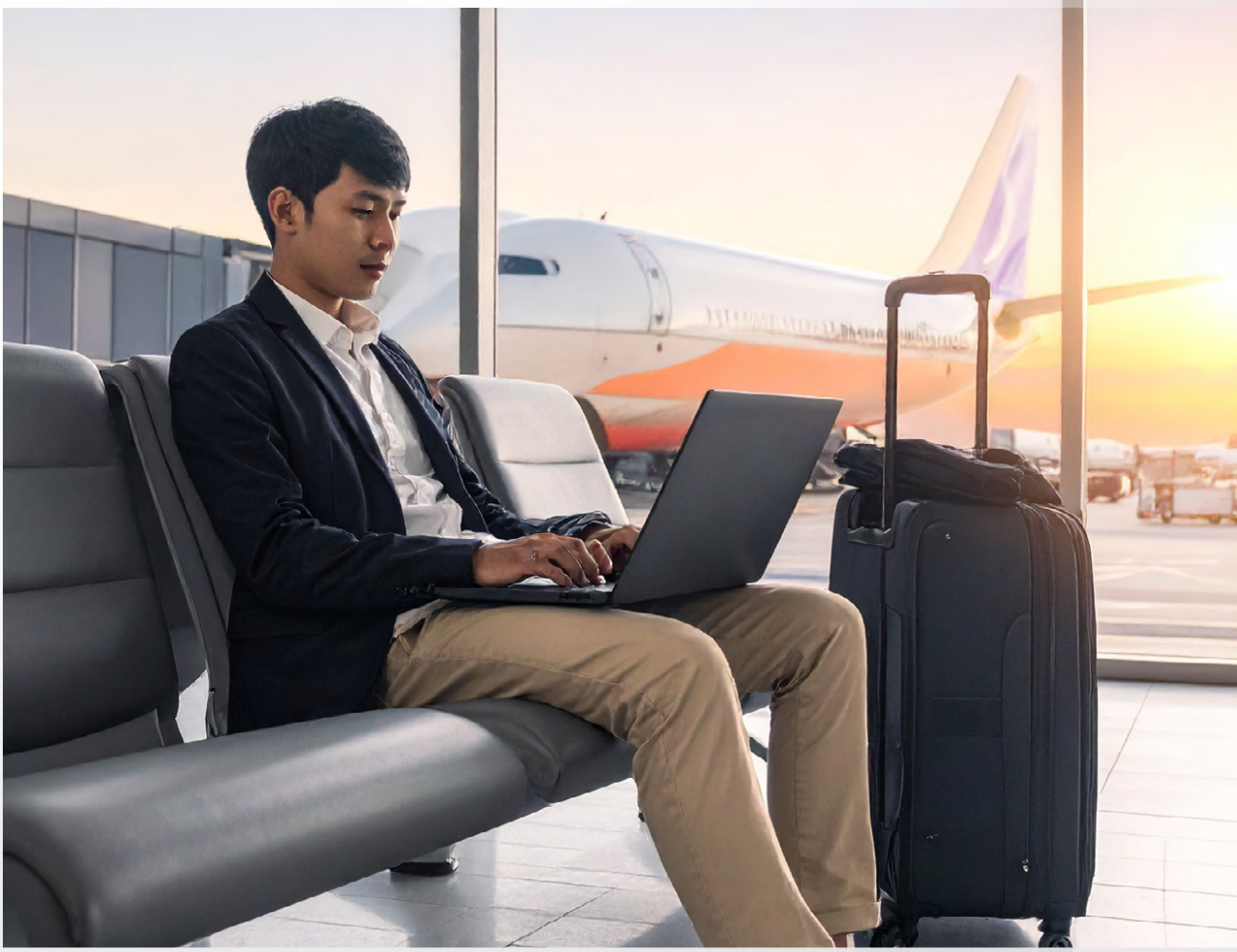
HPE | Cybersecurity INSIDERS

Business Report

2026 Zero Trust Report

Bridging the Execution Gap — Unifying Security from Edge to Cloud



Introduction

Modern enterprises no longer operate within fixed network boundaries. Users connect from anywhere, applications run in the cloud, and data moves freely across ecosystems that traditional network perimeters and security controls were never built to defend. As environments grow more dynamic, the central question for security leaders has shifted from “Who can we trust” to “How do we verify everything, everywhere?”

Zero Trust emerged as the corrective strategy to this reality: never assume trust, always verify. It replaces static, perimeter-based controls with continuous validation of every user, device, and session, wherever they operate. Yet despite near-universal acceptance, Zero Trust execution remains uneven.

Based on a survey of 851 IT, networking, and cybersecurity professionals, the 2025 Zero Trust Report reveals a widening gap between strategic intent versus operational reality: organizations know what Zero Trust requires but struggle to enforce it consistently across hybrid and multi-cloud environments.

Zero Trust has moved from aspiration to architecture. The challenge is no longer conviction, but integration: unifying fragmented tools, policies, and signals into one adaptive security fabric that enforces continuous verification from edge to cloud. Organizations that simplify through SASE and accelerate with AI are proving that security can finally keep pace with the cloud, and with the business itself.

This report examines why Zero Trust progress has stalled and how organizations are breaking through by unifying architectures, extending enforcement universally, and accelerating protection through intelligence. Zero Trust has moved from aspiration to architecture. The challenge is no longer conviction, but integration: unifying.

Key Survey Findings

Zero Trust execution gap widens
82 percent view Universal Zero Trust Network Access (ZTNA) as essential to their security strategy, yet only 17 percent have fully implemented it—a 65-point divide between strategic intent and operational reality in Zero Trust adoption. Organizations rate their current Zero Trust effectiveness at just 6 out of 10, reflecting a maturity plateau driven not by lack of conviction, but by architectural fragmentation, overlapping tools, and policy drift across hybrid, multi-cloud environments.

Excess access erodes trust from within
Internal exposure remains the most persistent weak point: 56 percent cite employee over-privilege and 48 percent highlight SaaS and cloud misgovernance as top sources of unauthorized access. More than half (52 percent) admit that excessive entitlements are widespread, confirming that incomplete enforcement continues to undermine the principle of least privilege.

Unified platforms deliver the breakthrough
Nearly one-third (29 percent) say unified platform adoption would most accelerate their Zero Trust journey. Meanwhile, 63 percent already favor single-vendor SASE (34 percent) or hybrid platform models (29 percent). By converging software-defined wide area networking (SD-WAN) and security service edge (SSE) capabilities within a single policy framework, enterprises are turning Zero Trust from an aspirational model into an operational reality.

CISOs view Zero Trust as a business enabler
Sixty-three percent pursue Zero Trust to reduce breach impact, with agility (41 percent) and cost reduction through consolidation (33 percent) as the key drivers. Leaders now view Zero Trust as the path to faster change and operational efficiency.

Different paths, same destination
Most organizations begin their Zero Trust journey through access modernization, such as VPN replacement with ZTNA (30 percent) or early platform consolidation (26 percent), confirming that secure connectivity and simplification are the first steps toward a unified architecture.

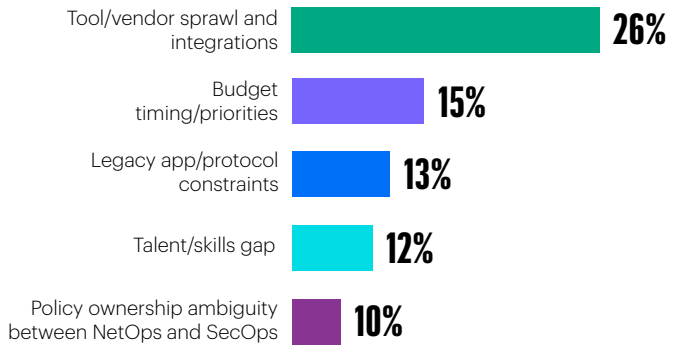
The New Reality: Security Outpaced by Complexity

Hybrid work, SaaS adoption, and cloud-first operations have erased the traditional perimeter, creating an environment where trust can no longer be assumed and security must evolve at the same speed as change itself. Employees connect from anywhere, often on personal devices. Data flows through multiple clouds and SaaS platforms. Partners and contractors now access systems once considered internal. As connectivity expands, visibility fragments, and the question shifts from "Who can we trust" to "How do we verify everything, everywhere?"

That erosion of certainty has made trust the weakest link in modern defense. Every implicit connection, unchecked credential, and unmanaged device becomes an entry point for attackers who no longer need to break in — they simply log in with stolen or abused credentials and move laterally across the network undetected. Furthermore, managing multiple tools with multiple policies creates complexity and potential inconsistencies, increasing the risk of gaps that bad actors can slip through. Zero Trust emerged as the corrective strategy to this reality: never assume trust, always verify. It replaces static, perimeter-based controls with dynamic and continuous validation of every user, device, and session, wherever they operate. Yet translating that principle into practice has proven far more difficult than agreeing on its importance.

The obstacle isn't conviction or funding — it's complexity. One in four organizations (26 percent) identify tool and vendor sprawl as their biggest barrier to advancing Zero Trust and SASE — outpacing challenges related to budget, skills, or legacy systems. After years of layering point solutions to solve isolated problems, most security teams now navigate a maze of overlapping controls that operate independently rather than cohesively. The result: blind spots and human error multiply exactly where adversaries thrive — in the seams between systems. It's no surprise, then, that on average most organizations rate their current Zero Trust effectiveness at only 6 out of 10.

Progress will depend less on adding tools and more on connecting them. The path forward is simplification: unifying identity, device, and network policy under a single, adaptive framework that eliminates friction, restores visibility, and turns Zero Trust from aspiration into daily operational reality.



Performance/user-experience concerns 8%, Lack of executive/board alignment on Zero Trust strategy 7%, Compliance/sovereignty constraints 5%, Difficulty proving ROI 4%

Figure 1. Key Barriers to Zero Trust and SASE Adoption

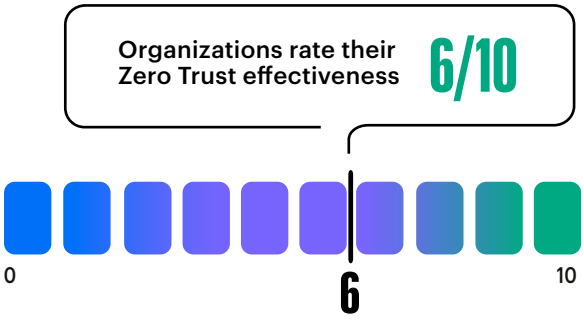


Figure 2. Zero Trust Effectiveness

The Exposure Layer: Over-Privileged Access

Even as Zero Trust becomes a strategic priority, most organizations are discovering just how much implicit trust still remains in daily operations. Over-entitled user accounts, inconsistent SaaS permissions, and unmanaged devices continue to create silent pathways for attackers to blend into legitimate traffic — not through sophisticated exploits, but by simply logging in and moving laterally.

These are not failures of Zero Trust as a concept; they are signs that verification still isn't continuous or universal across every identity, device, and application.

The survey data reveals where this exposure concentrates. A majority, 56 percent, cite employee over-privilege as the leading contributor to unauthorized access, followed by SaaS and cloud applications at 48 percent — areas where adoption has surged faster than governance.

Legacy systems (36 percent) and third-party access (30 percent) remain persistent gaps, extending implicit trust into corners of the enterprise least equipped for modern enforcement. In total, 52 percent report that excessive access is either very or moderately widespread, underscoring how least-privilege principles often erode once scale and complexity set in.

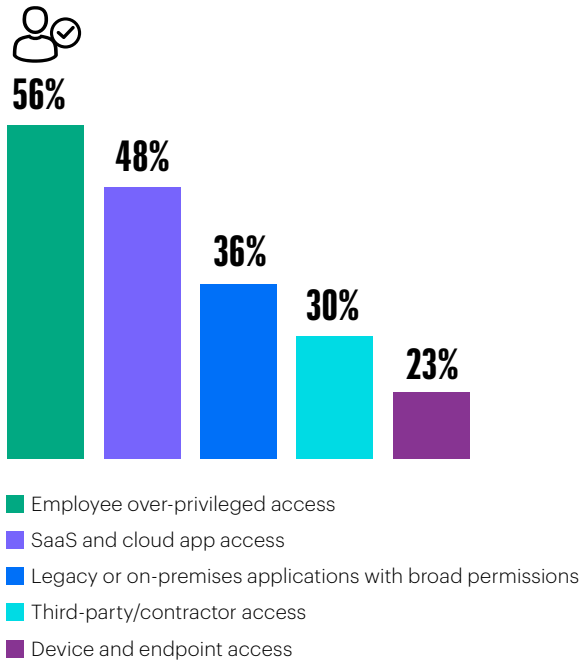


Figure 3. Key Factors Contributing to Excessive Access

Closing these gaps requires secure connection where every session should be validated through identity, device posture, and context — automatically adapting or revoking access as risk changes. When those controls operate through a unified, cloud-delivered policy fabric, Zero Trust stops being a static ideal and becomes a living system of active defense. Privilege control transforms from administrative task to measurable risk reduction.

From Intention to Impact: How CISOs Are Redefining Zero Trust

After years spent patching control gaps, security leaders are reframing Zero Trust as more than a defensive architecture — it's becoming the foundation for operational agility. In this new model, visibility, automation, and unified policy management deliver not only stronger protection but also faster transformation.

The goal is no longer just to stop breaches, but to make security an enabler of speed, scale, and innovation. The data reflects this shift clearly. Sixty-three percent of respondents cite reduced security risk and breach impact as the top outcome driving their Zero Trust and SASE strategies. Yet nearly as many now connect Zero Trust to modernization: 41 percent prioritize greater operational agility, and 33 percent seek lower cost through tool and vendor consolidation.

Operational agility translates into faster, safer change — securely onboarding new applications, enabling hybrid work without VPN friction, accelerating partner and contractor access, and supporting cloud migrations and site rollouts with consistent policy and user experience. This pragmatic balance marks a turning point: CISOs want architectures that not only harden the enterprise but also remove friction from change.

Zero Trust is evolving from a checklist of controls into an operating model that connects identity, device posture, and network context through a unified policy plane.

Organizations adopting this unified approach report tangible performance gains: faster partner onboarding, fewer support tickets related to VPN connectivity, and 20–30 percent cost reductions in the first year through license consolidation and reduced operational overhead. By merging prevention and efficiency into a single architecture, leaders are proving that security and agility are no longer opposing forces but become a measurable advantage.

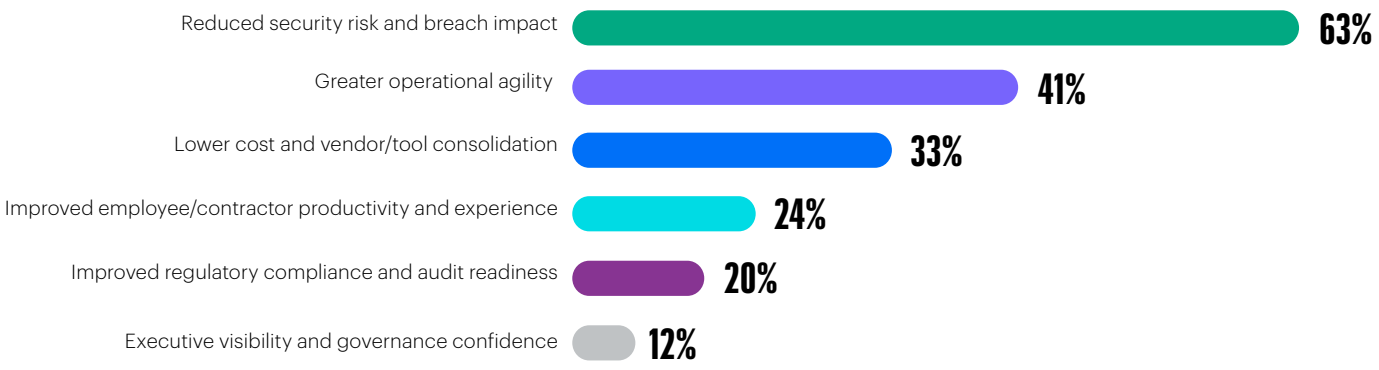


Figure 4. Business Outcomes Drive Zero Trust and SASE

Many Paths, One Destination: The Starting Points of Zero Trust

Zero Trust transformation rarely begins from scratch. Most organizations modernize along distinct technical paths, each chosen to relieve the most immediate source of friction on the road toward unified security. The survey data shows there is no single dominant route — but two clearly lead the way.

Thirty percent of organizations take an access-first approach, replacing legacy VPNs with Zero Trust Network Access (ZTNA) and introducing per-application connectivity for private apps.

This modernization often begins with third-party and contractor access — still implicated in roughly 60 percent of breaches — where agentless ZTNA provides a faster, more secure alternative to VPNs by granting browser-based, least-privilege access without installing client software.

Another 26 percent pursue a platform-first path, consolidating access, inspection, and data protection early through integrated SSE or SASE architectures. Identity-first strategies account for 17 percent, while network-first approaches represent 14 percent, reflecting environments where governance or segmentation maturity drives the agenda. Only 10 percent begin cloud-first, indicating that SaaS and cloud protection generally extend from access modernization rather than serving as standalone entry points.

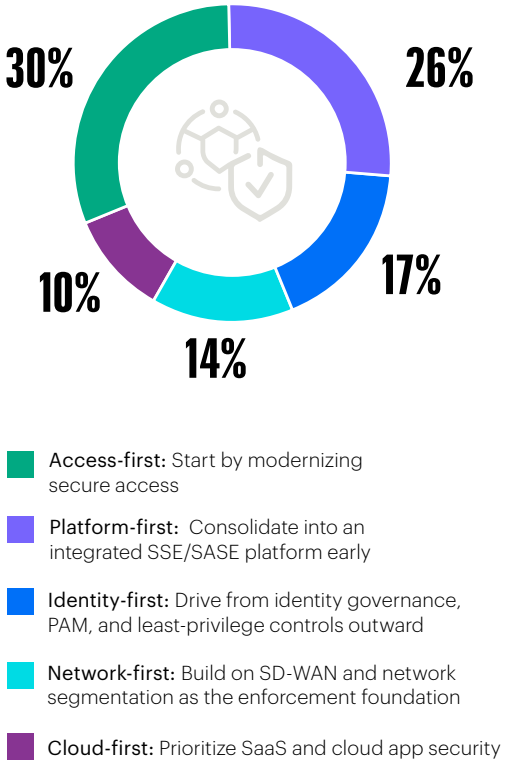


Figure 5. Common Paths to Zero Trust

Each path addresses a different friction point — access bottlenecks, tool sprawl, or visibility gaps — but all converge on the same destination: unified, cloud-delivered Zero Trust enforcement. Organizations that connect access modernization to early platform unification achieve faster returns and a more durable foundation for continuous verification at scale.

How SASE Operationalizes Zero Trust at Scale

Zero Trust transformation rarely begins from scratch. Most organizations modernize along distinct technical paths, each chosen to relieve the most immediate source of friction on the road toward unified security. The survey data shows there is no single dominant route — but two clearly lead the way.

Zero Trust defines what must change — verification for every identity, device, and connection — but it does not prescribe how to deliver that enforcement consistently across hybrid networks, cloud workloads, and remote users without multiplying tools or latency.

Secure Access Service Edge (SASE) provides that delivery architecture. It converges networking (SD-WAN) and security (SSE functions including ZTNA, SWG, CASB, and DLP) into a single, cloud-delivered framework that enforces identity- and context-based policy wherever users and data operate. And instead of routing traffic back through data centers, SASE directs it optimally. Instead of tying policy to IP addresses, it follows identity. Instead of maintaining separate security stacks for office, branch, and remote workers, one unified fabric covers all.

The survey data confirms this convergence is well underway: 34 percent of organizations favor a single-vendor SASE platform, while 29 percent pursue a hybrid approach — showing that nearly two-thirds (63 percent) are consolidating rather than diversifying.

For organizations seeking to replace fragmented networks and disjointed security controls, SASE represents the operational delivery architecture of Zero Trust — the means to unify enforcement, simplify management, and accelerate transformation without compromise.

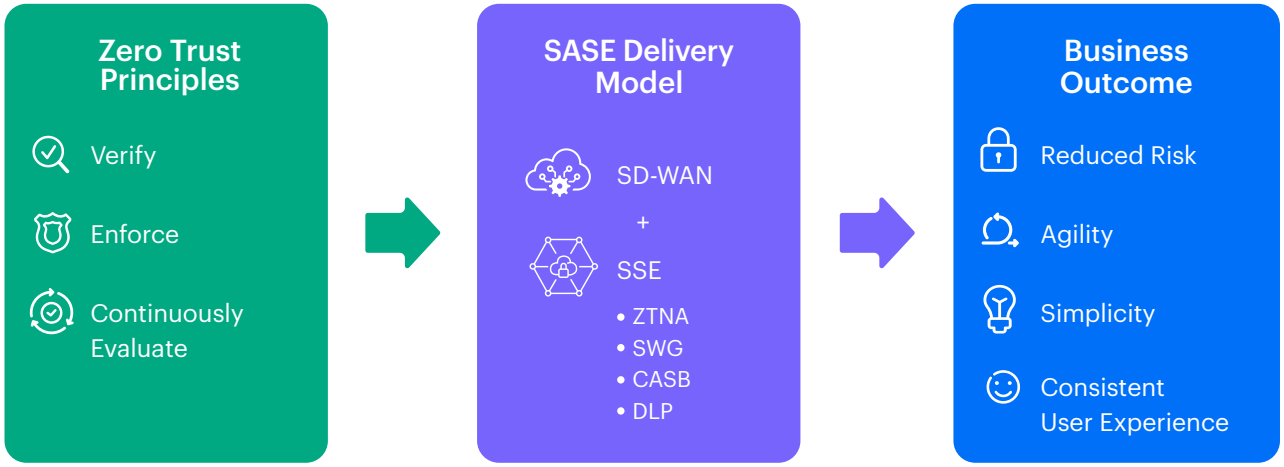


Figure 6. SASE Turns Zero Trust Principles into Business Outcomes

By converging networking and security into a cloud-delivered policy fabric, SASE makes continuous verification practical — turning Zero Trust from a framework into everyday reality.

The Integration Wall: Why Zero Trust Progress Stalls

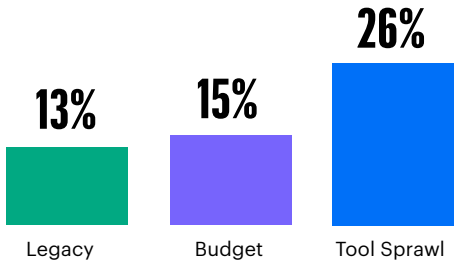
Even with clear strategy and the right architectural model in sight, many organizations remain trapped in operational complexity. After years of incremental security projects, most enterprises now operate a patchwork of tools that overlap in function but not in policy. Each protects a piece of the environment. Together, they create the very gaps adversaries exploit.

The survey data reveals the scale of the problem. Tool and vendor sprawl ranks as the single largest barrier to advancing Zero Trust and SASE, cited by 26 percent of organizations, ahead of both budget and legacy technology. Seventy-eight percent manage secure-access policy across more than two separate systems, while only 17 percent operate from a unified platform. The outcome is predictable: inconsistent enforcement, duplicated effort, and delayed response when policies must adapt across clouds, sites, and remote users. Fragmentation, not funding, is what keeps progress slow.

Fragmentation isn't just inefficient, it is risky. Every disconnected console delays the moment when identity or device risk signals reach enforcement points. Policies drift, exceptions accumulate, and the promise of continuous verification breaks down in practice.

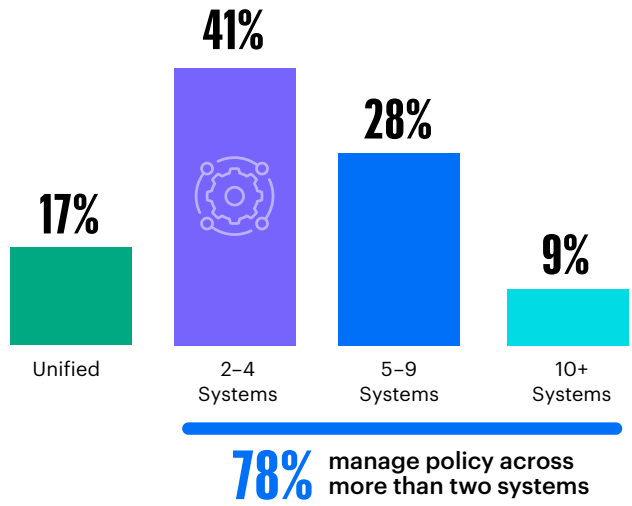
SASE directly addresses this integration wall. By converging SD-WAN, SSE, and Zero Trust controls into a single policy fabric, it replaces tool coordination with automatic policy inheritance where every control operates from the same data, identity, and intent. Security teams manage one adaptive framework instead of orchestrating many.

Enterprises that overcome this wall don't just simplify operations but reclaim time, clarity, and confidence. Unification restores speed to security — and security to transformation. Time is an organization's most finite resource. Reclaiming it enables teams to focus on initiatives that drive revenue or reduce risk, maximizing the impact of high-end engineering and analyst talent.



Talent/skills gap 12% | Policy ownership 10% | Other 24%

Figure 7. Top Barriers to Adoption



Don't know 5%

Figure 8. Number of Systems That Manage Access Policy

Progress rarely happens all at once. Successful programs begin with focused use cases — modernizing a single access path or branch site — then expand systematically. Successful Zero Trust and SASE modernization builds on existing investments, rather than starting over.

Simplification as Strategy: The Turn Toward Unified Architectures

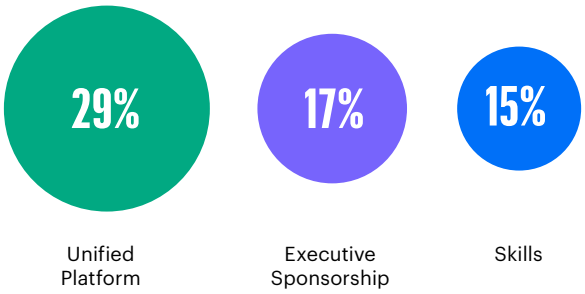
After years of expansion, the measure of security maturity is no longer how many controls an organization deploys, but how well those controls work together. The survey clearly shows that the industry is pivoting from diversification to consolidation.

Nearly one in three respondents (29 percent) say unified platform adoption would most accelerate their Zero Trust and SASE progress — outpacing executive sponsorship (17 percent) and skills investment (15 percent) as the top driver of advancement.

At the same time, 34 percent already favor a single-vendor SASE platform combining SD-WAN and SSE, while another 29 percent pursue a hybrid model that integrates a primary platform with select best-of-breed tools. In total, 63 percent are now consolidating rather than expanding toolsets.

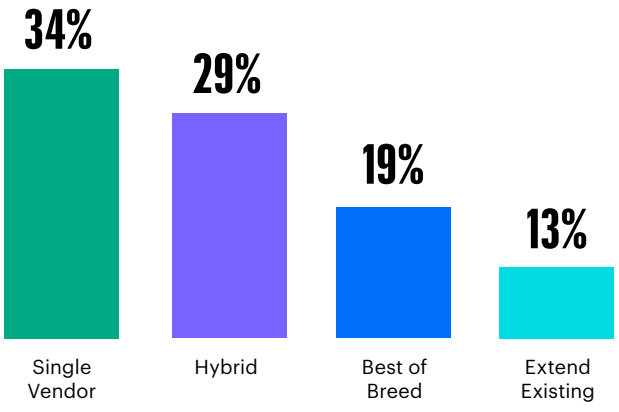
The benefits go well beyond cost efficiency. Unified architectures remove friction between networking and security teams, create a single policy source of truth, and enable faster change across sites, clouds, and remote users.

Policy consistency improves visibility. Automation reduces human error. Instead of managing dozens of disconnected consoles, teams orchestrate a single security policy fabric that applies context-aware controls everywhere — from headquarters to home office, from private applications to SaaS.



NetSec operating model 13% | Device and network enforcement 11% | Data & SaaS controls modernization 9% | User experience assurance 6%

Figure 9. SASE Accelerators



Other 5%

Figure 10. Preferred SASE Strategy

For organizations still operating through fragmented systems, the mandate is clear: unify identity, device, and network enforcement under a single, cloud-delivered policy plane. Simplify first, then scale safely. That's how Zero Trust and SASE evolve from parallel initiatives into one adaptive operating model that moves at the pace of the business.

Universal ZTNA: The Execution Engine of Zero Trust

Once architectures unify, enforcement must follow. That's where Universal Zero Trust Network Access (ZTNA) becomes the operational core of a modern security fabric. It extends the principles of least privilege and continuous verification to every user, device, and application — without the constraints of traditional VPN or perimeter-based design.

Unlike traditional ZTNA, Universal ZTNA fills a critical gap in today's SASE framework by extending Zero Trust beyond remote users to campus and branch networks. By combining Secure Service Edge (SSE) and Network Access Control (NAC), it applies one identity- and context-based policy everywhere — remote, branch, and on-site — eliminating the fragmentation of separate access systems.

The survey findings confirm that 82 percent of organizations view Universal ZTNA as essential to their security strategy. Yet execution lags dramatically: Only 17 percent have fully implemented Universal ZTNA, while 46 percent remain in partial deployment and another 24 percent are planning to implement. The result is a 65-point execution gap between conviction and execution that defines the next phase of Zero Trust maturity.

By converging SSE and NAC under a single, cloud-delivered policy engine, Universal ZTNA simplifies operations and reduces tool sprawl—enforcing per-session verification across all access paths without added latency or user friction. The result is stronger protection, unified visibility, and consistent policy enforcement from edge to cloud, transforming Zero Trust from a remote-access control into a universal enforcement model that closes the SASE gap, cuts complexity, and makes continuous verification operationally real.

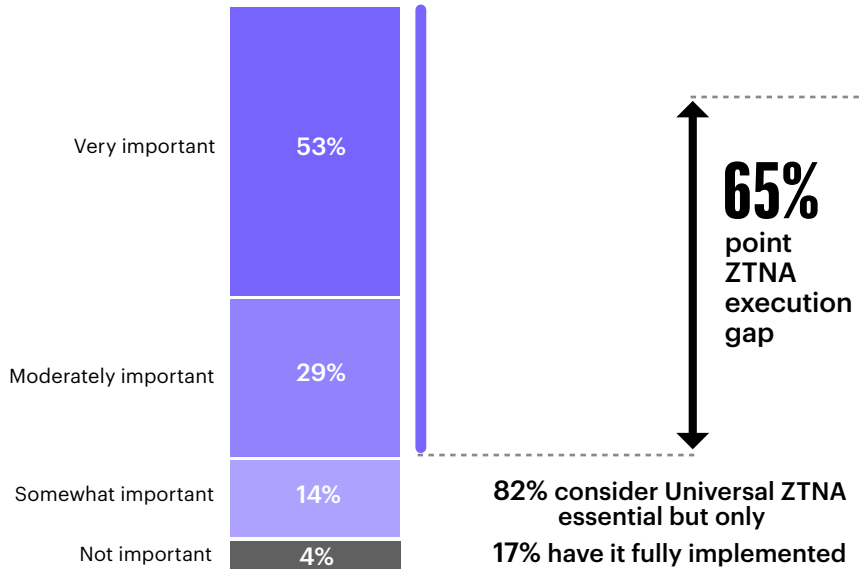


Figure 11. Importance of Universal ZTNA

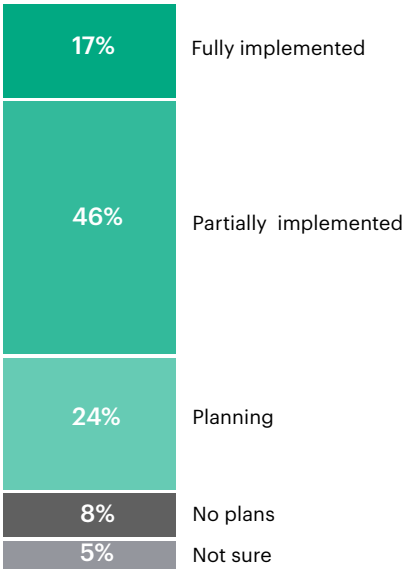


Figure 12. ZTNA implementation progress

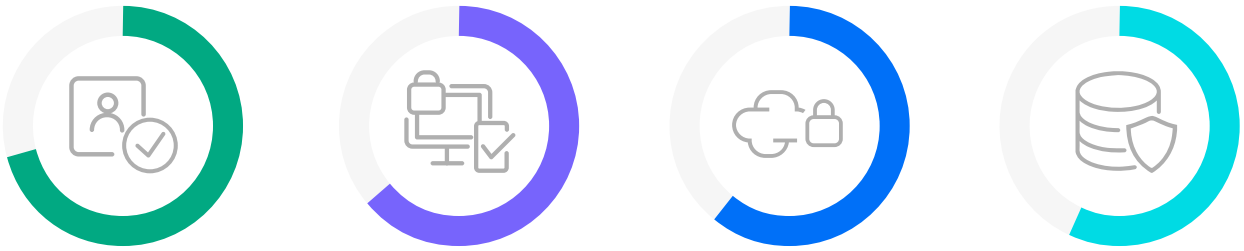
Beyond Access: Extending Zero Trust Across the Enterprise

For most organizations, the next stage of Zero Trust maturity isn't about adding new tools, but about applying the same principles across the enterprise. Once identity, access, and policy are unified through architectures such as SASE and enforced by Universal ZTNA, the focus shifts to coverage: extending those controls with equal precision across users, devices, data, and workloads.

The survey data shows this expansion is already in motion. Identity and access remain the top priority for 71 percent of respondents, but security leaders are now extending Zero Trust logic deeper into the environment: device and network enforcement rank at 64 percent, cloud and SaaS security at 61 percent, and data protection at 57 percent. This progression marks a clear evolution from defending the perimeter to securing the entire transaction chain, from authentication through data access.

In mature Zero Trust programs, these layers no longer operate as separate disciplines but as connected expressions of the same policy framework. Identity establishes who connects, device posture confirms trustworthiness, data controls govern what can be accessed, and threat detection validates behavior in real time. Together they form a continuous trust loop — one architecture, many enforcement points.

Enterprises that reach this level of integration experience measurable gains: simplified compliance audits, faster incident containment, and a security posture that evolves naturally with business change. At this stage, Zero Trust becomes invisible infrastructure, embedded in every connection rather than added as an afterthought. When executed correctly, users experience fewer disruptions and security becomes as seamless as connectivity itself.



Threat Detection & Response 49% | User experience and monitoring 33% | None of the above 3%

Figure 13. Zero Trust Expands Beyond Access

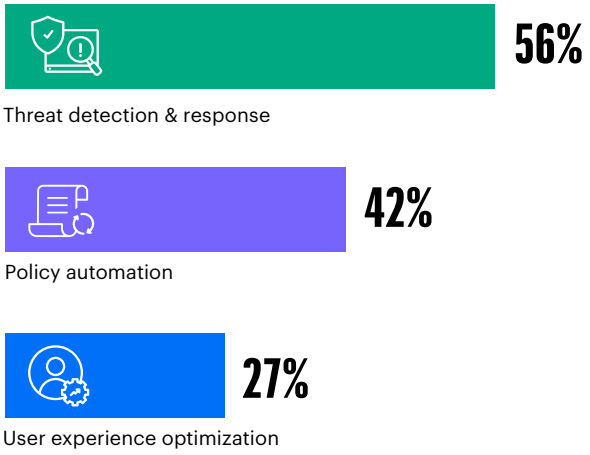
AI: The New Force Multiplier

As Zero Trust becomes embedded across the enterprise, artificial intelligence is transforming how security operates — analyzing telemetry at scale, detecting anomalies faster than human teams can respond, and dynamically adapting controls based on behavioral context.

In mature environments, AI doesn't replace human judgment but instead augments it through intelligent copilots that assist analysts and administrators, automating routine tasks, surfacing insights, and suggesting actions in real time. Together, they turn Zero Trust from a static policy framework into a living, collaborative system of continuous defense.

The survey results highlight how quickly this shift is accelerating. Fifty-six percent of organizations already use AI or machine learning for threat detection and response, while 42 percent apply it to policy automation, adjusting access, segmentation, and verification in real time. Another 27 percent leverage AI to optimize user experience, applying intelligence once reserved for protection to performance and usability.

Together, these findings confirm that automation is no longer experimental. Instead, it is becoming the operational fabric of Zero Trust.



Threat Detection & Response 49% | User experience and monitoring 33% | None of the above 3%

Figure 14. AI Becomes a Zero Trust Force Multiplier

When AI and Zero Trust intersect, the result is speed, precision, and consistency. Risk signals trigger policy changes instantly; new threats are contained before they spread. Access decisions reflect real-time behavior rather than static rules. And because AI interprets intent across users, devices, and data, security teams can redirect focus from reactive firefighting to strategic improvement.

From Fragmented to Unified: The Zero Trust Execution Matrix

The findings from this year's survey are clear: Zero Trust works best when it's unified. Complexity, overlapping tools, and inconsistent enforcement remain the chief obstacles to progress. The first step is always visibility: map who and what connects, then modernize one access path at a time to prove the model and build momentum.

Organizations advancing fastest are simplifying architectures, unifying identity and policy under a single control plane, and applying automation to keep protection both continuous and invisible. The matrix below distills these steps into a pragmatic framework for turning Zero Trust strategy into sustained operational reality.

	FOCUS AREA	KEY ACTIONS	STRATEGIC OUTCOME
1	**Simplify the Architecture** Complexity is now the top barrier: 26% cite tool and vendor sprawl. Most enterprises manage policy across multiple systems (78%).	• Rationalize overlapping tools and retire legacy VPN paths. • Converge SD-WAN and SSE into an integrated, cloud-delivered SASE fabric. • Establish a single policy source of truth across sites, users, and clouds.	Unified visibility and faster policy propagation. Lower operational overhead with less time spent managing tools, and more time improving protection.
2	**Unify Enforcement** Zero Trust maturity stalls when enforcement is inconsistent: only 17% have fully implemented Universal ZTNA, though 82% call it essential. Universal ZTNA unifies Secure Service Edge (SSE) and Network Access Control (NAC) to extend Zero Trust and SASE across remote, campus, and branch networks with one policy fabric.	• Deploy Universal ZTNA for all users, devices, and resources. • Integrate identity, device posture, and network context into one decision plane. • Replace static network access with continuous, per-session verification.	Consistent, adaptive access control. Least privilege becomes automatic and auditable, reducing internal exposure and human error.
3	**Amplify with Intelligence** Manual processes can't scale. 56% use AI for threat detection and 42% for policy automation.	• Apply AI/ML to detect anomalies and refine policy dynamically. • Automate posture checks, segmentation, and access reviews. • Use analytics to measure and improve Zero Trust coverage over time.	A self-learning security posture that adapts in real time, reducing effort and improving both protection and user experience.

Closing Perspective

Zero Trust maturity depends less on how many controls an organization deploys and more on how seamlessly, consistently, and intelligently they operate as one unified system.

This report reveals a clear paradox: organizations broadly understand what Zero Trust requires, yet many struggle to implement it completely. With an average effectiveness rating of 6 out of 10, a 65-point gap between ZTNA importance and implementation, and the persistence of privilege sprawl despite years of investment, the conclusion is inescapable — architectural fragmentation remains the root cause preventing continuous verification at scale.

When these three levers align — simplification, unification, intelligence — Zero Trust evolves from aspiration to advantage: secure, scalable, and ready for the cloud-connected future. The organizations advancing fastest are connecting the controls they already have into a single adaptive fabric that finally makes continuous verification operationally real. The transition won't happen overnight, but it is achievable.

Start with visibility, modernize one access path, and prove the model. Then scale systematically. Zero Trust isn't a single destination — it's an ongoing discipline. And that discipline now has a unified architecture.

The path forward is clear:

1

Simplify the architecture to eliminate operational friction

What's causing your VPN headache? Rationalize redundant tools. Converge SD-WAN and SSE into a unified, cloud-delivered SASE fabric. Establish a single policy source of truth across all environments

2

Unify enforcement so every connection is verified consistently

Deploy Universal ZTNA — which combines SSE and NAC to extend SASE to campus and branch networks — across all users, devices, and resources. Integrate identity, device posture, and network context into one decision plane. Replace static network access with continuous, per-session verification.

3

Amplify with intelligence to make protection adaptive

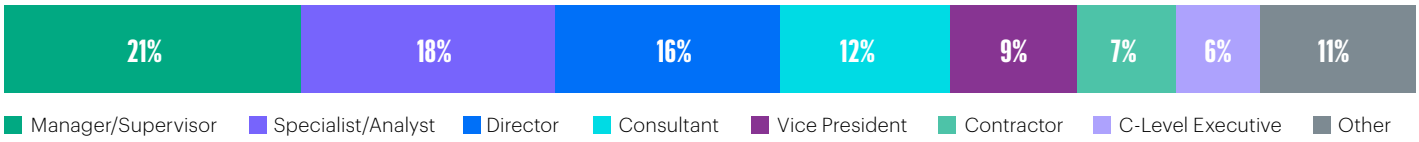
Apply AI to detect anomalies and potential threats, refine policy dynamically, and automate posture checks. Use analytics to continuously measure and strengthen coverage.

Methodology & Demographics

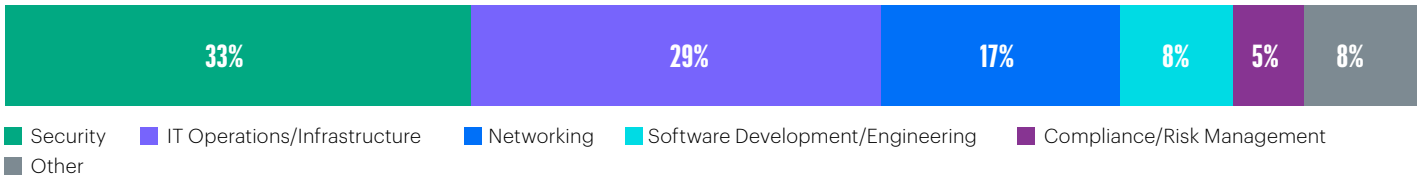
The 2026 Zero Trust Report is based on a global survey of 851 IT, networking, and cybersecurity professionals conducted in late 2025. Respondents represent organizations across multiple industries and company sizes, with roles spanning security operations, network engineering, architecture, and executive leadership.

Survey participants were asked to assess their organization's Zero Trust and SASE maturity, implementation priorities, architectural approaches, and operational challenges. All responses were self-reported and reflect organizational perspectives as of the survey period.

PRIMARY JOB FUNCTION

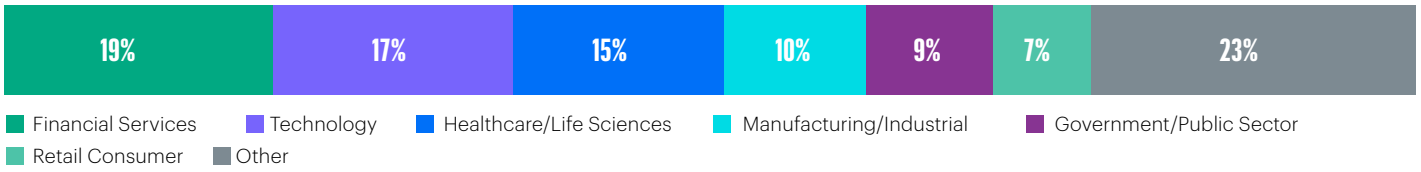


DEPARTMENT



COMPANY SIZE

INDUSTRY



About HPE

HPE is a leader in essential enterprise technology, bringing together the power of AI, cloud, and networking to help organizations achieve more. HPE empowers customers across industries to optimize operational performance, transform data into foresight, and maximize their impact. HPE networking and security solutions help organizations secure the modern workplace and deliver simplified, secure, anywhere access to applications and data while enhancing end-user experience.

Discover more about

AI-powered HPE Aruba Networking single-vendor SASE

Cybersecurity
INSIDERS

STRATEGIC INSIGHT FOR CYBERSECURITY LEADERS

Cybersecurity Insiders provides independent research and analysis focused on the operational reality of enterprise cybersecurity. We gather insights from senior security and IT leaders to examine how high-level strategies translate into day-to-day execution. Our analysis identifies the measurable gaps between intended strategy and actual risk exposure, offering a credible, data-driven foundation for security decision-making and industry benchmarking.

For more information, visit

cybersecurity-insiders.com

Jan 2026 // Version 2.0

a00155604enw