zscaler | Cybersecurity INSIDERS

# Zscaler ThreatLabz 2025 VPN Risk Report

# Table of Contents

# Executive Summary

The Zscaler ThreatLabz 2025 VPN Risk Report delivers an incisive look at the evolving risks associated with virtual private networks (VPNs) and underscores the urgent shift towards zero trust architectures as organizations strive to meet future-proofed security demands. Once heralded as the backbone of remote access, VPNs have increasingly become focal points for cyber threats, transitioning from essential tools to significant security risks for organizations worldwide. This report, drawing insights from over 600 IT and security professionals, reveals a critical pivot in the cybersecurity landscape: **more than half of the organizations surveyed experienced attacks due to VPN vulnerabilities in the past year alone,** highlighting the dire need for a new approach in today's increasingly hybrid work environments.

In 2025, the dissatisfaction with traditional VPNs has catalyzed a shift, with enterprises overwhelmingly recognizing that patching these vulnerabilities is a race they can no longer win. This realization is driving the widespread adoption of zero trust models, which promise granular access control and significantly reduce security risks. Notably, **81% of organizations are now pivoting to implement zero trust strategies by 2026, with 65% planning to completely phase out VPNs within the same period.** Moreover, operational frustrations such as slow connections, frequent disconnections, and complex authentication processes have only added to the urgency, propelling a surge in demand for zero trust solutions that ensure both seamless and secure access.

All of these shifts happen within the context of an AI-enabled threat landscape. Indeed, the rise of AI-driven cyberattacks will impact VPN security in unprecedented ways. Attackers will increasingly leverage AI for automated reconnaissance of VPN vulnerabilities, which are easily scanned over the public internet. Techniques like intelligent password spraying and rapid exploit development will allow threat actors to compromise VPN credentials at greater scale. Further down the attack chain, AI-powered evasion techniques will make it even more difficult to detect VPN-based intrusions before significant damage occurs. As such AI-driven threats grow, VPN risks will only magnify, driving enterprises to adopt proactive security measures and accelerating the already pronounced shift towards zero trust solutions.

Acknowledging these shifts, the ThreatLabz report not only charts the decline of VPNs from indispensable tools to liabilities but also provides actionable insights for enterprises navigating this transformative landscape.

# Key_ Findings

## 1. Obsolescence of VPNs Accelerates:

A significant 65% of enterprises are set to replace their VPN services within the next year, marking a 23% increase from 2024. This trend is primarily driven by the inability of VPNs to meet the security and compliance demands of modern enterprises, highlighting their role in exacerbating risks rather than mitigating them.

## 2. Escalation of VPN-Exploited Cyberattacks and Ransomware Concerns:

The past year saw a worrying increase in cyber incidents linked to VPN vulnerabilities, with 56% of organizations reporting such breaches, an alarming rise from previous figures.  Meanwhile, 92% of respondents have concerns that unpatched VPN vulnerabilities will lead directly to ransomware attacks. These findings support the trend that, struggling to maintain the rapid pace of vulnerability patching, enterprises need a robust security overhaul to fill these critical security gaps and mitigate the ever-present risks of VPN exploitation.

## 3. End-User Dissatisfaction Influences Security Redirection:

User frustrations over VPN inefficiencies—ranging from slow speeds to cumbersome, complex, or broken authentication—are increasingly influencing organizational strategies. This end-user discontent is driving the push towards zero trust architectures that offer uninterrupted, secure access without the traditional hassles associated with VPNs.

## 4. The Zero Trust Shift from VPN: From Concept to Implementation:

Reflecting a major strategic shift, 81% of organizations are actively moving towards implementing zero trust frameworks within the next year. This marks a pivotal transition from viewing zero trust as a theoretical ideal to recognizing it as a practical necessity to replace VPNs while enhancing security in dynamic and distributed IT environments.

# VPN Risks: Why 81% of Organizations Are Pivoting to Zero Trust by 2026_

VPNs were designed to provide remote access, but times have changed—and so have attackers. Today, VPNs often serve as entry points for ransomware attacks, credential theft, and cyber espionage due to vulnerabilities that are difficult to patch quickly; implicit trust models that provide complete network access; and widespread access permissions. In all, security vulnerabilities are the single largest challenge enterprises face with VPNs (according to 54% of respondents)—underscoring the fact that attackers routinely exploit unpatched flaws or bypass protections to infiltrate networks.

The risks become even more pronounced with third-party VPN access. A massive 93% of respondents express concerns over backdoor vulnerabilities introduced by external VPN connections, as attackers increasingly exploit third-party credentials to breach networks undetected. It's not just about initial access, either—VPNs also make breaches more destructive. Unlike zero trust solutions that enforce granular policies to prevent movement within networks, VPNs provide broad access, allowing attackers to move laterally and escalate privileges. Overall, 71% of respondents identify lateral movement as a top concern, recognizing how it amplifies the scope and impact of a breach.

These challenges, paired with everyday concerns like slow performance, complex authentication, and frequent disconnections, make it clear why enterprises are moving away from VPNs in favor of zero trust models. The 2025 VPN Risk Report, based on insights from 632 IT and cybersecurity professionals, aims to shed light on the state of VPN usage in 2025 to better understand risks and challenges as well as offer enterprises best practice guidance to improve their cybersecurity posture and their approach to secure remote access.

This report's findings offer IT and security leaders data-driven insights into the reasons to retire outdated VPNs and adopt a modern, cloud-delivered zero trust architecture.
The shift from implicit trust to continuous verification is no longer optional—it is essential for securing today's distributed enterprises, reducing IT complexity, and ensuring a seamless user experience.

# VPN Security_ Concerns

## The Obsolescence of VPNs: Security Risks and User Frustrations

Organizations that continue to rely on VPNs for remote access find themselves increasingly exposed to security gaps, operational inefficiencies, and mounting end-user dissatisfaction, reinforcing the growing sentiment that VPNs belong to a bygone era of access security.

The top challenge—security and compliance risks, cited by 54% of respondents—reinforces the critical vulnerability of VPNs in the face of ransomware, privilege escalation, and lateral attack movement. Attackers view VPNs as weak links ripe for exploitation, while organizations struggle to patch these outdated systems fast enough to keep up with advanced threats.

User frustration has reached a boiling point: 51% of respondents identify poor VPN performance—including elements like sluggish connectivity, drop-offs, and cumbersome authentication protocols—as a roadblock to productivity. VPNs remain an operational burden, with 41% of survey respondents citing difficulties in management and 37% flagging high costs for continued maintenance. These figures illustrate how resource-intensive VPNs have become, draining IT budgets and forcing teams to spend unnecessary time on repetitive troubleshooting tasks.

### Out with Legacy Approaches, in with Zero Trust

A recent breach serves as a stark reminder of VPN vulnerabilities. In January 2025, a Chinese cyber espionage group successfully exploited a zero-day in Ivanti's Pulse Secure VPN, granting unauthorized access across corporate networks. This attack, one of several targeting VPN technology in recent months, highlights why organizations can no longer afford to rely on legacy access models for defending their infrastructures.

With these challenges, numerous legacy VPN vendors have begun branding cloud-delivered

**Eliminating VPN dependencies is no longer an optional upgrade—it's an immediate necessity. Organizations need to transition to true zero trust frameworks that offer identity-driven, least-privileged access and granular segmentation. These cloud-delivered architectures help reduce lateral attack surfaces, improve user experiences, and slash IT complexity—a trifecta of benefits that VPNs simply cannot match.**

**What do you see as the biggest challenges with your VPN solutions?**

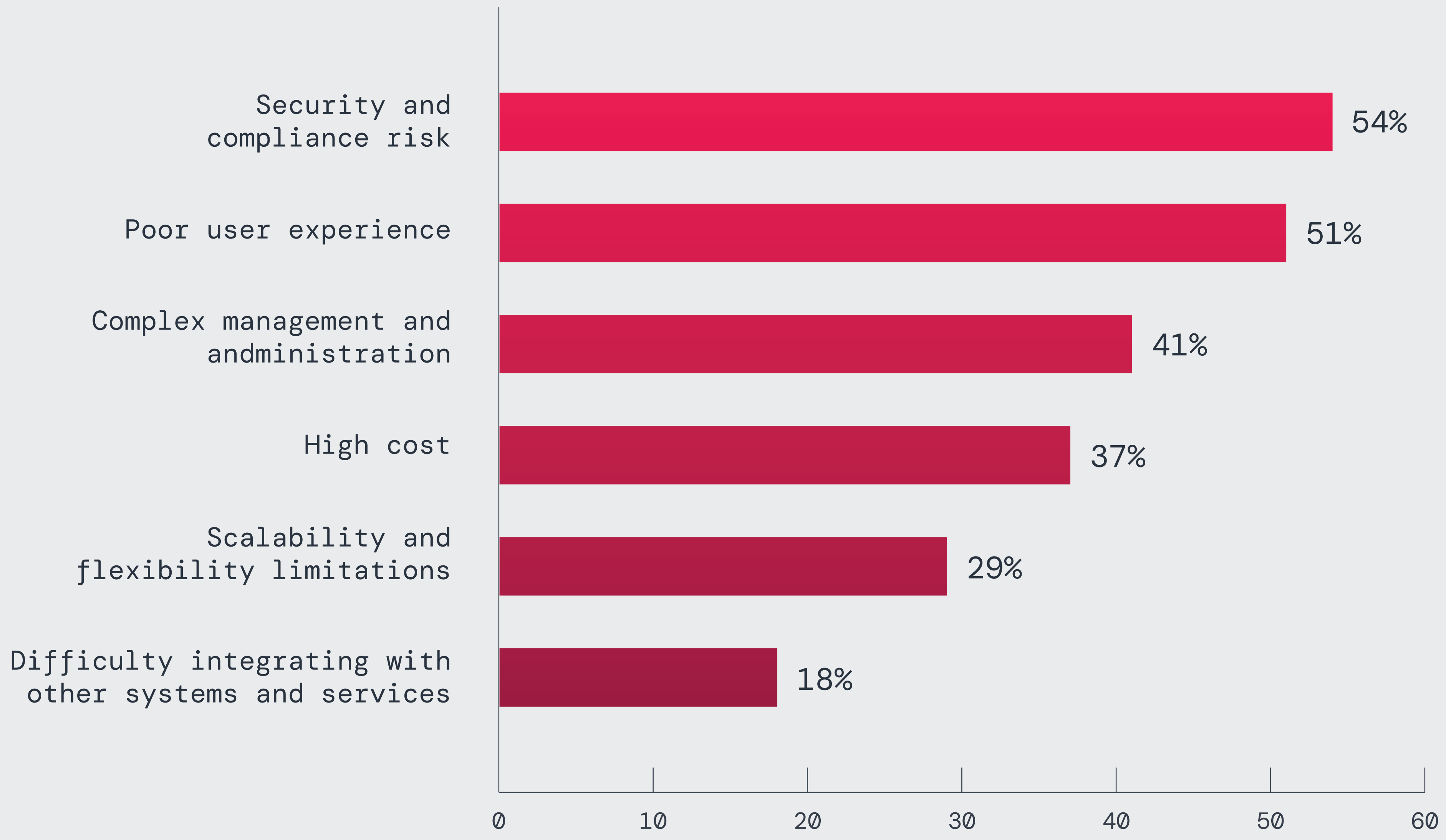


**Figure 1:** The biggest challenges with VPN solutions.

virtual machines as zero trust solutions. However, cloud-hosted VPN services remain fundamentally the same from an architectural perspective — they are internet-connected services with a public IP address that can be breached. Case in point: the industry recently witnessed massive spikes in scanning activity that targets more than twenty thousand public VPN IP addresses hosted by one of the largest security vendors. Historically, this kind of activity has indicated some likelihood that attackers may be preparing to exploit yet-to-be-disclosed vulnerabilities in targeted VPN assets. In other words: if you are reachable, you are breachable — which is why, from an architectural perspective, cloud-based VPN technology can never achieve true zero trust principles, no matter the branding.

## Ransomware and VPNs: A Perfect Storm of Risk

Ransomware groups continue to exploit vulnerabilities in VPNs with devastating precision, leveraging both zero-day flaws and known weaknesses before organizations can deploy security patches. VPNs have become a 'low-hanging fruit' for attackers due to their widespread adoption and reliance on outdated network trust models.

Overall, 92% of survey respondents expressed high levels of concern about ransomware targeting unpatched VPN vulnerabilities, highlighting the critical need for more robust protection mechanisms. This data underscores why VPNs are now seen as liabilities rather than reliable tools for mitigating modern cyber risks.

Real-world examples continue to validate these fears. In January 2023, multiple US healthcare organizations fell victim to a ransomware attack driven by an unpatched Citrix NetScaler vulnerability (CVE-2023-4966). This exploit enabled attackers to infiltrate systems, disrupt hospital operations, lock patient records, and force facilities to divert critical emergency care—all because the vulnerability had not been patched in time.  This incident underscores the pervasive risk posed by unpatched VPNs. Threat actors regularly scan for exposed systems, ensuring they can capitalize on vulnerabilities before organizations apply fixes, leaving organizations at risk for compromise, operational disruption, and financial loss.

**Organizations must step off the endless treadmill of patching and adopt proactive defensive strategies tailored for evolving threats. Zero trust frameworks prioritize identity-driven access control and continuous verification, ensuring a major reduction in ransomware risk—even when vulnerabilities remain unpatched. Automated detection systems and dynamic policies further contain potential breaches, preventing attackers from moving laterally or escalating privileges.**

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

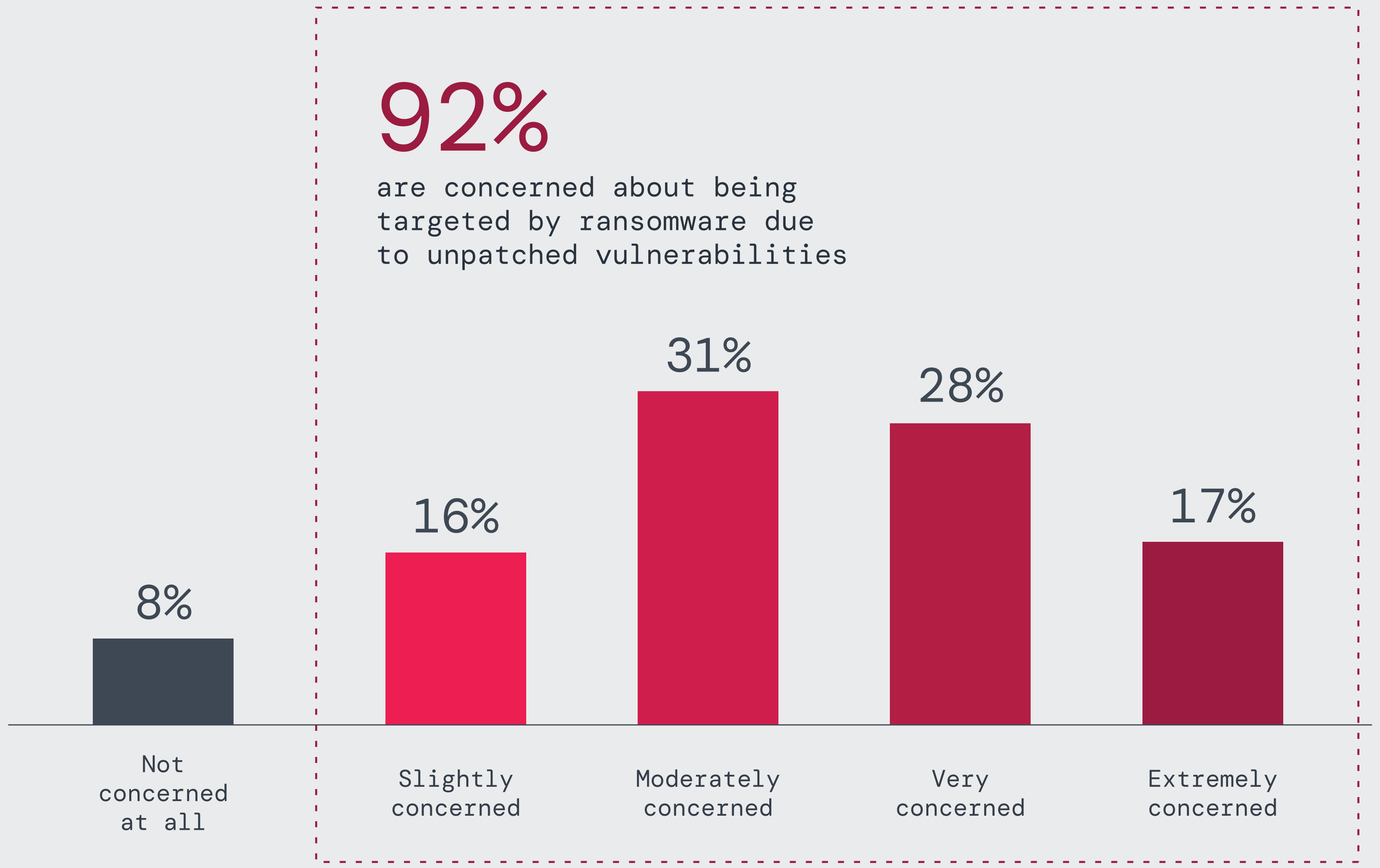


**Figure 2:** Concerns about ransomware attacks.

# VPNs and Lateral Movement: Increasing the Blast Radius of Breaches

In addition to enabling initial compromise through ransomware and other threats, VPNs facilitate lateral movement——a dangerous attack technique. Attackers exploit the extensive access VPNs provide to escalate privileges and infiltrate deeper into target networks, often with devastating consequences.

A total of 71% of respondents expressed some level of concern for this risk, with 32% expressing high levels of concern. These feelings are justified as VPNs typically grant broad network access, allowing attackers to move undetected, escalate privileges, and exfiltrate sensitive data once inside.

In September 2024, attackers exploited multiple zero-day vulnerabilities in Ivanti's Cloud Service Appliance (CSA), notably CVE-2024-8963 and CVE-2024-8190, to breach several organizations, as confirmed by the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI. Attackers bypassed administrative controls, executed arbitrary commands, harvested credentials, and implanted web shells, enabling lateral movement across networks. Despite previous security incidents involving Ivanti VPNs, these new exploits demonstrate that patching or rearchitecting legacy VPN solutions still fails to address the fundamental security flaws inherent in network-based remote access models.

**How concerned are you that attackers will move laterally across your network if a VPN is compromised?**

89% are concerned about attackers moving laterally across

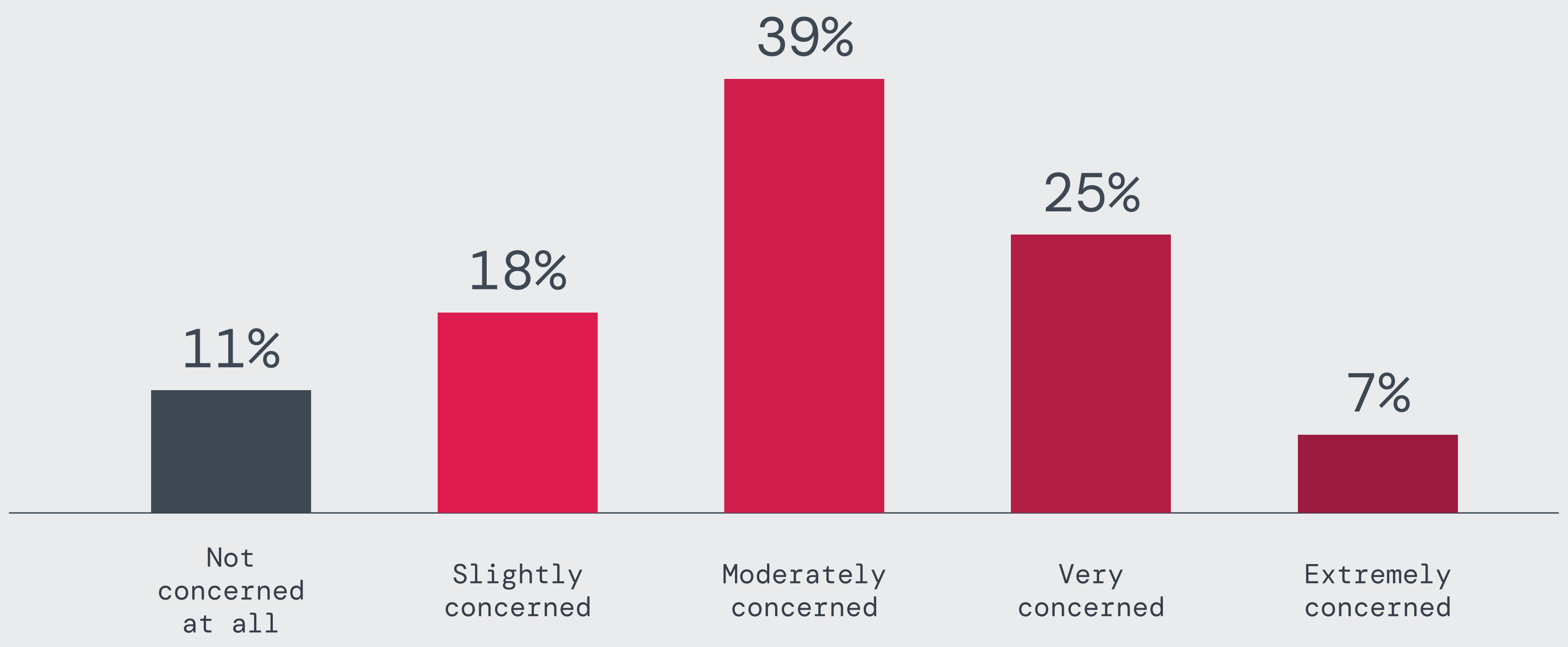


**Figure 3:** Enterprise concerns that will move laterally across the network if a VPN is compromised.

**To mitigate these risks, organizations must transition from VPN-based access to Zero Trust Network Access (ZTNA) with strict segmentation. Unlike VPNs, which grant users broad network access, ZTNA provides application-level access based on identity and context, ensuring users can only access the specific resources they need. This approach prevents lateral movement even if attackers gain initial access, drastically reducing the attack surface and potential blast radius of breaches. Additionally, implementing network and micro-segmentation strengthens security by isolating critical systems and preventing unauthorized communication between compromised and secure assets.**

# VPN CVEs from 2020-2025: A Rising Wave of High-Severity Vulnerabilities

No software is immune from security vulnerabilities, nor should it be expected to be. However, in the case of VPN technology, vulnerabilities, particularly zero-day threats, can be particularly damaging, because threat actors can easily probe for impacted VPN infrastructure and exploit it before any patch is released or has been applied. CVE reporting is a good thing, as this community-wide effort helps vendors and customers follow best practice and improve their cyber hygiene through patching and disclosure. How these CVEs are discovered and the information they contain reflects changes in the evolving threat landscape.

Zscaler ThreatLabz analyzed 411 VPN Common Vulnerabilities and Exposures (CVEs) from 2020-2025, as reported by the MITRE CVE Program. The findings indicate a surge of VPN vulnerabilities that have gradually risen through the first half of this decade. These CVEs cover a wide range of VPN failures — from exploitation of web-based management interfaces through command injection and input validation vulnerabilities, to cryptographic failures and DoS and DDoS attacks. There is no shortage of recent VPN vulnerabilities, many of which have led to major, highly visible security breaches.

Many of these CVEs are critical. In 2024, for instance, 60% of the 83 VPN vulnerabilities reported by NIST indicated a high or critical CVSS score. Meanwhile, remote code execution (RCE) vulnerabilities, which allow attackers to execute arbitrary commands and potentially lead to system compromise, were the most common VPN CVEs.  In other words, far from being innocuous, the majority of VPN CVEs in the past year left their users extremely vulnerable to exploits that attackers execute with relative ease. Moreover, many of these CVEs were zero-day exploits. While CVEs in 2025 are still low in the early part of the year, major vulnerabilities have already been disclosed, such as two zero-day exploits, CVE-2025-0282 and CVE-2025-0283.

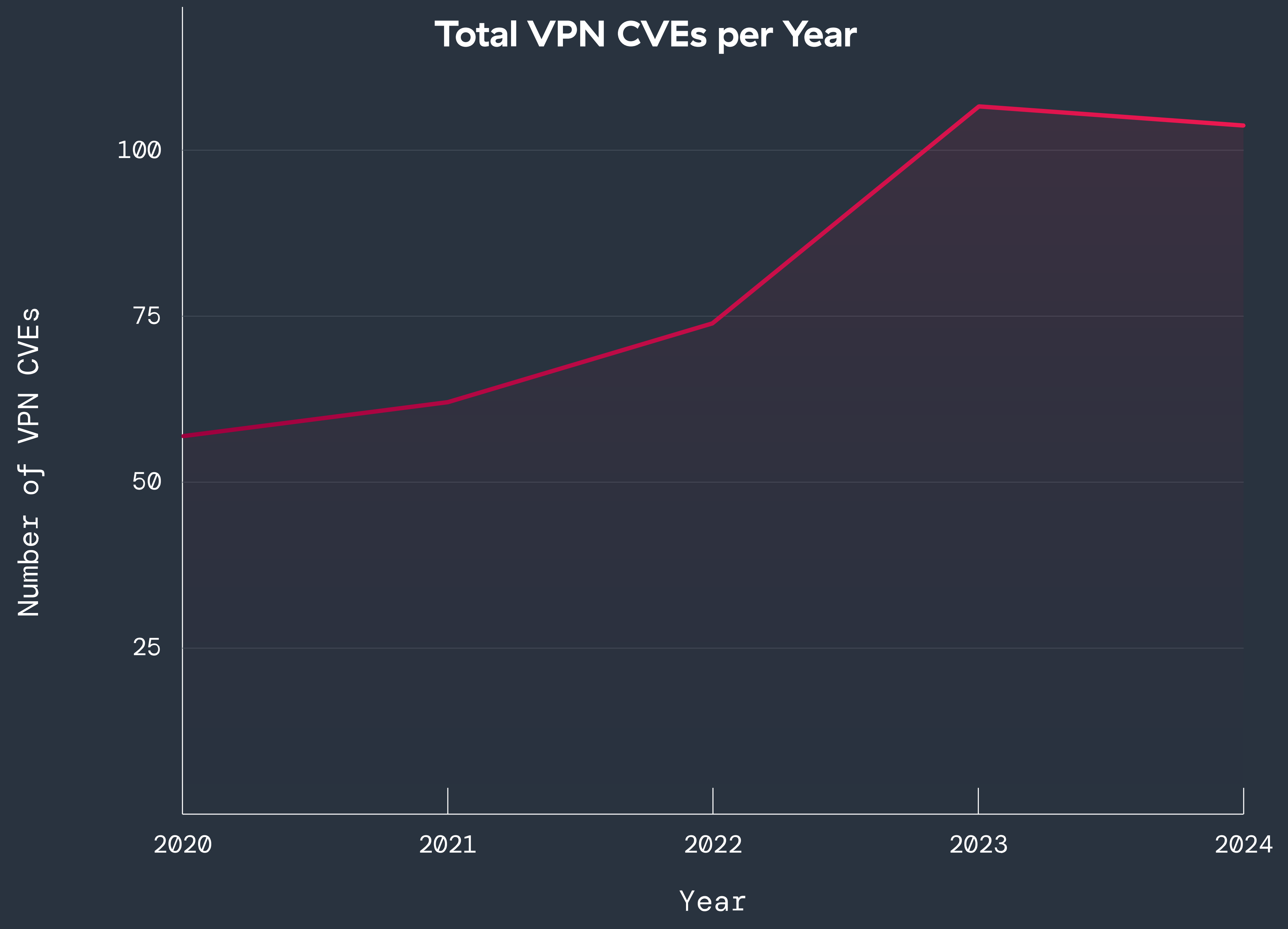


**Figure 4:** Total VPN CVEs for each year, from 2020-2024.

# Key Trends: CVE Impact Types

To understand the potential harm of these vulnerabilities if they were to be exploited, ThreatLabz assessed VPN CVEs across five categories of attack: remote code execution (RCE), privilege escalation, information leakage, denial of service (DoS) and authentication bypass. Note some categories are catch-all groupings for separate, but closely related, kinds of attacks: for example, authentication bypass includes attacks that may bypass second-factor or multi-factor authentication (MFA), while other bypass basic authentication measures. In general, any RCE vulnerability will be a high-priority item to remediate for any organization.

VPN CVEs by Impact Type

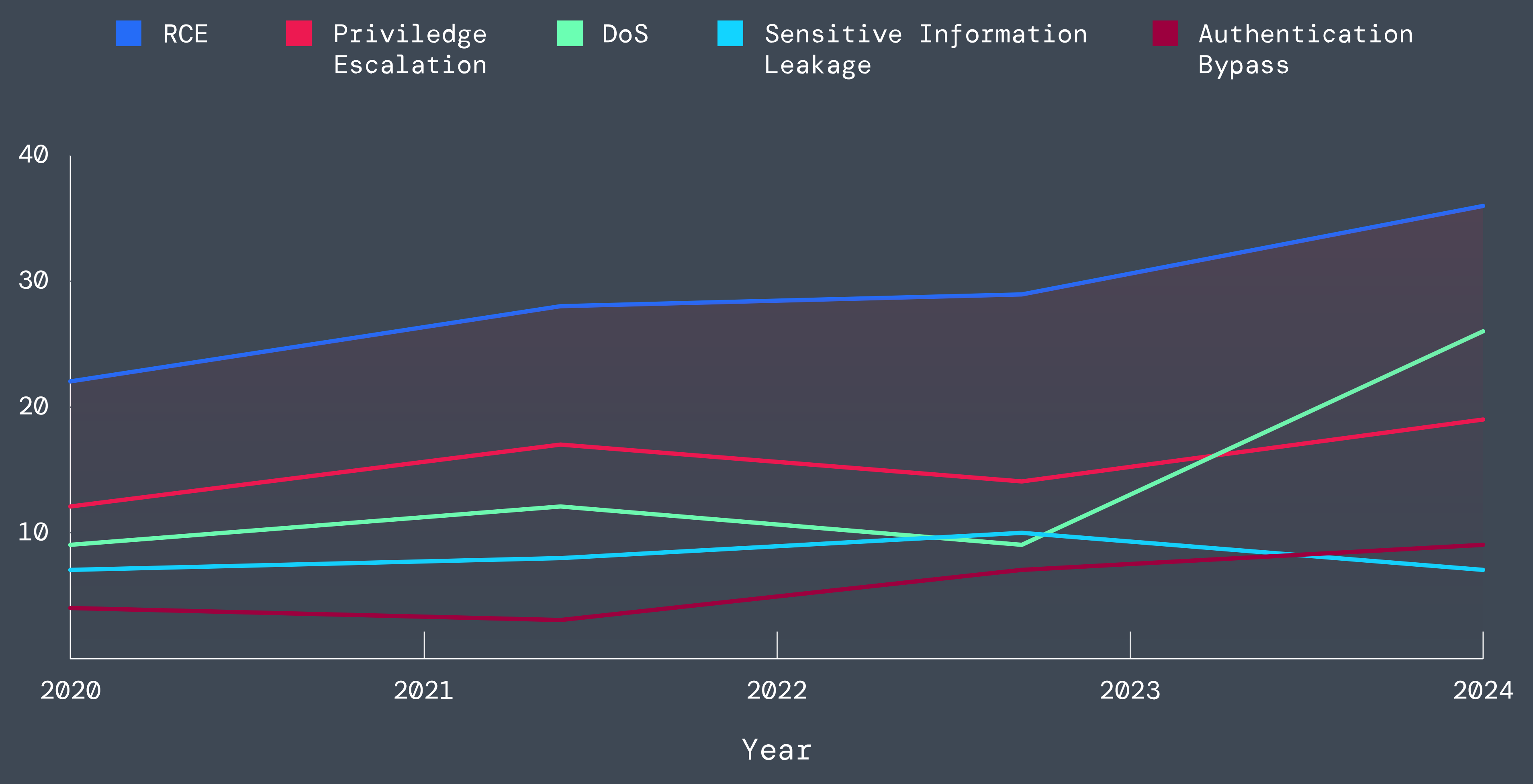


**Figure 5:** The impact type of VPN CVEs from 2020-2024, covering RCE, privilege escalation, DoS Sensitive Information Leakage, Authentication Bypass.

## 1. RCE Remains the Top Threat

- **Observation:** RCE vulnerabilities top the list across all four years, with 32 alone in 2024. RCE accounts for 149 CVEs including 2025 data, making it the most frequent and critical vulnerability type.
- **Implication:** RCE vulnerabilities allow attackers to execute arbitrary commands on VPN devices, potentially leading to full system compromise. Enterprises should prioritize patching and securing systems vulnerable to such exploits.

## 2. Privilege Escalation is Steadily Growing Over Time

- **Observation:** There is a steady increase in privilege escalation CVEs (66.7%), peaking in 2024 with 20 vulnerabilities.
- **Implication:** Attackers increasingly exploit VPN flaws to escalate privileges, gaining administrative control over systems. Enterprises must ensure secure system configurations and restrict privilege access tightly.

## 3. Denial-of-Service (DoS) Vulnerabilities Show a Sharp 200% Rise

- **Observation:** DoS-related CVEs tripled from 9 in 2020 to 27 in 2024, becoming the second-highest impact type in recent years — 85 CVEs overall, including 2025 data so far.
- **Implication:** DoS attacks are evolving in sophistication, making VPN systems prime targets for operational disruptions. Enterprises should adopt rate-limiting and traffic shaping to mitigate these risks.

## 4. Sensitive Information Leakage is Rarer but Still Critical

- **Observation:** Though relatively less common, with 41 CVEs total, sensitive information leakage vulnerabilities expose critical credentials, encryption keys, and user data.
- **Implication:** This impact type is particularly damaging for confidentiality and compliance. Enterprises should implement robust encryption, secure coding practices, and traffic monitoring to detect and prevent data leaks.

## 5. Steady Growth in Authentication Bypass Vulnerabilities

- **Observation:** Authentication bypass incidents have been relatively low, but consistent, growing from 4 in 2020, to a peak of 6 in 2023, to 4 vulnerabilities in 2024 — totaling 30 CVEs over time.
- **Implication:** Attackers are targeting weaknesses in multi-factor authentication (MFA) and login logic to impersonate users. Enterprises should strengthen MFA configurations and monitor for abnormal login behaviors.

# Key Trends:
# Critical VPN Vulnerabilities

Beyond impact types, ThreatLabz also analyzed the severity of VPN CVEs each year. **Overall, ThreatLabz found the CVEs with CVSS scores of HIGH or CRITICAL grew 38.9% from 2020 to 2024.** Indeed, 66.3% of all CVEs in 2024 year were rated as HIGH or CRITICAL, indicating a potential severe impact to organizations when such CVEs are exploited before they are patched. Moreover, ThreatLabz analyzed critical trends across different types of vulnerabilities represented in the CVE data that enterprises should understand to better defend against evolving VPN threats.

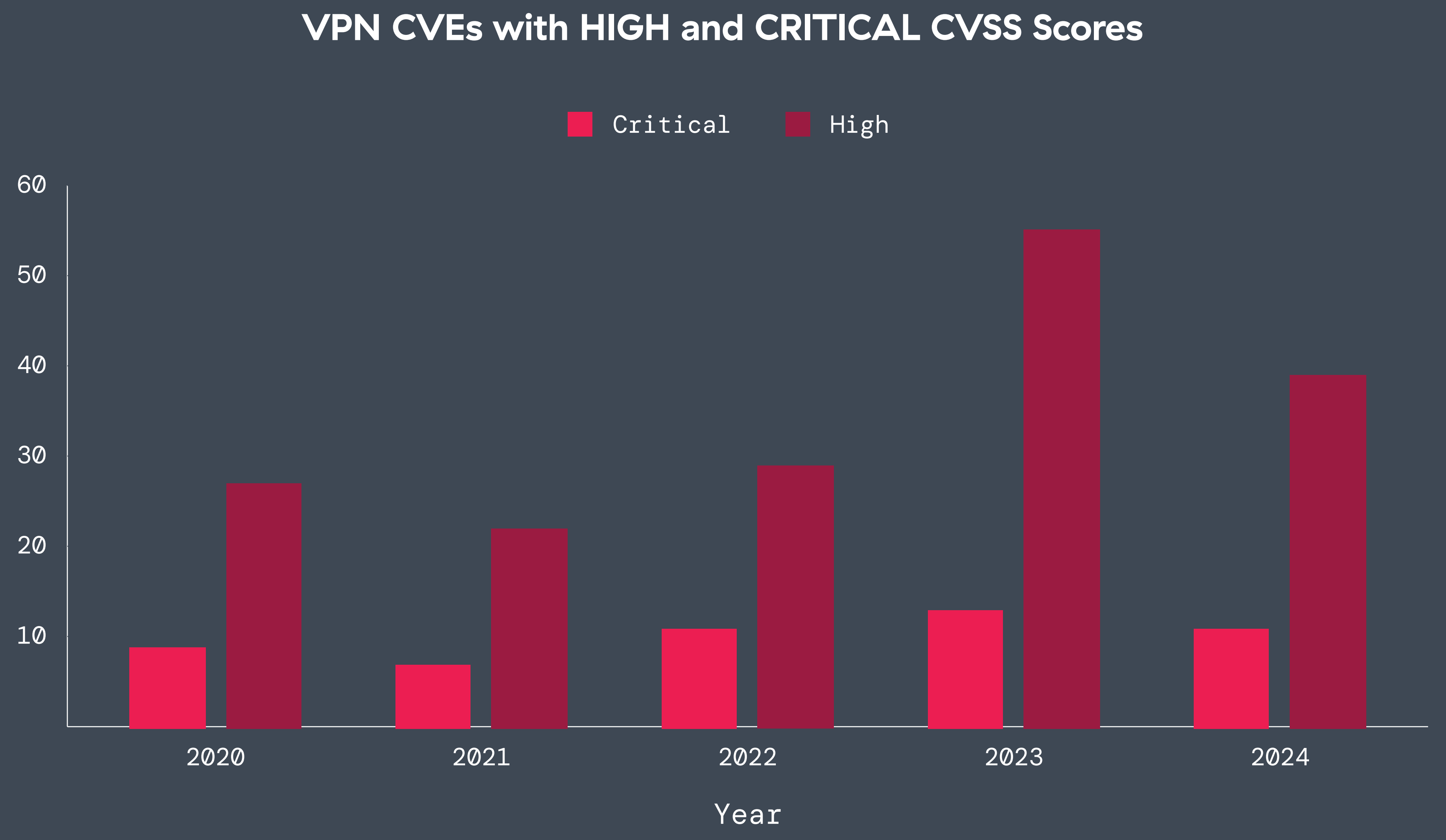


**Figure 6:** The volume of VPN CVEs with HIGH and CRITICAL CVSS scores from 2020-2024.

## 1. Increasing Exploitation of Web-Based Management Interfaces

- **Trend:** Command injection and input validation vulnerabilities have consistently risen, indicating attackers' growing focus on administrative and management portals, both from an administrator and end-user perspective. As these interfaces are inherently exposed to the internet via their architecture, they are prone to exploitation from threat actors.
- **Escalation:** While these vulnerabilities were present in 2020—2021, they significantly intensified from 2022 onward, suggesting attackers see these management interfaces as attractive and accessible targets, especially due to inadequate security coding practices.

## 2. Widespread Authentication and MFA Bypasses

- **Trend:** Attacks specifically targeting authentication methods—including MFA bypasses, session hijacking, and improper session management—steadily increased.
- **Escalation:** Earlier years (2020—2021) primarily saw simpler authentication bypasses, while from 2023—2025, these evolved into more advanced, automated, and persistent attacks aimed explicitly at MFA weaknesses, indicating attackers' intent to undermine stronger security measures.

## 3. Rise in Local Privilege Escalation Exploits

- **Trend:** Local privilege escalation vulnerabilities have become more prevalent and increasingly severe.
- **Escalation:** What began as minor configuration oversights in 2020—2021 intensified by 2024—2025 into more sophisticated privilege-escalation methods, such as DLL hijacking, giving attackers deeper system-level access.

## 4. Growing Sophistication of DoS and DDoS Attacks

- **Trend:** DoS attacks evolved from basic resource exhaustion (2020—2021) to sophisticated DDoS amplification techniques (2024—2025).
- **Escalation:** Attackers transitioned from simple malformed packet-based disruptions to more advanced amplified attacks, reflecting a strategic escalation to maximize operational disruption.

## 5. Persistent and Intensifying Cryptographic Failures

- **Trend:** Issues related to cryptographic implementation—such as improper certificate validation, leaked keys, and insufficient TLS verification—have escalated notably.
- **Escalation:** Starting around 2022, there was a noticeable spike in cryptographic vulnerabilities, peaking in 2024—2025 with high-severity flaws. This increase shows adversaries' strategic interest in exploiting encryption-related weaknesses to undermine VPN confidentiality.

# VPN Security_ Concerns (Cont.)

## The Challenges of Implementing Segmentation

Given the risks of lateral movement, many organizations try to limit attack spread through segmentation. While segmentation is a critical defense mechanism to reduce attack surface, its implementation is often challenging.

The survey highlights these challenges, with 51% of organizations anticipating or encountering configuration complexity. Additionally, 39% report a lack of expertise and resources, while 24% face performance bottlenecks—indicating that legacy network architectures are poorly equipped to support the granular access controls required for today's IT environments.

Segmentation challenges played a notable role in the 2023 MGM Resorts ransomware attack, where attackers gained initial access through social engineering but were able to move laterally due to insufficient segmentation. The breach disrupted hotel operations, ATMs, and casino gaming systems, costing the company an estimated US$100 million in damages. This case highlights how poor segmentation allows attackers to pivot across critical systems, amplifying the impact of an initial intrusion.

**To address these challenges, organizations should implement cloud-based, identity-driven segmentation models that streamline policy enforcement and reduce manual overhead. Unlike traditional network segmentation, which relies on complex firewall rules and VLAN configurations, a zero trust approach enables dynamic segmentation based on user identity, device posture, and real-time risk assessments. This ensures only authorized users can access specific applications while keeping the broader network secure.**

**What problems did your organization encounter or foresee while implementing segmentation?**

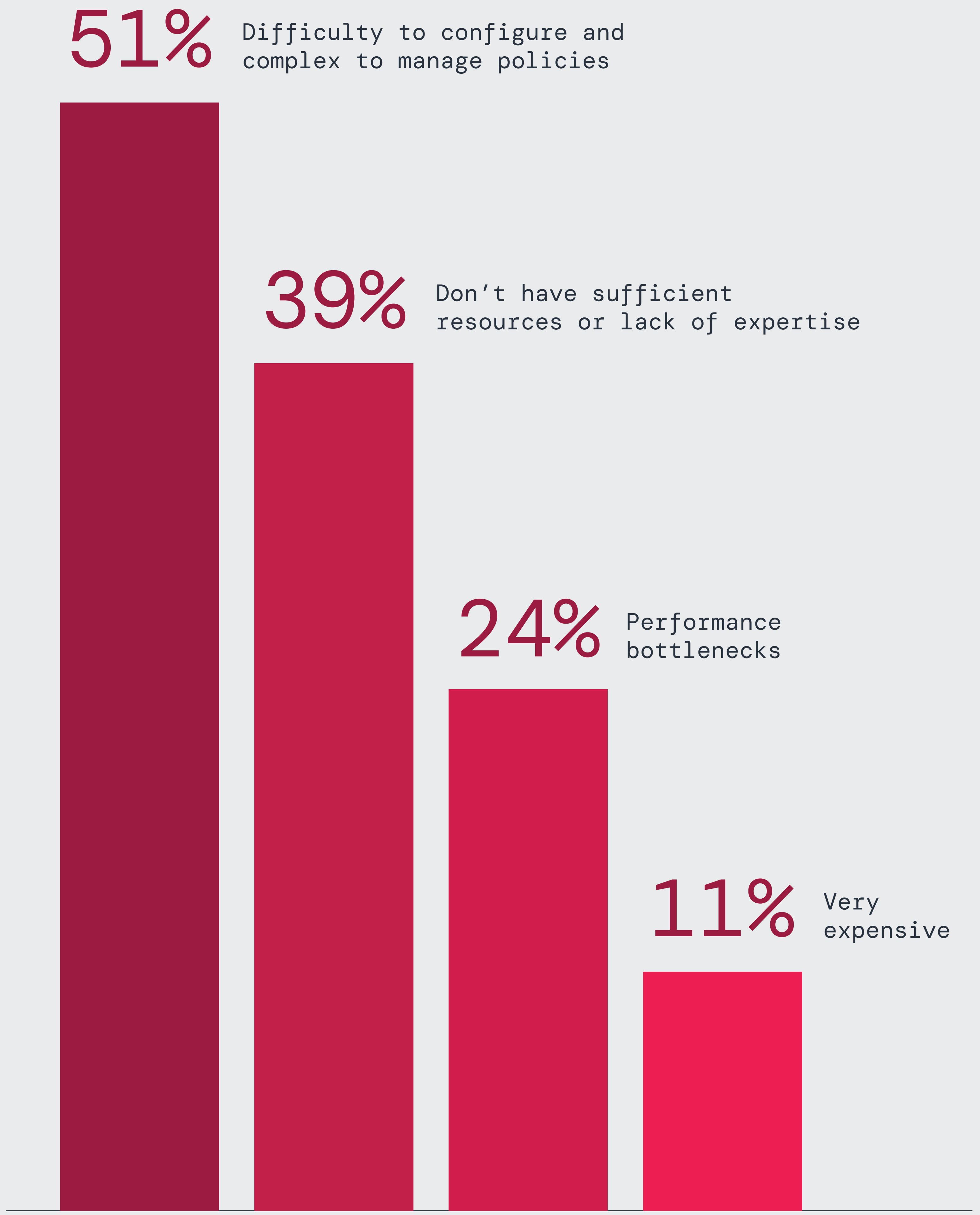


**Figure 7:** The top challenges enterprises face when implementing segmentation.

# VPNs Increase M&A Cybersecurity Risks

Beyond day-to-day security challenges, major IT transitions—such as mergers and acquisitions (M&A)—pose additional risks and expand attack surfaces. These transitions often involve merging disparate networks, applications, and identities, which can lead to inherited vulnerabilities, misconfigurations, and weak security controls.

Nearly two-thirds (64%) of respondents expressed concern about cyberthreats following M&A, acknowledging the security gaps that arise during IT integrations.

A recent example is the 2023 Capita data breach, where attackers exploited security weaknesses following a corporate acquisition, gaining unauthorized access to sensitive data. The incident stemmed from misaligned security policies between the merged entities, allowing threat actors to move laterally across the newly integrated network. This breach underscores how inconsistent security controls, legacy VPN access, and unsegmented environments create ideal conditions for cyberattacks during M&A activity.

**To mitigate these risks during M&A, organizations must prioritize cybersecurity due diligence, enforce least-privileged access, and implement segmentation. Unlike VPN-based access models, zero trust prevents merged IT environments from inheriting broad access permissions, effectively reducing the risk of lateral movement and privilege escalation. By replacing VPNs and perimeter-based defenses with identity-driven access controls that validate every request, organizations can secure both legacy and newly integrated IT environments.**

**Are you concerned about being vulnerable to cybersecurity attacks post M&A?**

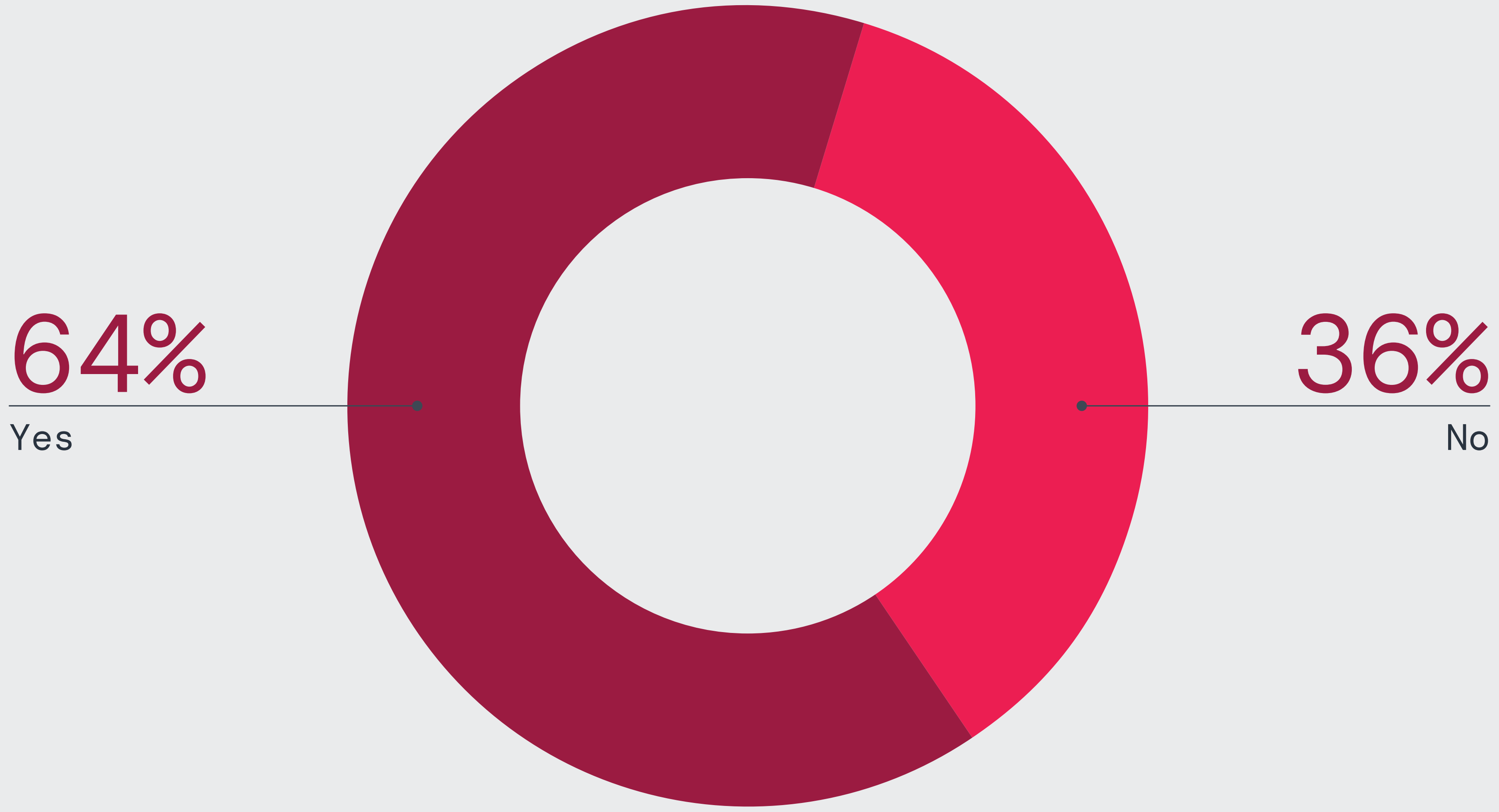


**Figure 8:** Enterprises are concerned about cyber attacks after M&A

# Third-Party VPN Access: A Backdoor for Attackers

Third-party access has emerged as one of the most vulnerable entry points for attackers. Traditional VPNs, by design, rely on broad network access once authentication is completed, extending this privilege to external vendors and partners. This practice creates blind spots that attackers are eager to exploit. Attackers can exploit stolen or weak credentials, misconfigurations, and unpatched vulnerabilities to hijack these trusted connections. With 93% of respondents expressing critical concerns about backdoor vulnerabilities, third-party access represents a ticking time bomb for organizations reliant on static, trust-based access models.

This concern is well-founded. In August 2024, Enterprise Financial Group (EFG) suffered a significant data breach exposing the personal information of nearly 20,000 clients. The breach was traced back to vulnerabilities in a third-party VPN used by EFG, which attackers exploited to infiltrate the network and access sensitive data. This incident underscores how third-party VPNs create security gaps that attackers can exploit as entry points into corporate networks.

**Organizations should start by auditing third-party VPN access and enforcing stricter policy controls, such as time-limited access, end-to-end traffic inspection (device to application), and adaptive authentication. Transitioning to a zero trust model will enable enforcement of application-specific access, ensuring external partners only have the minimal access required. Furthermore, continuous monitoring and risk-based policies can significantly mitigate third-party vulnerabilities.**

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

93% are concerned about third parties serving as potential backdoors into their networks through VPN access

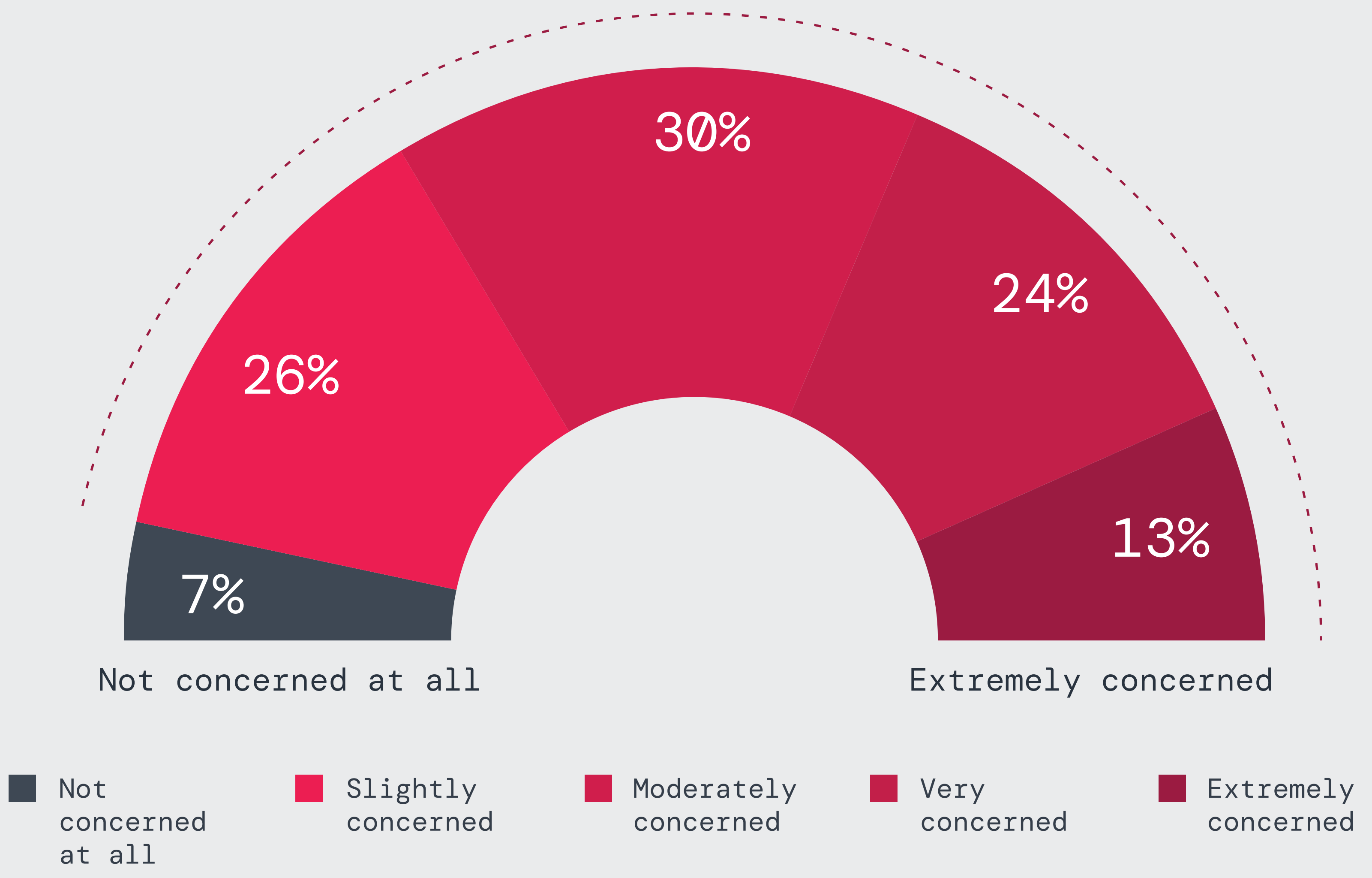


**Figure 9:** Enterprise concerns about third-party VPN access facilitating cyber attacks.

# Challenges and Gaps with Legacy Protective_Measures

## Traditional Tools Leave for Private Applications Exposed

Securing private applications against increasingly sophisticated web-based threats—such as ransomware, credential theft, and API abuse—has become a mission-critical priority for modern enterprises. Yet many organizations continue relying on legacy tools ill-equipped to counter today's threat landscape.

According to the survey, firewalls (84%), web application firewalls (WAFs, 58%), and VPNs (43%) still dominate organizations' web attack defenses. However, attackers are increasingly bypassing these tools—leveraging unpatched devices, poor configurations, and inherent weaknesses in perimeter-based security models—showing that these legacy defenses no longer meet the demands of modern threat landscapes.

Recent breaches highlight the shortcomings of such perimeter-based defenses. In August 2024, Chinese hackers — a group dubbed Salt Typhoon — infiltrated major US telecommunications firms, including AT&T and Verizon, by exploiting vulnerabilities in unpatched network devices and routers. This attack compromised sensitive metadata of more than 1 million users, demonstrating how sophisticated adversaries can circumvent traditional security measures like firewalls and VPNs.

**The only viable solution for effectively protecting private applications is to move beyond outdated perimeter defenses and adopt zero trust access models. Zero trust architectures eliminate reliance on network-based security, allowing users to connect directly to applications under strictly enforced policies of granular, least-privileged access. Unlike firewalls and VPNs, zero trust architectures enable users to connect directly to applications with granular, least-privileged access. This approach blocks unauthorized access attempts and prevents lateral movement, session hijacking, and credential theft—the tactics attackers commonly use to circumvent traditional perimeter defenses.**

**What products do you use to protect your private applications against web-based attacks?**

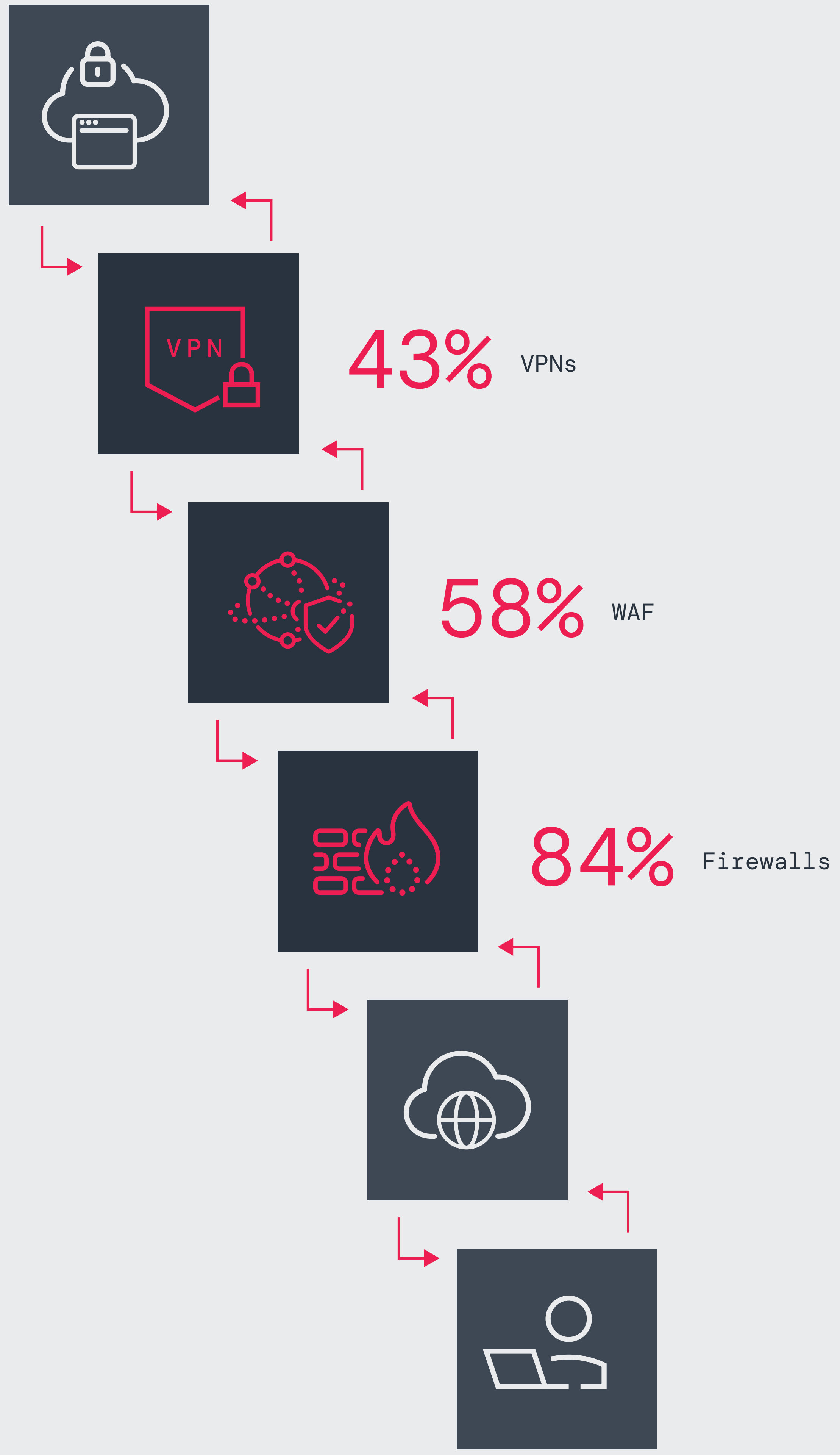


**Figure 10:** The security products in-use by enterprises to defend private applications from web-based threats.

# NAC Deployment in VPN Environments: A Limited Safeguard

A notable 54% of surveyed organizations report using NAC to secure VPN access to private resources. However, these deployments have yet to prevent the breaches and exploits commonly associated with VPN vulnerabilities, highlighting NAC's inability to address the systemic risks of network-based trust models.

NAC solutions enforce device posture checks, authentication, and network segmentation. However, they fail to address core VPN security issues such as broad access permissions, lateral movement risks, and reliance on implicit trust.

Recent breaches demonstrate that even with NAC in place, VPN vulnerabilities remain a critical weakness. In November 2023, the US Department of Energy confirmed a major security incident involving compromised VPN credentials, which allowed attackers to bypass access controls and infiltrate sensitive internal systems. This highlights how attackers can exploit VPN weaknesses directly, either through stolen credentials, unpatched vulnerabilities, or session hijacking—rendering NAC an incomplete defense if the underlying trust model remains unchanged.

Are you using a NAC (Network Access Control) in between your VPN and Private Resources?

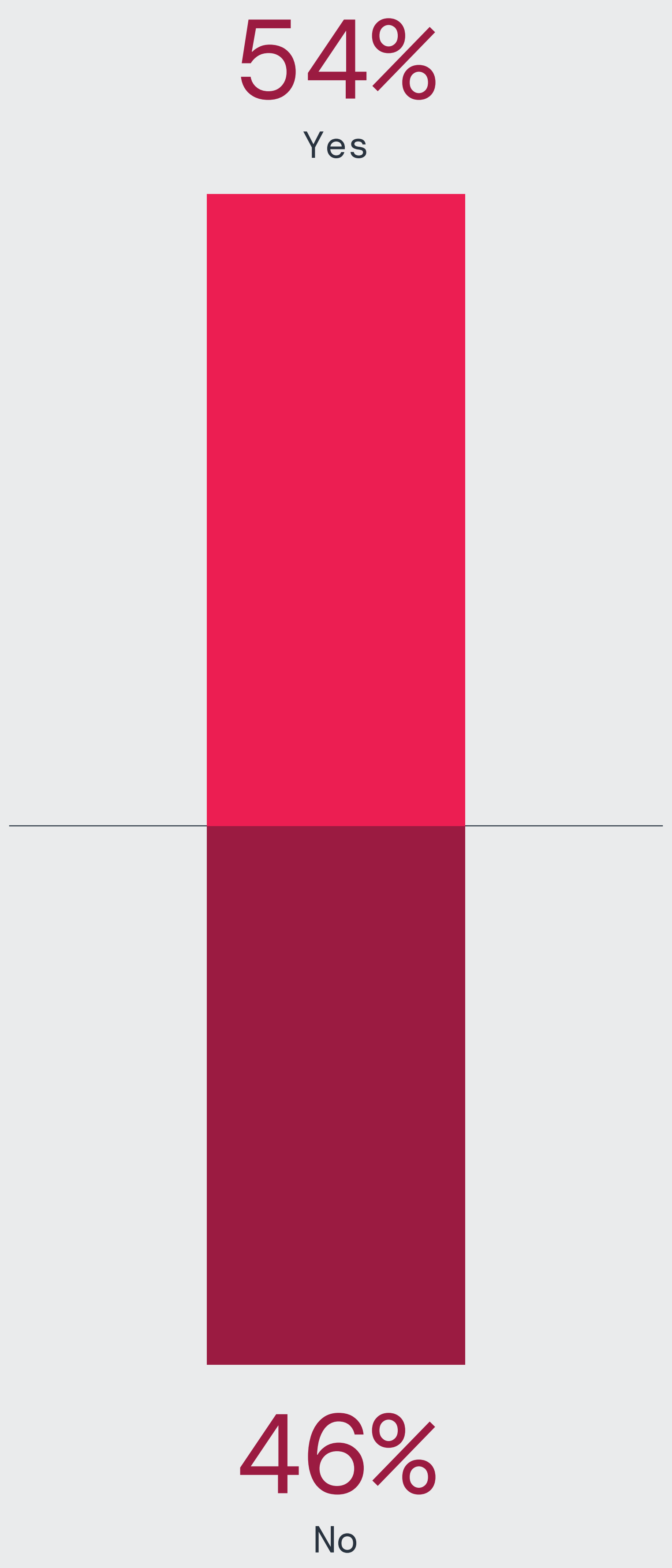


**Figure 11:** Proportion of enterprises using NAC in between VPNs and private resources.

**To overcome the limitations of NAC and legacy VPN architectures, organizations must adopt a zero trust security model. Zero trust eliminates broad network trust by allowing users to connect directly to specific applications under continuously validated policies tied to identity, device posture, and context. Zero trust not only blocks unauthorized access but also shuts down lateral movement, thwarting attackers before they can escalate privileges or exfiltrate data.**

# VPN User Experience_ and Management_Issues

## The VPN Performance Problem: Frustrating Users and Overloading IT

VPNs are not just a security liability—they are also a major source of user dissatisfaction. End users increasingly express frustrations with VPN performance issues, which create obstacles for productivity and add to the growing strain on IT teams.

Slow connection speeds are the most common complaint (23%), underscoring VPNs' reputation for latency, congestion, and poor performance when accessing cloud applications from home. Authentication challenges also remain a significant issue, with 20% of respondents citing complex login processes and 17% struggling with application access due to authentication errors.

These performance challenges disrupt daily business operations, dampen productivity, and turn the IT help desk into a bottleneck as teams wrestle with frequent troubleshooting requests—a problem that only worsens as remote and hybrid work environments grow in complexity.

**Replacing VPNs with zero trust network access (ZTNA) not only eliminates bandwidth congestion but also vastly improves the end-user experience by enabling direct, secure, and latency-free connections to applications. Unlike VPNs, which route all traffic through a central gateway and create performance bottlenecks, ZTNA enables direct and secure access to applications without performance degradation. By adopting identity-driven access controls, continuous verification, and cloud-delivered security, organizations can not only eliminate common VPN frustrations but also boost workforce productivity and reduce the IT burden of troubleshooting and supporting inflexible VPN frameworks.**

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

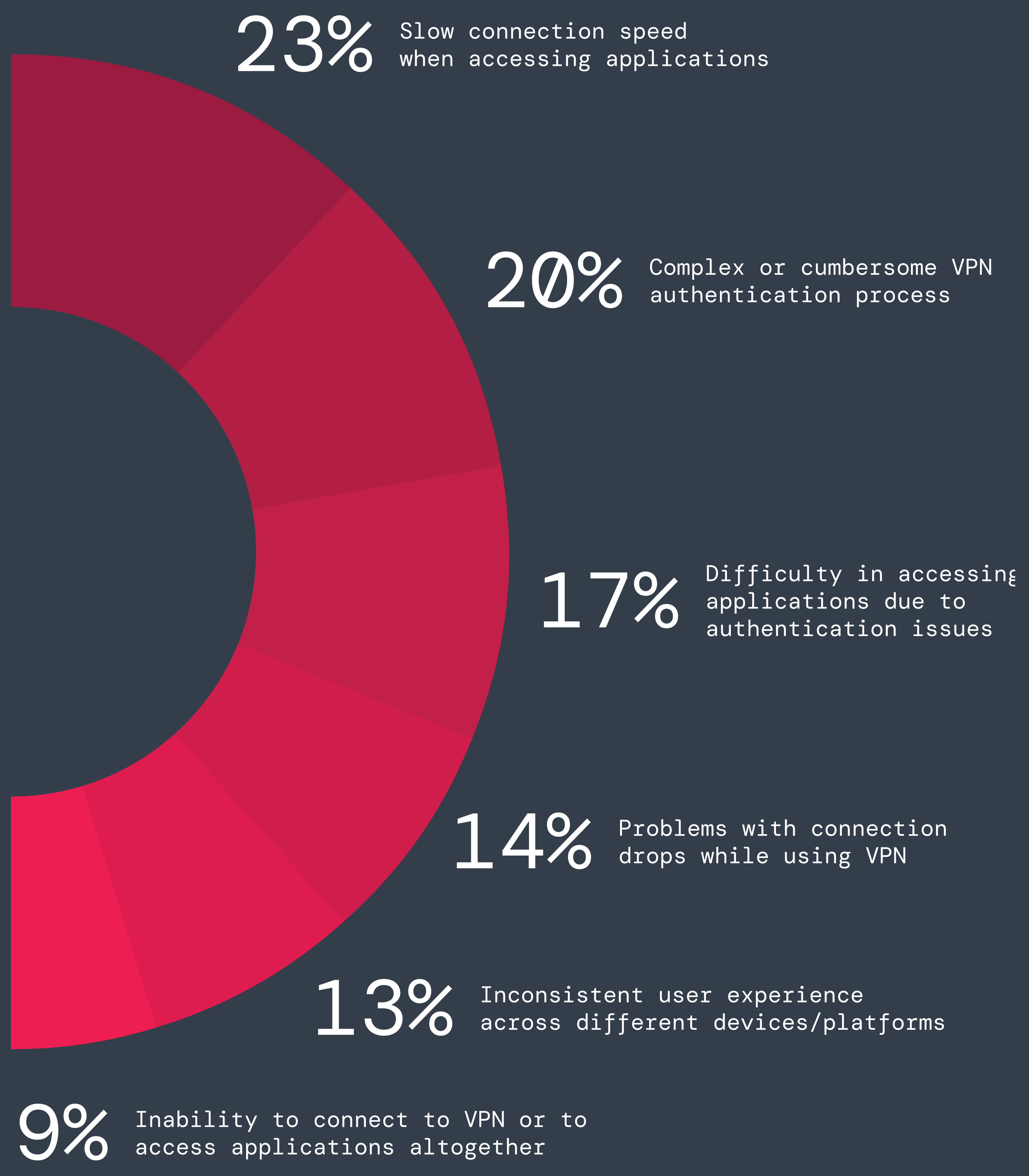


**Figure 12:** The most common complaints among VPN users.

# VPN Management: Overwhelming IT Teams and Exposing Vulnerabilities

VPNs are overloading IT teams with persistent security vulnerabilities, resource-heavy maintenance demands, and outdated access models that no longer align with the needs of today's cloud-focused enterprise environments. The top concern among these teams (52%) are security gaps that will lead to security incidents — underscoring the ongoing risks related to credential theft, unpatched software exploits, and attackers leveraging VPN access for unchecked lateral movement. These risks underscore why VPNs are increasingly viewed as liability-rich access solutions.

VPNs have become a financial and operational drain for IT teams, with 41% of respondents highlighting exorbitant resource costs tied to their upkeep. The relentless cycle of patching, troubleshooting, and log monitoring is necessary to secure outdated infrastructure but leaves teams stretched thin and unable to focus on higher-value activities.

The inability of VPNs to enforce granular access controls is another critical weakness, cited by 35% of respondents. Instead of granting precise, identity-driven access to specific applications, VPNs often provide broad, unrestricted network connectivity, dramatically increasing the potential for insider threats and lateral movement by attackers. Furthermore, 26% cite the operational overhead of managing VPN concentrators and other devices, illustrating the complexity of maintaining hardware appliances, network tunnels, and access gateways to sustain remote connectivity. These complexities are especially untenable in an era when cloud-native and remote work environments require more agile and scalable solutions.

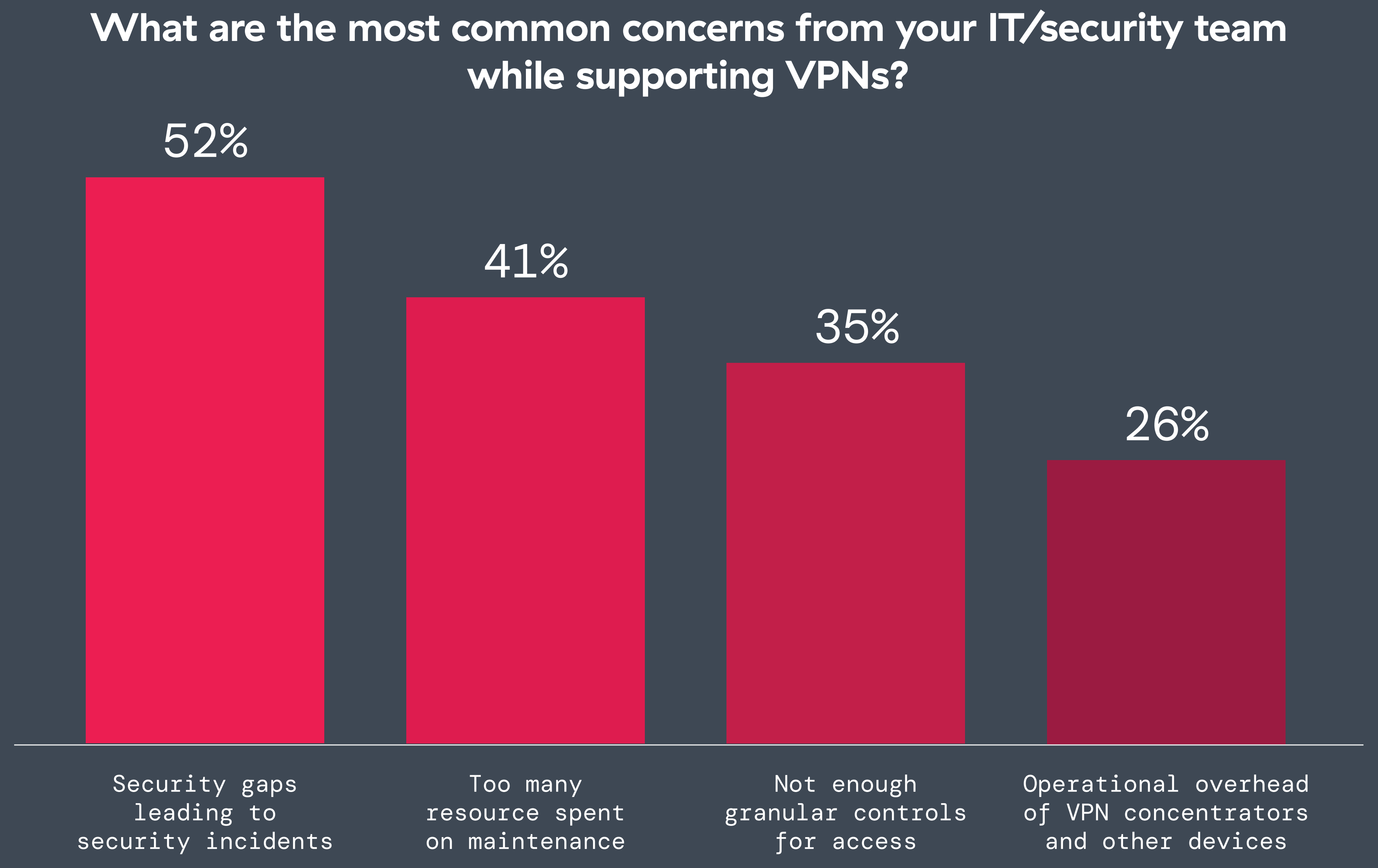


**Figure 13:** The top concerns of IT and security teams while supporting VPNs.

**To address these challenges, organizations should transition from network-based VPN access to a cloud-delivered zero trust model, which eliminates implicit trust, reduces attack surfaces, and streamlines IT operations. Adopting zero trust reduces VPN-related operational overhead, simplifies access management, and minimizes security risks at scale. IT teams are freed from the burden of constant maintenance tasks, enabling them to focus on proactive security initiatives while simultaneously delivering faster, more seamless user experiences.**

# The Heavy Burden of VPN Management

Managing VPN infrastructure continues to strain IT teams, with the top concerns centering on reliability, performance, and maintenance overhead. Troubleshooting VPN connectivity and stability issues remains the top challenge, cited by 54% of respondents. IT teams face ongoing struggles to maintain consistent VPN uptime, with connection failures creating widespread disruptions that degrade productivity, compromise security, and frustrate employees.

Balancing VPN performance and user experience remains a significant challenge (50%) as VPNs often introduce latency, disconnections, and inconsistent speeds, particularly in cloud-first environments. Additionally, 47% of IT professionals highlight frequent patching demands and resource costs as a major roadblock, underscoring the operational challenges of mitigating persistent vulnerabilities and maintaining outdated systems.

These challenges have played a role in several high-profile breaches. From December 2023 through early 2024, multiple government agencies were targeted in a VPN-related attack. Delays in patching a widely known vulnerability enabled threat actors to exploit outdated VPN software, gaining unauthorized network access. This case highlights the inadequacy of reactive patching cycles, even among organizations with dedicated IT teams, and demonstrates how incomplete VPN defenses expose critical sectors to evolving threats.

**With VPN infrastructure consuming significant IT resources for connectivity troubleshooting, security patching, and performance optimization, organizations must reevaluate the long-term viability of VPN-based access. By replacing VPN concentrators and network appliances like firewalls and NACs with a cloud native architecture, IT teams can eliminate infrastructure bottlenecks, reduce patching cycles, and remove the need for manual troubleshooting of connection failures.**

**Policy-driven, least-privileged access ensures that users connect only to authorized applications—without the burden of managing complex firewall rules or network segmentation policies. By transitioning to a cloud-delivered zero trust model, enterprises will be able to eliminate VPN-related bottlenecks while ensuring seamless, policy-driven access to applications—without the burden of managing network infrastructure, software patches, or complex scaling efforts.**

**What are the top three concerns in managing your VPN infrastructure?**

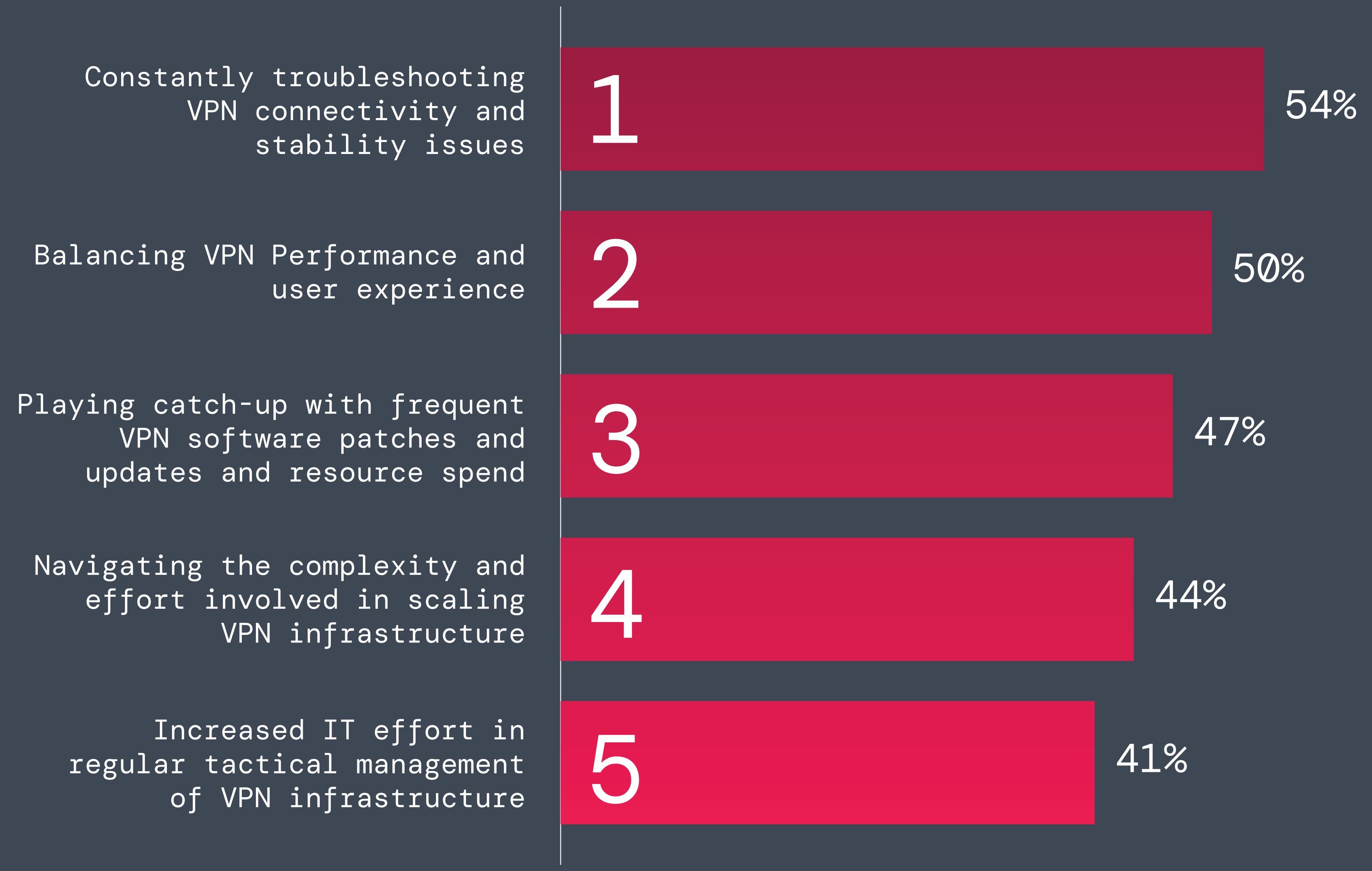


**Figure 14:** The top concerns among IT teams managing VPN infrastructure.

# Overly Broad VPN Access Controls: A Critical Security Gap

The root cause of many VPN security risks lies in how VPNs define access. Instead of providing precise, application-specific access, many organizations still grant broad network access and rely on implicit trust models, leaving critical systems exposed.

Survey findings reveal that 52% of organizations still depend on outdated access models such as static network firewall rules (28%) or open access for authenticated users (24%). These outdated controls make it easy for attackers to traverse networks undetected, escalate privileges, and exfiltrate critical data once access is gained.

Recent incidents underscore the dangers of such broad access. In early 2024, Global Affairs Canada (GAC) experienced a significant security breach due to a compromised VPN used by employees to access the Ottawa headquarters. Attackers exploited vulnerabilities in the VPN, gaining unauthorized access to the network and potentially exposing sensitive information. The event demonstrated how unrestricted and over-privileged network access provides an ideal framework for lateral movement and deeper infiltration.

**To mitigate these risks, organizations should eliminate implicit trust and enforce granular, identity-driven access controls. Shifting from broad network-based access models to direct, application-level segmentation ensures a given user can only reach the specific resources required for their role, significantly reducing attack surfaces and preventing lateral movement.**

**How do you define VPN users' access to applications?**

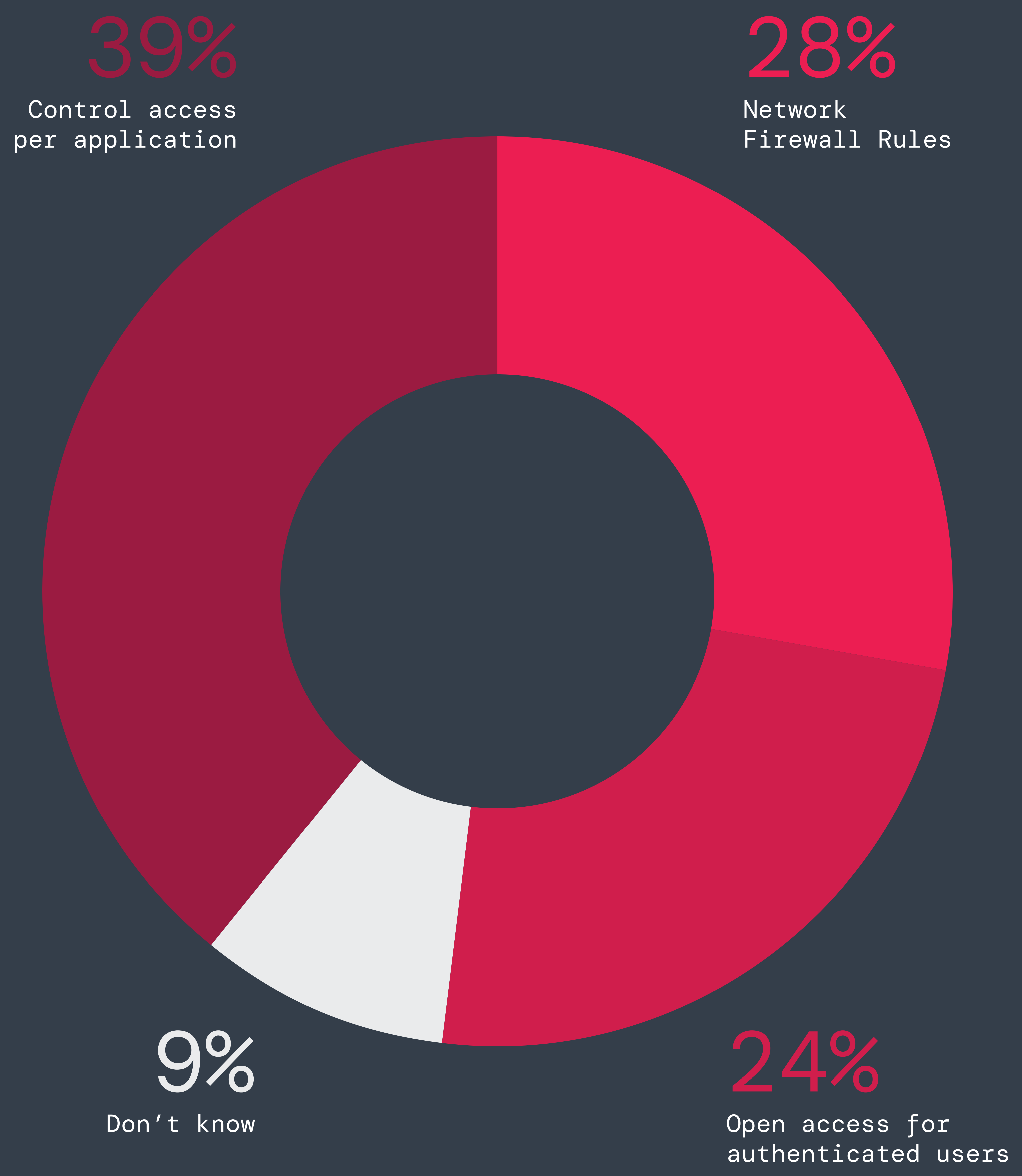


**Figure 15:** The ways that enterprises define VPN users access to applications.

# VPN Replacement: A Shift Toward Secure Access

The mounting security vulnerabilities, user experience challenges, and high maintenance overhead of VPNs are driving organizations to accelerate their transition to modern secure access technologies like ZTNA. This shift signals the growing realization that VPNs are no longer capable of meeting modern security or operational demands.

The survey confirms this momentum, with 65% of respondents saying their organizations are either replacing or planning to replace their VPNs within the next year.

**As organizations increasingly shift away from VPNs, they must prioritize adoption of cloud-delivered security models that enforce granular, application-level access rather than broad network connectivity. ZTNA eliminates VPN-related risks by ensuring that users can only access the resources they need, based on identity and security posture, without ever placing them on the corporate network. This approach enhances security, reduces operational complexity, and improves user experience, making VPN replacement an urgent and necessary step for modern enterprises.**

**What are your plans for replacing your current VPN service?**

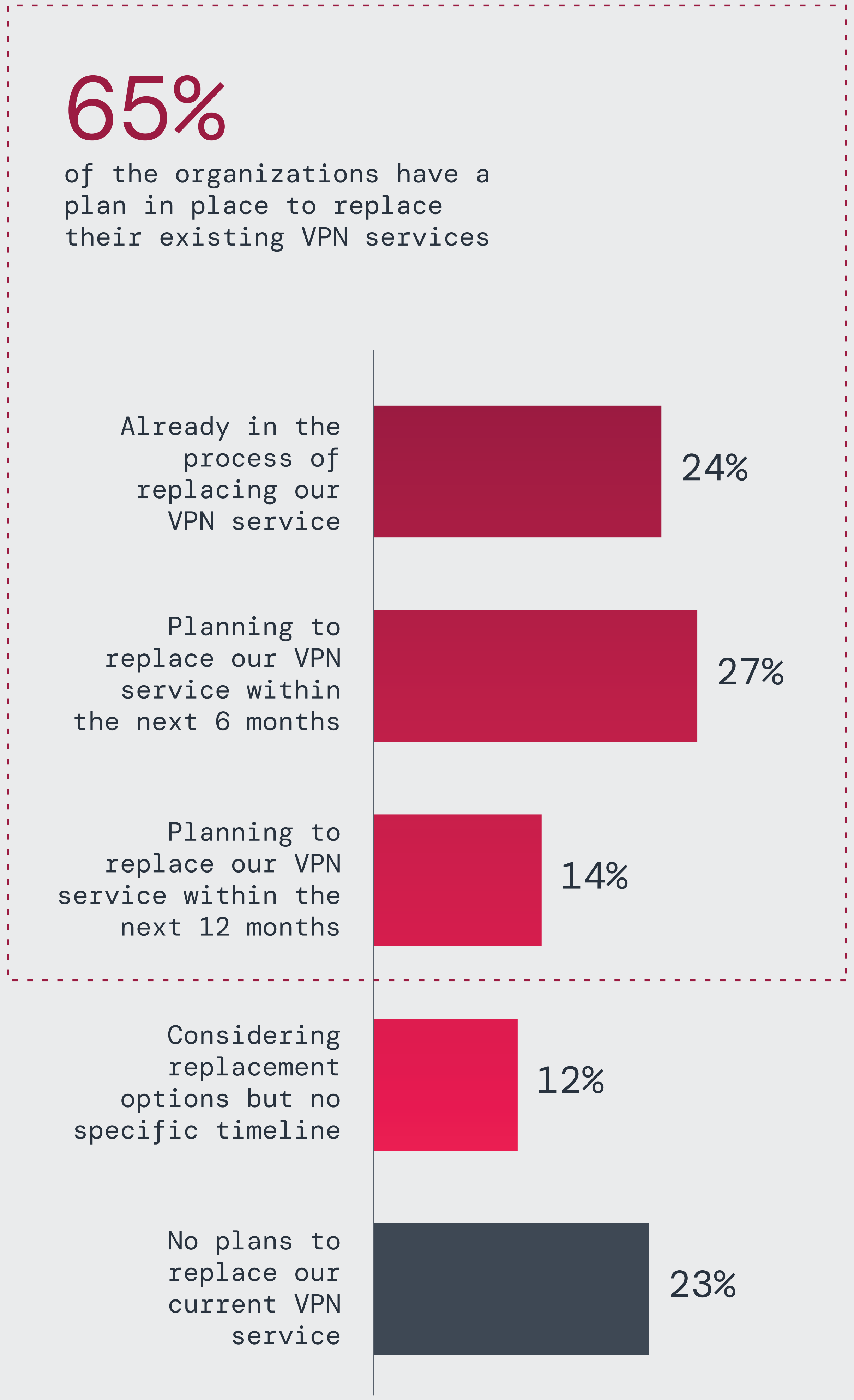
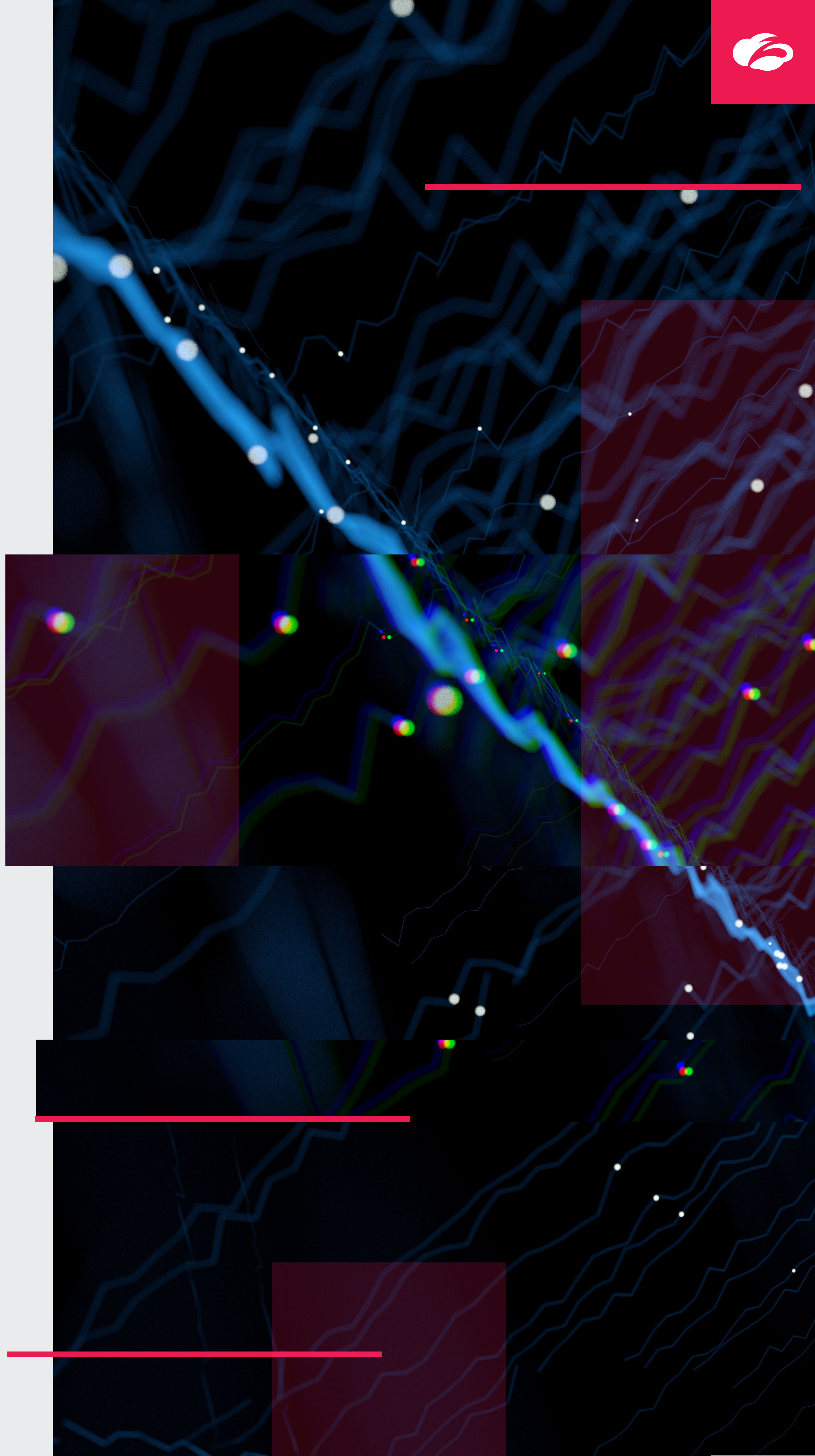


**Figure 16:** Enterprise plans to replace existing VPN services.



# Zero Trust_ Adoption

## Zero Trust Replacing VPN At Scale

As the trend of VPN replacement accelerates, the large majority of organizations are turning to zero trust architectures to enable granular access controls, reduce their attack surfaces, and improve user productivity. Survey results underscore the growing momentum of this paradigm shift: 81% of respondents indicate plans to adopt zero trust slated within the year. Among these, 35% are already implementing zero trust solutions, 24% anticipate rollouts within six months, and 22% have deployment strategies slated for the following year—showcasing zero trust as the industry's leading strategy for replacing legacy access technologies like VPNs.

**Successful zero trust adoption requires alignment between security teams and business operations. Organizations should conduct risk assessments to identify their most vulnerable access points—whether remote access, third-party integrations, or critical applications—and prioritize zero trust deployment accordingly. Leveraging automation for policy enforcement can accelerate the transition while reducing administrative overhead.**

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

96% of companies have already implemented, are planning, or bought into a zero trust strategy

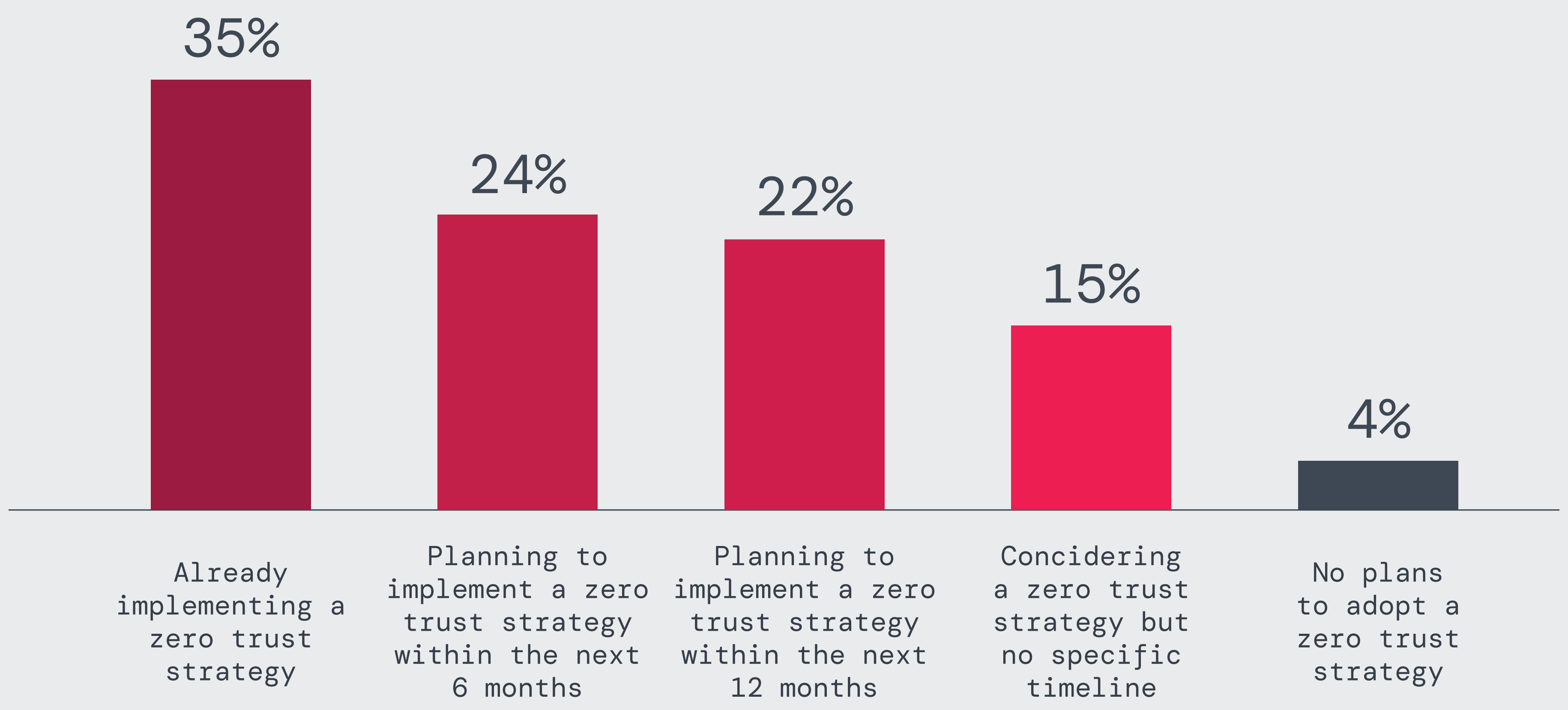


**Figure 17:** Enterprise plans for implementing a zero trust strategy.

# Zero Trust Priorities: Remote Work Drives Adoption

The shift away from traditional VPNs underscores a significant transformation: organizations are turning to zero trust architectures to address security gaps, streamline IT operations, and meet the demands of decentralized remote workforces. This strategic pivot highlights zero trust as the modern solution to mitigate VPN risks and simplify security management.

Survey results indicate that securing remote workforces is the primary motivation for this shift, with 37% of organizations focusing on remote work and 28% on hybrid workforce security. This move reflects a broader trend toward security models that offer direct, application-specific access, thereby reducing the complexities associated with managing multiple point products inherent in legacy VPN setups.

Implementing a zero trust framework not only strengthens security, but also alleviates the operational burden of managing numerous security solutions. By unifying security policies and controls into a cohesive system, organizations can reduce administrative overhead and streamline operations. For example, a zero trust platform that performs multiple policy actions in a single scan can eliminate the need to chain together various solutions, simplifying the user experience while maintaining robust security.

**To effectively secure remote and hybrid workforces with a zero trust architecture, organizations should focus on integrating security measures that minimize complexity. Implementing a unified zero trust platform can consolidate various security functions, reducing the need for multiple point products and simplifying management. This approach improves security and operational efficiency, allowing IT teams to focus on strategic initiatives rather than managing a complex array of security tools.**

What is the primary use case for deploying a Zero Trust solution?

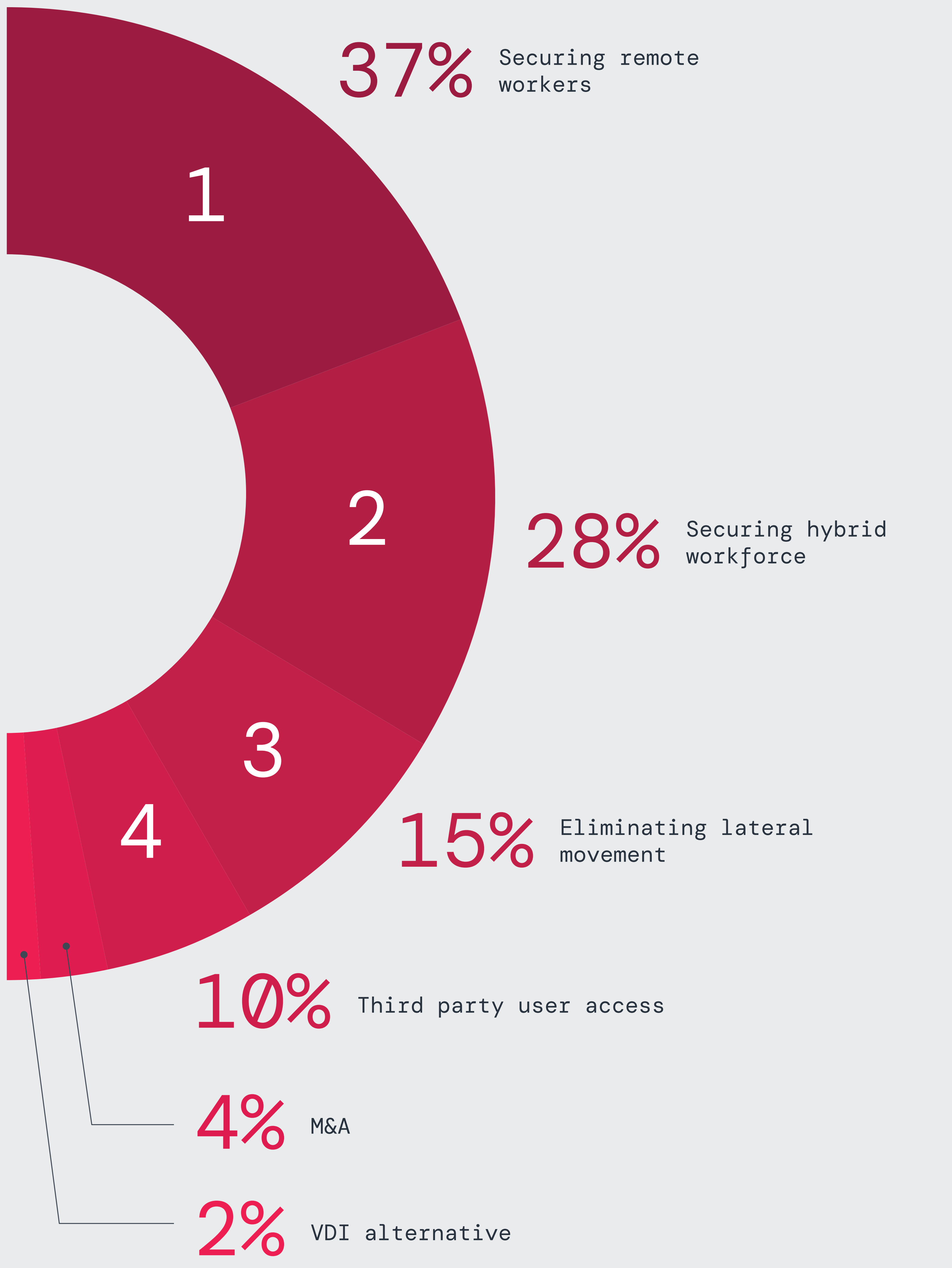


**Figure 18:** Enterprises' primary uses case for zero trust solutions.

# Key Advantages of Replacing VPNs with Zero Trust

The adoption of zero trust solutions is transforming enterprise security, delivering far-reaching benefits beyond secure access—particularly in simplifying management, enhancing performance and scalability, dramatically reducing attack surface, and improving resource efficiency. Organizations replacing VPN models with zero trust are not merely upgrading tools; they're future-proofing their entire remote access strategy.

The vast majority of respondents (76%) see improved security and compliance as a primary advantage, reinforcing how zero trust replaces implicit network access and reduces exposure to ransomware, credential theft, and lateral movement risks.

Additionally, 64% report gains in management simplicity, scalability, and user experience as a primary advantage, as zero trust eliminates the operational burdens of managing VPN concentrators, constant patching, and access troubleshooting.

Close to half (45%) of respondents cite the replacement of VPN with a zero trust solution as a critical step toward a full zero trust architecture.

Meanwhile, 34% highlight the superior scalability and flexibility that make zero trust a more effective solution for securing remote and hybrid workforces. Other benefits add to the zero trust value profile: improved end-user experience (32%), seamless integrations across IT and security systems (28%), and reduced operational costs through resource savings (18%). Collectively, these advantages illustrate why organizations are rapidly phasing out legacy VPNs in favor of zero trust.

ManpowerGroup, a global leader in workforce solutions, offers a compelling case study for securing access with zero trust.  Faced with the task of supporting a vast remote workforce, the organization successfully replaced its legacy VPN infrastructure with a Zscaler zero trust solution. Remarkably, within just 18 days, ManpowerGroup scaled secure application access to more than 30,000 users, achieving uninterrupted business continuity while drastically reducing help desk tickets by 97%. This deployment highlights the ability of a zero trust architecture to scale rapidly, simplify operations, and drive measurable outcomes for productivity and security.

**If you have replaced a VPN solution with a Zero Trust solution, what do you view as the primary advantages, compared to the previous VPN solution?**

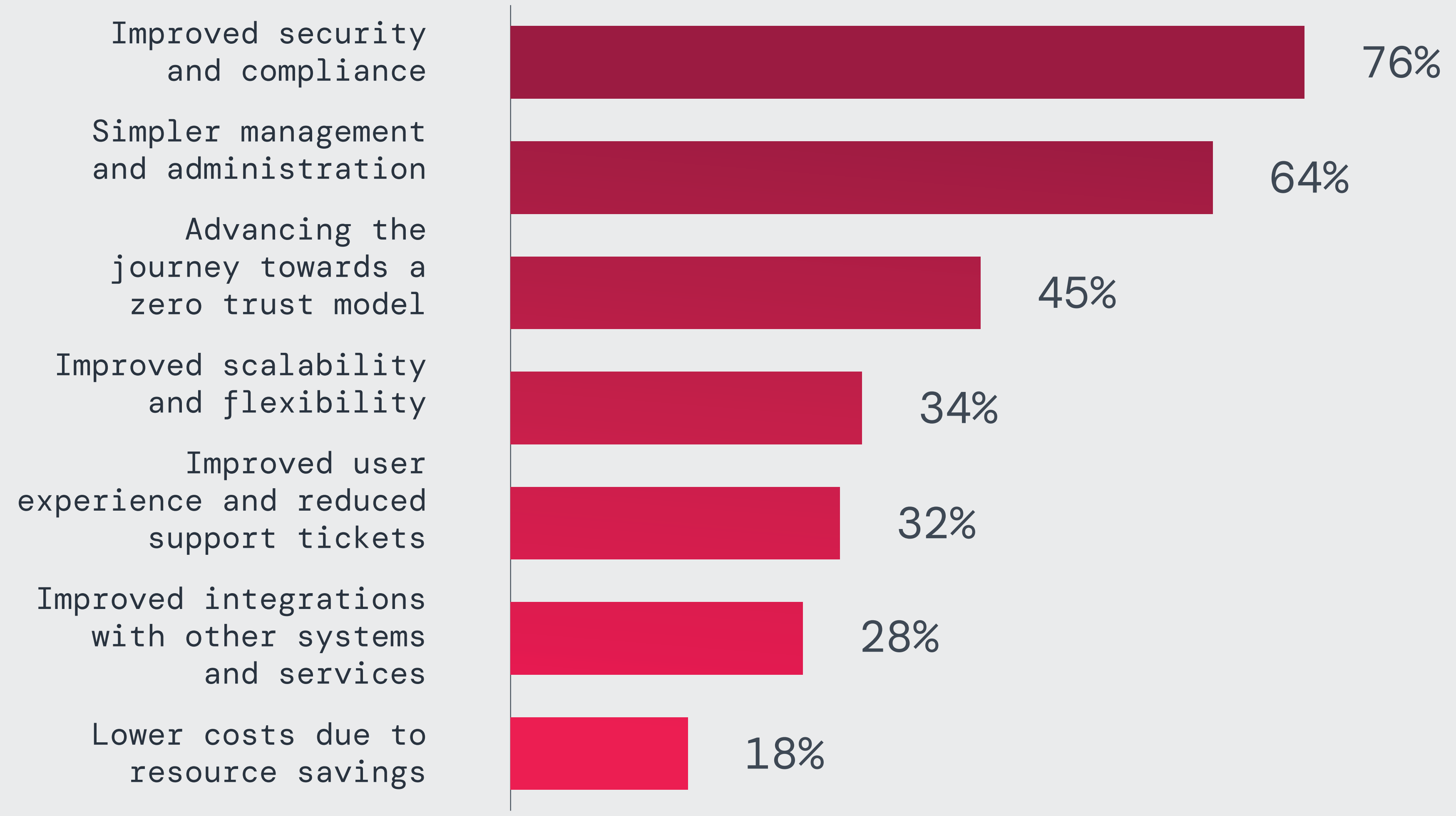


**Figure 19:** Enterprises share the primary advantages of a zero trust solution, compared to a previous VPN solution.

**Zero trust adoption should begin with tactical changes that eliminate VPN-driven network access in favor of direct, application-level connections to counter lateral movement risks. Organizations can prioritize replacing legacy access for critical use cases, such as securing remote and third-party user connections, before scaling zero trust capabilities across their IT ecosystem. Automating access policies — using a single policy set — and integrating identity-based security will further simplify simplify zero trust management while enabling scalability across distributed systems. These intelligent frameworks empower IT teams to maintain real-time security control without sacrificing agility or efficiency.**

# VPN Risk Predictions for_2025

## Critical VPN Vulnerabilities Will Continue to Emerge

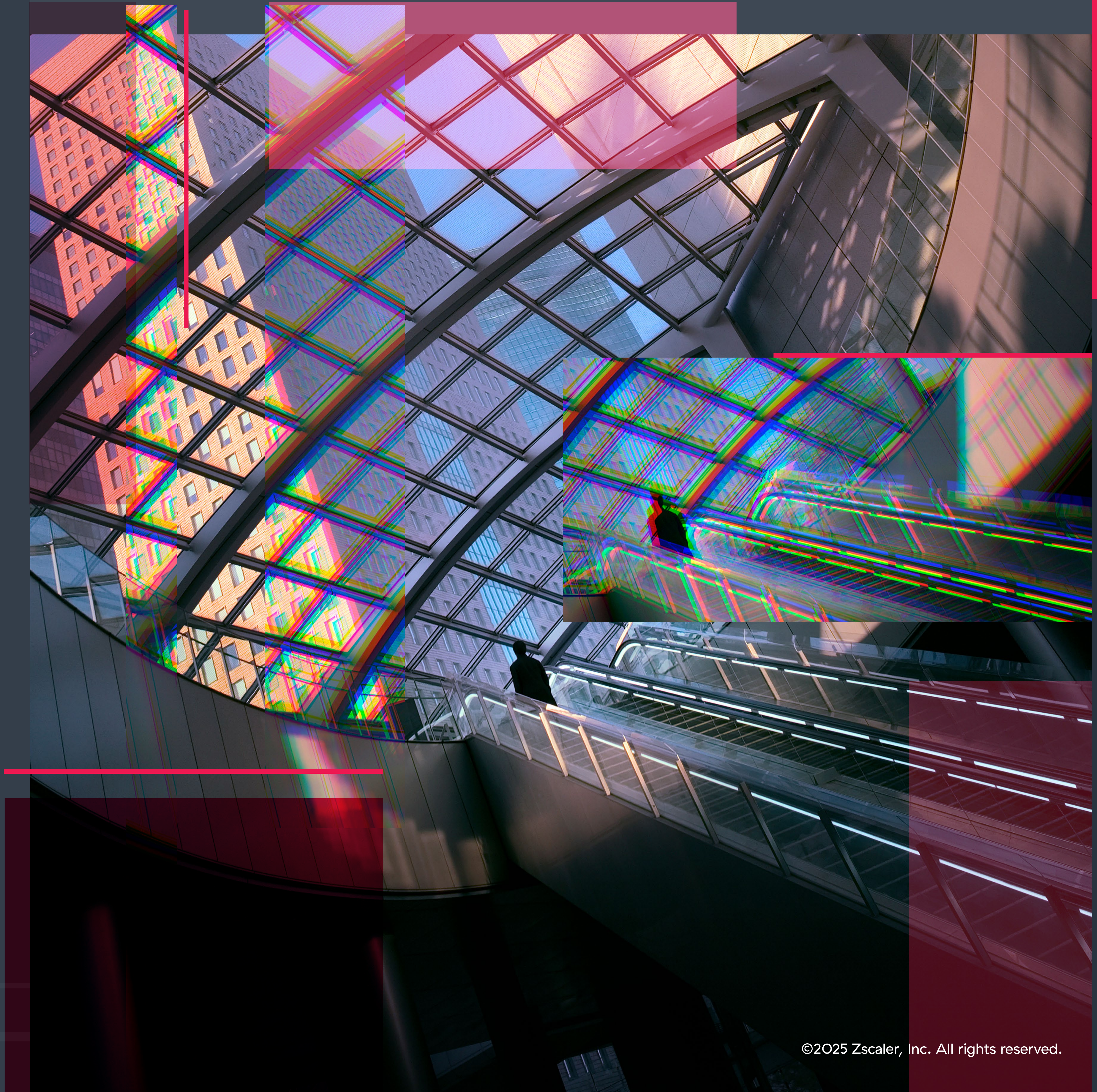
The growing number of VPN exploits in recent years will accelerate in 2025. VPN technologies are a prime target for attackers because they expose enterprises to the internet, making vulnerabilities easy to scan and exploit. As organizations struggle to patch VPN flaws in time, attackers will continue to discover and weaponize new high-severity vulnerabilities, as seen in the January 2025 Ivanti Pulse Secure breach. Security researchers and cybercriminals alike are actively probing VPN infrastructures, making ongoing disclosures of critical CVEs inevitable.

## Ransomware Groups Will Intensify VPN Exploits

As 92% of survey respondents express concern about unpatched VPN vulnerabilities, ransomware actors will continue to exploit known and zero-day VPN flaws as a primary method of initial access. Ransomware-as-a-service (RaaS) groups frequently scan for exposed VPNs with unpatched vulnerabilities, allowing them to deploy ransomware before IT teams can respond. The January 2025 ransomware campaign targeting US healthcare organizations demonstrates how VPN security gaps offer attackers direct access to sensitive systems. As these attacks become more automated, the need to transition to zero trust security will grow even more urgent.

## Lateral Movement via VPNs Will Drive More Destructive Attacks

Attackers exploit the broad access VPNs provide to move laterally, escalate privileges, and exfiltrate data—among the most effective techniques cybercriminals and nation-state actors use. With 71% of organizations concerned about this risk, network segmentation is often seen as a solution, but its complexity makes implementation difficult. Many organizations lack the skilled personnel to manage segmentation effectively, leading to projects that take months to complete or stall entirely. To mitigate these challenges, enterprises should adopt zero trust segmentation, which enforces strict least-privileged access to applications, eliminating lateral movement pathways without the operational burden of traditional network segmentation.



## Third-Party VPN Access Will Remain a Key Threat Vector

As 93% of respondents express concern over third-party VPN vulnerabilities, attackers will continue targeting weak external access points. Stolen third-party credentials and misconfigured VPN access remain among cybercriminals' top entry points. The 2024 Enterprise Financial Group (EFG) breach demonstrated how attackers exploit third-party VPN connections to infiltrate corporate environments. Many organizations lack visibility into third-party access permissions, making it difficult to enforce security policies. To mitigate these risks, organizations must transition to a zero trust framework, enforcing strict least-privileged access and continuous verification for all external connections.

## AI-Driven VPN Exploits Will Increase

The rise of AI-driven cyberattacks will impact VPN security in unprecedented ways. Attackers will increasingly leverage AI for automated reconnaissance, intelligent password spraying, and rapid exploit development, allowing them to compromise VPN credentials at scale. AI-powered evasion techniques will make it even more difficult to detect VPN-based intrusions before significant damage occurs. Meanwhile, AI-powered VPN security solutions may introduce unforeseen security gaps, leading to new attack vectors that cybercriminals will exploit. As AI-driven threats grow, organizations must adopt proactive security measures such as continuous identity verification and zero trust access controls.

## Major VPN-Related Breaches Will Make Headlines

Following multiple high-profile breaches in 2024, organizations will face greater pressure to disclose VPN-related cyber incidents. With new SEC regulations mandating transparency on cybersecurity risks, organizations suffering VPN exploits will face increased regulatory scrutiny, reputational damage, and potential financial penalties. As VPNs continue to serve as a primary entry point for attacks, organizations will be forced to reevaluate legacy access models, accelerating the move toward zero trust security.

## Zero Trust Investments Will Surge as VPNs Decline

With 65% of organizations already replacing or planning to replace their VPNs within a year, investment in zero trust security is accelerating, fundamentally reshaping the remote access landscape. Regulatory requirements and cyber insurance mandates are pushing organizations to move beyond VPNs as legacy solutions fail to meet security, scalability, and compliance demands. Zero trust adoption not only reduces cyber risk, but also eliminates the high costs of maintaining VPN concentrators, network appliances, and continuous patching cycles. As a result, VPNs are increasingly viewed as obsolete, prompting an industry-wide shift toward zero trust security models.

**These predictions highlight a growing consensus: organizations that delay zero trust adoption will remain highly vulnerable as VPN exploits increase. The future of secure access depends on proactive risk mitigation, not reactive patching—making now the time to move beyond VPNs.**

# Best Practices for Secure_Access

## Reduce VPN Risks and Strengthen Zero Trust Security

1. **Remove network-based access to minimize the attack surface**
   Prevent attackers from exploiting exposed network entry points by phasing out VPNs and network-based access in favor of direct, application-specific connectivity. Survey data shows that 54% of organizations cite security risks as their top VPN challenge, reinforcing the need to remove VPN dependencies and firewall-based security models that expose enterprises to attack.

2. **Stop initial compromise with inline threat prevention**
   Inspect all encrypted and unencrypted traffic inline to block zero-day exploits, malware, and ransomware payloads before they reach users. As 92% of organizations worry about ransomware targeting VPN vulnerabilities, real-time traffic inspection and policy-based blocking are essential. A cloud native security model eliminates the need for on-premises firewalls and reduces the attack surface.

3. **Strengthen authentication and identity security**
   Implement phishing-resistant multifactor authentication (MFA), such as FIDO2 credentials, biometrics, or hardware tokens to verify user access. Avoid legacy authentication methods like SMS-based MFA and push notifications, which attackers frequently bypass. Integrate identity-driven security with continuous verification instead of relying on one-and-done authentication.

4. **Enforce least-privileged, context-based access with ZTNA**
   Replace broad VPN access with zero trust network access (ZTNA) to ensure users only connect to authorized applications—never the network itself. Granular, just-in-time (JIT) access controls based on identity, device posture, and real-time risk analysis ensure users can only access what they need, when they need it.

5. **Eliminate lateral movement with zero trust segmentation**
   Connect users directly to applications, not the network, to prevent attackers from moving across systems if they gain initial access. Zero trust segmentation and identity-aware microsegmentation ensure that even if a user is compromised, an attacker cannot pivot to other resources or escalate privileges. ZTNA eliminates VPN tunnels, which are a major enabler of lateral movement.

6. **Secure third-party and external access with identity-based controls**
   Enforce least-privileged access for third parties, vendors, and contractors, applying strict session controls, device health checks, and continuous monitoring. Replacing VPN-based third-party access with ZTNA significantly reduces risk exposure from compromised vendor credentials—a welcome change for the 93% of organizations concerned about third-party VPN risks.

7. **Enhance data protection with integrated zero trust policies**
   Deploy inline data loss prevention (DLP) and cloud access security broker (CASB) controls to inspect, encrypt, and prevent unauthorized data movement in real time. A zero trust security framework ensures that all user traffic is inspected and controlled, even in SaaS applications and cloud environments.

8. **Deploy AI-driven security and continuous monitoring**
   Use real-time AI-powered analytics, deception technology, and automated behavioral detection to stop threats before they escalate. ZTNA solutions provide real-time risk scoring, preventing compromised accounts from accessing sensitive applications. Daily proactive threat hunting and risk-based access controls significantly reduce breach impact.

9. **Continuously assess and adapt security posture**
   Conduct automated risk assessments, penetration testing, and adversary simulations to dynamically adjust zero trust security policies. Security misconfigurations and lack of enforcement are key contributors to major breaches, making automated, policy-driven enforcement critical for reducing human error.

10. **Eliminate VPN infrastructure and automate security policy enforcement**
    Remove the need for VPN concentrators, firewall rule management, and manual access control lists by adopting a cloud-delivered zero trust model. ZTNA enables dynamic security policies that adapt in real time to compliance changes, regulatory updates, and evolving cyberthreats——without manual configuration or hardware dependencies.

By implementing these best practices, organizations can eliminate the security risks of VPNs with a resilient zero trust security framework, ensuring continuous verification, least-privileged access, and proactive threat mitigation.

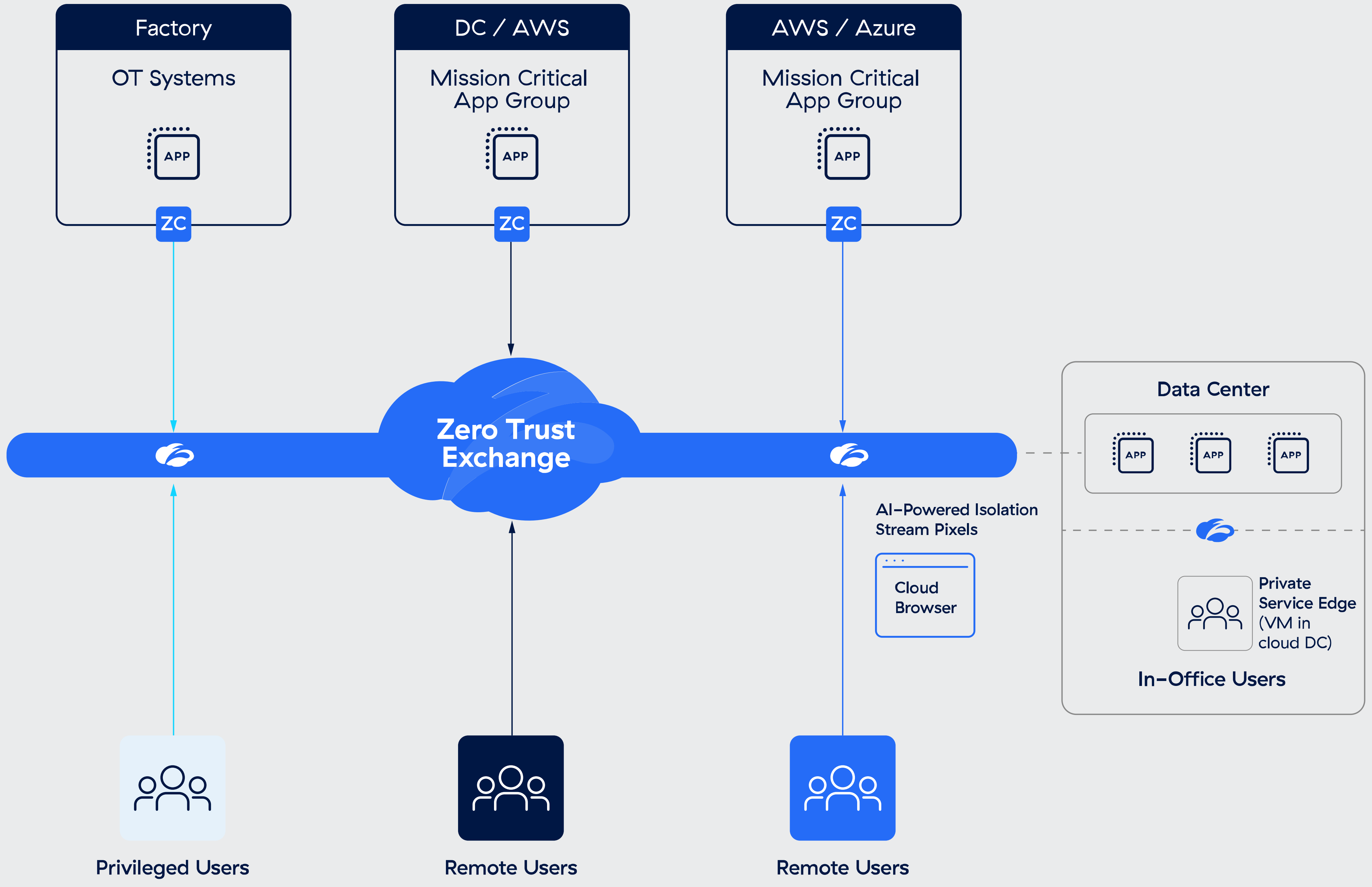
# How Zscaler Transforms Secure_Access

Traditional VPNs and firewalls significantly expand an organization's attack surface by placing users directly on the network. This broad access makes it easier for attackers to exploit vulnerabilities, gain entry, and move laterally within the environment. As threats continue to evolve and hybrid work becomes the norm, relying on these outdated technologies poses critical security risks that demand more secure, adaptive solutions.

**Zscaler Private Access™ (ZPA)** provides a secure, scalable alternative to legacy remote access solutions like VPNs. As a cloud native solution, ZPA enables zero trust access for all users by offering direct connectivity to private applications. To minimize the attack surface, applications are shielded behind the Zscaler Zero Trust Exchange™ platform. This approach eliminates lateral movement through AI-powered user-to-application segmentation and defends against sophisticated threats with integrated traffic inspection, as well as application and data protection.

ZPA can be deployed in a matter of hours to replace legacy VPNs and remote access tools with a holistic zero trust platform. Powered by the world's largest security cloud, ZPA delivers fast, reliable, and low-latency connectivity to users anywhere in the world. Its cloud native architecture ensures elastic scalability, seamlessly supporting the needs of distributed and hybrid workforces across various geographies.

With ZPA, enterprises can embrace cloud-first, hybrid workforce models with confidence, knowing their resources are protected, their users are productive, and their IT operations are future-proofed.



# Key Benefits of Zscaler Private Access (ZPA)

## Minimize the attack surface to protect against ransomware attacks

VPN vulnerabilities expose organizations to malicious users, leading to ransomware attacks and credential theft. ZPA eliminates this risk by hiding all applications behind the Zero Trust Exchange and granting users direct, zero trust access only to authorized applications. By preventing unauthorized users, including third-party vendors and contractors, from discovering applications and moving laterally, ZPA effectively protects against ransomware attacks. It enables secure remote access for all applications, including private apps, network-connected applications like VoIP, and server-to-client apps. Additionally, ZPA minimizes the impact of disruption through a comprehensive business continuity solution and helps organizations meet strict compliance requirements.

## Eliminate lateral threat movement

ZPA enforces least-privileged access by connecting users directly to specific applications, preventing access to other applications in the network. It provides visual insights into user-to-application access and policies applied, enhancing visibility and control. ZPA AI-Powered Segmentation automatically generates recommendations for app segments and policies, simplifying segmentation implementation while ensuring scalability and robust security.

## Gain granular visibility and analytics

ZPA provides detailed, real-time visibility into application usage, user behavior, and access patterns. IT teams can use this data to monitor, audit, and quickly identify potential threats, enhancing overall security posture. This can also help in ensuring regulatory compliance.

## Deliver clientless access to mitigate third-party vulnerabilities

ZPA Clientless Access simplifies third-party access by allowing contractors and partners to securely connect to applications via any browser without requiring a client. It isolates unmanaged devices from the corporate network, protects sensitive data, and integrates with Google Chrome Enterprise Browser for enhanced BYOD security. This modern approach reduces costs, minimizes risks associated with third-party access, and eliminates reliance on legacy VDI management.

## Prevent private app compromise

ZPA minimizes the risk of private app compromise and data loss by performing full inline inspection of end-to-end private app traffic. Robust data loss prevention capabilities ensure sensitive information remains secure while blocking unauthorized access. By hiding applications from the public internet and enabling secure user-to-app connections based on zero trust principles, ZPA reduces the attack surface, prevents lateral movement, and protects against breaches, enhancing overall security.

## Simplify policy management and speed up deployment

ZPA streamlines IT operations by simplifying remote access deployment, policy management, and user-to-app segmentation. Previously time-consuming tasks—such as user onboarding, patching, and upgrades—can now be completed in minutes, significantly reducing IT effort. With centralized management and automated policy recommendations, ZPA enables IT teams to improve efficiency, minimize complexity, and focus on strategic initiatives rather than day-to-day operations.

## Enforce device posture-driven access control

ZPA integrates with endpoint posture assessment tools to verify the security posture of user devices before granting access. This ensures that only compliant devices can connect, mitigating risks from unmanaged or compromised devices.

## Deliver superior user experiences

ZPA ensures optimal user experiences by providing fast, seamless, and secure connectivity to business-critical applications. Unlike VPNs that backhaul traffic through a centralized data center, ZPA enables direct user-to-application connections via the Zero Trust Exchange. This drastically reduces latency and improves application performance, whether users are on-site, remote, or on the go. By minimizing multiple logins and dependency on client-based software, ZPA simplifies access and boosts productivity. Additionally, ZPA's proactive monitoring capabilities streamline issue resolution, ensuring uninterrupted, high-quality access for all users.

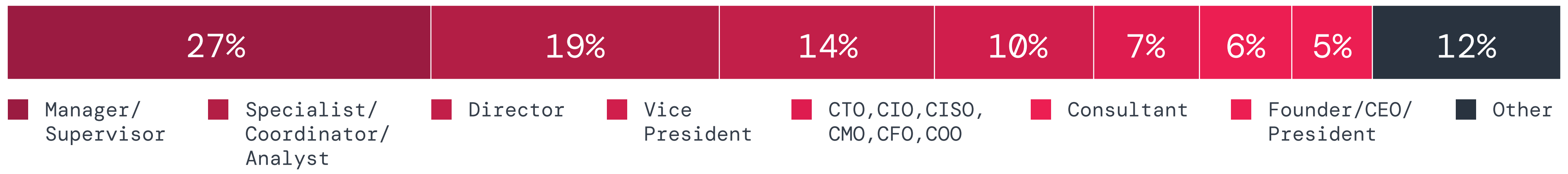
## Reduce total cost of ownership

ZPA significantly reduces total cost of ownership by eliminating the need for multiple point products such as VPNs, firewalls, NACs, and VPN concentrators. Built on a cloud native zero trust architecture, ZPA removes infrastructure costs related to hardware support, maintenance, repairs, and updates. Its simplified management and automated policy enforcement reduce operational overhead, allowing IT teams to save time and resources while improving security and scalability.

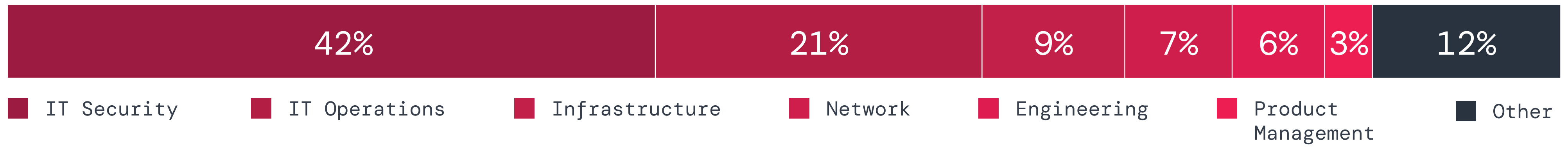
# Methodology_and Demographics

This report is based on a comprehensive survey of 632 IT and cybersecurity professionals conducted in early 2025, examining VPN security risks, enterprise access trends, and the adoption of zero trust architectures. Respondents included executives, IT security practitioners, and network infrastructure leaders across various industries. The findings in this report provide a data-driven perspective on the decline of VPNs and the shift to zero trust, offering critical insights for organizations modernizing their access security strategies.

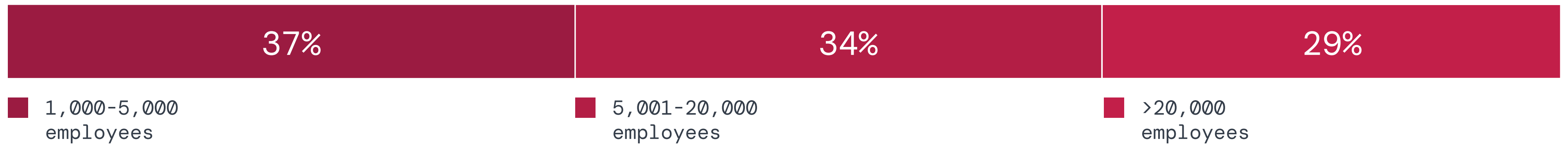
Career Level



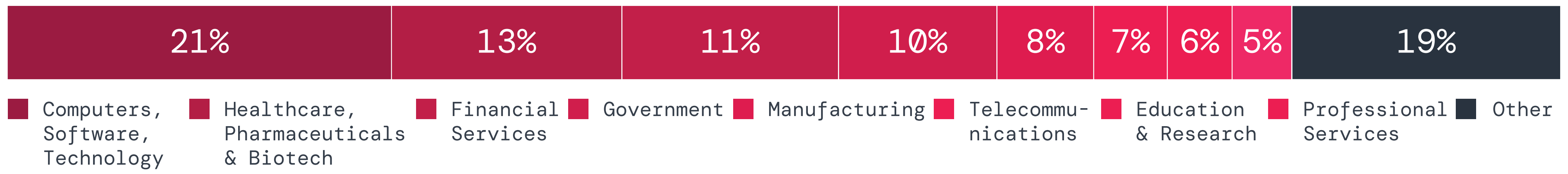
Department



Company Size



Industry



# About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. To learn more, visit **www.zscaler.com.**

# About ThreatLabz

ThreatLabz is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabz regularly publishes in-depth analyses of new and emerging threats on its portal, **research.zscaler.com**.

# About Cybersecurity Insiders

**CYBERSECURITY INSIDERS – YOUR TRUSTED SOURCE FOR DATA-DRIVEN CYBERSECURITY INSIGHTS**

Cybersecurity Insiders delivers evidence-backed insights and third-party validation, empowering cybersecurity leaders to make informed, strategic decisions. Built on more than a decade of research with a global network of over 600,000 cybersecurity professionals, we deliver actionable intelligence that helps leaders navigate evolving threats, evaluate new technologies, and shape forward-looking strategies with confidence.

For cybersecurity vendors, we turn research insights into results — building credibility, visibility, and trust through high-impact formats such as data-powered market reports and webinars that establish thought leadership, CISO guides that showcase best practices, product reviews that validate solutions, how-to articles that educate buyers, and award recognition that elevates 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.

Learn more: cybersecurity-insiders.com

**Holger Schulze**
CEO & Founder
Cybersecurity Insiders

zscaler™ | Zero Trust Everywhere

**About Zscaler**

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

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