

ESG SHOWCASE

SASE as a Managed Service

Date: June 2022 **Author:** Bob Laliberte, Principal Analyst; and Kevin Rhone, Practice Director

ABSTRACT: Highly distributed modern IT environments, an increasing IoT footprint, and hybrid work models create larger attack surfaces and more risk for organizations. Unfortunately, legacy security and network architectures are not up to the task, and a new framework is required. The secure access service edge or SASE provides a blueprint for converging network and security capabilities to deliver secure connectivity in a highly distributed environment. Organizations are turning to managed service providers (MSPs) to enable them to accelerate the deployment and optimization of these SASE frameworks.

Overview

Modern IT environments are highly distributed. Applications are distributed across private data centers, public clouds, and edge locations; and employees are distributed among corporate, home, and remote locations. In addition, IoT devices are proliferating in all locations. To remain agile and productive, all users and devices require secure connectivity to the applications regardless of location.

This is no easy task, given that this distributed environment has a much larger attack surface and potentially has an exponentially higher number of endpoints. This complexity makes it significantly harder to effectively connect and protect the entire environment. To make matters worse, many organizations still rely on outdated security and network architectures.

Unfortunately, legacy VPN technologies used to connect users and devices to applications and each other are architected to drive all the traffic back through corporate data centers. While this enables all traffic to pass through the corporate security stack, performance can suffer. This is due to the hub-and-spoke network and centralized security architecture that leads to undue latency, which, in turn, impacts performance and experiences. A new approach is required that enables organizations to be highly distributed, yet also remain securely connected while delivering enhanced performance and differentiated experiences.

As a result, new network and security frameworks have been established to overcome these challenges and ensure secure connectivity without compromising performance or experience. This is called the secure access service edge or SASE, and it provides the framework to securely connect highly distributed modern environments.

Given the requirement to converge network and security operations, many organizations are looking to accelerate deployments by consuming SASE as a managed service. This is where managed (or co-managed) SASE services provided by experienced managed service providers (MSPs) that take responsibility for delivering a range of end-to-end services is valuable.

SASE Is Gaining Traction

Highly distributed modern IT environments and hybrid work models are becoming mainstream, and IoT devices continue to proliferate. According to ESG research, almost two thirds (63%) of organizations report they have either hybrid workers or remote workers today and virtually an equal amount (62%) say it will remain that way two years from now.¹ In addition to remote workers, the number of remote sites is growing, with just over half of the respondents (55%) reporting that they have 25 or more remote sites, and nearly three quarters (71%) reporting that they will have 25 or more sites two years from now. The hybrid work model has enabled the return to work, but offices today are highly instrumented to ensure worker safety and enable more efficient and seamless reservation of shared resources. This requires an effective combination of networking and security.

Given these changes, it is easy to understand why SASE is becoming so popular. The combination of SD-WAN technology and several cloud-based security technologies ensures organizations can enable secure connectivity to or from any application, user, or device and maintain high levels of performance and differentiated experiences.

While still a relatively new construct, organizations are beginning to adopt these frameworks. According to ESG research, more than a third of organizations (37%) have begun to implement SASE, and just over 40% are planning to implement it within 24 months.

Figure 1. SASE Adoption



Source: ESG, a division of TechTarget, Inc.

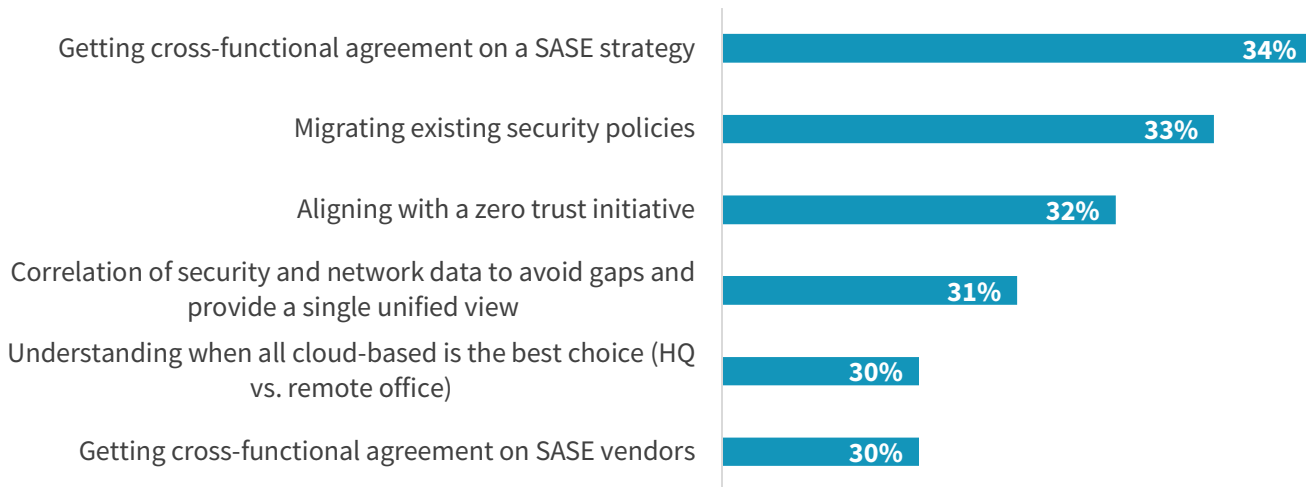
¹ Source: ESG Research Report, [SASE Trends: Plans Coalesce but Convergence Will Be Phased](#), December 2021. All research references and charts in this showcase have been taken from this research report.

Challenges Deploying SASE

However, converging security and networking technologies is not easy. There are several challenges that exist and span people, process, and technology. ESG research highlights the most common challenges, including getting cross-functional agreement on a SASE strategy, migrating existing security policies, correlating security and network data to avoid gaps, and getting cross-functional agreement on SASE vendors.

Figure 2. Top Six SASE Challenges

Which of the following challenges has your organization faced or expected to face when implementing SASE? (Percent of respondents, N=589, multiple responses accepted)



Source: ESG, a division of TechTarget, Inc.

When asked what actions their organizations plan to take over the next 12-18 months to implement or optimize its SASE strategies, 45% of respondents stated that they expect to work with managed services providers, and 39% said they expect to work with professional services to help deploy SASE solutions.

Figure 3. Actions to Implement or Optimize SASE Deployment

Which of the following actions do you believe your organization will take over the next 12-18 months to implement or optimize its SASE strategies? (Percent of respondents, N=589, multiple responses accepted)



Source: ESG, a division of TechTarget, Inc.

Managed Services to the Rescue

Many customers are turning to managed services to overcome these operational challenges and accelerate their time to value through SASE solutions. Customers are relying on managed service providers to help solve for the key challenges they noted across the SASE lifecycle:

- Integrating, orchestrating, and correlating network and security operations and data to promote increased efficiencies and get cross-functional alignment between siloed in-house network and security operations (Responses 1, 4, and 6 in Figure 2. Top Six SASE Challenges).
- Planning, implementation, and ongoing performance monitoring to ensure successful migration and contextualization for existing security policies (Response 2 in Figure 2. Top Six SASE Challenges).
- Enabling remote and hybrid worker support via onboarding and ongoing management of users and endpoints to promote zero trust security initiatives (Response 3 in Figure 2. Top Six SASE Challenges).
- Due to the proliferation of endpoints and increasing volumes of data, MSPs are able to help customers increase network efficiency and optimize IaaS and SaaS experiences, while also helping them understand when and where all cloud-based is the optimal choice (Response 5 in Figure 2. Top Six SASE Challenges).
- By offering SLA-based support and technical services, managed services can help customers proactively troubleshoot, provide incident reporting, and dig into root cause analysis, saving customers time and lost revenue due to network downtime.

The Bigger Truth

While highly distributed environments offer greater agility and increase employee productivity, they also create more risk with a larger attack surface. Organizations need to be aware of this and take steps to replace ineffective legacy storage and networking architectures that are holding the company back and potentially contributing to the increased level of risk.

To remain competitive and ensure the proper level of protection, organizations need to securely connect all locations while simultaneously optimizing performance and user experiences. Deploying a SASE framework can accomplish these goals, but it can be difficult to overcome internal cultures, existing process, and technology debt.

Fortunately, MSPs now provide the appropriate network and security expertise and staff capacity to converge complex security and networking technologies, accelerate the deployment of SASE frameworks, and ensure they remain optimized over time. Organizations that need to modernize their security and network environment to accommodate rapidly distributed applications, devices, and employees will be well-served to engage MSPs with broad, updated technical skills and expertise to assess, design, recommend, implement, and co-manage their transformed environments.



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

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



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



www.esg-global.com



contact@esg-global.com



508.482.0188