer hypothetical—92% of respondents express concern that VPNs are jeopardizing their security, with 38% very or extremely concerned.

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

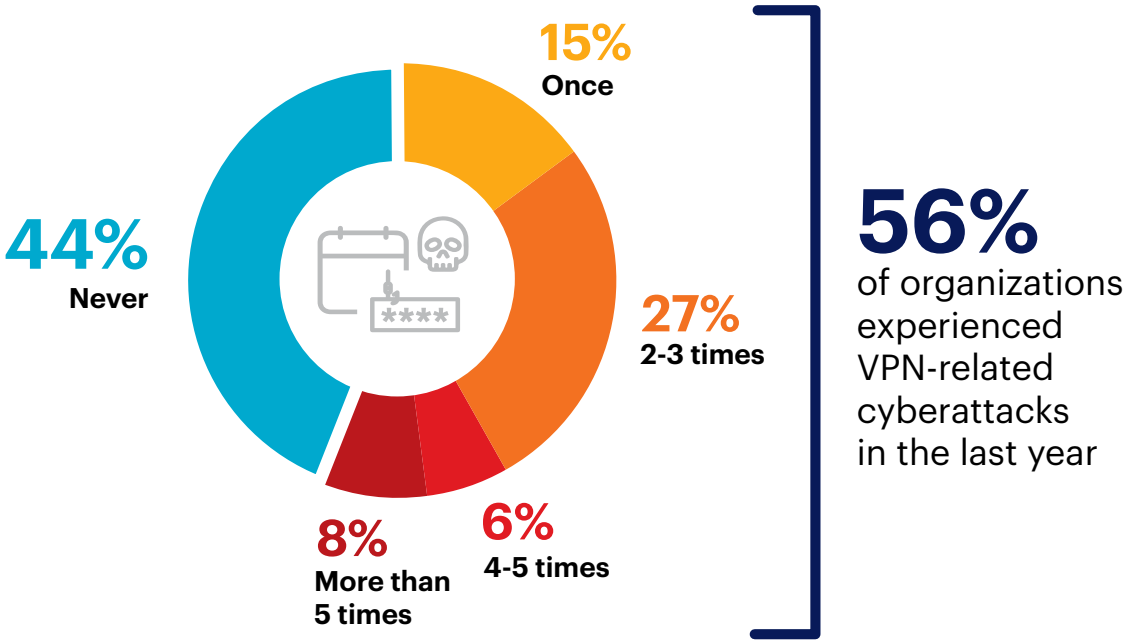


A series of high-profile VPN exploits in recent years has heightened cybersecurity concerns. Notably, attacks exploiting vulnerabilities in widely used VPN solutions have led to significant breaches affecting both enterprises and government agencies. In early 2025, security teams urgently addressed a critical vulnerability (CVE-2025-0282) in Ivanti Connect Secure VPN appliances, which allowed unauthenticated remote code execution. This vulnerability was actively exploited by attackers to gain unauthorized access to corporate networks.

Cases like this expose organizations to data exfiltration, ransomware infections, and operational disruptions, further validating concerns that VPNs are more of a security liability than a defense mechanism.

56% of organizations surveyed reported at least one VPN security incident in the past year, with 41% experiencing multiple VPN-related breaches, and 8% facing more than five incidents. This highlights that VPN weaknesses are not just occasional risks, but ongoing security liabilities.

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



With widespread concern about VPN security, the shift toward ZTNA is no longer just an option—it is becoming an operational imperative. Unlike VPNs, ZTNA eliminates broad network access rights, continuously verifies users and devices, and enforces least-privilege policies to reduce the attack surface and prevent the very security failures that make VPNs a persistent liability.

TIP: Netskope One Private Access – Eliminating VPN Security Gaps

Netskope's ZTNA (Netskope One Private Access) closes VPN attack pathways by replacing broad network access with identity-based, least-privilege controls. With continuous verification and zero trust enforcement, it constrains lateral movement and neutralizes persistent threats.

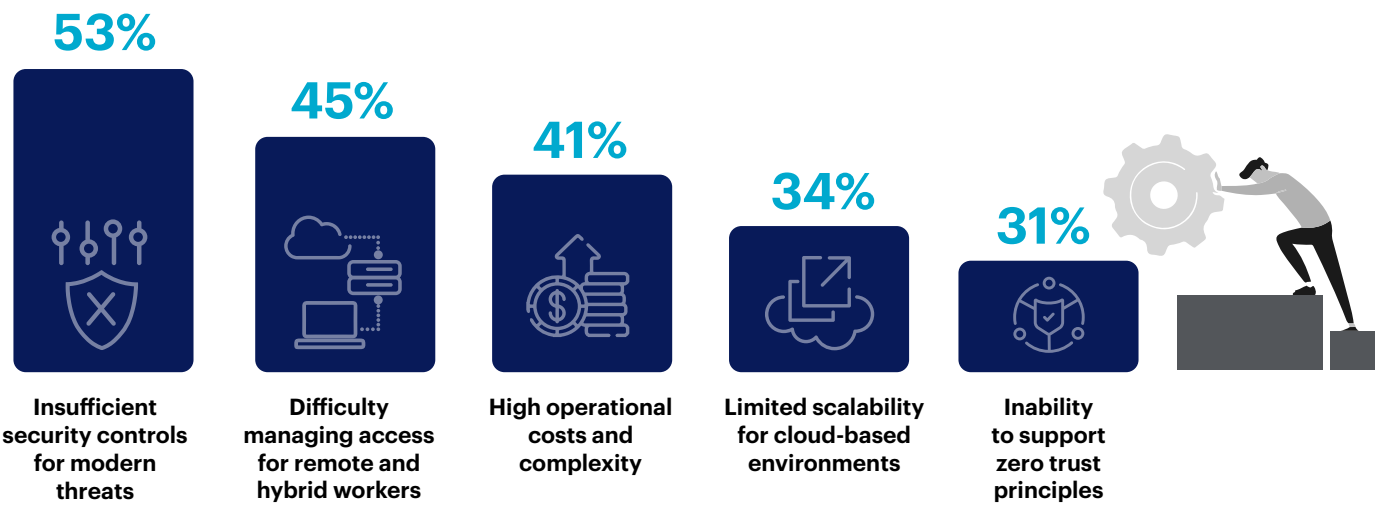
Network Access Control: A System Struggling to Keep Up

While VPN vulnerabilities expose organizations to external threats, outdated NAC systems present a different but equally concerning risk. Originally built for perimeter-based security, NAC solutions are struggling to keep up with modern, cloud-first environments, leaving security teams with blind spots, inefficiencies, and an inability to implement fine-grained access policies.

The most significant concern, cited by 53% of respondents, is that NAC solutions lack sufficient security controls to address modern threats. Traditional NAC was designed for static, perimeter-based networks. Operating primarily at Layer 2 and relying on 802.1X for user/device authentication, NAC solutions lack the ability to evaluate broader security signals, gather contextual insights, and enforce a true zero trust strategy. While some can profile devices, this alone is insufficient for adaptive, risk-based access control, making them ill-equipped to handle the sophistication of today's cyber threats, such as ransomware, insider threats, and cloud-based attacks.

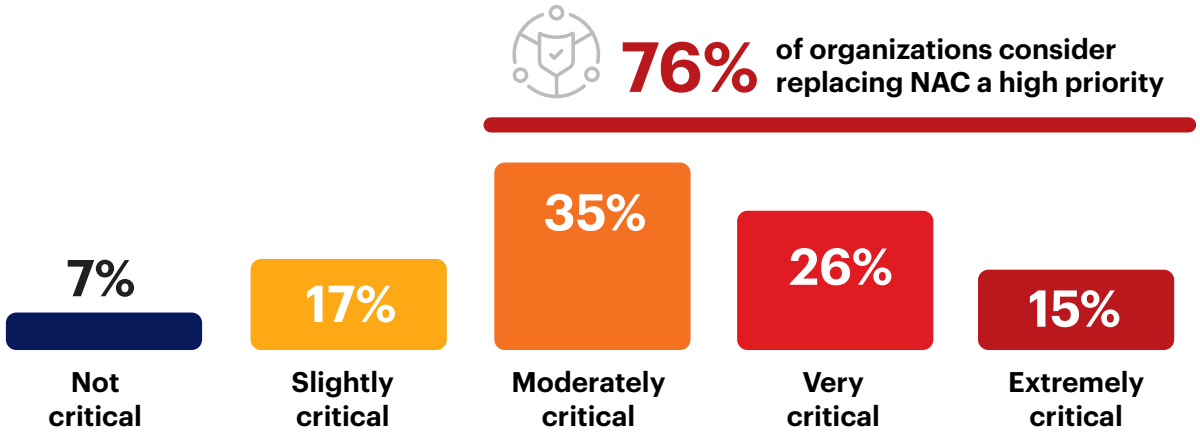
45% of respondents struggle with managing access for remote and hybrid workers, which underscores NAC's limitations in securing endpoints beyond the traditional corporate network— something it was never designed to do. Additionally, 41% point to high operational costs and complexity, reflecting the administrative burden and hardware often required for NAC deployments. 34% cite limited scalability in cloud-based environments as a problem, reinforcing the idea that legacy NAC solutions were never designed for the dynamic and elastic nature of cloud adoption. Lastly, 31% acknowledge NAC's failure to support zero trust principles, revealing a growing dissatisfaction with solutions that rely on implicit trust rather than continuous verification.

What challenges does your organization face with its current NAC (network access control) solution?



The survey data demonstrates a clear urgency to replace NAC: 76% of organizations consider replacing NAC a high priority, with 41% deeming it very or extremely critical. This reflects widespread recognition that NAC's rigid structure, reliance on predefined trust, and limited visibility into user behavior are no longer viable in today's dynamic environments.

How critical is it for your organization to replace legacy NAC solutions with a more flexible and secure alternative, such as zero trust network access (ZTNA)?



This urgency is well-founded. The 2024 CISA security incident exploited vulnerabilities in Ivanti's NAC solutions, specifically Ivanti Connect Secure and Ivanti Policy Secure. Attackers exploited multiple zero-day vulnerabilities—Including CVE-2023-46805 and CVE-2024-21887—to gain unauthorized access to CISA's systems. These vulnerabilities allowed attackers to bypass authentication and execute arbitrary commands, leading to the compromise of two CISA systems.

A ZTNA model could have mitigated this risk by enforcing continuous authentication, restricting lateral movement, and ensuring real-time risk-based access controls.

Incidents such as these make it clear that organizations need to transition away from legacy NAC and adopt a Universal ZTNA model, using ZTNA for both on- and off-premises access to applications. Universal ZTNA uses an on-premises component to connect users to applications if both are at the same location, enforcing the ZTNA policy without the need to send traffic to the cloud service and back to the application. Unlike traditional NAC, ZTNA dynamically enforces least-privilege access, continuously verifies users and devices, and scales effortlessly across cloud and remote environments. By embracing a more flexible and identity-aware approach to access security, businesses can enhance threat neutralization while enabling greater agility, adaptability, and streamlined operations.

Excessive Privileges: A Growing Security Concern

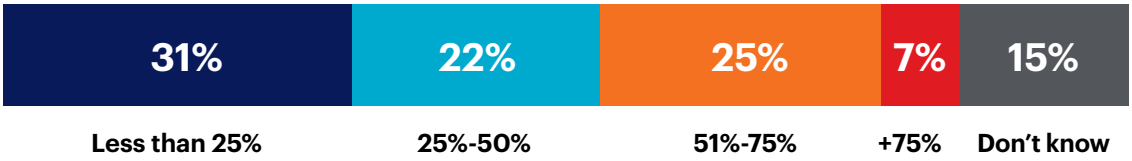
Beyond the challenges posed by VPNs and NAC, organizations face another critical access-related risk: users possessing privileges beyond what is necessary for their daily tasks, thereby expanding the attack surface and increasing the likelihood of security incidents.

The survey confirms this troubling reality: 32% of respondents estimate that more than half of their security incidents stemmed from users having more access than necessary. An additional 22% believe that between 25% and 50% of incidents derive from this issue.

A high-profile example of excessive privilege misuse occurred in the 2021 Verkada data breach, where attackers obtained "super admin" credentials that granted unrestricted access to 150,000 surveillance cameras across hospitals, prisons, and manufacturing facilities. The breach exposed how overprivileged accounts create massive security gaps, allowing attackers to compromise entire systems through a single credential.

To mitigate these risks, organizations must enforce least-privilege access policies, continuously monitor entitlements, and minimize the number of accounts with elevated permissions.

About what percentage of your organization's security incidents in the last 12 months do you believe were caused by end users possessing access privileges beyond what they require for their daily work?



TIP: Netskope One Private Access – Enforcing Least-Privilege Access for Stronger Security

A ZTNA project creates the perfect opportunity to re-evaluate legacy privileges that have accumulated over time (often as an individual moves through job roles), and can ensure that all privileges are aligned to exactly what each user needs for their current role. Netskope enforces identity-aware, least-privilege access, ensuring users access only what they need—nothing more. With continuous access evaluation and adaptive security controls, Netskope reduces the risk of credential misuse, lateral movement, and large-scale breaches, strengthening zero trust security.

The VPN User Experience Problem

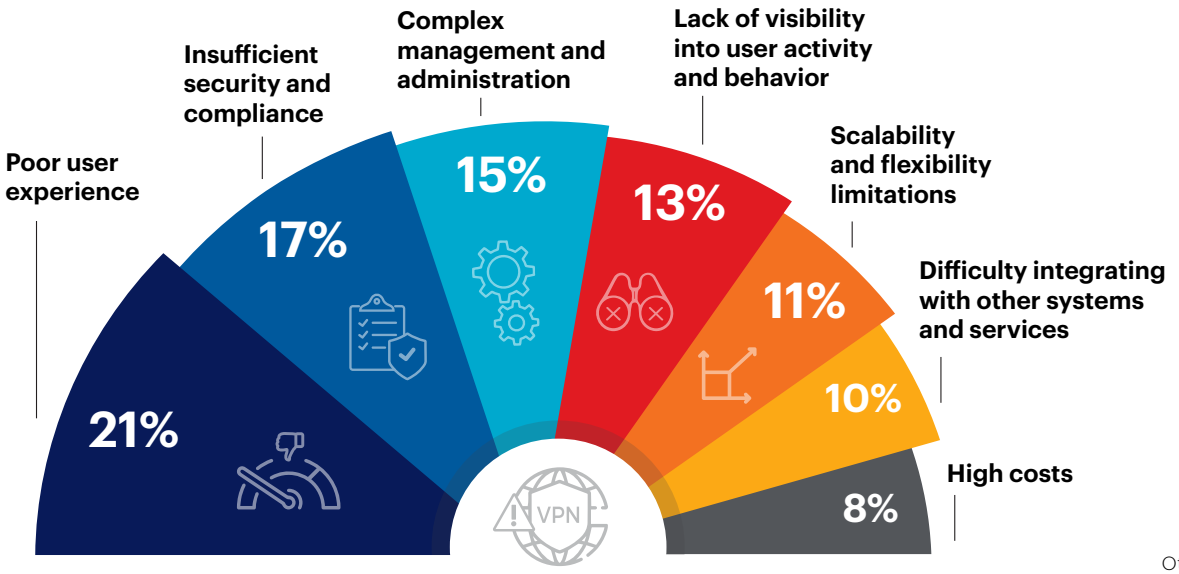
Persistent User Frustrations with VPN Access

Despite their long-standing use, VPNs are increasingly seen as a source of frustration rather than a reliable access solution. Originally designed to remotely manage networks, their remit expanded slightly in the pre-cloud, office-centric era to allow a small number of employees to access corporate networks remotely. Today, VPNs struggle to meet the security, performance, and usability demands of modern mostly-remote workforces. The survey data reflects this growing dissatisfaction, with both security and operational concerns driving organizations to rethink their reliance on VPNs.

The most highlighted issue, cited by 21% of respondents, is poor user experience, with slow speeds and frequent disconnections reducing productivity and pushing users toward risky workarounds. 17% highlight insufficient security and compliance, reinforcing that VPNs inherently grant excessive trust, making it easier for attackers to move laterally within a network once they gain access. Additionally, 15% cite complex VPN management, adding to IT burdens, while 13% point to a lack of visibility into user activity, limiting security teams' ability to detect insider threats or compromised accounts.

ZTNA provides a faster, more seamless experience by enabling direct, secure access to applications without routing traffic through congested VPN gateways. ZTNA optimizes connectivity, reduces latency, minimizes disruptions, and streamlines authentication. As organizations phase out VPNs, they can significantly enhance remote access reliability and ensure a smoother, more efficient experience for their workforce.

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



Other 5%

TIP: Netskope One Private Access – Optimized User Experience Without VPN Hassles

Netskope delivers fast, identity-based access to applications by eliminating VPN slowdowns, disconnections, and congestion, and ensuring an optimal user experience. With adaptive security controls, optimized traffic routing, and a high-performance architecture, users enjoy secure, high-speed access without compromising security or productivity.

VPN Performance and Usability Struggles

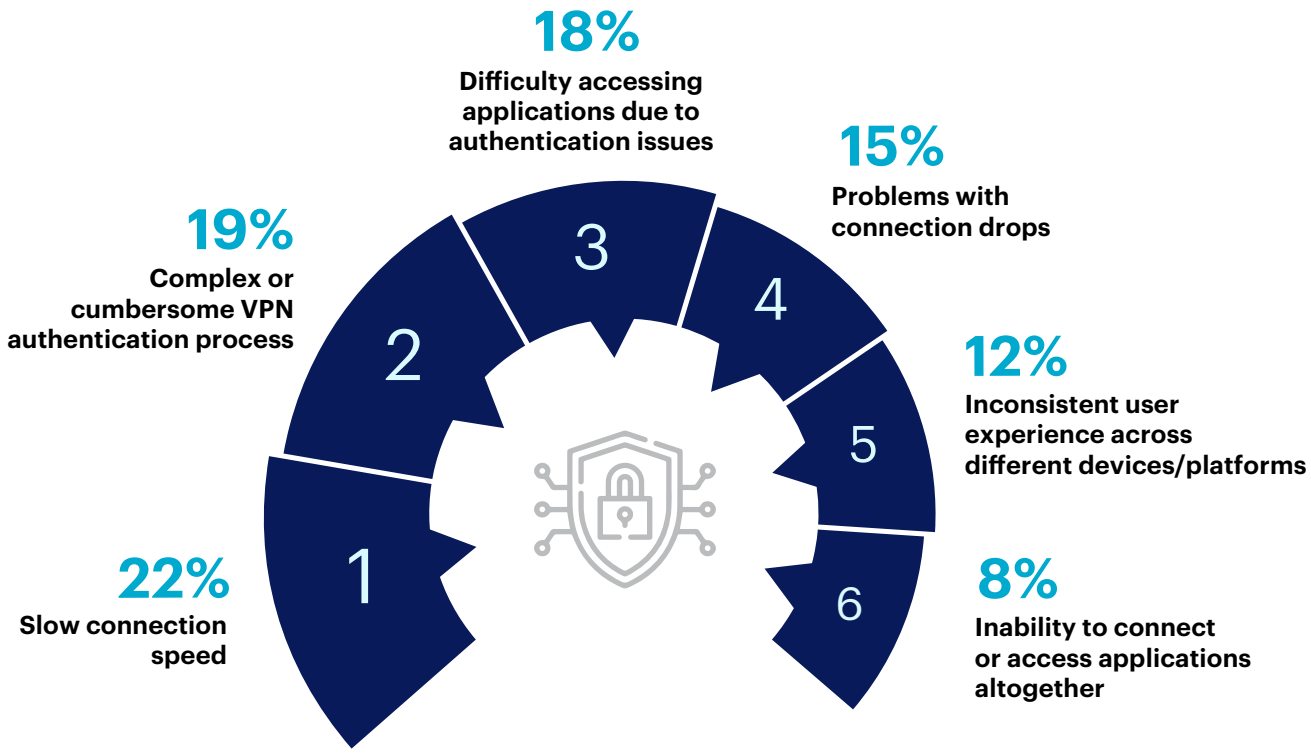
VPN performance challenges are more than just an inconvenience—they lead to lost productivity, increased IT support tickets, and growing frustration among employees.

The most common user complaint, cited by 22% of respondents, is slow connection speed, a direct result of the reliance of VPNs on the public internet. Authentication issues are another major pain point, with 19% reporting users frustrated by cumbersome login processes such as having to remember which VPN gateway or profile to use for specific applications, or frequent re-authentication requests. 18% struggle to access applications due to misconfigurations or compatibility issues.

Connection instability compounds these problems, as 15% report users experiencing frequent VPN dropouts that force them to reconnect and lose progress on tasks. Another 12% report inconsistent performance across different devices, making remote work unreliable.

Organizations relying on VPNs will continue to battle these inefficiencies. Shifting to ZTNA provides direct, identity-based access to applications without routing traffic through overloaded VPN concentrators, resolving performance issues while enhancing security.

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



Other 6%

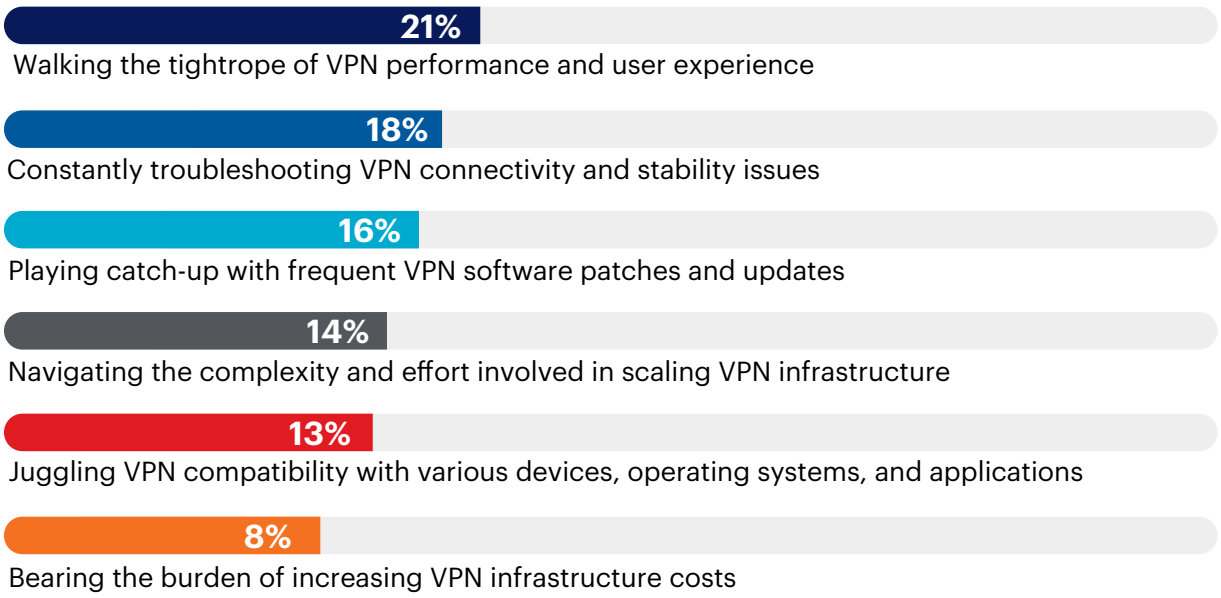
The Operational Burden of VPN Management

While VPN performance issues frustrate end users, IT teams bear the brunt of ongoing maintenance, troubleshooting, and scalability challenges. VPNs were not designed for today's highly dynamic, cloud-driven environments, forcing security teams to constantly patch vulnerabilities, manage connection stability, and expand capacity to meet demand.

For 21% of organizations, maintaining VPN performance without degrading user experience is the biggest challenge, as congestion and latency issues create ongoing disruptions. 18% report frequent troubleshooting of connectivity and stability problems, pointing to the fragile nature of VPN tunnels, which are often impacted by network congestion or software conflicts. 16% struggle with the relentless patching required to secure VPNs, as these systems remain a frequent target for attackers. Scalability is another pain point, with 14% of organizations reporting difficulty expanding VPN infrastructure to accommodate growing hybrid and remote workforces. 13% cite compatibility issues across different devices and operating systems, highlighting the rigid architecture of VPNs.

For IT teams already stretched thin, these management burdens are unsustainable. As networks become more distributed, VPNs will only become more complex and costly to maintain. ZTNA eliminates these persistent issues by providing direct, identity-based access to applications, removing the need for complex tunnel configurations, frequent patching, and scalability constraints—offering IT teams long-term relief from the inefficiencies of VPNs.

What is the biggest headache in managing your VPN infrastructure?



Other 10%

TIP: Netskope One Private Access – Eliminating VPN Complexity for IT Teams

Netskope replaces VPN tunnels, constant patching, and scalability issues with direct, identity-based access on the high-performance NewEdge Network. With simplified management, deep visibility, and real-time insights, IT teams get faster troubleshooting, reduced complexity, and a future-ready secure access solution.

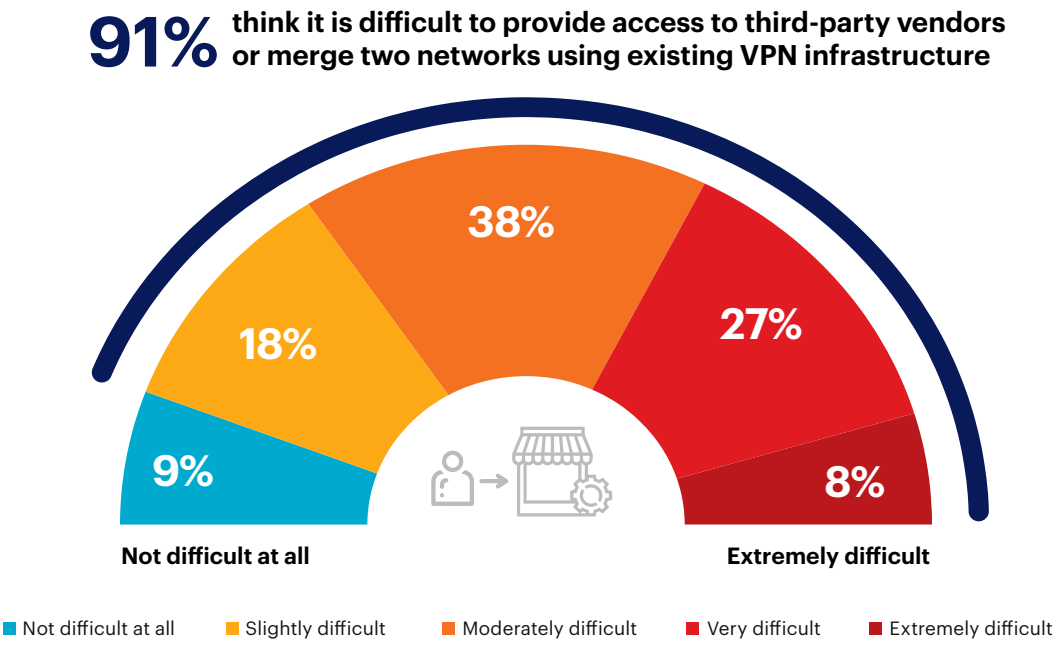
VPNs Struggle with Mergers and Third-Party Access

VPN limitations create systemic challenges when organizations need to extend access to third parties or integrate networks after a merger.

The survey reveals that 91% of respondents find providing access to third-party vendors or merging VPN networks difficult, underscoring VPNs' rigidity and administrative complexity in dynamic business environments. Notably, 35% of organizations describe the process as very or extremely difficult, highlighting VPN-based access models' struggles with scalability, policy enforcement, and security risks.

Traditional VPNs are ill-suited for modern business agility. ZTNA offers a more adaptable solution for mergers and acquisitions and third-party access, allowing organizations to grant granular, role-based access to third parties without exposing the broader network. By eliminating the need for complex VPN configurations and enforcing identity-aware policies, ZTNA streamlines post-merger IT integration and vendor access management, reducing friction and security risks.

How challenging is it to provide access to third-party vendors or merge two networks using your existing VPN infrastructure during a merger or acquisition?



TIP: Netskope One Private Access – Flexible, Secure Access for Third Parties & Mergers

Netskope eliminates VPN complexity by enabling agent-based or agentless onboarding for contractors, M&A integrations, and BYOD users. With granular, identity-aware policies, it ensures secure, scalable access without exposing the broader network—streamlining third-party management while reducing risk.

The Rise of ZTNA: Adoption Trends and Transition Strategies

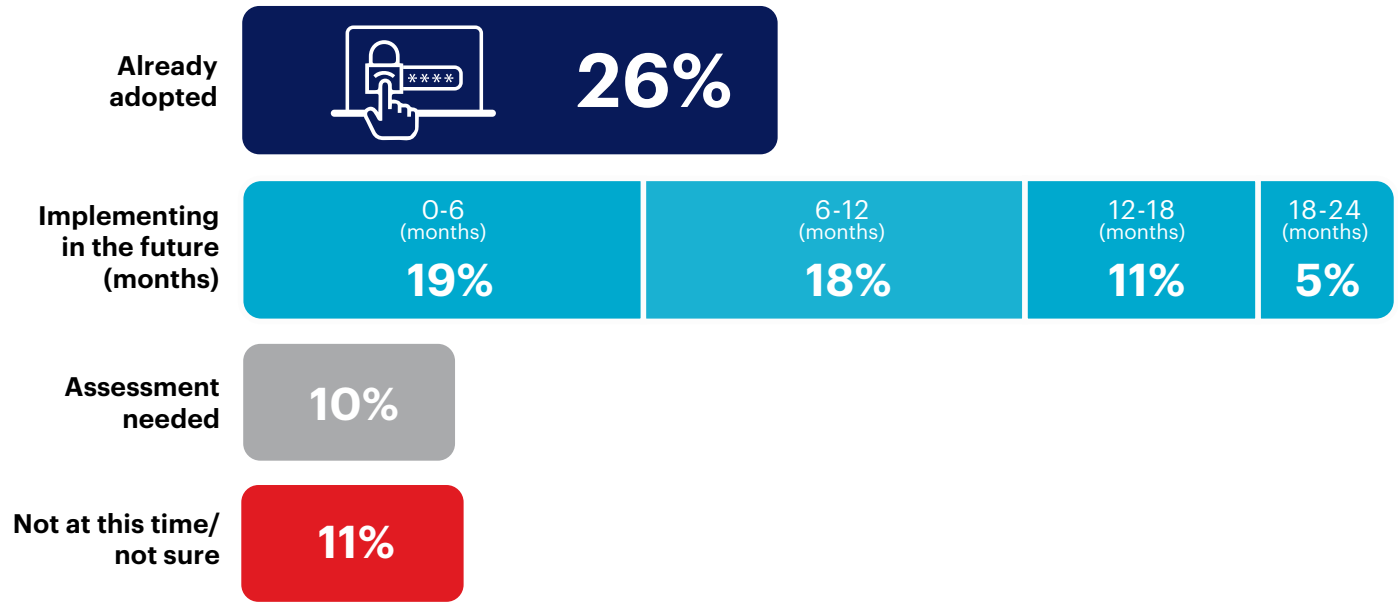
The Shift Away from Traditional VPNs

As organizations grapple with all these challenges, many are actively evaluating modern remote access alternatives for replacing traditional VPNs.

In terms of timing, the survey shows that 79% of organizations have either already adopted ZTNA or plan to do so within the next 24 months, signaling a decisive industry shift.

Adoption momentum is strong, with 26% of organizations having already deployed ZTNA and another 37% planning to implement it within the next year. Unlike in past years, when zero trust was seen as a long-term strategy, many organizations now view ZTNA as an immediate priority to modernize remote access and reduce security risks—and as a step toward developing a full zero trust strategy.

Do you plan to adopt a zero trust network access (ZTNA) service within the next 24 months?



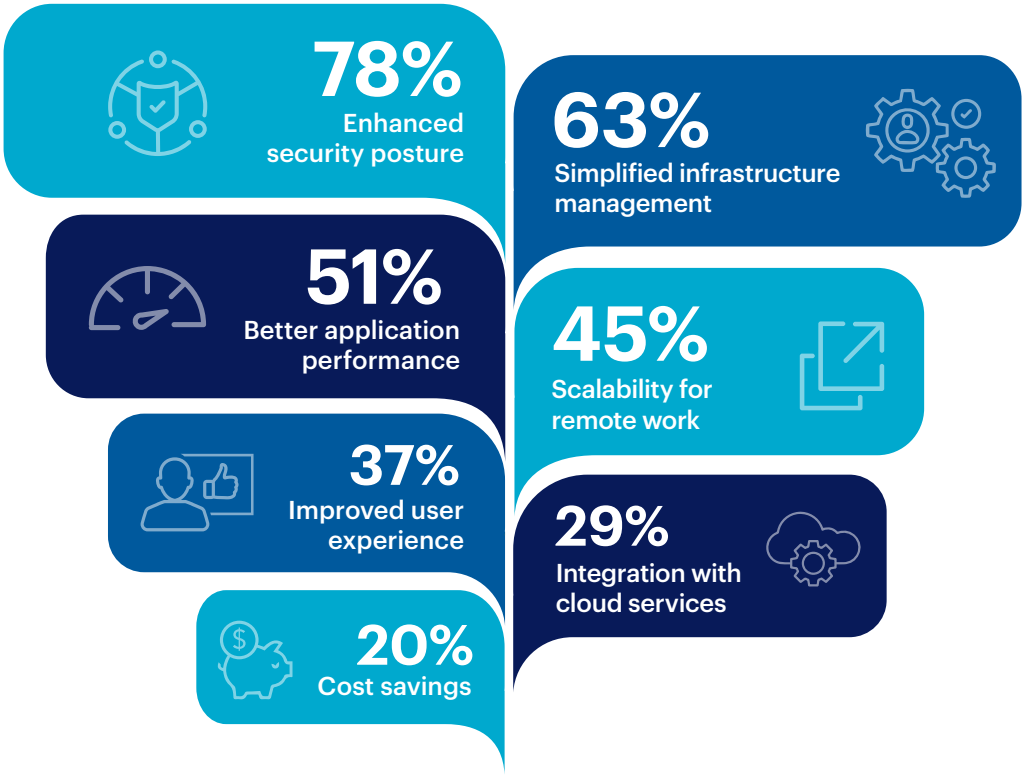
Why Organizations Are Replacing VPNs with ZTNA

Organizations are making the shift from VPN to ZTNA to address security risks, reduce complexity, and improve performance.

- Security remains the primary driver to ZTNA, with 78% of organizations prioritizing enhanced security posture.
- 63% of organizations seek to simplify infrastructure management.
- 51% are focused on performance, looking for faster, more efficient connectivity.
- 45% of organizations are prioritizing remote work scalability, ensuring access solutions can support a distributed workforce without constant VPN capacity upgrades.
- 37% seek a more seamless user experience, identical when both on- or off-premises, reducing authentication friction and connection instability.
- 29% are looking for better integration with cloud services, as organizations shift from traditional data centers to SaaS and hybrid environments.

While cost savings (20%) remain a secondary factor for most, organizations recognize that ZTNA delivers more than just security improvements—it can also bring significant budgetary gains too by reducing management resource requirements, removing hardware shipping and localized maintenance, and allowing for greater scalability to better match usage levels.

What benefits does your organization seek by transitioning from VPN to a ZTNA solution?



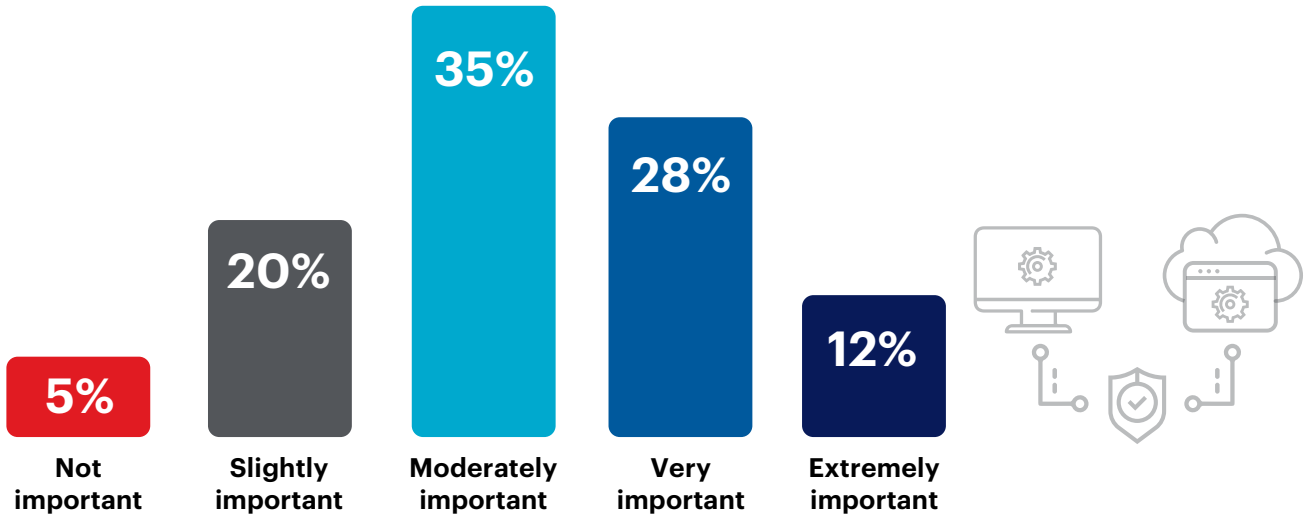
ZTNA Replaces VPN and NAC for Access Security

As organizations accelerate ZTNA adoption, many are prioritizing a full replacement of legacy VPN and NAC solutions to support hybrid cloud environments with seamless policy enforcement. The survey confirms this trend, with 75% of respondents considering it at least moderately important for ZTNA to provide consistent access across both on-premises and cloud applications. A strong 40% categorize this need as very or extremely important, underscoring the urgency of moving beyond outdated access models.

Businesses can transition to ZTNA at their own pace, based on their specific needs, workloads, and security priorities. Moving critical applications and cloud services to ZTNA immediately enhances security, performance, and user experience, eliminating VPN bottlenecks and risks. The key is to shift away from outdated access models, embracing ZTNA's dynamic, least-privilege approach to build a scalable, future-ready security posture.

With ZTNA increasingly positioned as the foundation of modern access security, organizations still relying solely on VPN and NAC will struggle to maintain efficiency and security at scale. Selecting the right ZTNA solution is critical, as not all ZTNA offerings are the same. Simply running VPN alongside a first-generation ZTNA is not enough. To fully eliminate legacy VPNs, organizations must adopt a ZTNA solution that supports all essential legacy applications. Without this capability, they risk retaining outdated VPN infrastructure for certain applications, leading to operational inefficiencies, security gaps, and added complexity.

How important is it for your ZTNA solution to fully replace VPN and NAC by enabling hybrid use cases, providing seamless access to both on-premises and cloud applications with consistent policy enforcement?



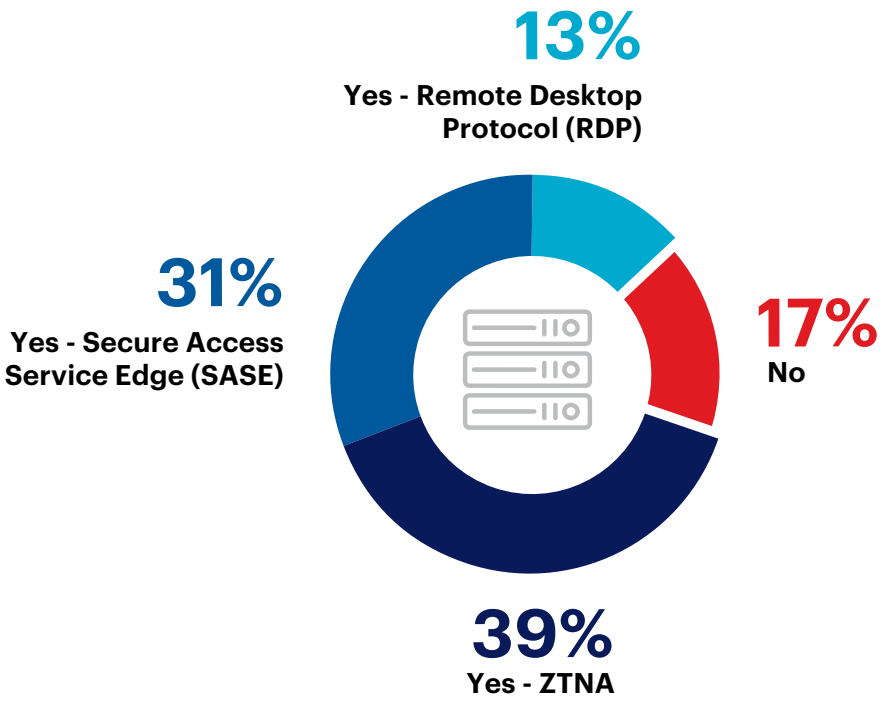
ZTNA and SSE: A Unified Security Strategy

As organizations transition to ZTNA, many are integrating it into broader secure access service edge (SASE) and security service edge (SSE) strategies to enhance security, streamline access control, and ensure consistent protection across cloud and on-premises environments. Rather than managing disconnected security tools, businesses are prioritizing converged solutions that unify access enforcement, data protection, and real-time threat neutralization.

The survey confirms this trend, with 31% of organizations considereing SASE as a remote access alternative.

The popularity of an integrated SASE approach to zero trust reflects a broader shift toward cloud-native security, integrating zero trust principles with networking capabilities to reduce complexity and improve visibility.

Have you considered remote access alternatives to traditional VPN?

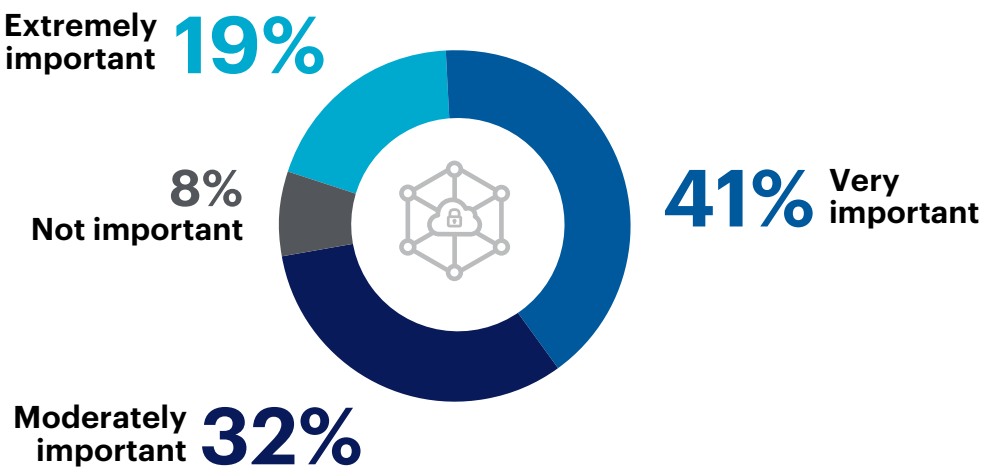


Looking specifically at the SSE security components of a SASE architecture, 60% of respondents consider ZTNA's integration into SSE very or extremely important, and another 32% rate it as moderately important. This highlights the increasing recognition that ZTNA alone is not enough—organizations need an access strategy that works seamlessly across web, SaaS, and private applications while maintaining continuous monitoring and adaptive security policies.

While standalone ZTNA significantly improves access control, SSE takes it further by integrating web security, SaaS governance and control, and threat neutralization into a single, cohesive platform. Organizations still relying on fragmented security tools face inefficiencies, limited visibility, and policy inconsistencies that increase risk.

By adopting ZTNA as part of an SSE or SASE platform, businesses gain unified security controls, seamless access management, and real-time visibility—essential for protecting hybrid workforces without adding complexity.

How important is it that a ZTNA service is part of an overarching security service edge (SSE) platform?



TIP: Netskope One Private Access – Seamless Integration Within a Unified, Scalable SSE Platform

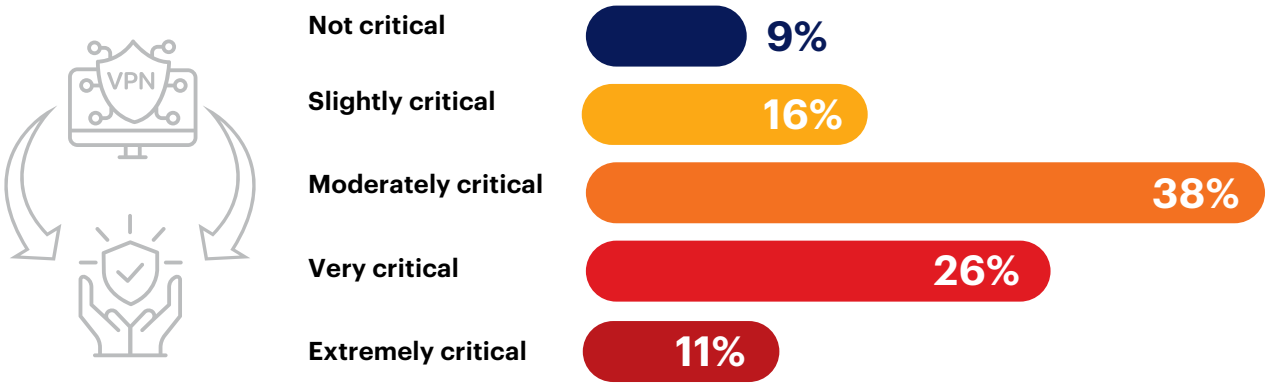
Netskope goes beyond standalone solutions by integrating ZTNA into the full Netskope One SASE/SSE platform. This ensures consistent policy enforcement across web, SaaS, and private applications, unifying access control, data protection, and threat prevention for better security, visibility, and operational efficiency. Customers also benefit from a scalable architecture, allowing them to easily add new security services over time; with AI-powered Netskope One Digital Experience Management (DEM), organizations gain real-time traffic visibility, performance insights, and an optimized user experience, all seamlessly integrated into a broader zero trust strategy.

The Growing Demand for Application-Aware Access

Modern access solutions must support real-time services such as VoIP and remote assistance tools without introducing latency or connectivity disruptions. While a VPN can process server-initiated traffic after the VPN connection is established, their well-known problems of latency, unreliable connections, and security gaps degrade user experience and operational efficiency. These challenges are especially problematic for latency-sensitive services, where even minor delays can result in communication failures, lag, and lost productivity.

The survey highlights the growing demand for modern access solutions that support both endpoint-initiated and server-initiated applications. 75% of organizations consider fully replacing VPNs with more application-aware solutions at least moderately critical, with 37% viewing this shift as very or extremely critical. However, to successfully eliminate legacy VPNs, organizations must choose a ZTNA solution that also supports all essential legacy applications. Without this capability, they risk being forced to maintain outdated VPN infrastructure for selected applications, creating further operational inefficiencies, security gaps, and unnecessary complexity.

How critical is it for your organization to fully replace legacy VPNs with solutions supporting client-initiated and server-initiated applications, including real-time services like VoIP and remote assistance tools?



TIP: Netskope One Private Access – Full VPN Replacement

Replacing legacy VPNs is crucial for supporting endpoint- and server-initiated applications, especially VoIP and remote assistance. Netskope One Private Access provides a complete VPN replacement, enabling network-level connectivity for server-to-endpoint scenarios and application-level connectivity for endpoint-to-server scenarios—ensuring secure, least-privilege connectivity without network exposure.

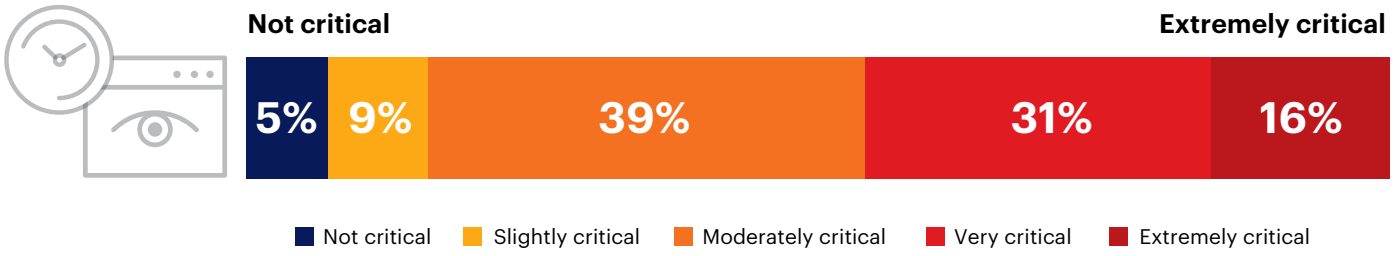
Real-Time Visibility: The Key to Secure ZTNA Adoption

As organizations transition from VPNs to ZTNA, real-time visibility into user activity and data access is becoming an operational necessity. The ability to continuously monitor access patterns and detect anomalies is essential for enforcing least-privilege policies and preventing unauthorized access before threats escalate.
The survey data confirms this priority, with 86% of respondents considering real-time visibility at least moderately critical when transitioning from VPN to ZTNA, and 47% ranking it as very or extremely critical.

Traditional VPNs provide limited visibility, granting broad network access with little insight into who is accessing what, from where, and under what conditions. ZTNA eliminates this blind spot by tracking user behavior in real time, dynamically adjusting permissions based on risk signals, and enforcing granular policies that adapt to changing security contexts. This enables security teams to proactively identify and contain threats rather than react to security incidents after they occur.

For organizations embracing ZTNA, visibility and adaptive controls must go hand in hand. The most effective deployments treat real-time insights as an integral part of access security, ensuring that ZTNA policies are continuously informed by user activity, risk indicators, and evolving threats.

How critical is real-time visibility into user activity and data access when transitioning from VPN to a ZTNA solution?



TIP: Netskope One Private Access – Real-Time Visibility for Smarter, More Secure ZTNA

Netskope One Private Access, fully integrated into the Netskope One SASE/SSE platform, provides continuous monitoring, adaptive access controls, and AI-driven insights to dynamically adjust privileges based on risk. With deep analytics and automated threat detection, organizations gain full visibility and control.

Best Practices for Replacing VPN with ZTNA

As organizations transition away from VPNs, adopting ZTNA requires a strategic approach to maximize security, performance, and operational efficiency. Below are best practices to ensure a smooth and effective migration.

1

Start with a hybrid transition plan

Many organizations (45%) are gradually shifting users from VPN to ZTNA rather than making an immediate switch. A phased approach ensures critical applications and user groups transition first, allowing IT teams to refine policies and address challenges before full-scale deployment. Start with high-risk or frequently accessed cloud applications, then expand to broader workloads.

2

Enforce least-privilege access from day one

ZTNA is designed to minimize over-permissioned access, addressing risks such as excessive user privileges, which contributed to more than half of all security incidents for 32% of organizations. Reassess all privileges and implement role-based access controls (RBAC) to ensure users have access only to the specific resources they need—nothing more.

3

Eliminate broad network access in favor of application-level controls

Unlike VPNs, which provide network-wide access, ZTNA restricts access only to the applications and data users need. This reduces the risk of lateral movement attacks, which have been a major factor in VPN breaches. Implement granular policies that verify device posture, user identity, and contextual risk factors before granting access.

4

Integrate ZTNA with an SSE or SASE strategy

ZTNA adoption is most effective when implemented as part of an SSE or SASE platform, which 60% of organizations prioritize for its ability to unify access controls, data protection, and SaaS governance and security. SSE provides deeper visibility, inline threat neutralization, and secure access for all types of traffic, with a single and consistent policy framework.

5

Optimize user experience with direct-to-app connectivity

One of the most cited VPN frustrations is slow connection speeds (22%), often because traffic is backhauled through corporate data centers. ZTNA improves latency and reliability by enabling direct, policy-driven access to applications without routing through a VPN concentrator.

6

Strengthen real-time monitoring and anomaly detection

ZTNA enables continuous authentication and risk-based access control, but security teams must also actively monitor for unusual access behaviors. Since 86% of organizations consider real-time visibility critical, integrate ZTNA logs with SIEM or SOAR platforms for anomaly detection and automated response to suspicious access attempts.

7

Modernize authentication with passwordless and MFA strategies

VPNs have long relied on static credentials, which are frequently compromised. Many VPNs now accommodate multi-factor authentication, but 19% report that users struggle with cumbersome VPN authentication, often forcing users to find workarounds that weaken or circumvent security. ZTNA enables passwordless authentication, adaptive MFA, and single sign-on (SSO) to create a frictionless but highly secure login experience.

8

Regularly assess and adapt access policies

Zero trust is a strategy, a mindset—not a one-time deployment. As the workforce evolves, access needs change and new threats emerge. The policies implemented in zero trust strategies, including those for ZTNA-based remote access, must be continuously refined. Conduct routine audits of access logs, permissions, and policy effectiveness to ensure security remains adaptive and aligned with business needs.

Conclusion

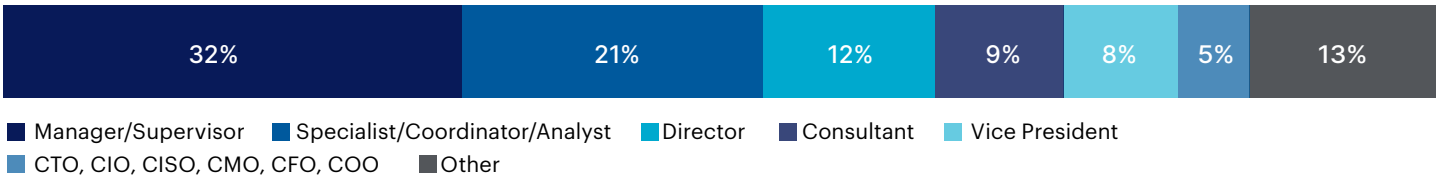
Successfully replacing VPNs with ZTNA requires a thoughtful, phased approach that prioritizes security, scalability, and user experience. Organizations that embrace least-privilege access, leverage SSE, and implement continuous monitoring alongside adaptive policies will not only eliminate VPN vulnerabilities and NAC headaches but also build a more resilient and efficient access model for the modern enterprise.

Methodology and Demographics

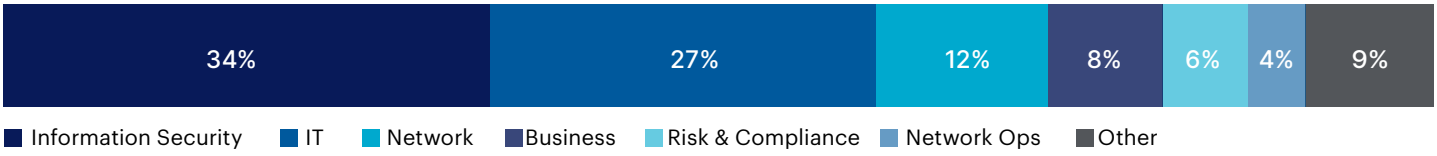
The VPN survey was fielded in early 2025 and reflects input from 683 cybersecurity professionals across diverse industries and company sizes. Respondents include a balanced distribution of IT security practitioners, network engineers, and executives overseeing VPN usage, remote access controls, and zero trust programs. Using a stratified sampling approach, the survey achieved a 95% confidence level with a margin of error of ±3.75%, ensuring statistically valid industry representation.

This research explores the security exposures, management burdens, and user friction tied to legacy VPNs while spotlighting the growing shift toward zero trust network access (ZTNA). The findings offer a data-backed perspective on how organizations mitigate VPN-related risks, modernize access strategies, and implement least privilege models to counter today's dynamic threat landscape.

CAREER LEVEL

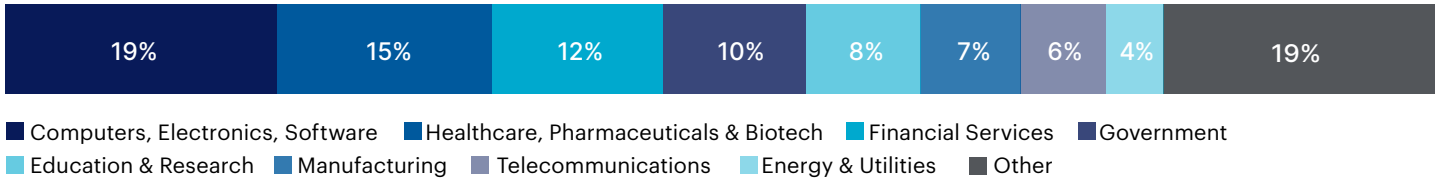


DEPARTMENT



COMPANY SIZE

INDUSTRY



About Netskope

Netskope, a leader in modern security and networking, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for people, devices, and data anywhere they go.

Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications—providing security and accelerating performance without trade-offs.

To learn more visit

netskope.com

Cybersecurity
INSIDERS

TURNING CYBERSECURITY INSIGHTS INTO STRATEGIC INFLUENCE

Cybersecurity Insiders delivers evidence-backed insights that empower security leaders to make informed, strategic decisions. Backed by over a decade of research and a global network of 600,000+ cybersecurity professionals, we provide actionable intelligence to help leaders navigate emerging threats, evaluate new technologies, and shape forward-looking strategies with confidence.

For cybersecurity vendors, we turn research into results — delivering credibility, visibility, and demand through high-impact formats such as:

- Data-powered market reports that establish thought leadership,
- Webinars that build trust with buyers through credible, expert-led narratives,
- CISO guides that showcase best practices,
- Product reviews that independently validate solutions,
- How-to articles that educate buyers, and
- Award programs that elevate brand reputation.

By combining this content with built-in distribution, we help brands earn trust, amplify awareness, and drive demand in a crowded cybersecurity market.

For more information visit

cybersecurity-insiders.com