Cybersecurity
INSIDERS

2024

VPN Risk Report

HPE aruba networking

Introduction

In the past, Virtual Private Networks (VPNs) have been the go-to solution for remote access. However, with the surge in remote work and distributed workforce models and the rise of cloud adoption, the basic connectivity provided by VPNs is being put to the test. As cyber threats continue to evolve at a rapid pace, VPNs struggle to provide the secure, segmented access that organizations require. Instead, they often grant full access to the corporate network, increasing the risk of cyberattacks once malicious actors obtain login credentials.

As the landscape of remote access security evolves, VPNs are increasingly seen as inadequate. The focus is shifting towards adopting Zero Trust to meet changing business needs. When contemplating the technologies that could replace VPNs, many teams are gravitating toward a Zero Trust Network Access (ZTNA) approach, which effectively eliminates the need for corporate VPNs.

Our 2024 VPN Risk Report, based on a survey of 593 IT professionals and cybersecurity experts, offers a comprehensive analysis of the current state of VPNs. It uncovers the risks and challenges businesses encounter due to VPN usage and provides insights into the future of secure remote access and its implications for businesses like yours.

Key findings from the report include:

- 92% of respondents are concerned that VPN will jeopardize their ability to keep their environment secure.
- 81% of users are dissatisfied with their VPN experience.
- 56% of respondents are looking for an alternative to the traditional VPN.
- 75% view Zero Trust as a priority for their business.
- 59% of organizations have adopted or plan to adopt ZTNA within the next 2 years.

We thank HPE Aruba Networking for their invaluable contribution to this VPN Risk Report. Their expertise in Zero Trust and secure access solutions has greatly enhanced our findings.

We hope this report serves as a valuable resource for IT and cybersecurity professionals on your journey towards Zero Trust security.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

2024 VPN Risk Report

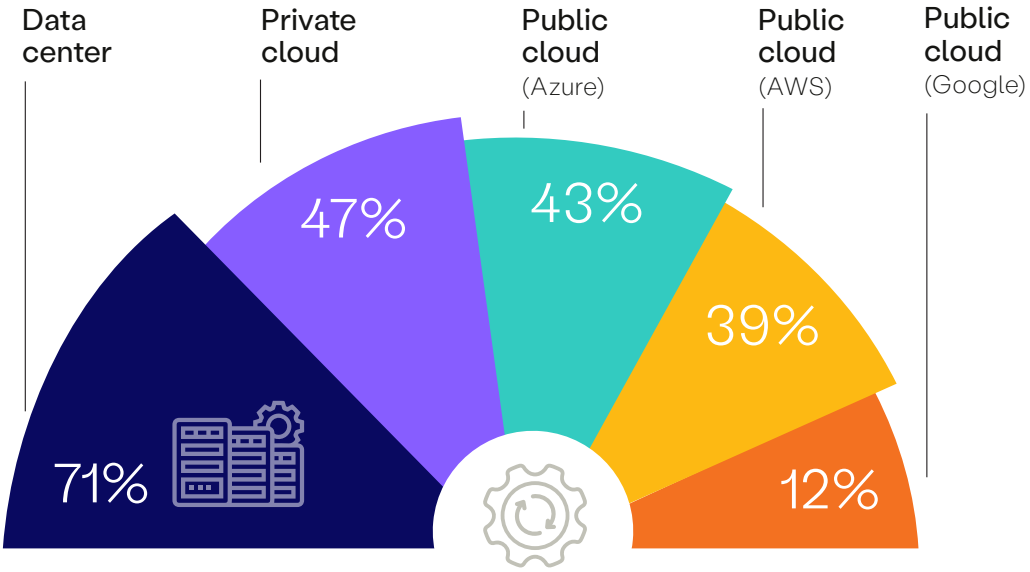
The State of VPN

The Evolving Enterprise

The past year has witnessed a seismic shift in the business landscape, driven by increased workforce mobility and changes in the location of business resources. This transformation is part of the broader digital revolution sweeping across industries.

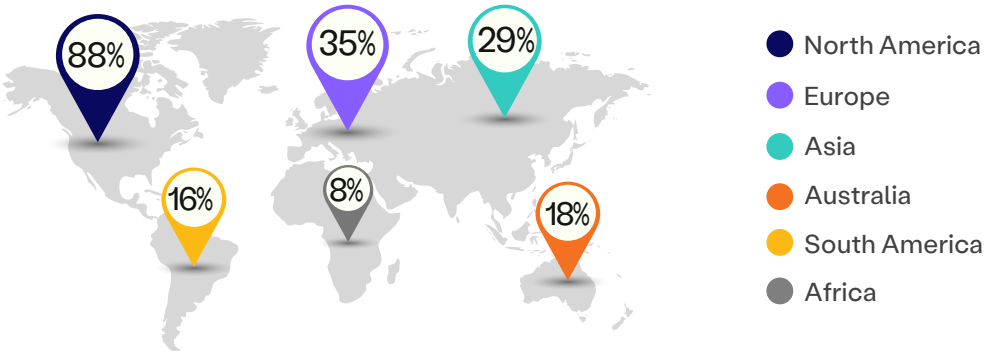
While a significant 71% of organizations continue to run private applications in data centers, there's an undeniable shift towards cloud adoption. Today's businesses operate in hybrid and multi-cloud environments, balancing the need to support mission-critical applications in data centers with the advantages offered by the cloud. However, both VPNs and ZTNA services often struggle to bridge this gap effectively.

Where are your private applications currently running?



In the current scenario, organizations are tasked with supporting a geographically dispersed workforce. A staggering 88% of organizations support remote workers in North America, followed by 35% in Europe and 29% in Asia. This presents unique challenges, as different countries and regions have varying security standards, compliance requirements, and availability levels.

What geographies are your remote users connecting from?



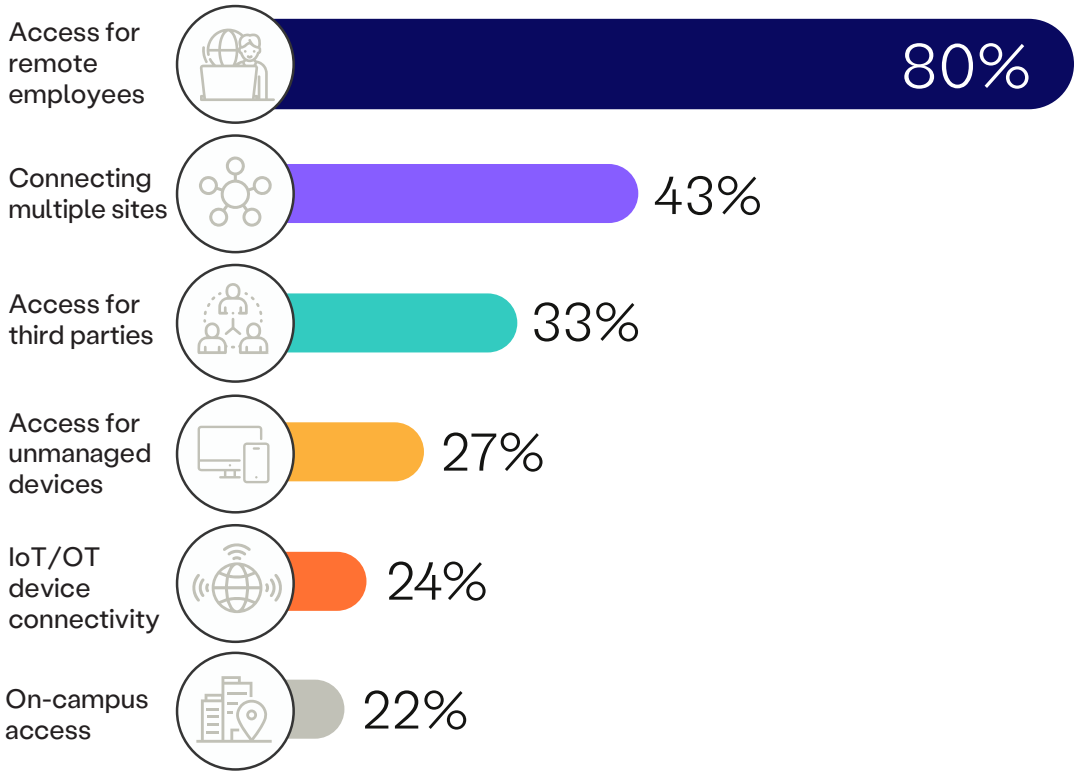
VPN Utilization

The transition to remote work has accelerated the adoption of remote access solutions, with 96% of organizations leveraging VPNs to secure access to private applications. Despite being a technology that's nearly three decades old, VPNs remain widely used, primarily because most alternative technologies have served as supplements rather than replacements.

Does your organization currently use a VPN service?

A substantial 80% of organizations use VPNs to secure their remote employees' access, underscoring the industry-wide shift towards remote work. Additionally, 43% of organizations use VPNs to connect multiple sites and 33% secure third-party access through VPNs. These diverse needs extend beyond the original intended purpose of VPNs, which was employee remote access.

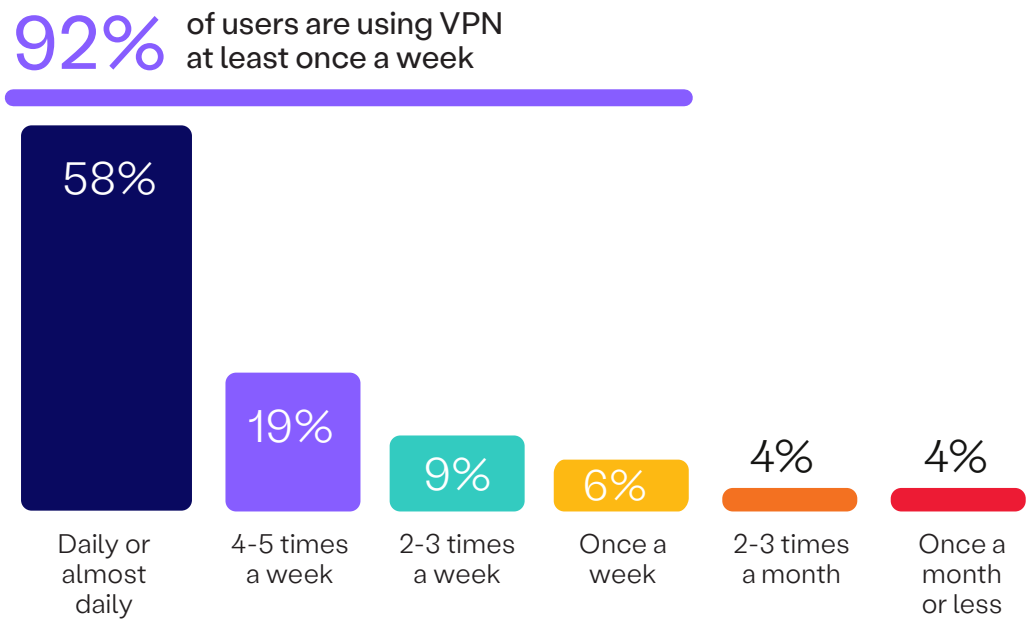
What is the primary purpose for your organization's use of VPN?



VPN Frequency and Quantity

With the majority of organizations relying on VPNs, it's no surprise that most end-users (58%) use VPNs daily. In fact, 92% use it at least once a week, indicating a heavy dependence on VPNs for business operations and a tendency to grant network access to end-users from various locations.

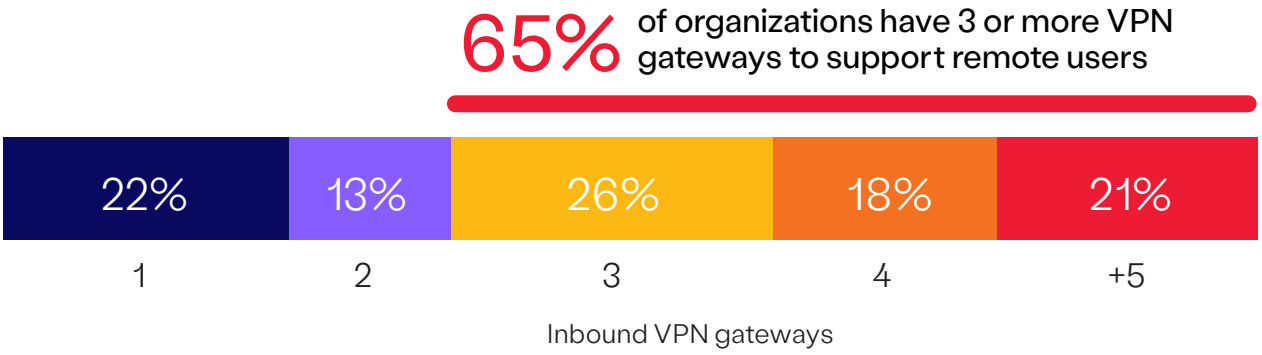
How often do your end-users utilize VPN?



To support a global workforce requiring daily resource access, most organizations depend on three or more VPN gateways (65%) which leads to a varied level of network and operational complexity. For larger organizations with five or more gateways (21%), managing secure remote access becomes an increasingly daunting operational challenge.

Organizations with multiple or expanding VPN gateways may need to consider more sophisticated methods or technologies to manage growing complexities and ensure adequate capacity, security, and redundancy.

How many different inbound VPN gateways do you have globally?



2024 VPN Risk Report

Risks and Challenges of VPN

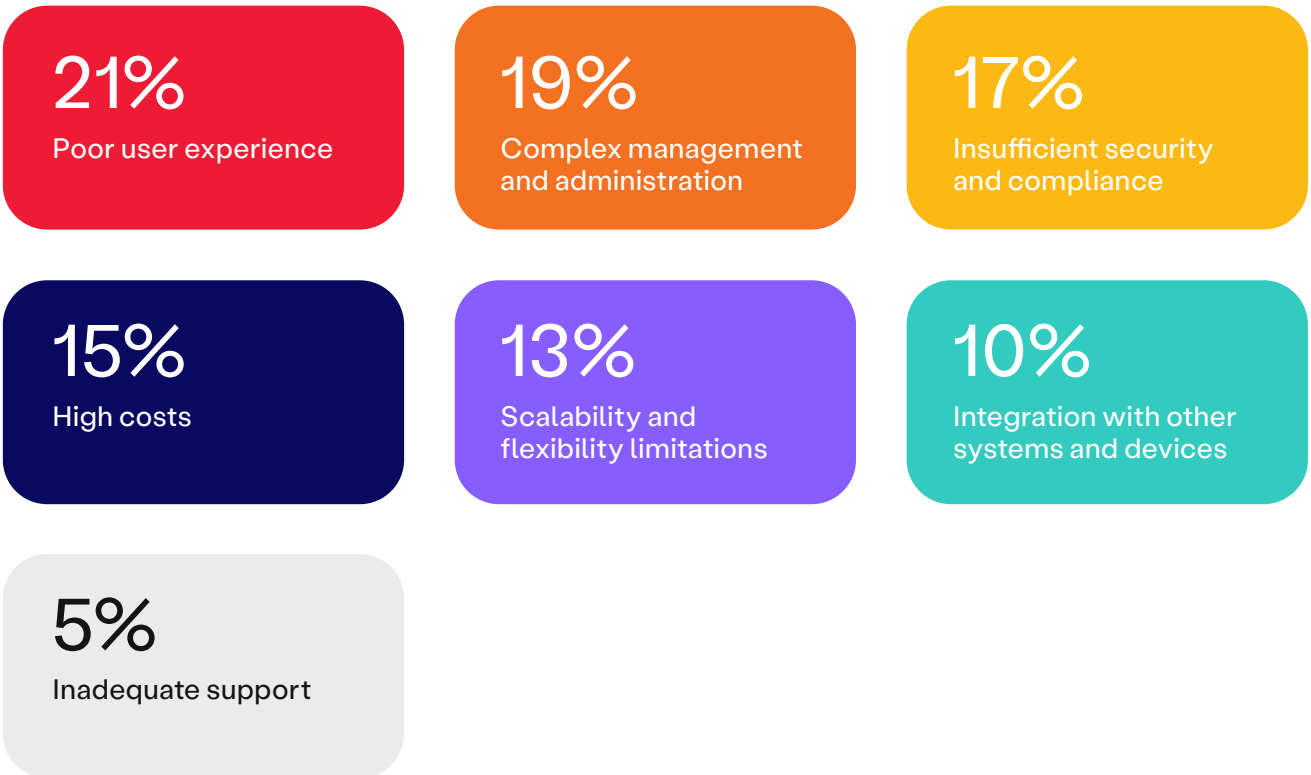
Challenges of VPNs

The most significant challenge with VPNs, as reported by 21% of survey respondents, is the poor user experience. This includes slow connections and frequent disconnections, which directly impact employee productivity and overall business continuity. It's surprising yet understandable that user experience tops the chart of the most impactful VPN issues. Executive teams and board members are under increasing pressure to ensure that remote and hybrid access do not hinder or disrupt the overall success of the business.

Complexity in management and administration follows user experience at 19%. The growing demand for high-performing VPN access can stretch IT resources thin and strain teams. Additionally, 17% of respondents cited insufficient security and compliance, a concern central to protecting sensitive data and adhering to regulatory standards. High costs (15%) and scalability limitations (13%) further complicate the effective deployment of VPN services, potentially hindering business growth and adaptability.

To effectively address and overcome these challenges, organizations should consider modern access technologies such as scalable Zero Trust Network Access (ZTNA). These provide simplified, secure application access and focus on adaptive, cloud-managed solutions that ensure reliable, always-on connectivity for remote users.

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

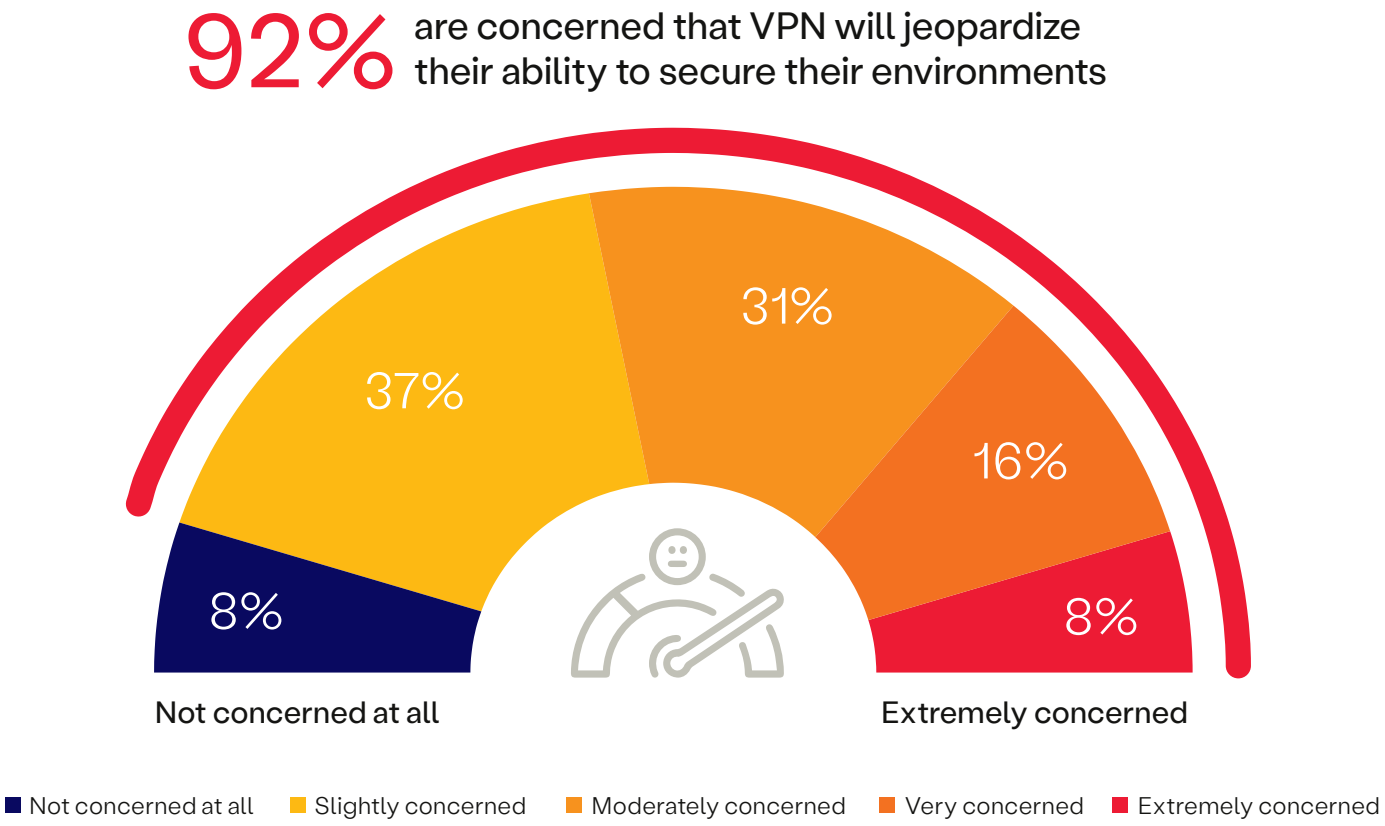


VPN Security Concerns

While user experience and operational efficacy are important, arguably the most crucial aspect of VPNs is their ability to keep your business secure. When asked about their level of concern for their VPNs opening them up to risk, 92% of respondents expressed some level of apprehension regarding their VPNs' ability to secure their environments. More than half (55%) had at least moderate levels of concern.

This alarm may stem from the fact that a significant number of attacks in the previous year have been associated with VPNs, providing a doorway into the corporate network. The fact that cybercriminals have identified this weak point in network security is reflected in the level of concern among respondents.

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



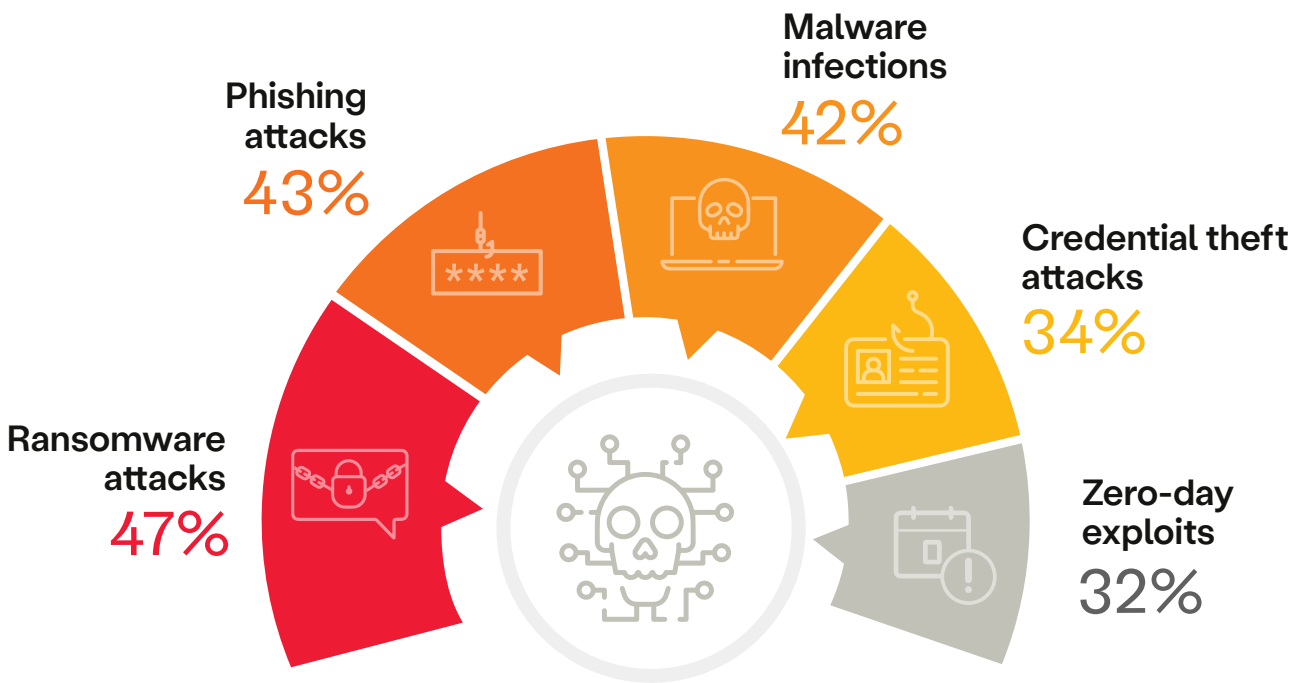
Top VPN Vulnerabilities

Survey participants were asked about the types of cyberattacks most likely to exploit VPN vulnerabilities in their environment. This is a crucial perspective for organizations to tailor their cybersecurity strategies more effectively.

The results serve as an interesting reminder to organizations that VPNs are exposed to a multitude of attacks, not just ransomware, which often gets the most attention. The survey data reveals that while ransomware (47%) tops the list of VPN vulnerabilities, it is closely followed by phishing (43%) and malware (42%). These are the predominant attack types that exploit the end-user and then take advantage of the VPN access point.

To strengthen defenses against such a broad spectrum of cyber threats, organizations should adopt secure access solutions leveraging a Zero Trust model. These solutions enhance defense by verifying each access request and limiting broad network access. They provide granular control at the application level, offering stronger protection against various cyber threats, including sophisticated attacks, compared to traditional VPNs.

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



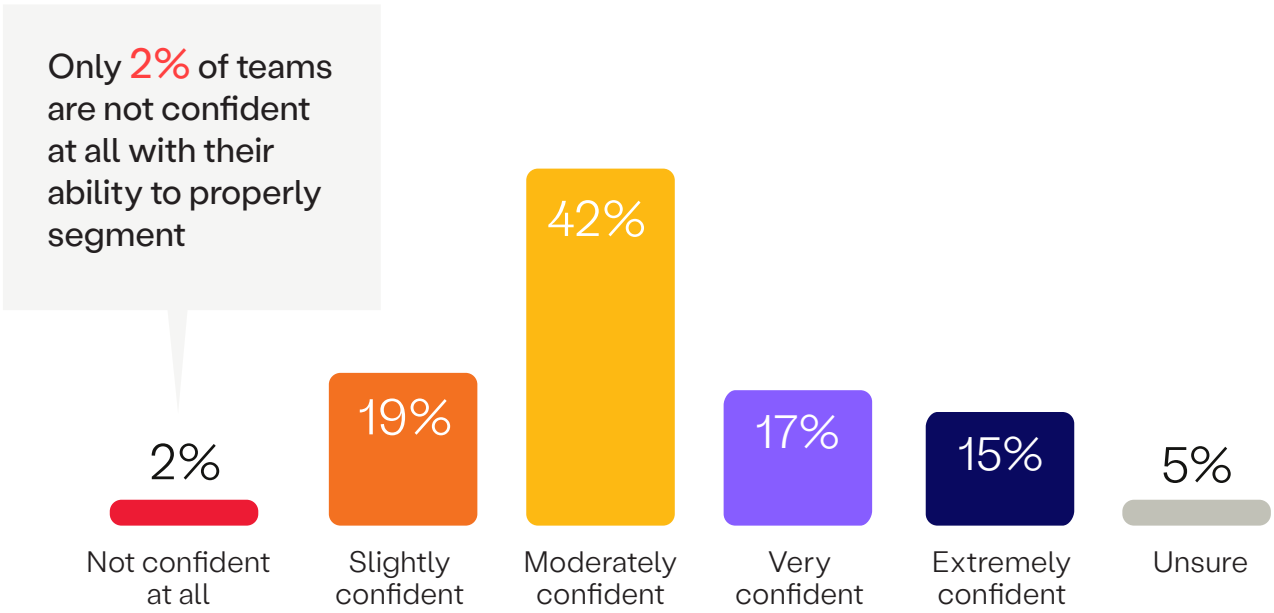
Man-in-the-middle attacks 28% | Distributed Denial of Service (DDoS) attacks 26% | Remote code execution 25% | Data exfiltration attacks 23% | Advanced Persistent Threat (APTs) 21% | Privilege escalation attacks 19% | Brute force attacks 19% | Cross-site scripting 11% | SQL injection 6%

VPN and Least-Privilege Access

In the face of escalating VPN vulnerabilities, security teams are compelled to prioritize prevention and containment strategies. Yet, a startling revelation emerges when these teams assess the efficacy of their VPN segments in curbing network attacks. A mere 2% voice doubts about the VPN's capacity to restrict lateral movement effectively. This statistic is deeply concerning, especially in light of the increasing exploitation of VPNs, which often results in unauthorized lateral network access. It raises the specter of overconfidence, potentially opening the floodgates to further breaches.

Traditional VPN technology achieves segmentation through intricate network partitioning, which often deters organizations from pursuing more detailed segmentation. In response to this challenge, security teams are encouraged to explore Zero Trust technologies. These innovative solutions enable policy-based segmentation, bypassing the complexities of network segmentation. Offering superior granularity and ease of implementation, Zero Trust technologies can significantly enhance the confidence and effectiveness of security teams.

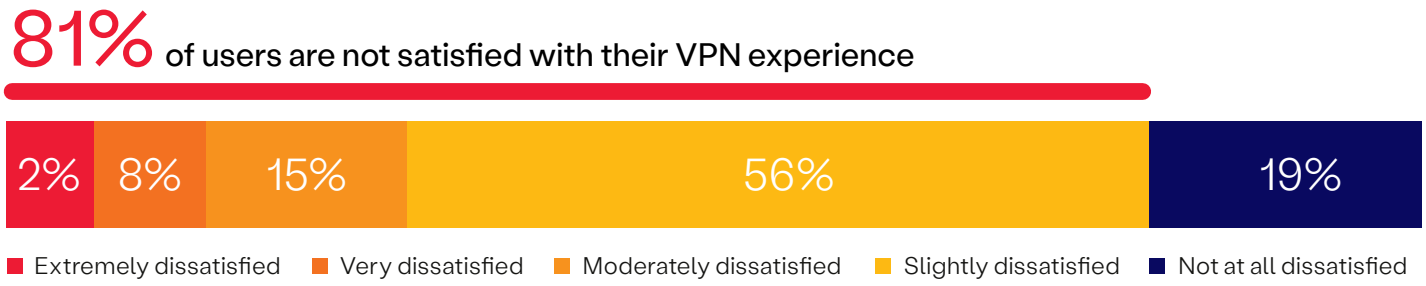
How confident are you that VPN segmentation will effectively limit how far an attack can spread within your network?



VPN Experience and Complaints

While VPN is universally used (96%), it is alarming to discover that a significant 81% of users report dissatisfaction with their VPN experience. This dichotomy creates a clear disconnect between the security and technology choices of IT and the preferences of end-users. As the greatest challenge with VPNs remains the subpar user experience, there is an evident and ongoing demand for improved access experiences. It's crucial to remember that end-users, often considered the weakest link in the security chain, will seek workarounds if their demands are not met, potentially escalating security risks.

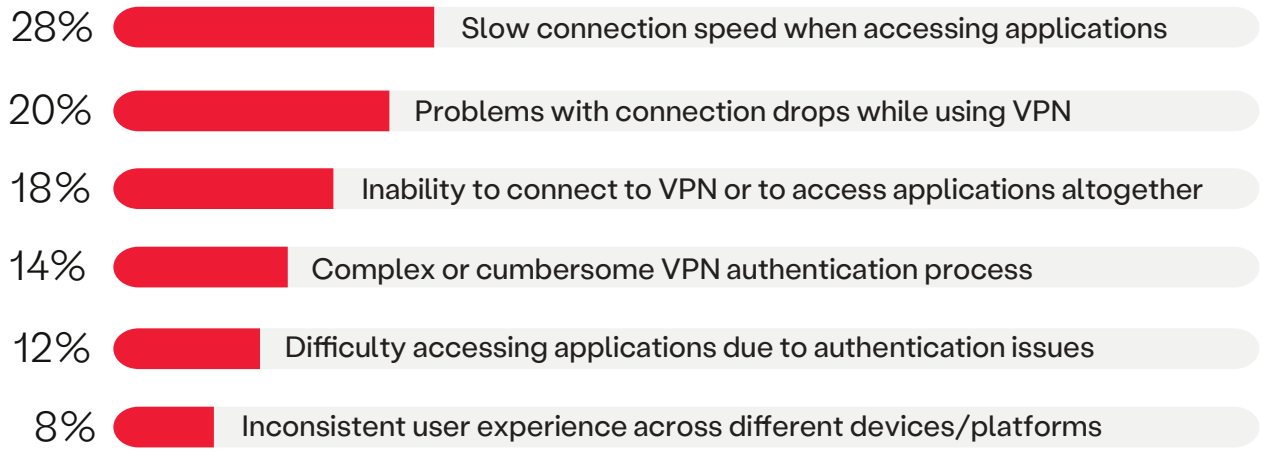
How dissatisfied are your users with their VPN experience?



The most prevalent complaint among VPN users is the sluggish connection speed experienced when accessing applications via VPN, with 28% of users highlighting this as a critical issue. Other notable concerns include frequent connection drops (20%), difficulties in connecting to the VPN or accessing applications (18%), the complexity of the VPN authentication process (14%), and issues arising from authentication problems (12%).

Overall, VPNs pose a multitude of user experience issues, ranging from initial connection challenges to problems during VPN connections, and even productivity-inhibiting slowness once access is achieved. This underscores the need for a more user-centric approach to secure access.

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



2024 VPN Risk Report

The Future of VPN

Exploring VPN Alternatives

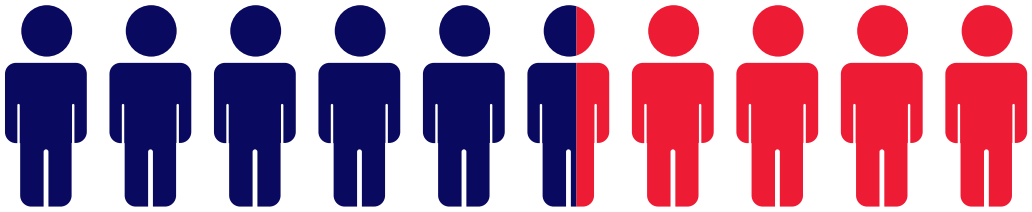
VPN technology has been around for 30 years, and many organizations are seeking out technologies that can give them a competitive edge in the modern world of cloud and mobility. In fact, with increasing remote work and evolving cyber threats, finding efficient and secure access solutions has become a priority for over half of respondents (56%) who are considering alternatives to traditional VPN for remote access.

This indicates a significant shift in thinking as organizations seek out alternatives to network-centric security solutions and opt for an alternative that offers better security, enhanced productivity, more flexibility, and better operational efficiency.

Have you considered remote access alternatives to traditional VPN?

5.6 respondents out of 10

have considered remote access alternatives to traditional VPN



YES 56%

NO 44%

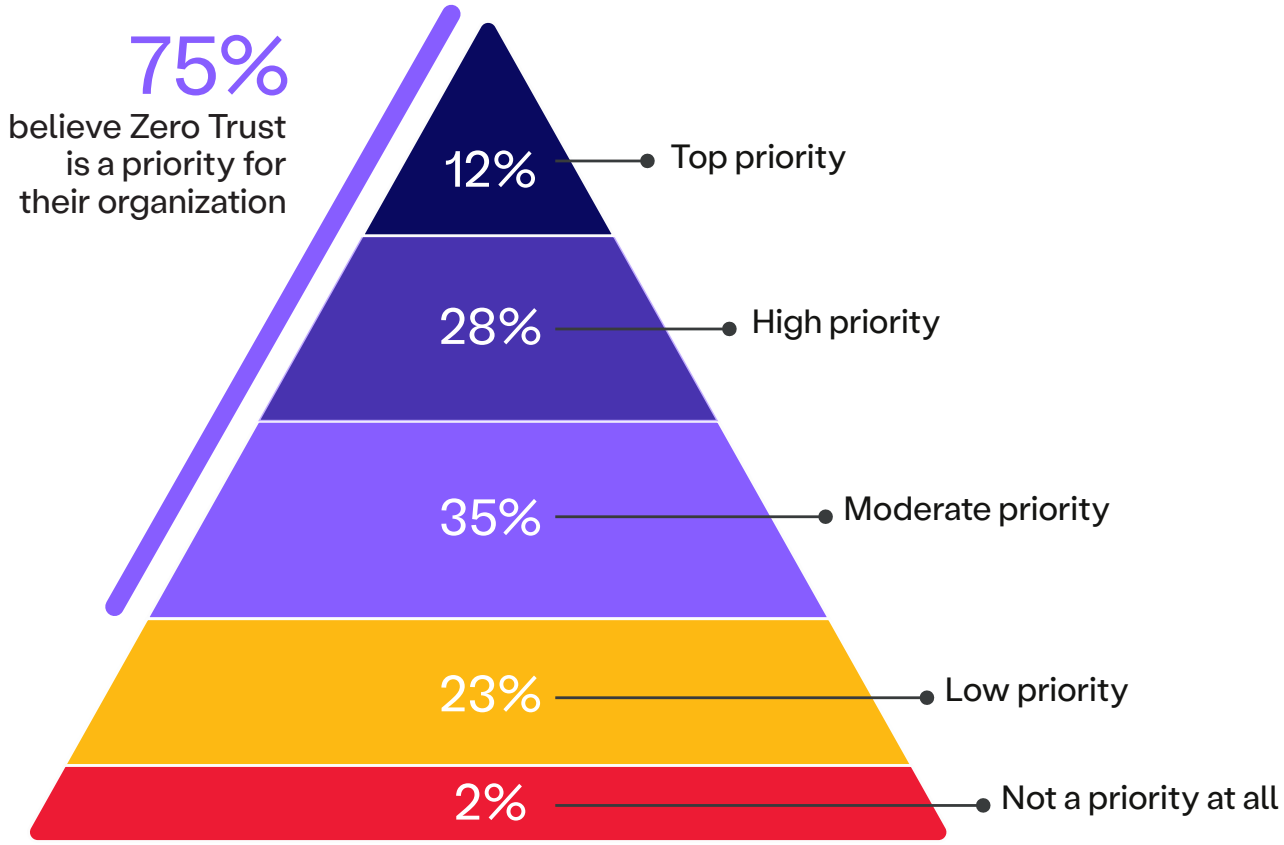
Prioritizing Zero Trust

Adopting a Zero Trust strategy is increasingly important for organizations to enhance their cybersecurity posture in response to evolving threats, remote work challenges, and increasing VPN issues.

Three of four organizations (75%) view adopting a Zero Trust strategy as a priority for their organization, with 40% seeing it as one of their highest priorities. This sentiment resonates with the 56% of organizations contemplating alternatives to traditional VPNs.

Given the shifting cybersecurity landscape and persistent issues with traditional VPNs, it's advisable for organizations to prioritize implementing a Zero Trust framework, which aligns with the move towards more secure and efficient remote access solutions.

How big of a priority is adopting a Zero Trust strategy for your organization?

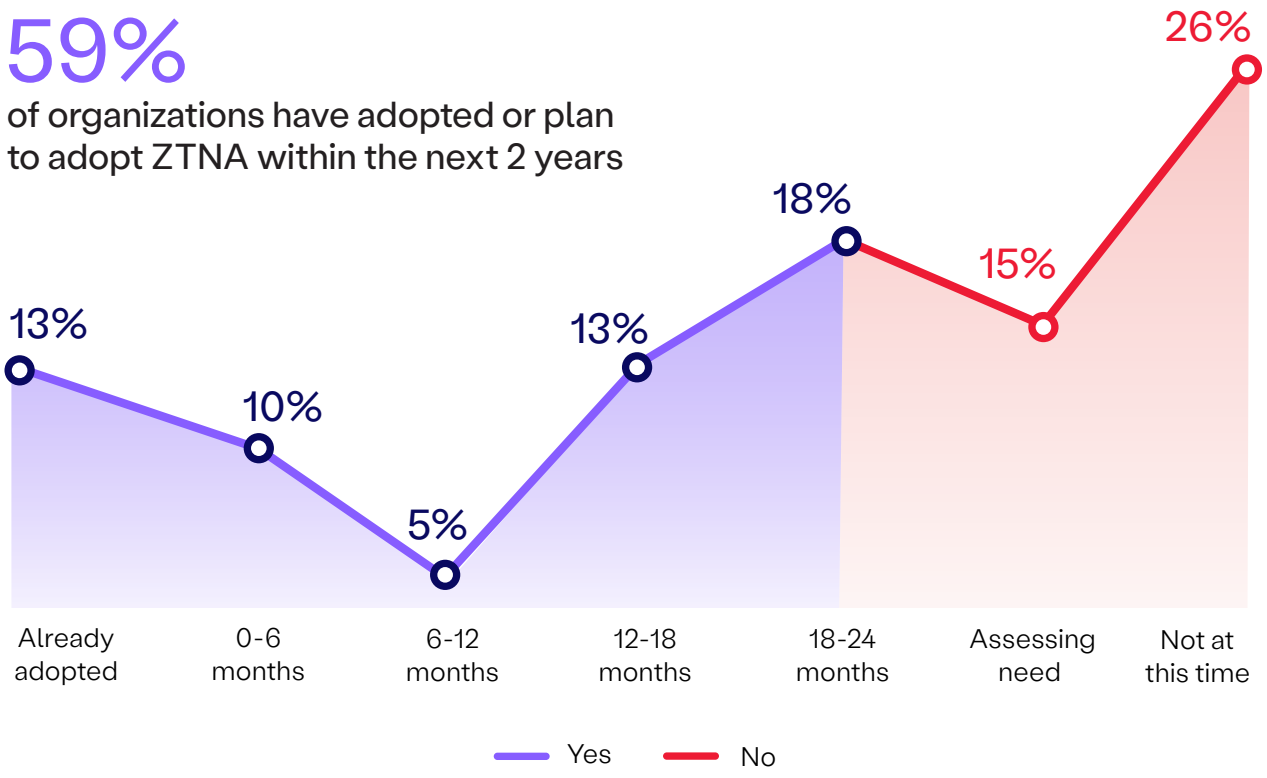


Zero Trust Network Access (ZTNA) Adoption

The decision to adopt a Zero Trust Network Access (ZTNA) service marks a significant stride towards a comprehensive Zero Trust strategy, particularly in light of the challenges and limitations associated with traditional VPNs. As Zero Trust gains priority, ZTNA adoption follows suit, with a majority of organizations (59%) having adopted or planning to adopt ZTNA within the next two years.

As organizations chart their adoption course, they should consider solutions that embody essential Zero Trust principles and robust Security Service Edge (SSE) architectures. It's important to remember that not all ZTNA solutions are created equal.

Do you plan to adopt a Zero Trust Network Access (ZTNA) service within the next 24 months?

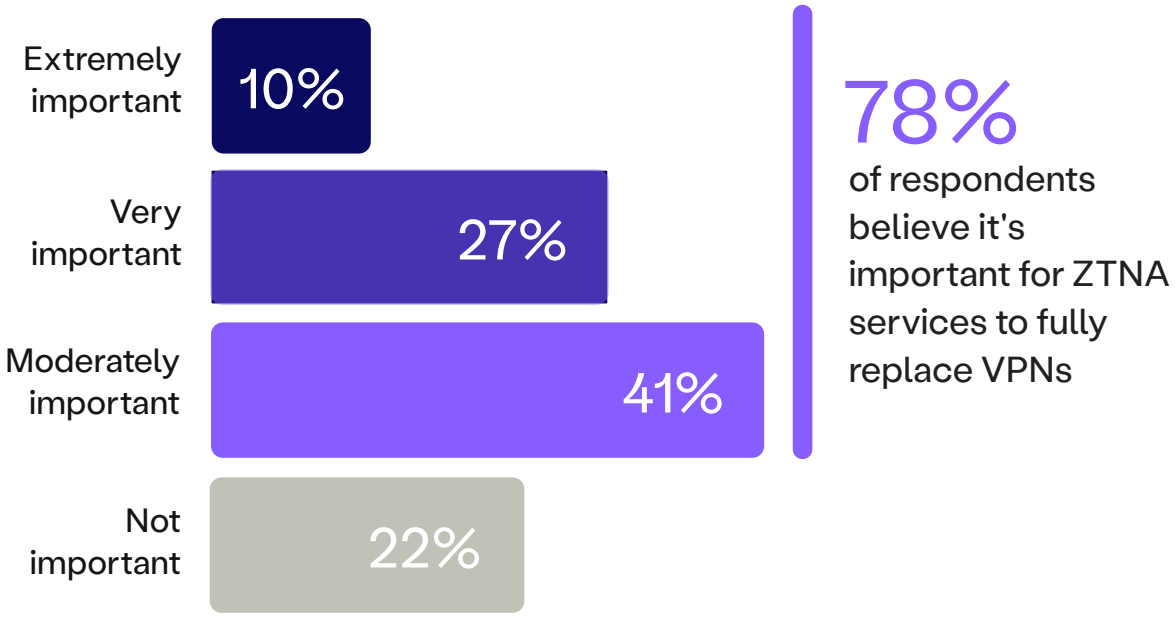


ZTNA as a VPN Replacement

While the majority of respondents are actively planning on adopting ZTNA, it's crucial that the chosen solution can effectively replace legacy VPN technology. A significant 78% of respondents believe that it's important for a ZTNA service to fully replace VPN.

Despite most respondents advocating for full technology replacement, many ZTNA technologies on the market cannot fully replace VPN due to limitations on port and protocol support. When assessing a ZTNA, ensure that the offering can fully replace VPN and aligns with your business needs.

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

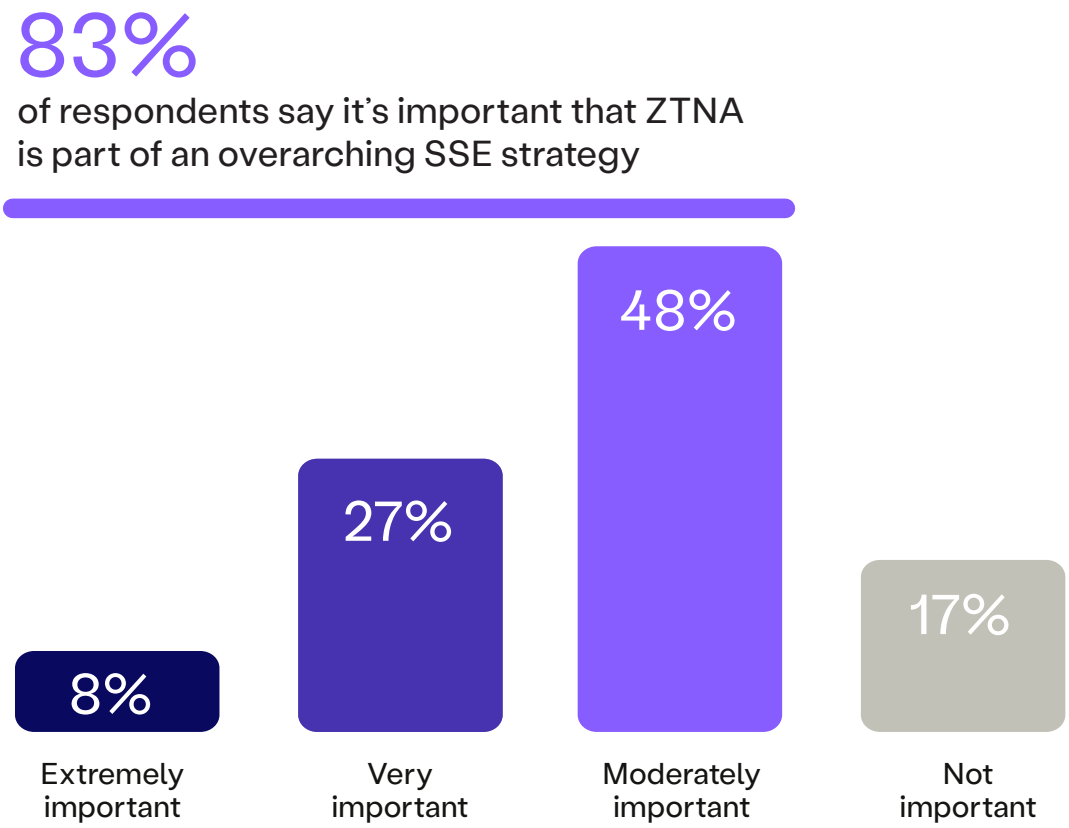


ZTNA and Beyond

Another consideration for organizations is the extent to which a ZTNA solution integrates into a broader Security Service Edge (SSE) platform. 83% believe that it's important for a ZTNA solution to be part of an overarching SSE strategy, with 35% viewing it as very or extremely important.

This could largely be attributed to the growing trend for organizations to move towards system unification and simplification. Security Service Edge (SSE) offers organizations a single platform for all their application access needs, encompassing not just private applications, but also SaaS apps and the open Internet. As your organization begins to assess a ZTNA service, ensure that it forms part of a larger security strategy so that the platform evolves alongside your needs.

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

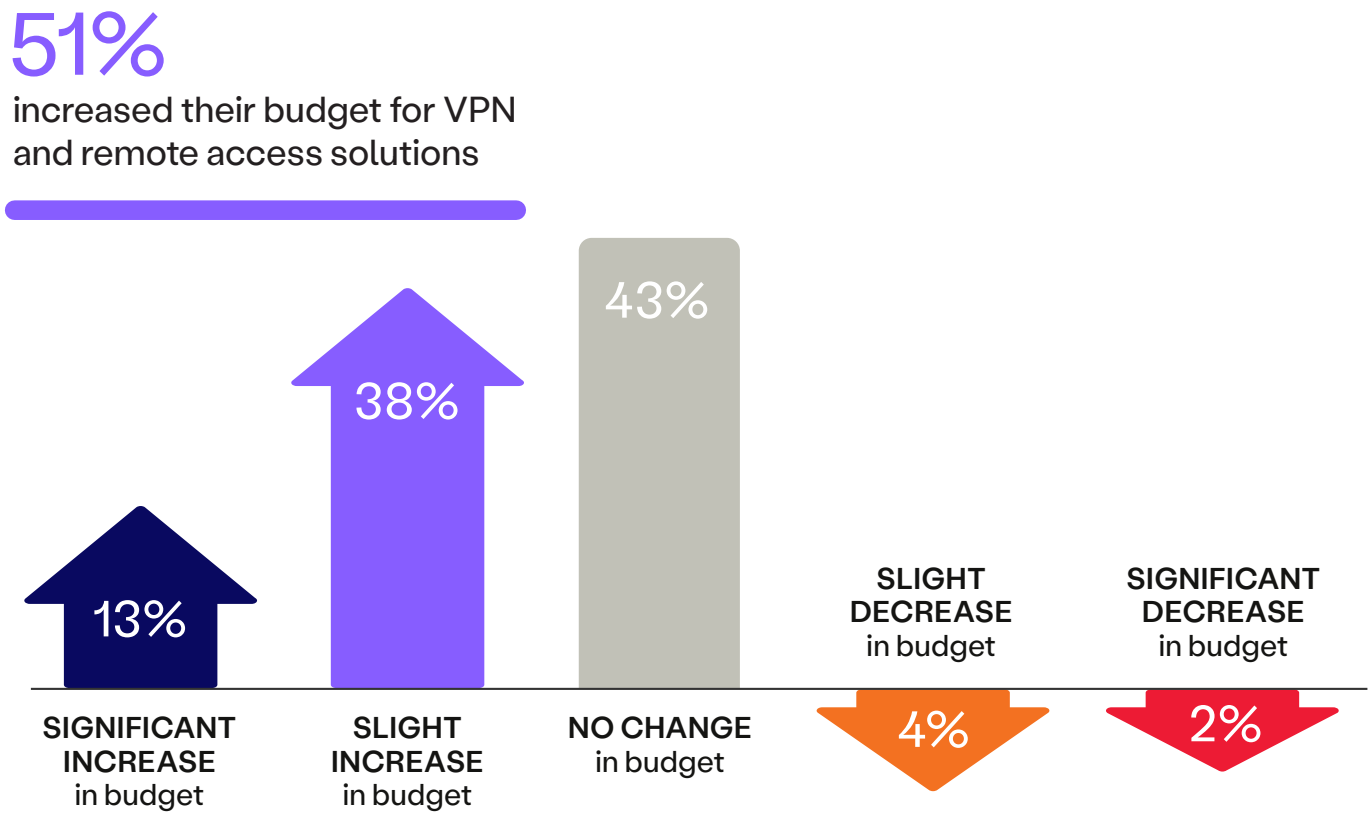


2024 Budget Allocation

Changes in budget allocation for VPN infrastructure and remote access solutions are indicative of evolving priorities and strategies in response to increasing remote work demands and related cybersecurity challenges. Consequently, a majority of organizations (51%) have seen increased budgets for remote access solutions, with 13% reporting a significant increase.

Organizations should evaluate their current investment in remote access solutions and consider how to best utilize their resources, whether increasing or decreasing, in a manner that advances the business. Consider shifting funds towards more secure and efficient alternatives like ZTNA to future-proof your business and optimize not only cost but also security and user experience.

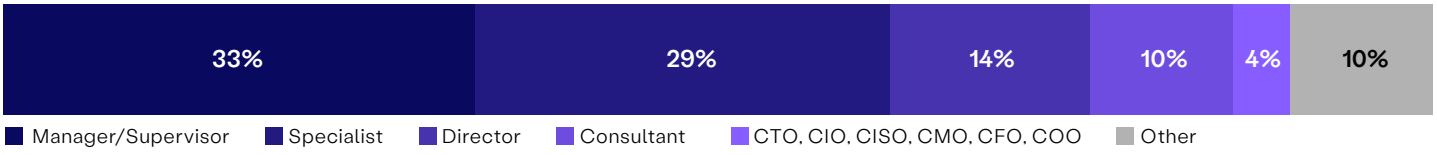
How has your organization's budget allocation for remote access solutions changed this year compared to the previous year?



Methodology & Demographics

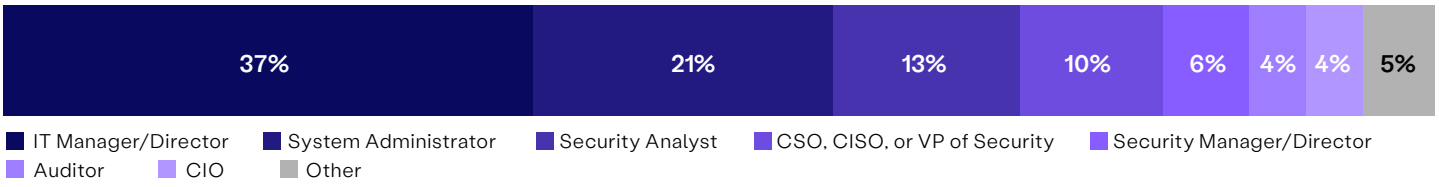
This survey was conducted in December of 2023 with a sample of 593 respondents, representing a diverse range of industries and organizational sizes. Respondents included IT professionals, cybersecurity experts, and decision-makers responsible for their organization's network security and remote access strategies. The survey aimed to gather insights into current trends, challenges, and attitudes towards VPN infrastructure and alternative remote access solutions, reflecting the evolving landscape of cybersecurity and remote work practices. The data collected provides a snapshot of industry perspectives and practices in this domain.

Career level



Department

Primary role



Company size

HPE aruba networking

HPE Aruba Networking helps businesses capture, secure, and transport data to users and applications from edge to cloud. Built on decades of reimagining the future and innovating to advance the way people live and work, HPE delivers unique, open, and intelligent technology solutions as a service. With offerings spanning Cloud Services, Compute, High-Performance Computing & AI, Intelligent Edge, Software, Storage, and now Security, HPE provides a consistent experience across all clouds and edges, helping customers develop new business models, engage in new ways, and increase operational performance.

Learn how HPE can help you modernize your security with our holistic HPE Aruba Networking SSE offering.

LEARN MORE

Ready to experience the power of ZTNA as part of our SSE platform? Take a free 24-hour test drive today!

ZTNA TEST DRIVE

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