Enterprise Strategy Group™

Networking and Security Convergence: Assessing SASE Progress and Best Practices

John Grady | Principal Analyst
Jim Frey | Principal Analyst
ENTERPRISE STRATEGY GROUP

JUNE 2025

Research Objectives

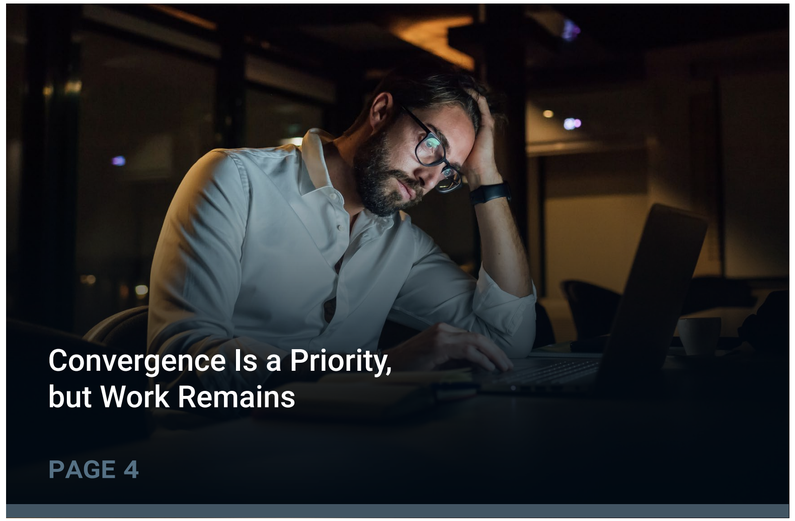
SD-WAN and security technologies have been converging via SASE to simplify the infrastructure stack and deliver better experiences and protection for users. However, questions remain as to how quickly organizations are acting to tightly couple both networking and security tools and teams. Network and security organizations have different objectives, KPIs, workflows, and vendor preferences. Taken together, this means that while convergence has an appealing value proposition, it can be difficult to implement in practice. Networking and security leaders need to understand where their forward-thinking peer organizations are in this process to plan accordingly and ultimately solve the key business challenges they face.

To gain insights into these trends, Enterprise Strategy Group surveyed 428 cybersecurity, networking, and IT professionals in North America (US and Canada) involved with secure access service edge (SASE) technology and processes.

This study sought to:

- **Understand** the challenges organizations face maintaining separate networking and security teams and tools.
- **Explore** the drivers, use cases, and key attributes organizations associate with SASE.
- **Assess** the appetite for and progress with converging networking and security functions.
- **Determine** the benefits organizations anticipate or have seen from SASE.

Key Findings

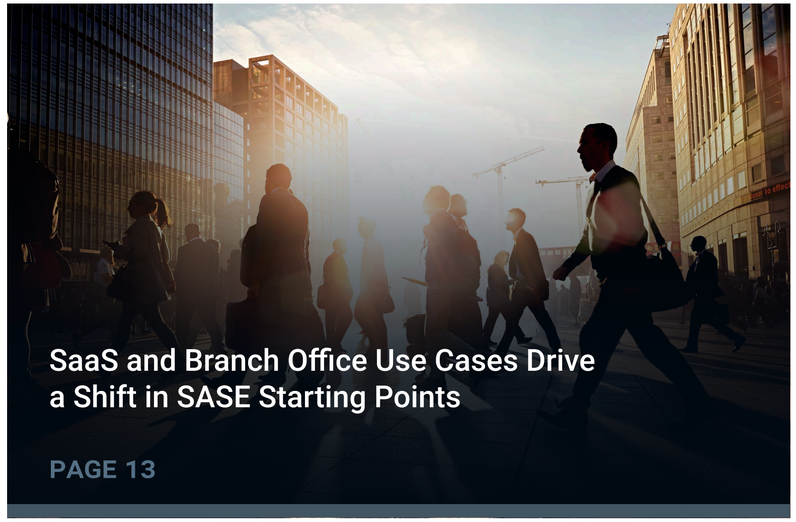


Convergence Is a Priority, but Work Remains

PAGE 4

SASE Is Becoming Ubiquitous, but Not Always Focused on Convergence

PAGE 9

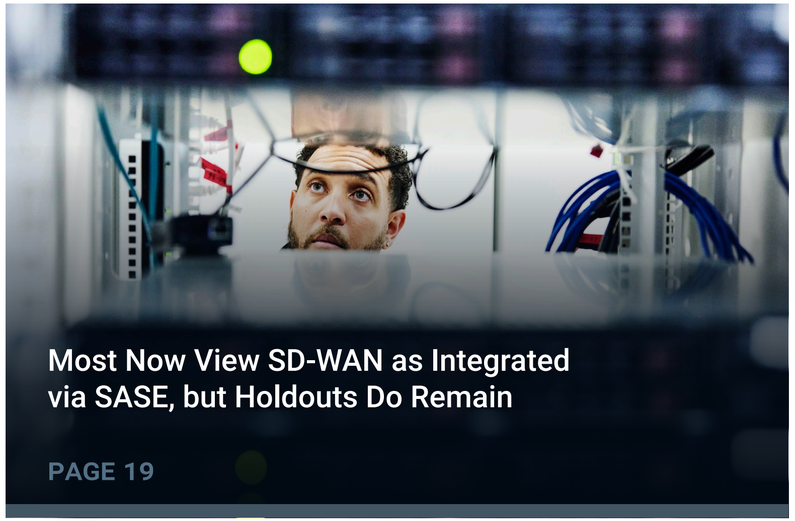


SaaS and Branch Office Use Cases Drive a Shift in SASE Starting Points

PAGE 13

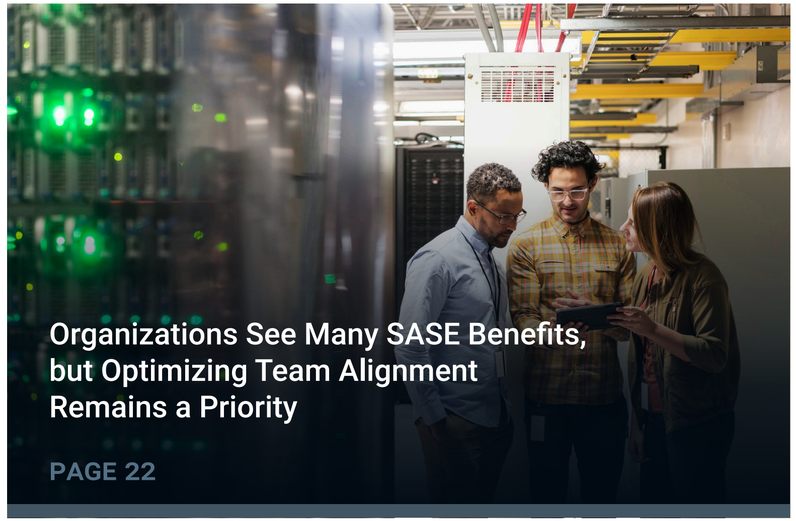
Organizations See the Value of AI SASE Solutions

PAGE 17



Most Now View SD-WAN as Integrated via SASE, but Holdouts Do Remain

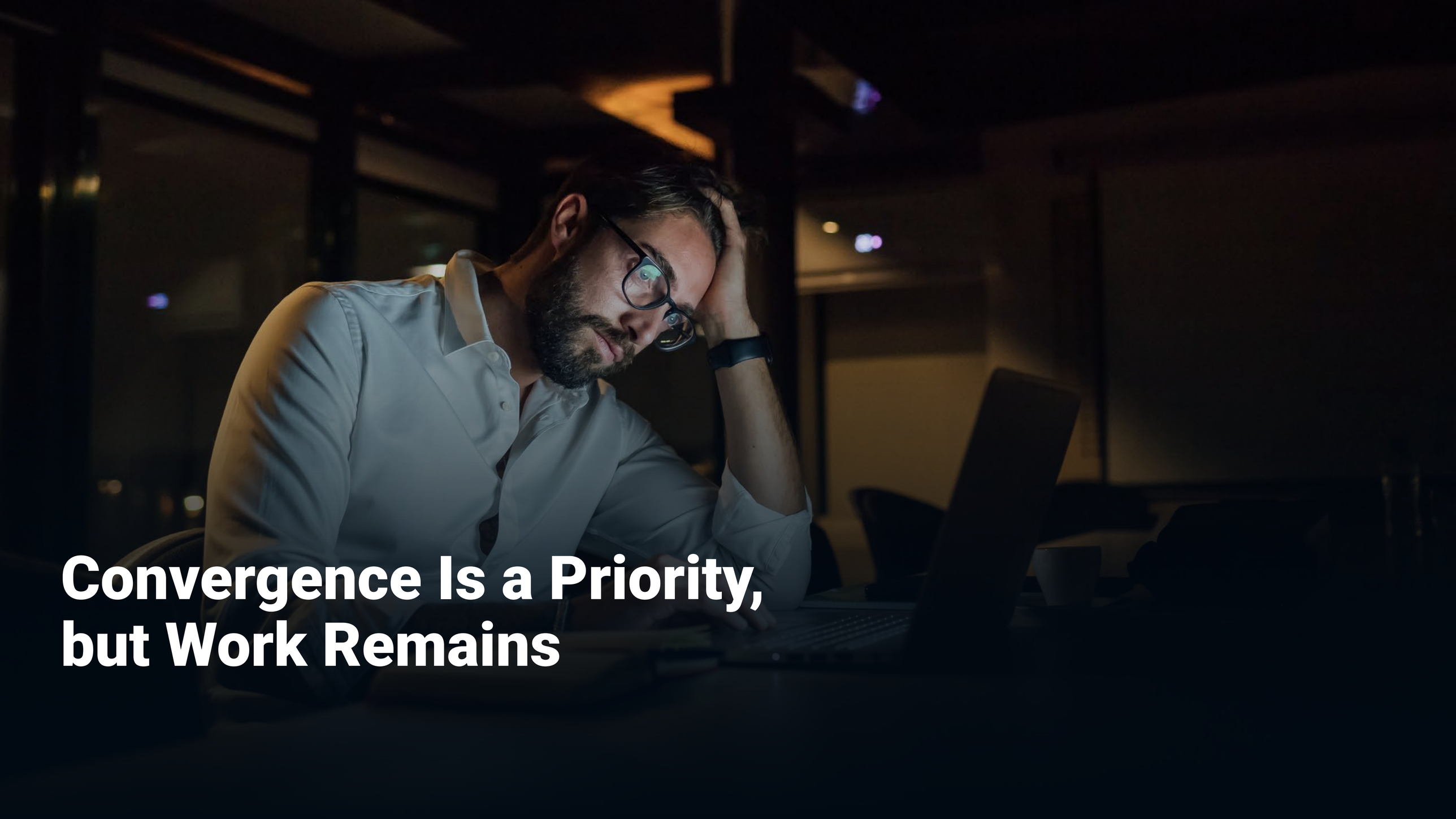
PAGE 19



Organizations See Many SASE Benefits, but Optimizing Team Alignment Remains a Priority

PAGE 22

BACK TO CONTENTS



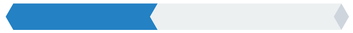
Convergence Is a Priority, but Work Remains

Separate Networking and Security Tools Create Challenges

Maintaining separate tool stacks for networking and security creates issues of many kinds, both on the operational side as well as for ensuring consistent policies and compliance. Overall, 92% of participants saw some issues, and the average respondent indicated three challenges or more. Among the most common challenges cited were ensuring proper network performance (44%), ensuring consistent policy across all users and applications (43%), and maintaining visibility across applications and devices (42%). One potential silver lining: Less than a third saw the dual-stack issue as negatively affecting root cause analysis, the lowest response of all.

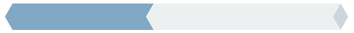
Challenges experienced with maintaining separate network and security tools.

Ensuring proper **network performance**



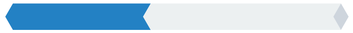
44%

Ensuring policy is consistently applied across all users and applications



43%

Maintaining visibility across applications and devices



42%

Efficiently creating and managing **policies**

41%

Maintaining consistent **user experience**

41%

Maintaining **compliance**

39%

Complexity managing **traffic routing** across locations and **security tools**

37%

Difficulty identifying the **root cause** of incidents or outages

30%

We have not experienced any challenges

8%

BACK TO CONTENTS

Siloed Network and Security Teams Also Create Issues

As was the case with separate tools, separate network and security teams lead to a variety of challenges. Nine of ten respondents (91%) indicated their organization has experienced at least one challenge with a more siloed approach. Communication (32%) and workflow (30%) issues were commonly cited.

At a higher level, the different priorities, needs, and KPIs of networking and security groups can make it harder to align on strategy, budget allocation, and vendor selection. The wide range of issues acknowledged here indicates that individual organizational experiences will vary widely, but that nearly all these potential challenges are real and worthy of recognizing as teams work to create common objectives, workflows, and processes.

Challenges experienced between individuals or teams responsible for networking and security.

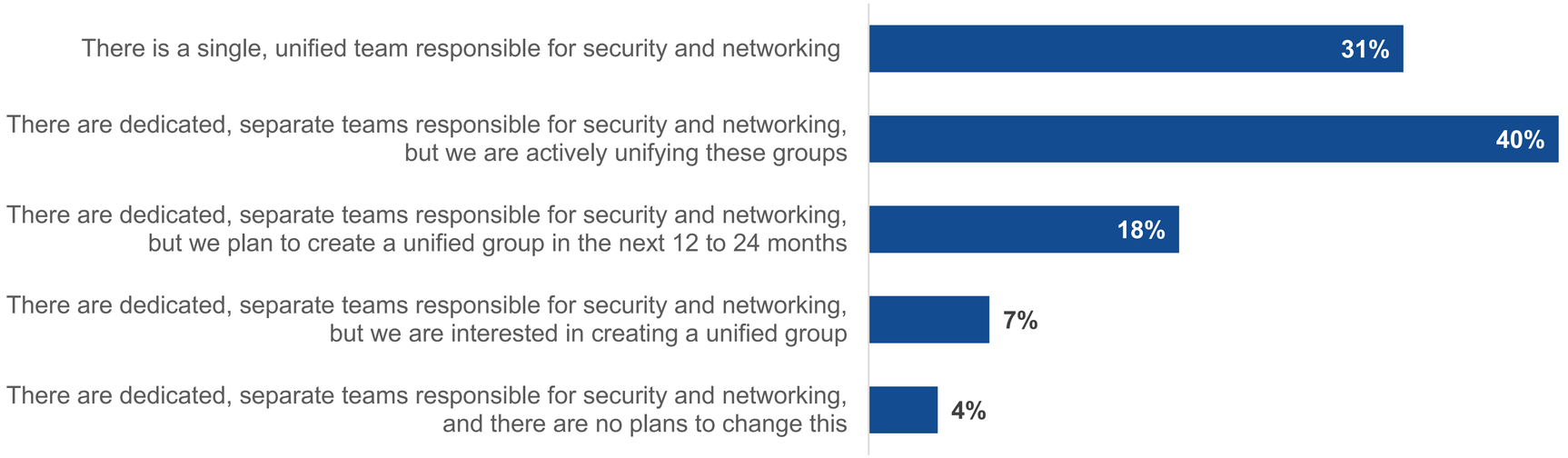
BACK TO CONTENTS

Convergence Is a Clear Priority

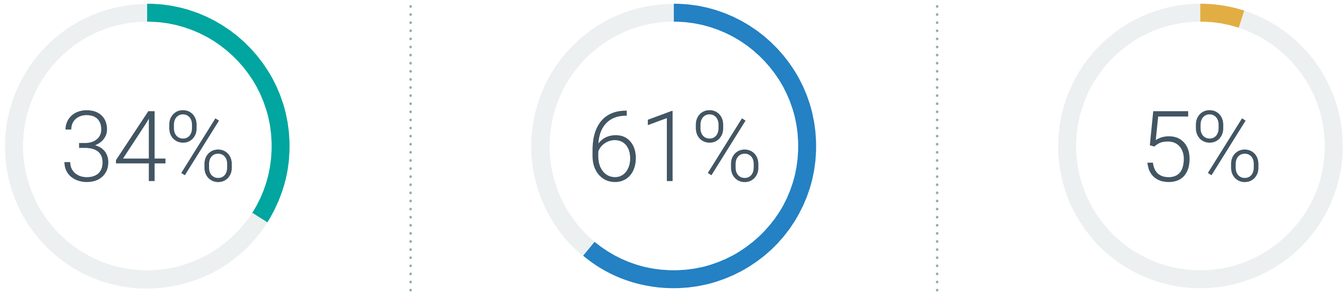
With those challenges in mind, it is unsurprising that so many organizations are in the process of converging networking and security. From an organizational perspective, less than one-third have unified networking and security teams today, but many are working toward or interested in unification. Moreover, only 4% indicate they have no interest in or plans for unifying teams.

More broadly, 34% of organizations indicated that converging networking and security technologies and processes was their top IT priority, while an additional 61% said it was among their top IT priorities. Given the wide range of other IT priorities, including ongoing digital transformation initiatives, infrastructure modernization projects, implementing AI, and more, this is a significant finding.

Team structure relative to procuring, deploying, and managing networking and security tools and technology.



Importance of converging network and security technologies and processes.



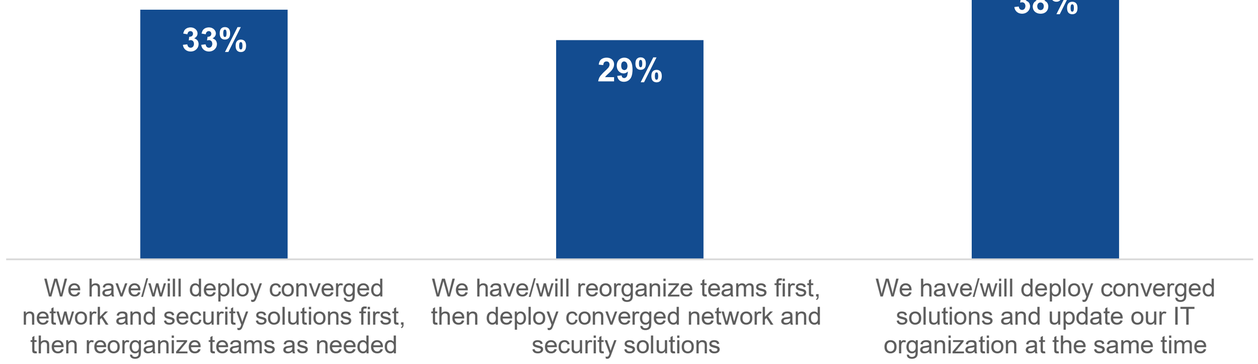
BACK TO CONTENTS

No Consensus on How to Begin Convergence

Yet while there is clear agreement on convergence at a high level, some of the specifics remain in flux. When it comes to whether technology or teams should be the initial focus, 33% said they would focus on converged solutions, 29% said teams, and 38% indicated they would tackle both at the same time.

One way to accelerate these projects and better ensure alignment is to select a champion outside of the CIO or CISO to oversee and spearhead the project. Nearly all organizations (95%) said they had followed this model, with more than half (59%) indicating it was an individual from the security team, while 33% said it was someone from the networking team. Regardless of background, this type of role can help operationalize the vision of the CIO or CISO and ensure these projects are successful in the long term.

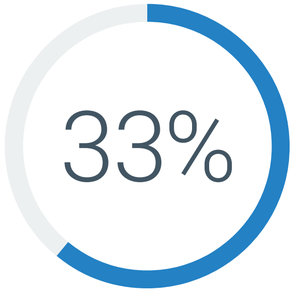
Current or expected efforts to support network and security convergence.



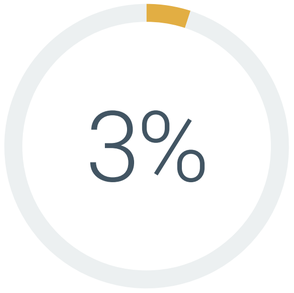
"One way to accelerate these projects and better ensure alignment is to **select a champion outside of the CIO or CISO**."

Have organizations tasked one individual with primary responsibility for leading efforts on network and security convergence?

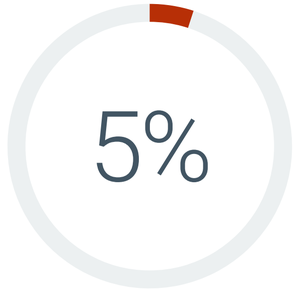
Yes, an internal individual from our security team



Yes, an internal individual from our networking team



Yes, an external individual or resource



No

BACK TO CONTENTS

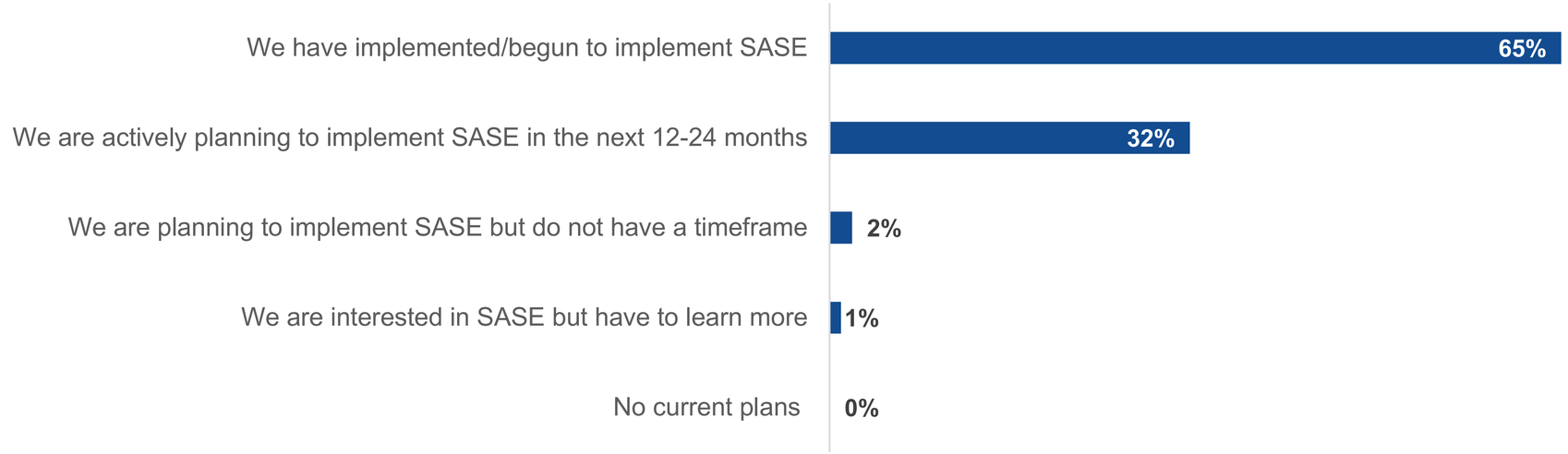
SASE Is Becoming Ubiquitous, but Not Always Focused on Convergence

Disagreement on Whether SASE Is a Convergence or Replatforming Initiative

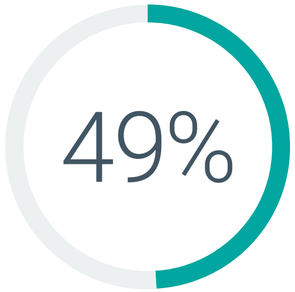
One of the best, but certainly not only, examples of networking and security convergence from a technology perspective is secure access service edge (SASE). Definitionally, SASE has always been focused on convergence, specifically of SD-WAN with secure web gateway, zero-trust network access, cloud access security brokers, and other security functions. But in reality, many organizations have focused on the network and security side separately. That said, adoption and interest are widespread, with 65% saying they have implemented or are in process and 32% planning to implement in the next 12-24 months.

Yet even now, with higher level convergence initiatives as a priority, there is a disagreement on how to think about SASE. While 49% do view it as a path to converge network and security technology, 45% see it as an avenue to redeploy existing capabilities in the cloud. This means that while SASE may be a strategic initiative, more tactical aspects still must be considered.

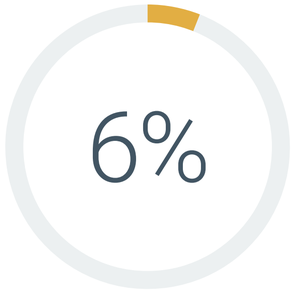
Adoption of SASE strategy.



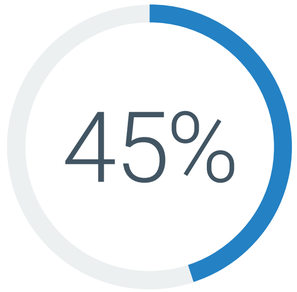
Perspective on SASE.



A path to converge network and security technologies



A path to add new capabilities that were missing from our network and/or security architecture



A path to redeploy existing network and/or security tools and capabilities in the cloud

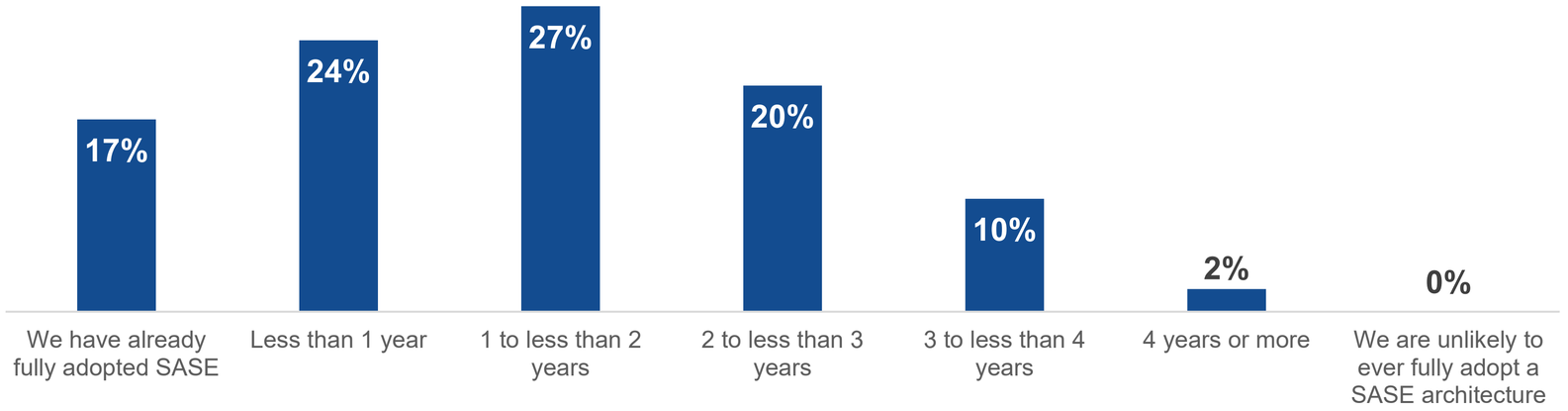
BACK TO CONTENTS

Views on What Constitutes Full Adoption of SASE Vary

Regardless of how organizations view SASE initiatives, there is agreement among most that this is an ongoing process that will take more than a year. Only 17% say they have fully adopted SASE, and 32% believe it will take at least two years to complete.

But what constitutes completion varies. The most common view is that fully integrating the different components of SASE constitutes full adoption. One in five (21%) say full coverage across all users, 20% pointed to organizational collaboration, and 19% cited using all the components of SASE. While reducing vendor count is valuable in many ways, it was clearly a lesser priority than other objectives, with only 11% selecting it as the most important consideration.

Expected length of time to fully adopt a SASE architecture.



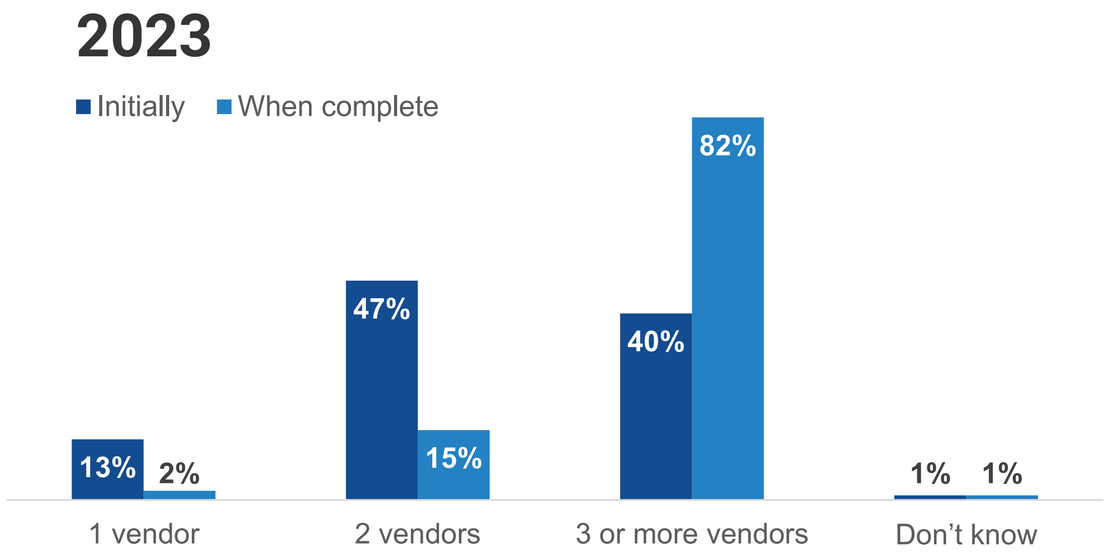
<u>Most important</u> considerations in terms of full adoption of SASE.

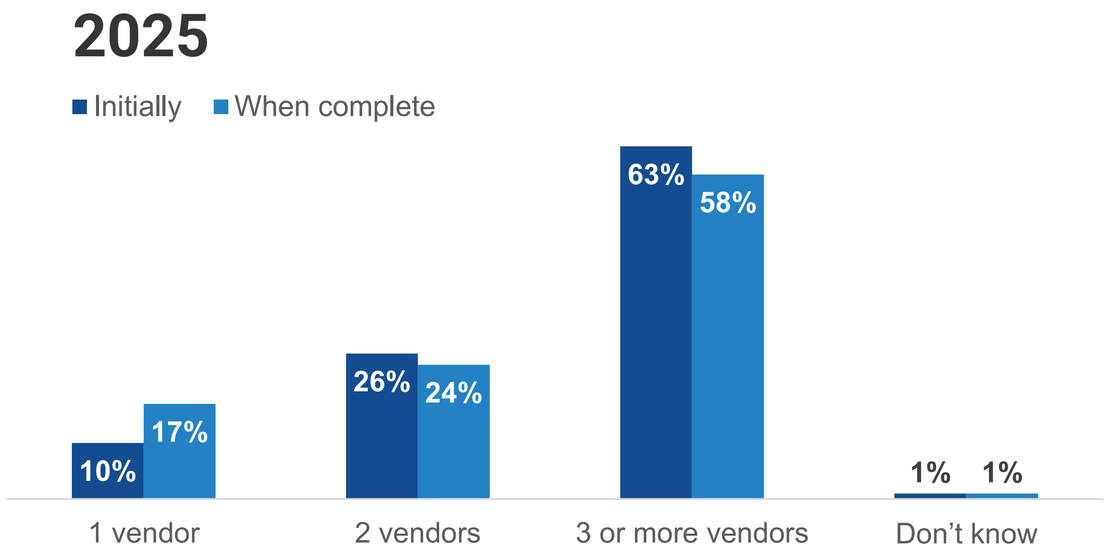
BACK TO CONTENTS

Most Still View SASE as Multi-vendor, but Fewer Than Previous Years

Views have also shifted around when it comes to single-vendor SASE. In 2023, only 2% of organizations believed they would use a single vendor when their SASE project was complete. In 2025, this rose to 17%, with an additional 24% expecting to use two vendors. This is a step in the right direction, with fewer now believing they'll use three or more vendors, but a far cry from the widespread calls for a single-vendor approach. Most telling, the number of organizations expecting to be using three or more vendors when their SASE implementation is complete fell from 82% to 58%. Those respondents with a unified networking and security team were most likely to anticipate using one or two vendors (53%). Based on the inclination toward network and security convergence, as more teams become unified, the likelihood is that the number of respondents expecting to use only one or at most two vendors for SASE will continue to increase.

Number of vendors organizations work with to support SASE architecture.





BACK TO CONTENTS

SaaS and Branch Office Use Cases Drive a Shift in SASE Starting Points

"Many organizations have been focused on **private application and internet access**."

Many Are Focusing on SaaS and Branch Use Cases

Organizations hope to support a wide range of use cases with SASE. At the highest level, these can be split into securing SaaS application access, securing and optimizing branch connectivity, securing private application access, and securing internet access.

Many organizations have been focused on private application and internet access, which may explain why SaaS access (36%) and the branch (27%) were so commonly selected. The complexity of SaaS ecosystems, with interconnected third-party applications, plug-ins, and generative AI applications, along with the increasing focus on the branch as employees return to the office are additional reasons so many respondents focus on these use cases.

Initial or most critical SASE use cases.

36% Securing **SaaS application** access

27% Securing and optimizing **branch connectivity**

19% Securing **private application** access

17% Securing **internet** access

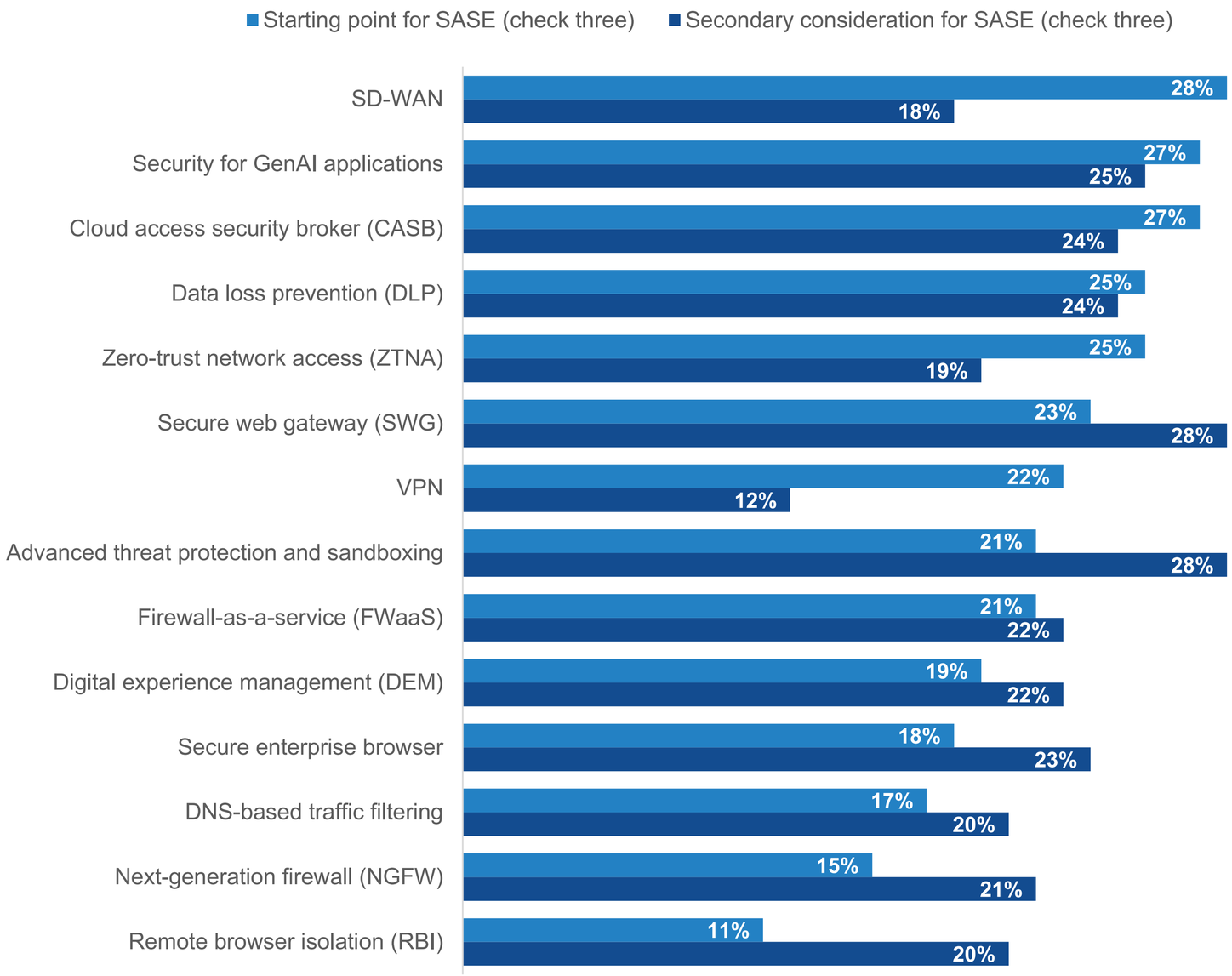
BACK TO CONTENTS

Priority Starting Points Generally Align With Use Cases

In the past, ZTNA and SWG have been toward the top of the list for starting points for SASE. Here, respondents coalesced around SD-WAN (28%), GenAI security (27%), and CASB (27%), with ZTNA (25%) and SWG (23%) coming just behind. DLP (25%) was also toward the top of the list, highlighting the importance of data visibility and control in a SASE architecture.

More emerging capabilities such as digital experience management (19%), secure enterprise browser (18%), and remote browser isolation (11%) were notably lower as a starting point but saw more responses as a secondary consideration.

Prioritization of tools used to build out SASE architecture.



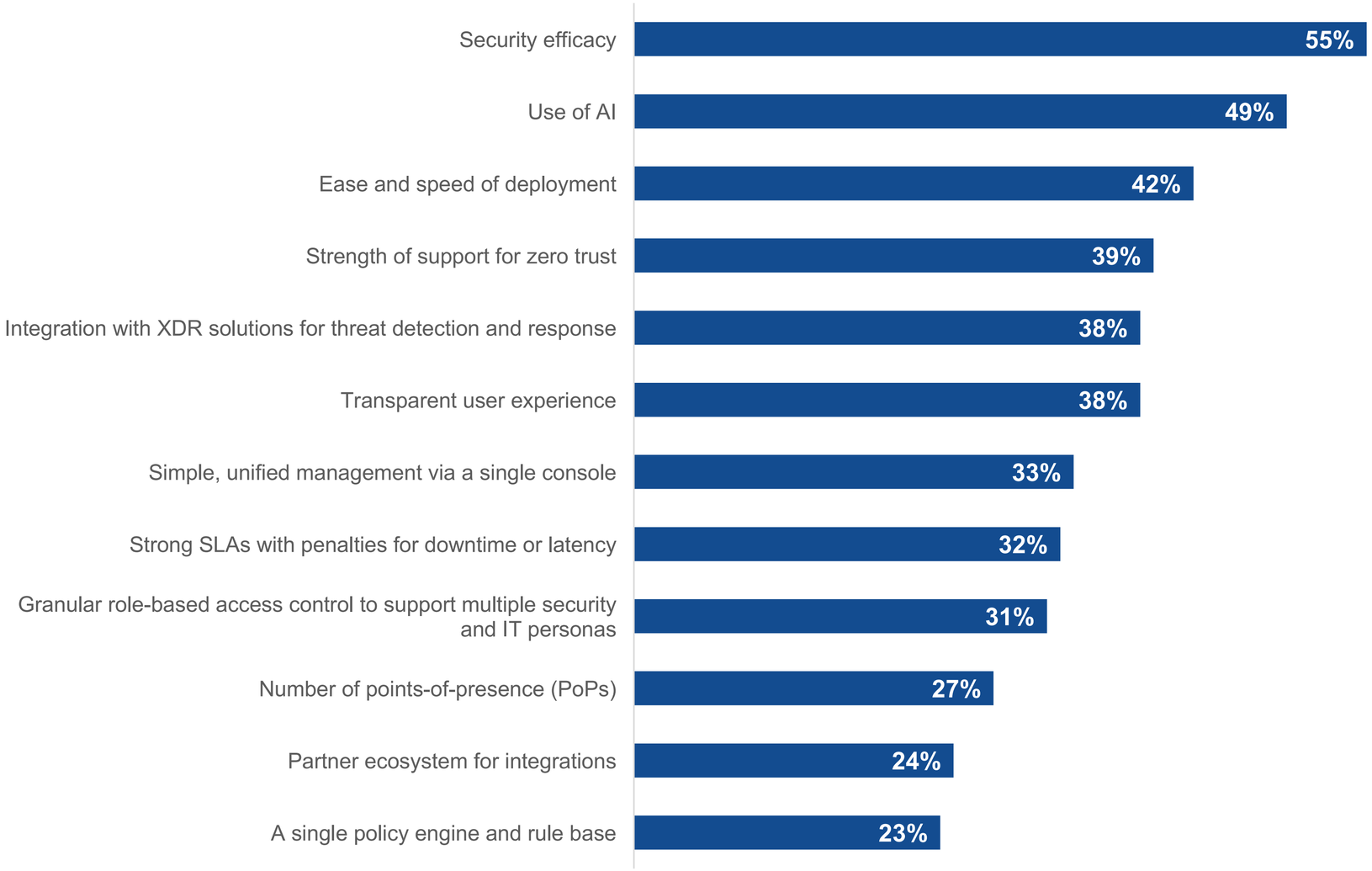
BACK TO CONTENTS

Security Efficacy and Enablement via AI Are Top SASE Attributes

As one might expect, network and security teams look for a wide range of attributes when it comes to SASE solutions. The two attributes that stood out above the rest were security efficacy (55%) and use of AI (49%). Most organizations will not sacrifice security, and AI plays a role in both enhancing security and enabling productivity and ease of use.

Simplifying operations was a key theme, with respondents noting that ease and speed of deployment (42%), simple unified management via a single console (33%), and a single policy engine and rule base (23%) are important. On the security side, support for zero trust (39%) and integration with XDR (38%) were cited. Finally, performance clearly matters, with strong SLAs (32%) and number of PoPs (27%) commonly cited.

Most important attributes when comparing SASE solutions.



BACK TO CONTENTS

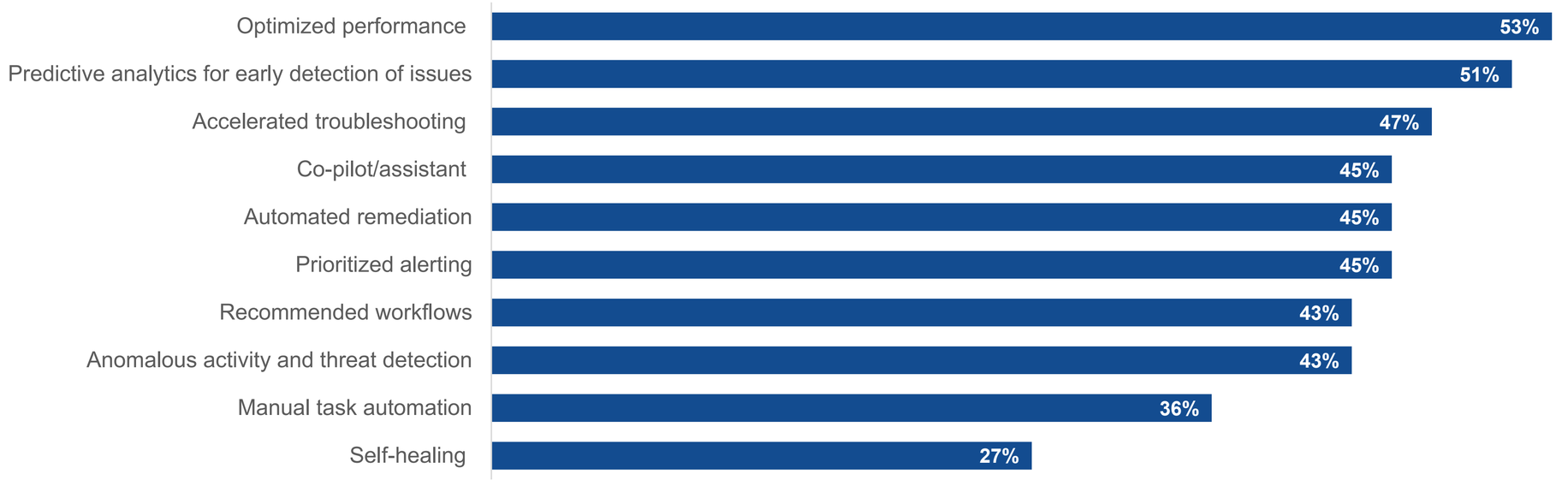
Organizations See the Value of AI SASE Solutions

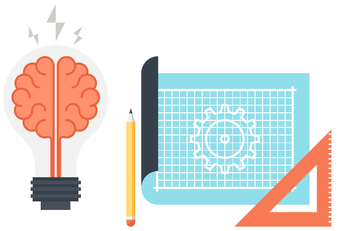
Using GenAI to Improve SASE Solutions Is Important

As seen previously, when asked what attributes are most important when comparing the SASE solutions of different vendors, nearly half (49%) cited the use of AI. There is incredible optimism around how AI can help SASE solutions deliver better outcomes for organizations. The most commonly cited important AI feature for SASE was optimizing performance (53%), followed closely by predictive analytics for early detection of issues (51%). These features can be related, as early issue detection can ensure performance by preventing or shortening an outage. Accelerated troubleshooting (47%), co-pilots (45%), automated remediation (45%), and prioritized alerting (45%) were also commonly mentioned.

But while automated remediation rated highly, manual task automation (36%) and self-healing (27%) were lower on the list, perhaps pointing to varying levels of confidence in automated actions taken by AI.

Most important AI features and capabilities for SASE environments.





Nearly half

of organizations cited the use of AI as an important SASE attribute.

BACK TO CONTENTS

Most Now View SD-WAN as Integrated via SASE, but Holdouts Do Remain

Integration of SD-WAN and SASE Strongly Preferred, but Some Organizations Retain Separate Approaches

Nearly all organizations are looking toward integrated SASE and SD-WAN solutions, split almost evenly between single and multi-vendor, but with nearly a quarter planning to continue operating existing SD-WANs independently of SASE. Smaller organizations leaned toward single vendor while larger companies leaned toward multi-vendor, reflecting relative differences in complexity. The significant number of shops running independent SD-WAN indicates that intentions to integrate are being offset by the long tail of legacy technology deployments.

SD-WAN strategies in the context of SASE.

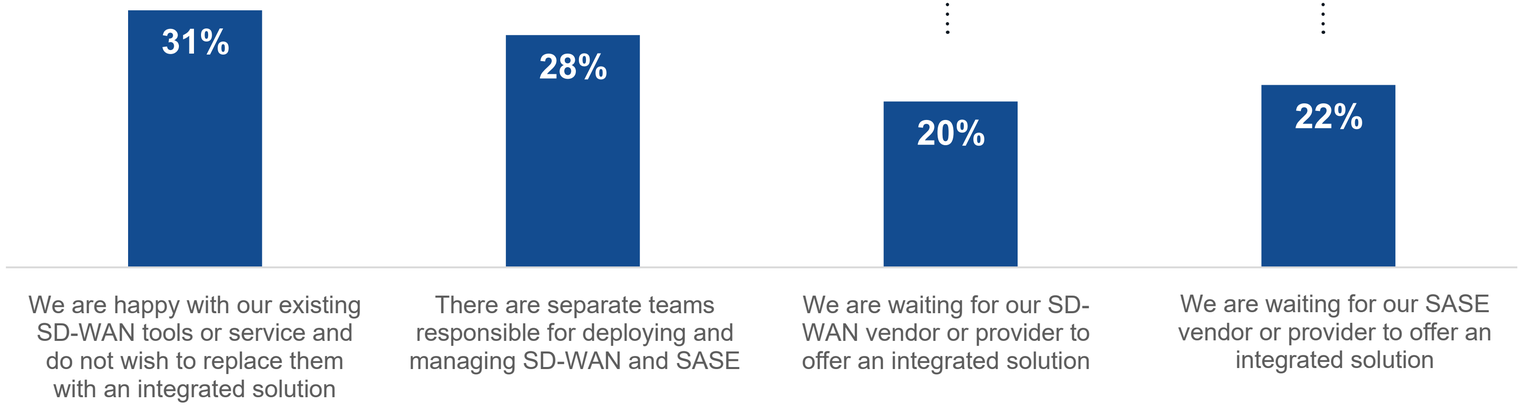
47% We plan to deploy or have deployed SD-WAN technology as part of an **integrated** multi-vendor or SASE solution

43% We plan to deploy or have deployed SD-WAN technology as a **tightly integrated** single-vendor SASE solution

24% We have an existing SD-WAN that will **operate independently** of a SASE solution

More than two in five (42%) of those continuing to operate an independent SD-WAN are simply waiting for vendors or providers to offer integration. The remaining groups are less likely to integrate, with about a third indicating happiness with the status quo and the remaining having assigned these functions to different teams.

Primary reason organization chose to maintain SD-WAN solutions separate from SASE.

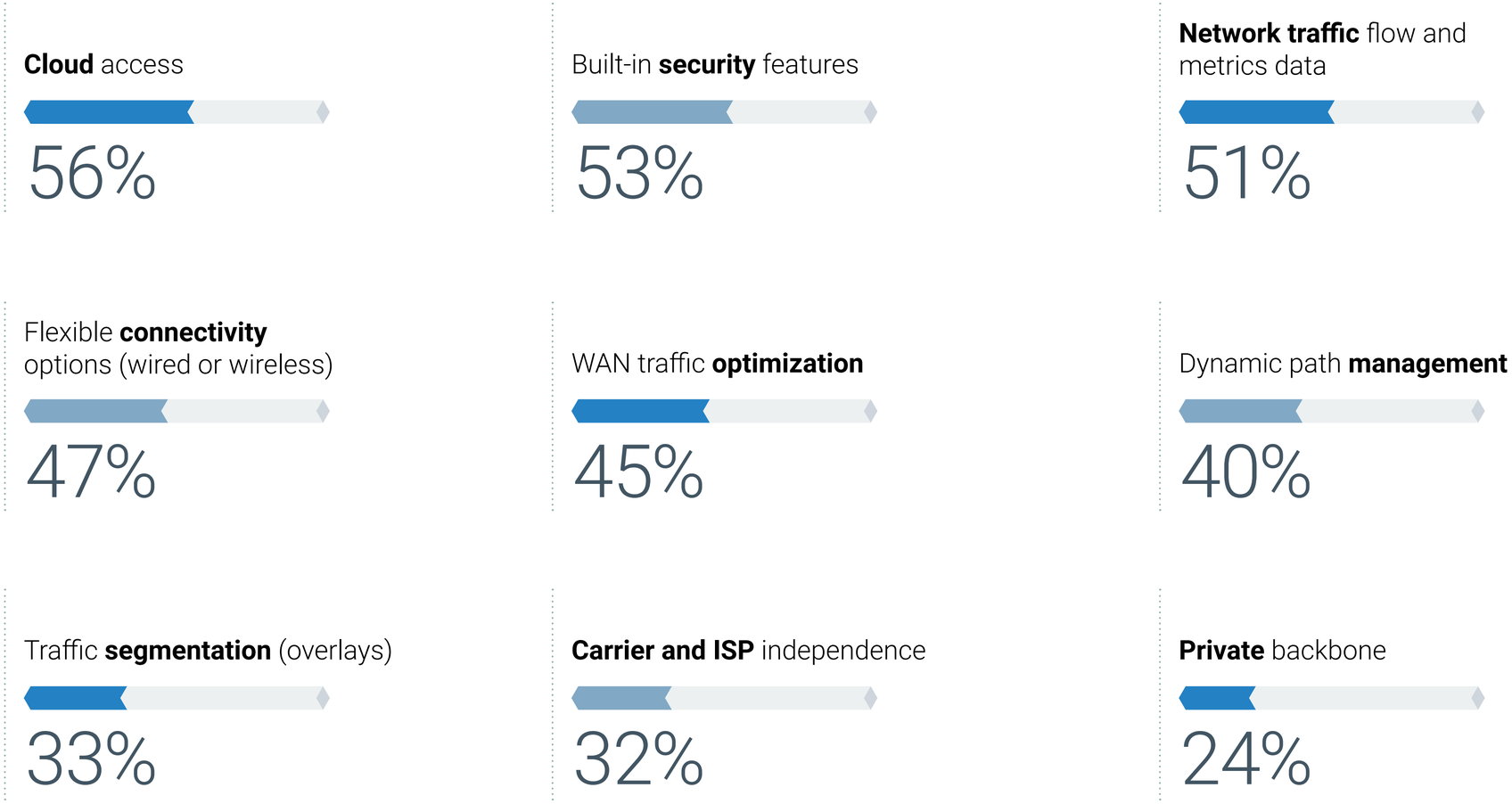


BACK TO CONTENTS

Cloud, Security, and Monitoring Emerge as Most Prized SD-WAN Features for Single-vendor SASE Integration

Technical SD-WAN capabilities are valued, but not as strongly as basic cloud connectivity, integrated security, and flow/metrics for monitoring, all of which were called out by more than half of respondents. Among more traditional features, WAN traffic optimization got an extra strong nod from large organizations (i.e., those with over 5,000 employees) (50%) and retail/wholesale shops (53%).

Most important SD-WAN features to have in a tightly integrated single-vendor SASE solution.



BACK TO CONTENTS

Organizations See Many SASE Benefits, but Optimizing Team Alignment Remains a Priority

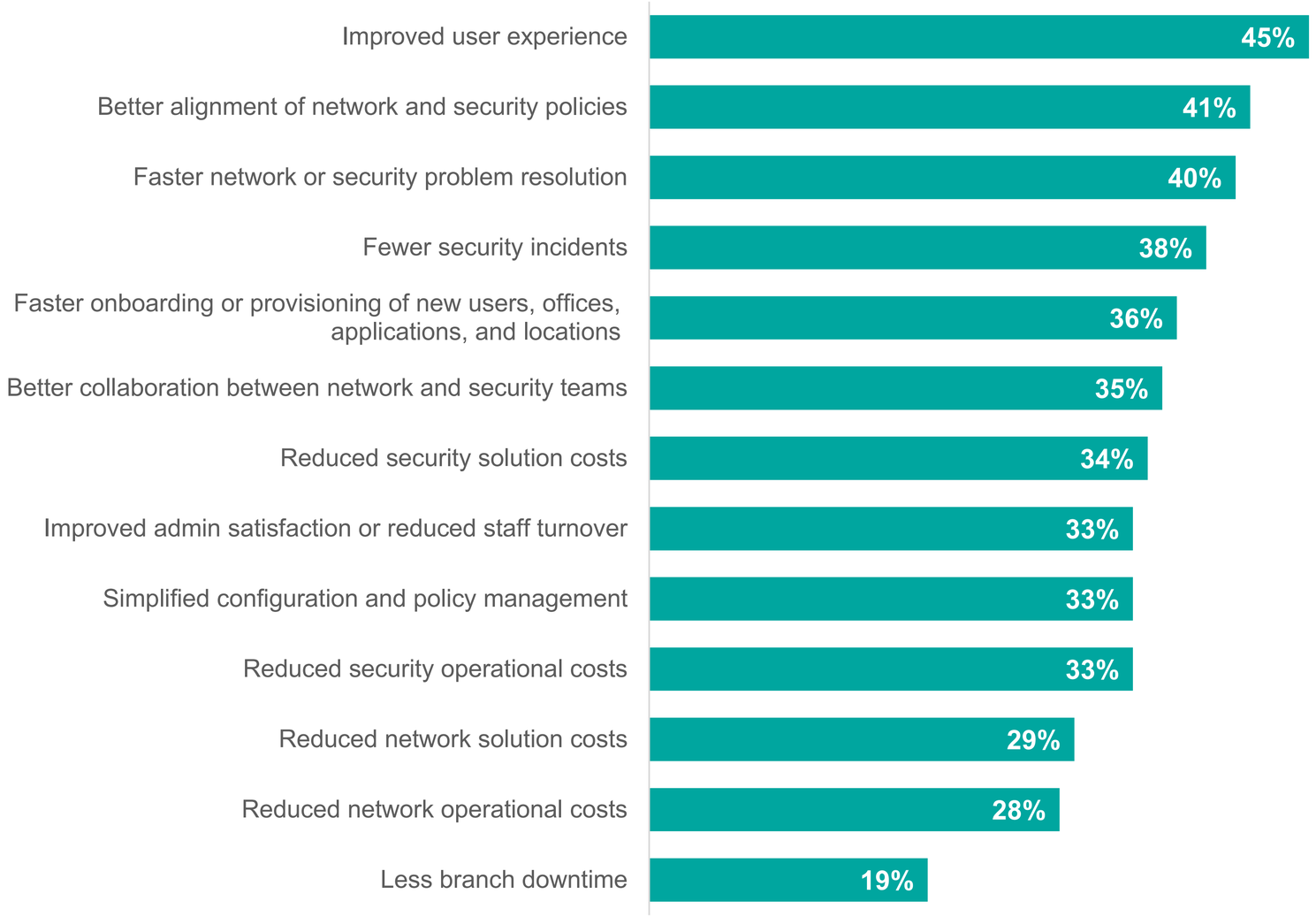
SASE Benefits Realized

While it remains early for many organizations in terms of their SASE implementation, those who have moved forward are seeing tangible benefits. In fact, on average, respondents cited at least four different benefits spanning business, security, and networking. Nearly half (45%) cited improved user experience, and 46% in total cited some sort of reduced costs (operational or solution across networking or security). Further, 38% said their organization experienced fewer security incidents, and 36% reported faster onboarding or provisioning of new users, offices, applications, and locations.

When it comes to supporting convergence from an organizational perspective, 41% said SASE had created better alignment of network and security policies while 35% noted better collaboration between network and security teams. So, while many still have work to do, teams are achieving success.

These benefits will vary by organization size. For instance, smaller organizations indicated the highest levels of achieving reduced security operations costs. On the other side, large organizations reported observing fewer security incidents at twice the rate, and faster network or security problem resolution at three times the rate of smaller organizations.

SASE benefits experienced to date.



BACK TO CONTENTS

Organizational Alignment and Services Engagement Are Clear Priorities

What's next? Regardless of where they are with convergence generally, and SASE specifically, there is a clear plan to continue to focus on organizational improvements. More than half (58%) said they plan to reorganize their IT teams to ensure better collaboration across security operations, network operations, and IT operations. Similarly, 55% expect to prioritize cross-functional collaboration specifically on networking and security.

Services also play an important role around SASE, with 51% planning to engage professional services firms for strategy or implementation, and 46% expecting to work with managed services providers. Finally, while not a top priority, nearly a third (32%) plan to reduce the number of vendors they work with.

Creating more alignment between security and networking simply makes sense. Ensuring proper protections are in place as connections are created is the only way to scale in today's environments. But striking a balance between organizational changes and technology implementation is critical.

Actions organizations will take over the next 12-18 months to implement or optimize SASE strategies.

BACK TO CONTENTS

aryaka

ABOUT

Aryaka is the leader in delivering Unified SASE as a Service, a fully integrated solution combining networking, security, and observability. Built for the demands of Generative AI as well as today's multi-cloud hybrid world, Aryaka enables enterprises to transform their secure networking to deliver uncompromised performance, agility, simplicity, and security. Aryaka's flexible delivery options empower businesses to choose their preferred approach for implementation and management. Hundreds of global enterprises, including several in the Fortune 100, depend on Aryaka for their secure networking solutions. For more on Aryaka, please visit www.aryaka.com.

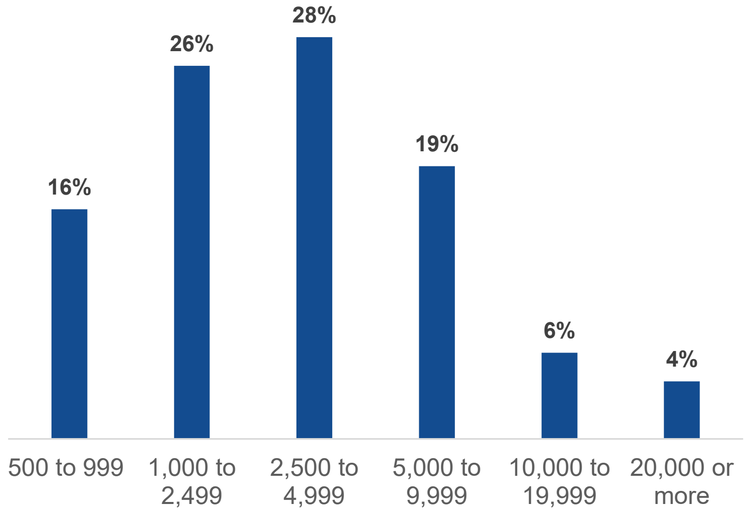
Learn more

RESEARCH METHODOLOGY AND DEMOGRAPHICS

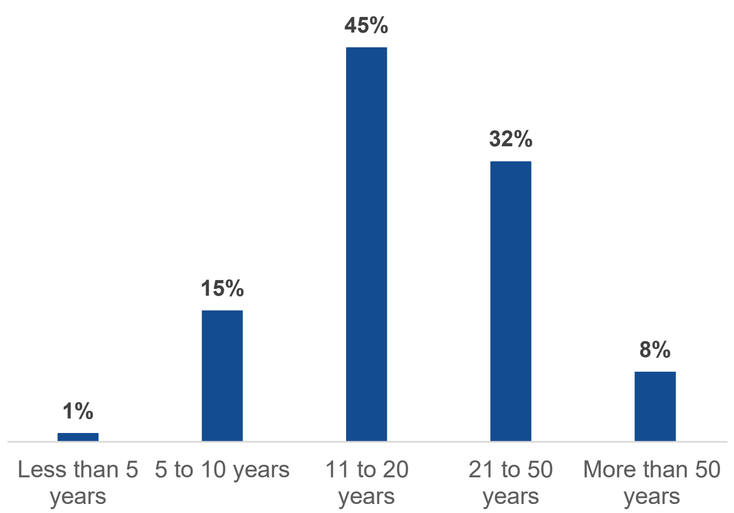
To gather data for this report, Enterprise Strategy Group conducted a comprehensive online survey of cybersecurity, networking, and IT professionals from private- and public-sector organizations in North America between April 16, 2025, and April 28, 2025. To qualify for this survey, respondents were required to be involved with secure access service edge (SASE) technology and processes. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 428 cybersecurity, networking, and IT professionals.

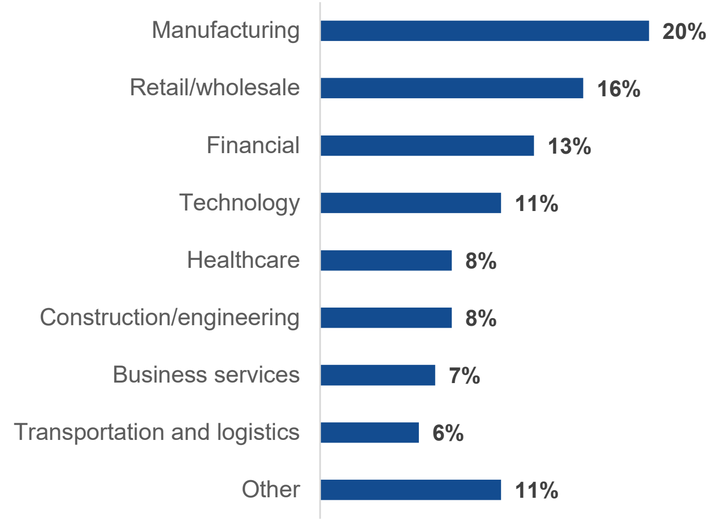
Respondents' organizations by number of employees.



Respondents' organizations by years in operation.



Respondents' organizations by industry.



BACK TO CONTENTS

Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.