Special Report

June 2023

SASE Enables Zero-Trust Networking, Improves Business Agility, Reduces Costs and Streamlines Digital Transformations

Commissioned by

verizon business

S&P Global Market Intelligence

Table of contents

Table of contents

Executive summary

A sea change is occurring in how organisations secure their network perimeters, users, applications and data. Previous approaches based on discrete silos of network and security controls, with remote access provided via virtual private networks (VPNs), are rapidly being replaced by both secure access service edge (SASE) and zero-trust network access (ZTNA) architectures. This paper summarises SASE business drivers, decision-making criteria, purchase modalities, deployment approaches, business value and lessons learned through qualitative data from in-depth interviews and a virtual executive discussion board, combined with quantitative data from S&P Global Market Intelligence research. Note that the focus of this paper is primarily on SASE, as ZTNA methodologies are deployed alongside and as a function of SASE.

Success story

We begin with a successful SASE implementation case study shared by one of the study participants. We conducted an in-depth interview with the chief technology officer (CTO) of a large UK services organisation that manages education, roads and transport, libraries, health, job placement and public safety for nearly a million people. This organisation's experience provides a useful overview of a SASE journey.

Key drivers for this organisation included:

- Supporting remote work. This began as a rapid shift during the COVID-19 pandemic and continues today.
- Reducing costs. The organisation phased out a traditional network service provider that was no longer needed after SASE, saving between £500,000 and £1 million per year.
- Increasing flexibility. Prior to SASE, when the organisation opened new offices, it needed to establish secure, point-to-point network connections, typically via VPN, before employees could begin work — a process that could take weeks or months. After implementing SASE, only commodity internet service over Wi-Fi is required, enabling nearly immediate use of new facilities.

"SASE is the enabler. It enables our people to go basically anywhere, connect to Wi-Fi and just work. This is important, especially when you've got people who sometimes need to go into people's homes, in the front lines at a hospital or working with police and fire services. SASE has also resulted in a 30% reduction of support calls, and we're thinking by the end of the year, they will be down 50%."

– CTO, services, 5,001-10,000 employees, UK

SASE primer

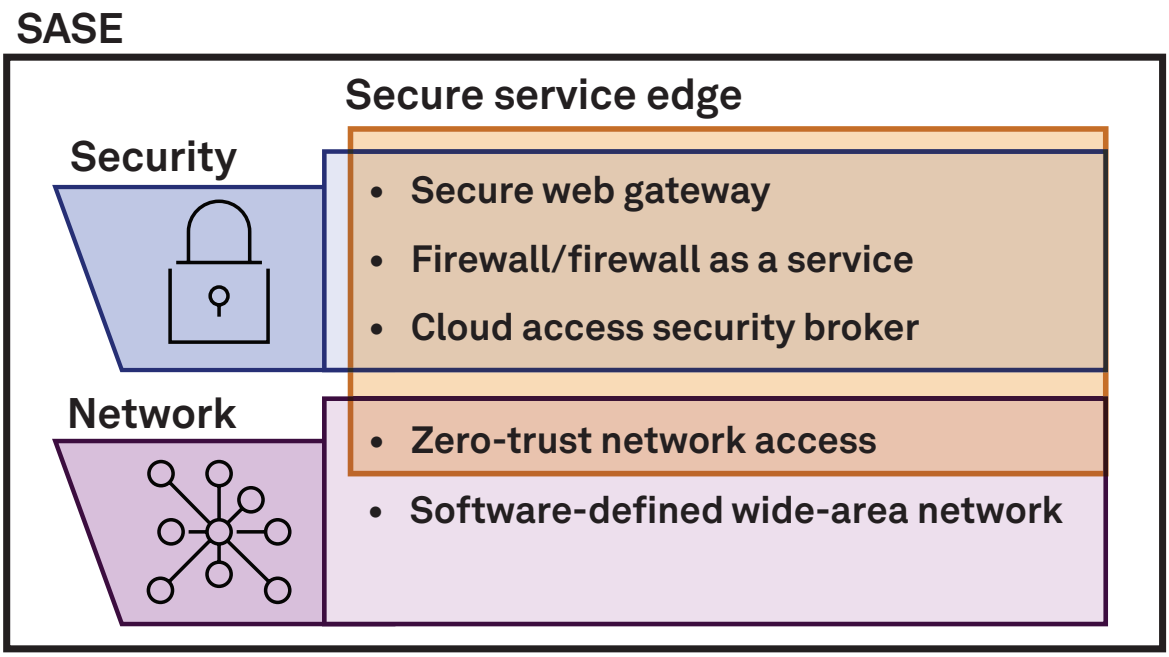
Over the past few years, significant events occurred that fundamentally changed organisations' remote access requirements. These included wholesale cloud migrations, digital transformation and shifting to remote work, as well as an emphasis on decreasing costs and improving user experience.

Traditional network architectures — built around defence-in-depth concepts that assumed a relatively static network perimeter and relied heavily on security at the network edge — have disappeared. Applications, data and users can now be located virtually anywhere, resulting in constantly expanding and changing attack surfaces. By necessity, security authentication must now be enforced at an entity level (such as a user or device), and the mechanisms used to verify and assign trust have followed suit, embodying the core of zero-trust principles: "never trust, always verify."

One area of confusion about SASE is a lack of awareness regarding its definition. SASE is a deployment model and framework based on five key technologies composed of network and security components:

- Firewall as a service (FWaaS). This is a next-generation firewall delivered as a centralised cloud-based service.
- Secure web gateway (SWG). Also known as an internet filter, the SWG enforces web security policies and controls access to internet content at the application level.
- Cloud access security broker (CASB). Placed in the path between cloud service users and providers, CASBs control user access and enforce security policies such as authentication and authorisation.
- Software-defined wide-area network (SD-WAN). SD-WAN enables organisations to build highly performant WANs over the internet, improving flexibility and decreasing costs incurred by traditional MPLS-based connections.
- Zero-trust network access (ZTNA). This restricts application access to a set of authorised users or entities and establishes a secure boundary around applications, requiring verification of identity, context and policy adherence before granting access. Applications become virtually invisible to non-authorised users. ZTNA is a key enabler of zero-trust principles.
- Secure service edge (SSE). SSE is a derivative offering based on SASE designed to address specific use cases around eliminating VPN infrastructure and licensing costs in organizations that do not require an access component. SASE and SSE share similar architectural characteristics, issues and challenges. Within the scope of the study, SASE was the only solution offered, but because SSE is so similar to SASE derivative, it is likely that organisations using SSE considered it equivalent to SASE when formulating survey responses.

Figure 1: SASE components with converged security and network services



Source: S&P Global Market Intelligence, 2023.

SASE is defined as a set of cloud-native offerings that are centrally managed either by a company's IT staff, a service provider or a combination. And while SASE vendors tend to promote the idea of an entire suite provided and managed by a single vendor, this appears rarely to be the case. Many organisations deployed SASE components before SASE emerged as a concept — and it makes good business sense to pick best-of-breed SASE components regardless of who supplies them. Our data reinforces this. According to 451 Research's Voice of the Enterprise: Information Security, Technology Roadmap 2023 study, several core SASE components have already been implemented, including SWG (65% of respondents) and ZTNA (network isolation/micro segmentation [51%] and software-defined perimeter [57%]). The study also shows that nearly two-thirds of respondents (62%) plan to increase SASE investments in 2023.

This report consists of four sections that correspond to a typical SASE deployment cycle. First is initial planning, vendor selection and the decision-making process, followed by deployment specifics, including implementation stages, maturity levels, digital transformation state, third-party involvement and project key performance indicators (KPIs) used. The third section is a discussion of project barriers, realities experienced versus expectations and lessons learned, including advice from participants who were actively involved in deploying these projects in the real world. This paper concludes with a discussion of important factors for organisations to consider before moving to SASE.

Problem, solution, vendor identification and decision-making

We discovered compelling needs driving organisations toward adoption of SASE solutions. More mature, technically sophisticated organisations are driven more by business and digital transformation needs than technical requirements. Larger organisations, typically over 10,000 employees, suffer from technical debt and incompatible legacy systems that slow and complicate deployments. Smaller organisations tend to adopt solutions faster and can often source the entire SASE stack from a single vendor, whereas many larger organisations previously deployed parts of the SASE stack, particularly SD-WAN. Vendors responded to this case by offering secure service edge, as described above.

Problem identification

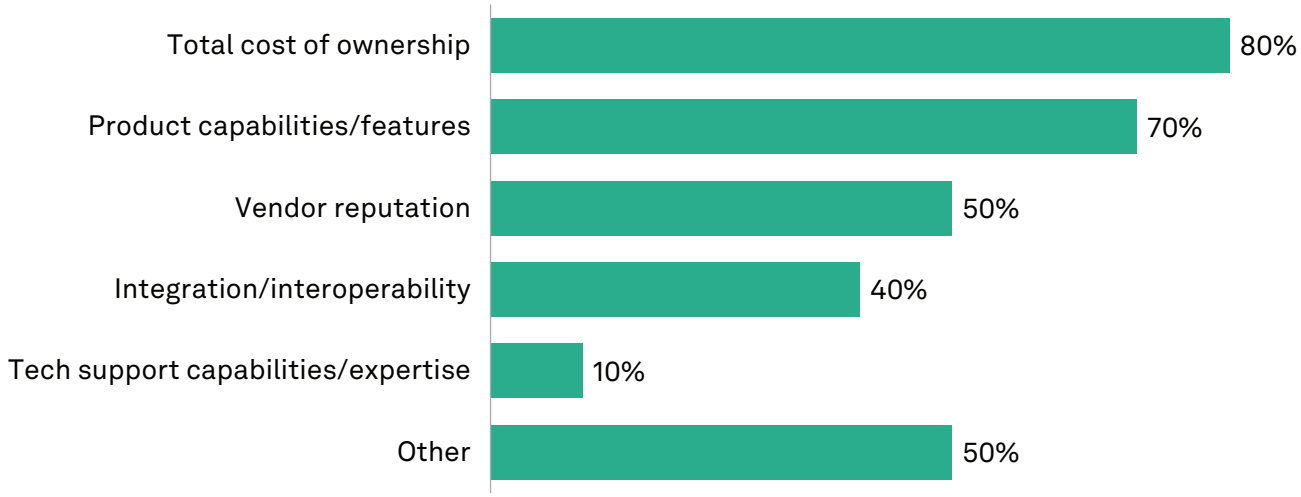
Study participants shared many common pain points that drove them to initiate a SASE project. From a business perspective, improved business agility, cost reductions, support for hybrid work (office plus remote workers), improved end-user experience, reduced threat impact and risk, improved compliance and competitive pressure all factored into the decision. From a technical perspective, network, security, IT modernisation and simplification, and simplified management of rapidly growing networks were all key factors. And while it may take months or years for some organisations to fully realise the vision of edge-to-edge, borderless security, most organisations found "quick wins" such as reducing or eliminating VPN and WAN infrastructure and licence costs, improving user experience and supporting flexible work locations.

Solution determination, vendor identification and decision-making

We examined the resources and processes that study participants used to determine a "shortlist" and final SASE vendor. In most cases, respondent organisations did not diverge from traditional procurement processes, conducting research using vendor websites, industry analysts, trusted advisors and industry peers. Some organisations used external services when they lacked internal expertise. Developing a shortlist of vendors was a common challenge because there are at least 20 SASE offerings on the market.

While some organisations evaluated up to 10 vendors initially, shortlists typically consisted of an incumbent vendor plus two or three well-regarded leaders. They conducted trials and proofs of concept using internal and vendor resources with an emphasis on proving out technical requirements. Requirements for in-depth business justifications were often relaxed due to urgent needs such as rapid transitions to remote work and overriding risk levels. However, in about 40% of cases, sales cycles took more than a year from beginning research to contract signing, likely due to the complexity of the buying process and stakeholders involved. Key decision-makers were typically the CISO, CIO or other senior technical leaders. Smaller organisations tended to arrive at a final decision more quickly than larger ones.

Figure 2: Top factors when choosing a SASE vendor



Q. What were the top three deciding factors and attributes of the vendors/partners you chose?
Base: EMEA respondents (n=10).
Source: S&P Global Market Intelligence custom SASE study, March 2023.

"Unsanctioned/shadow IT – consumerisation of SaaS makes it very easy for a business unit to spin up an instance of a service and start using it with business data. We need visibility and control, but not stifle agility and collaboration. Non-corporate networks — i.e., home, coffee shops etc. — we don't have full visibility of networks outside our traditional infrastructure. We need insight and to be able to build trust where appropriate based on identity."

– Head of information security, risk and compliance, healthcare, 5,001-10,000 employees, UK

Deploying SASE

The study revealed key deployment details, including overall approach, implementation status and duration, the relation to larger network transformation and digital transformation projects, and which internal organisations led the project. The study also examined usage of third-party versus internal resources, most critical benefits, their state of digital transformation, and whether single or multiple vendors were selected.

Deployment approach

Participants indicated a variety of deployment approaches. None indicated embarking on a "big bang" implementation: Some organisations rolled SASE out to high-risk users and apps first, while others chose lower-risk users and applications. For example, some organisations with high short-term risk exposures, such as the potential for breaches or failing compliance audits, chose to solve the issue for those groups first. Others, less concerned about short-term risk, took a more conservative approach such as deploying to staff already using modern cloud apps.

"Quick wins, riskiest first, greatest business impact."

– CIO, engineering, 1,001-5,000 employees, France

"We're adopting a rolling out to least-risk users first, taking a more risk-averse rollout to key ops areas that downtime would cause significant impact and potential patient harm."

– CTO, healthcare, 1,001-5,000 employees, UK

Implementation status and project duration

In terms of deployment process, 25% of participants were in the evaluation/RFP/PoC stage, 50% were mid-implementation and 25% were complete or nearly complete. Interestingly, there was no real pattern behind deployment maturity. Overall project duration (from initial sign-off to production) varied from 6-12 months to 3+ years. Nearly half (45%) of all respondents indicated durations of 12 months or less; another 45% fell in the 13- to 36-month range; and the remaining 10% indicated 3+ years.

Larger project involvement

In Europe, three-quarters of participants indicated that SASE was deployed as part of a digital transformation initiative, whereas in APAC, only one-third indicated this was the case. About two-thirds of respondents indicated that network transformation was conducted concurrently with SASE deployment, about 30% reported that network transformation was complete prior to the SASE project, and only one respondent indicated that network transformation was implemented after the SASE project. Network transformation is clearly a key part of most SASE projects.

Teams/organisations involved

Since SASE touches network and security teams, the study sought to determine which internal teams led the project. In most cases, the project was jointly led by network and security teams (70%), and only 15% were led by the security team alone. In none of the examples that we evaluated did the networking team lead the project alone, and the rest of the projects were led by some other combination of teams.

Third-party support

Many more organisations used third-party support for deployment than for evaluation. In Europe, this support was most often from systems integrators (SIs) rather than value-added resellers and solution vendors, whereas in APAC, most third-party support was provided by solution vendors, while SIs were used primarily as advisors. The differences between EMEA and APAC are likely cultural because many APAC organisations maintain strong relationships with solution vendors and prefer to rely on them for post-sale services.

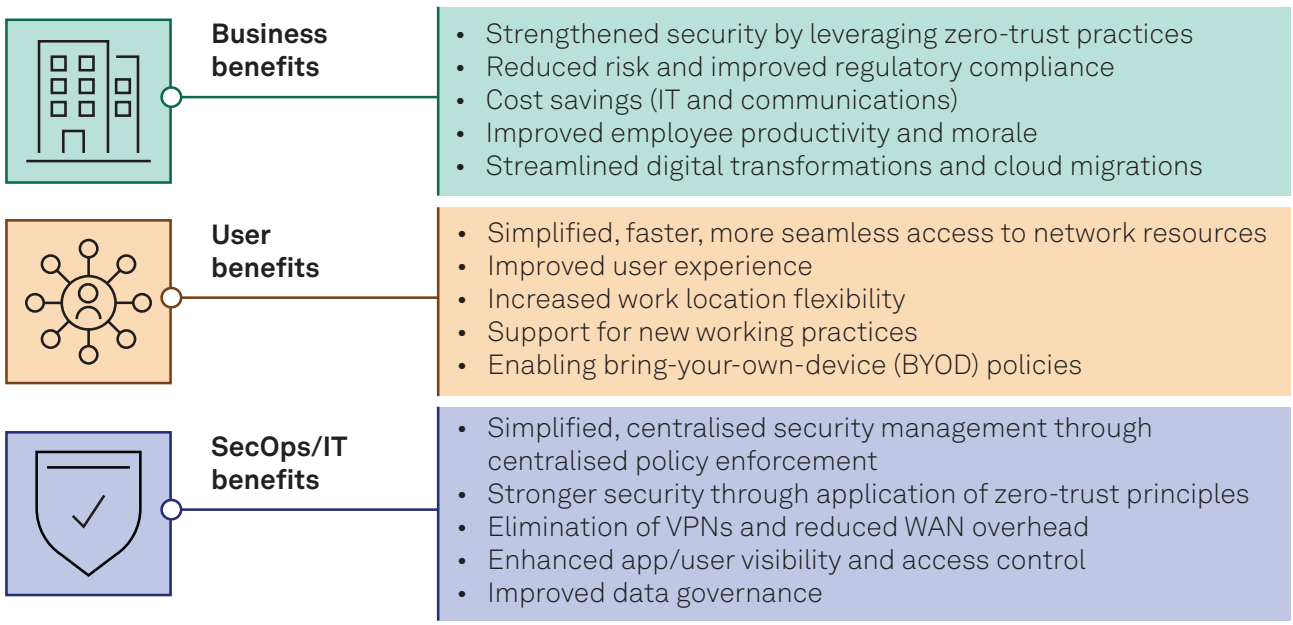
Top benefits from SASE

Participants in the study mentioned many specific benefits from their SASE deployments. We separated them into three benefit categories: business, user and SecOps/IT.

Respondents ranked reduced risks of attacks and breaches and reduced attack surface/vulnerabilities as the top SASE benefits from both business and IT security perspectives. User benefits included simplified remote access, improved user experience, better work location flexibility and the ability to support BYOD.

In addition, many study participants cited the benefits of zero-trust network architecture through micro-segmentation of the network, which substantially reduces the attack surface and potential "blast radius" from breaches.

Figure 3: Key reported benefits of SASE implementation



Source: S&P Global Market Intelligence custom SASE study, March 2023.

"This is very linked to the question about reduced attack surface. The ability for us to restrict movement around the network massively reduces the risk of an external attacker being successful. Improved access control also reduces the risk of accidental loss too."

– CISO, data services, 1,001-5,000 employees, UK

State of digital transformation

For the purposes of this study, we defined "digital transformation" as the percentage of modernised or cloud-native applications in production. One-quarter of respondents said their organisations are in "catch up" mode — i.e., moving rapidly to a more mature state — while the remainder said they are in a nearly or fully mature state. Primary drivers of digital transformation include market pressures to improve profitability and reducing time to market to counter competitive threats. The study shows that while most respondents aligned SASE projects with larger digital transformation efforts, the projects were generally not managed together; funding, deadlines and other factors of SASE implementation were independent from broader digital transformation initiatives.

Single vs. multiple vendors, and perceived strengths

Despite vendor claims about providing all SASE components, half of study respondents indicated that they used more than one vendor. Although participants named 18 vendors, four emerged as more frequently mentioned. In alphabetical order, these were Fortinet, Netskope, Palo Alto Networks and Zscaler. This is still an early market, and the sheer number of multi-vendor deployments indicates that many organisations are likely continuing to use incumbent vendors for certain capabilities and potentially choosing "best of breed" capabilities from others.

SASE outcomes, barriers and lessons learned

The final phase of the study concentrated on SASE project barriers, outcomes and lessons learned. This includes discovering the differences between expectations and reality, the effect of SASE on digital transformation, KPIs used, overcoming roadblocks and gathering participants' advice on key lessons learned.

Project expectations vs. outcomes

It is valuable to examine the differences between a project's expected outcomes versus reality. For SASE, expectations included reduced risk, cost savings and improved productivity/user experience. For those participants who had completed or nearly completed their SASE projects, most reported that they achieved their expected outcomes and also discovered some unexpected ones. The following is a comprehensive list of expected outcomes created by one participant, a CIO of a large insurance organisation in the UK:

- Reducing attack surface via micro-segmentation and enforcement of trust levels.
- Securing all communications, regardless of the network, via risk-based dynamic access.
- Accelerating and automating response through proactive threat detection and analysis from real-time contextual monitoring.
- Simplifying compliance checks through simplified controls, increased automation and standardisation.
- Securing flexible access to resources through dynamic policies.
- Improving productivity and user experience.
- Supporting digital, internet-ready products and services.
- Implementing faster, more agile security solutions.
- Achieving sustained cost savings.
- Enabling simplified processes and provisioning.

Participants expressed positive actual outcomes, although many were mid-deployment and had yet to fully realise the potential benefits of implementation. Most outcomes were measured as "soft," difficult-to-quantify benefits, with hard benefit evaluations to come later due to overriding urgency driving the deployment.

Key performance indicators

KPIs are generally difficult to define and quantify in projects that are based on relatively new technology and that are still in progress. In this study, one-third of participants reported no set KPIs; one-third reported some "hard" KPIs and one-third reported some "soft" KPIs. Some respondents reported a mix of hard and soft KPIs.

"Safer environment, stopped malicious user and antagonistic behaviour... Quicker problem management and higher uptime."

– CIO, healthcare, 10,000+ employees, Sweden

"[SASE] has simplified the onboarding of new employees and the needing to change passwords so often."

– CIO, hospitality, 1,001-5,000 employees, UK

"[SASE] has enabled simplified implementation of new sites and business areas. Due to software-defined policies at the edge, this has delivered value through quickness of deployment."

– CTO, healthcare, 1,001-5,000 employees, UK

"One unexpected benefit of a SASE framework is to have synergies and convergence of interests between infra/network and security where usually it is a fight between what performance/user experience versus security constraints will be considered (which is rare enough to be highlighted!). Here we have a common ground where both can be conciliated."

– Principal for applications and data security, mining & metals, 10,000+ employees, Singapore

Effects of SASE on the overall digital transformation journey

Most organisations did not consider their SASE deployment a part of a larger digital transformation initiative, but instead managed it independently. This is likely because digital transformation projects started before SASE implementations and will continue long after; it may also be related to short-term factors that required fast deployment of SASE. Respondents' views were mixed when asked whether SASE was beneficial to the digital transformation effort. Some said that SASE helped their overall digital transformation project by reducing risk and simplifying the user experience, while others said that it slowed the transformation process. The latter view is likely a function of technical debt hurdles that had to be cleared before the project could continue.

"It has also given us the flexibility of 'bolting on M&A' acquisitions with little additional effort. Also, we can respond to changing business operations."

– Head of digital solutions, utilities, 5,001-10,000 employees, Hong Kong

"In terms of acceleration of the (digital transformation) journey, I would be a little be more cautious saying it has/will have an impact."

– Principal for applications and data security, mining & metals, 10,000+ employees, Singapore

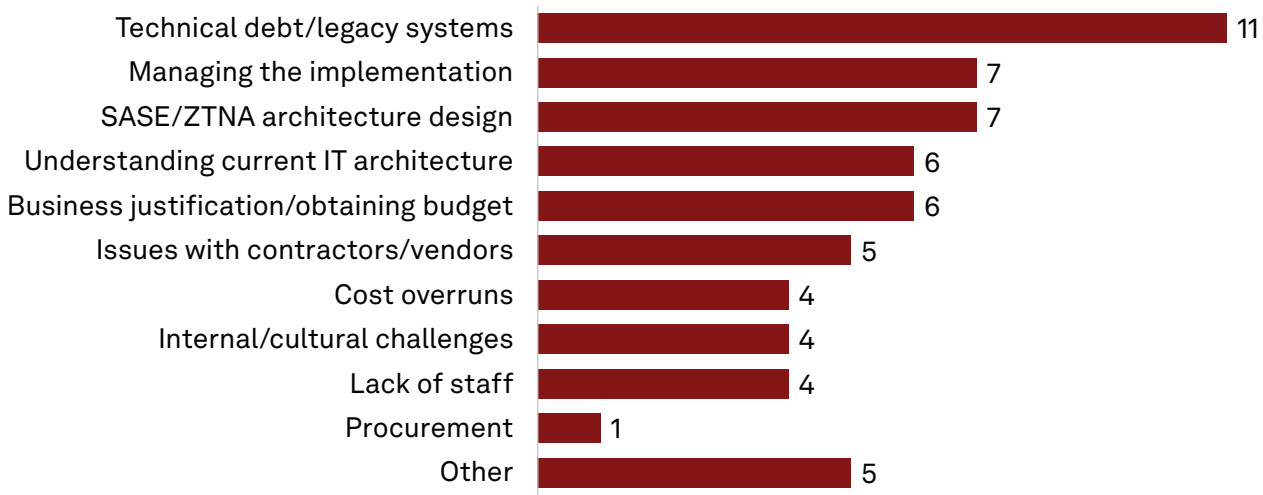
"We started off with streamlining connectivity and the effort that spearheaded the related identity and access management projects are now supporting almost all the other applications as well. So, yes, there was an acceleration effect in our DX journey."

– Regional information security manager, IT services, 5,001-10,000 employees, Australia

Barriers to SASE implementation

Several themes emerged regarding the barriers participants encountered and expected to encounter during SASE implementation.

Figure 4: Top SASE deployment roadblocks



Q. Please select the top three barriers that you already encountered or believe you may encounter during the lifespan of the SASE project.
Base: All respondents (n=20).
Source: S&P Global Market Intelligence custom SASE Study, March 2023.

> "The biggest hurdle we will have in our implementation will be the technical debt we will have to pay off before we can complete the project. This will not only involve updating many old, tried-and-true systems, but also changing the mindset of folks who are cloud-averse because they currently lack the requisite knowledge to successfully deploy their systems to the cloud and, therefore, actively block efforts to move from our brick-and-mortar datacentres to Azure, AWS, etc."
>
> **– CISO, legal services, 5,001-10,000 employees, Germany**

Lessons learned

The final section of the study focused on gathering participants' insights gained through the life cycle of their SASE project. We split these into four sections: needs assessment; upskill, plan and prepare; SASE vendor/partner selection; and deployment planning.

Needs assessment

Participants called out the need for a strong requirements framework and business case development prior to initiating the project. They recommended taking a "security first" approach and advised prospective implementors not to run SASE implementation like a network infrastructure replacement. They also cited the importance of obtaining firm support from key stakeholders and establishing strong governance structures.

"If you're just starting the journey, establish how to quantify the current risk level of not having zero trust, then clearly identify how you're going to demonstrate the value when the new solution is in place."

– CISO, data services, 1,001-5,000 employees, UK

Upskill, plan and prepare

Progressing into project planning and preparation, participants emphasised ramping up internal competencies and resources well in advance. A common theme was the importance of completely understanding the data, application and device assets involved in or affected by SASE. Most participants indicated that they already had detailed "software bill of materials-like" asset inventories from digital transformation projects and governance, risk and compliance processes, which provided a head start. Participants also noted the need to "go heavy" on planning, benchmarking and KPIs, as well as the importance of contingency planning and establishing strong internal communications.

"Include an architect within your integrator's team and ensure they're working with your own architects. Deploy based on risk."

– CISO, data services, 1,001-5,000 employees, UK

SASE vendor/partner selection

Study participants recommended focusing first on vendor competencies, drilling down into specific SASE requirements and comparing vendor claims versus actual competencies, although they reported that this was challenging. Participants also mentioned the importance of using a tried-and-tested partner and establishing strong vendor and partner relations.

"The complexity of the environment (consuming entities, providing entities, etc.) requires the collaboration with vendors who could support the objectives of being able to build on MVPs, ensuring zero-trust sustainability and scalability, enhancing customer-centricity (internal and external), securing our business, enabling the future of work, reducing complexity, and managing regulation and compliance. While we used multiple vendors and multiple solutions based on a best-of-breed approach, we also tried to balance with a standardised approach per domain (e.g., identity, devices, etc.)."

– CIO, insurance, 10,000+ employees, UK

Deployment planning

When the time came to deploy, respondents indicated that using a standardised deployment model was particularly important, as well as carefully planning and scheduling the rollout. Some recommended starting small, achieving quick wins and early lessons first before expanding the project.

"Define the program principles and target architecture and commit to them — such as start small and scale with use cases; build in reusable format; prioritise SaaS apps which are cloud-ready, focus on future-proof solutions; build the foundational capabilities; etc."

– CIO, insurance, 10,000+ employees, UK

Conclusions

The study revealed many key findings. For most organisations, SASE makes strong business sense in terms of reducing cybersecurity risk, improving user experience, enabling remote and hybrid workers, and improving compliance with regulations and internal policies. It is also increasingly important in terms of enabling and securing digital transformation efforts.

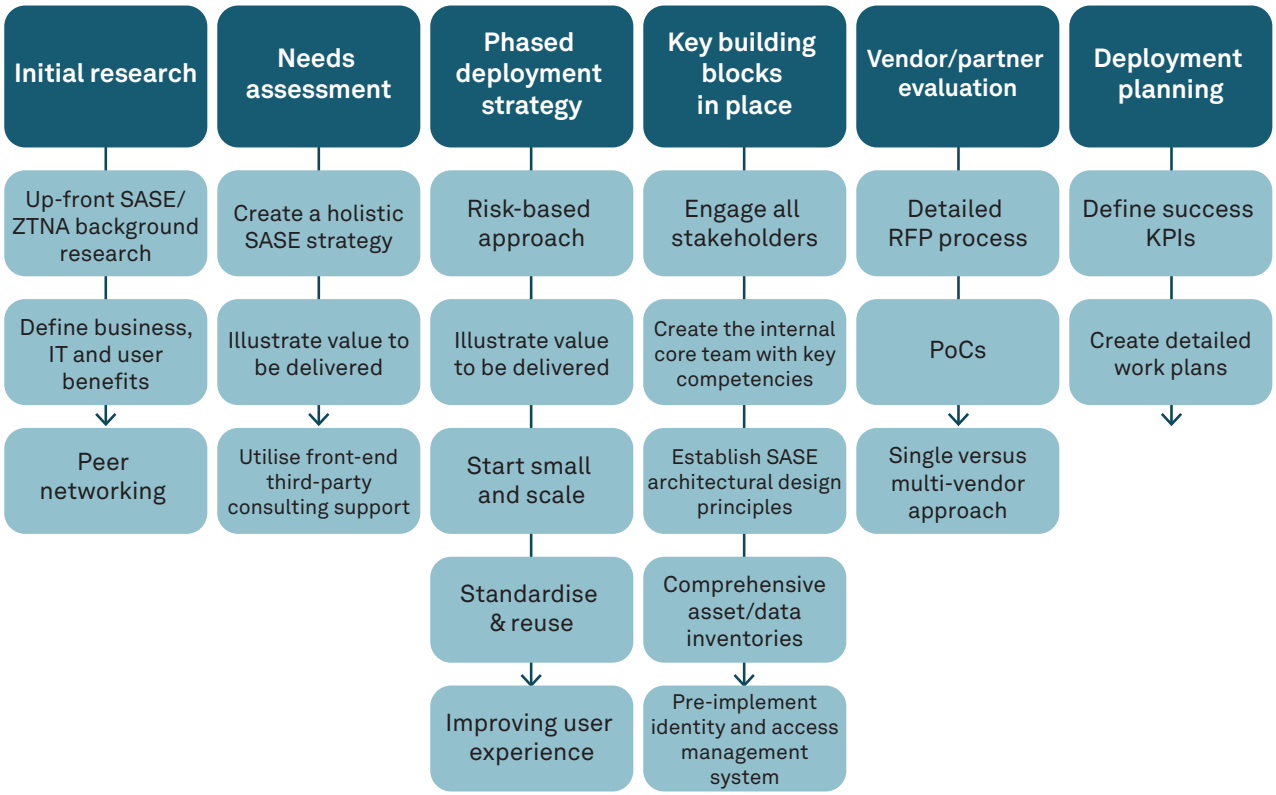
Like any major technology project, the journey must be carefully scoped, planned and executed, using appropriate vendors, technologies and partners. Study participants emphasised the importance of obtaining a clear understanding of what data, applications, users and devices will be affected, and although most also indicated that this information is available because of compliance and digital transformation requirements, obtaining the data could be difficult and time-consuming. Participants primarily conducted initial research on SASE solutions in-house, using vendor websites, industry analysts, conversations with industry peers and, in some cases, third-party trusted advisors.

Some organisations started with a small project with the goal of obtaining quick wins to show quick business value to stakeholders, while others were forced to move quickly and at a broader scale to reduce risk or to support mass changes in worker location. Involving stakeholders in this process early is key to determining risk appetite and the ultimate deployment approach. Unlike many IT and security investments, business justification was not a major concern for many study participants in terms of obtaining budget because it appears that many organisations understood that SASE is a required component in modernisation efforts and were prepared to incur the cost and accept accompanying risks.

Regardless of the implementation plan, the process of selecting vendors and partners is challenging due to the crowded vendor field. Participants preferred incumbent security or network vendors, although most evaluated others based on recommendations from peers or trusted sources. Participants frequently cited the need to fully test solutions through in-depth demonstrations and proofs of concept, and half of participants indicated that they could not find all the functionality required with a single vendor. Larger organisations indicated that implementation planning was more difficult due to technical debt and legacy systems that required extensive retooling and modernisation before becoming “SASE compatible.” Use of third parties varied, with solution vendors and SIs being the most popular choice. Organisations struggled to identify quantifiable KPIs, and most indicated that using “hard” KPIs was not a priority during implementation. Project durations varied from six months to more than three years.

Study participants provided a lot of guidance regarding overcoming barriers; the following graphic summarises their advice.

Figure 5: Respondents' advice for addressing SASE implementation roadblocks



Source: S&P Global Market Intelligence custom SASE Study, March 2023.

For most organisations today, SASE is clearly the way forward in terms of increasing security, reducing risk and supporting digital transformation. The SASE market is growing rapidly, with more than 20 vendors vying for attention, although four vendors were mentioned repeatedly in the study. We expect some market consolidation to occur as larger vendors make strategic acquisitions to gain market share and fill in gaps, enabling them to provide a full SASE solution stack.

Methodology

This report is based on 10 in-depth 30- to 40-minute interviews conducted in late 2022 and a three-day online Executive Discussion Board with 20 participants conducted in March 2023. The study participants were evenly split between Europe (France, Germany, Sweden and the United Kingdom) and Asia-Pacific (Australia, Hong Kong, India and Singapore). Participants work for organisations from a wide variety of industries with 1,000+ employees in Europe and 5,000+ employees in Asia-Pacific, and they lead or are involved in managing and/or implementing SASE technology purchases. Respondents have an average of 20 years' experience in information security, and their job titles include CISO, CIO, CTO and regional security head. Because of the small sample size of the study, results should be interpreted anecdotally.

About the author

Mark Ehr

Senior Consulting Analyst

Mark Ehr is a Senior Consulting Analyst in the S&P Global TMT team based in Denver, Colorado, USA. Prior to joining S&P, he spent 12 years at IBM in roles including worldwide security sales enablement and QRadar SIEM product management.

Prior to IBM, he worked for BigFix, Cabletron, Enterprise Management Associates, Ping Identity, Polarsoft, Siebel Systems, and Sybase, in roles including consultant, entrepreneur, industry analyst, product marketer, software developer, and tech seller.

Mark holds a bachelor's degree in Computer Science from Metropolitan State University of Denver.

About S&P Global Market Intelligence

S&P Global Market Intelligence's Technology, Media and Telecommunications (TMT) Research provides essential insight into the pace and extent of digital transformation across the global TMT landscape. Through the 451 Research and Kagan products, TMT Research offers differentiated insight and data on adoption, innovation and disruption across the telecom, media and technology markets, backed by a global team of industry experts, and delivered via a range of syndicated research, consulting and go-to-market services, and live events.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html