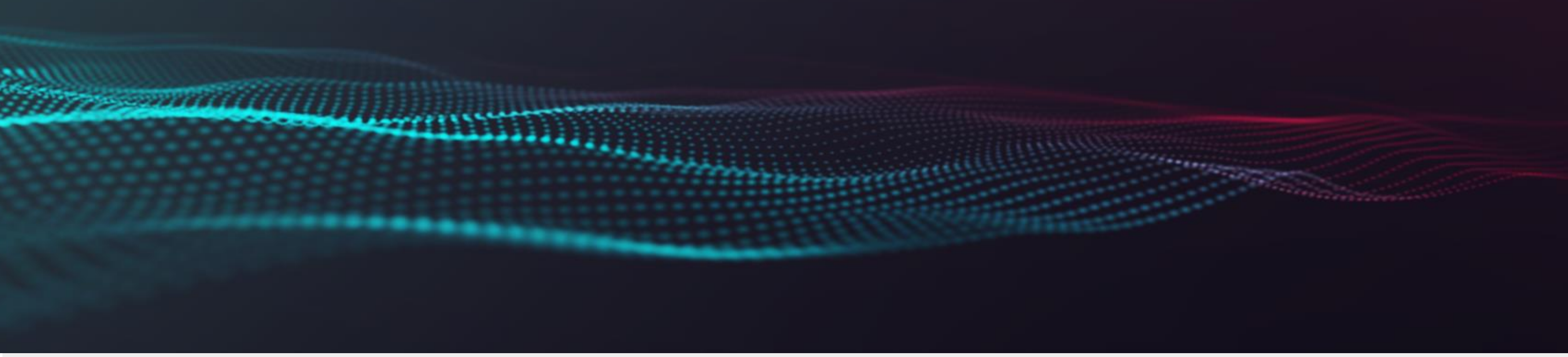
Enterprise Strategy Group | Getting to the bigger truth.™



ESG RESEARCH INSIGHTS REPORT

Quantifying the Benefits of SASE

Identifying Where Organizations that Apply a Converged Approach Achieve Better Security and Business Outcomes

By John Grady, ESG Senior Analyst
Adam DeMattia, Director of Research

March 2021

This ESG White Paper was commissioned by Forcepoint
and is distributed under license from ESG.

Contents

Executive Summary

The concept of secure access service edge (SASE) has generated an enormous amount of market attention and user interest in the short time since it has been introduced. This should not be all that surprising considering the fundamental changes cloud and mobility have had on the enterprise over the last decade and the comparatively little innovation network security technology has seen during that time.

Further, the pandemic has forced organizations to confront the reality that the cybersecurity models they have used for decades are no longer effective in a highly distributed world, creating an additional groundswell around SASE.

> **The pandemic has forced organizations to confront the reality that the cybersecurity models they have used for decades are no longer effective in a highly distributed world, creating an additional groundswell around SASE.**

While we understand the potential benefits pushing organizations towards SASE (better security, improved user experiences, and more efficient operations), the fact that the market remains in its early stages leaves a shortage of information around the actual benefits those organizations that have implemented SASE have seen. To gain insight into how the maturity of an organization's approach to SASE impacts both security and business objectives, Forcepoint commissioned the Enterprise Strategy Group (ESG) to conduct a research study, the key findings from which include:

- Organizations with mature SASE approaches were better prepared to support a distributed workforce. The agility and flexibility afforded by cloud-delivered solutions, coupled with the use of Zero Trust strategies, enables mature organizations to be significantly more confident in their ability to secure remote users.
- Mature SASE organizations are expanding security functionality while simultaneously reducing the number of vendors they use. Stronger, more strategic relationships with fewer vendors and better upfront solution qualification enable mature organizations to be more efficient in their use of security tools.
- SASE reduces the friction associated with lines of business adopting cloud services. The consistent visibility afforded by SASE into both managed and unmanaged cloud resources means security teams can take a more accepting approach to cloud adoption, ultimately leading to more satisfied users.
- SASE supports organizational resilience. By ensuring that security is not an inhibitor to cloud adoptions, SASE allows organizations to support a higher number of applications in the cloud, providing more agility and adaptability to meet societal and macro-economic disruptions.
- Organizations prioritizing SASE benefit from reduced security costs. The reduction of vendors and consolidation of tools result in both lower solution and subscription procurement costs, as well as a reduction in operational costs.

The Emergence of Secure Access Service Edge

The trend towards decentralization continues to shape the IT strategy of many organizations. More than ever, applications and data are cloud-resident, and the users accessing those resources are likely to be somewhere other than in corporate offices.

Yet despite these foundational changes to network architectures, many organizations continue to rely on traditional perimeter security approaches. These are often predicated on backhauling traffic from remote users to the on-premises security stack for inspection. The issues with this approach are numerous:

- When users access cloud applications in this model, the circuitous route traffic must take to flow through on-premises security tools can introduce latency and negatively impact the user experience.

- In the case of on-premises applications, the issue is not backhauling but rather the use of overly permissive, hardware-centric VPN solutions that allow broad network access, cannot elastically scale to meet spikes in demand, and often become the target of attackers due to their visibility on the public internet.

- Whether accessing on-premises or cloud-based applications, the prevalence of employee-owned devices and third parties further complicates consistently securing this matrix of connectivity.

64% of ESG research respondents indicated that network security at the perimeter is more difficult than it was 2 years ago.

Partly as a result of these challenges, cybersecurity has become more difficult and less effective for many organizations. Specifically, 64% of ESG research respondents indicated that network security at the perimeter is more difficult than it was 2 years ago.[1]

To better address these changing dynamics, a new architecture has emerged called secure access service edge (SASE), which converges multiple security controls in a cloud-delivered model, providing centralized management and distributed enforcement. There is no definitive list of tools SASE must include, but many organizations have focused on secure web gateway (SWG), cloud access security broker (CASB), Zero Trust Network Access (ZTNA), data loss prevention (DLP), and firewall-as-a-service (FWaaS). While SASE was originally positioned with more emphasis on branch and remote office use cases, the increase in remote work due to the pandemic has highlighted the critical need to consistently provide secure access regardless of where the user is located.

Identifying the Stages of SASE Maturity

To better understand the benefits organizations are enjoying after implementing SASE architectures, Forcepoint commissioned ESG to conduct a study of 400 IT and information security professionals. Based on their responses to five key questions[2] about network security technology, controls, and processes, participating organizations were grouped into one of three cohorts based on SASE maturity:

1. Emerging: Organizations in the “Emerging” cohort exhibit between zero and two mature SASE characteristics. These organizations are more likely to take a more reactive approach to security by not always incorporating security and monitoring capabilities during the network design process. They are unlikely to have implemented Zero Trust strategies or to be actively consolidating security vendors and may use fewer perimeter security controls.

2. Follower: Those respondents grouped in the “Follower” category exhibit three or four mature SASE characteristics. These organizations are likely to be using numerous tools and have some level of integration and visibility across them. However, they may be behind in terms of Zero Trust adoption, vendor consolidation, or proactive network and security design processes.

3. Leader: The organizations identified as “Leaders” exhibit all five mature SASE characteristics. These respondents always incorporate security controls into their network design process, have implemented Zero Trust, use an

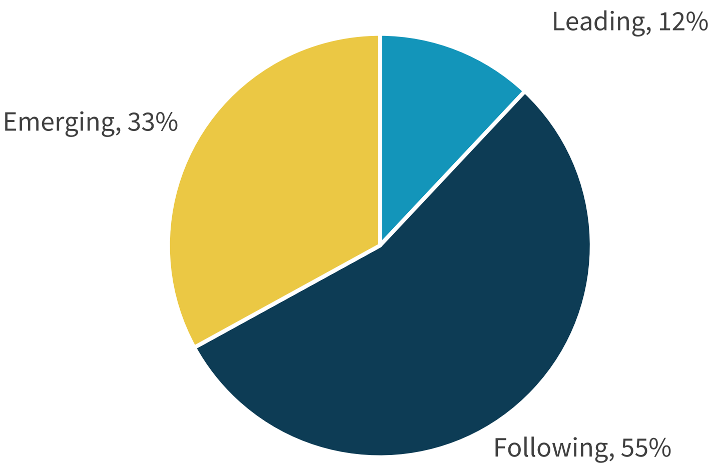
[1] Source: ESG Master Survey Results, *Transitioning Network Security Controls to the Cloud*, July 2020.
[2] For more information, see Appendix II: Survey Questions ESG Used to Evaluate SASE Maturity.

extensive set of network security controls while at the same time consolidating vendors, and have strong integration and visibility across the perimeter controls in place.

Unsurprisingly, few organizations have reached the third stage of SASE maturity and can be accurately described as Leaders (see Figure 1). Those identified as Leaders can use this report within their organization to validate the advantages they can expect to see based on the benefits others who have adopted SASE architectures have reaped. The majority (55%) of our respondents were grouped in the Follower category. These organizations have a solid foundation from which to build towards a more mature SASE approach and can use the data in this report to close the gaps between themselves and Leaders. One-third of organizations represented were grouped as Emerging. While these organizations may still have work to accomplish with regards to SASE, understanding the benefits the approach provides and best practices Leaders employ can help them to prioritize areas of focus to refine their SASE approach over time.

Figure 1. Distribution of SASE Maturity Stages

Respondents by SASE maturity. (Percent of respondents, N=400)



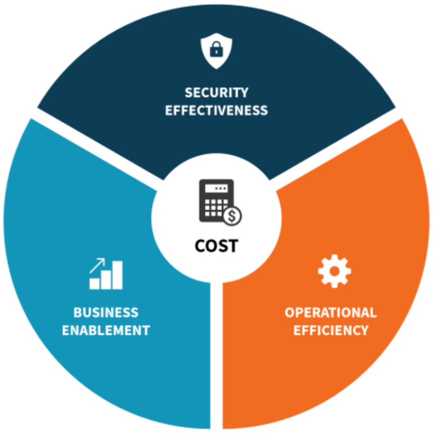
Source: Enterprise Strategy Group

Understanding the Value of SASE

The charter of the cybersecurity team has evolved over time. In the past, security leaders were empowered to enforce strict controls, often assuming the persona of “Dr. No.” The impact to users was not considered a high priority and the centralized nature of IT ensured that the cybersecurity team had the required visibility to maintain security while enabling the business. Yet technology’s expanding presence into the lines of business, facilitated by the self-service model of the cloud, has forced security teams to ensure the controls they put in place do not limit the innovation the business needs to be successful, nor negatively impact the experience or productivity of users.

At the same time, despite the priority status cybersecurity spending sees in many organizations, budget constraints do remain a reality. Providing effective security that is operationally efficient, while enabling the business, and doing so within a limited budget, can be a very difficult task (see Figure 2). However, our research shows that those organizations that have achieved a level of maturity with regards to SASE are able to deliver positive outcomes across all these areas.

Figure 2. Cybersecurity Teams Must Generate Both Security and Business Outcomes



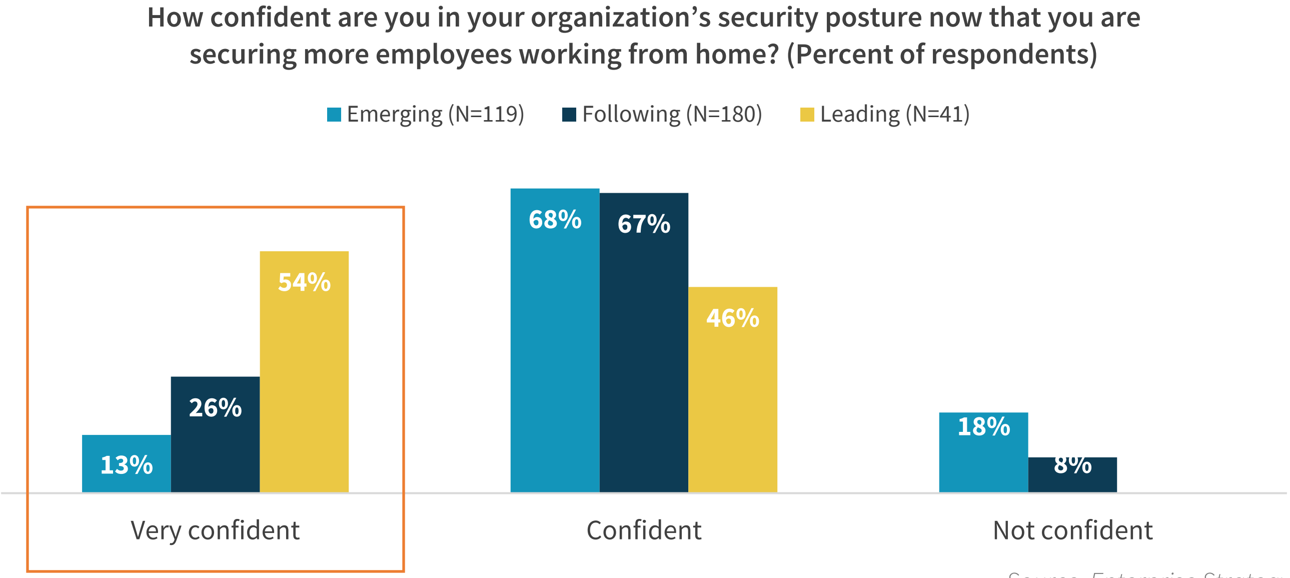
Source: Enterprise Strategy Group

Security Effectiveness

SASE improves security efficacy across distributed environments.

As discussed, a key driver of SASE has been the need to better architect security to address the inverted access paradigm: users and applications are more commonly outside of corporate offices and data centers than within. The pandemic has only exacerbated this trend, with respondents reporting that the percentage of their employees working remotely has increased from 20% prior to the COVID outbreak to 53% today. Leading organizations were much more likely to characterize the efforts to pivot security towards remote users as very smooth—39% versus only 8% of Emerging organizations. But of even more importance than the friction (or lack thereof) of securing remote users is the effectiveness of the approach. Here again, our Leaders performed much better than their Emerging counterparts and were 4.2 times more likely to indicate that they were very confident in their ability to secure employees working from home (see Figure 3).

Figure 3. Confidence in Securing a Distributed Workforce Rises with SASE Maturity



Source: Enterprise Strategy Group

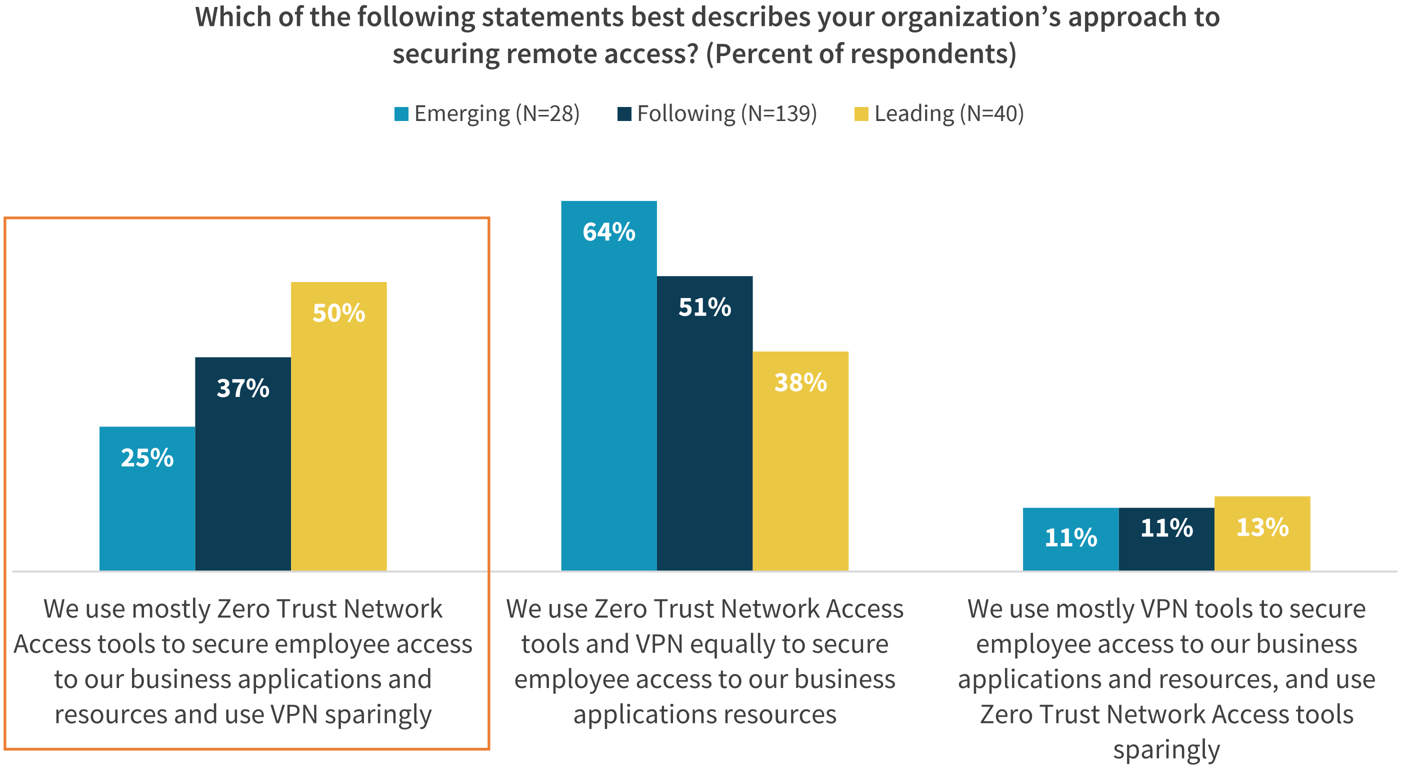
Why is this important at this stage in the pandemic? Simply put, the remote work scenario that was foreign to many just a year ago is here to stay. While our respondents believe the number of remote workers will decrease from where it stands today once the pandemic subsides, they anticipate the percentage of employees working remotely will remain 80% higher than prior to the pandemic. The emergence of this hybrid workplace means that organizations must take a longer-term view towards securing the distributed workforce and avoid stop-gap solutions that may increase complexity over the long term.

With that as the backdrop, what puts mature SASE organizations in a better position to support this model? While there is no single reason these organizations were more successful, one that does stand above the rest is the prioritization and early adoption of Zero Trust network access tools as a core component of SASE. Zero Trust is predicated on ignoring location and considering all possible context when assessing the trust of entities accessing corporate resources. While originally developed with traditional networks in mind, this approach is ideally suited for environments where users, devices, and applications are interspersed throughout various public and private networks.

Nearly three-quarters (73%) of Leaders have definitive plans to significantly reduce or eliminate the use of VPNs for remote access, compared to only 30% of Emerging organizations.

With regards to our findings, Leading organizations have already made a significant transition away from VPN and towards ZTNA, putting them in a better position to scale consistent secure access to a remote workforce (see Figure 4). The shift will only continue, as nearly three-quarters (73%) of Leaders have definitive plans to significantly reduce or eliminate the use of VPNs for remote access, compared to only 30% of Emerging organizations. The fact that so many of those already using ZTNA have further plans to move away from VPN should serve as a strong validation point with regards to these solutions.

Figure 4. Leading Organizations Have Prioritized Zero Trust Network Access



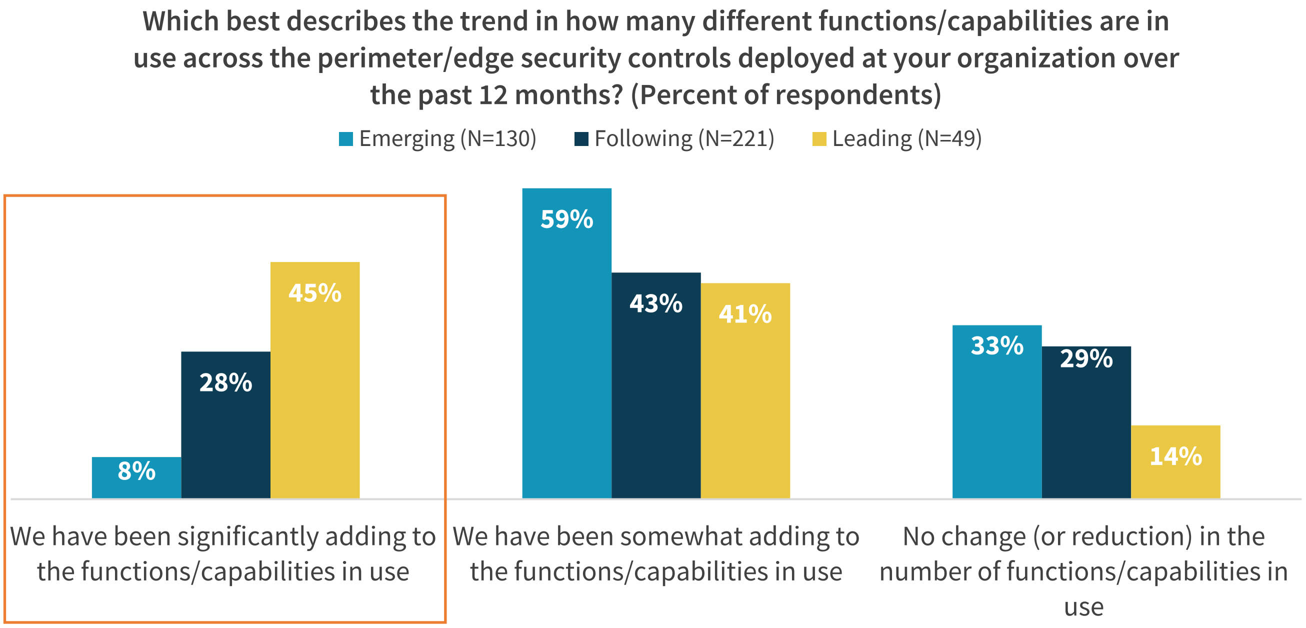
Source: Enterprise Strategy Group

Operational Efficiency

SASE encourages the use of expanded security functionality.

A core component of SASE is vendor consolidation and streamlining of the perimeter security infrastructure through a converged approach. Various benefits come from having fewer vendors in the environment such as improved efficiency, increased simplicity, and more consistent management. However, this consolidation does not require sacrificing functionality. In fact, Leading organizations are 5.6 times as likely as Emerging organizations to have been significantly increasing the capabilities and functions in use at the edge (see Figure 5).

Figure 5. Mature SASE Organizations Are Able to Utilize More Solution Functionality



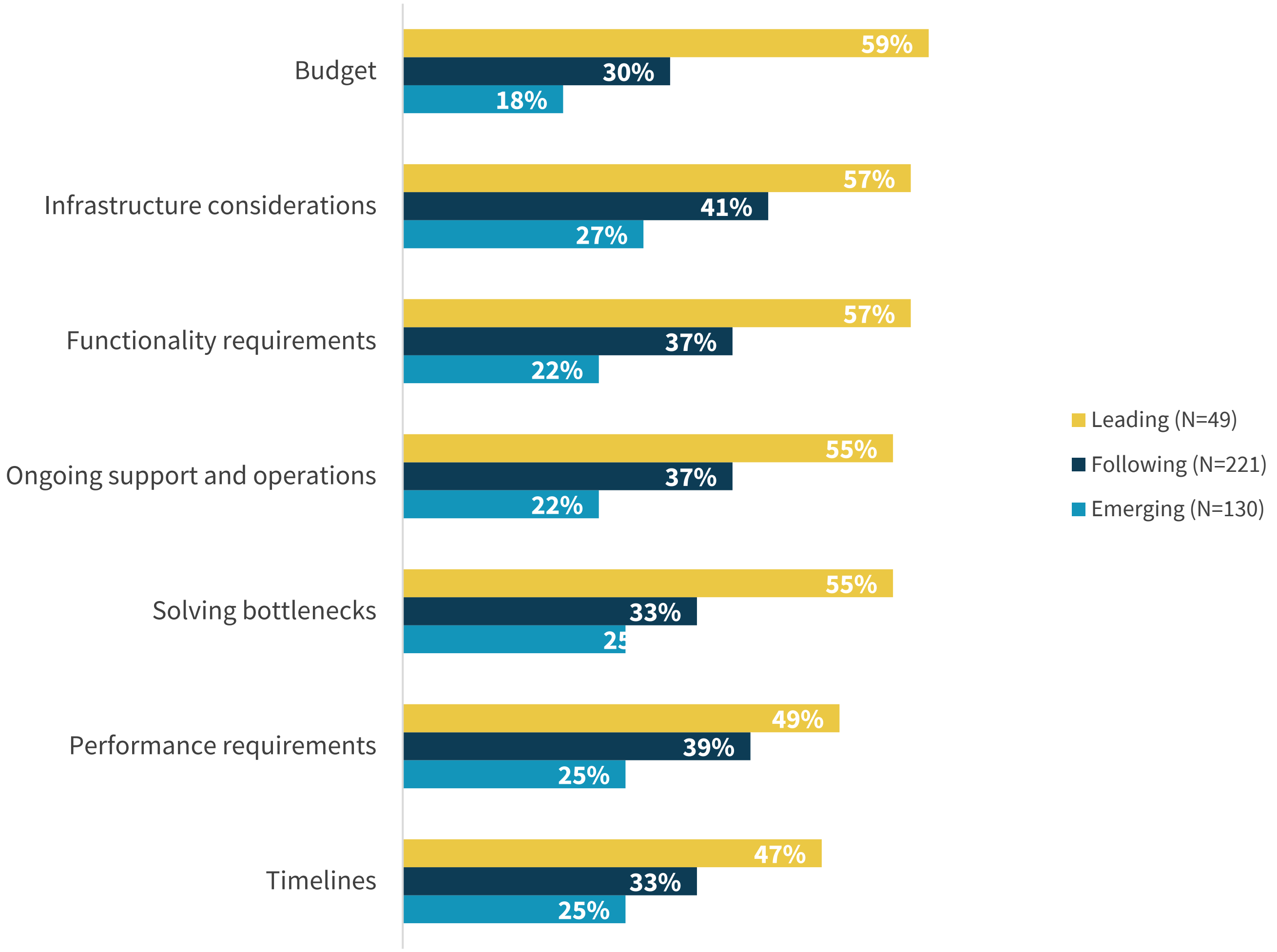
Source: Enterprise Strategy Group

Mature SASE organizations report significantly better collaboration across all the different groups involved in perimeter security procurement, deployment, and management.

Organizational dynamics play a key role in enabling this outcome. Procuring, deploying, and managing security tools is a team sport, requiring collaboration across a variety of groups, including IT, network, and security operations. Traditionally, IT operations has held tremendous influence over the selection and purchase of security tools. However, the pendulum is swinging towards the security and network organizations, giving these specialists more influence in the process and ensuring that the tools procured better align to their specific needs. The combination of fewer vendors and better upfront solution qualification helps ensure that the functional capabilities of products deployed are used to their full extent and that organizations do not end up with unused shelfware. With that in mind, it should come as no surprise that Leading organizations report significantly better collaboration across all the different groups involved in perimeter security procurement, deployment, and management (see Figure 6).

Figure 6. Strong Cross-functional Collaboration is a Key to SASE Success

Think about interactions the IT operations, network operations, and security operations teams have had. What is the quality of the collaboration in each of the following areas? (Percent of respondents rating collaboration as "Extremely good")



Source: Enterprise Strategy Group

Business Enablement

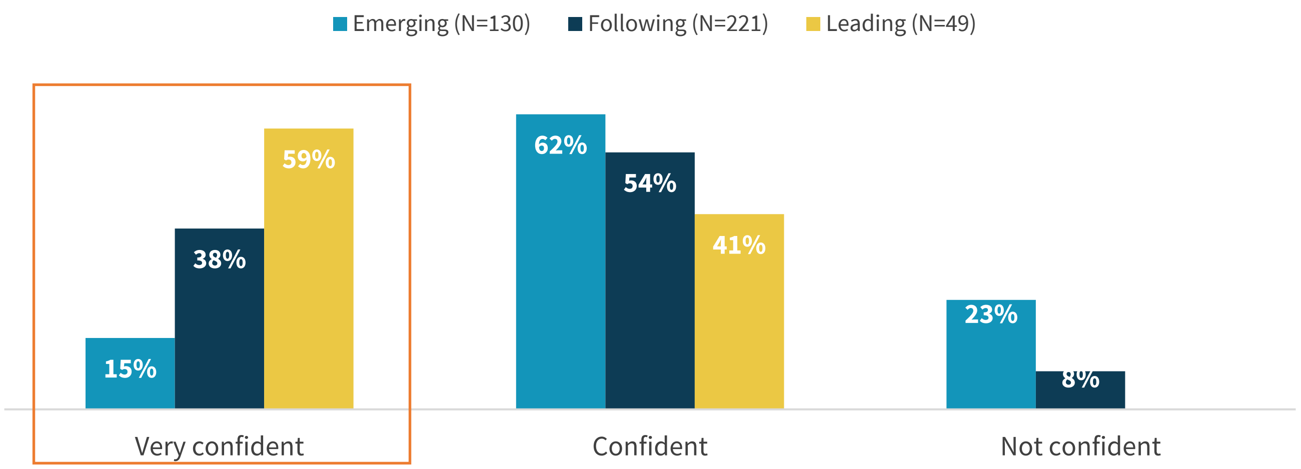
SASE enables consistent multi-cloud visibility.

The convergence of previously siloed tools, reduction of vendors, and better utilization of product capabilities also provide better visibility across the usage of cloud services. Most organizations have resources spread across a multitude of SaaS and IaaS providers. CASB, ZTNA, and even traditional VPN tools may all support access to these applications to one extent or another. Managing visibility across all these different tools is cumbersome and ineffective.

This is even more important in the decentralized IT model previously discussed. The security team is too often left out of the loop as the lines of business utilize cloud services. Granular visibility into cloud usage can ensure security teams are aware of the cloud resources in use, can prioritize protection towards those that may be business-critical or that house sensitive corporate data, and generally keep pace with the lines of business. Our research found that Leading organizations are 3.9 times as likely as Emerging organizations to be very confident in their cloud visibility (see Figure 7).

Figure 7. SASE Helps Reduce the Cloud Visibility Gap

How confident are you that the IT/security team is aware of all IaaS and SaaS usage by line-of-business employees at your organization? (Percent of respondents)



Source: Enterprise Strategy Group

A critical aspect of this visibility is data security, and DLP specifically. While the user, device, and application are all important aspects of access control, ultimately, the type and sensitivity of the data being used must be accounted for. This is complicated by the fact that different toolsets often have visibility over different parts of the infrastructure in support of DLP. CASB, endpoint, network, and secure web gateway tools all may have some level of DLP functionality. Leading organizations realize this and are more than 3x as likely as Emerging organizations to use at least 4 tools with DLP capabilities. However, as we've seen, these organizations are actively reducing the number of vendors in their environments and doing a better job of integrating visibility across all these controls to ensure consistency and reduce blind spots. With regards to data loss prevention, this is critical to ensure that corporate policy is correctly enforced regardless of where data resides or where the user accessing it is located.

SASE facilitates greater organizational resilience.

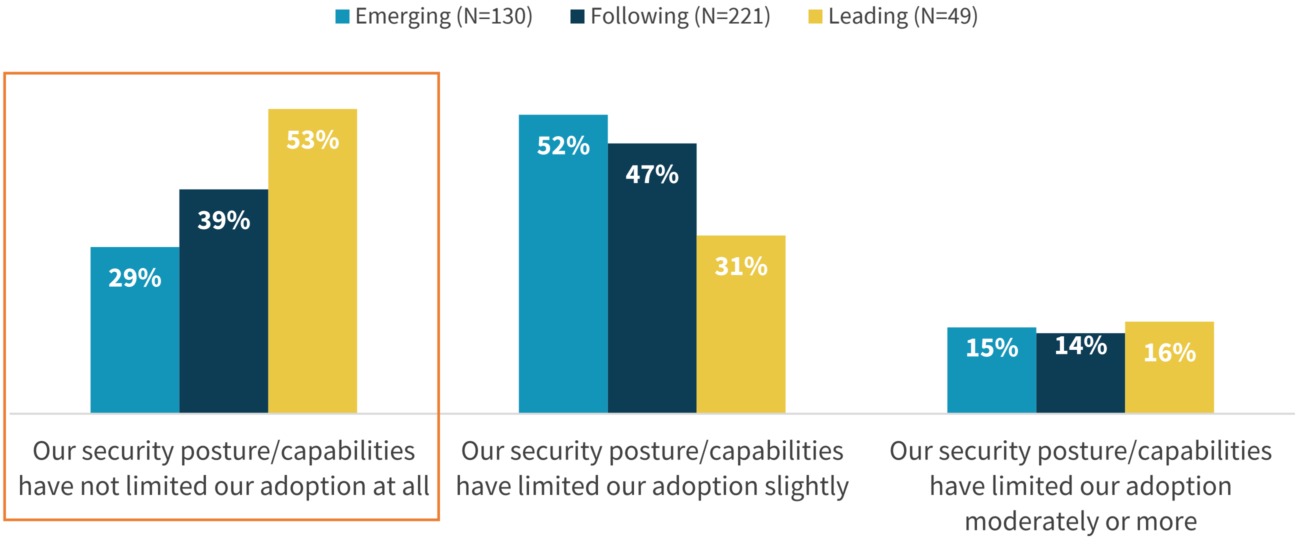
As discussed, cybersecurity must be considered through the lens of not just protecting the organization but also enabling the business as well. SASE represents the evolution of network security for networked resources to better address the reality of modern enterprise environments. This means moving beyond firewall-centric architectures and towards approaches that incorporate web, SaaS, private application, and data security. The goal must be a frictionless experience for business leaders and developers to allow them to focus on generating revenue and positive user experiences for customers.

The organizations that have prioritized SASE and realized cloud acceleration benefits are 4.4 times as likely to have extremely satisfied line-of-business users.

Due to the improved level of visibility SASE provides, a majority (53%) of Leading organizations report that security does not limit cloud adoption. Only 29% of Emerging organizations feel the same way (see Figure 8). More specifically, Leaders run an average of 128 business-critical cloud applications as compared to their Emerging counterparts who run an average of 81. Even more telling, the organizations that have prioritized SASE and realized cloud acceleration benefits are 4.4 times as likely to have extremely satisfied line-of-business users. To summarize: SASE ensures that security is not an inhibitor to cloud adoptions, enables organizations to support a higher number of applications in the cloud, and ultimately leads to more satisfied users.

Figure 8. SASE Reduces Impediments to SaaS and IaaS Adoption

How would you describe how your organization's security posture/capabilities has impacted its organization's adoption of IaaS and SaaS? (Percent of respondents)

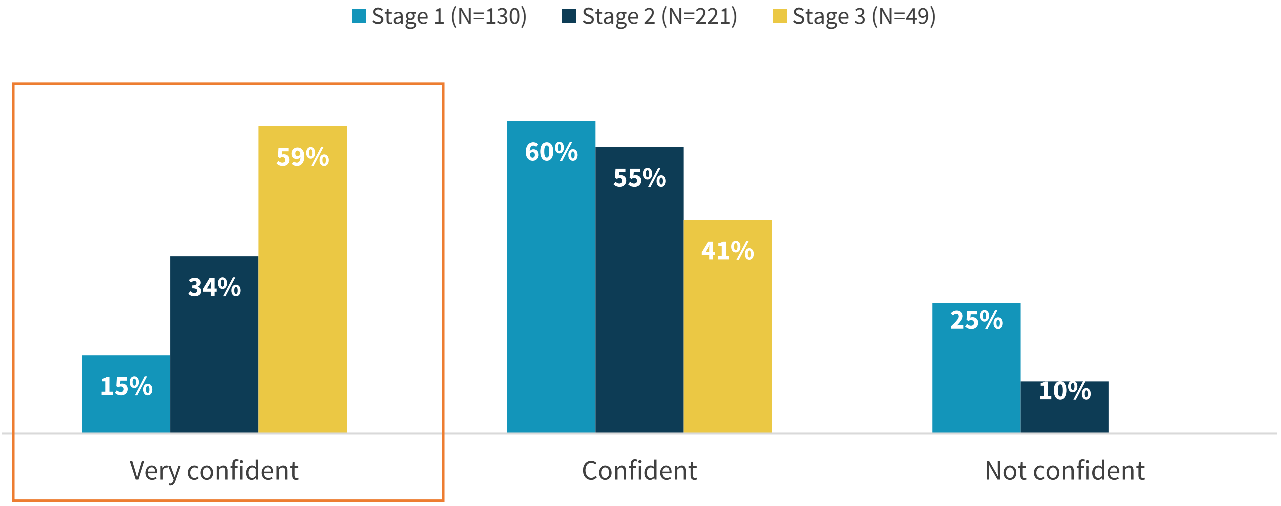


Source: Enterprise Strategy Group

The reasons for shifting resources to the cloud have been well established over the years, with resiliency being a prime motivator for many. The scalability and flexibility of the cloud enables organizations to be more agile and adaptive, something that should take on more importance considering the impact of the pandemic. So how does SASE impact resiliency? Leading organizations were 3.9 times more likely than their Emerging counterparts to be very confident in their organizational resilience (see Figure 9).

Figure 9. Mature SASE Organizations Have More Confidence in Their Resilience

How confident are you in your organization's ability to adapt and thrive through major societal and macroeconomic disruptions? (Percent of respondents)



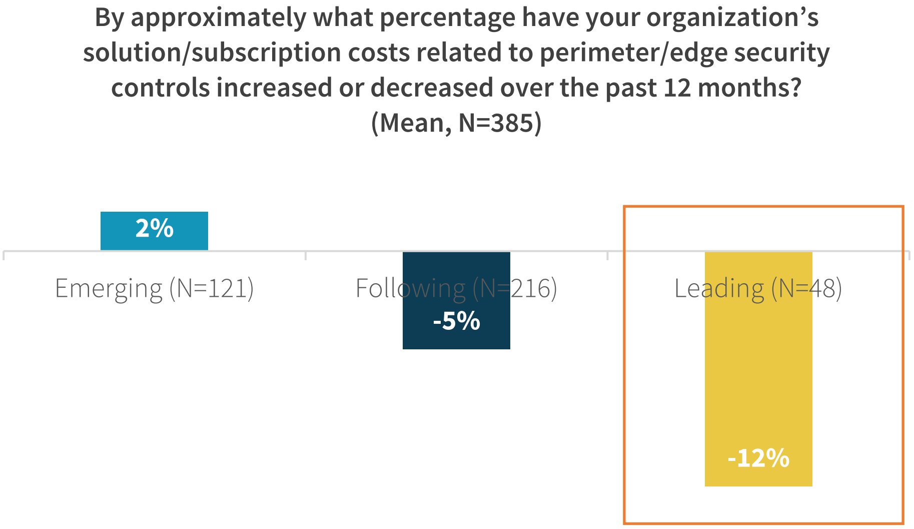
Source: Enterprise Strategy Group

Cost

SASE helps organizations reduce costs.

Despite recognizing all the aforementioned benefits, organizations with a mature approach to SASE are more likely to report cost savings across both solution/subscription and operational expenses (see Figure 10). Working with fewer vendors and developing more strategic partnerships with suppliers can help optimize upfront procurement costs. Yet perhaps more importantly, Leading organizations reported a 14% reduction in operational costs, compared to just a 1% reduction by Emerging organizations. Reducing the number of management systems administrators must be trained on, eliminating duplicative policy management across different systems and the potential for human error that it can cause, and improving the efficiency of threat detection and response are all direct benefits of SASE approaches, which ultimately can help reduce operational costs.

Figure 10. Despite Using More Tools and Functionality, Mature SASE Organizations Report Lower Costs



Source: Enterprise Strategy Group

In Conclusion: The Bigger Truth

As our research has shown, the significant market attention surrounding SASE is clearly warranted. Leading organizations report significantly higher security, operational, business, and cost benefits than their Emerging counterparts. Specifically:

- Leaders are 4.2 times more likely to be very confident in their ability to secure employees working from home.
- Leaders are 5.6 times more likely to have been significantly increasing the capabilities and functions in use at the edge.
- Leaders are 3.9 times more likely to be very confident in their visibility across their distributed cloud environments.
- Over half (53%) of Leaders say security has not limited their organization's adoption of cloud services at all.
- Leaders report a 12% reduction in solution/subscription costs and a 14% reduction in operational costs.

Fundamentally rearchitecting cybersecurity architectures is no small project and not one any organization should undertake lightly. Yet while SASE is ultimately just that type of initiative, there are two important things to keep in mind when beginning to assess where and how to begin with SASE. First, the shift to SASE does not have to occur all at once. In fact, many organizations have taken a use-case-based approach and plan to expand over time. Second, the benefits derived as a result of SASE architectures can help the organization be more resilient and agile, helping to elevate SASE initiatives from a cybersecurity issue to a broader business initiative.

By exploring the steps mature SASE organizations have taken, analyzing the benefits they have seen, and mapping both to priorities and capabilities of one's own organization, it becomes easier to find a starting point, start the journey, and begin reaping the tangible benefits of SASE in the short term.

Appendix I: Research Methodology and Demographics

To gather data for this report, ESG conducted a comprehensive online survey of information security and IT professionals responsible for evaluating, purchasing, and managing network and cloud security products and services. More than two-thirds of respondents held senior IT or security titles (i.e., CIO, CISO, VP of IT/IS, or equivalent) while the remainder held middle management and staff titles. Respondents were based evenly across North America (50%) and Europe (50%). All respondents were employed at organizations with 500 or more employees. Specifically, 11% were employed at midmarket organizations (i.e., those with 500 to 999 employees) and 89% at enterprises (i.e., organizations with 1,000 or more employees). Respondents represented numerous industry and government segments, with the largest participation coming from technology/communications (20%), business and financial services (18%), manufacturing (14%) healthcare and life sciences (13%), retail/wholesale (10%), and government agencies (9%).

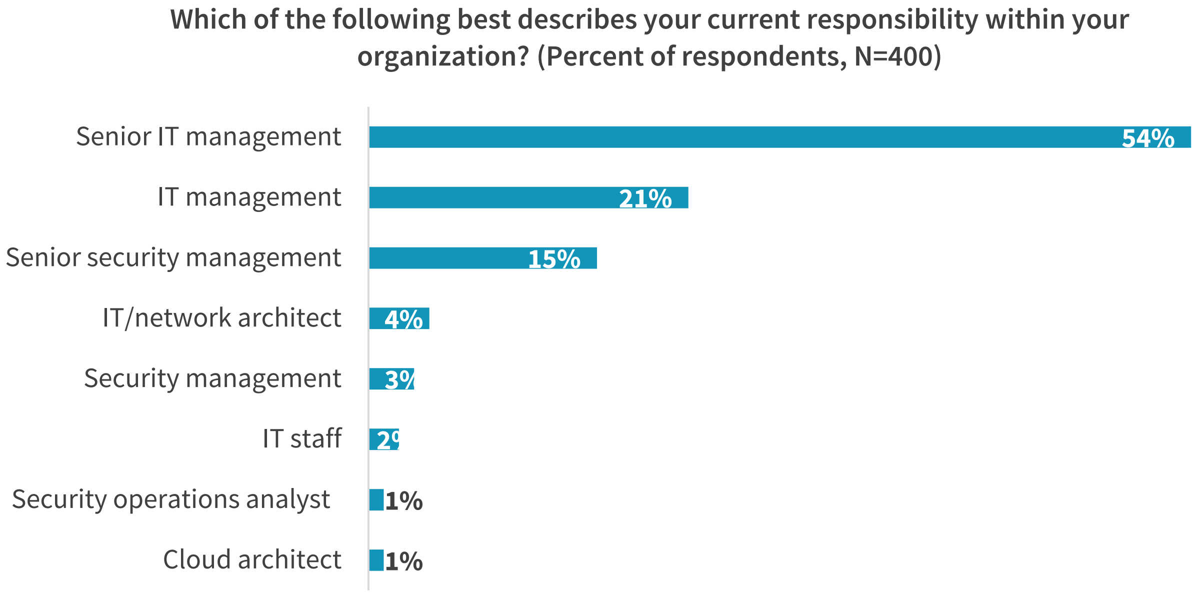
The survey was fielded between November 13, 2020 and November 30, 2020.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 400 respondents remained.

All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents. Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

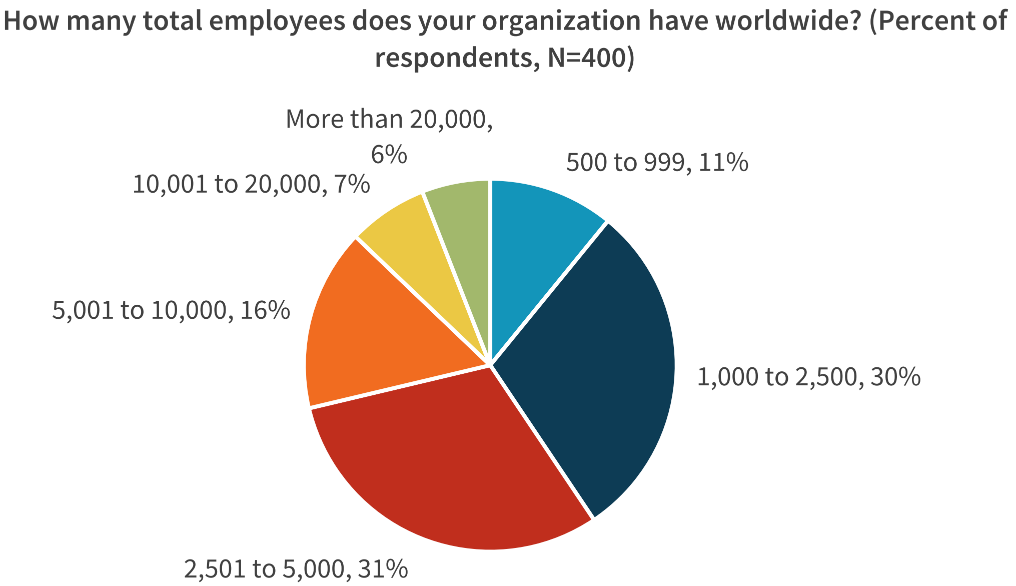
Figures 11 - 14 detail the full demographics of the respondent base: individual respondents' roles, as well as respondent organizations' total number of employees, annual revenue, and primary industry.

Figure 11. Survey Respondents, by Current Responsibility



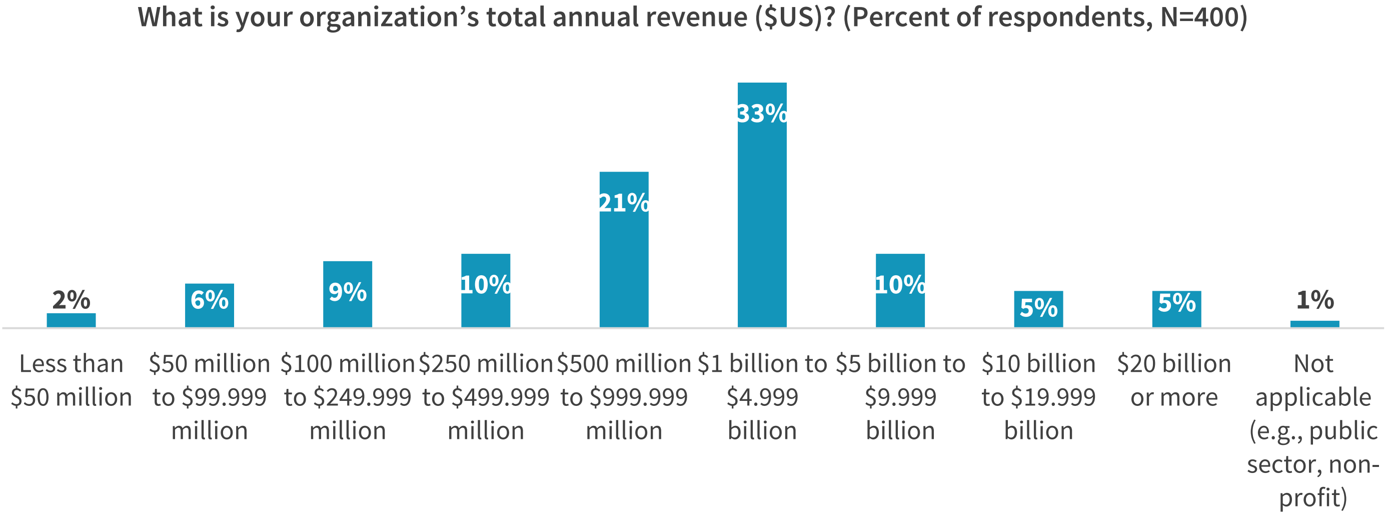
Source: Enterprise Strategy Group

Figure 12. Survey Respondents, by Company Size (Number of Employees)



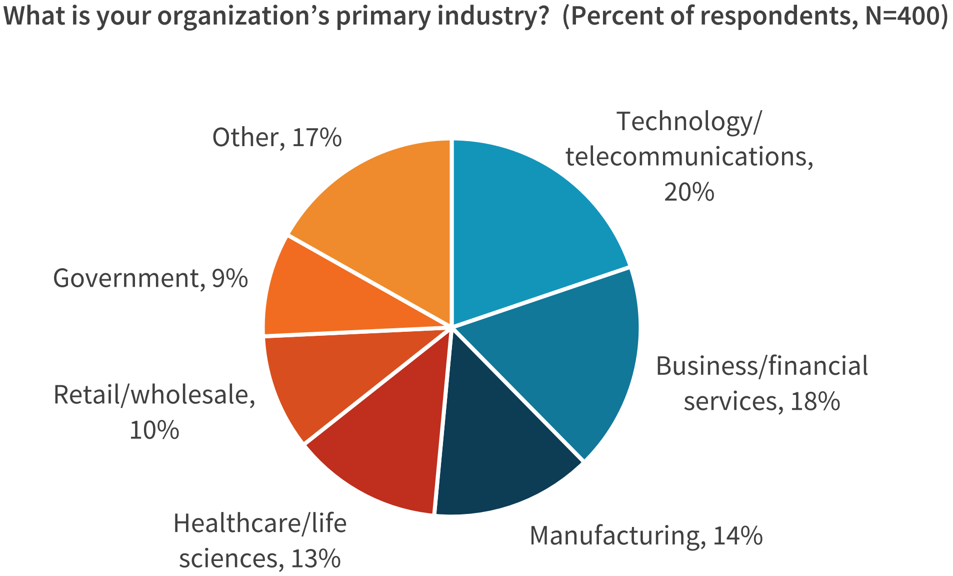
Source: Enterprise Strategy Group

Figure 13. Survey Respondents, by Company Size (Annual Revenue)



Source: Enterprise Strategy Group

Figure 14. Survey Respondents, by Industry

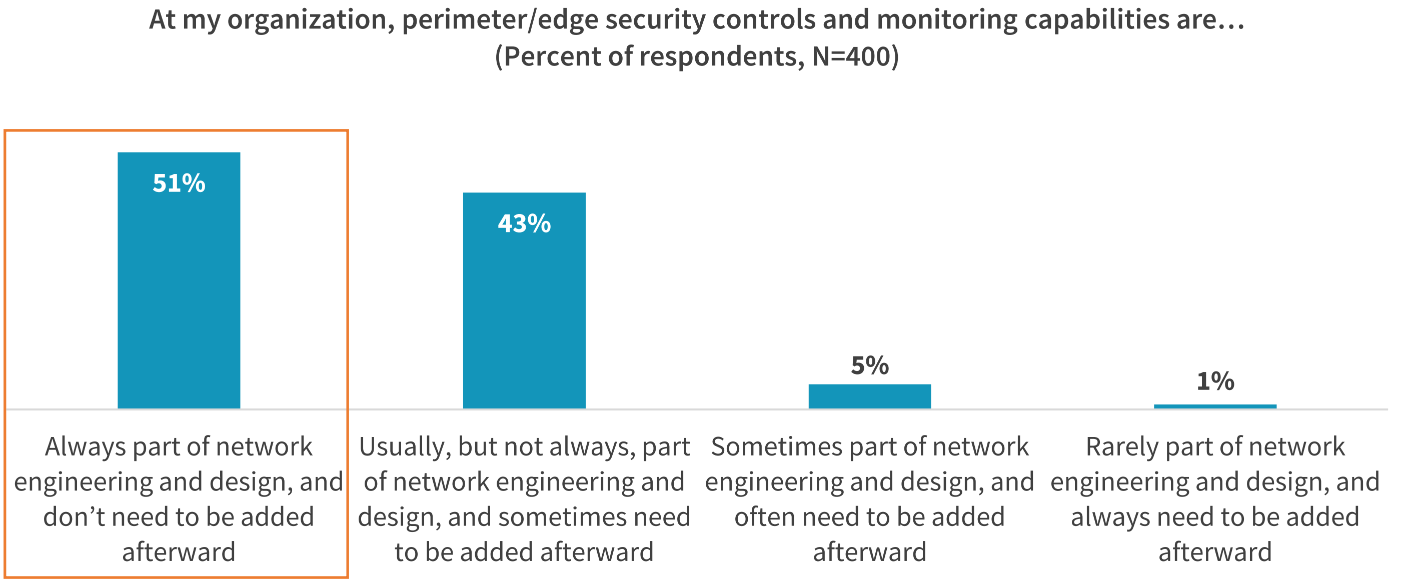


Source: Enterprise Strategy Group

Appendix II: Survey Questions ESG Used to Evaluate SASE Maturity

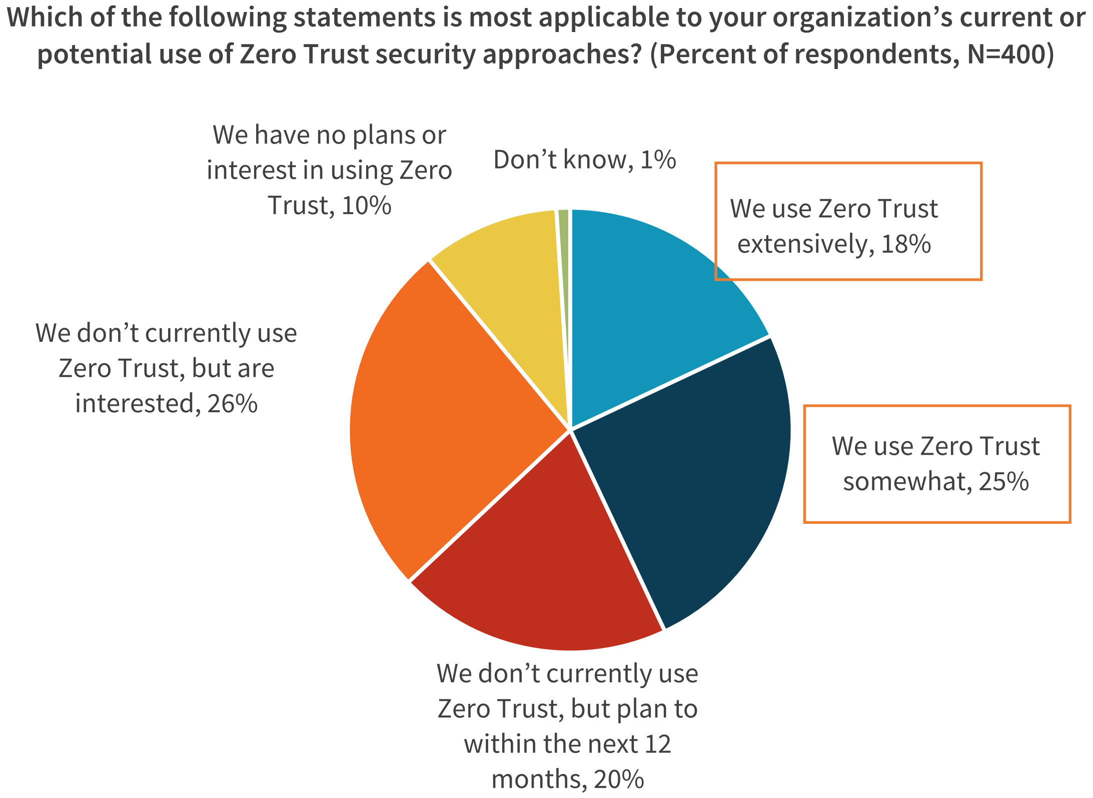
ESG assessed the SASE maturity of organizations participating in the research survey based on their responses to five key questions about network security technology, controls, and processes. Figures 15 - 19 detail these questions and the highlighted responses indicate those that ESG evaluated as most mature.

Figure 15. Maturity Characteristic 1: Proactive Edge Security Architecture



Source: Enterprise Strategy Group

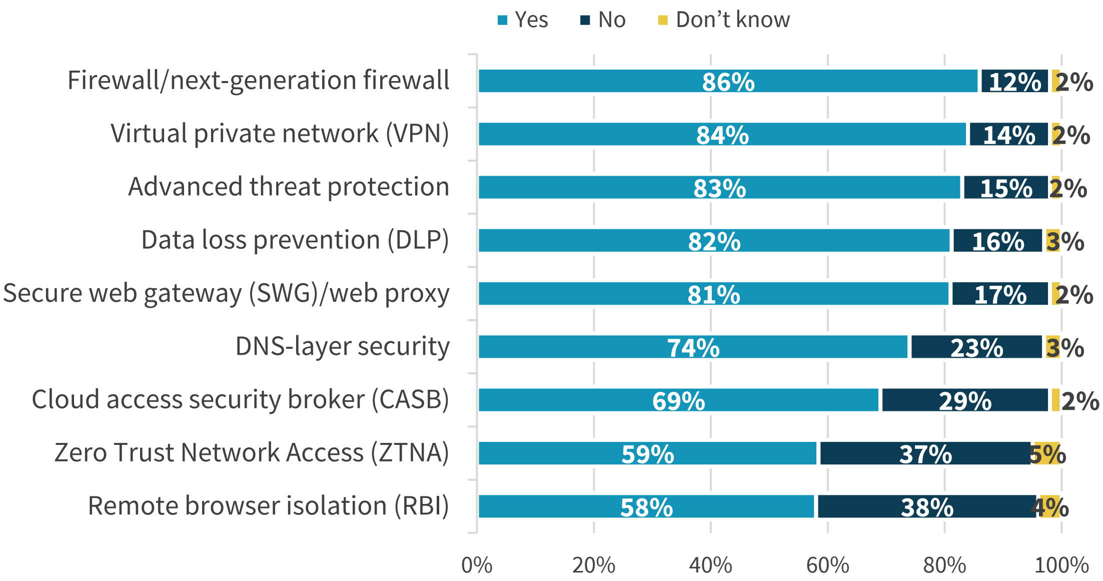
Figure 16. Maturity Characteristic 2: Zero Trust Security Philosophy



Source: Enterprise Strategy Group

Figure 17. Maturity Characteristic 3: Deployment of a Robust set of Security Controls and Capabilities

Please indicate if your organization has deployed each of the following edge/perimeter security controls and monitoring tools. (Percent of respondents, N=400)

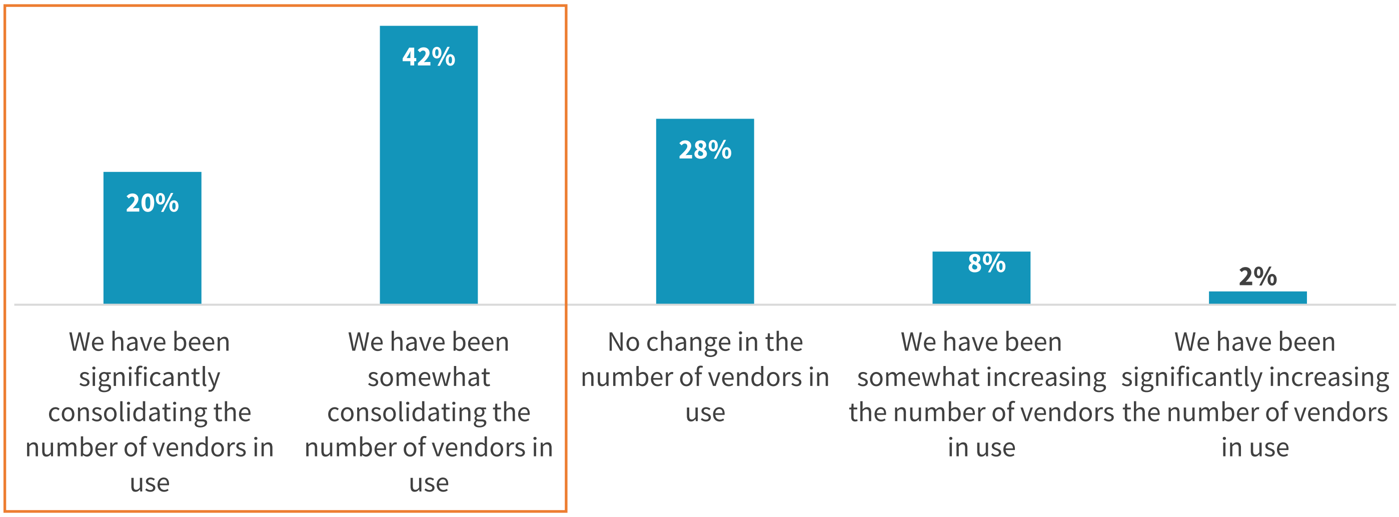


To be considered a Leader, organizations must have reported 6+ controls are in use (omitting VPN)

Source: Enterprise Strategy Group

Figure 18. Maturity Characteristic 4: Active Consolidation of Edge Security Vendors in Use

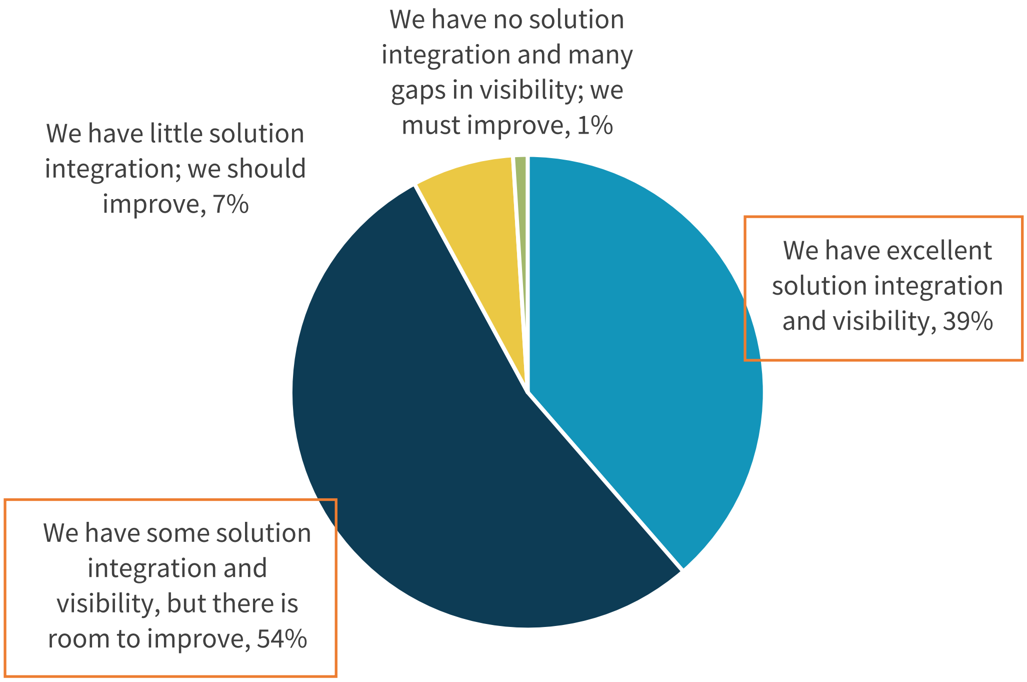
Think of the number of vendors in use across all perimeter / edge security controls. Which best describes the trend in how many vendors are in use at your organization over the past 12 months? (Percent of respondents, N=400)



Source: Enterprise Strategy Group

Figure 19. Maturity Characteristic 4: Active Consolidation of Edge Security Vendors in Use

How would you describe your organization's solution integration and security visibility across perimeter/edge security controls? (Percent of respondents, N=400)



Source: Enterprise Strategy Group

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188