open systems

2026

MANAGED SASE & ZERO TRUST REPORT

Hybrid Complexity, Visibility Gaps, and the Shift to Managed SASE

Research by

Cybersecurity INSIDERS

Overview

Organizations no longer treat "hybrid" as a transitional phase. It is the new operating reality in which users, applications, and partners require secure access from everywhere, continuously. This shift has fundamentally changed how secure access must be delivered and sustained. Zero Trust principles - grounding access decisions in identity and continuous verification rather than network location - are now widely accepted. SASE architectures have emerged to deliver these capabilities through unified cloud services. Yet many organizations are still struggling to operate these models consistently at scale.

To understand how leaders are navigating the gap between SASE strategy and day-to-day execution, we surveyed over 500 senior security and IT leaders across the United States and the United Kingdom who are directly responsible for connectivity, security and performance across hybrid environments.

Three key findings illustrate the execution gap:

- **Visibility has not kept pace with hybrid complexity.** More than 90% of organizations secure users, applications, data centers, and third parties simultaneously. Yet roughly two-thirds cite lack of end-to-end visibility as their top operational challenge, revealing a growing gap between environmental scope and operational control.
- **Zero Trust is advancing, but most organizations remain in a middle state.** While the market has moved beyond legacy VPN-only access, fewer than one in ten organizations have achieved a fully integrated Zero Trust architecture. Most operate with partial deployment and inconsistent enforcement across environments.
- **Execution capacity is the primary constraint.** Nearly half of organizations report the parallel operation of VPN and ZTNA as a major operational burden, fragmenting policy and increasing support overhead. In response, roughly four in five now prefer co-managed or fully managed SASE models, reflecting a shift toward operating models designed to absorb integration complexity rather than passing it to internal teams.

The market is aligned on the strategic direction of SASE and Zero Trust. What holds back progress is execution capacity. As a result, organizations are reassessing not whether to adopt SASE, but how secure access must be delivered to achieve consistent execution and long-term operational resilience.

Hybrid is Permanent - Visibility Has Not Kept Pace

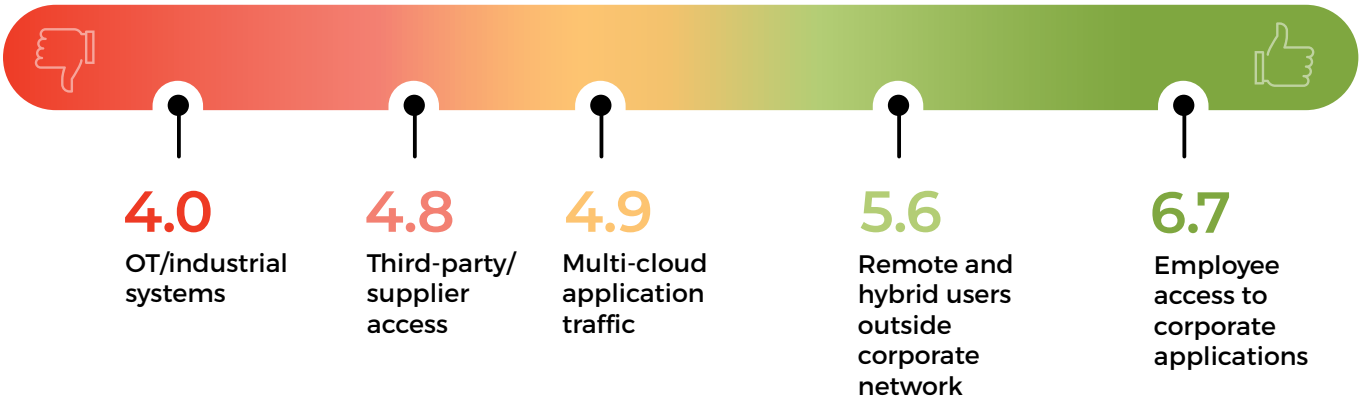
Hybrid is no longer a transition phase. It is how organizations operate today: securing users, applications, data centers, branches, and third-party partners simultaneously across environments that were never designed to function as a single system.

The survey data confirms this scale. More than 90% of organizations secure remote employees and SaaS applications, around 85% secure branch locations, and between 70% extend access to third-party partners. While connectivity across these environments is largely solved, visibility is not. As hybrid complexity has expanded, what security and network teams can realistically observe has failed to keep pace. Two-thirds of respondents cite lack of end-to-end visibility as their top operational challenge, reflecting a growing gap between environmental scope and operational control.

We see this confidence cliff clearly in the data: respondents rate their ability to monitor core applications at six out of ten. But as access moves toward the edges - remote users, multi-cloud traffic, and third-party access - confidence drops sharply, falling to around four out of ten. With 70% of organizations relying on external partners, these blind spots sit squarely within normal operations.

The Confidence Cliff: Visibility Degrades at the Edges

How confident are you in your organization's ability to monitor and control the following access scenarios?



The consequences surface immediately in operational metrics. Degraded remote performance, inconsistent user experience, rising ticket volumes are each cited by roughly half of respondents. In response, organizations are increasingly turning to AI to cope with signal overload, prioritizing incident detection, anomaly monitoring, and support automation. Visibility, in this context, is less about collecting more data and more about enabling timely, actionable decisions. This is the operational reality into which SASE is being deployed.

Zero Trust: The Middle State

If visibility gaps drive day-to-day operational pain, Zero Trust represents the strategic destination most organizations have already committed to. The challenge is no longer whether Zero Trust is the right model, but why progress slows once initial deployments are in place.

The survey shows a market that has decisively moved beyond VPN-only access yet remains concentrated in partial and uneven stages of Zero Trust execution. Only 13% still rely on traditional VPN-only models, while just 9% describe their environment as a fully integrated Zero Trust architecture. Between these two extremes lies the vast majority of roughly 80% of organizations operating in a sustained middle state that is often operationally messy.

That middle state typically takes three forms:

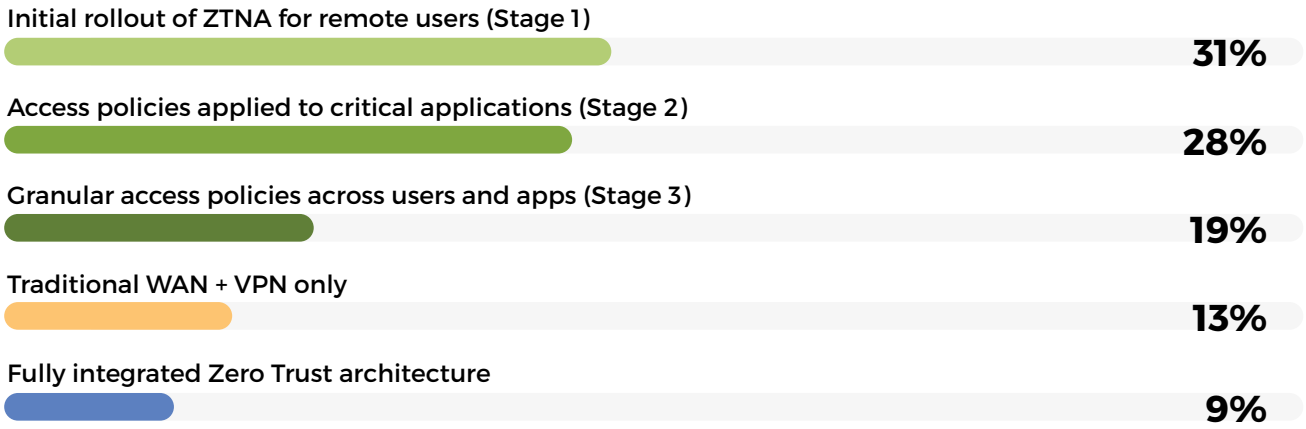
Stage 1 – The Quick Win (31%):
ZTNA deployed primarily for remote users, delivering immediate security and user experience gains without requiring broad architectural change.

Stage 2 – The Extension (28%):
Access controls extended to critical applications for both remote and on-site users, increasing coverage but still relying on mixed enforcement models.

Stage 3 – The Policy Layer (19%):
Granular, policy-driven access using ZTNA, SWG, and CASB, often implemented unevenly across environments as integration complexity grows.

The Zero Trust "Middle State": Most Organizations Are Stuck in Partial Deployment

Which best describes your organization's current Zero Trust maturity status?



The data helps explain why this stall persists. ZTNA is the most common entry point for SASE (63%), followed by SD-WAN (around 50%), with SWG and CASB adopted later. This remote-first sequencing delivers immediate relief for remote workers, improving experience and eliminating VPN backhaul However, this remote-first approach often creates silos. Organizations succeed in securing the remote worker first but then struggle to replicate that same architecture across branches, third parties, and on-premises data centers. The result is a modern front door (ZTNA) attached to a legacy house, unable to bridge the gap to full integration. Zero Trust foundations are in place, but translating partial deployment into end-to-end integration across the broader environment has proven harder than anticipated.

The Execution Gap: When Complexity Outpaces Capacity

Most organizations are aligned on the strategic direction of SASE and Zero Trust. What is slowing progress is not a lack of budget or intent, but a growing gap between environmental complexity and execution capacity.

The survey identifies three structural barriers that define this execution gap:

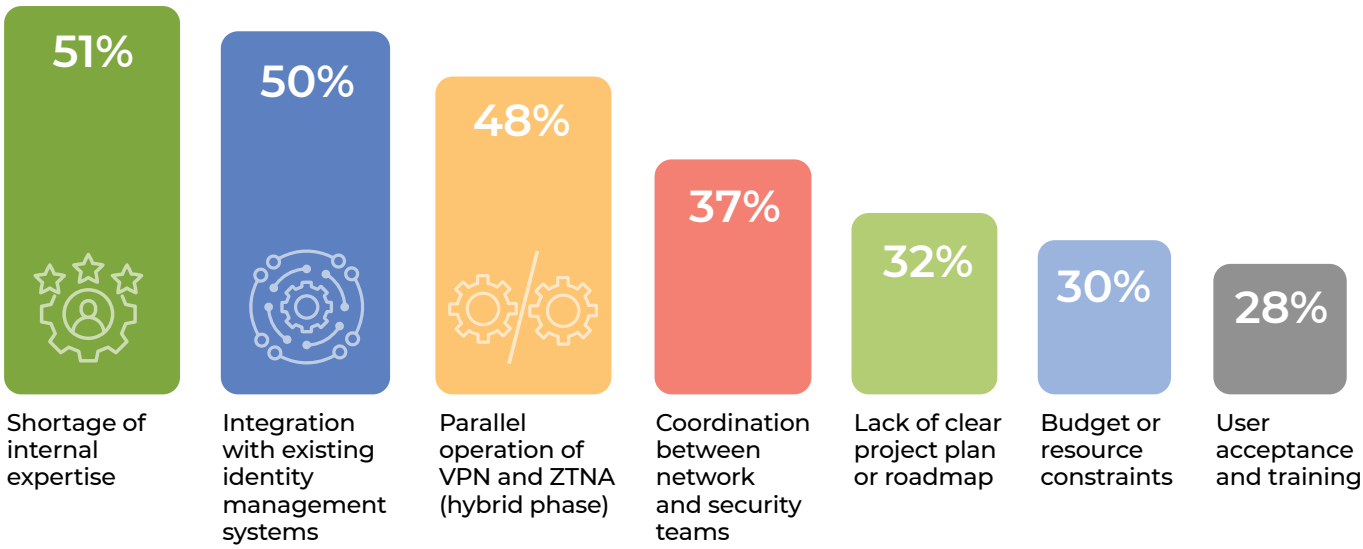
1. Integration Friction:
Integration with existing systems is the most frequently cited challenge for SASE (53%). At the ZTNA layer, more than half of respondents (52%) struggle to integrate with identity management systems. The tools are deployed, but policy, identity context, and telemetry remain fragmented across the stack, limiting consistent enforcement.

2. The Skills Gap:
Internal expertise shortages are the second most significant barrier (51%). Organizations are attempting to operate next-generation, policy-driven architectures with teams and workflows built for legacy firewall and VPN environments, limiting consistent execution at scale.

3. The Parallel Operations Tax:
Nearly half of organizations (48%) identify the parallel operation of legacy VPN and ZTNA as a major operational burden. Maintaining two access models fragments policy, increases support overhead, and complicates the user experience. For many, this duplication has become a persistent operational tax rather than a temporary transition phase.

The Execution Gap: Parallel Operations and Skills Shortages

What are your biggest challenges in ZTNA adoption and operations?



This is the crux of the execution gap. The challenge is no longer deploying SASE or ZTNA components. Instead, it is about sustaining integration, identity alignment, and operational consistency in live environments where legacy and modern access models coexist.

As this burden grows, the focus shifts from how to deploy secure access to how it can be operated safely and consistently at scale.

Why SASE? Security and Simplicity Before Cost

Organizations are adopting SASE to restore security and operational control in increasingly complex hybrid environments. Direct cost savings are a secondary consideration; the primary drivers reflect what breaks under legacy access models in day-to-day operations.

The reasons for moving away from VPN-centric architectures are consistent and pragmatic:

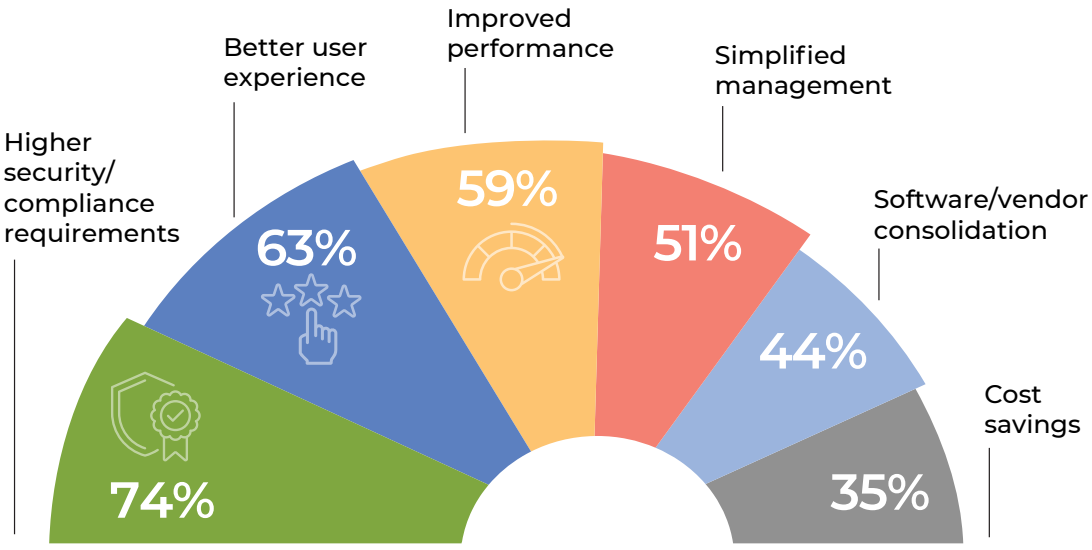
1. Security & Compliance Remain the Baseline:
Higher security and compliance requirements are the leading reasons for abandoning VPNs (76%). Enabling secure hybrid access is also the top overall driver for SASE adoption (54%). In distributed environments, perimeter-based access no longer provides sufficient control.

2. User Experience and Performance Matter:
Improved user experience is cited by 63% of respondents, while 59% highlight performance gains from eliminating VPN backhauling. Organizations are no longer willing to trade productivity and reliability for security controls that frustrate users and overload support teams.

3. Visibility Underpins Consistent Enforcement:
Improving visibility across users and applications is a primary motivator for 45% of respondents. In fragmented hybrid environments, visibility is not a "nice to have" - it is a prerequisite for enforcing security policies consistently and responding effectively when issues arise.

Drivers for moving from VPN to ZTNA

What are your main drivers for moving from VPN to ZTNA?



Cost considerations are addressed indirectly through consolidation rather than upfront savings. More than half of organizations (55%) identify vendor consolidation as their primary cost-optimization lever, often funding SASE by retiring legacy firewall and VPN estates instead of seeking incremental budget increases. Regulatory and data sovereignty pressures - particularly in the UK – reinforce this pattern. Organizations are optimizing first for secure access, visibility, and operational simplicity. Financial benefits follow through consolidation and reduced operational drag, not through standalone cost reduction.

The operating model shift: From deployment to co-managed SASE

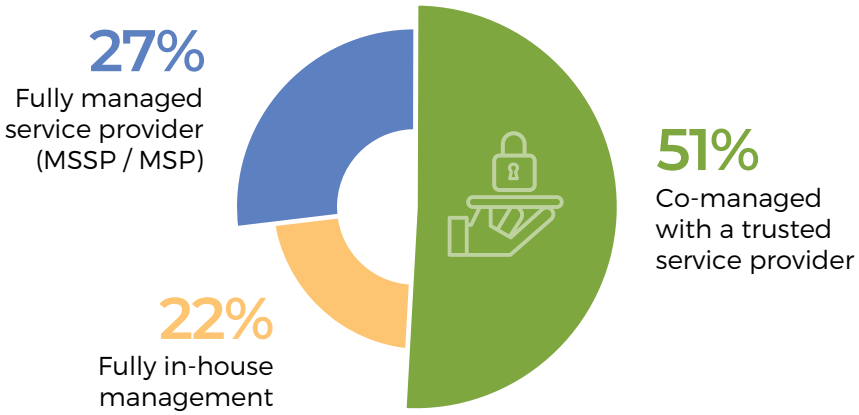
The execution gap has forced a fundamental rethink of how SASE is delivered. The question is no longer whether to adopt SASE, but how secure access can be operated predictably and sustainably under real-world conditions. The survey shows a clear shift toward shared operational responsibility. Nearly eight out of ten organizations now expect partner involvement in SASE operations.

How SASE should be delivered, support for co-managed models is decisive:

- **Co-Managed (the dominant model):** 51% organizations retain control over policy and visibility while sharing operational responsibility to manage integration complexity and sustain execution.
- **Fully Managed:** 27% preferred where internal capacity is constrained and the priority is offloading day-to-day operations to ensure reliability and compliance.
- **In-House Only:** 22% chosen primarily by organizations with mature teams and stable environments capable of sustaining continuous operational load.

The Operational Shift: Co-Managed is the Preferred Model

How would you prefer your SASE solution to be delivered?



This shift does not represent a return to traditional outsourcing. It reflects a pragmatic response to execution constraints - particularly integration complexity, skills shortages, and the burden of operating parallel access models – without relinquishing governance or control.

In practice, this means retaining ownership of policy, governance, and visibility while relying on a partner to absorb continuous operational load, including integration across hybrid environments, 24×7 monitoring, and ongoing platform maintenance. Taken together, these findings mark a pivotal shift in buyer expectations. SASE is no longer being evaluated as a product to deploy, but as a critical service that must be delivered consistently over time.

The New SASE Mandate

The survey data delivers a clear message. Buyers are no longer evaluating SASE based on architecture diagrams or feature lists. Their expectations are shaped by execution constraints, hybrid operating reality, and regulatory pressure.

Three mandates now define how SASE is evaluated:

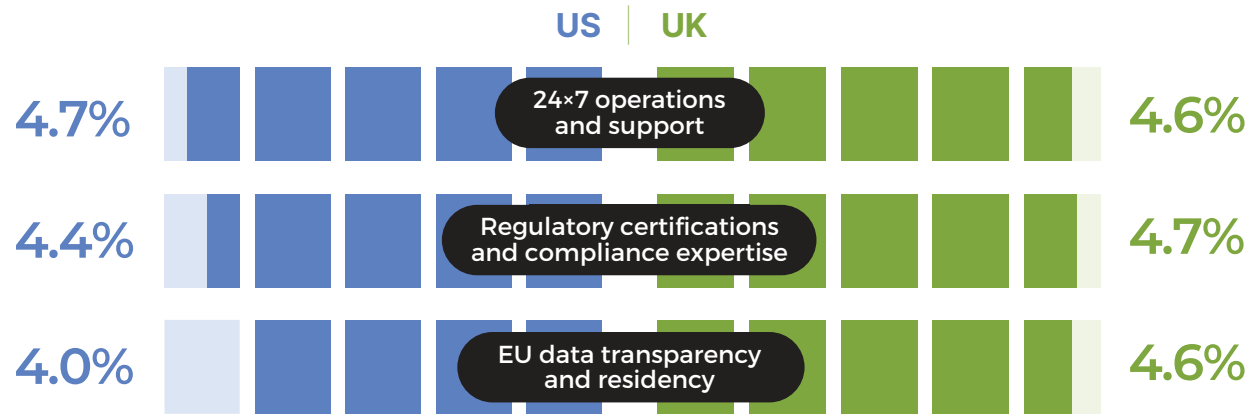
1. Visibility first, connectivity assumed:
Organizations are already hybrid and multi-cloud: over 90% secure remote users and SaaS applications, 73% secure third-party access. Connectivity is table stakes. What buyers lack is end-to-end visibility, cited by 68% as the top operational challenge. SASE platforms that lead with visibility and Zero Trust enforcement resonate more strongly than those positioned around networking.

2. Co-managed is the preferred operating model:
Only 22% of organizations want to manage SASE entirely in-house. The rest expect partner involvement to address integration complexity (55%), skills shortages (48%), and policy management overhead (42%). Buyers want SASE delivered as a continuous service, not deployed as a one-time project.

3. Compliance and residency are baseline requirements:
For organizations with UK or EU exposure, compliance and data residency are design requirements, not differentiators. UK respondents rate compliance expertise and EU/UK data transparency at 4.7 out of 5 when selecting providers. Providers who treat these as optional will not make the shortlist.

The SASE Evaluation Checklist: Compliance and Support are Critical

When selecting a network or security provider, how important are the following criteria?



The market is aligned on the destination: Zero Trust. What separates leaders from laggards is not strategy, but execution. Organizations that succeed will treat SASE as an operating model transformation and prioritize partners who offer a clear, sustainable path to consistent execution over time.

Action Plan: Closing the SASE Execution Gap

The survey findings point to a consistent pattern: organizations have committed to SASE and Zero Trust strategically but struggle to operate them at scale. Closing the execution gap requires focus on a small number of practical decisions - and an honest assessment of whether internal capacity matches operational ambition.

STEP 1: CLOSE THE VISIBILITY GAP BEFORE EXPANDING SCOPE

Visibility degrades fastest at the edges: remote users, multi-cloud traffic, and third-party access. Before extending Zero Trust to new domains, ensure observability is unified across what you already operate.

Action:

Select a high-risk third-party vendor and trace their access journey from identity to application. If correlating a third-party identity to a specific data request takes more than five minutes, the visibility gap is an operational risk.

Prioritize:

- End-to-end visibility across users, applications, and data flows
- Platforms with native data unification (vs. aggregated feeds) for consistent monitoring and cleaner alerting from core to edge
- AI-assisted detection to extend team capacity and reduce noise

STEP 2: PLAN DELIBERATELY FOR THE MIDDLE STATE

Most organizations will operate with parallel VPN and ZTNA environments for longer than expected. Treat this as a managed phase, not a temporary inconvenience.

Action:

Conduct a policy overlap assessment. Identify which user groups and applications are currently accessible via both VPN and ZTNA, then eliminate legacy VPN rules that persist only by default.

Prioritize:

- Clear criteria for which users and applications remain on VPN vs. ZTNA
- Defined migration triggers and timelines for each application tier
- Operational playbooks that reduce support overhead during coexistence

STEP 3: MATCH THE OPERATING MODEL TO EXECUTION CAPACITY

The shift toward co-managed SASE reflects a realistic assessment of what internal teams can sustain over time. Evaluate delivery models based on ongoing operational load, not just initial deployment effort.

Action:

Track your Maintenance vs. Innovation Ratio. If more than half of senior engineering time is spent on integration, patching, and firefighting rather than forward progress, the execution gap is structural.

Prioritize:

- Co-managed models to reduce risk and sustain forward momentum
- Delivery models designed for continuous operation, not one-time deployment

The SASE Partner Checklist

When selecting a managed or co-managed SASE partner, the survey data highlights five evaluation criteria:

- ☑ **Continuous operations:**
  Clear SLAs for detection, escalation, and resolution - not just uptime
- ☑ **Platform integration:**
  Native architectures that reduce policy fragmentation and integration overhead
- ☑ **Engineering depth:**
  Direct access to senior engineers, not tiered support queue
- ☑ **Compliance and residency:**
  Demand certifications (ISO 27001, SOC 2) plus clarity on data hosting jurisdiction to manage extraterritorial legal risks (e.g., CLOUD Act)
- ☑ **Partnership track record:**
  Ask for customer retention rates and average tenure as indicators of sustained execution quality.

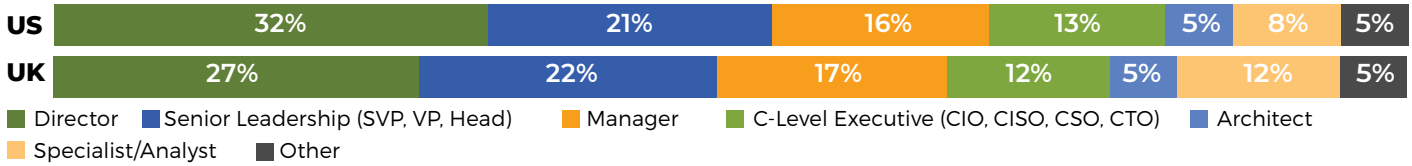
Cost still matters, but consolidation is the primary financial lever. Organizations funding SASE through retirement of legacy estates show stronger alignment between investment and outcomes than those focused on standalone cost reduction.

Methodology and Demographics

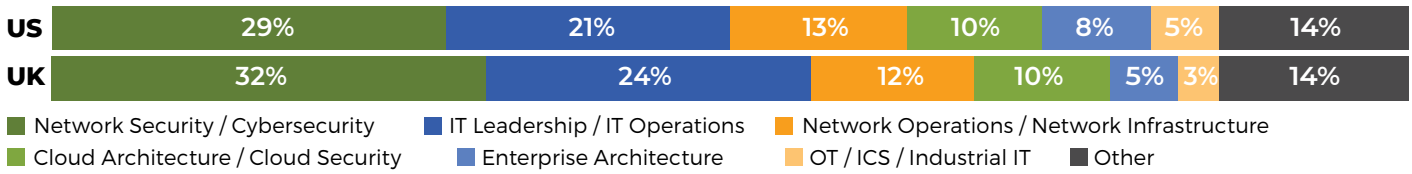
This report reflects the perspectives of senior practitioners directly accountable for making secure access work in real-world environments. The survey includes 505 senior security and IT leaders, with 263 respondents from the United States and 242 from the United Kingdom, all responsible for managing connectivity, performance, and security across hybrid environments spanning remote users, cloud applications, data centers, branch locations, and third-party access. Two-thirds hold Director-level roles or above, and nearly 70% work in senior security, IT, or network operations functions - placing them at the center of SASE and Zero Trust execution decisions.

At the aggregate level (n=505), results have a margin of error of approximately ±4.4 percentage points at a 95% confidence level.

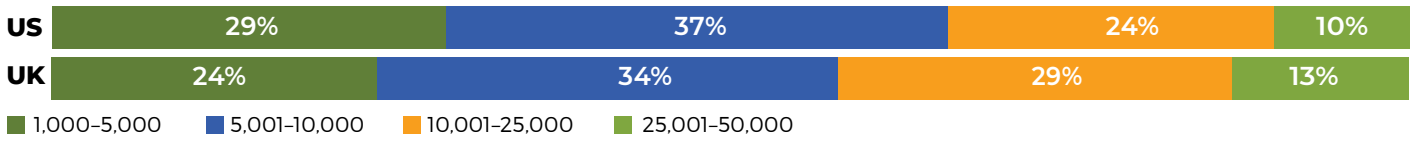
CAREER LEVEL



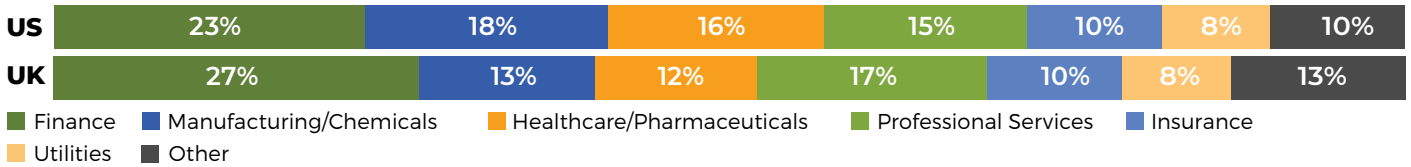
DEPARTMENT



COMPANY SIZE



INDUSTRY



Open Systems is an international provider of co-managed SASE and Zero Trust operating models, helping enterprises and organizations securely operate complex hybrid and multi-cloud environments. Founded in 1990 and headquartered in Switzerland, the company generates over USD 100 million in annual revenue and supports global enterprise customers with more than 60,000 employees across operations in more than 180 countries.

Open Systems combines cloud-native networking and security with transparent, co-managed 24×7 operations to close the execution gap many organizations face when deploying modern architectures. As a European alternative to US- and Israel-based security providers, Open Systems places strong emphasis on regulatory alignment, operational visibility and shared responsibility, enabling secure, reliable and scalable network and security operations in an increasingly distributed IT landscape.

www.open-systems.com

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 1.5