Hewlett Packard Enterprise

2025

VPN Exposure Report

Why organizations are adopting a modern secure access strategy

Research by

Cybersecurity INSIDERS

Introduction

Are VPNs exposing your business to risk?

Virtual Private Networks (VPNs) were once the standard for remote access, but today they are one of the most exploited entry points for cyberattacks. With the rise of remote and hybrid work, organizations relying on VPNs face escalating threats, including credential theft, ransomware, and persistent unauthorized access, with attackers relentlessly exploiting VPN vulnerabilities.

Apart from security risks, VPNs present considerable operational difficulties and user inconveniences, such as slow connection speeds, frequent disconnections, and complex authentication processes that hinder productivity and collaboration. It has become evident that there is a need for an improved approach to secure remote access.

This 2025 VPN Exposure Report is based on a comprehensive survey of 648 IT, network, and cybersecurity professionals to examine the current state of VPN security and the shift toward modern alternatives like Zero Trust Network Access (ZTNA) and Security Service Edge (SSE).

By analyzing security risks, operational challenges, and survey insights from IT and security professionals, this research provides a clear picture of how enterprises are addressing VPN vulnerabilities and planning their transition to more secure access models.

Key findings from this report include:

- **VPN breaches on the rise** – 48% of organizations have experienced a VPN-related cyberattack, with 30% suffering multiple incidents. Attackers frequently exploit stolen credentials, zero-day vulnerabilities, and VPN misconfigurations to gain unauthorized access and establish persistence.
- **VPN complexity is an operational liability** – 72% of organizations maintain between two and five different VPN services, leading to fragmentation, high IT overhead, and an increased attack surface. 67% operate at least three VPN gateways globally, complicating security policy enforcement across remote and third-party users.
- **Users are frustrated with VPNs** – 83% are reporting user dissatisfaction due to slow connections, cumbersome authentication, and frequent disconnections. These issues hinder productivity and drive users toward insecure workarounds, undermining organizational security.
- **Confidence in VPN security is plummeting** – IT leaders rate their ability to detect and mitigate VPN vulnerabilities at just 6.1 out of 10. Confidence in VPN segmentation as a security control is even lower at 4.1, demonstrating widespread doubt that VPNs can effectively prevent lateral movement and over-privileged access.
- **Organizations are actively exploring VPN alternatives** – 61% of organizations are seeking alternatives to traditional remote access VPNs in pursuit of enhanced security, user experience, and streamlined management. Additionally, 79% of organizations intend to implement a ZTNA solution as a replacement for VPNs within the next two years.

This report provides network and security leaders with critical insights into VPNs' growing risks and how enterprises are moving toward more secure remote access solutions. Backed by fresh survey data and real-world examples, it offers a clear assessment of VPN vulnerabilities, IT complexity, and the Zero Trust strategies organizations are adopting to replace outdated access models.

VPN exposure & attack

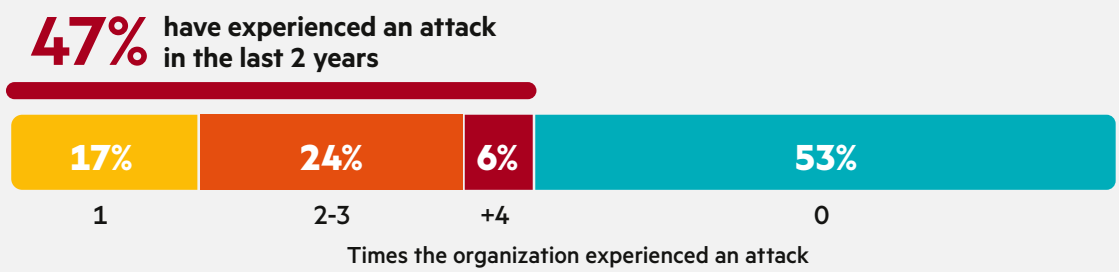
VPN attacks – A persistent reality

VPNs have long been integral to enterprise security strategies, yet their inherent vulnerabilities have rendered them frequent targets for cyberattacks. Alarmingly, nearly half of organizations (48%) have experienced VPN-related breaches, with 47% experiencing 1 or more attacks in the last 2 years. These intrusions often stem from issues like credential theft and ransomware, exploiting the extensive access VPNs provide to infiltrate critical systems. VPNs provide attackers with excessive network access, making establishing persistence easier and repeatedly exploiting organizations relying on outdated access models.

Has your organization experienced a cyberattack as a result of VPN vulnerabilities?

In a widely reported breach in February 2025, attackers exploited a zero-day vulnerability (CVE-2025-0282) in Ivanti's Connect Secure VPN, allowing them to bypass authentication and gain deep access into enterprise networks. Financial institutions and government agencies were among the hardest hit, with attackers using the flaw to exfiltrate sensitive data and establish persistent footholds. This breach is just one example that underscores how VPN vulnerabilities remain a prime target, enabling attackers to repeatedly exploit organizations relying on outdated access models. [Source: Google Cloud Threat Intelligence, February 2025]

How many times has your organization experienced an attack in the last 24 months?



Recent high-profile VPN breaches show attackers exploit vulnerabilities quickly. Enterprises should switch to solutions like ZTNA for stricter access controls and network segmentation to prevent breaches.

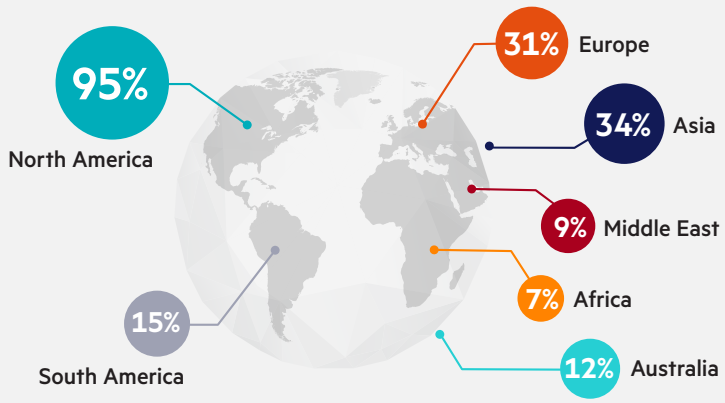
Expanding attack surfaces

Expanding attack surfaces in a borderless enterprise

The exploitation of VPN vulnerabilities is not an isolated occurrence; it directly correlates with the evolution of enterprise attack surfaces. The emergence of an increasingly globally dispersed workforce, hybrid work, and cloud adoption have fundamentally changed how users access business apps, making traditional perimeter-based security models increasingly less effective.

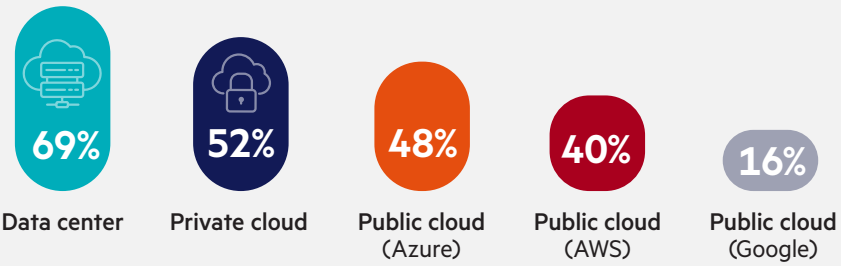
Our survey data highlights this transformation: while 95% of respondents report remote users connecting from North America, the findings highlight the global nature of the workforce with active users in Asia (34%), Europe (31%), South America (15%), Australia (12%), the Middle East (9%), and Africa (7%).

What geographies are your remote users connecting from?



The attack surface has also expanded due to increased cloud adoption. While private applications continue to run in data centers (69%), there is also significant use of private cloud (52%) and public cloud services, including Azure (48%), AWS (40%), and GCP (16%). This trend suggests the utilization of multi-cloud environments, which increases the complexity of enforcing consistent security policies across various platforms and providing uniform access experiences.

Where are your private applications currently running?

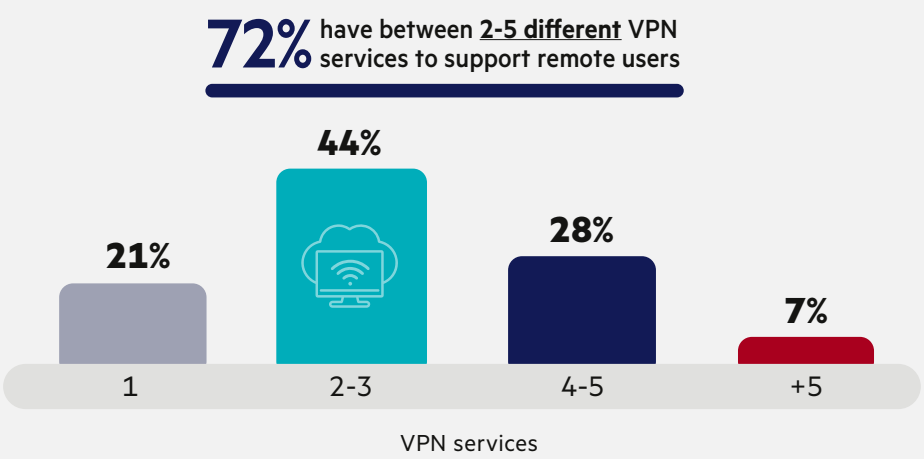


VPN usage trends

The burden of VPN complexity

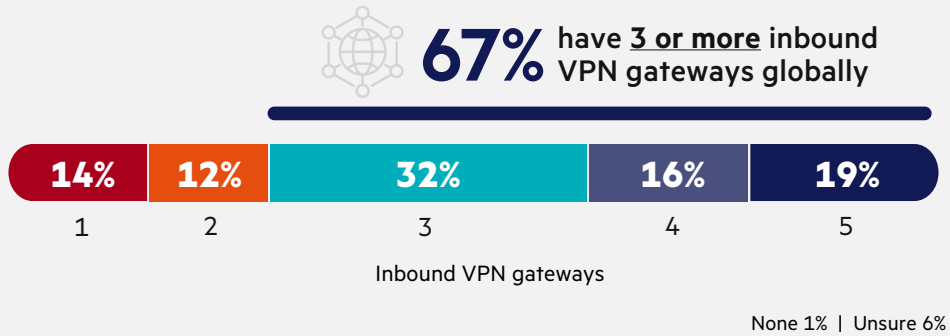
As organizations attempt to secure ever-expanding attack surfaces, the inherent complexity of VPNs has emerged as a significant security risk in itself. Instead of simplifying access, many enterprises now contend with multiple VPN solutions, fragmented gateways, and infrastructures that struggle to scale effectively.

How many different VPN services do you have?



The survey reveals that 72% of organizations maintain between two and five different VPN services, largely driven by geographic segmentation, differing stakeholder needs, and the remnants of past mergers. Compounding this issue, 67% of organizations manage three or more gateways per VPN solution globally. Such fragmentation increases operational costs and expands the attack surface, as each VPN service and gateway serves as a potential entry point for cyber threats.

How many different inbound VPN gateways do you have globally?

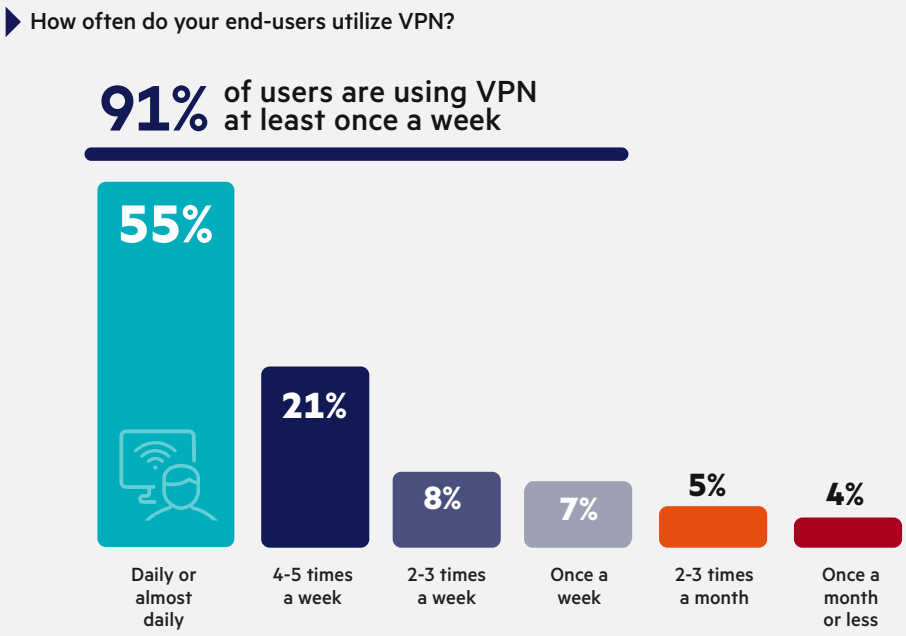


None 1% | Unsure 6%

The burden of VPN complexity (continued)

Heavy reliance on VPN compounds this issue, with 55% of users relying on VPNs daily and 91% using them at least weekly. Legacy VPN architectures, initially designed for occasional remote work, now face challenges in efficiently supporting a distributed workforce.

Scaling VPN systems demands substantial hardware investments, including the VPN concentrator itself, internal and external firewalls, global load balancing, DDoS protection, and more. Additionally, the ongoing need for maintenance can't be overlooked. VPNs typically grant users broad network access instead of application-specific permissions, increasing the attack surface and allowing lateral movement if credentials are compromised.



Managing multiple VPN services and fragmented policies is unsustainable. Security and IT teams should unify access management to reduce complexity and enforce least-privilege access across private applications, cloud, web, and internet.

Lack of confidence

Declining confidence in VPN security

With VPN's architectural weaknesses and inherent complexity, organizations are increasingly doubtful of VPN's ability to prevent breaches, contain attacks, and provide a secure remote access model.

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

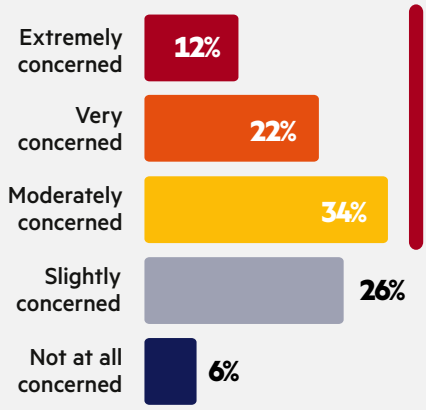
How confident are you that VPN segmentation will effectively limit how far an attack can spread within your network?

Organizations rate their ability to detect and mitigate VPN vulnerabilities at a mere 6.1 out of 10, which equates to a D- on the traditional grading scale. This rating highlights a level of hesitation and uncertainty in promptly identifying and addressing potential threats. Confidence in VPN segmentation as a containment measure is even lower, at 4.1, reflecting widespread skepticism that VPN-based access controls can effectively prevent lateral movement during a breach.

Additionally, 68% of respondents express strong concern that VPNs could compromise their overall security posture, reinforcing the perception of VPNs as liabilities rather than safeguards.

With confidence in VPN security plummeting, enterprises that fail to modernize their remote access strategy risk operational disruptions, compliance failures, and increasing breach costs. Teams must have confidence in their remote access solutions. If confidence is lacking, teams must adapt and consider technologies that reinforce confidence and safeguard the business.

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



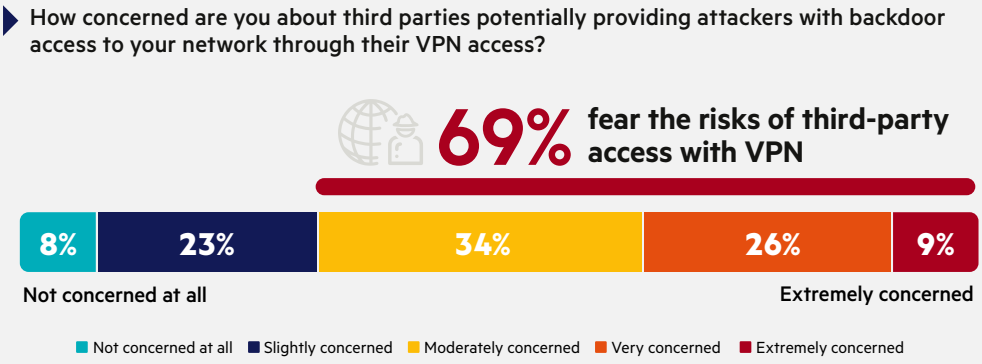
68% are concerned that VPN might compromise the security of their environment

Areas of concern

VPN security deficiencies

Organizations are increasingly recognizing the inherent security shortcomings of traditional VPN architectures. A significant 25% of respondents identify security and compliance issues as their primary concern with VPN usage, surpassing challenges related to user experience (23%) and management complexity (20%).

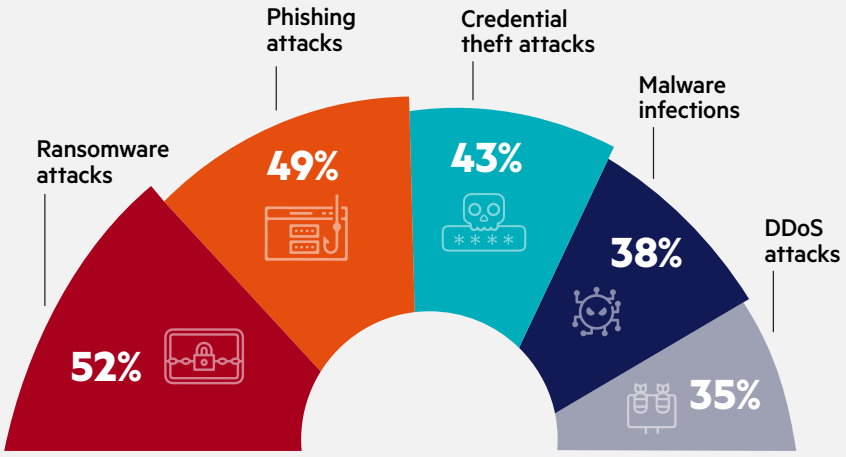
Third-party VPN access remains a major concern, with 69% of organizations fearing it could introduce exploitable security gaps. This apprehension is well-founded, as compromised third-party credentials have previously facilitated unauthorized access to critical infrastructure, leading to significant operational disruptions.



VPN security deficiencies (continued)

When considering prevalent cyber threats, 52% of respondents rank ransomware as a top concern, followed by phishing (49%) and credential theft (43%). These attack vectors are often interconnected; for instance, phishing campaigns can lead to credential theft, facilitating ransomware deployment.

What type of cyberattacks are you most worried about exploiting your organization?



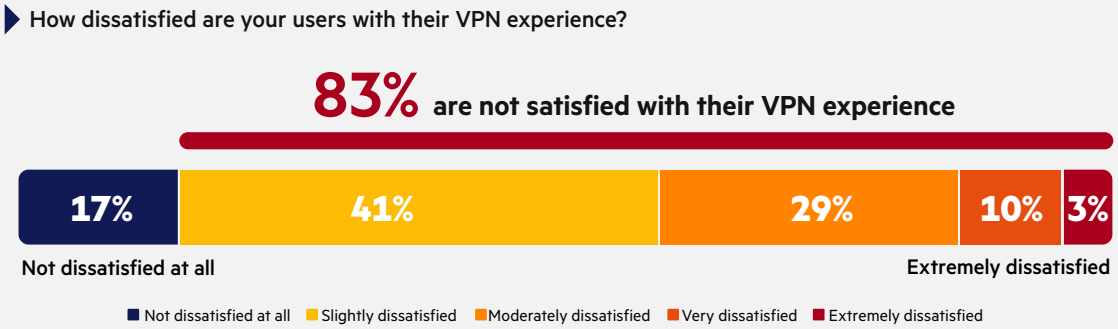
A January 2025 cyber insurance report identified stolen VPN credentials as the leading cause of ransomware infections. Attackers exploited vulnerabilities in enterprise VPNs, using compromised credentials to move laterally, encrypt data, and demand multimillion-dollar ransoms. The report found that 69% of breaches stemmed from third-party VPN access, reinforcing how VPN's broad network access model remains a critical weakness in today's threat landscape. [Source: Coalition's Cyber Threat Index 2025]

Internet-based attacks exploit unrestricted and unmonitored network access, so ensure that Zero Trust principles are applied when considering secure access alternatives. Select solutions that provide application access without broad network access, enforce granular least-privileged access, and cloak the corporate network and exposed IPs.

Dissatisfied users

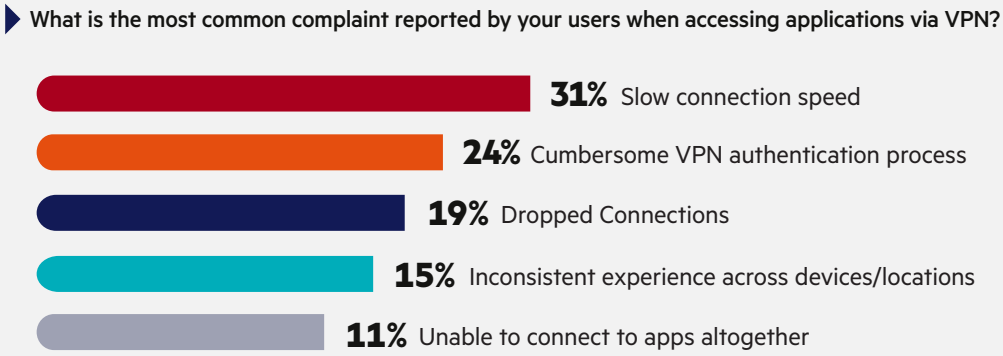
User frustration with VPNs

VPNs are not just a security risk—they have become a significant source of frustration for users, with 83% reporting dissatisfaction due to slow connections (31%), cumbersome authentication (24%), and frequent disconnections (19%). These issues not only hinder productivity but also drive users toward insecure workarounds, undermining organizational security.



The impact of these performance issues extends beyond mere inconvenience. Slow speeds and connection failures disrupt workflows, particularly in cloud-heavy environments where real-time collaboration and remote access to private applications are essential. Beyond frustrating users, VPN reliability issues create an unsustainable burden for IT teams. Administrators are already burdened with maintaining complex VPN infrastructures, patching vulnerabilities, and mitigating security risks—yet they also face a daily influx of user complaints about poor performance, frequent disconnects, and login failures. As VPN problems escalate, IT departments are forced to divert scarce resources from strategic security initiatives to troubleshooting access issues, further driving up operational costs.

Enterprises facing mounting user experience and support issues with VPN must recognize that these problems are inherent to the appliance-based VPN model itself. To ensure fast, seamless, and secure access, organizations should consider transitioning to modern access solutions that are built on the scale of cloud. Unlike VPN, which creates bottlenecks by forcing all traffic through centralized gateways, cloud-based alternatives like ZTNA provide direct, optimized connections to private applications. This reduces latency, eliminates dropped connections, and simplifies authentication—all while strengthening security at scale.



Exploring VPN alternatives

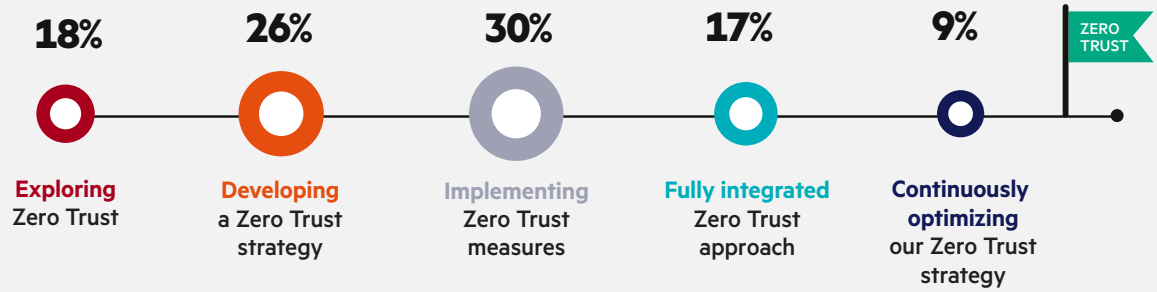
Transitioning from VPN to Zero Trust architectures

The cumulative challenges associated with VPNs—security vulnerabilities, performance bottlenecks, and administrative burdens—have prompted organizations to seek more robust alternatives for secure access. Survey data shows that 61% of enterprises are actively exploring alternative solutions such as ZTNA as part of the greater Security Service Edge (SSE) platform.

Have you considered remote access alternatives to traditional VPN?

When asked about their progress on a Zero Trust journey, 82% of teams reported having started incorporating a Zero Trust strategy. Most teams (30%) are currently in the implementation phase, while 26% are developing their Zero Trust strategies. Moving away from technologies like VPN is part of the broader trend towards advanced security strategies such as Zero Trust, which aim to reduce breach risks and IT overhead, while ensuring secure access to critical applications.

Where does your organization currently stand in its Zero Trust journey?

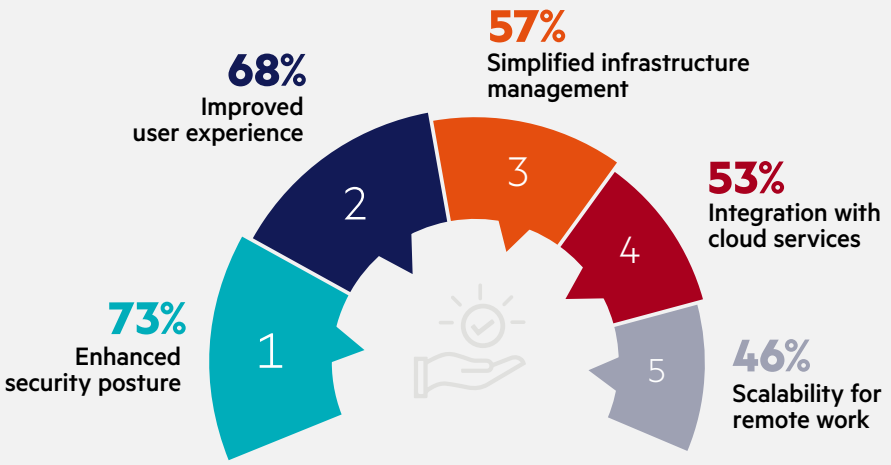


Zero Trust adoption with ZTNA

Key drivers of ZTNA adoption

The transition to ZTNA is not just about phasing out VPN—it is about solving the fundamental challenges that VPN failed to address. When asked about the key benefits of the transition to ZTNA, 73% of organizations report enhanced security posture, reinforcing the critical role VPN vulnerabilities play in driving ZTNA adoption.

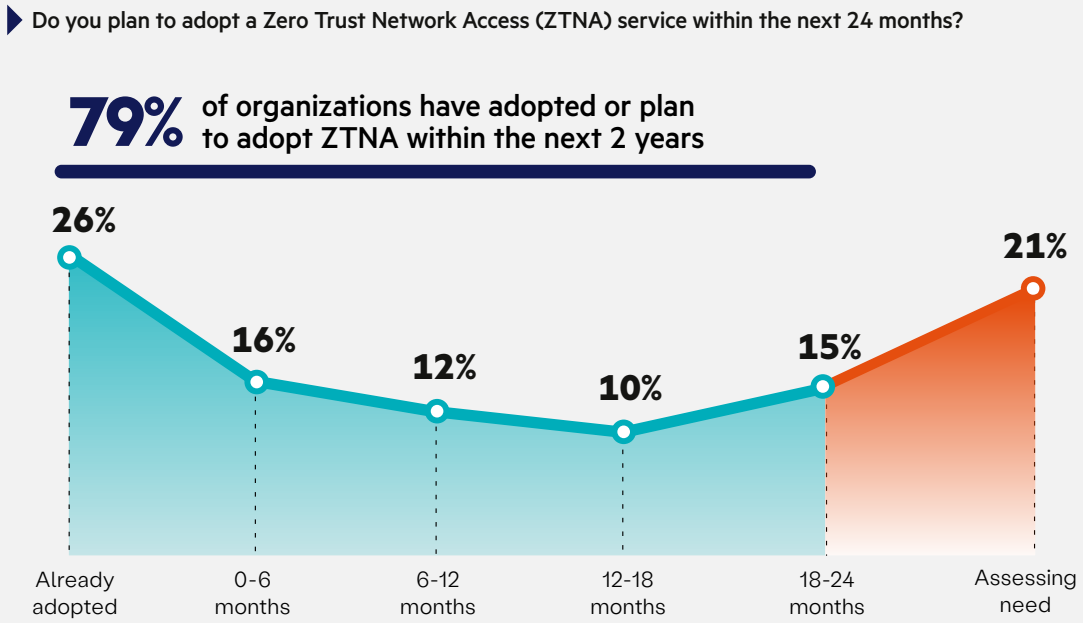
What benefits does your organization seek by transitioning from VPN to a ZTNA solution?



Beyond security, 68% of organizations seek improved user experience, acknowledging that VPN's slow speeds, frequent disconnects, and cumbersome authentication processes have become major productivity bottlenecks. IT complexity is also a pressing issue, with 57% prioritizing simplified infrastructure management and 53% looking for better integration with cloud services. This reflects the reality that VPN struggles to support modern, hybrid work and cloud environments.

Key drivers of ZTNA adoption (continued)

The shift to ZTNA is continuing to grow in popularity, with 79% of enterprises already adopted or planning to adopt ZTNA within the next 24 months and about 1 in 4 companies having already made the transition. This rapid pace of adoption reflects a growing recognition that VPN is no longer sustainable, pushing organizations to modernize remote access with a more secure, scalable, and efficient solution.



Organizations considering a transition from remote access VPN to a Zero Trust approach should assess ZTNA as a preliminary step towards SSE adoption. It is important to note that ZTNA solutions may vary, so ensure your selected vendor offers a cloud architecture and flexibility capable of supporting the global scale, security, and simplicity required by your business.

Important ZTNA considerations

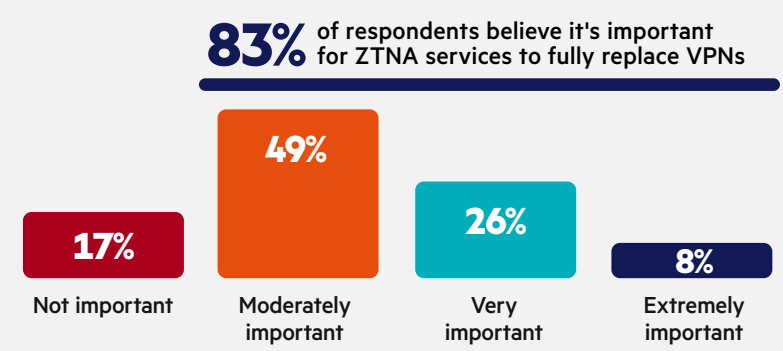
Full VPN replacement with integrated SSE

The majority of organizations are planning to transition to ZTNA, with 83% seeking solutions to fully replace VPNs.

Rather than creating technology redundancies, it is essential for the selected ZTNA solution to completely replace network-centric VPNs to eliminate inherent security risks and operational challenges without adding new ones.

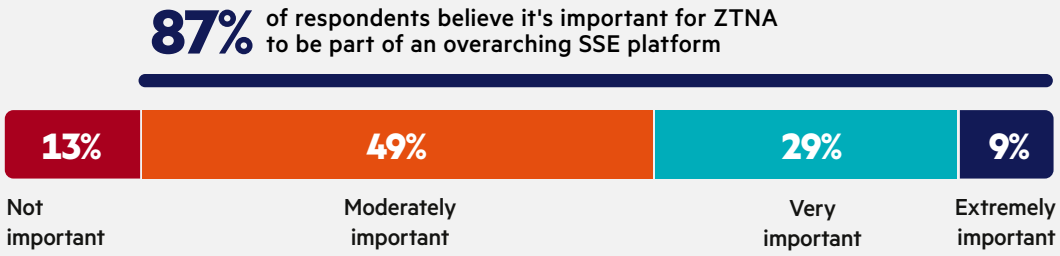
Not all ZTNA services offer a direct replacement for VPNs, so it's important to evaluate carefully.

How important is it that your ZTNA service fully replaces VPN?



Furthermore, 87% of respondents consider integration with a broader Security Service Edge (SSE) platform very important—many would say essential. This reflects an understanding that ZTNA's effectiveness is compounded when combined with SSE services like Secure Web Gateways (SWG), Cloud Access Security Brokers (CASB), and Data Loss Prevention (DLP), providing unified and comprehensive security, visibility, and control over both internal applications and external cloud services.

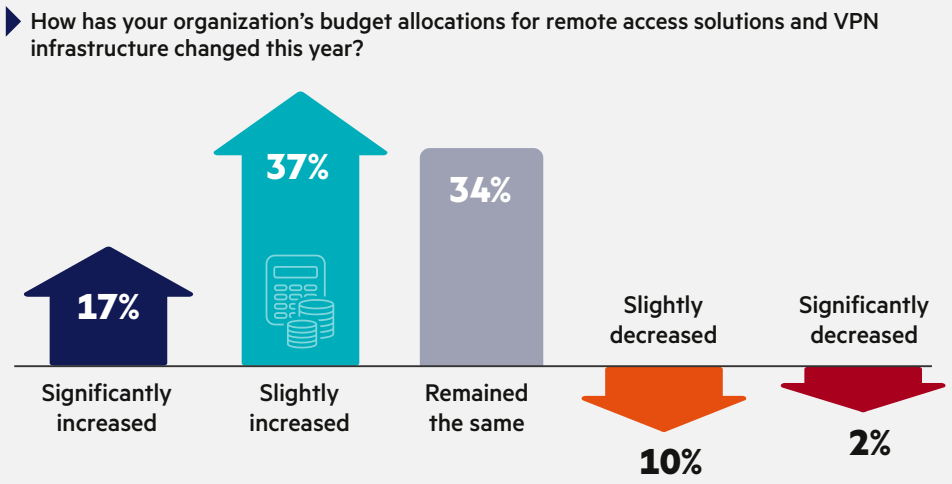
How important is it that a ZTNA service is part of an overarching Security Service Edge (SSE) platform?



Budget considerations

Budgets shift toward Zero Trust

Let's start with the good news! Compared to last year, 54% of organizations have increased their remote access budgets. The critical question now is: Where should you allocate your funds for maximum security impact?



For those with a budget boost, it's essential to leverage your investments wisely. Focus on future-proofing your business with cutting-edge technologies like Zero Trust Network Access (ZTNA) and Security Service Edge (SSE), rather than expanding traditional VPNs.

Now, 34% of organizations state that their budgets have remained the same when compared to the previous year. For those experiencing this, use this period to explore modern remote access technologies and build a strong business case for a more secure and efficient approach. Ensure that any ZTNA or SSE vendors you consider provide a ROI analysis to support your decision.

Meanwhile, 12% of organizations are facing reduced budgets. These teams must achieve more with fewer resources, not only in technology but likely in staffing as well. It's crucial for them to prioritize solutions that ensure robust security while emphasizing simplicity in management. Utilize the statistics in this report to underscore the dangers of relying on VPN technology. Remember, nearly 50% of respondents reported breaches directly linked to VPN vulnerabilities.

Regardless of your budget situation, allocate your funds wisely for intentional, security-first purposes. This approach not only serves your business now but also builds a robust zero trust foundation for future growth.

Best practices for moving from VPNs to ZTNA

As VPNs become a prime target for cyberattacks, organizations are shifting toward ZTNA for secure remote access. These modern approaches reduce excessive network exposure, enforce least-privilege access, and integrate advanced security controls.

1

Identify your VPN challenges

What's causing your VPN headache? The most common issues that teams identified are (1) VPN lacking the necessary security and compliance (2) VPN offering a poor access experience for end-users and (3) the growing complexity of managing VPN services.

2

Evaluate VPN replacement options

What technology should you consider? 61% are considering a remote access alternative to traditional VPNs and 79% plan to adopt ZTNA within the next 2 years. Consider how ZTNA can complement your business in ways that VPN cannot.

3

Consider ZTNA within a broader SSE framework

Why prioritize ZTNA within an SSE platform? 87% of organizations prioritize ZTNA solutions that are part of a larger SSE platform. Ensuring SSE integration consolidates ZTNA, SWG, CASB, and DLP, ensuring consistent security across all users, devices, applications, across global locations.

4

Migrate from VPN in phases

Ready to make the switch? Migrating from VPN doesn't have to be done all at once. Consider a phased approach to VPN replacement and prioritize high-risk users and applications first, then expand ZTNA and SSE across their IT environments. A great place to start is by securing third-party access or enabling secure hybrid work for employees.

Conclusion

VPNs are no longer fit for securing modern enterprises. ZTNA and SSE provide the least-privilege, identity-driven security model needed to protect today's remote workforce while eliminating VPN's security and operational risks.

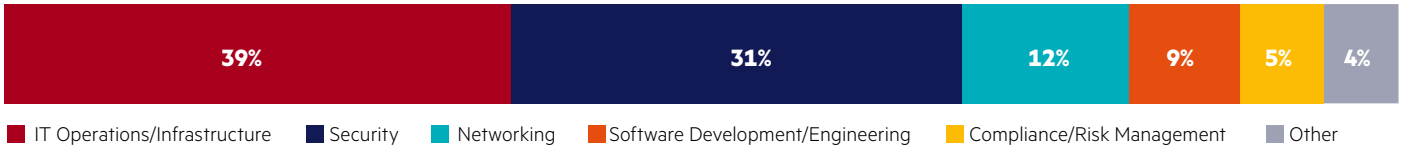
Methodology

The VPN exposure survey was conducted in early 2025, with 648 respondents from organizations of various industries and sizes. Participants included IT professionals, network architects, and cybersecurity leaders responsible for remote access security, VPN management, and Zero Trust initiatives. Using a stratified sampling methodology, the survey achieved a 95% confidence level with a margin of error of ±3.85%, providing statistically reliable insights.

The survey examines the security risks, operational complexities, and user challenges associated with VPNs, while analyzing the accelerating transition to ZTNA and SSE. Findings provide a data-driven view of how enterprises are addressing VPN vulnerabilities, restructuring remote access strategies, and adopting modern, least-privilege security frameworks to mitigate evolving cyber threats.

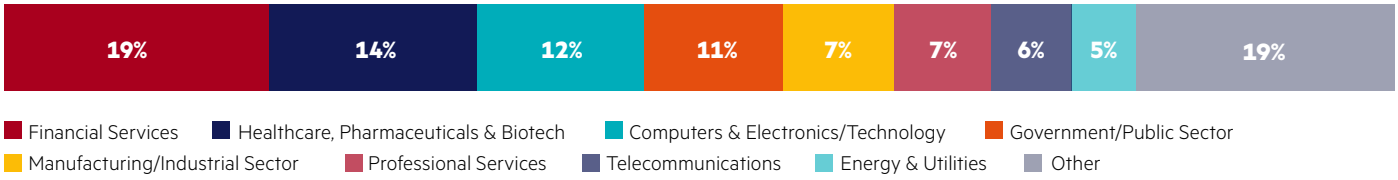
CAREER LEVEL

DEPARTMENT



COMPANY SIZE

INDUSTRY



Hewlett Packard Enterprise

Introducing the HPE Aruba Networking SASE platform

The HPE Aruba Networking SASE platform offers a powerful, edge-to-cloud solution that seamlessly integrates networking and security functions into a unified solution. By combining our industry-leading SD-WAN with our award-winning SSE, our SASE platform ensures secure, uninterrupted access to applications and data from anywhere, enhancing both user experience and productivity.

The HPE Aruba Networking SASE platform simplifies deployment and management by merging networking and security into a single, intuitive interface. The SASE platform not only streamlines operations and reduces complexity but also provides security at cloud-scale for your modern digital enterprise.

Learn how HPE can help modernize secure connectivity with our unified HPE Aruba Networking SASE offering.

Learn more

Ready to experience the power of SASE in real time? Take a free 24-hour test drive today!

SASE test drive

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