Enterprise Strategy Group™ by TechTarget

SSE Leads the Way to SASE

And Despite Early Stages, Many Are Seeing Success

John Grady, Senior Analyst

JUNE 2023

Research Objectives

Modern enterprise complexity is challenging cybersecurity programs. One of the biggest reasons is the broadening distribution of applications and employees away from traditional corporate locations, which is fueling complexity and creating networking and security challenges. Secure access service edge (SASE) technology can help address these issues, but adoption paths can widely vary. Indeed, the breadth of SASE and organizational considerations that must be accounted for when converging networking and security lead to a variety of starting points.

In order to investigate how businesses are faring with adoption plans, the use cases they seek to support, and the technologies they prioritize as part of SASE rollouts from a cybersecurity perspective, TechTarget's Enterprise Strategy Group (ESG) surveyed 390 IT and cybersecurity professionals at organizations in North America (US and Canada) responsible for evaluating, purchasing, and managing network security technology products and services, specifically security service edge technology and processes.

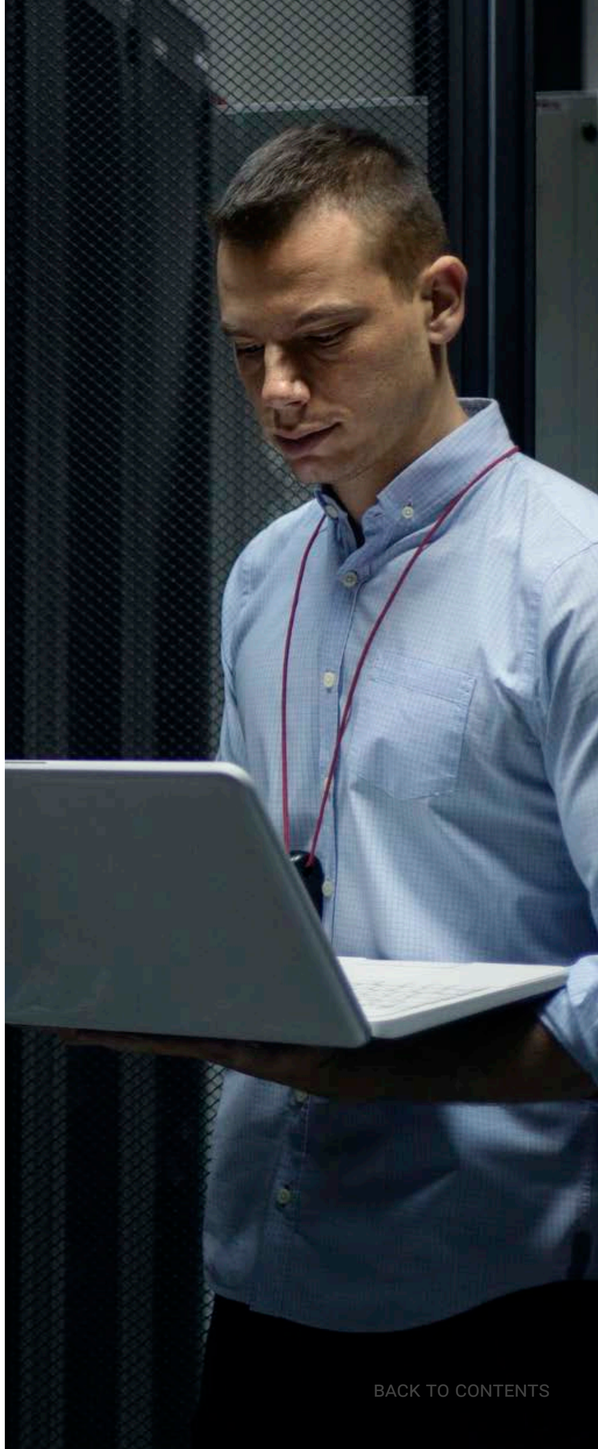
This study sought to:

Identify top drivers for SASE and SSE initiatives and whether they are changing.

Determine if companies are making progress with organizational changes to support network and security convergence.

Understand the primary technologies and capabilities users are seeking in SSE solutions.

Monitor interest in single-vendor solutions and anticipated project timelines.



BACK TO CONTENTS

KEY FINDINGS

CLICK TO FOLLOW

Transformative Drivers and Use Cases Make SASE a Multi-year Initiative for Most

PAGE 4

Security Criticality Leads Many to Start with SSE

PAGE 8

Navigating SSE Challenges Requires Flexible Solutions

PAGE 12

The Entire Security Stack Is in Play, but SWG, CASB, and ZTNA Lead the Way

PAGE 15

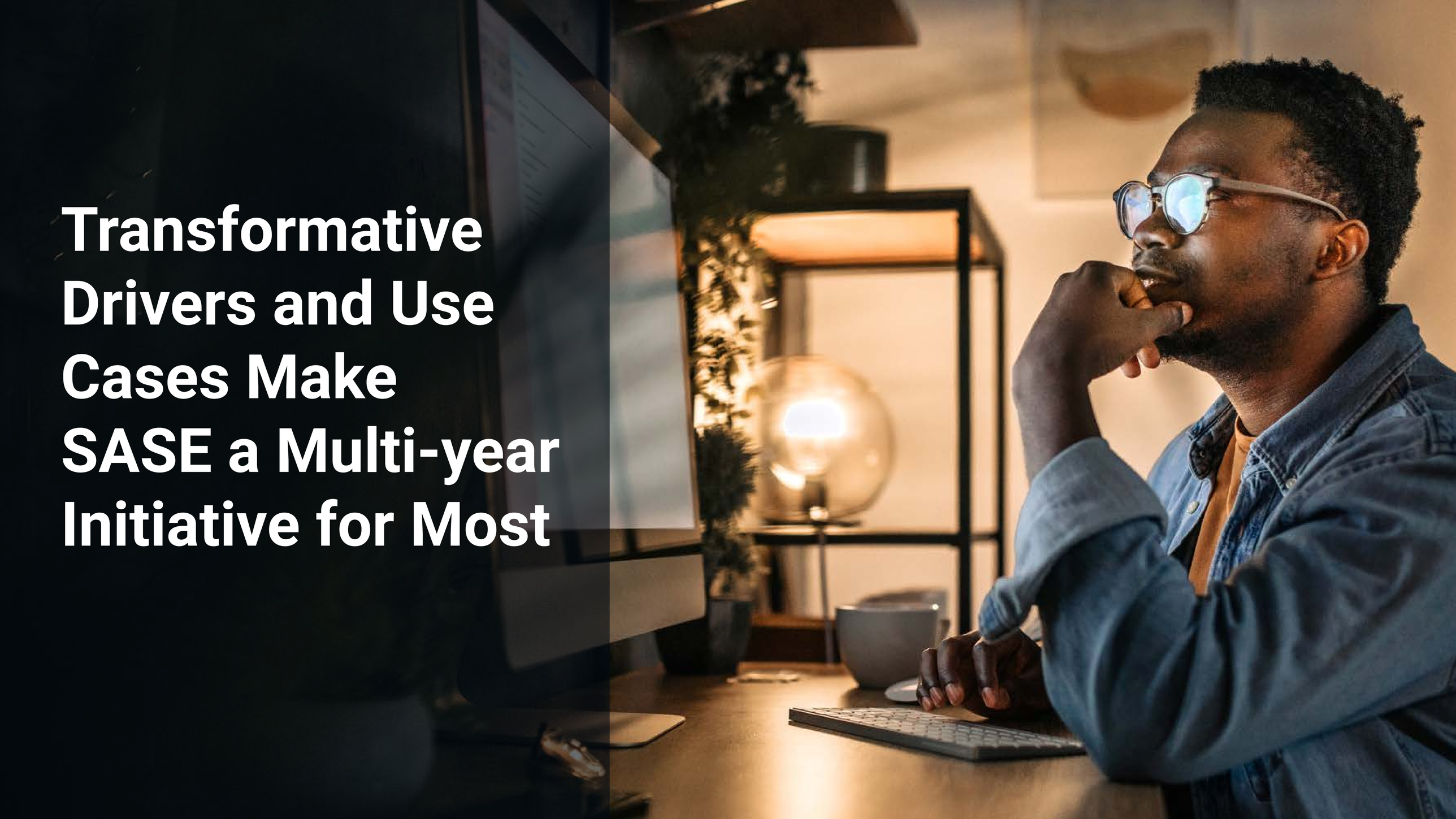
Multi-vendor SASE Views Persist, Though SSE Expectations Would Be Better Met by Single-vendor Approaches

PAGE 20

Despite Early Stages, Many Are Seeing Success

PAGE 23

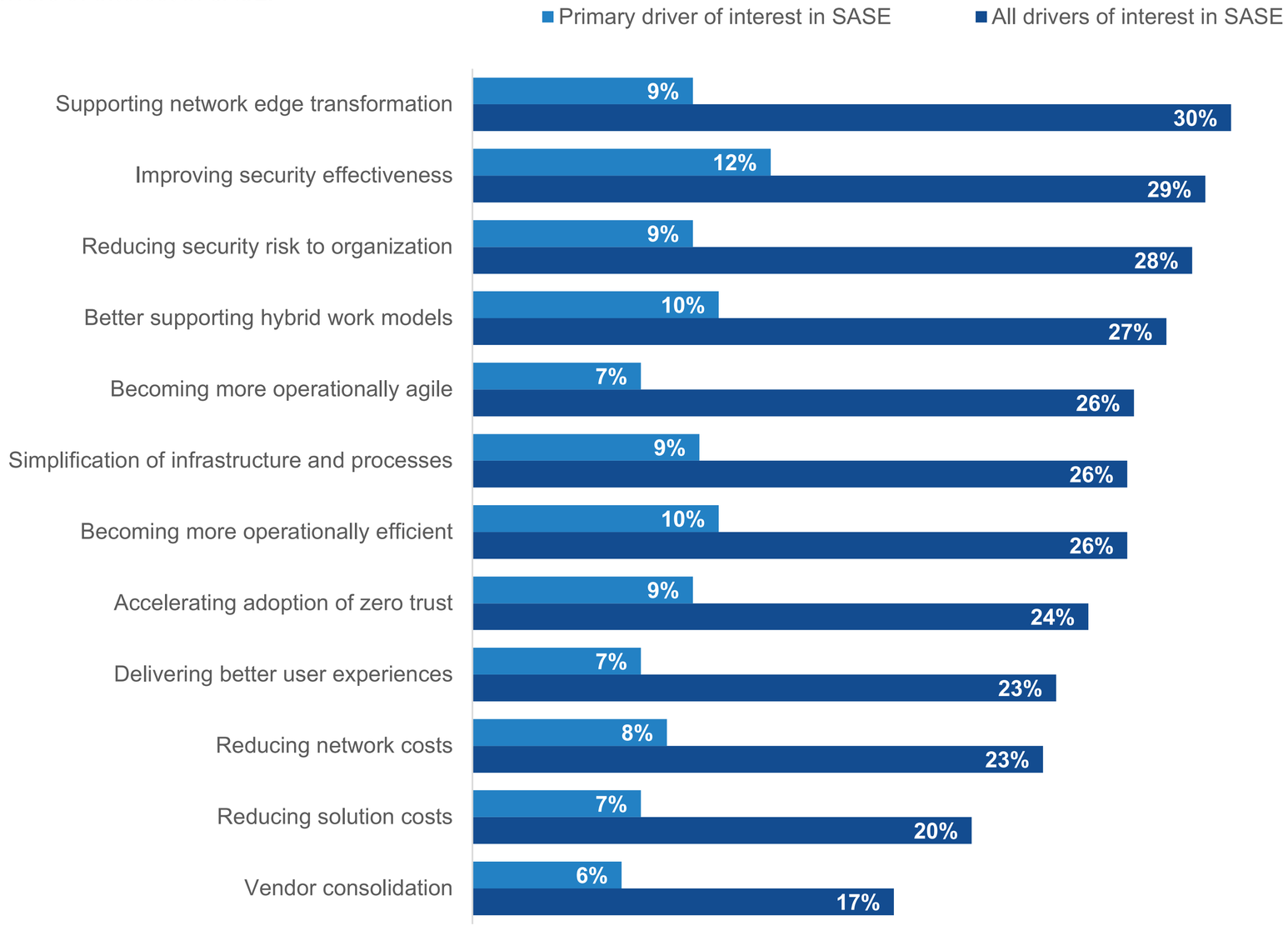
Transformative Drivers and Use Cases Make SASE a Multi-year Initiative for Most



Security Teams Highlight Both Network and Security Drivers for SASE

Despite only being introduced a few short years ago, the interest around secure access service edge (SASE) continues to grow. At its core, SASE is about the convergence of network and security technology. Yet more than that, it's about modernizing technologies to better meet the needs of today's distributed enterprise environment. This is highlighted by what organizations cite as the drivers of their interest in SASE. The most common response given is supporting network edge transformation (30%), followed by improving security effectiveness (29%), and reducing security risk (28%). Rounding out the top responses, supporting hybrid work models is cited by 27% of respondents. Interestingly, while vendor consolidation is a consideration for some (17%), it ranks toward the bottom of the list.

Drivers of interest in SASE.



BACK TO CONTENTS

Current or expected initial SASE use cases.

“One-quarter cite aligning network and security policies for applications and services.”

Use Cases for SASE Are Fragmented

On average, respondents selected three use cases they believe will be their organizations’ initial focus for SASE. One-quarter cite aligning network and security policies for applications and services. Reducing/eliminating the internet-facing attack surface for network and application resources and improving remote user security are the next most commonly identified use cases among early and planned SASE adopters. Overall, this fragmented set of use cases can be grouped by higher level themes including improving operational efficiency, supporting flexible work models, and enabling more consistent security.

BACK TO CONTENTS

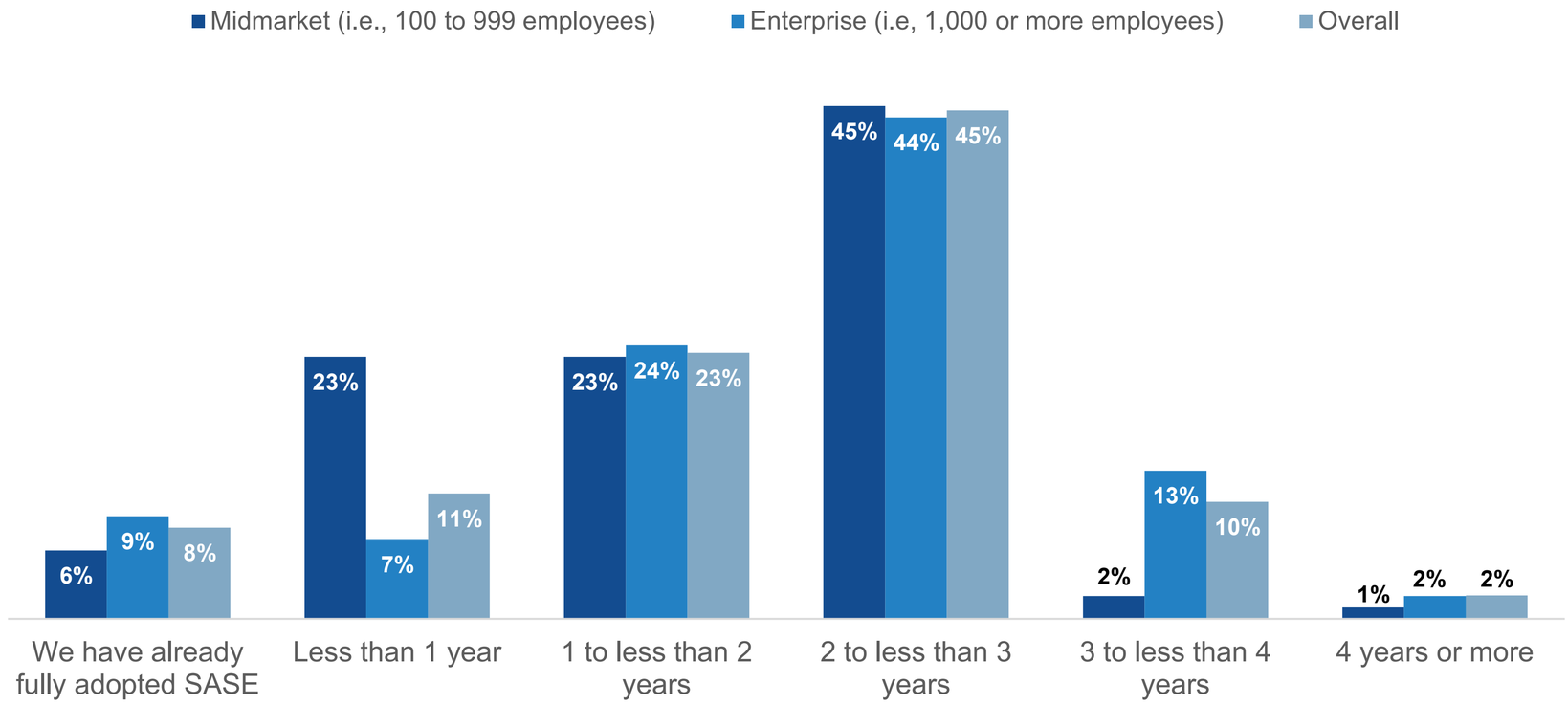
57%

believe it will take at least two years to fully adopt SASE, up from 34% in 2021.

SASE Transitions Are Multi-year and Will Take Longer in the Enterprise

In recognition of the fact that SASE initiatives are transformative, there is recognition that these projects are almost always a multi-year effort. Overall, more than half (57%) believe it will take at least two years to fully adopt SASE, up from 34% in 2021. This belief is more prevalent among those organizations with more than 1,000 employees (59%) compared with their midmarket counterparts (48%). This highlights the need for organizations to educate themselves, identify both short- and long-term needs, and ensure the broader IT organization is fully aligned on the initiative before getting underway.

Expected length of time to fully adopt a SASE architecture.



BACK TO CONTENTS

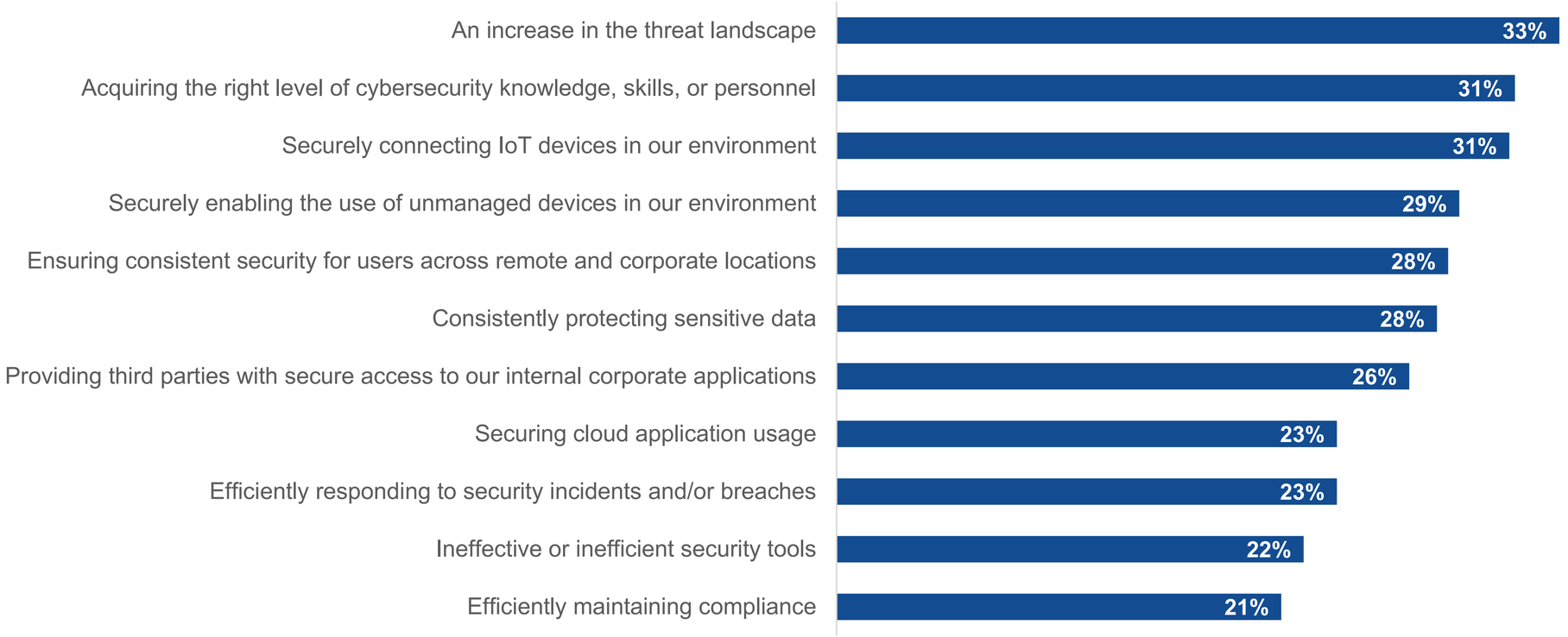
Security Criticality Leads Many to Start with SSE

Security Teams Face a Multitude of Challenges

Security teams obviously have a difficult job. First and foremost, they need to defend against a variety of threats ranging from phishing and ransomware to sophisticated nation-state attacks. It follows that one-third cite an increase in the threat landscape as a challenge that has been most impactful to their organization. Further, security teams have to do more with less, with 31% noting that acquiring the right level of cybersecurity knowledge, skills, or personnel is an issue.

At the same time, the security team is increasingly tasked with supporting the business. Ensuring IoT devices are connected securely (31%), supporting BYOD and the use of managed devices (29%), providing secure access to third parties (26%), and securing cloud application usage (23%) are some of the challenges cited by respondents that fall into this camp.

Most impactful cybersecurity challenges.



ONE-THIRD

cite an increase in the threat landscape as a cybersecurity challenge that has been most impactful to their organization.

BACK TO CONTENTS

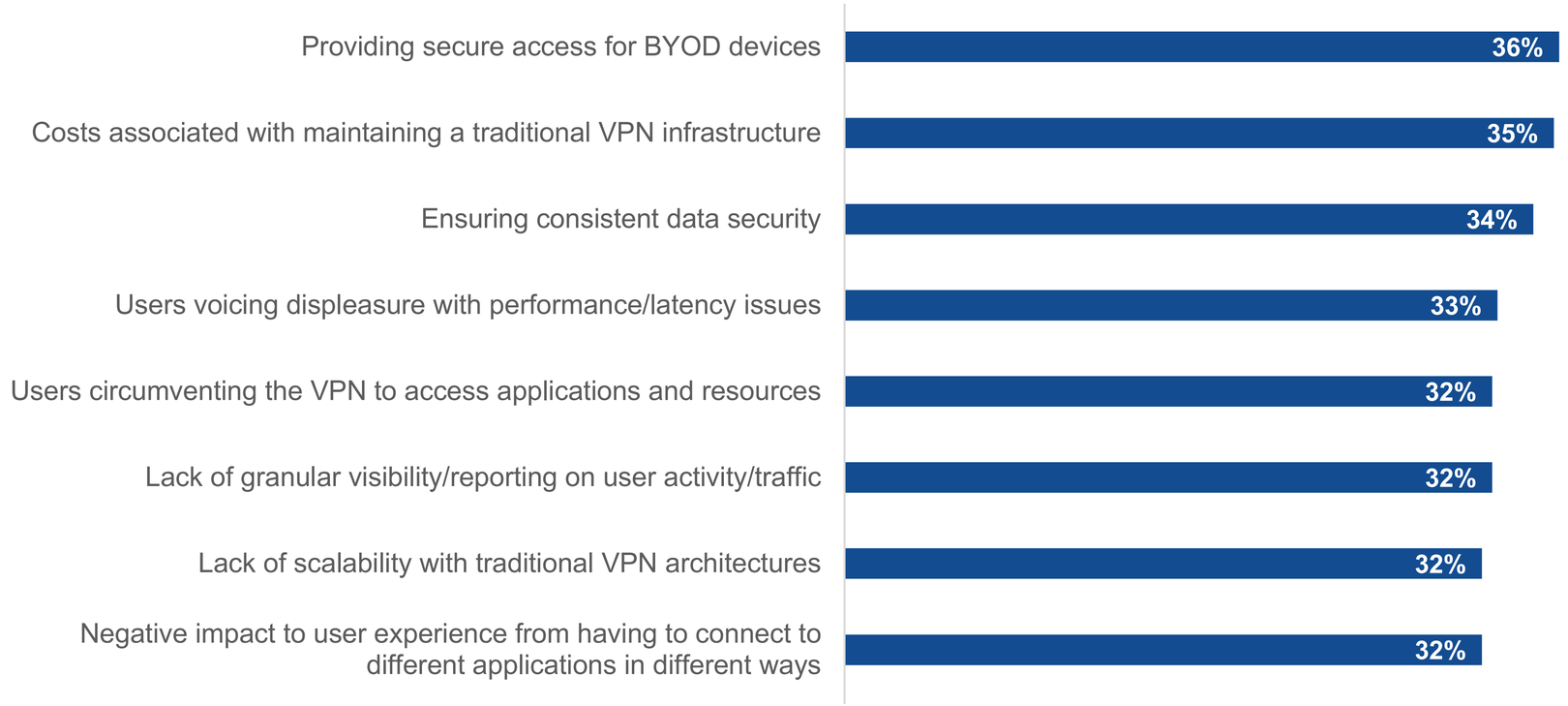
98%

of respondents cite a challenge of some sort in terms of securing remote user access to corporate applications and resources.

Secure Access in Particular Remains an Issue

Several of the challenges previously noted involved secure access. Overall, 98% of respondents cite a challenge of some sort in terms of securing remote user access to corporate applications and resources. Supporting BYOD devices is at the top of the list, mentioned by more than one-third (36%) of organizations. However, the cost, poor security, and limited scalability of VPN is prominently noted. Specifically, 35% cite VPN costs, 32% note users circumventing the VPN, and 32% point to the lack of scalability with traditional VPN architectures. User experience is also an issue, with 33% saying that users voice displeasure with performance or latency issues and 32% pointing to the negative impact to user experience from having to connect to different applications in different way.

Challenges specific to securing remote user access to corporate applications and resources.



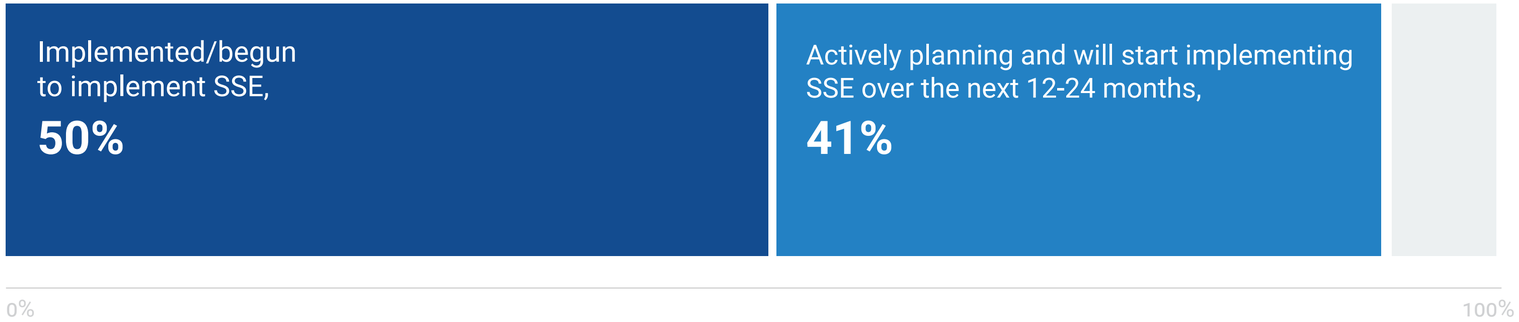
BACK TO CONTENTS

The Vast Majority Are Moving Forward with SSE

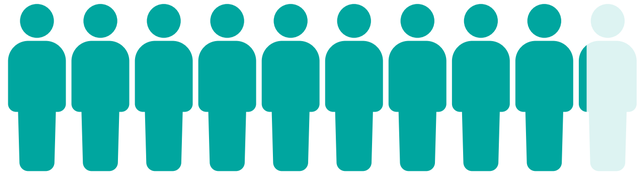
All these challenges highlight the criticality of security, and the need for a more modern approach. Specifically, one that provides consistent, distributed enforcement for users wherever they are, a zero-trust approach to application access, and centralized policy management, all of which are provided through security service edge (SSE), the security component of SASE. Respondents seem to agree, with nearly three-quarters (72%) indicating they have chosen to focus on the SSE side of SASE first or expect to. And many are moving quickly. Indeed, half say they've implemented or begun to implement SSE and an additional 41% will begin implementing SSE in the next 12-24 months or are actively planning to.

| Initial approach to SASE strategy.

| SSE adoption strategy.



An additional 7% said they're planning to implement but have no timeframe, and 2% said they're interested but would have to learn more.



MORE THAN 9 IN 10

have implemented/begun to implement SSE or will do so over the next 12-24 months.

BACK TO CONTENTS

Navigating SSE Challenges Requires Flexible Solutions

Tactical and Strategic Challenges Are Top of Mind

While SSE makes sense at a high level, many organizations have concerns about the challenges they may face in adopting this approach. At the top of the list is supporting multiple architectures for different types of traffic, which was cited by 36% of respondents. SSE comprises a number of capabilities and support for enforcement in a variety of locations. Ensuring that traffic is properly inspected via proxy, firewall, or content analysis and in locations as close to the user as possible are critical to a successful implementation. Otherwise, the user experience can be negatively impacted, a concern voiced by 34% of respondents. Ensuring an SSE project aligns with the organization's zero-trust initiative is also top of mind and was cited by 33% of respondents. Respondents also voice more tactical concerns such as transitioning existing controls to the cloud (29%), getting actionable and usable advice (27%), and migrating existing security policies (25%).

SSE implementation challenges.

36%

Supporting multiple architectures for different types of traffic

34%

Ensuring user experience is not impacted

33%

Aligning SSE with our zero-trust initiative

29%

Transitioning existing on-premises controls to the cloud

27%

Getting actionable, usable technical advice

26%

Becoming locked in with a vendor

26%

Ensuring interoperability between vendors

25%

Migrating existing security policies

24%

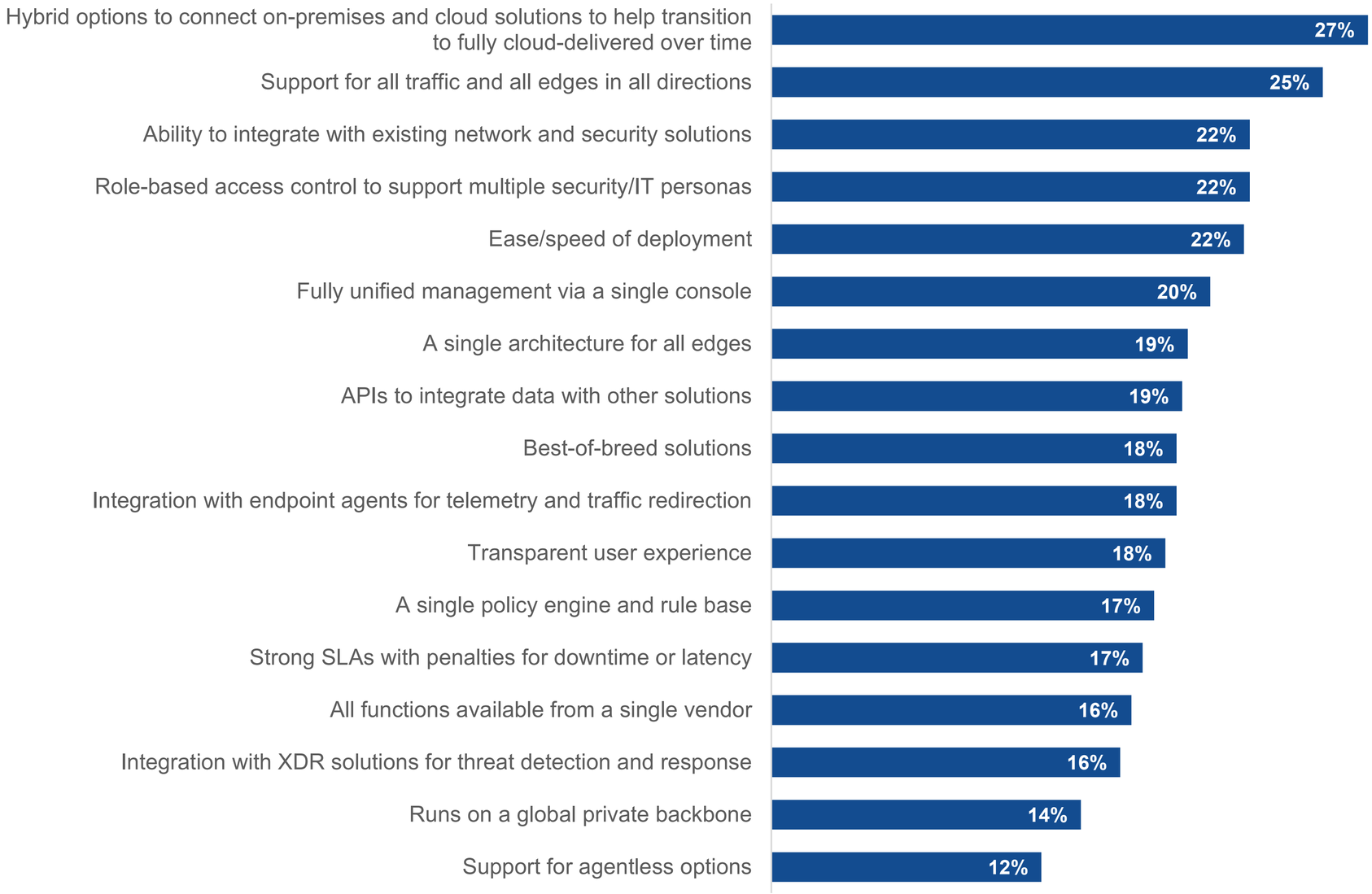
Determining a starting point

24%

Assessing and comparing vendor capabilities

BACK TO CONTENTS

Important attributes when considering an SSE solution.



Breadth of Coverage Rates Highest

Respondents prioritize attributes and capabilities in SSE solutions that would help them alleviate anticipated challenges. More than one-quarter (27%) cite hybrid options to connect on-premises and cloud solutions to ease the transition to fully cloud-delivered over time. This addresses concerns about the difficulty in moving from on-premises to cloud. One-quarter point to support for all traffic and all edges in all directions, with an additional 19% citing a single architecture for all edges to help overcome concerns about supporting multiple architectures for different types of traffic.

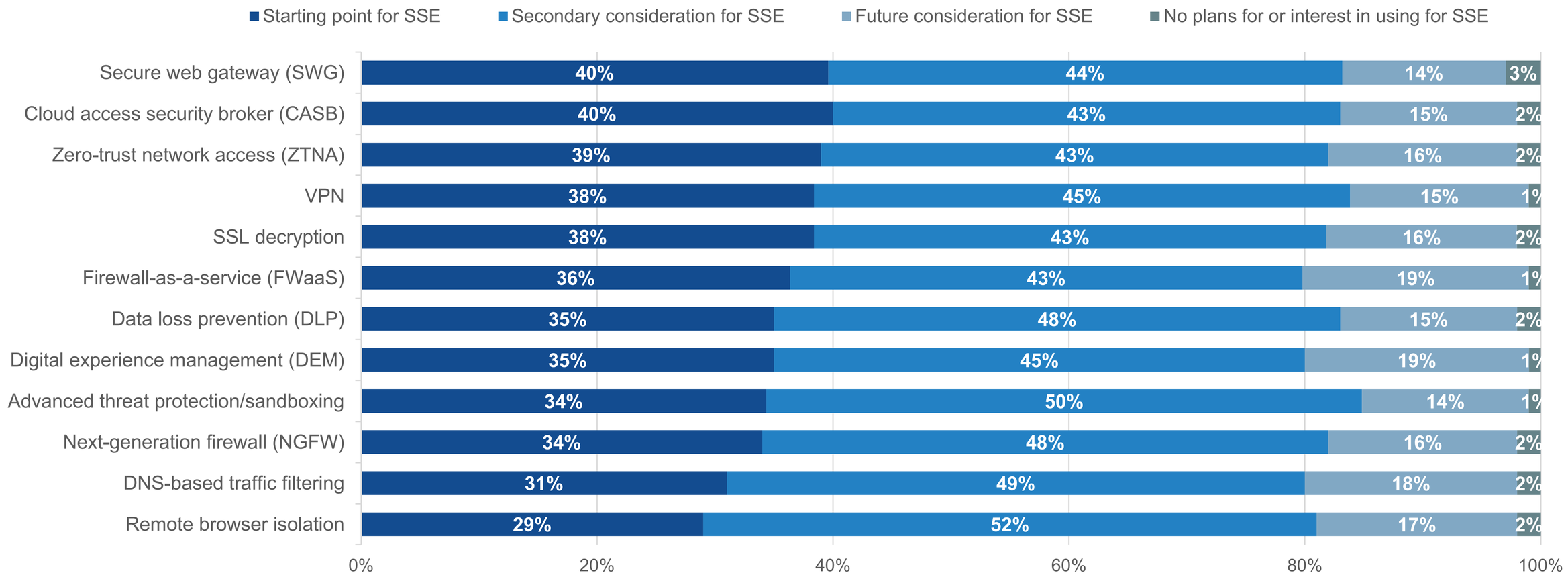
BACK TO CONTENTS

The Entire Security Stack Is in Play, but SWG, CASB, and ZTNA Lead the Way

SSE Architectures Will Incorporate Many Security Technologies, but Core Capabilities Will Lead

While many respondents see the entire stack as part of SSE at some point, converging secure access to public applications, private applications, and the broader internet through secure web gateway (SWG), cloud access security broker (CASB), and zero-trust network access (ZTNA) remains a common first SSE motion. At least 39% of respondents pointed to each of these tools as a starting point for SSE.

How organizations prioritize security tools as they build out SSE architectures.



BACK TO CONTENTS

Users Are Interested in More Advanced ZTNA Capabilities as Part of SSE

When ZTNA was first introduced, much of the interest stemmed from its scalability and cloud-centric architecture as compared with on-premises VPN appliances. There were obviously security benefits, but many organizations did not fully take advantage of them early on. That seems to be changing as organizations are ready for more advanced ZTNA use cases and need capabilities to support them. Specifically, 33% cite support for contextual access policies (such as geolocation, time of day, device type, etc.). One-third (33%) cite continuous security monitoring and enforcement as well. This can help prevent insider threats and attackers leveraging compromised credentials by remaining in-line even after initial authentication checks have passed. Similarly, 31% point to content inspection to monitor for data leakage, malware, or anomalous behavior.

Most important zero-trust network access attributes as part of an SSE architecture.

33%

Support for contextual access policies

33%

Continuous security monitoring and enforcement

32%

Preventing the lateral movement of threats

31%

Device posture assessment

31%

Content inspection to monitor for data leakage, malware, or anomalous behavior

28%

Policy enforcement on-premises without routing traffic to the cloud

28%

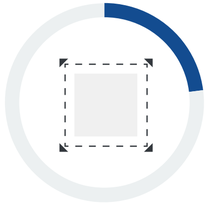
Delivered as a cloud service

26%

Corporate applications protection

25%

Agentless deployment options



23%

Attack surface reduction

BACK TO CONTENTS

65%

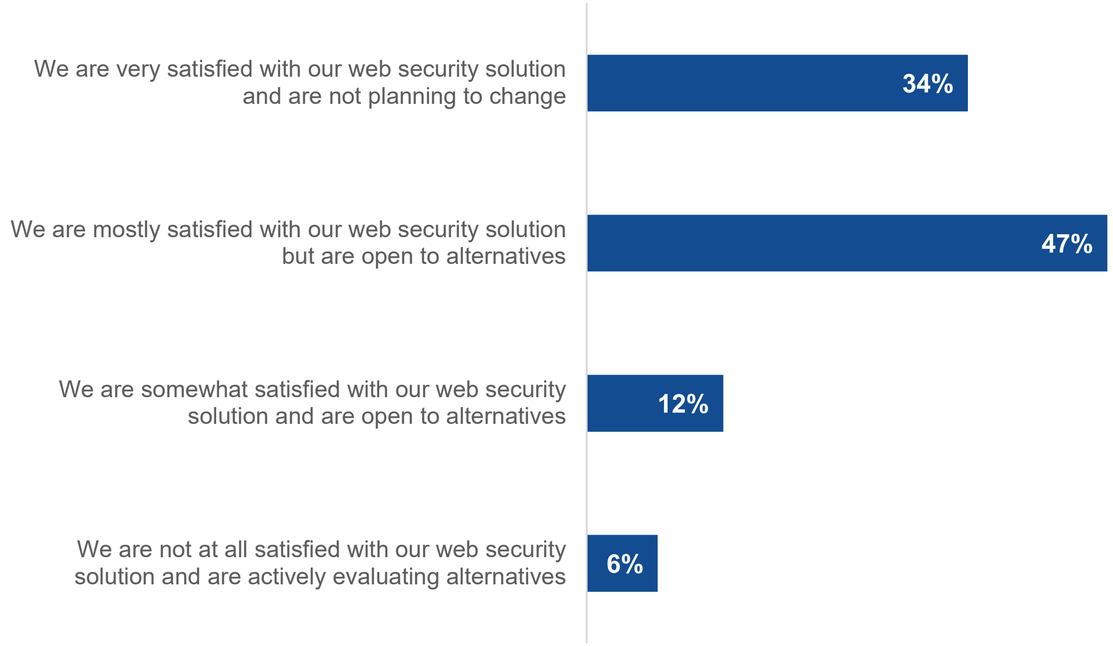
of organizations are open to web security alternatives or are actively evaluating new solutions.

Critical SWG Capabilities for SSE

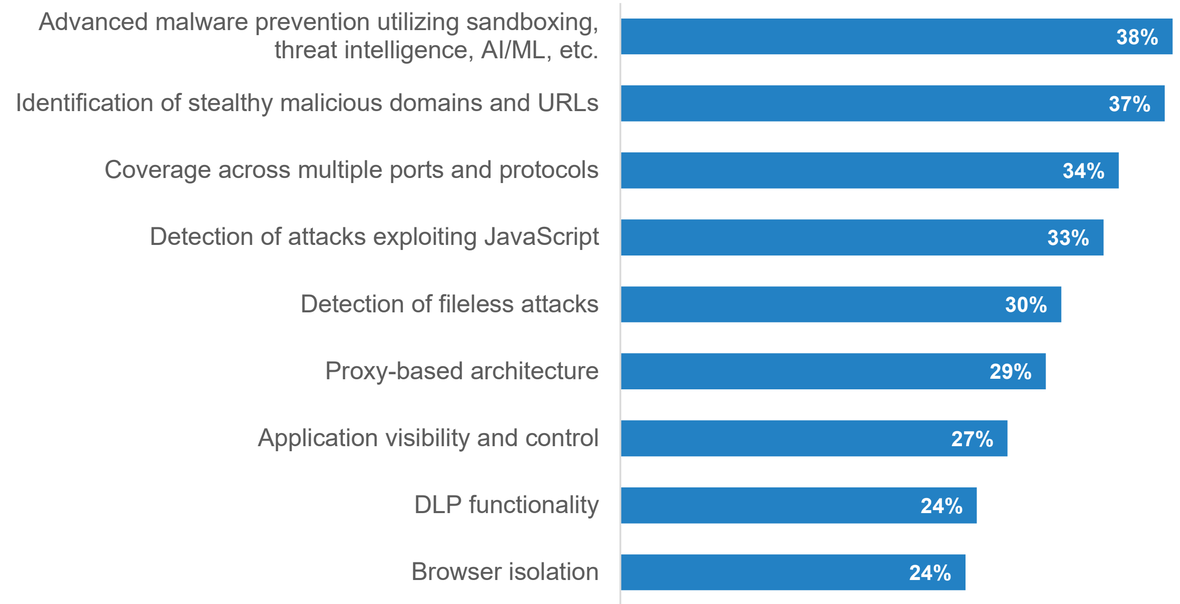
Secure web gateways are an established part of the security stack. However, many organizations seem to be using SSE as an opportunity to explore alternatives. While few are actively evaluating web security alternatives, only one-third do *not* see themselves changing vendors. Those who have implemented or begun to implement SSE are more likely to be very satisfied (46%) than those who have yet to begin (23%), confirming SWG displacement as an initial SSE motion.

When considering a secure web gateway as part of SSE, strong threat prevention is absolutely critical. Advanced malware prevention using sandboxing, threat intelligence, and AI/ML is cited by 38%, identifying stealthy malicious domains and URLs by 34%, detecting attacks exploiting JavaScript by 33%, and detecting fileless attacks by 30%.

Current state of web security deployments.



Most important secure web gateway capabilities as part of an SSE architecture.

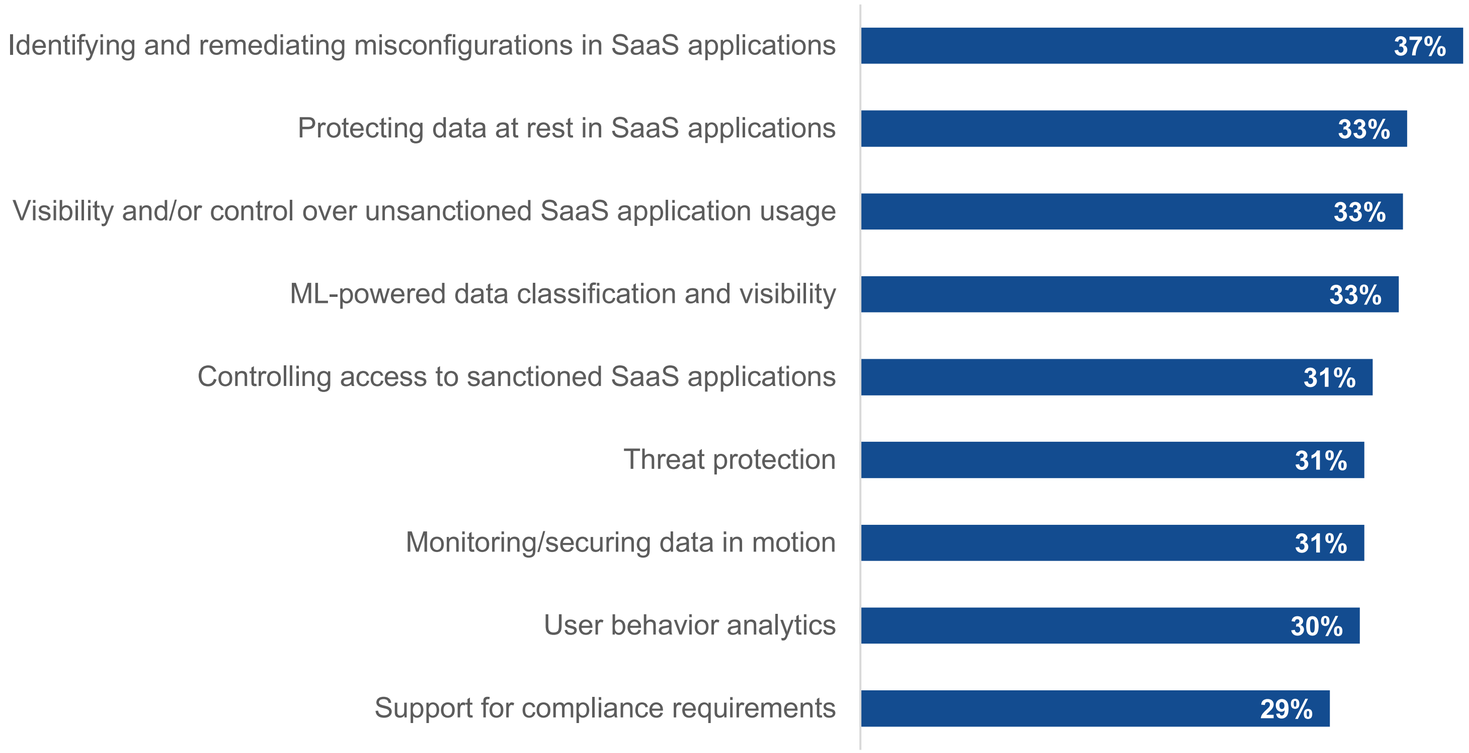


BACK TO CONTENTS

Critical CASB Capabilities for SSE

Over time, the use cases for cloud access security brokers (CASBs) have shifted from compliance toward security. Controlling access to unsanctioned applications (33%) as well as sanctioned applications (31%) are core capabilities. However, the need to ensure the SaaS applications themselves are properly configured has quickly become a fundamental component of CASBs. SaaS security posture management (SSPM) involves identifying and remediating misconfigurations in SaaS applications and is cited by 37% as a most important capability in a CASB as part of SSE.

Most important CASB capabilities as part of an SSE architecture.



> “The use cases for cloud access security brokers (CASBs) **have shifted from compliance toward security.”**

BACK TO CONTENTS

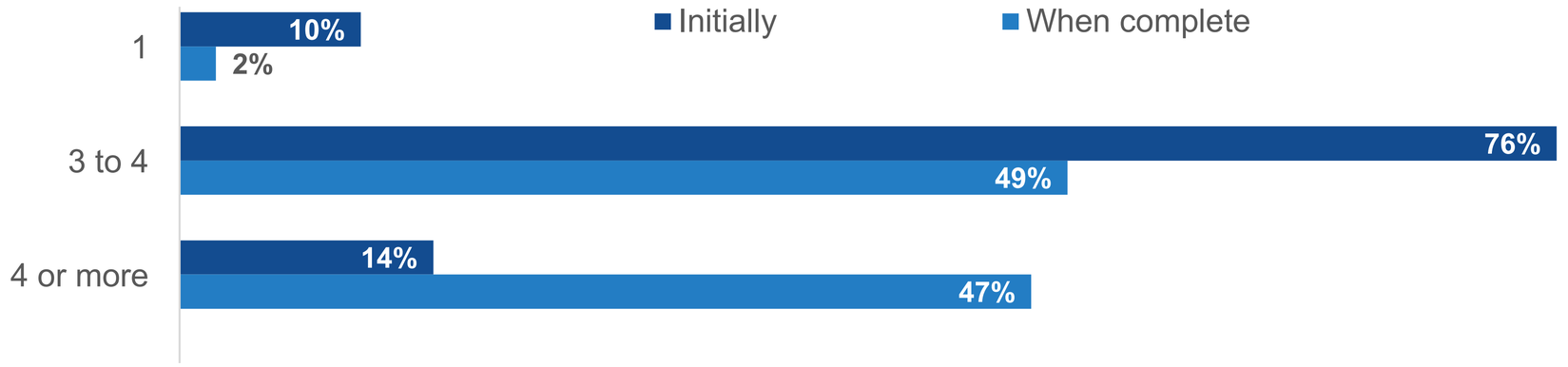
Multi-vendor SASE Views Persist, Though SSE Expectations Would Be Better Met by Single-vendor Approaches

Many Users Appear to Feel ‘Stuck’ with Multi-vendor SASE

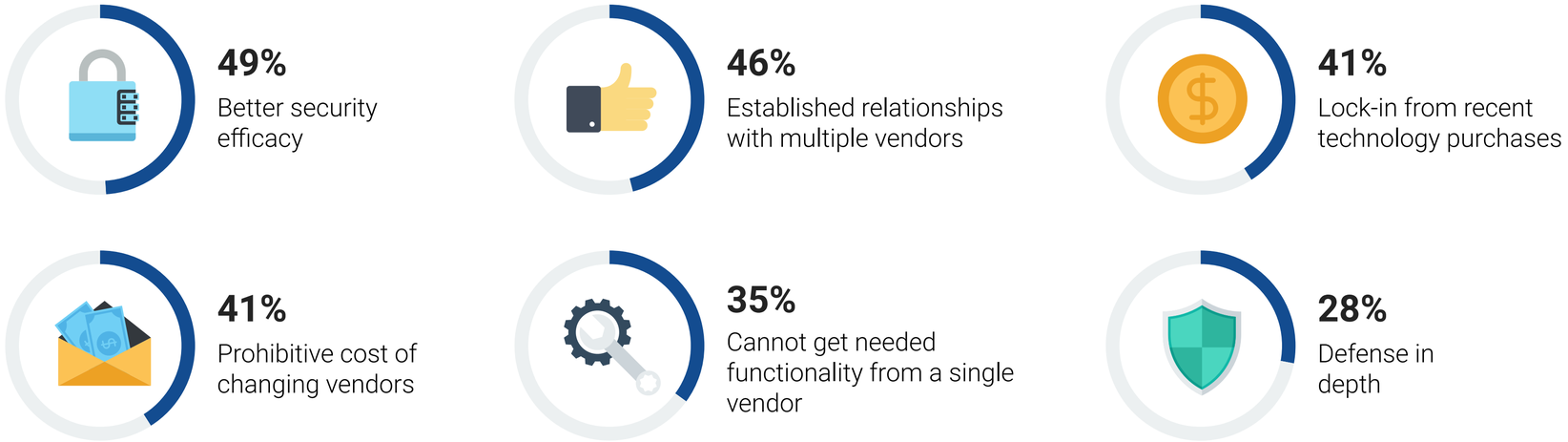
Vendor consolidation has always been a key part of the SASE and SSE concepts. However, some users have been slow to agree with this structure. In fact, the vast majority of organizations expect to use multiple vendors initially and post-implementation, with 83% anticipating using 3 or more vendors for SASE when the initiative is complete. More education and focus could highlight the efficacy, efficiency, and simplicity benefits of single-vendor solutions.

When asked why they expect to take a multi-vendor approach to SASE, nearly half (49%) say they believe they will have better security efficacy. However, many appear to feel “stuck.” Specifically, 46% cite established relationships with multiple vendors, 41% point to lock-in from recent technology purchases, and 41% note the prohibitive cost of changing vendors. While these objections may be legitimate in the short term, security teams should keep an eye on their longer-term goals and explore vendors who can help alleviate some of these issues through specialized migration programs.

Number of technology vendors *expected* to be used to support SASE architecture.



Reasons for using multiple SASE vendors once initiative is complete.



BACK TO CONTENTS

Key Reasons for SSE Interest Would Be Addressed by Single-vendor Approaches

Further, many of the specific reasons respondents cite for their interest in SSE would be best addressed by a single-vendor approach. Many point to improved integrations across controls for different reasons. These include more efficient management (36%), better protection (33%), and risk reduction (33%). A platform from a single vendor may be able to fulfill most efficiently. Vendor consolidation for cost savings or ease of procurement was also cited by 30% of respondents, highlighting the fact that it is an important concept for at least some organizations. Over time, it is likely that perceptions around single-vendor SASE will align more with security teams' anticipated outcomes.

Reasons organizations are interested in SSE.

BACK TO CONTENTS

Despite Early Stages, Many Are Seeing Success

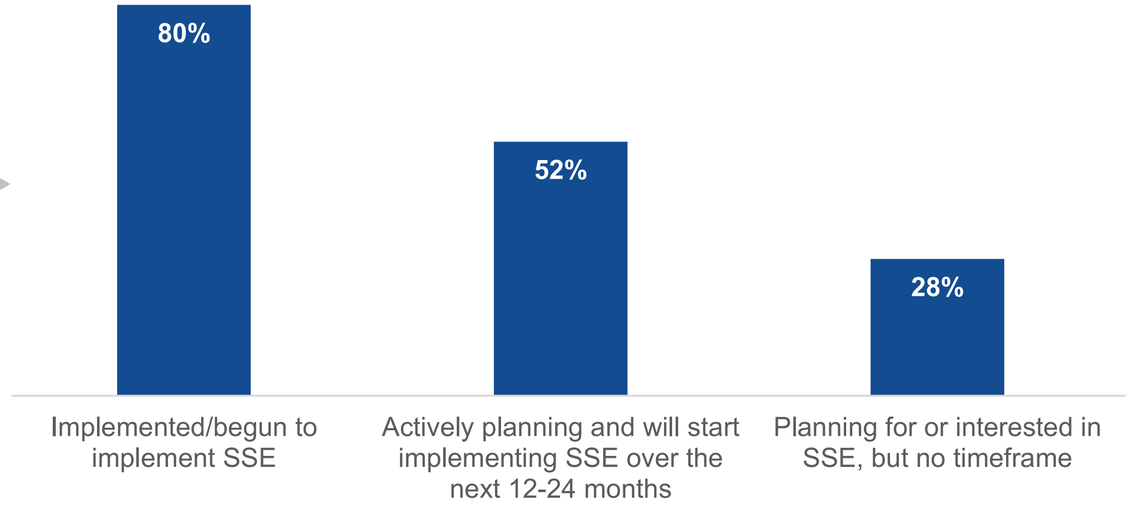
Those Moving Forward with SSE Are More Likely to Say Cybersecurity Is Getting Easier

Ultimately, most remain in the early stages of their SSE journey. However, early adopters are seeing success that should help others see the benefits of the architecture. When asked how cybersecurity has changed over the last two years, nearly two-thirds say it has gotten somewhat (48%) or much (16%) easier. These numbers are even more pronounced according to SSE usage status. Specifically, 80% of those organizations that have implemented or begun to implement SSE say it has become easier, compared with 52% of those actively planning for SSE, and, most tellingly, only 28% of those in the planning or interest but no timeframe stage.

45%
Cybersecurity has become **somewhat easier** than it was 2 years ago

16%
Cybersecurity has become **much easier** than it was 2 years ago

Percentage of organizations that say cybersecurity has become **easier** over the past 2 years by current SSE implementation status.

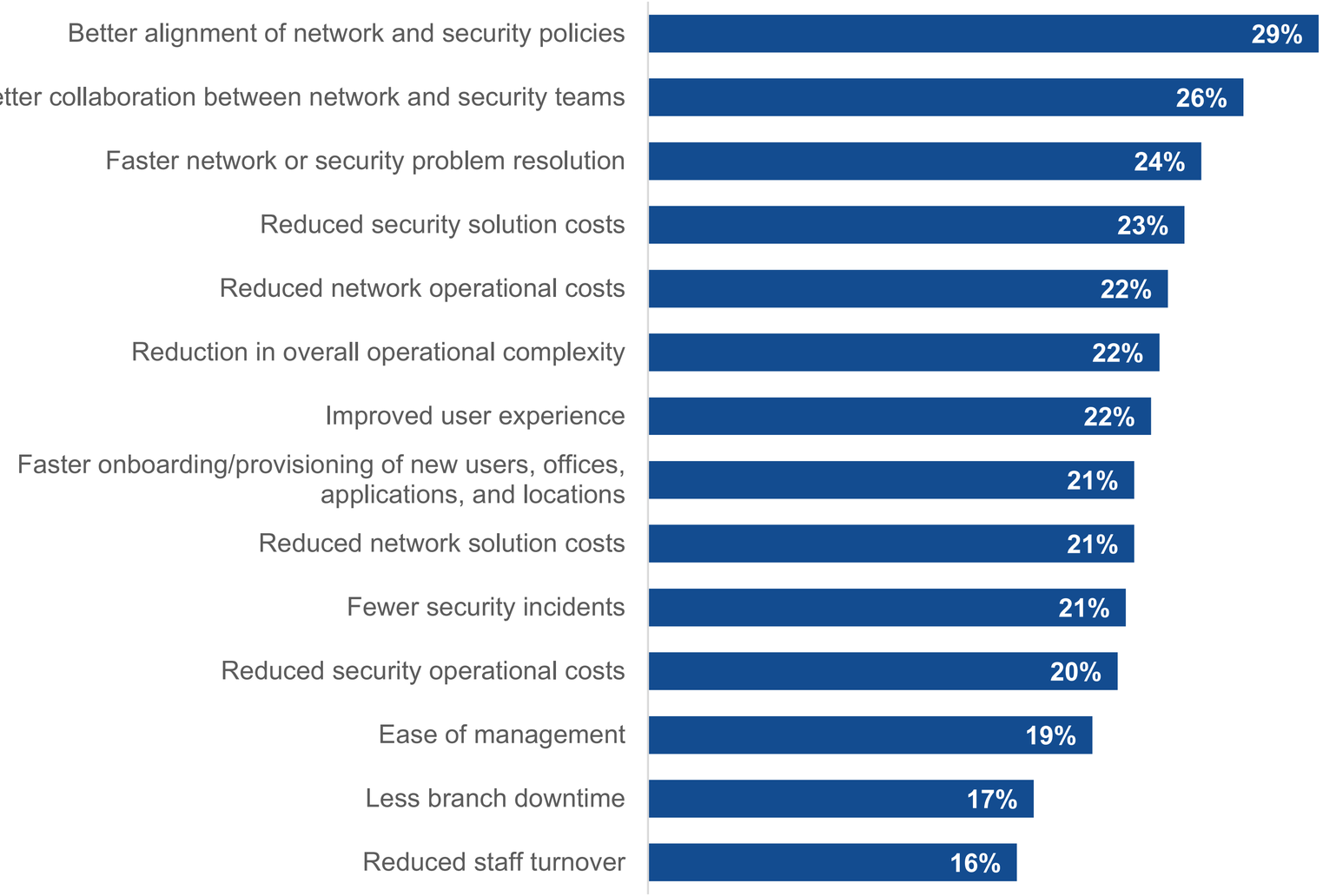


BACK TO CONTENTS

Benefits Realized from SASE

Among those who have implemented or begun to implement SASE, 68% report at least three benefits from the initiative. Nearly two-thirds (64%) report reduced costs across either security solutions, network solutions, security operations, or network operations. Similarly, 62% cite efficiency benefits of some kind, such as faster problem resolution, ease of management, faster onboarding, or reduction in complexity. These proof points should grab the attention of any organization thinking about SASE and SSE. As discussed, it can be a long journey, so beginning to plan now is critical to accelerating the time to value.

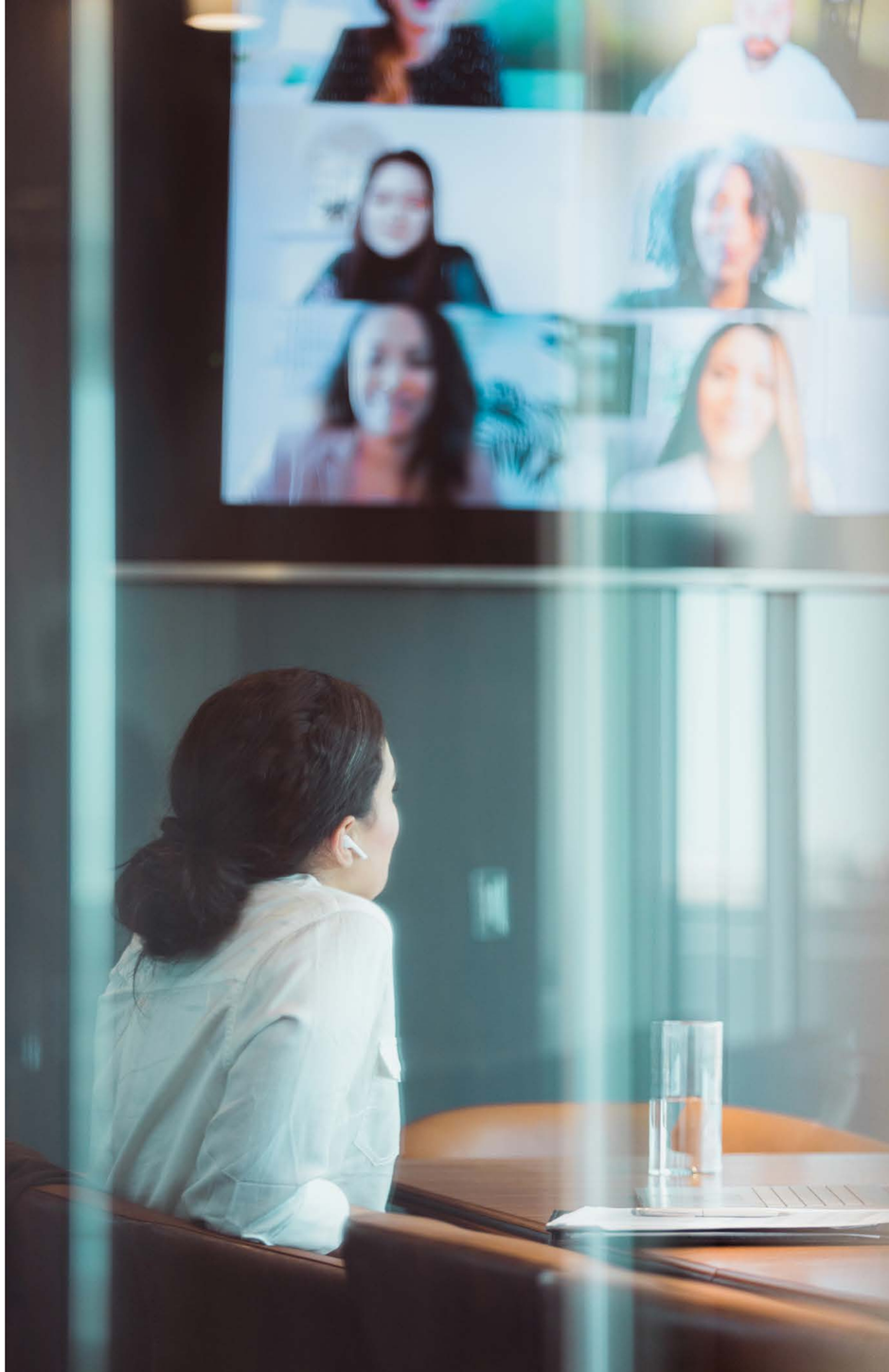
Benefits organizations have realized from SSE to date.



BACK TO CONTENTS

Zscaler is universally recognized as the leader in zero trust. Leveraging the largest security cloud on the planet, Zscaler anticipates, secures, and simplifies the experience of doing business for the world's most established companies.

LEARN MORE



ABOUT ENTERPRISE STRATEGY GROUP

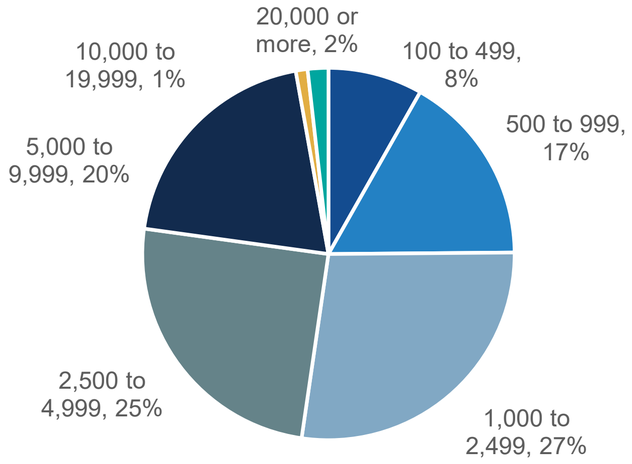
TechTarget's Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Research Methodology and Demographics

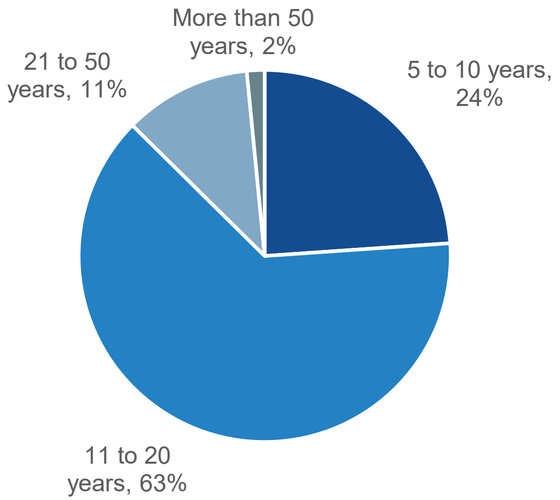
To gather data for this report, TechTarget's Enterprise Strategy Group conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America between March 13, 2023 and March 17, 2023. To qualify for this survey, respondents were required to be responsible for evaluating, purchasing, and managing network security technology products and services, including security service edge technologies 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 390 IT and cybersecurity professionals.

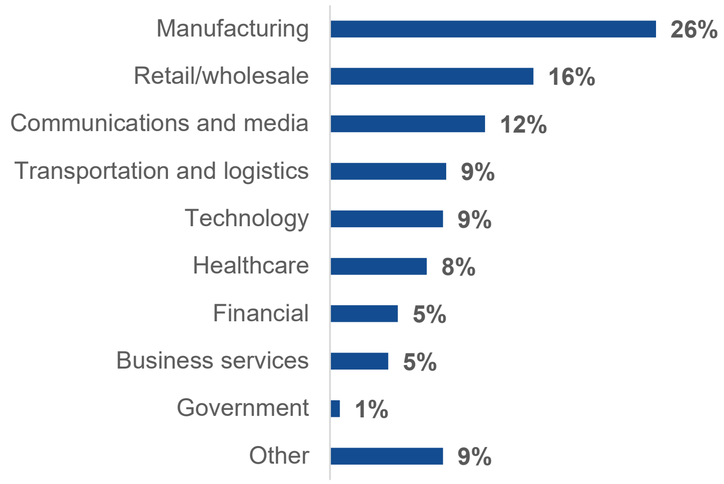
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



BACK TO CONTENTS

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.