tailscale

The State of Zero Trust 2025

07.2025 //zero trust is dead. long live zero trust.

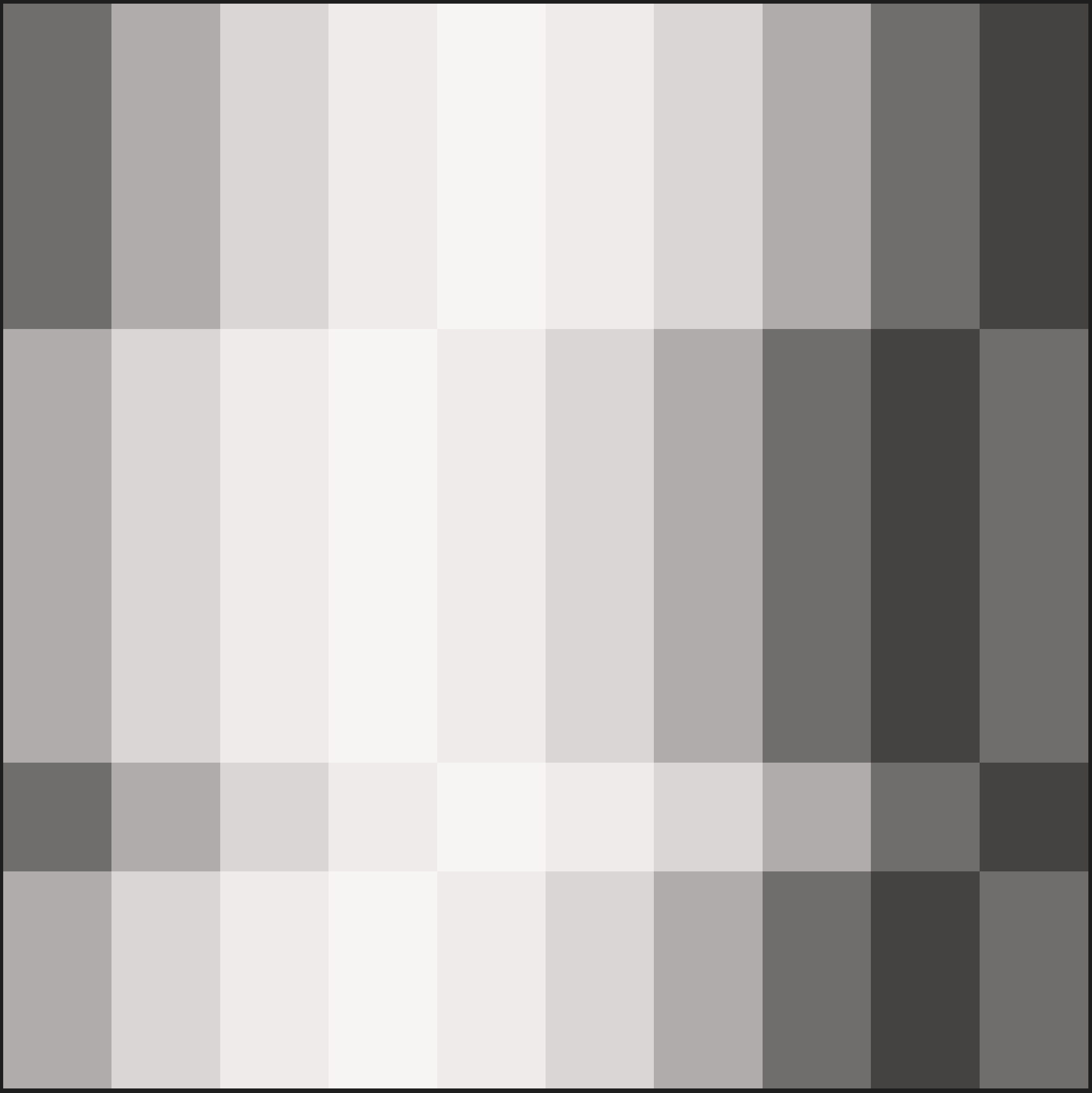


Table of Contents

00// Introduction 3

01// Data transparency 4

02// Executive summary 5

03// The push toward identity-native access 8

04// Legacy VPNs 11

05// Productivity vs. security 14

06// Security trends and the road ahead 17

07// What’s next 20

08// Recommendations 22

00//

Introduction

from Avery Pennarun, CEO of Tailscale

It’s 2025, and the perimeter is dead.

If your mental model of a secure network still involves “inside” and “outside,” it’s time for an update. Most companies know this — at least, they say they do. Our latest survey suggests Zero Trust has become the new checkbox buzzword. Unfortunately, saying “Zero Trust” and actually doing it are two very different things.

These are my three takeaways from the data:

1 `_everyone's frustrated`

IT teams are overwhelmed by tool sprawl and manual processes. Security leaders are stuck enforcing policies users constantly work around. Engineers just want to get things done — and they say current access setups are too slow, too fragile, and too painful. Different problems, same conclusion: the legacy model isn’t working.

2 `_zero trust is half-deployed at best`

Nearly every organization says they’re “on a Zero Trust journey,” which is a polite way of saying they aren’t done, and maybe never will be. Fewer than a third have implemented the foundational parts — strong identity, least privilege, and verifying before trusting. It’s a journey, sure — but one where most teams don’t have a map, the GPS is glitchy, and someone in the back is asking if we’re there yet.

3 `_there's some light at the end of the tunnel`

There’s real interest in emerging approaches: identity-first networking, modular security systems, and policy engines that adapt (instead of break) when things change. And with AI accelerating both innovation and risk, there’s new urgency to get access right — not just for users, but for services, agents, and infrastructure itself.

This report isn’t about adding more buzzwords — it’s about creating a clear baseline of where the industry really stands on Zero Trust today. We hope it helps surface the biggest gaps, highlight emerging practices that are actually working, and offer practical direction for where secure access goes next.

01//

Data transparency

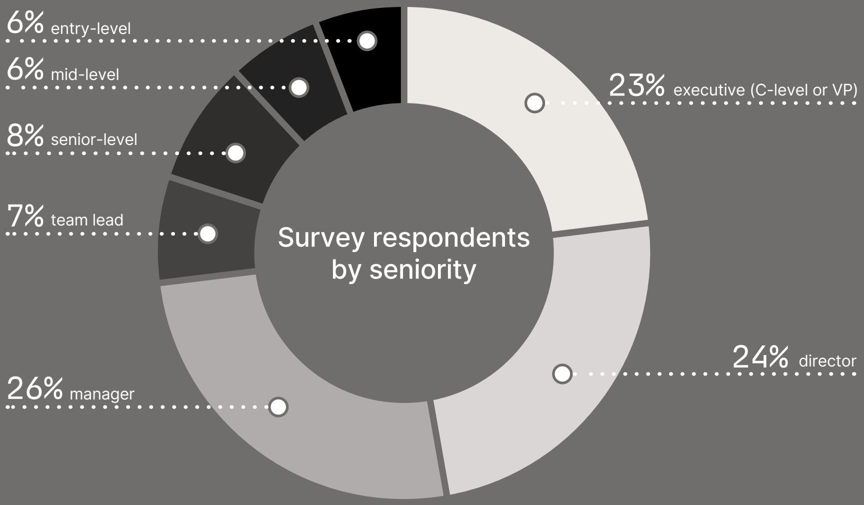
All statistics and insights in this report are based on Tailscale's 2025 Secure Access and Zero Trust Adoption Survey, conducted with 1,000 IT, security, and engineering professionals. In this report, we've referenced the specific question IDs tied to each data point. If you'd like to review the full methodology or explore the raw survey data, please reach out to our communications team at **press@tailscale.com** — we'd be happy to share more.

This report was created with a focus on objectivity and clarity, using verified survey data and rigorous analysis to surface the most pressing challenges in secure access and Zero Trust adoption today. Every effort was made to approach the data impartially and transparently.

That said, Tailscale is not a neutral observer. We see these challenges every day — and we've built our platform to address many of them. If you're interested in learning how Tailscale can help solve the secure access issues outlined in this report, **visit us at tailscale.com**, or **reach out to our sales team for a demo**.

Methodology

Tailscale conducted this study in partnership with **Kelsey White** and **PureSpectrum**. The online survey was completed by n=1,000 engineering, security, development, and IT professionals across the United States and Canada, representing a range of industries. Management-level employees comprised about two-thirds of the sample, including twenty-three percent from the C-suite. Nearly half of the respondents work at enterprise firms. Data was collected from April 21 to 28, 2025.



02//

Executive summary

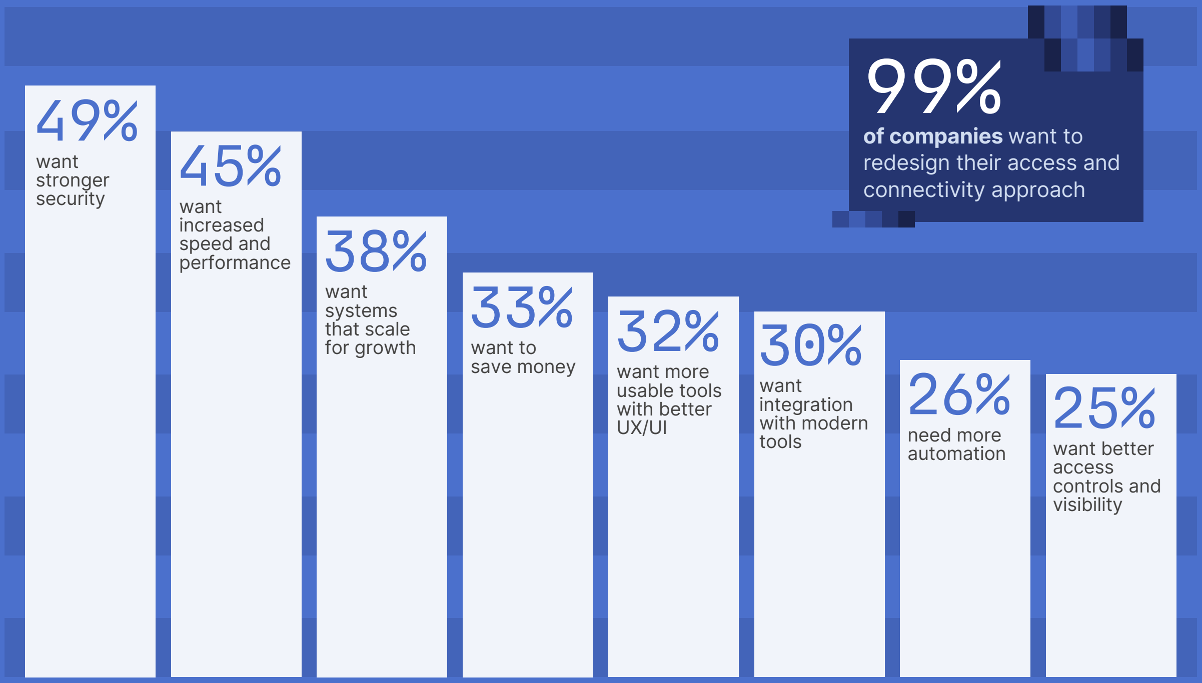
Zero Trust in theory, not in practice

In 2025, organizations are under pressure to secure increasingly distributed, hybrid, and cloud-native environments — but the tools they rely on are frustrating and outdated (especially VPNs). Most teams know their current network access model is broken. It's slow, fragile, and full of friction, but adoption of identity-first principles is accepted in theory and inconsistently executed in practice. With the threats and opportunities of AI looming, there is a never-more-urgent need to simplify and modernize secure infrastructure access.

What's in this report

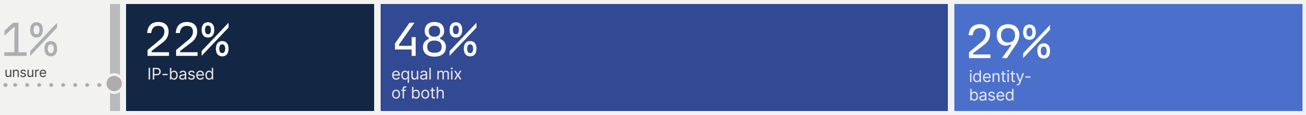
We surveyed 1,000 IT, security, and engineering leaders to understand the real state of Zero Trust. Inside, you'll find benchmarks on adoption, pain points with legacy systems, and emerging practices like identity-native access and just-in-time permissions — plus practical recommendations for what to do next.

Access and connectivity redesign priorities

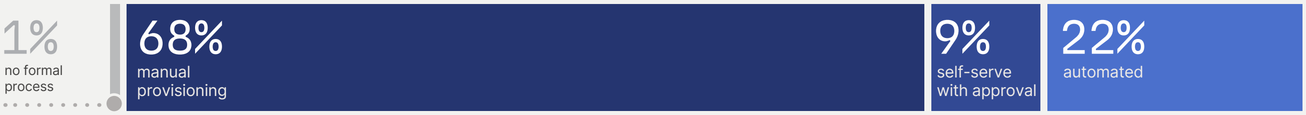


Only 1% report being satisfied with the status quo.

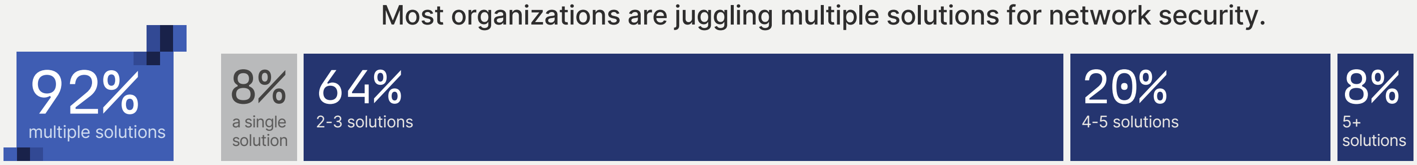
Fewer than a third of organizations use identity-based access as their primary model. "Never trust, always verify" has become a baseline aspiration.



A majority of organizations still rely on manual processes for network access creating complexity, friction, and security gaps.

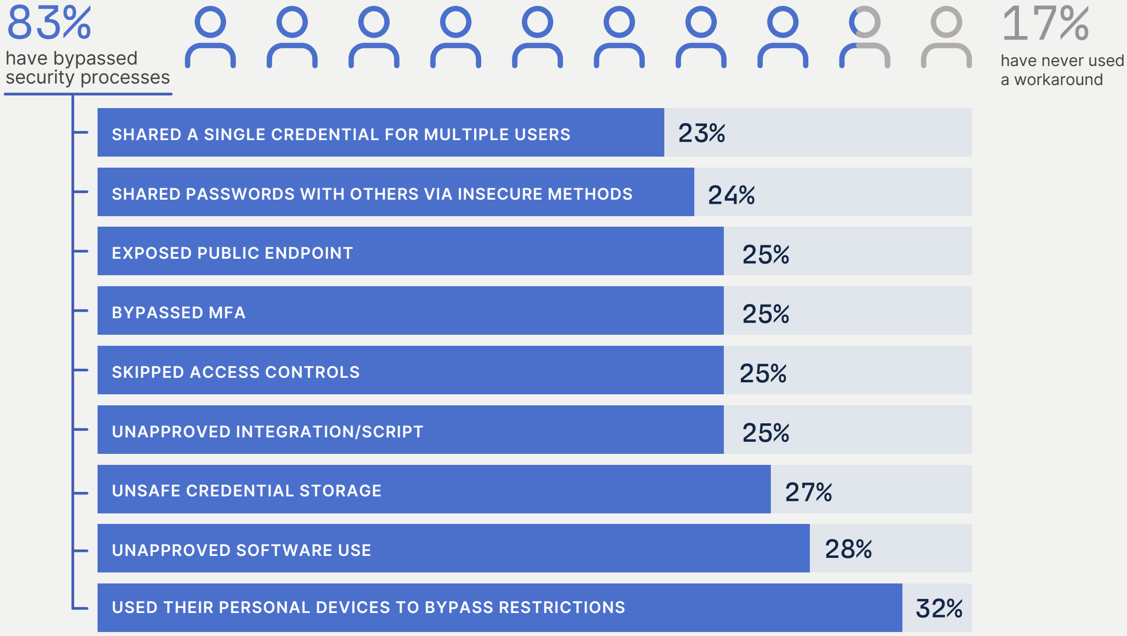


Most organizations are juggling multiple solutions for network security.



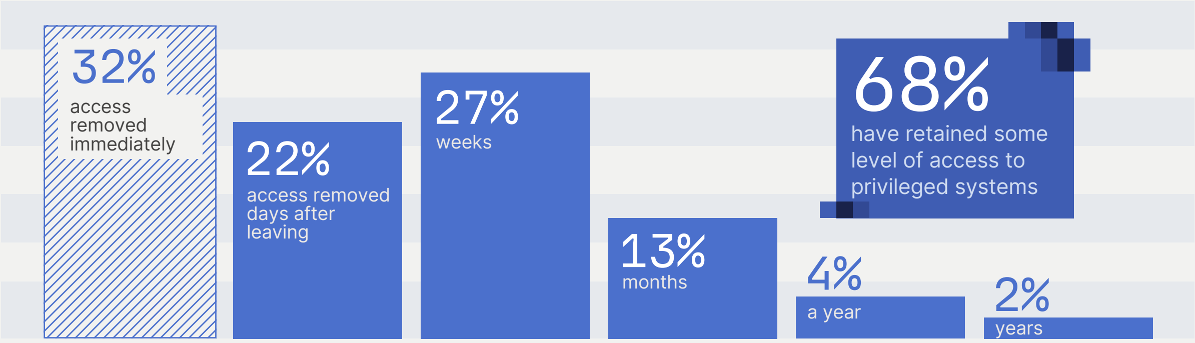
Only 8% rely on a single, unified platform, contributing to fragmentation and inefficiency.

These challenges have real impacts leading to dangerous workarounds.

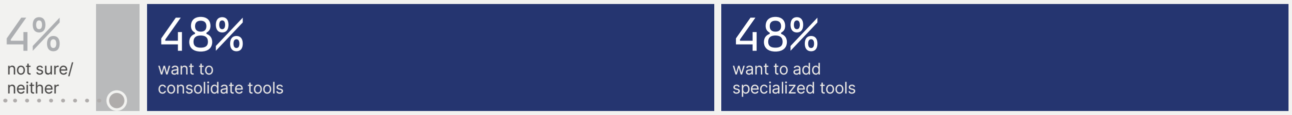


Engineers are frustrated by slow and complex security setups. 83% of overall survey respondents and 87% of developers admit to circumventing security measures just to stay productive.

Inadequate identity lifecycle management practices result in serious vulnerabilities — 68% of respondents report retaining access to former employers' systems after leaving.



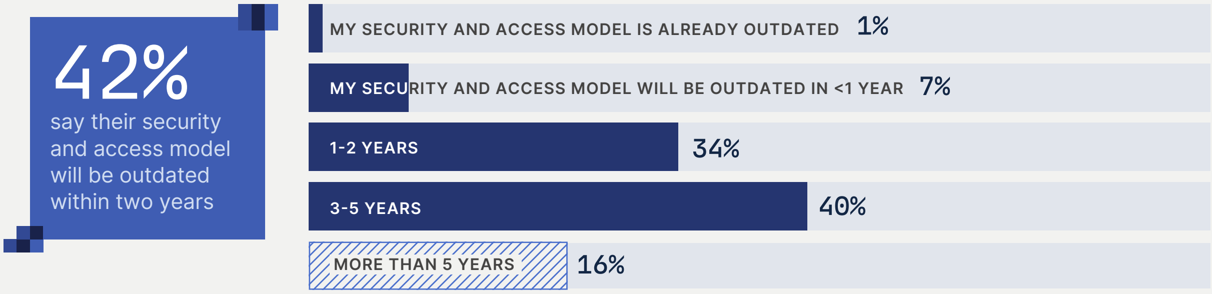
Organizations are increasingly recognizing these risks and complexities. Almost half are actively consolidating.



Industry experts point toward a clear shift to identity-first, Zero Trust solutions. Within the next two years, there is anticipation for significant industry momentum toward unified, cloud-native secure access platforms. This is sometimes referred to as "universal Zero Trust Network Access" (universal ZTNA).

The data paints an industry in transition.

Traditional security and access models are reaching breaking points under new demands.



We hope you use this report to recalibrate your Zero Trust strategy around what's actually working in the field. If identity isn't at the center of your access model, you're standing on quicksand. Security is only as strong as what users don't bypass. It's time to rebuild from first principles. Zero Trust isn't a checkbox — it's a blueprint for scaling secure access across both humans and machines. While the bulk of this report unpacks why the current state looks the way it does, if you'd prefer to jump straight to our recommendations or are short on time, you'll find actionable guidance in Section 8 on pages 22 through 23.

03//

The push toward Identity-native access

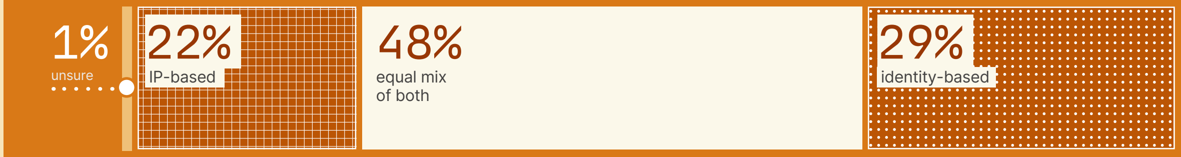
(and why it's hard)

tldr;

Identity-native access is the goal — but most companies are still in transition.

Executive alignment, legacy systems, and fear of disruption slow progress, even as more orgs adopt tools like ZTNA and mesh VPNs. Moving gradually, layering identity-based access controls on top of legacy infrastructure, and investing in solid identity foundations (SSO, MFA, device trust) is the most sustainable path forward.

Fewer than a third of organizations use identity-based access as their primary model



Identity-native is the goal — but most are still hybrid or IP-based

The concept of identity-native security — where access to systems is determined by user and device identity, not by network location — has become a pillar of Zero Trust strategies. Our research shows strong adoption of identity-based tools, nearly half use an IAM/SSO platform. Yet, true end-to-end implementation remains difficult.

Many organizations still operate in a hybrid mode. For example, they might authenticate users via SSO, but then restrict resources by IP addresses or VPN segmentation, effectively layering identity on top of a network-centric foundation. This is reflected in the 29% identity-based vs 21% IP-based split in primary access policy – with the majority (48%) saying it's a mix of both.

Executive understanding (or lack thereof) is a barrier

A lack of understanding at the executive level hinders Zero Trust initiatives. "Most C-levels I talk to don't really understand what Zero Trust is. It's not a specific tool or technology, but a mindset and strategy," "one industry representative noted in a recent social media conversation.

Many organizations were sold disparate "Zero Trust" products without a holistic plan, resulting in confusion and partial implementations. The term Zero Trust has been overused in vendor marketing, causing significant confusion and dilution of its core principles.

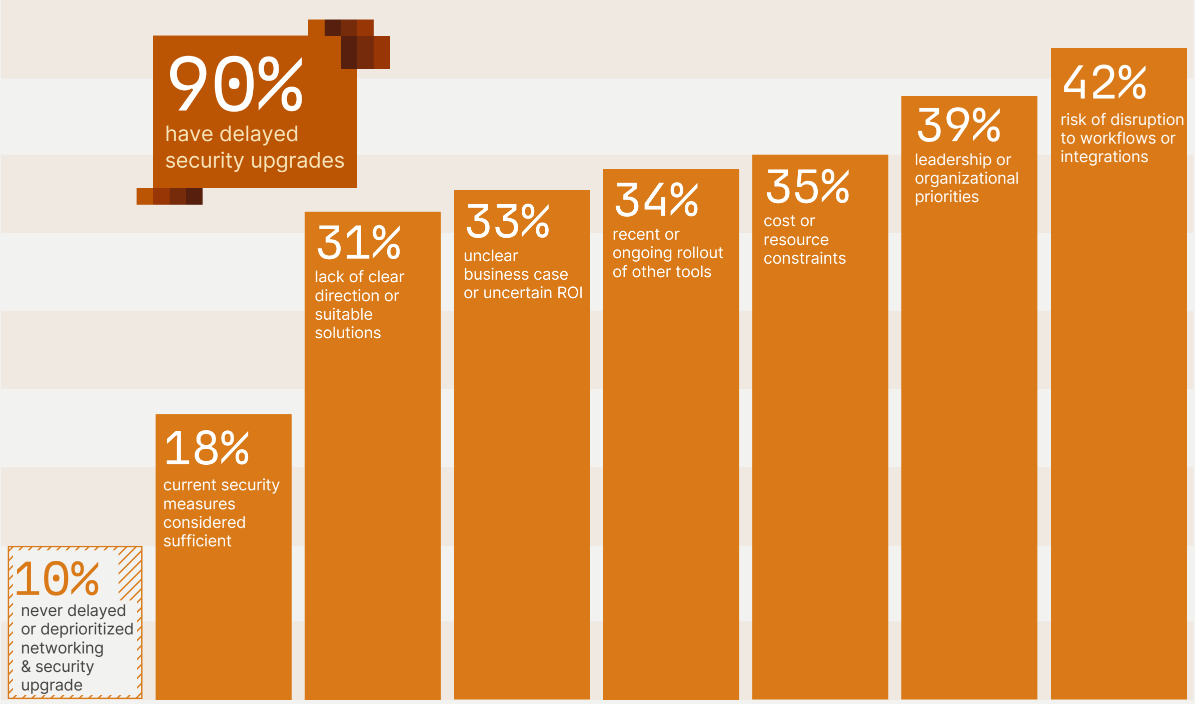
In short, companies know they should "never trust, always verify," but translating that into practice – beyond just buying another security tool – requires architectural changes and clarity of vision.

Legacy infrastructure is hard to replace

Legacy infrastructure and practices don't disappear overnight. Enterprises have years of investment in VPNs, firewalls, and internal networks built on implicit trust of those inside the perimeter. Shifting to an identity-based model often means rethinking application access, rewriting firewall rules to use user groups instead of IPs, and ensuring every system integrates with an identity provider.

It is telling that 42% of respondents said they have delayed security upgrades due to "risk of disruption to workflows or integrations" — the most common reason cited for delay. Even if IT knows a new Zero Trust approach is needed, they worry that ripping out the old access model could break things. 39% also cited conflicting leadership priorities as a reason for delay, which suggests that unless Zero Trust initiatives are championed from the top, they can get sidelined in favor of more immediately tangible projects.

Reasons for delaying or deprioritizing networking or security upgrades



Gradual migration is the only sustainable path

A big bang switch could disrupt the business. Organizations should gradually replace legacy methods, pursuing identity-first security in a way that augments. This is already happening to some extent: for example, 47% of companies have implemented at least some Just-In-Time access or time-limited permissions. These identity-centric approaches limit standing privileges and can be layered onto existing VPN setups to reduce risk. Some forward-looking organizations have started to sunset traditional VPNs entirely in favor of proxy-based ZTNA solutions that verify identity and device posture for each application session.

Adoption of mesh VPN and ZTNA is rising

In our survey, 27% are already using peer-to-peer mesh VPNs, like Tailscale, for identity-linked connectivity. 34% use cloud-delivered ZTNA platforms. This indicates a growing appetite for software-defined, identity-aware networking that is moving away from appliance-based concentrators.

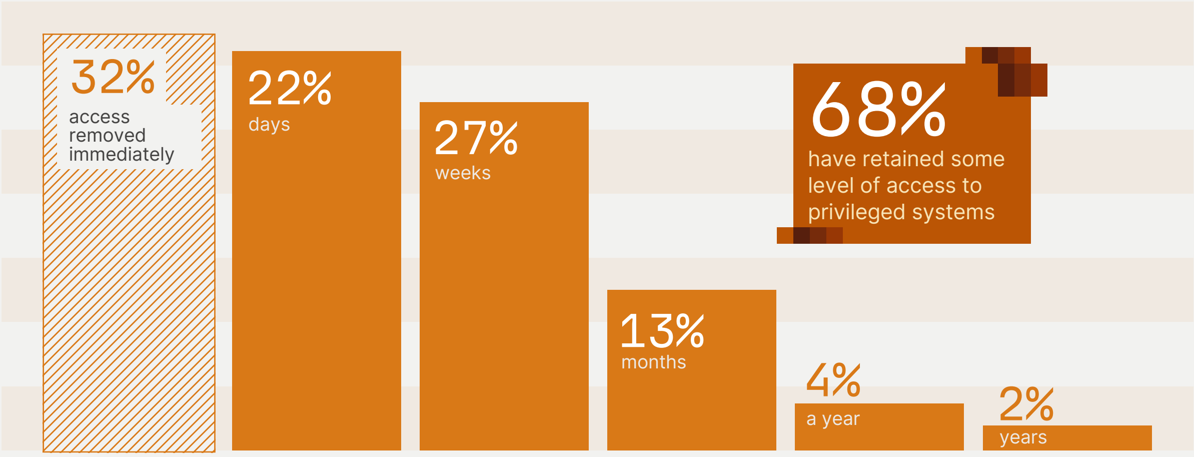
Treat identity as the new perimeter

One positive consequence of moving to identity-centric access is improved offboarding and auditing. The survey's alarming findings about lingering access for ex-employees (68% have retained access somewhere.) highlight that many companies don't have centralized visibility into who can access what. In an identity-first paradigm, ideally all access is mediated by a unified directory or identity provider, making it far easier to turn off one account and immediately revoke all associated permissions.

Companies with fully automated provisioning were far less likely to report long delays in onboarding or offboarding. Tightening identity lifecycle management not only closes security gaps, but also addresses compliance requirements.

The strategic imperative is to treat identity as the new perimeter: investing in solid identity infrastructure and re-engineering access policies to use those identities in a granular way, phasing out rules that assume a trusted network. Instead, adopt a model where ,even when on the office network, users have to authenticate and are only allowed to reach what their identity should reach. This consistency is key to Zero Trust.

How long access was retained to a previous employer's infrastructure



04//

Legacy VPNs

The weak link in modern infrastructure access

tldr;

VPNs are no longer fit for purpose.

They're slow, brittle, and overly permissive — and both IT and engineering teams are frustrated. The shift toward Zero Trust means moving away from network-based access and adopting identity-first, application-layer models that are more secure, scalable, and aligned with how teams work today.

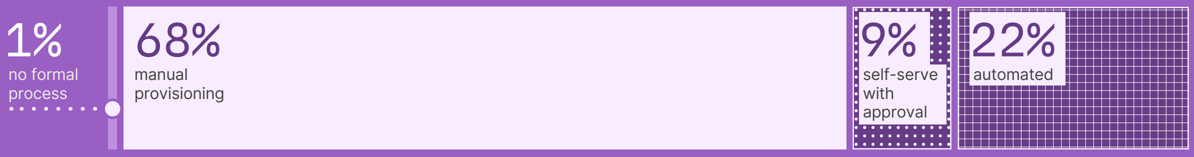
Virtual Private Networks (VPNs) have long been the standard for remote access, but in today's world of distributed teams, cloud workloads, and identity-driven security models, legacy VPNs are showing serious strain. Legacy VPNs extend the network perimeter rather than enforcing access based on user or device identity. This fundamental mismatch with Zero Trust principles has become a source of growing frustration.

Only 10% of survey respondents say their VPN has no major issues, and just 16% believe their current access model will still meet their needs five years from now.

Too much trust, and not enough control

Once a legacy VPN connection is established, it often grants broad, flat access to internal systems — far more than most users need. That's a legacy of network-centric design: once "inside," users are implicitly trusted. Modern Zero Trust models reject this.

A majority of organizations still rely on manual processes for network access



Access should be granted only after verifying who the user is, what device they're on, and whether they should reach a specific application, not based on IP address or VPN status.

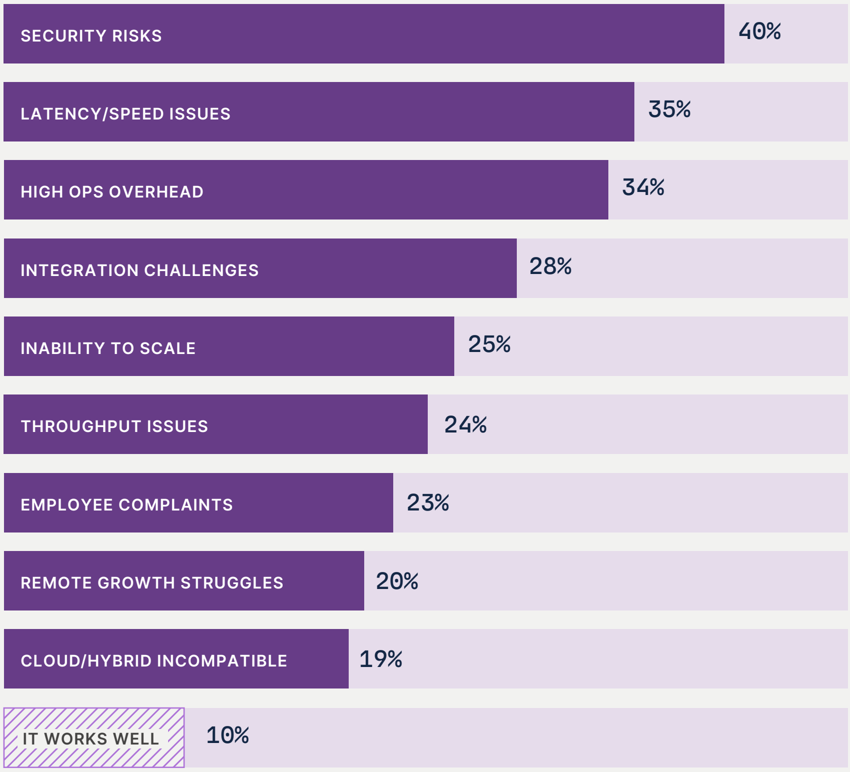
68% of companies still manage network ACLs manually, using static firewall rules and IP-based permissions. This creates operational drag and security risk. A shift to software-defined access can eliminate much of this complexity, using group-based policies that adjust dynamically based on identity.

Latency, overhead, and developer drag

Legacy VPN architectures are now untenable. 35% of respondents cite latency issues, and 24% report throughput limitations as key VPN frustrations.

Current VPN limitations

90% have one or more issues with their current VPN



Performance pain isn't limited to one role: 38% of developers and 33% of IT professionals flagged VPN speed as a problem. Developers may feel it more acutely because their workflows often involve large builds, test environments, or direct cloud resource interaction, but the complaints are widespread.

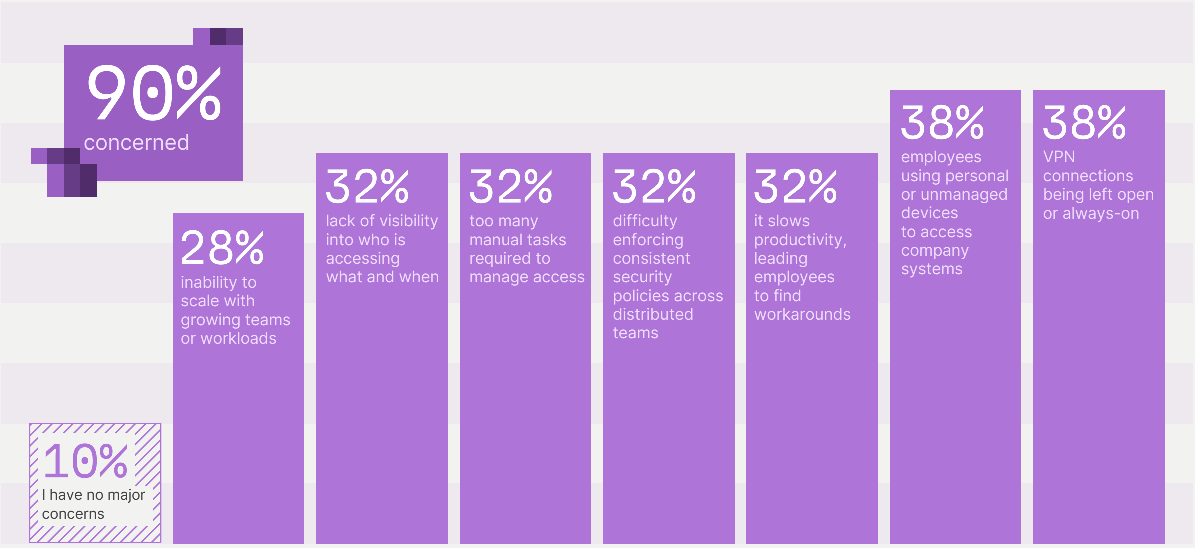
This isn't just an inconvenience. At companies that rely heavily on legacy VPNs, twice as many report they are slower than peers to launch new products than at companies using more modern access approaches. While correlation doesn't prove causation, it's a signal: teams that still rely on legacy VPNs may be slower to move.

Security shortcomings and untrusted devices

The survey's top-cited VPN limitation was security risk (40%). This can include the risk of a compromised VPN credential giving an attacker broad network access or VPN clients not enforcing device security hygiene. 38% of organizations worry about VPN connections being "always on." This can be a vector for malware to spread from a user's device into the corporate network.

With Zero Trust, the goal is to narrow each connection to the specific application/service and require re-authentication or continuous verification, reducing the blast radius of a stolen credential or compromised device. Furthermore, personal device use is rampant. 38% of respondents are concerned about unmanaged devices connecting, and legacy VPNs don't offer much help. Modern solutions can integrate key Zero Trust capabilities like device posture checks. This is especially helpful in environments managing IoT or edge workloads.

Remote network security concerns



Legacy VPNs need to be sunset

The industry implication is clear: Legacy VPNs are on the way out, especially for organizations that can't tolerate their downsides. We're seeing an acceleration in plans to retire legacy VPN products in favor of cloud-based secure access services. 34% of companies are now using cloud-delivered ZTNA platforms, and 27% have adopted mesh VPNs, like Tailscale, that use identity to control access rather than network location.

05//

Productivity vs security

The internal culture clash

tldr;

Security and productivity aren't opposites — they're co-dependent.

Rigid controls lead to workarounds. Poor UX undermines security. The future lies in building security into workflows and choosing flexible, identity-based platforms that support speed without compromising protection.

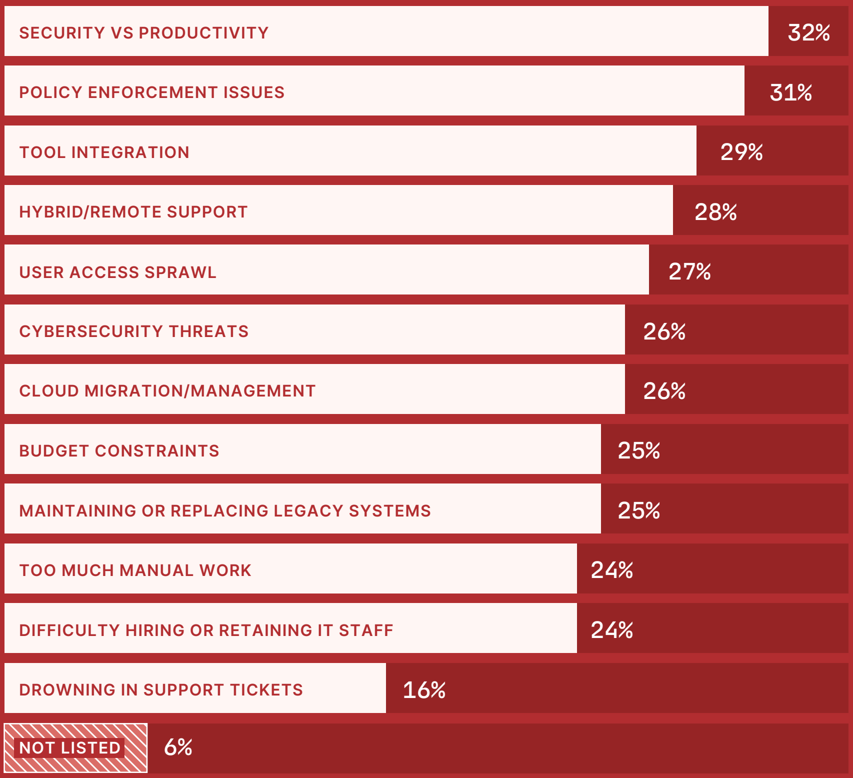
One of the clearest findings from this report is that IT, security, and engineering teams are aligned in frustration, but not always in approach.

32% of IT and security professionals say their top challenge is balancing security with speed and productivity, the most common pain point in the entire survey.

Right behind it? 31% cite enforcing IT rules and dealing with unauthorized tools. This captures the core tension: while IT teams are tasked with protecting systems, users are just trying to do their jobs — sometimes by working around those very protections. From the developer side, 22% say IT policies create friction or block workflows, and by their own admission, they frequently turn to shadow IT — spinning up personal cloud instances, using unapproved tools, or bypassing VPNs — not out of malice, but necessity.

This cultural disconnect doesn't just increase risk. It drains morale and creates friction between teams that should be aligned.

Biggest challenges IT & security teams are dealing with



Everyone wants the same thing

IT and developer respondents chose the same top two goals: stronger security and better performance.

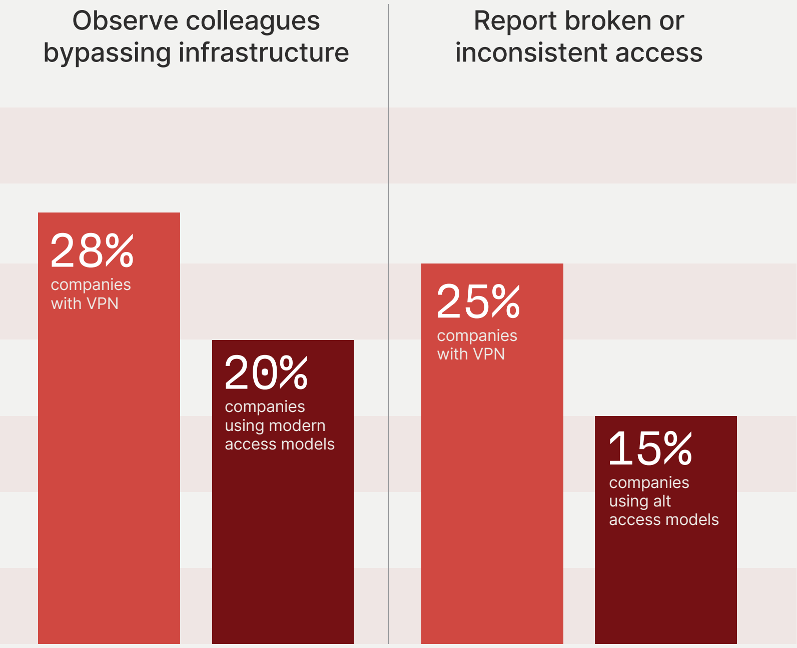
Still, 51% say their current remote access setup slows them down, and an equal 51% believe better security must come at the cost of performance. These responses suggest many teams have reluctantly accepted that friction is just part of staying secure.

UX is a security control

Here's a core insight: bad user experience is a security risk. If access policies are too complex or fragile, people will find ways around them. That might mean writing down complex passwords, reusing credentials, or worse — propping open insecure access paths.

The data backs this up. At companies using VPNs: 28% of employees observed colleagues bypassing infrastructure, and 25% of employees reported broken or inconsistent access.

While VPNs can exacerbate friction, even when companies use alternative access models, the tension between performance and security persists.



As one industry expert recently put it succinctly: “If it's not usable by employees, it won't get used.”

Secure productivity is possible

Modern security tools can enable, not block, safe productivity. For example:

33%
of companies already use Just-In-Time (JIT) access or time-based privileges

26%
of companies want more automation to reduce manual approvals and delays

These are strong signs of a shift toward platforms that offer secure defaults, allow developer self-service, and minimize the need for constant IT intervention. Security leaders are increasingly partnering with engineering to understand workflows and build guardrails. This collaborative model ensures that teams can move fast without creating security debt.

This sprawl creates headaches for IT and Security

When official processes are too rigid, users go around them. That's why:

31%
of IT leaders say managing unauthorized tools is a top challenge

30%
of employees are frustrated by using different access methods across systems

24%
of employees say their company's SaaS controls are easy to bypass

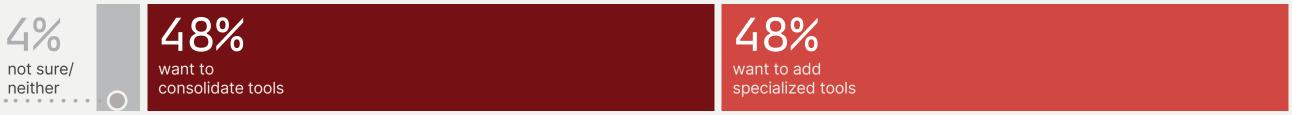
This sprawl creates headaches for IT — who must integrate, monitor, and secure too many disjointed systems. 29% of respondents cite integrating new tools as a major issue. More than two-thirds of survey respondents (68%) hear or have complaints about network access on a weekly or monthly basis.

The case for unification (but not lock-in)

The solution isn't one vendor to rule them all — it's a platform approach with centralized policies and visibility, even if enforcement happens in different places. When identity is consistent across systems, users get:

- One login
- One set of permissions
- A predictable, secure experience

Organizations are increasingly recognizing these risks and complexities.
Almost half are actively consolidating.



48% of companies are actively trying to consolidate tools — but consolidation brings its own risks.

Some all-in-one vendors may later limit flexibility or increase costs. That's why composability matters: platforms should integrate well, avoid lock-in, and support swap-in/swap-out flexibility.

26% of respondents say a full IT stack refresh would trigger reconsideration of their access tools, suggesting many organizations are aligning access upgrades with broader digital transformation projects.

06//

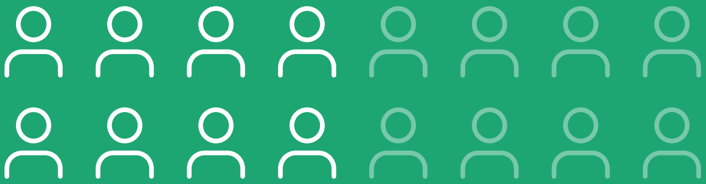
Security trends and the road ahead

The data doesn't just reflect the state of secure access today — it points to where we're headed. Beneath the frustration and fragmentation, there's a pattern emerging: a shared recognition that the old model is failing and a growing appetite for something better.

"Zero Trust" gets concrete, with focus on unified policy and visibility

In the next year, we predict enterprise organizations will measure Zero Trust maturity by how well they cover all the pillars (identity, devices, network, applications, data) in an integrated way. The end-state vision is an environment where a user on a corporate laptop in a café gets the same level of secure access (no more, no less) as they would sitting in HQ — because the access decision hinges on their identity, device posture, and context, not their physical network.

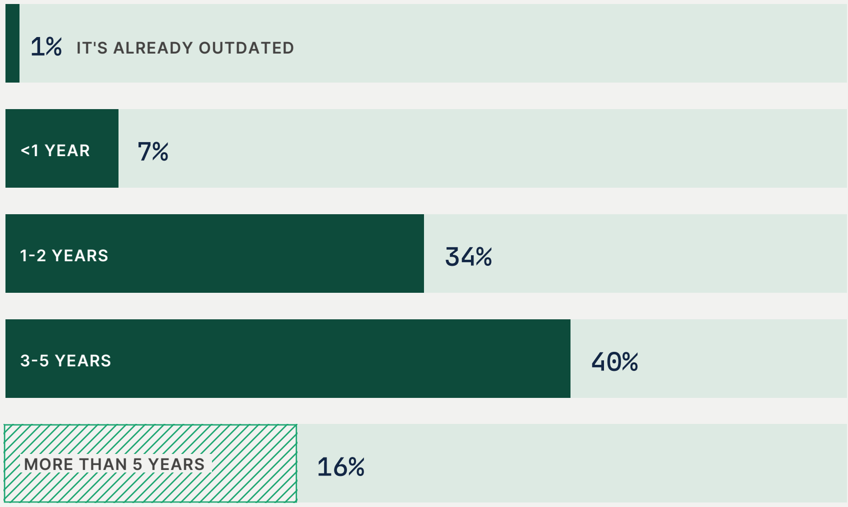
Our data shows 50% of respondents agree with the statement, "My company's security rules feel disconnected from how modern development actually works." Expect that percentage to drop as rules catch up to modern, cloud-native workflows.



50%

say their company's security rules feel disconnected from how modern development actually works

42%
outdated within two years


How long current setup will meet needs

The decline of legacy VPNs — and the shift toward identity-first access

Our data shows that 42% of organizations believe their current access infrastructure won't meet their needs beyond the next two years — a strong signal that change is already underway.

In their place, modern secure access platforms are emerging built on identity. These platforms vary in implementation, but share a common goal: give users secure, reliable access to the resources they need without exposing the entire network or back-hauling traffic through central gateways.

Some vendors call this Zero Trust, and others frame it as part of broader network transformation, but the core idea is the same: replace implicit trust with continuous verification and fine-grained controls.

As a result, we expect organizations who want to ensure both their security and productivity to remain competitive will retire or phase out their legacy VPNs by the end of 2026, making way for more flexible, composable solutions..

But this shift isn't without risks. Customers and partners we've spoken to are increasingly wary of vendor lock-in as they rethink their access architecture. Some consolidation makes sense — nearly half (48%) of organizations in our survey say they're actively trying to streamline and unify their security stack.

Automation, AI, and the shift to adaptive security

As infrastructure grows more complex and distributed, manual access management simply doesn't scale. Already, 24% of IT and security teams cite "too much manual work" as a top challenge.

One emerging answer is automation, powered increasingly by machine learning and AI-driven systems. These tools can monitor access behaviors in real time, detect anomalies, and respond adaptively. For example, if a user who typically accesses marketing dashboards suddenly attempts to reach a sensitive production database, the system might:

- Block the request
- Require step-up authentication (e.g., a second factor)
- Or flag it for review while allowing conditional access

This marks a shift away from binary, rule-based (yes or no) access toward risk-aware, context-sensitive decisions — sometimes called Continuous Adaptive Trust or risk-based authentication.

Importantly, this doesn't just serve security teams. It can improve the user experience, too. Instead of indiscriminate MFA prompts on every login, users get fewer interruptions when their behavior matches expected patterns — while still being protected against unusual or high-risk activity.

Traditional VPNs or manual firewall rules weren't designed to secure access to $10k/hour GPU clusters or cloud AI pipelines that span multiple vendors. These environments demand:

- High-performance, low-latency connections
- Strict access controls to prevent resource abuse
- Real-time visibility into who is doing what and why

Security teams will need more granular, identity-aware access models to keep up — ones that can adapt dynamically without slowing down training cycles or model deployment.

Despite these benefits, adoption still lags. In our data, 55% of respondents expressed skepticism or said they didn't know where to look for better solutions. That knowledge gap is one of the biggest barriers to progress. Education around adaptive access, AI-enhanced threat detection, and modern Zero Trust architectures will be critical over the next two years.

It's also important to acknowledge the other side of the AI equation: threat actors are using AI, too. From hyper-personalized phishing to faster, more effective social engineering, AI is already increasing both the speed and sophistication of attacks. As the threat landscape evolves, defenders must evolve even faster — or risk being outpaced by automated adversaries.

These pressures are amplified in environments like manufacturing, logistics, and physical operations, where edge devices may have limited connectivity or can't tolerate latency introduced by centralized access architectures.

07//

What’s next

Tailscale’s predictions for the future of secure access

Based on insights from this research and conversations with security teams, developers, and IT leaders, we see a clear direction emerging for the next phase of access and infrastructure security. Here’s where we believe things are headed:

tldr;

Security will get better — and feel simpler.

The future of access is seamless, secure, and adaptive. Users will see fewer passwords and fewer roadblocks. Security teams will gain better visibility and smarter controls. Organizations that treat secure access as an enabler — not a cost — will gain both resilience and speed. And with AI introducing a wave of new agents, services, and attack surfaces, getting access right is more urgent than ever.

1 _identity will become the foundation of access architecture

In the coming years, new infrastructure projects will begin not with IP design, but with identity and access requirements. The idea that “identity is the new perimeter” will move from philosophy to standard operating procedure. Even legacy internal apps will be fronted by identity-aware proxies, and phishing-resistant authentication (like WebAuthn) will become mandatory for privileged access.

2 _implicit trust in networks will disappear

The old perimeter-based model is collapsing. Flat internal networks will be carved up via central policies. Expect every access — whether human or service, local or remote — to be authenticated, authorized, and encrypted. Even server-to-server communication in the same rack will follow Zero Trust principles.

3 _vpns won’t vanish, but they’ll be redefined

Legacy VPNs that grant broad access will fade, replaced by lightweight, identity-aware access tools. Peer-to-peer and mesh architectures will become more common. VPNs that survive will serve niche or legacy use cases — but their role will shift dramatically. The trend isn’t death, but reinvention.

4 _ai will power both defense and attack

Defenders are beginning to use AI for anomaly detection, risk scoring, and automation. We expect this to become table stakes. But attackers are moving faster: AI is already being used to generate targeted phishing, scan for mis-configurations, and automate lateral movement. This shift will raise the stakes and accelerate adoption of adaptive, real-time security responses.

5 _secure access to ai infrastructure will raise the bar

As companies invest in GPU clusters and shared model training infrastructure, access controls must become more dynamic and performance-sensitive. Legacy tooling wasn’t built for these environments. The expectation will shift: access to AI systems must be both seamless and verifiably secure.

6 _security will become part of engineering culture

The days of “security vs. developer productivity” are ending. Security policies will be designed with UX in mind, and developers will expect infrastructure that’s secure by default. Concepts like Just-In-Time access, dynamic permissions, and internal developer platforms with security baked in will become standard.

7 _composability will beat consolidation

While some enterprises will chase consolidation, the smarter move will be modularity. Customers will demand platforms that integrate cleanly, work with existing identity systems, and let them swap components as their needs evolve. Open APIs, interoperability, and ease of exit will become top buying criteria.

8 _zero trust will stretch from login to deployment pipeline

We expect Zero Trust principles to extend deep into CI/CD pipelines. Every API call, every build process, and every machine identity will be authenticated and verified. The software supply chain will become a major battleground — and Zero Trust will secure it end-to-end.

9 _standards will (finally) catch up

Expect convergence around practical frameworks from NIST, CISA, and others. These will give security teams a roadmap for measuring maturity and benchmarking progress. With government pressure and public case studies growing, many companies will align to formal standards by the end of 2026.

10 _zero trust will extend to edge and IoT environments

As compute moves outside the data center, organizations will apply identity-first principles to secure edge, IoT, and OT systems. That means encrypting device-to-device traffic, verifying every endpoint — even in constrained or disconnected environments (think factories, isolated locations, etc.) — and designing for policy enforcement at the edge.

08//

Recommendations

For IT, engineering, and security leaders

For CIOs, CISOs, CTOs, and IT managers looking to act on these findings, here are concrete recommendations to drive your organization toward a more secure, Zero Trust-ready state:

1 `_develop an identity-first access strategy`

Make identity the linchpin of your access control model. Conduct an audit of all critical systems to ensure they are integrated with your central identity provider (e.g., LDAP/AD or cloud SSO). If some apps don't support SSO, prioritize updating or replacing them. Move toward granting access based on roles/attributes rather than network location. For example, instead of a firewall rule that allows an entire subnet, use an identity-aware proxy that only allows authenticated user sessions.

2 `_accelerate vpn replacement plans`

If your organization still relies heavily on a legacy VPN for remote access, start piloting a Zero Trust Network Access solution within the next 6 months. Identify a set of users or an application that suffers from VPN performance issues and trial a Zero Trust platform. Many providers, including Tailscale, offer easy pilot deployments. Use the pilot to gather data – e.g., latency improvements, user satisfaction – to build the case for broader adoption.

3 `_tighten onboarding/offboarding processes`

The survey's results on lingering access demand immediate attention. Perform a review of your user offboarding process across HR, IT, and app owners. Establish a zero-tolerance policy for ex-employees retaining access. This may involve investing in an Identity Governance and Administration (IGA) tool that automates deprovisioning across all SaaS and on-prem apps when someone leaves. At minimum, maintain a checklist of all systems to remove access from, and have HR and IT jointly accountable for verifying completion within 24 hours of termination. Similarly, improve onboarding: aim to have new hires productive on Day 1 by pre-provisioning their access based on role.

4 `_consolidate and integrate tools (where it makes sense)`

Reduce complexity by consolidating overlapping security tools. If you have multiple VPN solutions, or both a legacy VPN and a newer Zero Trust solution, plan to retire one. Likewise, integrate wherever possible: feed your identity logs, VPN/ZTNA logs, and endpoint logs into a centralized SIEM or analytics platform so you can correlate events (e.g., detect when someone logs in from a new device and immediately downloads a large amount of data).

5 `_improve user experience — security should be mostly invisible`

Commit to reducing friction for end users. This means adopting measures like single sign-on (One login unlocks all apps they need.), eliminating separate VPN clients in favor of seamless authentication, and ensuring fast, reliable connections. Gather feedback from developers and employees about their pain points with current access. Then, prioritize fixes that also improve security. For example, if developers hate switching VPN contexts to access different cloud environments, implement a unified secure access solution that can reach all environments once they authenticate one time.

6 _enable and educate – turn frustrated users into allies

Instead of enforcing top-down rules only, involve users in crafting solutions. Set up an internal Security Champions program: designate tech-savvy members of each team to be liaisons for secure practices. When rolling out new security measures, explain the "why" to all staff, emphasizing how it protects the company and them personally. Provide training on how to use new tools (for instance, how to request temporary access through a new portal instead of jumping the fence). By improving awareness, you reduce unintentional violations.

7 _implement just-in-time and least privilege access

Embrace the principle of least privilege by not granting standing access unless necessary. Where possible, use Just-In-Time (JIT) access workflows: e.g., an engineer can request access to a production server for the next 2 hours, with managerial approval automatically logged, rather than having 24x7 access. Many IAM or PAM (Privileged Access Management) tools can facilitate this. It reduces risk, so no one has permanent access to sensitive systems if they don't need it, and it improves compliance, since access is tied to purpose and time.

8 _boost monitoring and incident response for access anomalies

Given many breaches involve credential misuse, strengthen your monitoring of access patterns and alert systems — e.g., logins from unusual locations, sudden access to unfamiliar systems, or activity outside normal hours. Use logs from your SSO, VPN, and access tools to create these alerts. As AI agents and automated systems become more common, detection rules should also cover machine-driven behaviors. If possible, layer in behavior analytics and regularly test for blind spots like orphaned accounts or insider threat scenarios.

9 _plan for scalability (network and operations)

With 84% of companies reporting increased throughput needs, design your secure access with scalability in mind. This means preferring cloud-delivered services that scale automatically and avoiding bottlenecks (which is another reason to move off legacy VPNs). It also means scaling your team's capability via automation – as user counts and device counts grow, you want automated provisioning, not proportional growth in IT headcount just to manage accounts.

10 _align with a zero trust framework and track progress

Choose a reputable framework (like NIST 800-207 or CISA's Zero Trust Maturity Model) and assess where you stand. Identify gaps — for instance, you might realize you have strong identity controls (pillar 1) but weak device visibility (pillar 2), or that your network segmentation is good, but you lack analytics (pillar 5). Create a road map to address these gaps incrementally.

By following these recommendations, IT and security leaders can make tangible improvements in their security posture while also addressing user frustrations. The journey to Zero Trust doesn't happen overnight, but every step — consolidating two tools, enabling MFA on one more app, reducing one manual process — meaningfully lowers risk. Importantly, many of these steps also streamline IT operations (fewer systems to manage, automated workflows) and improve user satisfaction (faster access, clearer processes), creating a virtuous cycle of security and productivity. Leaders should aim for those "win-win" actions that check both boxes.

If you're interested in learning how Tailscale can help solve the secure access issues outlined in this report, visit us at **tailscale.com**, or reach out to our sales team for a **personalized demo**. You can be up and running with Tailscale in just **10 minutes**.

//
if you would like to be included in future State of zero trust surveys, please submit your email **here**.

tailscale

The State of Zero Trust 2025

For more information on this report and its data sourcing or methodology, or to request an interview with someone at Tailscale, please contact:

`press@tailscale.com`