Publication date:
31 March 2023
Author:
Fernando Montenegro

The Rise of Single Vendor SASE

Improving security operations and collaboration with a unified approach

Brought to you by Informa Tech

Omdia commissioned research, sponsored by Palo Alto Networks

Contents

Executive summary

- For many organizations, SASE is becoming a key architectural choice for connecting branches and workers with the applications and data they need.
- SASE deployments offer opportunities for organizational improvements, cost reductions, and better security controls, and can be deployed in a phased approach.
- For those choosing single-vendor SASE, vendor security capabilities and strategic roles are key factors to consider.

Organizations are looking to streamline their security and networking infrastructure to not only reduce costs, but also to be more flexible in the face of changing, uncertain economic conditions and the shift to hybrid work. This is simultaneously a consequence of, and a driver for, digital transformation at the level of business and operational processes. Infrastructure must be more agile but do so in a manner that is efficient, robust, and secure.

Ensuring security in a hyper-connected world undergoing constant change is challenging. However, organizations are already well along the adoption path with Software-Defined Wide Area Networks (SD-WAN) to converge and control networking flexibility, Security Service Edge (SSE) to extend network security, and Secure Access Service Edge (SASE) for a comprehensive and fully integrated solution to both.

Most organizations have already started their SASE implementations, with pilots and limited deployments turning into wide-scale production use. There is some uncertainty, however, about the precise route to take. These projects cross organizational boundaries, which require consideration for managing selection, purchase, deployment, and operations, but they are already leading to significant improvements in internal communication and collaboration. In projects such as these, a single-vendor approach has emerged as a strong strategy for overall integration, maximizing the impact of advanced analytics using AI techniques, and more. This evolution of security architecture also presents a valuable opportunity for organizations to improve both security outcomes and collaboration. Moving to an adaptable networking and security infrastructure often requires integrating people and processes at least as much as the technology. While many are taking technology-led decisions to invest in SD-WAN, SSE, or SASE, they are doing so having already brought different internal teams together and demonstrating there is commitment from senior management to make it work.

Using a single vendor for a combined SASE offering is an option that is gaining popularity. Those choosing to do so look primarily at a vendor’s capabilities as a strong security provider, a true strategic partner for the organization, and one that can effectively address the needs for a seamless and secure digital user experience.

Introduction

Given the broad macroeconomic patterns of uncertainty and the need for efficient use of resources, organizations are actively seeking to transform and optimize their approach to technology. There is an understanding that digital transformation revolves around broader, holistic ways to process and analyze data, as well as deploy interesting new smart devices. Further, this is where artificial intelligence (AI) is quickly improving and playing a more active role, artificial intelligence (AI) capabilities are quickly improving, fostering powerful new connections between data and operations.

The shift from dedicated hardware-based products to a distributed, cloud-delivered service makes the technology both more efficient and effective. SD-WAN, for example, offers greater flexibility, resiliency, and adaptability to change than traditional networking.

The demand for these highly distributed network capabilities—be they enterprise networking connectivity needs or those coming from IoT/OT—comes not only from the changes in customer and supply chain relationships, but also evolving working practices, which were accelerated by the COVID-19 pandemic, and may be pushed further as organizations and individuals assess carbon footprints and adapt to climate changes. These evolving practices, driven by flexibility and efficiency, have a profound impact on security, which for many was already a complex challenge. The approach that secures services at the point of access, wherever that may be, is SASE, which efficiently combines network and security functions to preserve maximum flexibility, resilience, and security.

SSE appears as an intermediary technology, offering security features but making assumptions about the underlying networking capabilities. This approach may be necessary for some organizations unwilling or unable to make the transition to a unified SASE architecture and should be viewed as a steppingstone to SASE.

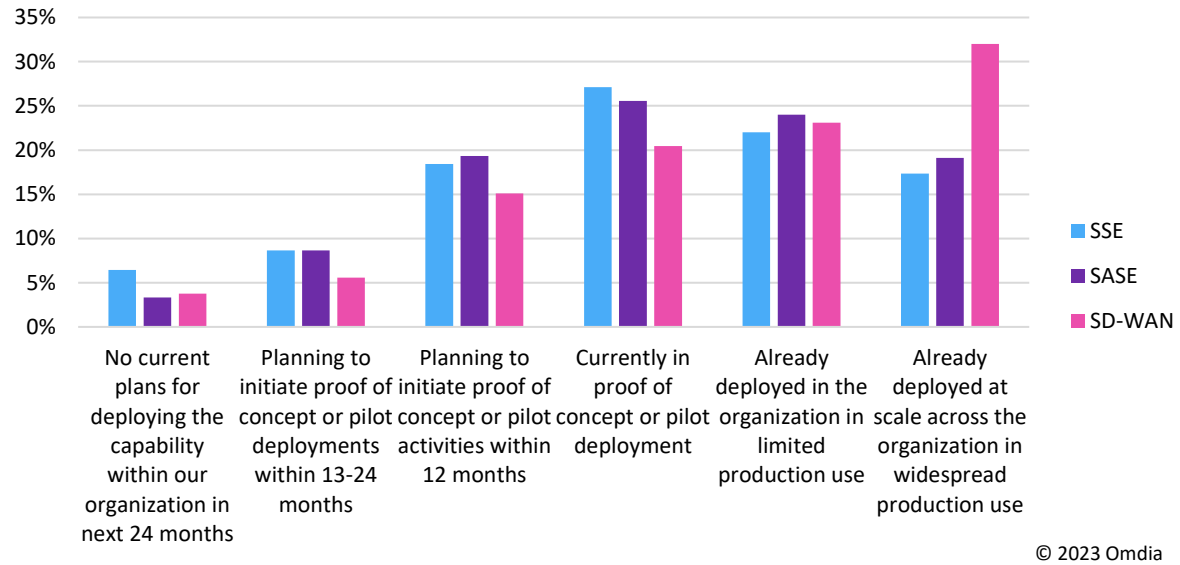
This paper looks at how flexibility and security need to be embedded into the distributed fabric of IT infrastructure, through SD-WAN, SASE, or SSE, and at the challenges organizations face as they move towards a more comprehensive and integrated approach. Specifically, it investigates common challenges around SASE deployments and investigates the requirements for a single-vendor SASE approach.

For the accompanying research, a sample of 450 respondents were surveyed, from organizations currently using or considering SD-WAN, SSE, or SASE. These organizations span a mix of industries and geographic regions, with a minimum of 1,000 employees and over 25 sites, branches, or other facilities. Roles and responsibilities ranged across senior and middle management to individual contributors, in either security or network functions, and additional responses from senior executives. This breadth of participation provides scope for understanding sentiment and strategy, as well as the realities of actual deployments. Please see the appendix for additional details.

SD-WAN started it, but SASE is growing quickly

Making far-reaching infrastructural changes is a significant commitment, generally requiring a refresh of operational processes and additional resources and skills to accompany the investment in technology. Larger organizations typically carefully plan and then trial with proof of concept or pilots before moving ahead with larger scale production deployments, but those with more complex needs—operating in more countries, greater numbers of employees—seem to be further along the adoption path.

Figure 1: Adoption stage for SD-WAN/SASE/SSE



Source: Omdia

This is very clear in the deployment of SD-WAN, which is in production use in over half (55%) of organizations, with almost a third (32%) reporting it is already deployed at scale. A further fifth (20%) are already piloting, with another fifth (21%) planning to within two years. With its ability to make larger networks easier to manage and be more cost effective, it should be no surprise those progressing furthest and fastest with production use are larger organizations and particularly those managing networks across more sites and countries.

The trend in SSE is of growing adoption, but the wave is lagging SD-WAN with a little over a third (39%) in limited or widespread production use, but again higher (51%) for organizations operating over five or more countries.

The wave of adoption for SASE is similar, but further ahead than SSE, with 43% already having some production use. This rises to 58% for organizations operating in five or more counties. Deployment at scale in widespread production use rises significantly from the average of 19% to 32% for organizations with over 25,000 employees.

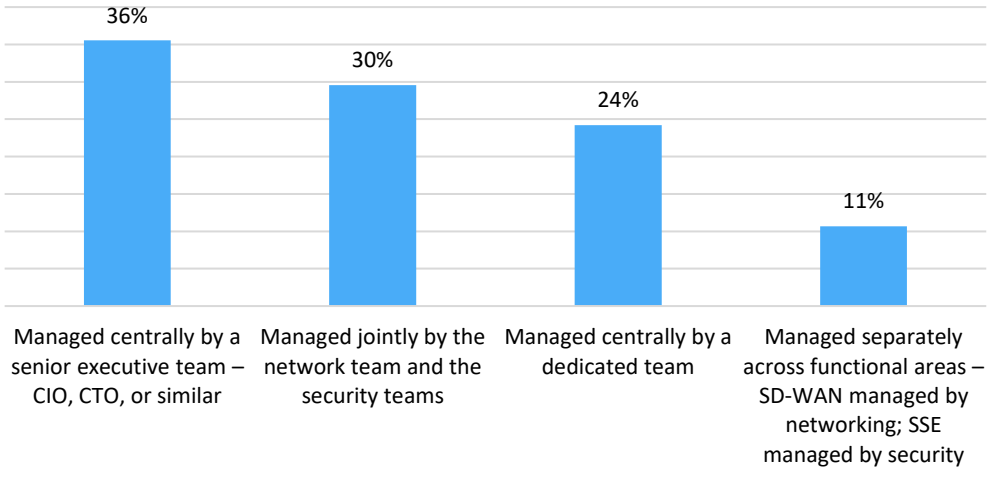
The data shows all technologies are moving ahead in their implementation status, with numerous respondents indicating production-level deployments. For organizations considering their plans as it relates to SASE deployments, there is ample evidence the approach is already eminently viable now.

SASE is an opportunity to improve the organization

Purchasing and operational decisions for infrastructure will always be driven by multiple agendas and needs, especially when performance and flexibility must be balanced against security and control, as is the case for SASE. Given the cross-functional nature and overlaps in the technologies involved, it would seem inevitable these deployments will bring different parts of the organization together and affect the communication and working dynamics.

The research shows managing purchasing decisions centrally appears to be the favored approach, with over a third (36%) opting for a senior management team in charge. Those who have already widely deployed SASE for production use at scale are more in favor of this approach (41%). This is understandable, given the transformative role SASE can have.

Figure 2: How does your organization make purchase decisions in relation to its SD-WAN/SSE/SASE initiative?

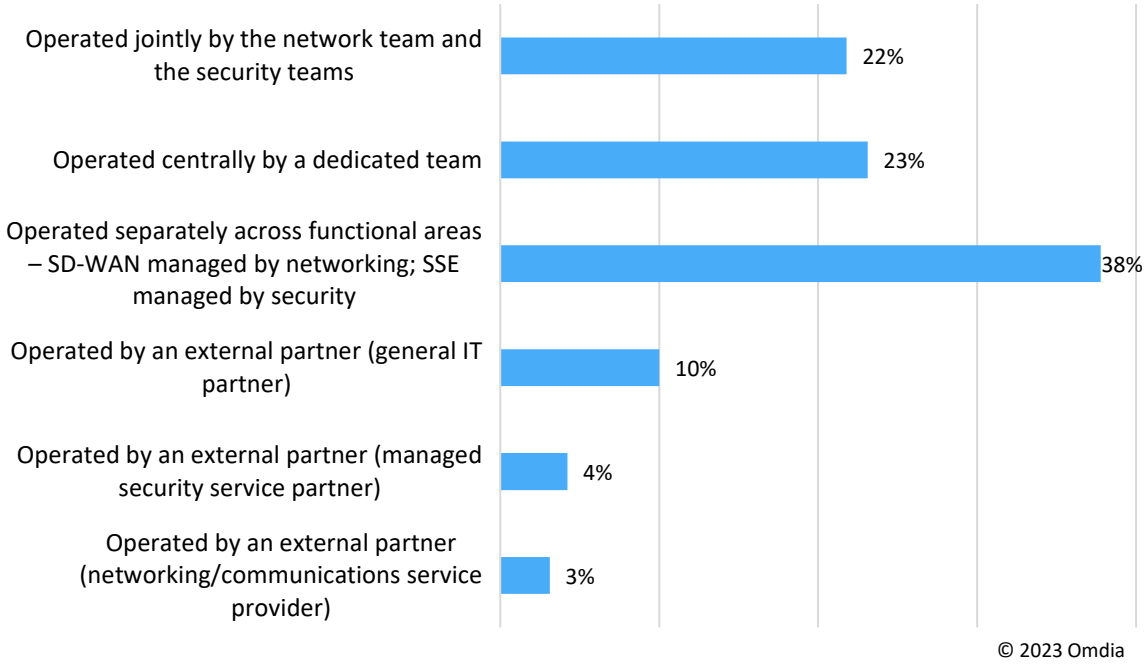


Source: Omdia

One important aspect to observe is these deployments are, by a large margin, still operated internally within the organization. While using external partners for support on production deployments is an option, the majority of deployments are operated by internal teams.

Within those teams, those with distinct technology options (SD-WAN, SSE) manage them separately, while SASE offers the opportunity for deeper integration.

Figure 3: How does your organization operate its SD-WAN/SSE/SASE initiative?



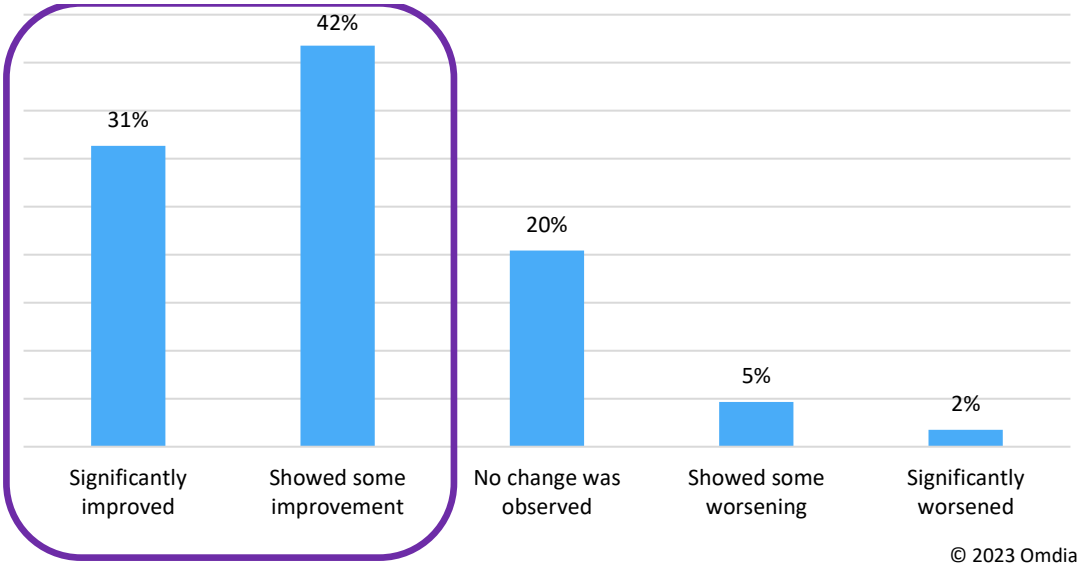
Source: Omdia

SASE deployments give the organization an opportunity for improvement in terms of collaboration between stakeholders. Encouragingly, the data shows many of those are taking that opportunity and seeing positive results. Most respondents (73%) indicated there was an improvement, 10x the number (7%) that indicated the situation had worsened, and almost a third (31%) thought communications had significantly improved.

For organizations with over 25,000 employees, those indicating overall improvement were even greater (82%), demonstrating that even major changes in larger and often longer-standing establishments can still lead to positive internal impacts.

How the organization gets to that point might be equally important. Those who made their SD-WAN/SSE/SASE purchasing decisions centrally managed by a senior executive team indicated a higher level of significant improvements in communications between line of business and IT functions.

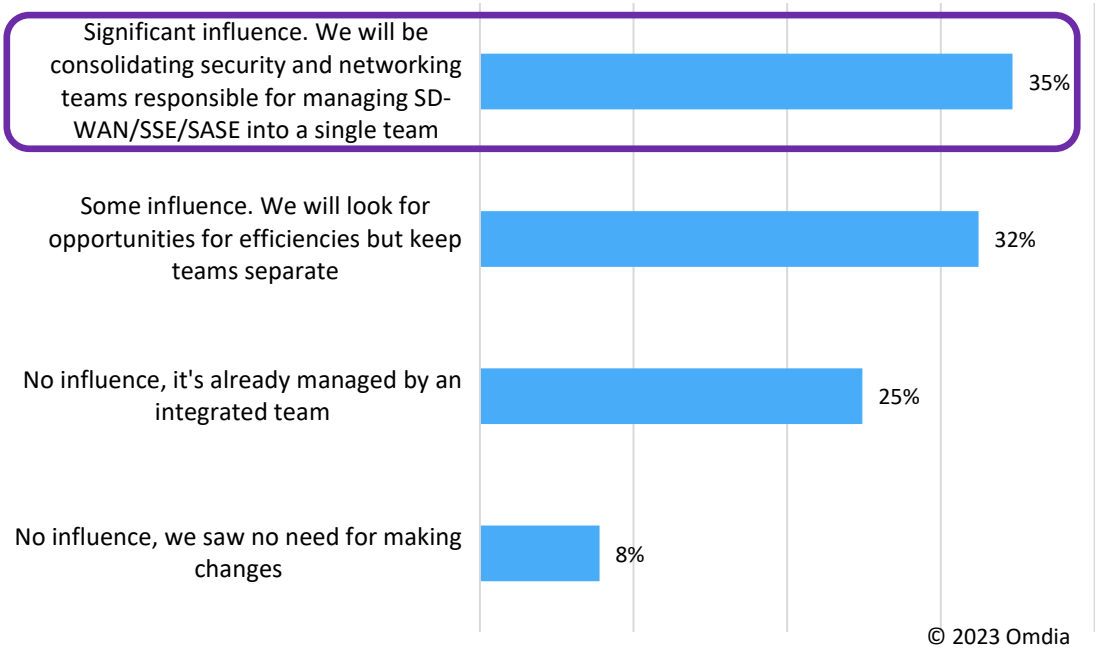
Figure 4: To what extent has the organizational efforts to deploy SD-WAN/SSE/SASE improved the communications between IT stakeholders and other stakeholders (lines of business, senior management) within the organization?



Source: Omdia

Does this affect the future? Certainly, while a quarter (25%) already managed their deployment with an integrated team, just over a third (35%) indicate their deployment experiences are a significant influence towards consolidating security and networking for SD-WAN/SSE/SASE into a single team.

Figure 5: To what extent have the organizational efforts and learnings to deploy SD-WAN/SSE/SASE influenced the organization to make changes to how it structures the teams supporting the deployment?



Source: Omdia

This optimization of teams also appears in correlation to SASE deployments: those that have already deployed SASE are also more likely to be managing their deployment in an integrated fashion (31% vs average of 25%).

The key point that surfaces from the research is that organizations can use their SASE projects to improve internal communications, streamline operations, and rethink how teams can be structured.

Organizations look for wins in cost reduction, security improvement, and integration

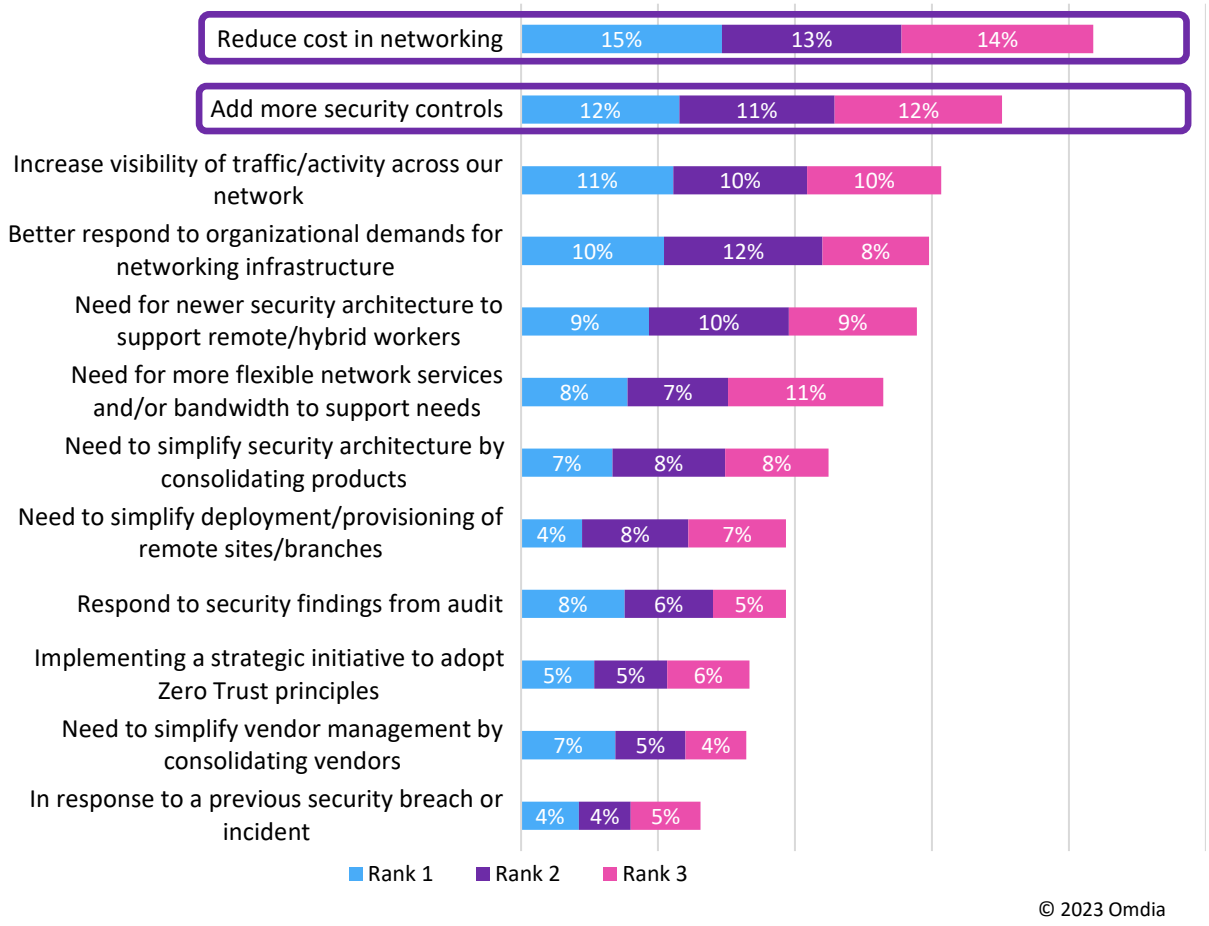
When asking what drives the interest in SASE and similar technologies, a few themes stand out.

As is often the case with IT, cost is a big driver. Reducing cost is a tangible benefit, and with the soaring use of networking, from connecting supply chains to a distributed workforce, addressing the cost of networking is the most important priority for first, second, and third selections.

Risk mitigation is another tangible benefit, sometimes overlooked, but it brings real and reputational cost when a risk becomes a reality in the form of a breach, intrusion, or attack. Adding more security control and visibility of activity are both seen as important drivers slightly behind cost reduction.

Being able to respond to change in the form of both organizational demands and changing working practices such as remote or hybrid working, both figure highly.

Figure 6: Considering the options below, please rank in order of importance (1 being highest) what are the top 3 drivers for your organization around SD-WAN/SSE/SASE

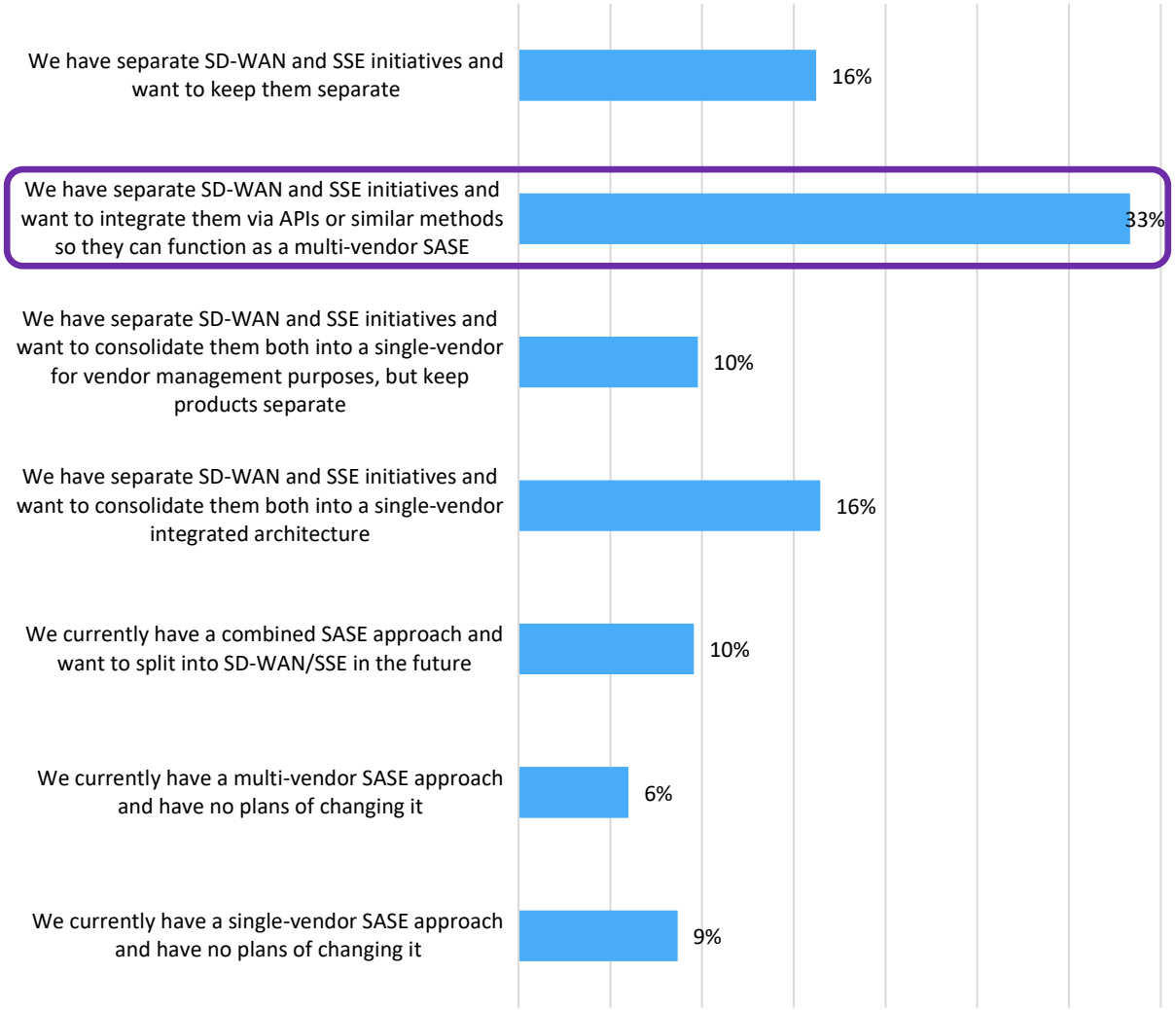


Source: Omdia

SD-WAN and SSE have been useful steps for organizations wanting to evolve both networking and security infrastructure, and many see SASE as a further positive step. Organizations must balance how many partners or suppliers they want to work with, and how to manage deployment. A single vendor proposition may deliver a more consistent and integrated approach.

The research shows almost three-fifths (59%) have separate SD-WAN and SSE initiatives that they want to combine in some way. A third (33%) want to integrate via APIs to develop a multi-vendor SASE, and 26% indicate they want some variation of single-vendor implementation (16% want a single vendor integrated architecture for SASE, and 10% a single vendor, but still with separate products). A quarter (26%) prefer keeping SD-WAN and SSE separate, with 16% already in that position, and 10% planning to split a currently combined SASE.

Figure 7: Given your current plans for SD-WAN/SSE/SASE, what is your preferred approach to deployment?



Source: Omdia

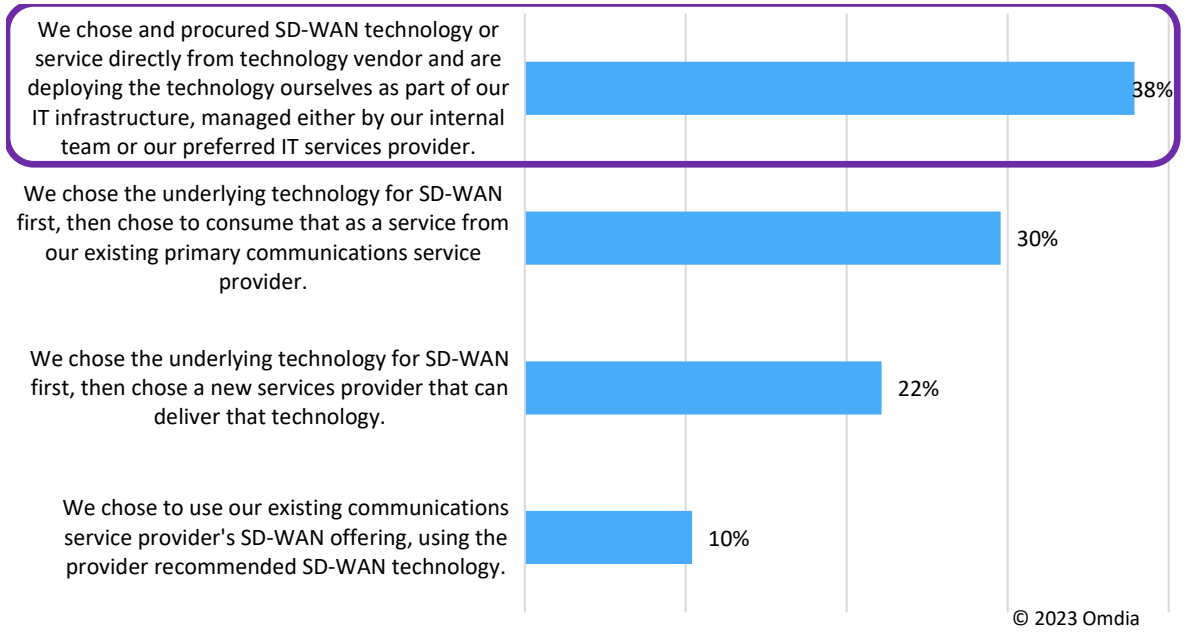
Choosing the path forward – technology ahead of provider

When forging a path ahead to deploy SD-WAN, SSE, or SASE, many organizations have two key choices to make: what technology to use, and whom to partner with?

A consistent theme that surfaced from the research is organizations are first looking at the technology being offered—which vendor (or vendors) offer SASE functionality—then later picking out if and how they will work with an external service provider.

For SD-WAN deployments, most organizations choose the technology first, with only 10% going first to a communications provider and using their offering. For those choosing technology first, 38% procure from the vendor and deploy on their own infrastructure, managing it themselves internally, or using an IT services partner. When considering those with an existing widespread production deployment of SD-WAN, the number taking this route grows to 56%.

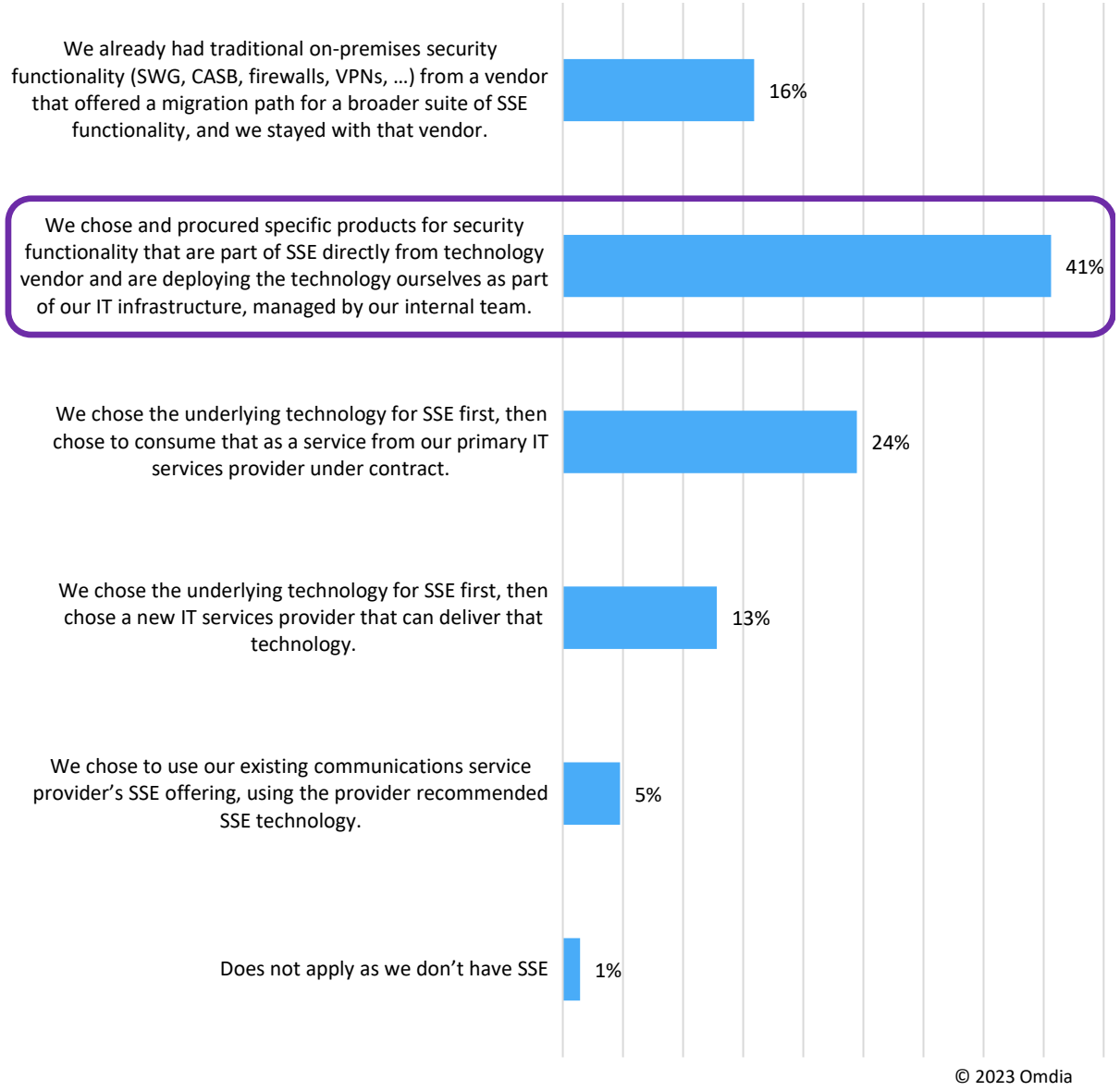
Figure 8: For SD-WAN technology, how did/does your organization perform vendor selection?



Source: Omdia

The decision takes a similar route with SSE, even when there is the option of a migration path from an existing security supplier, 41% will go with choosing specific products for SSE first.

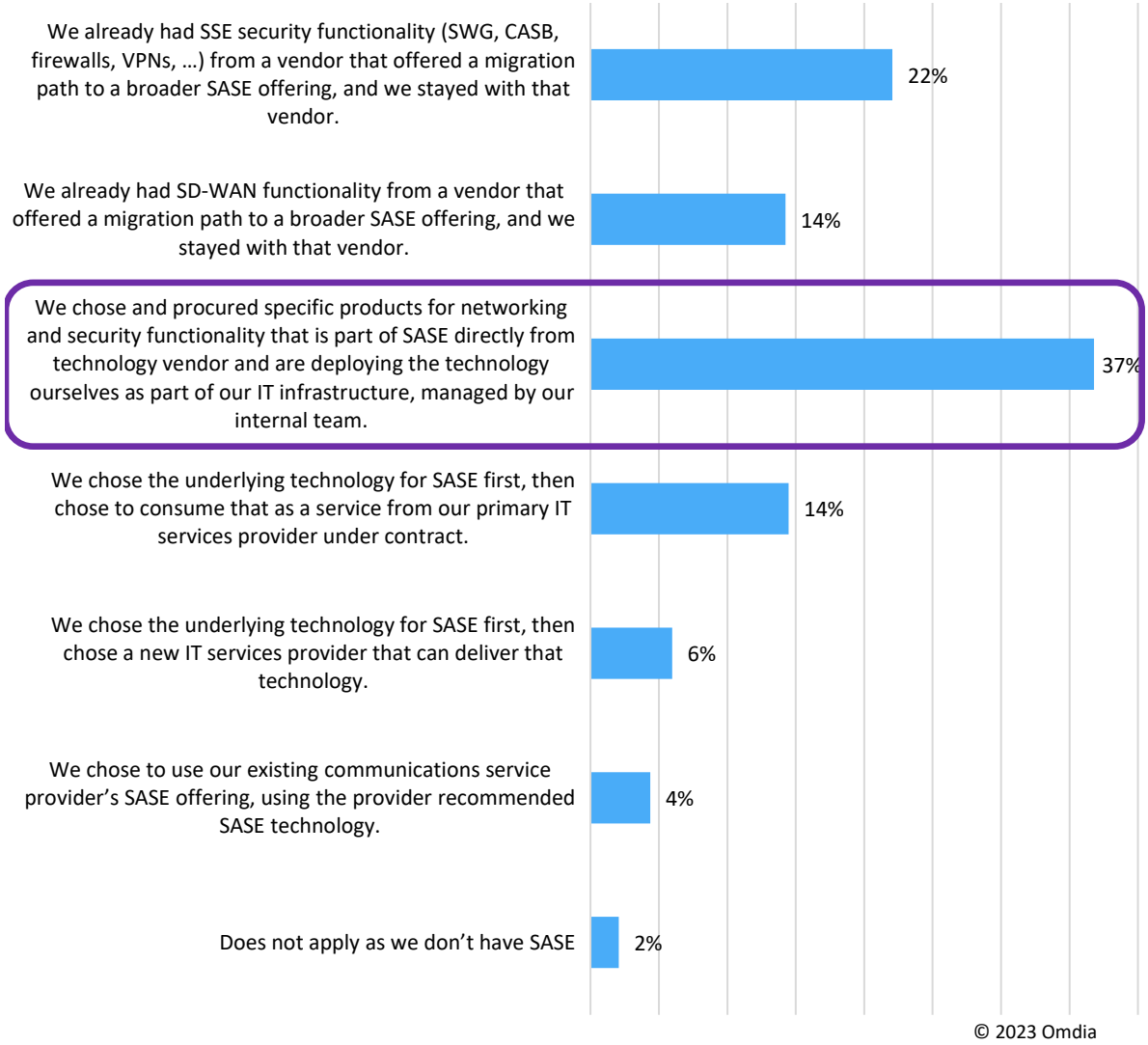
Figure 9: For SSE technology, how did/does your organization perform vendor selection?



Source: Omdia

Migration to SASE is more appealing, with 22% staying with an existing SSE vendor, and 14% with an existing SD-WAN vendor, but still over a third (37%) wanted to choose and procure specific products to deploy and manage themselves.

Figure 10: For an integrated, single-vendor SASE functionality, how did/does your organization perform vendor selection?



Source: Omdia

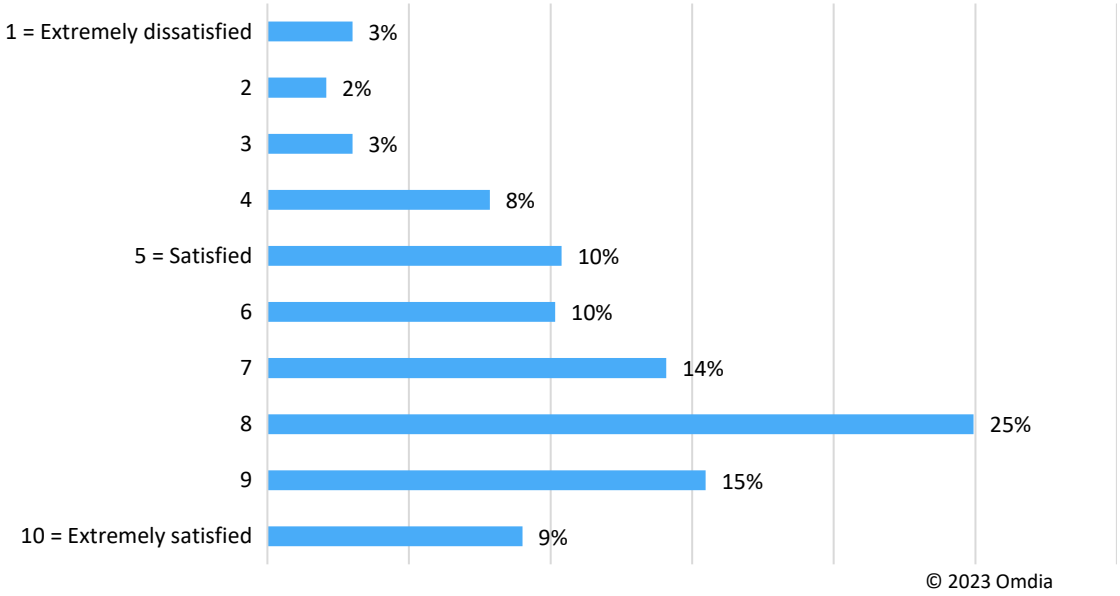
The focus on first choosing the technology for SASE is particularly relevant, as those choosing a single-vendor SASE deployment need high degrees of trust and alignment to the underlying technology.

How are deployments working out? Very well, particularly SASE

Looking into the experience of those that have already deployed SD-WAN, SSE, or SASE, there appears to be a common thread regarding satisfaction—most are satisfied, and for those considering a change, it is mainly around adding or swapping vendors or service providers.

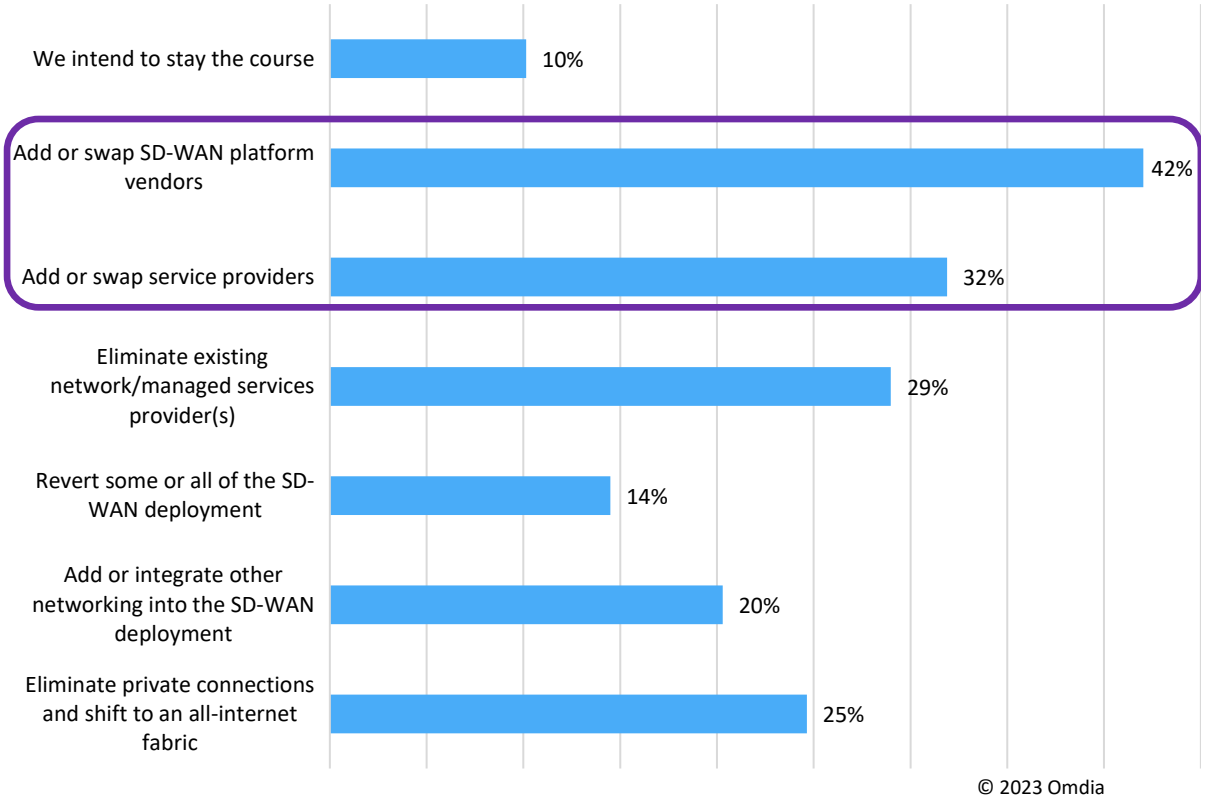
For SD-WAN, overall satisfaction remains similar even for those already deployed at scale, and if anything is slightly higher for larger organizations, those operating across 5 or more countries, and those where purchasing is managed jointly, rather than separately. Only a fraction (15%) indicate they are not satisfied. When they are, they seem to prefer to experiment with changing service providers rather than the technology.

Figure 11: How happy are you with your SD-WAN experience so far?



Source: Omdia

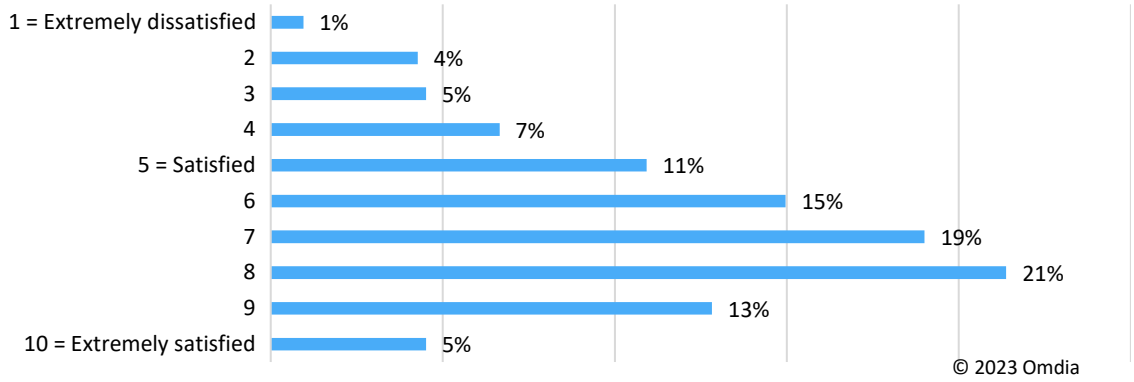
Figure 12: Are you considering any change in your SD-WAN direction?



Source: Omdia

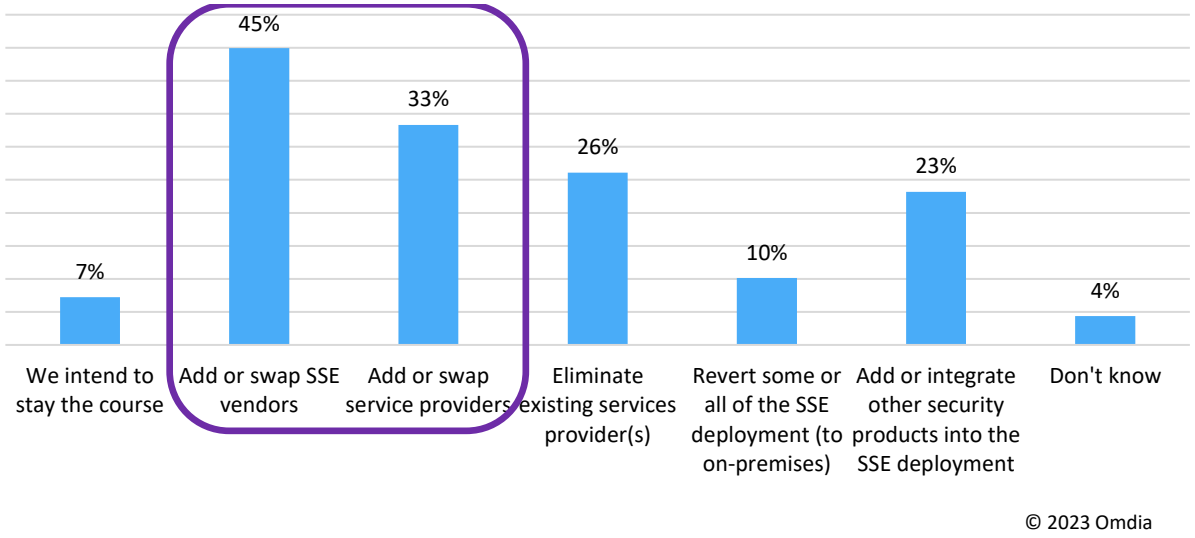
Overall satisfaction levels are similar for SSE, but of the 15% considering a change, many again (45%) want to add or swap SSE vendors.

Figure 13: How happy are you with your SSE experience so far?



Source: Omdia

Figure 14: Are you considering any change in your SSE direction?



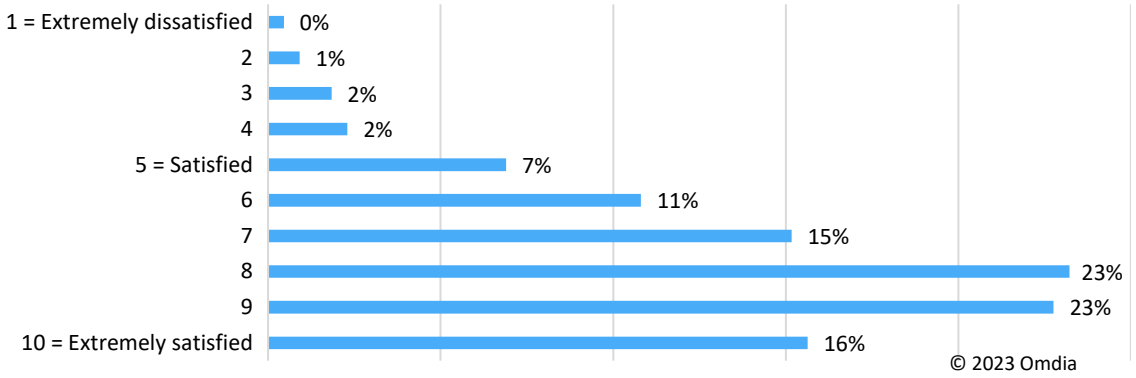
Source: Omdia

Importantly, overall satisfaction levels with SASE appear noticeably higher than both SSE and SD-WAN, with only 5% dissatisfied or considering a change at all.

Overall satisfaction is slightly higher for smaller organizations, those operating across multiple countries, and those with SASE deployment in widespread production use.

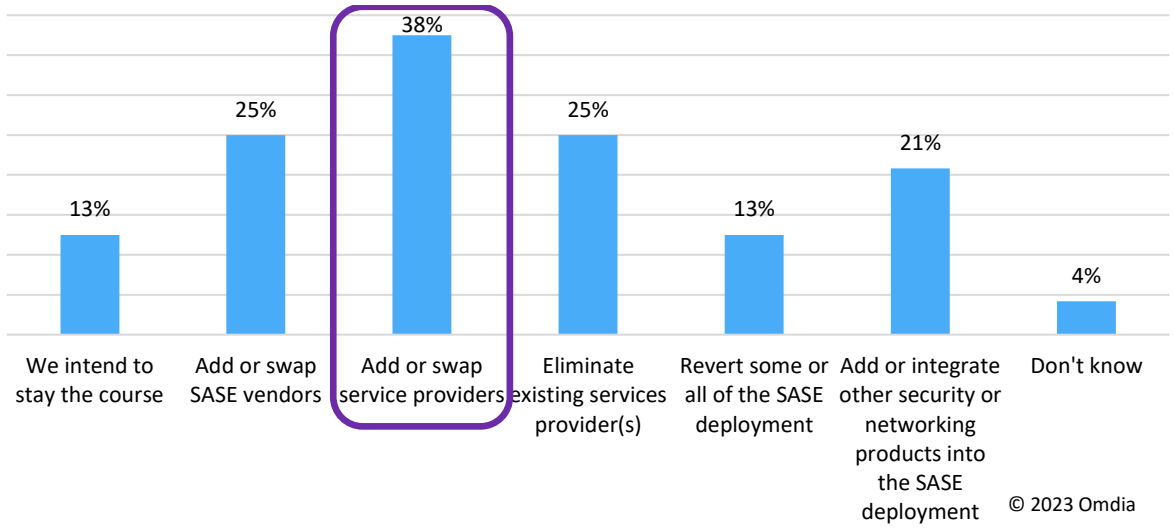
With so few considering change it is hard to read too much into their reasons but making changes to service providers again seems most prominent.

Figure 15: How happy are you with your SASE experience so far?



Source: Omdia

Figure 16: Are you considering any change in your SASE direction?



Source: Omdia

Lessons from experience – integration matters!

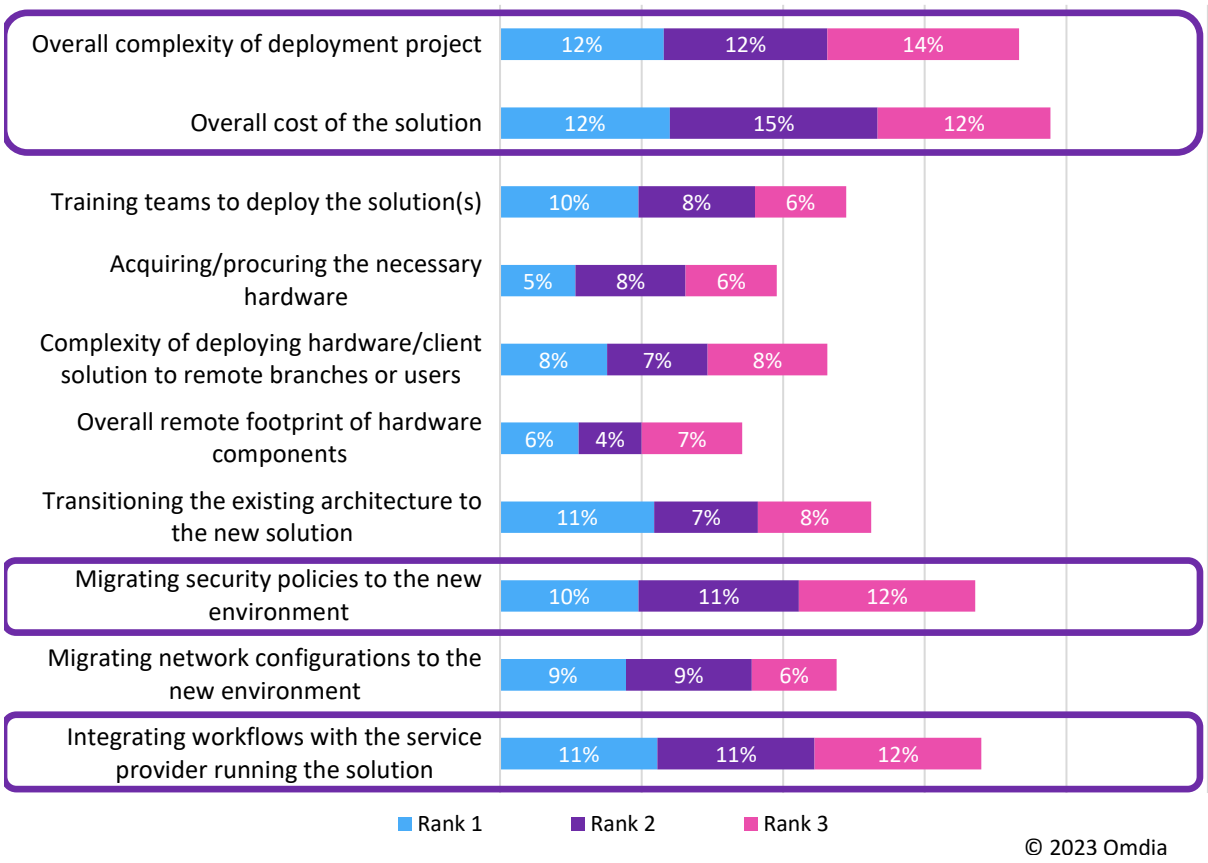
Overall satisfaction with SD-WAN, SSE, and SASE is positive, but there will have been challenges going through the deployment cycles, and lessons learned. Some of these are familiar and typical across all technology projects, but transformational changes to infrastructure can cause additional issues.

Overall cost will always be a highly ranked challenge for the deployment of IT projects, and these are no exception. Some of the high costs will be borne by the expected complexity of deploying SD-WAN/SSE/SASE, as well as for the need to involve different teams from within the organization. The process in making the transition to the new environment is also keenly felt, whether migrating existing policies or integrating workflows with a service provider.

While cost is the greatest challenge for small organizations, larger organizations struggle more with migration to the new environment. When asking only those who have already deployed SASE at scale, the overall complexity of the project rises significantly as a primary concern, which is not something raised by those who have deployed SD-WAN or SSE at scale.

These are aspects that vendors and service providers can readily and effectively address, and this would be worthwhile as the early days of adoption and use often set the tone for the ongoing relationship. With SASE specifically, this might be important as projects grow from initial pilots to full scale deployments.

Figure 17: Considering the options below, please rank in order of importance (1 being highest) what are the top 3 challenges your organization faced when deploying SD-WAN/SSE/SASE

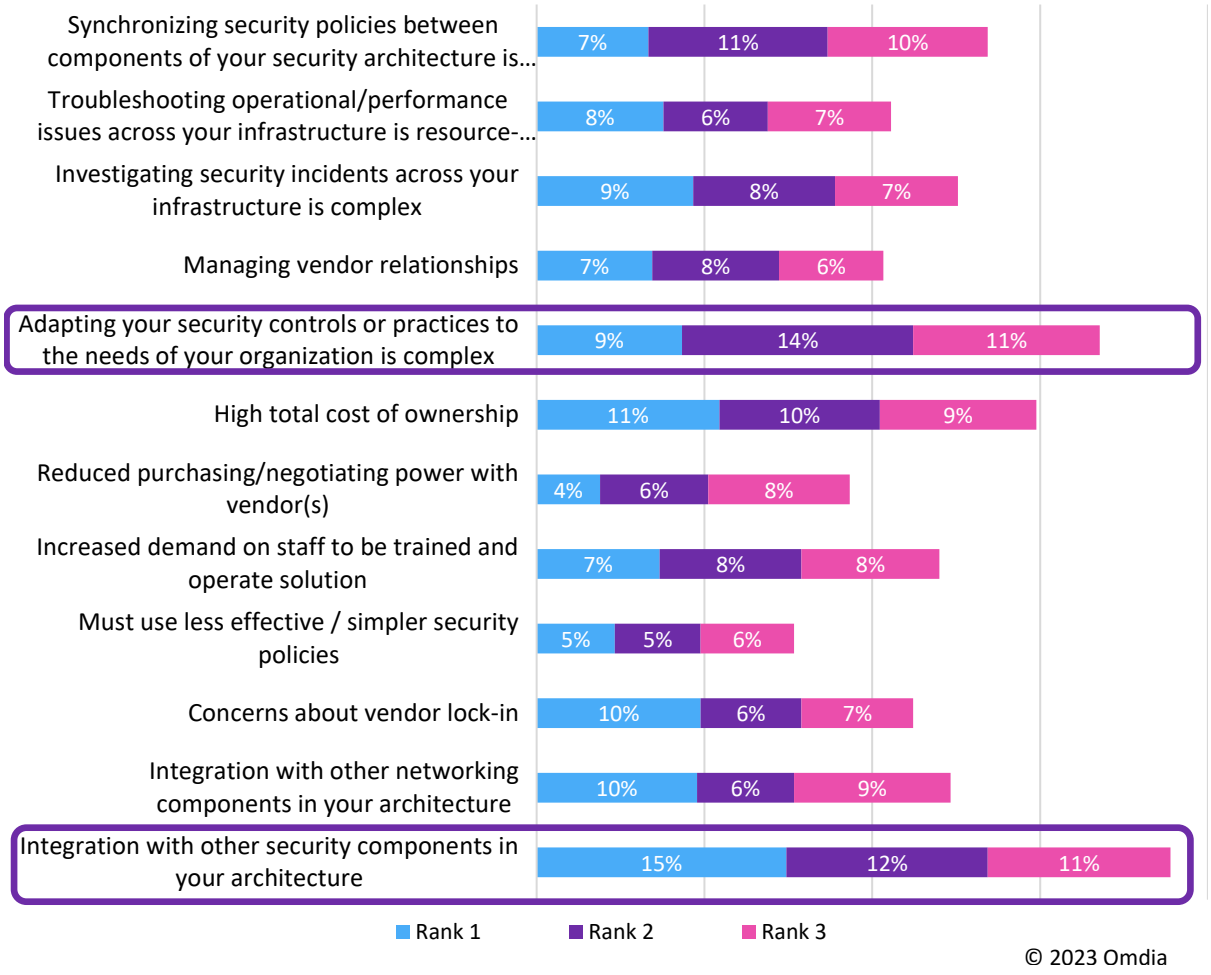


Source: Omdia

Looking at the overall approach to SD-WAN/SSE/SASE, it is the issues that involve alignment and integration to other security elements that are seen as the most important challenges. This includes the ever-present difficulty of integrating different security products and services, but also the alignment of security policies and processes to ensure that as well as delivering on providing effective security, they also best meet the wider needs of the organization.

Cost remains a significant concern, but vendor relationships and the risk of being locked into a particular vendor are not major concerns, despite the level of resources and commitment that needs to be invested in SD-WAN/SSE/SASE. The concerns over total cost of ownership are much higher in Europe, especially compared with Asia, Middle East, and Africa.

Figure 18: Considering the options below, please rank in order of importance (1 being highest) what are the top 3 challenges of your SD-WAN/SSE/SASE approach



Source: Omdia

Looking ahead: finding the right single-vendor SASE

A single vendor approach should address integration and alignment challenges, making a transition to SASE much easier. Putting faith in a single vendor and its technology may raise other concerns, and organizations need to assure themselves that if they are choosing a single vendor and architecture, that it meets all their needs. This includes an assessment of the vendor's credentials and integrity.

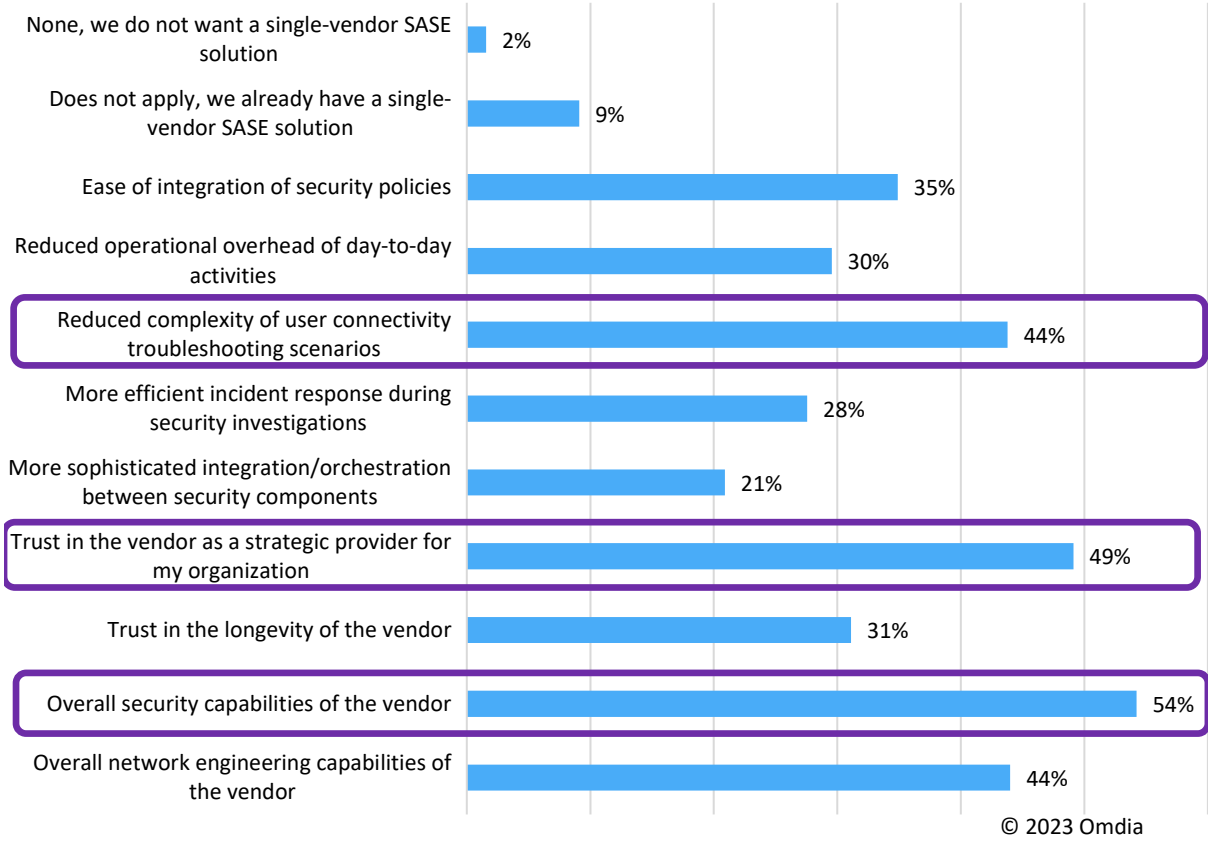
Very few organizations appear to be against the idea of a single vendor SASE solution. While the challenges of security integration and its effective use form part of the consideration, the relationship with the vendor and its capabilities appear more important.

Over half (54%) consider the overall security capabilities of the vendor to be the main factor in considering it for a single-vendor SASE solution, and just under half (49%) attach importance to the trust in the vendor as a strategic supplier. Overall networking capabilities remains a secondary consideration, even when asking those in senior, middle management, and contributor roles in the networking function.

Clearly there is an appetite for a single vendor SASE solution, to integrate and reduce the complexity of delivering effective security across highly connected organizations with distributed workforces.

The research shows that SASE vendors should demonstrate strong security capabilities, integrity, and the ability to streamline the operation of SASE to improve the user experience, in addition to making the solution easier to integrate into the organization's existing security needs. The reduction of complexity and troubleshooting is of particular interest in single-vendor SASE offerings, since the vendor can deploy their deep knowledge of both networking and security aspects, often aided by techniques such as AI-enabled analytics, to simplify troubleshooting scenarios.

Figure 19: What factors would drive you to consider a single-vendor SASE solution from a vendor?



Source: Omdia

Conclusions

The research shows many organizations are proceeding with their digital transformations, even in the current scenario of economic uncertainty. While larger organizations tend to be further ahead in their deployments of technologies such as SASE, the technology is widely applicable to smaller organizations as well.

There are benefits to deploying SASE, such as reduced complexity, improved security controls, better user experience, and freeing up internal resources to focus on other organizational needs.

SASE users report high levels of satisfaction and indicate that their initiatives contributed to organizational improvements as well.

Recommendations

As organizations consider how to approach SASE, the broad level recommendations are:

- Understand SASE is indeed emerging as a key approach in industry for tackling the modernization of network security functionality. With numerous benefits, the SASE approach has the potential to converge capabilities previously deployed across numerous projects, each leveraging separate point products.
- Consider ASE deployments, while strategic for the organization, can be tackled in incremental phases, with initial steps focusing on areas such as VPN replacements, branch networking upgrades, modernization of secure web gateways, and more.
- As these projects are started—aggregated into a “SASE architecture” view—consider areas such as migration of security policies and integration with the rest of the architecture are important considerations for success of the project.

The cost and complexity challenges of SASE means a single vendor approach will have many merits and should make it easier to progress in partnership though the adoption and deployment processes. However, careful selection and assessment of vendor credentials and capabilities is essential. This is more than a simple purchase of products, it is a path towards a partnership relationship, and trust in the vendor as a strategic provider is essential.

Appendix

Methodology

Computer-assisted interviews were conducted during 4Q22 with 450 people spread across the following regions— the US, Canada, Latin America, Europe, Asia, Middle East, and Africa—with a representation sample in each, but a bias towards US in terms of total numbers.

All had to be using or considering one or more of SD-WAN, SSE, or SASE (single- or multi-vendor), and have the involvement in purchasing network services and products from their organization. This involvement could be to identify need/specify requirements, recommend specific solutions, or approve purchase.

Respondents from companies that sell telecommunications or networking products or services, those with 25 or fewer sites, and those with fewer than 1,000 employees were excluded from the survey.

The roles considered included individual contributors, management, or senior management for either network function or security organization, plus senior IT or non-IT executive.

The organizations are spread evenly across eleven industry sectors, except for the agriculture, forestry, and fishing sector, where it was not possible to find sufficient large organizations to respond.

Author

Fernando Montenegro
Senior Principal Analyst, Cybersecurity
customersuccess@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.