



Enterprise Strategy Group | Getting to the bigger truth.™

RESEARCH HIGHLIGHTS

2021 SASE Trends

Plans Coalesce but Convergence Will Be Phased

John Grady, Senior Analyst

Bob Laliberte, Practice Director & Senior Analyst

OCTOBER 2021

Research Objectives

The amount of interest in secure access service edge (SASE) architectures has exploded over the last 18 months. Organizations struggle using traditional, on-premises-based network and security solutions to support distributed, cloud-centric enterprise environments. While this has been an increasing challenge over the last few years, the pandemic and resulting spike in newly remote workers pushed many organizations to a tipping point. At the same time, the broad applicability of SASE leads to some confusion about where to begin and which technologies are required, exacerbated by legacy organizational dynamics.

In order to gain insight into these trends, ESG surveyed 613 cybersecurity, networking, and IT professionals involved in networking and security technology and processes, with some level of familiarity with SASE, at organizations in North America (US and Canada) and Western Europe (UK, Germany, and France).

THIS STUDY SOUGHT TO:



Understand the trigger points that are influencing SASE initiatives, including the impact of remote work and zero trust, and how decision makers are prioritizing and timing purchasing decisions.



Gain insights into the planning, budgeting, purchasing, and implementation dynamics across stakeholders spanning network and security organizations.



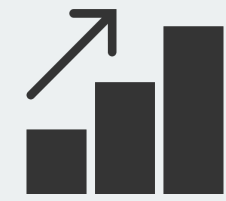
Examine the results SASE approaches have delivered regarding anticipated outcomes such as improving security, optimizing network performance, and reducing costs.



Determine the extent to which specific technologies and products support SASE now, and how that is expected to evolve over time.

KEY FINDINGS

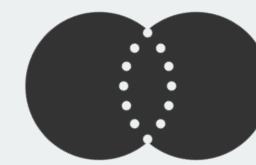
CLICK TO FOLLOW



Hybrid Work and Public Cloud Drive New Technology Adoption

SD-WAN and ZTNA Adoption Continue to Expand

PAGE 4



SASE Convergence Strategies Will Be Targeted to Start

Most Will Focus on Security or Networking Initially, and Few Anticipate a Single-vendor Approach

PAGE 8



Divergent SASE Approaches Drive Different Functional Needs

Zero Trust Is a Common Starting Point, but Little Consensus Beyond

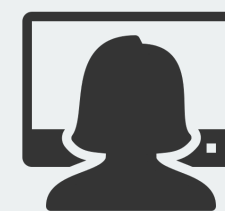
PAGE 12



Most Envision a Multi-vendor SASE Approach to Begin

Many Anticipate Adding Vendors as SASE Initiatives Mature

PAGE 15



Early SASE Adopters Report Benefits, but Work Remains

Faster Problem Resolution, Lower Costs, and Simplified Management Are Top SASE Benefits

PAGE 18



Improving Internal Alignment Will Be Critical

Security, IT, Networking, Cloud, and Risk and Compliance Teams Will All Have Input into SASE

PAGE 21

Hybrid Work and Public Cloud Drive New Technology Adoption



Enterprise Environments Continue to Become More Distributed...and Complex

Modern IT environments are becoming far more distributed. As the research illustrates, nearly all respondent organizations are using public cloud services (either IaaS or SaaS) to some extent. And it's not just the applications that are being distributed, but the workers as well, with organizations reporting that 62% of their employees will work either remotely or in a hybrid manner. The edge will also play an important role, with 71% of organizations reporting that they will need to support at least 25 remote office or branch locations moving forward. As a result of the shift toward more distributed environments, IT and security complexity increases. Organizations now have to provide secure connections to potentially thousands of locations to provide access to applications in private data centers, multiple public clouds, or numerous edge locations.



98%

use public cloud services (either IaaS or SaaS).



62%

of employees will work remotely or in a hybrid manner, on average.



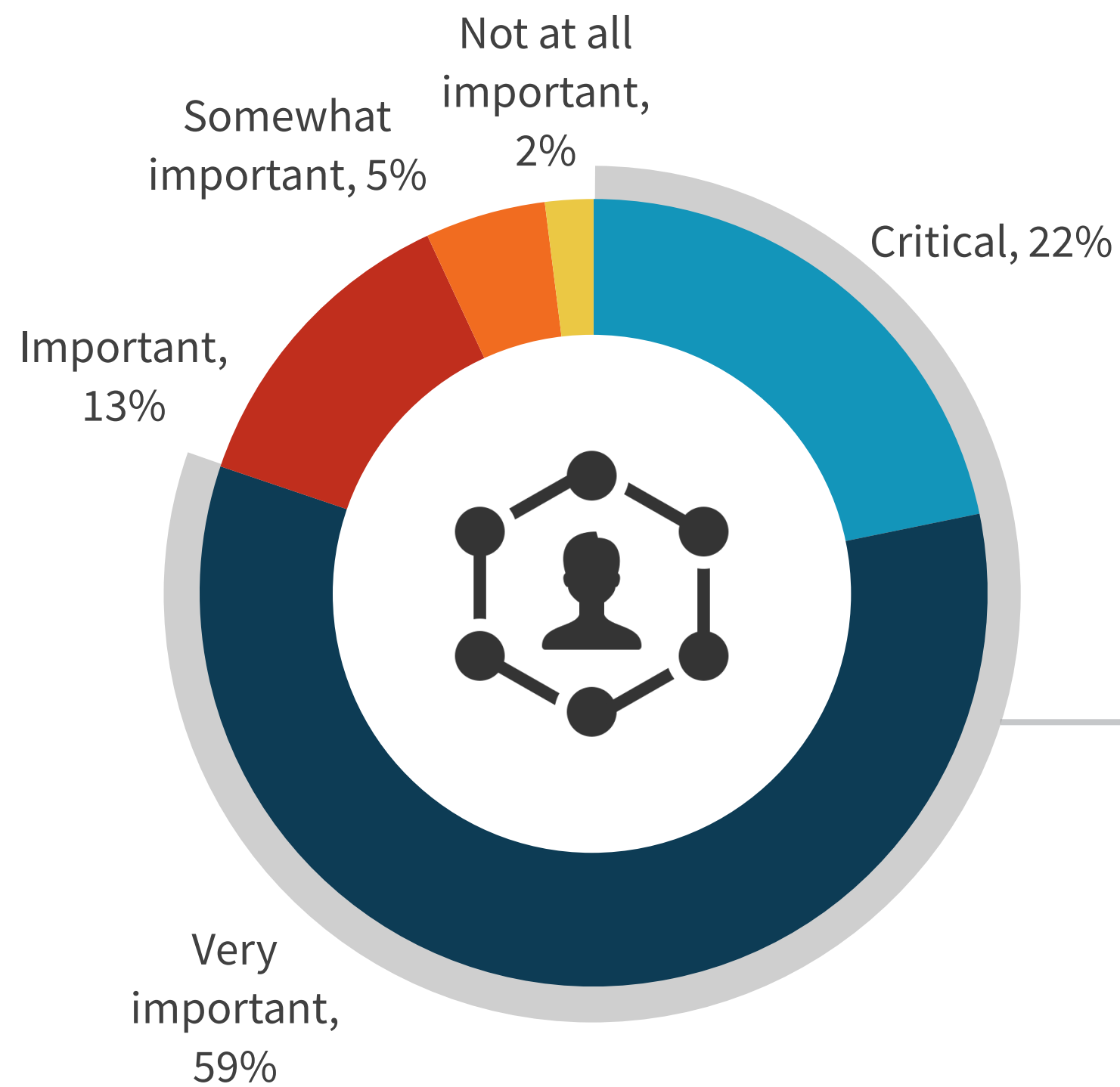
71%

of organizations will support at least 25 branch or remote office locations.

Complex Network Environments Require AI/ML for SD-WAN

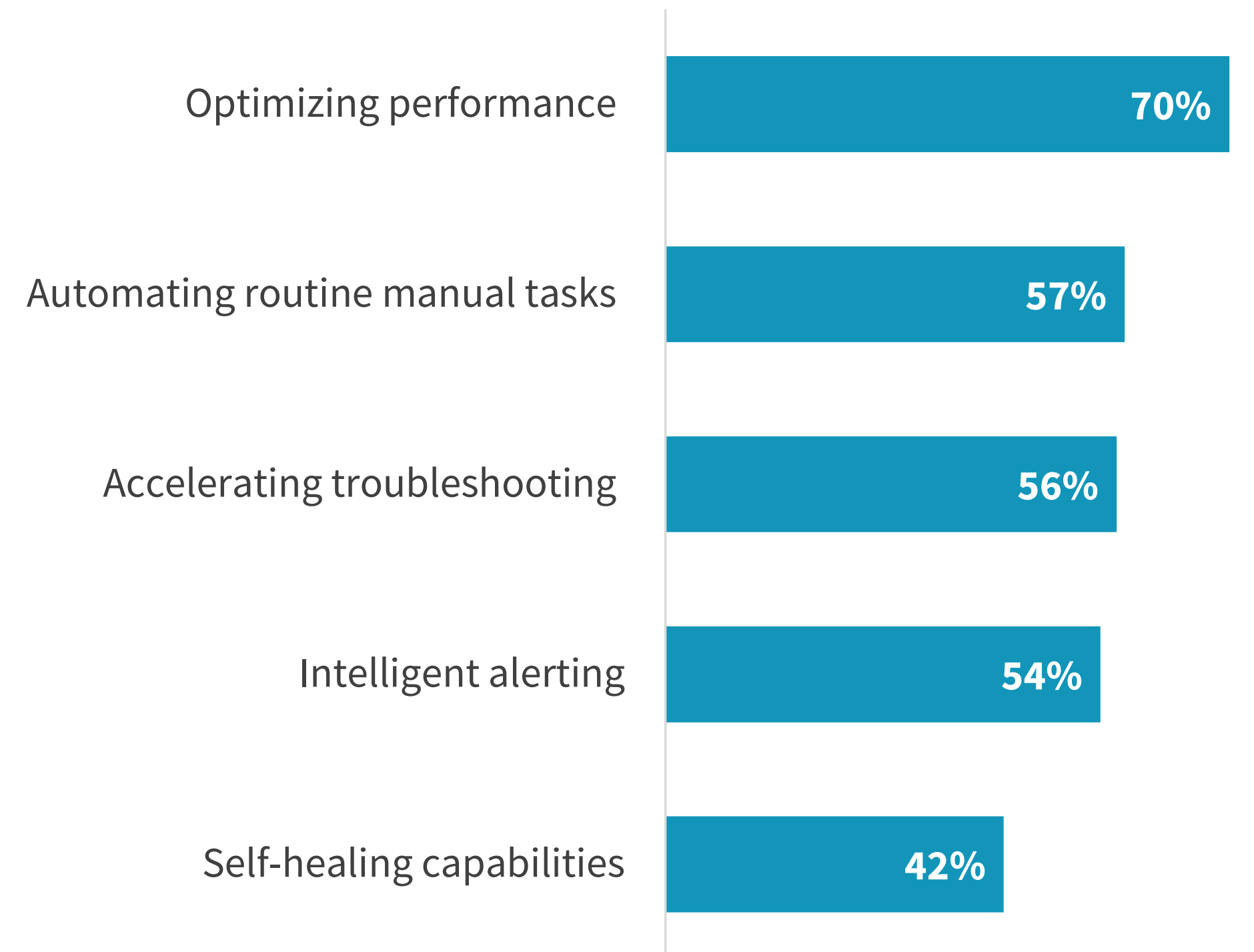
Given the increased level of complexity, human capabilities to manually optimize, troubleshoot, and make changes would quickly be exceeded. More than nine in ten respondents stated that having AI/ML capabilities in SD-WAN solutions would be important, with 81% reporting it would be very important or critical. When asked why, 70% identified performance optimization and more than half cited automating routine manual tasks (57%), accelerated troubleshooting (56%), and intelligent alerting (54%) as drivers for wanting AI/ML capabilities in SD-WAN solutions.

| Importance of AI/ML for SD-WAN.



“ 81% reporting it would be very important or critical.”

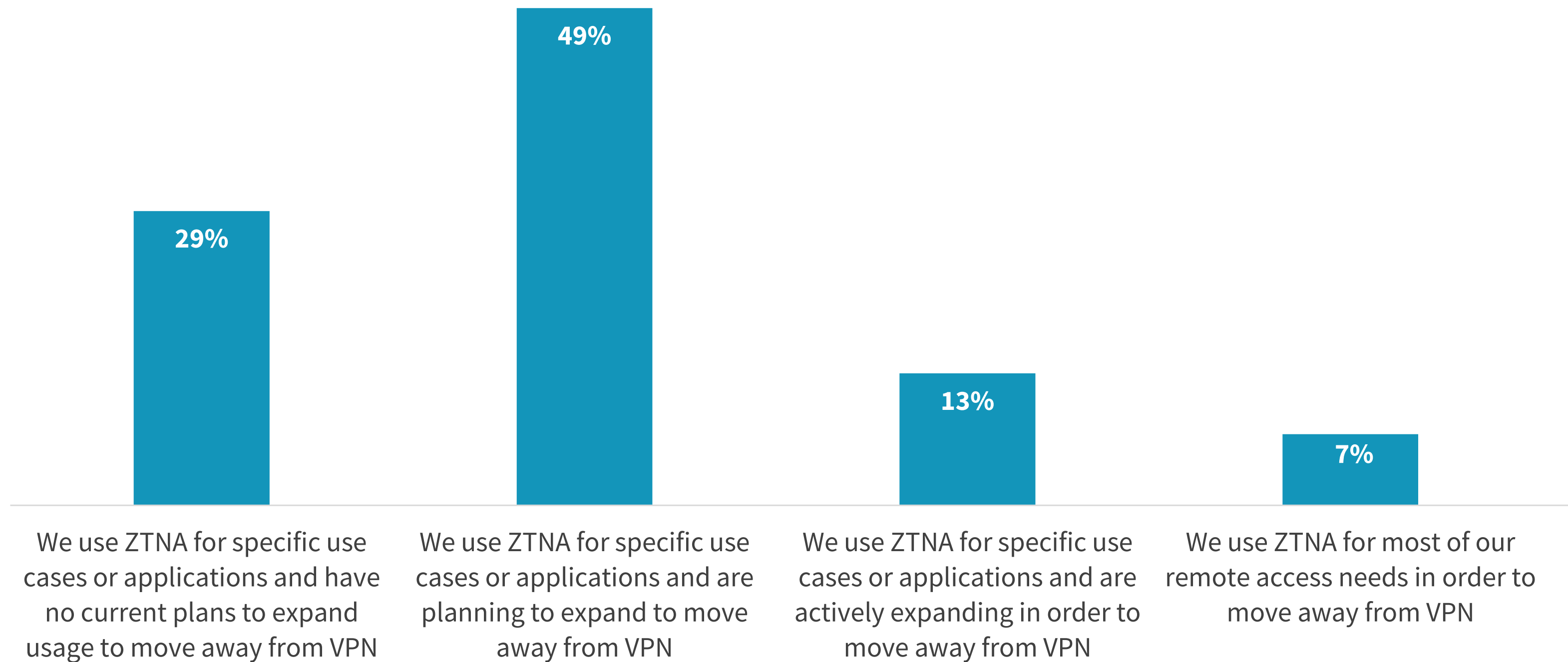
| Reasons AI/ML is important for SD-WAN.



ZTNA Is Seeing Increased Adoption to Modernize Secure Application Access

VPN solutions are widely used today, with many organizations significantly ramping up capacity at the start of the pandemic. However, creating a hub-and-spoke network back through the data center when remotely accessing cloud applications can impact performance and experience. As a result, many organizations have begun to deploy zero trust network access (ZTNA) solutions. However, most remain in the planning phase when it comes to the full-scale replacement of VPN. Specifically, 62% currently use ZTNA for specific uses but are actively expanding their usage or planning to expand their usage to move away from VPN. Only 7% of respondents have shifted to ZTNA for most of their remote access needs. Finally, slightly more than a quarter of respondents (29%) will continue to rely on ZTNA for use cases such as third-party access or M&A support while maintaining a VPN for other remote access needs.

Plans for zero trust network access tools.



“62% currently use ZTNA for specific uses **but are actively expanding their usage or planning to expand their usage to move away from VPN.**”

SASE Convergence Strategies Will Be Targeted to Start



To Begin, Most Will Take a Focused Approach with SASE

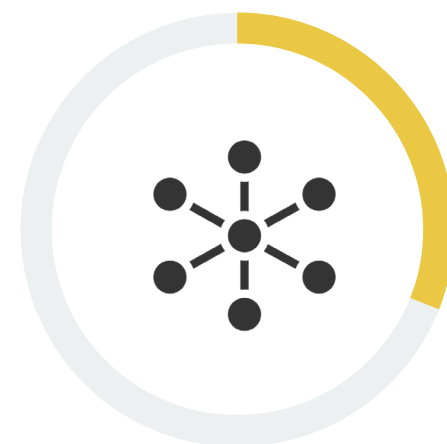
To better address the changing needs of the distributed enterprise, secure access service edge (SASE) has seen growing interest. A SASE architecture combines security functionality with WAN capabilities in a converged, cloud-centric architecture procured primarily as a service from a single or limited number of vendors. Yet while the idea of convergence is a key aspect of SASE, many organizations indicate they will take a targeted approach to start. Nearly half (48%) will begin with the security aspect of SASE in order to better secure remote and hybrid users, support zero trust initiatives, and reduce the attack surface. Roughly one-third (31%) will take a network-centric approach to SASE at the start to improve operational efficiency and optimize bandwidth utilization and connectivity. Finally, 21% of respondents indicated they would take a fully converged approach from the start to secure remote users, locations, and IoT deployments as well as support zero trust initiatives.

INITIAL APPROACH TO SASE:



48%

We will focus on the **security** aspect first



31%

We will focus on the **network** aspect first



21%

We will focus on both **security and networking** from the start

MOST COMMON USE CASES:

47% - ensure remote users' security

45% - support zero trust initiatives

43% - enable hybrid work environment

43% - reduce/eliminate internet-facing attack surface

39% - improve operational efficiency with centralized, cloud-based management

38% - optimize global connectivity

38% - create direct internet access for remote locations and users

37% - optimize bandwidth

48% - ensure remote users' security

43% - secure IoT deployments

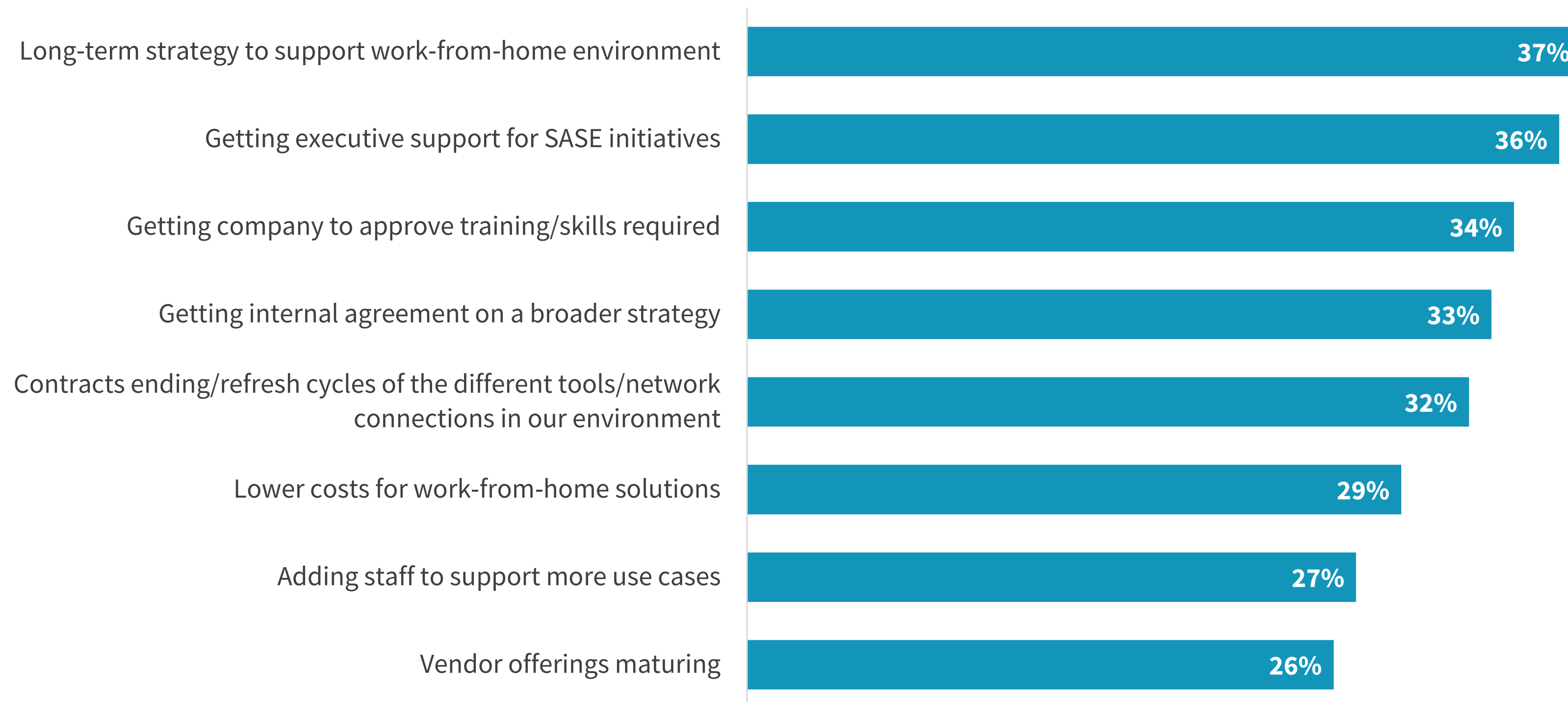
39% - support zero trust initiatives

39% - secure connectivity for remote locations and workers

SASE Expansion Will Require Internal Support and Strategies to Coalesce

Respondents cited a variety of drivers that would push them to evolve from a targeted SASE approach toward a broader, fully converged model. Aligning internal strategies and resources was at the top of the list, with clarity on long-term work-from-home strategies, executive support for SASE, and approving training and skills all ranking highly. Organizations may also be waiting to expand their SASE initiative until current contracts expire or refresh cycles come due, as noted by 32% of respondents. Finally, SASE remains a nascent market with both net new vendors and well-established vendors offering new technologies. In both cases, some organizations will take a wait-and-see approach to ensure the tools that support SASE architectures can deliver the capabilities necessary for the initiative to be successful.

| Top drivers for expanding SASE strategies.



“Aligning internal strategies and resources was at the top of the list, with clarity on long-term work-from-home strategies, executive support for SASE, and approving training and skills all ranking highly.”

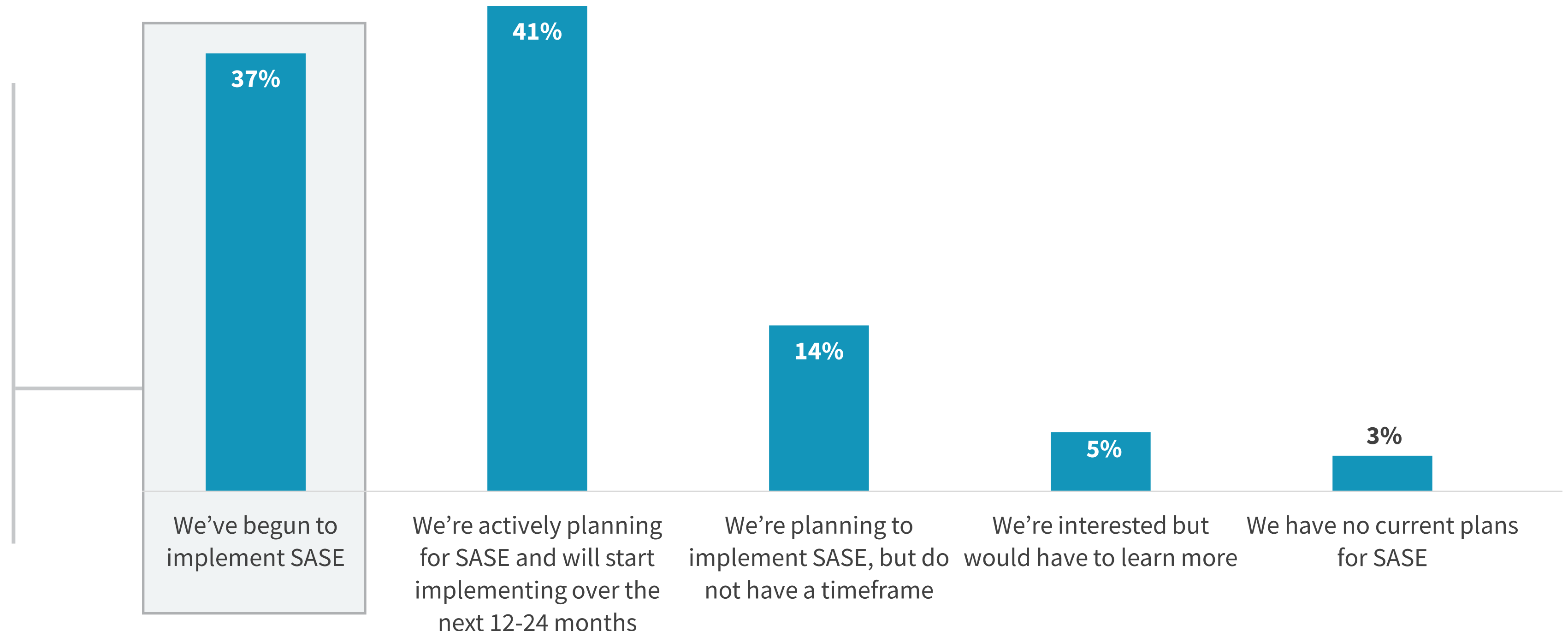
There Is Increasing Connection between SASE and Zero Trust

Despite the different approaches to SASE that exist, nearly all organizations either have begun to implement, are planning for, or are interested in SASE. While most remain in the planning or interest stage, the fact that more than one-third (37%) have begun to implement SASE less than 2 years after its introduction is a testament to the growing need for network and network security modernization.

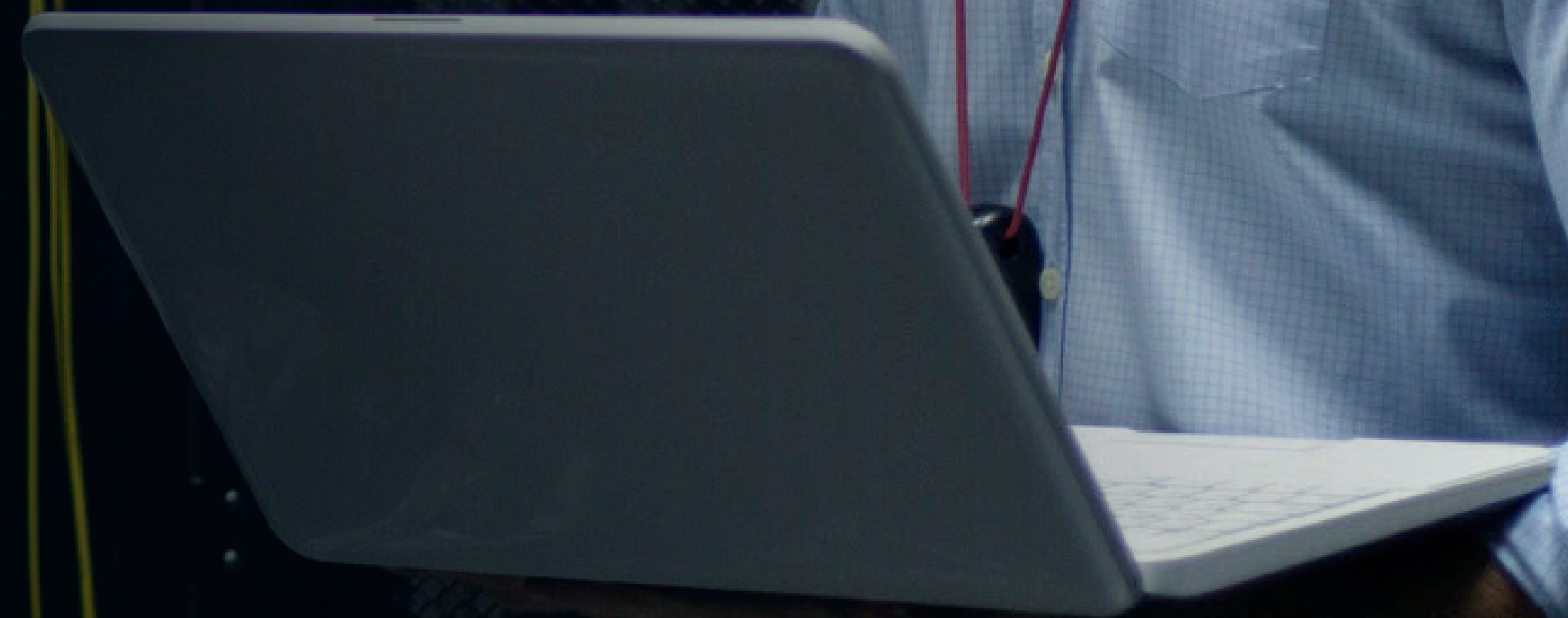
An important connection uncovered in the research was the relationship between zero trust and SASE. In fact, among respondents with a broad zero trust initiative underway, 61% indicated they had begun to implement SASE. ZTNA has always represented an area of overlap between SASE and zero trust, yet the common focus on identity, data, and granular access continues to drive these two initiatives closer together. Further, those organizations with more mature zero trust initiatives are more likely to have better internal alignment across all the groups and roles that must work together to support a SASE initiative.

| SASE adoption progress.

“ Among respondents with a broad zero trust initiative underway, **61% indicated they had begun to implement SASE.**”



Divergent SASE Approaches Drive Different Functional Needs

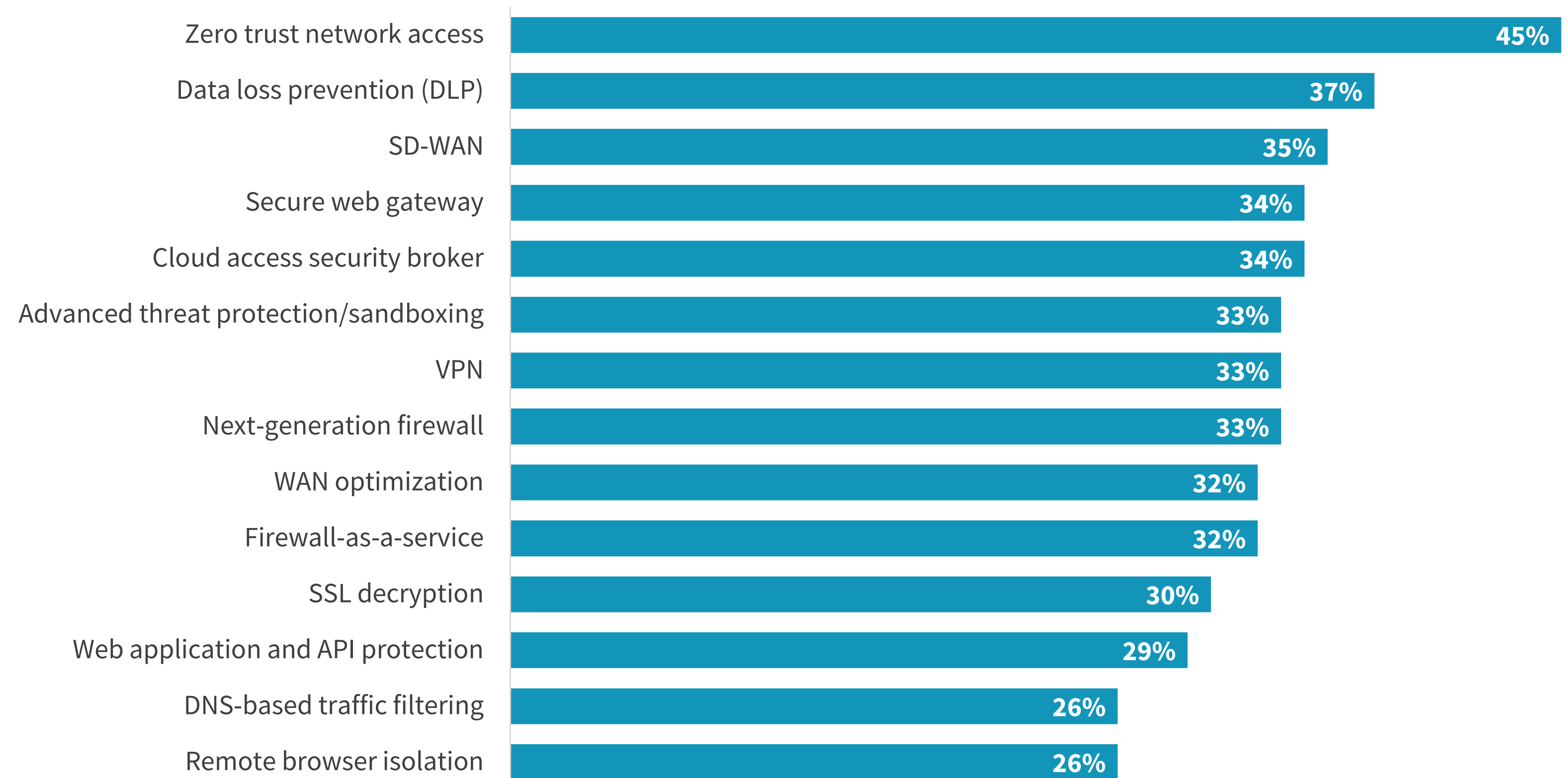


A Wide Set of Capabilities Is Required to Support SASE

There was limited consensus among respondents regarding which tools are the best starting point for SASE. The most common answer given by nearly half (45%) of respondents was zero trust network access. However, a broad middle ground exists beyond that, due in large part to the different approaches organizations may take and use cases they may seek to support. Securing a hybrid workforce may require ZTNA, DLP, CASB, and SWG, while providing secure connectivity for remote locations and users may require SD-WAN, firewall-as-a-service, and DNS-based traffic filtering. As a result, there is no “right” answer for where to start a SASE journey, making it more important to develop a long-term strategy with short-term milestones to support both current and future needs.

“ There is no ‘right’ answer for where to start a SASE journey, **making it more important to develop a long-term strategy with short-term milestones.**”

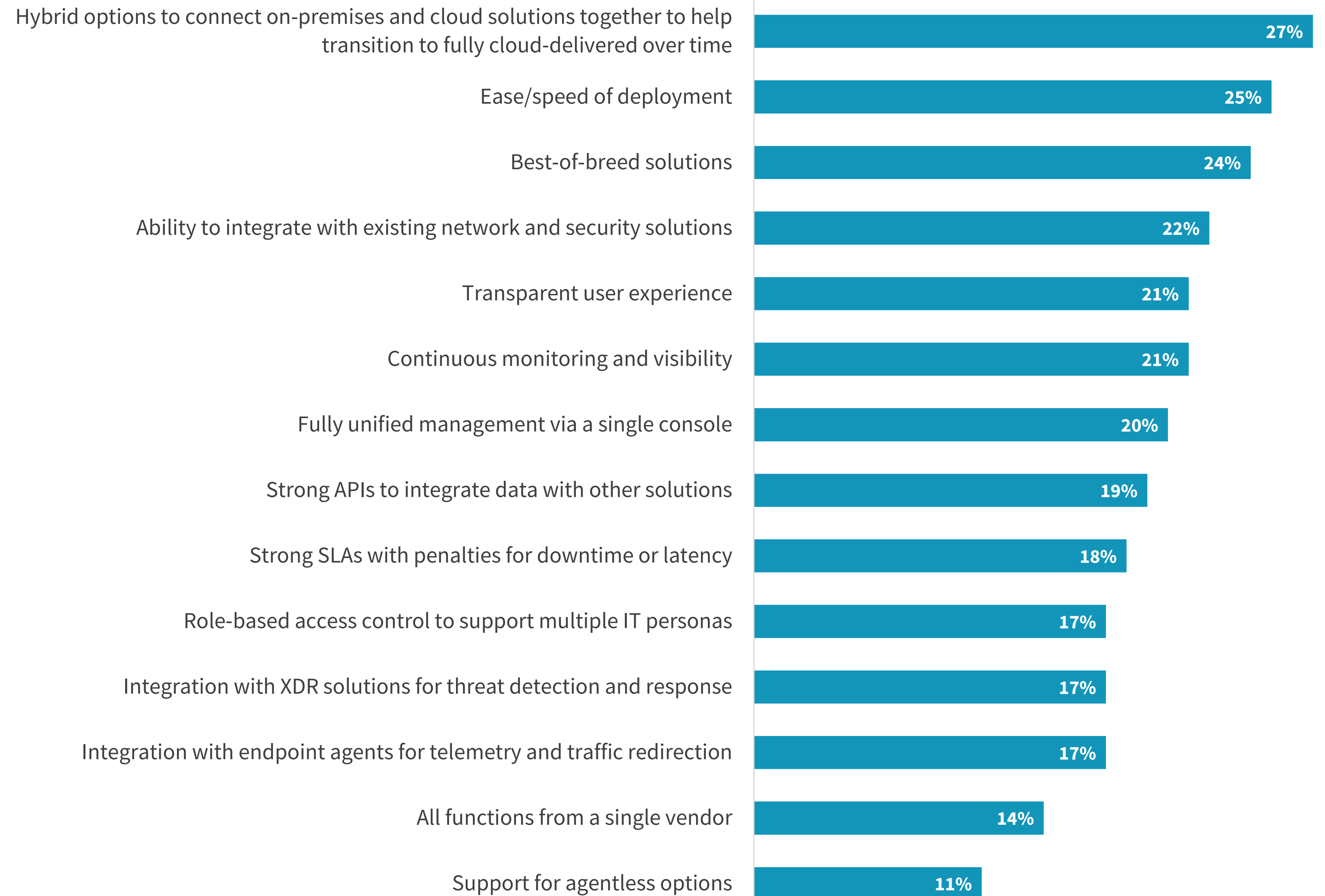
| Tools considered starting points for building out SASE architecture.



Hybrid Options and Integrations Remain Important

Similarly, organizations have different opinions when it comes to SASE solution attributes. In terms of those identifying attributes as most critical, 27% of respondents cited hybrid options to support a transition to fully cloud-delivered over time. Ease/speed of deployment was cited by 25% of respondents, while best-of-breed solutions were noted by 24%. This reinforces the fact that when it comes to SASE, users want the convenience of a platform, without sacrificing on performance or efficacy. Also of note is the fact that only 14% of respondents agreed that the ability to consume all functions from a single vendor is a critical attribute.

| Critical SASE solution attributes.



A group of men are seated around a conference table in a meeting room. The man in the foreground, wearing glasses and a blue denim shirt, is pointing towards the right side of the frame. Other men are visible in the background, some looking towards the same direction. The room has large windows and a modern, professional atmosphere.

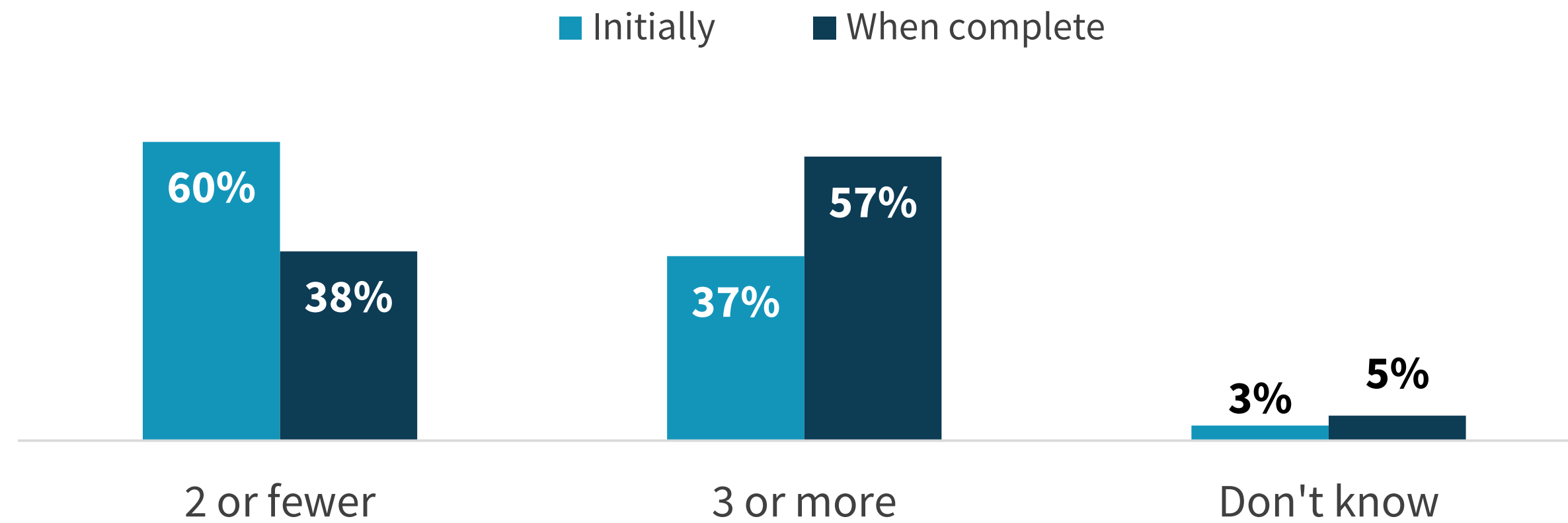
**Most Envision a
Multi-vendor SASE
Approach to Begin**

Rather Than Consolidating, Some Anticipate Adding SASE Vendors Over Time

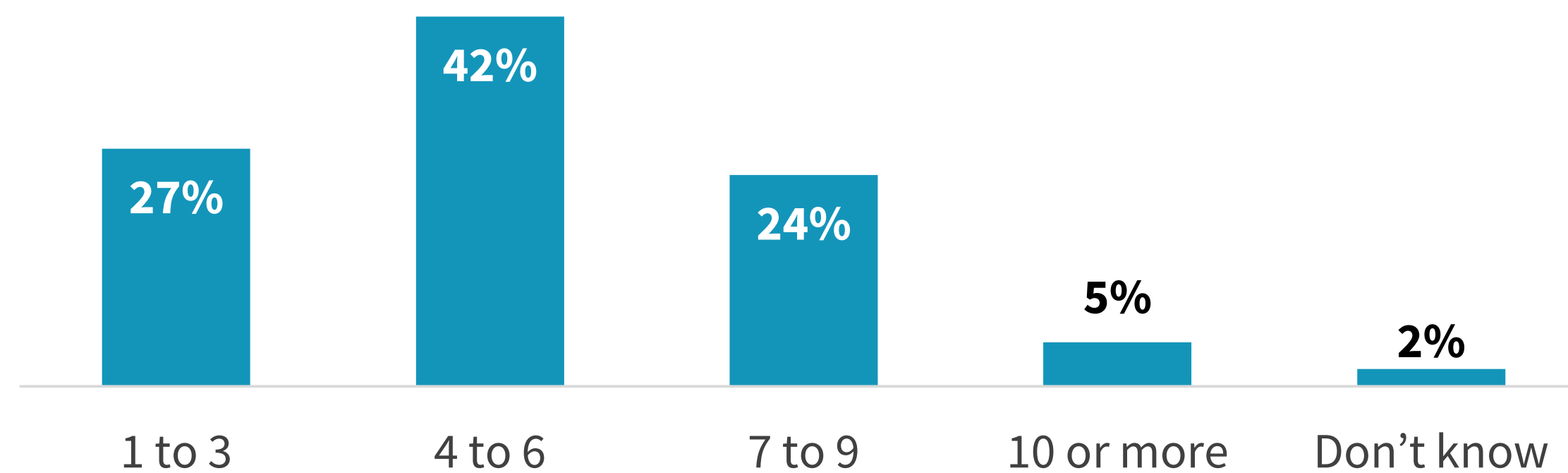
As mentioned, the ability to consume all functions from a single vendor was not a highly ranked critical attribute. Further, many organizations anticipate adding SASE vendors over time rather than consolidating. Specifically, while 60% plan on using one or two vendors for SASE initially, only 38% believe this will be the case when complete. This may point to current perceptions more than what the future will hold. The research found that 71% of respondents use at least four perimeter network security vendors today, with 29% using at least seven. Contextualizing a reduction from that level to one or two vendors may be difficult for some organizations. But as solutions mature and convergence benefits are proven out, more organizations may begin to prioritize vendor consolidation.

The desire for a single-vendor approach appears limited at this time.

| Number of SASE vendors.



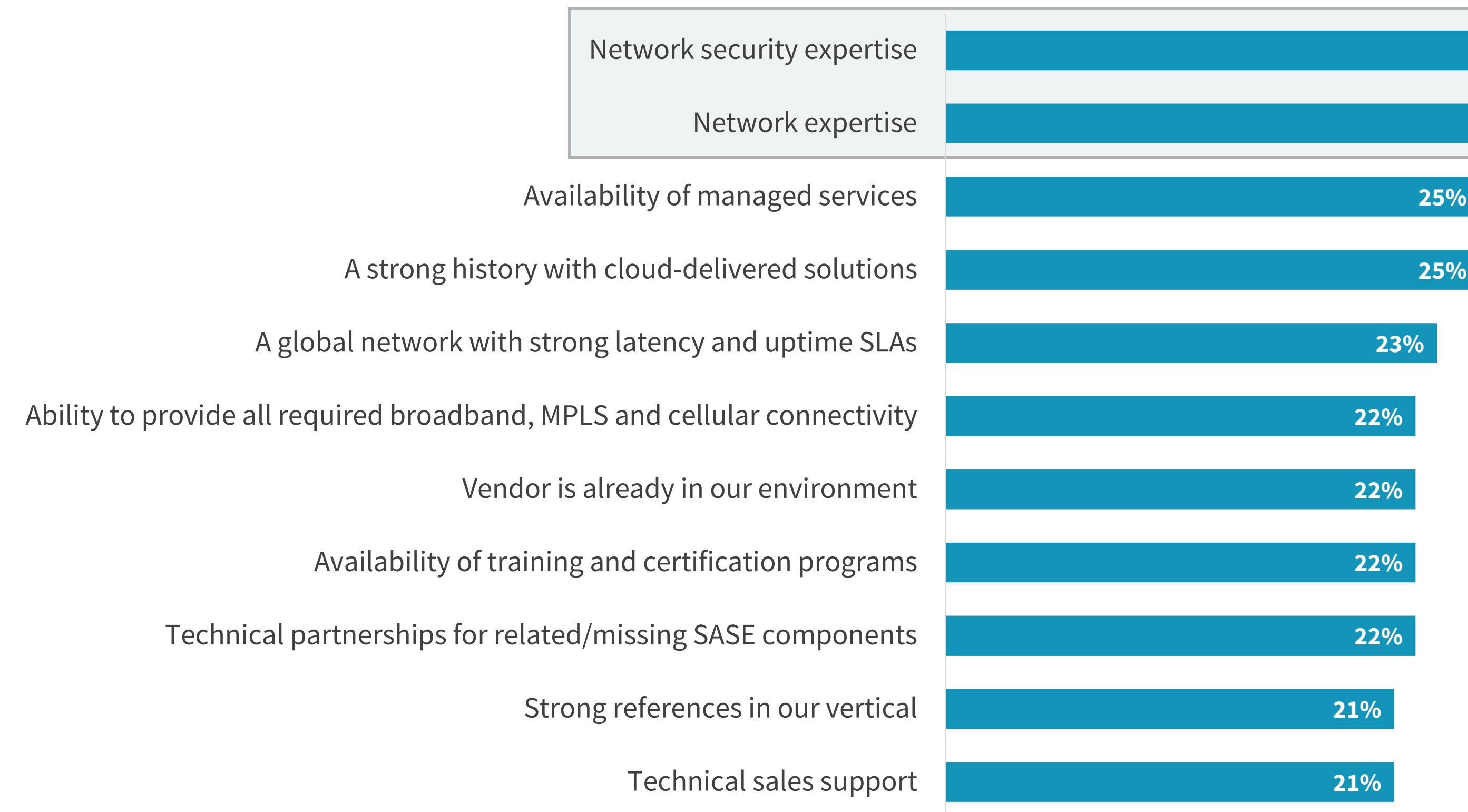
| Number of perimeter network security controls.



Customers Desire Experience and Support from SASE Vendors

When asked for the most important vendor criteria for SASE, our research respondents pointed to network security expertise (39%) and network expertise (31%) most frequently. The fact that specialized experience rates so highly certainly reinforces the current multi-vendor preference of many users. Additional attributes include the availability of managed services (25%), history with cloud-delivered solutions (25%), availability of training programs (22%), and technical sales support (21%). As ubiquitous as cloud-based tools have become, the reality is that many network and network security solutions remain on-premises. As such, users will look to vendors with a strong background in the cloud, support programs to help them navigate the transition, and even managed offerings to fill skills gaps or fully offload day-to-day operations.

| Most common SASE vendor criteria.



“ The fact that specialized experience rates so highly **certainly reinforces the current multi-vendor preference of many users.** ”

A photograph of two men in an office environment. The man in the foreground is wearing a grey button-down shirt and a black headset with a microphone. He is pointing his right index finger towards a computer monitor. The man in the background is wearing a dark blue button-down shirt and is looking at the same monitor. The background is slightly blurred, showing office shelves and windows. The overall lighting is soft and professional.

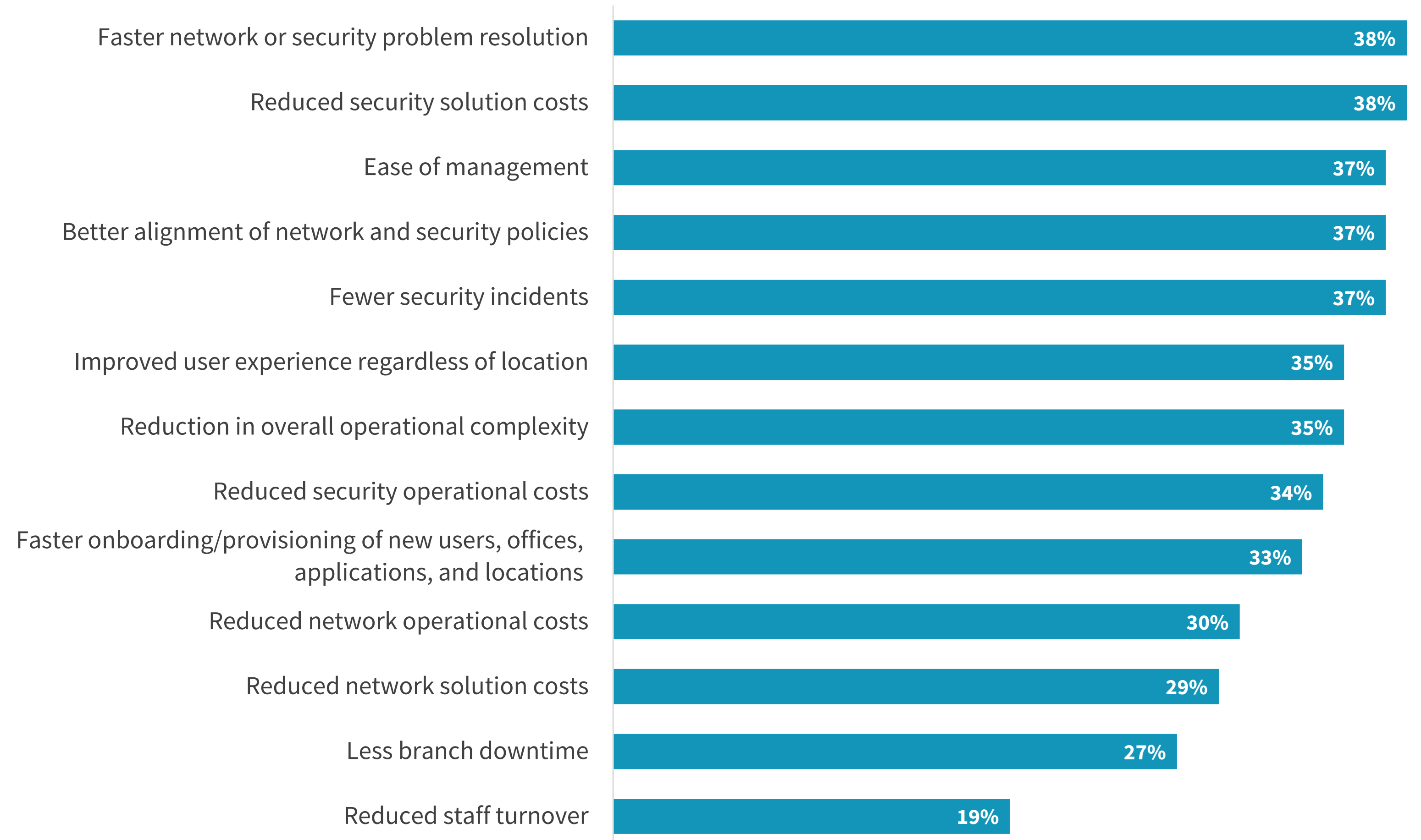
Early SASE Adopters Report Benefits, but Work Remains

SASE Delivers Efficient Management, Effective Security, and Lower Costs

While it is still early, respondents who have begun to implement SASE in their environments overwhelmingly report positive results. Many reported that SASE architectures provided more efficient management. Specifically, 37% cited ease of management, 37% indicated better alignment of network and security policies, and 35% reported a reduction in operational complexity. Additionally, more effective security has been experienced, with 38% pointing to faster problem resolution and 37% reporting fewer security incidents. Finally, despite not being a primary driver for SASE adoption, organizations report reduced costs as well. Respondents reported reduced solution costs for both security (38%) and networking (29%), as well as lower operational costs for security (34%) and networking (30%). Overall, 85% of respondents cited at least three benefits, indicating that many adopting SASE are seeing success.

“ Respondents who have begun to implement SASE in their environments **overwhelmingly report positive results.**”

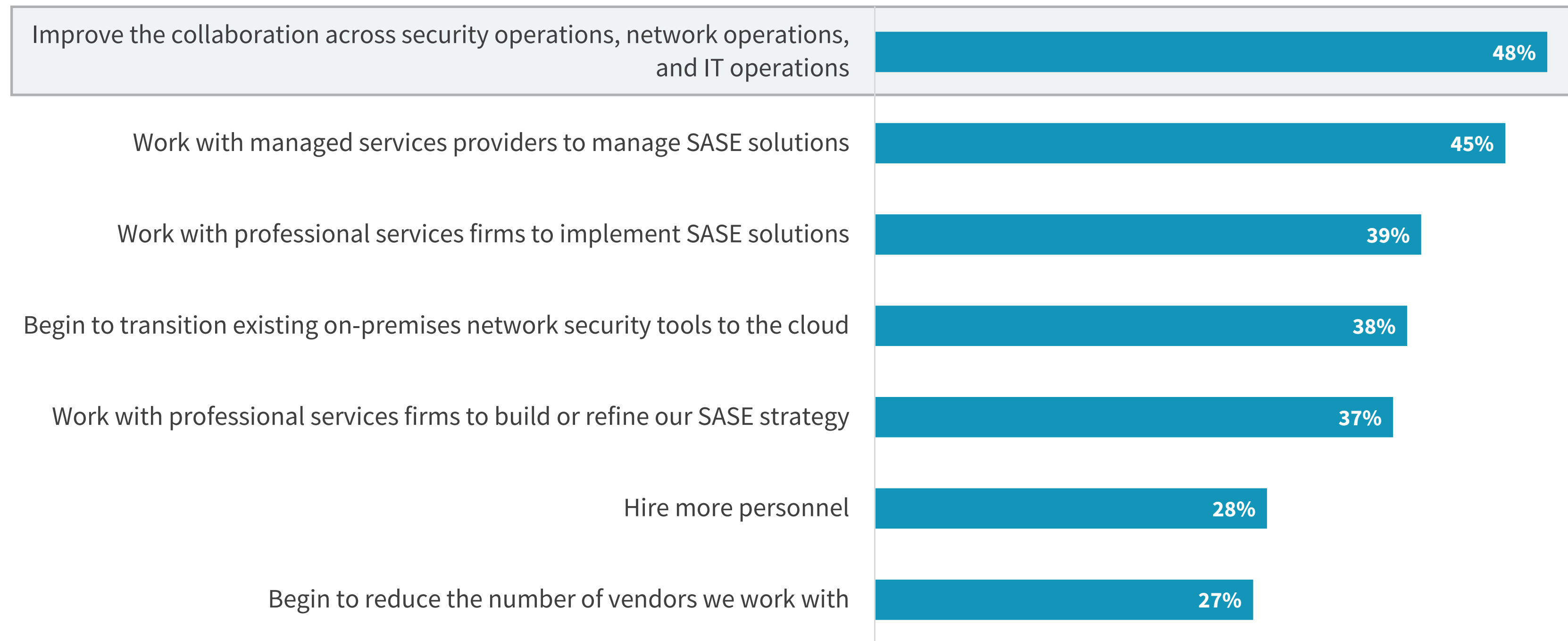
| Benefits seen by organizations implementing SASE.



Services Are of Interest to Implement or Optimize SASE Deployments

While many are seeing success, the fact remains that SASE is in its early stages, so there's work ahead for those planning for SASE implementation and for early adopters optimizing their approaches. Improving collaboration across the different groups involved with SASE was the most common action planned, cited by 48% of respondents. However, working with services providers to manage SASE solutions (45%), implement SASE solutions (39%), and build or refine SASE strategies (37%) were also frequently mentioned. Further, those organizations that have already begun to implement SASE were more likely to indicate they would work more with service providers moving forward, meaning the importance of bringing in outside skills to augment planning, deployment, and operation may be an underappreciated aspect of SASE for those yet to begin.

| Actions to implement or optimize SASE strategies.



“Improving collaboration across the different groups involved with SASE was the most common action planned, cited by 48% of respondents.”

Improving Internal Alignment Will Be Critical

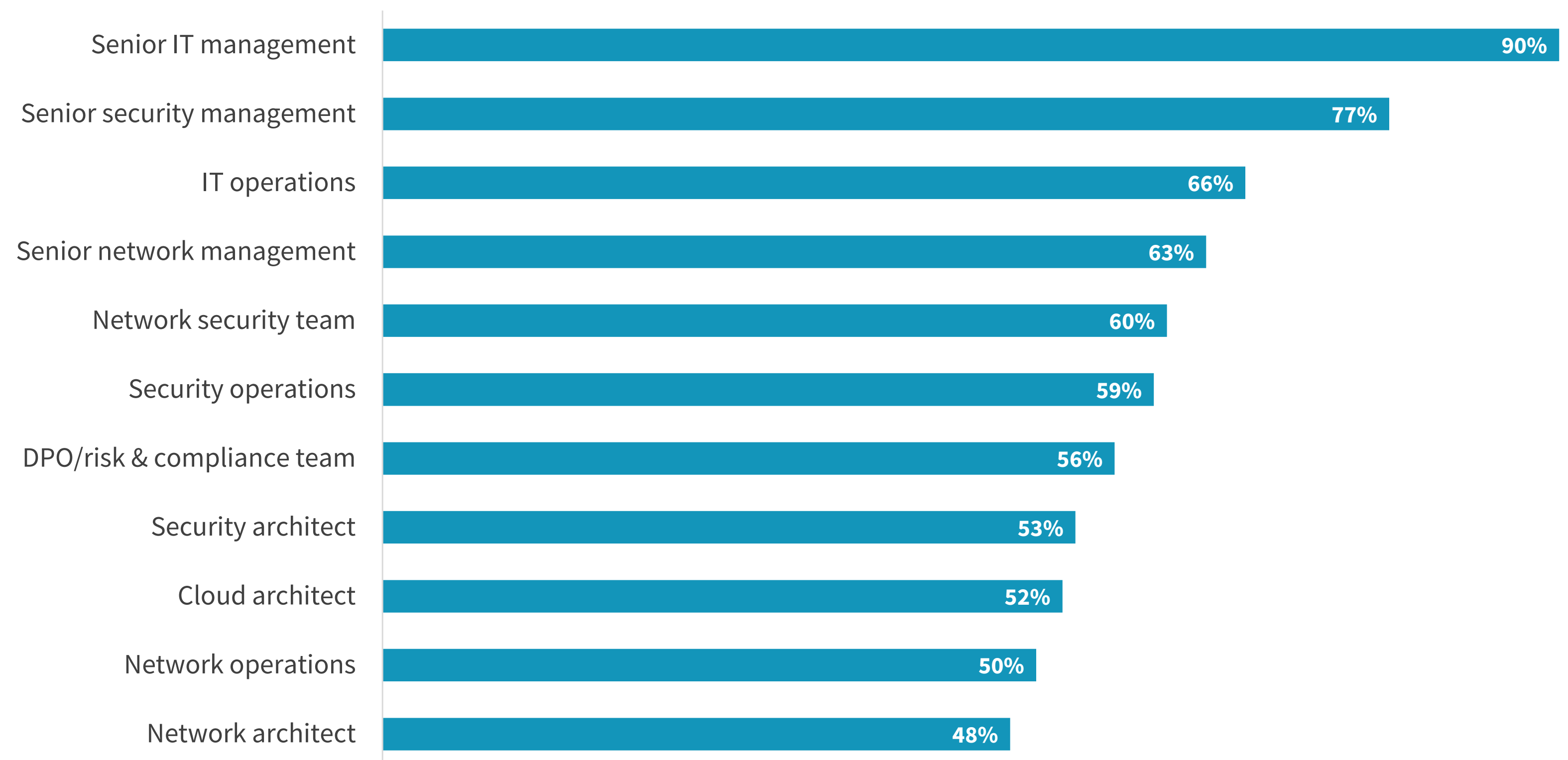
A background image showing a group of business professionals in a meeting. One person is pointing at a tablet displaying a bar chart, while others look on. The scene is dimly lit with a purple and blue color palette.

Planning and Evaluating for SASE ‘Takes a Village’

Not unlike other significant architectural shifts in IT, planning and evaluating for SASE will require input from numerous technology teams and roles. The research results indicate that senior IT management needs to be involved across all stages of the planning, evaluating, and decision-making process, and nine out of ten organizations report that this is the case for at least one of these phases. Additionally, it is worth noting that those organizations that are just beginning their SASE journey may underestimate the need to involve senior management. Organizations should learn from early adopters and include senior IT, security, and network leadership from the start.

“The research results indicate that senior IT management needs to be involved across all stages of the planning, evaluating, and decision-making process, **and NINE OUT OF TEN organizations report that this is the case for at least one of these phases.**”

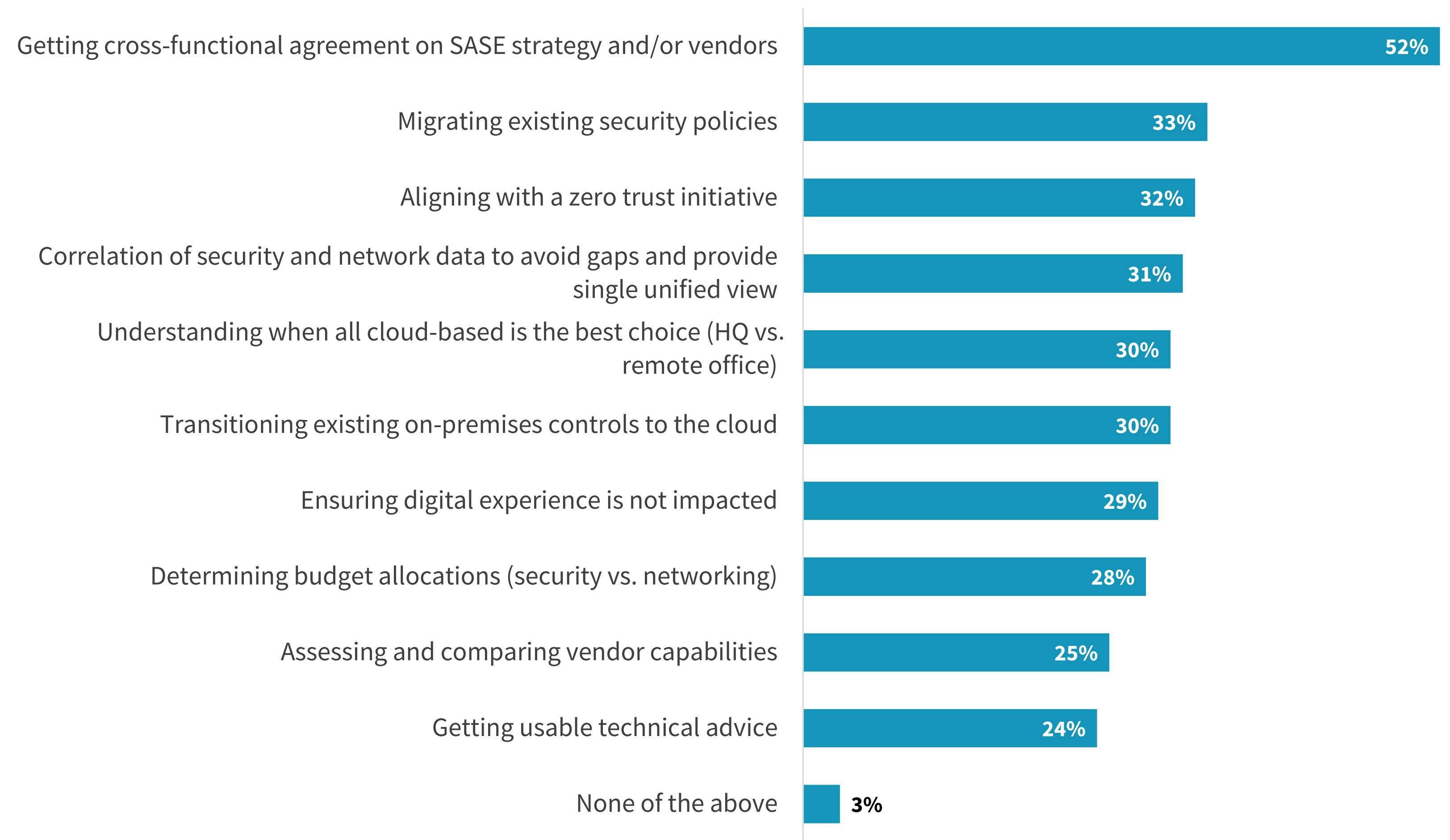
| Roles with input into SASE planning, evaluation, and/or decision making.



SASE Challenges

The previous data point also highlights one of the biggest challenges when implementing SASE: Getting all the disparate teams to agree on a strategy and then selecting vendors. Other significant challenges relate to migrating security policies and ensuring all network and security data can be correlated to deliver a single source of truth. The ability to align with a zero trust initiative also ranks highly. Certainly, having clarity around how SASE solutions will support zero trust strategies is important. Determining when and transitioning functions to the cloud also feature prominently and may require organizations to provide additional training.

| Most common SASE challenges.





Trend Micro Zero Trust Risk Insights continuously monitors the posture risks of devices, identities, applications, and data - largely using existing infrastructure. To make more informed access control decisions, it automatically shares risk scores with SASE solutions, either from a third-party or soon from Trend Micro.

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, our cybersecurity platform protects 500,000+ organizations and 250+ million individuals across clouds, networks, devices, and endpoints.

[LEARN MORE](#)

ABOUT ESG

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

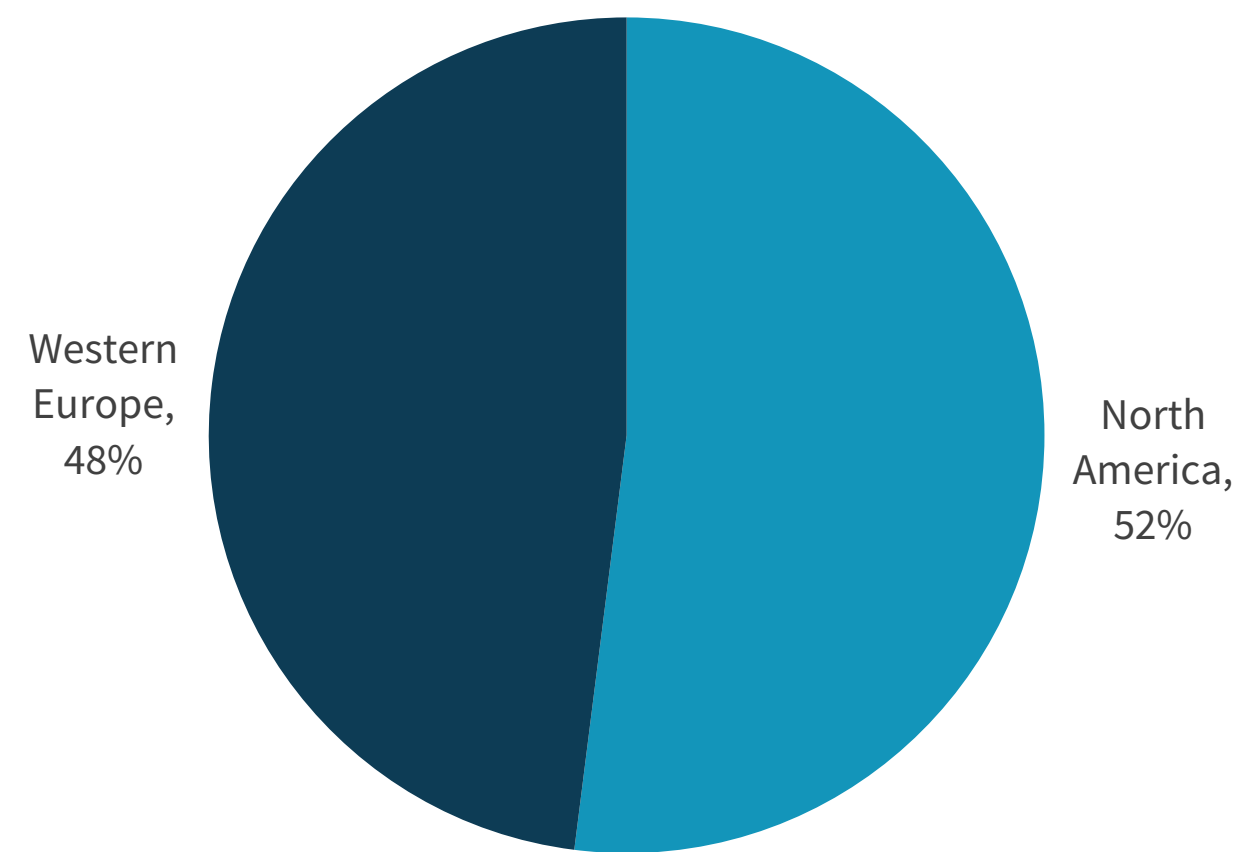


Research Methodology

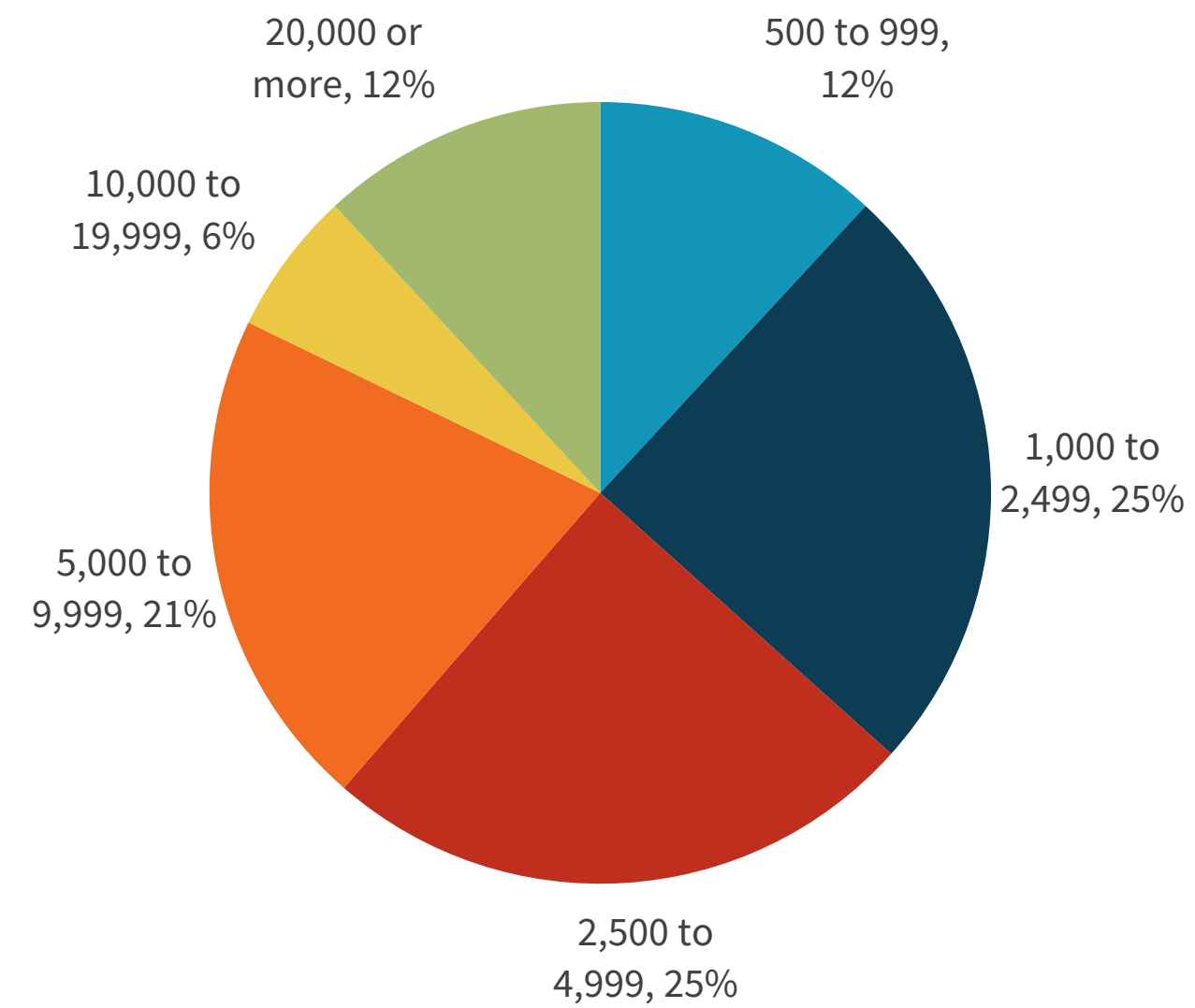
To gather data for this report, ESG conducted a comprehensive online survey of IT, network, and cybersecurity professionals from private- and public-sector organizations in North America and Western Europe between June 20, 2021 and July 20, 2021. To qualify for this survey, respondents were required to be IT, network, and cybersecurity professionals at least somewhat familiar with their organization’s network or security tools, policies, and procedures, as well as be at least somewhat familiar with SASE. 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 613 IT and cybersecurity professionals.

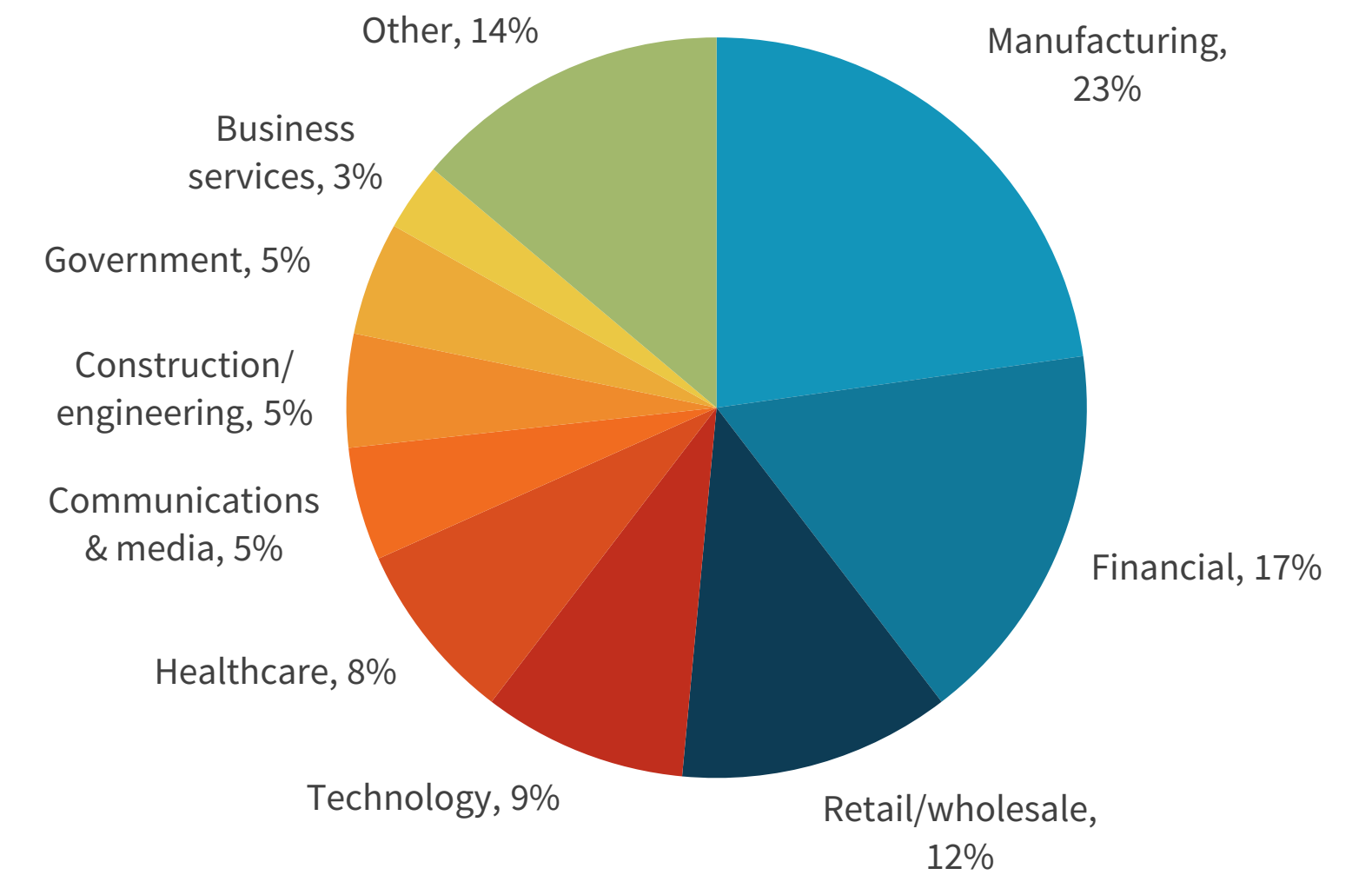
RESPONDENTS BY GEOGRAPHY



RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY INDUSTRY



All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

© 2021 TechTarget, Inc. All Rights Reserved.