ESG SHOWCASE

Democratizing SASE for the Midsize Enterprise

Date: March 2022 **Author:** John Grady, Senior Analyst

ABSTRACT: While secure access service edge (SASE) has generated a groundswell of interest as organizations seek to operationalize zero trust strategies, many offerings have been tailored towards large enterprise customers. Midsize organizations looking to migrate to SASE require the same strong security capabilities and network performance that large enterprises expect, but in a solution that reduces complexity and meets their budget requirements. ZTEdge from Ericom Software was specifically designed for midsize enterprises, built for delivery by certified managed security services provider partners, and offers broad functionality to support a variety of SASE use cases.

Interest in SASE Continues to Grow

As corporate environments have become increasingly distributed and dynamic, many organizations have struggled to provide consistent and secure connectivity between users and resources. Secure access service edge (SASE) has emerged to address this problem by converging previously siloed network and security capabilities into a cloud-native architecture, providing centralized management and distributed enforcement.

SASE is often split into two subcategories: security service edge (SSE), and WAN edge infrastructure. Security service edge may include capabilities such as secure web gateway (SWG), cloud access security broker (CASB), zero trust network access (ZTNA), firewall-as-a-service (FwaaS), and remote browser isolation (RBI), while WAN edge infrastructure consists of SD-WAN and related connectivity optimization services.

ESG research has found that interest in SASE architectures has become nearly ubiquitous. Specifically, 97% of organizations have begun to implement, are planning to implement, or are interested in learning more about SASE.[1] One of the reasons for this interest is the broad applicability of SASE in supporting a variety of use cases. In fact, the most cited reasons for interest in SASE are security focused and include improving security effectiveness (43%), reducing security risk (40%), and accelerating zero trust adoption (34%). However, there are operational drivers as well, with 34% of organizations citing an interest in SASE to improve operational efficiency, 33% to improve operational agility, and 32% to simplify infrastructure and processes (see Figure 1).[2] While many organizations are looking to SASE for cost savings and vendor consolidation, ultimately, companies across all industries, sizes, and levels of IT sophistication can find something of interest in SASE.

97% of organizations have begun to implement, are planning to implement, or are interested in learning more about SASE.

[1] Source: ESG Research Report, *SASE Trends: Plans Coalesce but Convergence Will Be Phased*, December 2021.
[2] Source: ESG. Complete Survey Results, *2021 SASE Trends: Plans Coalesce but Convergence Will Be Phased*, December 2021.

Figure 1. Top Reasons for Interest in SASE

Source: ESG, a division of TechTarget, Inc.

SASE Solutions are Often Designed for the Large Enterprise

Despite the broad applicability of SASE, most solutions have been built with large enterprise organizations in mind. Unfortunately, the realities that large enterprises face do not always align with the consolidation, simplification, and cost savings goals typically connected with SASE. In many cases, this has resulted in deployments that do not fully deliver on the converged, cloud-native, and management attributes SASE should provide. Specifically:

- Existing infrastructure requires hybrid approaches. Most enterprise organizations have already invested in standalone, on-premises versions of many of the tools that comprise a SASE architecture. Managing the replacement of existing tools and transitioning on-premises tools to the cloud leads many enterprises into a phased SASE implementation. ESG research has found that 70% of survey respondents anticipate it will take their organization at least one year to fully adopt a SASE architecture, with many anticipating a multi-year process.[3] This has resulted in many SASE solutions shifting on-premises capabilities to the cloud, rather than building out a cloud-first, cloud-native architecture.

- Reliance on multiple tools. Most large enterprises expect to use multiple tools for SASE, with 57% of cybersecurity and IT professionals expecting to use at least three tools to support SASE when the initiative is complete.[4] Because large

[3] Source: ESG Complete Survey Results, *2021 SASE Trends: Plans Coalesce but Convergence Will Be Phased*, December 2021.
[4] Source: ESG Research Report, *SASE Trends: Plans Coalesce but Convergence Will Be Phased*, December 2021.

enterprises may piece together specific capabilities from multiple vendors, SASE pricing and packaging is not always optimized towards a single vendor, cost-conscious approach.

- Distributed management responsibility. Large enterprise organizations typically have sizable, specialized IT and security teams. As a result, SASE platforms designed for the enterprise do not always focus on optimizing management. When administrators have distinct and specific responsibilities over portions of the SASE stack, a unified console is often less of a priority.

Large enterprises, with their fragmented hybrid IT environments, sizable budgets, and deep bench strength of security and IT staff, can easily adopt the more complex and expensive SASE solutions that have become the norm in the market. Unfortunately, small and midsized enterprises have very real budget and staffing challenges to deal with, making adoption of most SASE platforms a difficult proposition.

Key SASE Attributes for the Midsize Enterprise

Smaller organizations face many of the same challenges as their large enterprise counterparts. Cloud usage continues to increase, users must access corporate resources from a variety of locations, and the threat landscape continues to become more disruptive. Yet, on top of these issues, midmarket organizations with 500-1,000 employees are likely to face more stringent budget constraints, while being more affected by the cybersecurity skills shortage. Whereas large enterprise organizations may have a sizeable IT staff, midmarket organizations may rely on a handful of people for cybersecurity, who are frequently generalists responsible for multiple IT domains. So while SASE on the whole is extremely relevant to this segment of the market, solutions designed for large enterprises do not address the specific realities of the midmarket.

While an organization's specific SASE requirements will vary based on factors such as use case, existing tools, or network architecture, there are three high-level attributes midmarket organizations should prioritize when evaluating SASE platforms: ease of use, broad functionality, and performance.

Ease of Adoption and Use

SASE solutions should be straightforward for midsize organizations to deploy and manage. Deploying extensive hardware on-premises or even virtual connectors in the cloud can quickly become burdensome. SASE platforms that allow organizations to simply point their traffic to the provider's cloud, which automatically handles route optimization, scaling, and orchestration, are ideal for smaller organizations. Additionally, use case-based competitive pricing that enables customers to target the areas of their greatest need, streamline the approval process, and quickly get started with SASE can help address the budget constraints many smaller organizations face.

As mentioned, while single-pane-of-glass, unified policy management is often referenced as part of SASE, many solutions fail to deliver on these points. Even solutions that provide a truly unified management experience can represent a burden for smaller organizations due to the skills shortage. As a result, the ability to consume SASE as a managed service is critical for smaller organizations to help alleviate the skills gap and reduce time to value. In fact, ESG has found that 45% of organizations plan to work with managed service providers to implement or optimize their SASE solutions over the next 12-18 months.[5]

[5] Ibid.

.

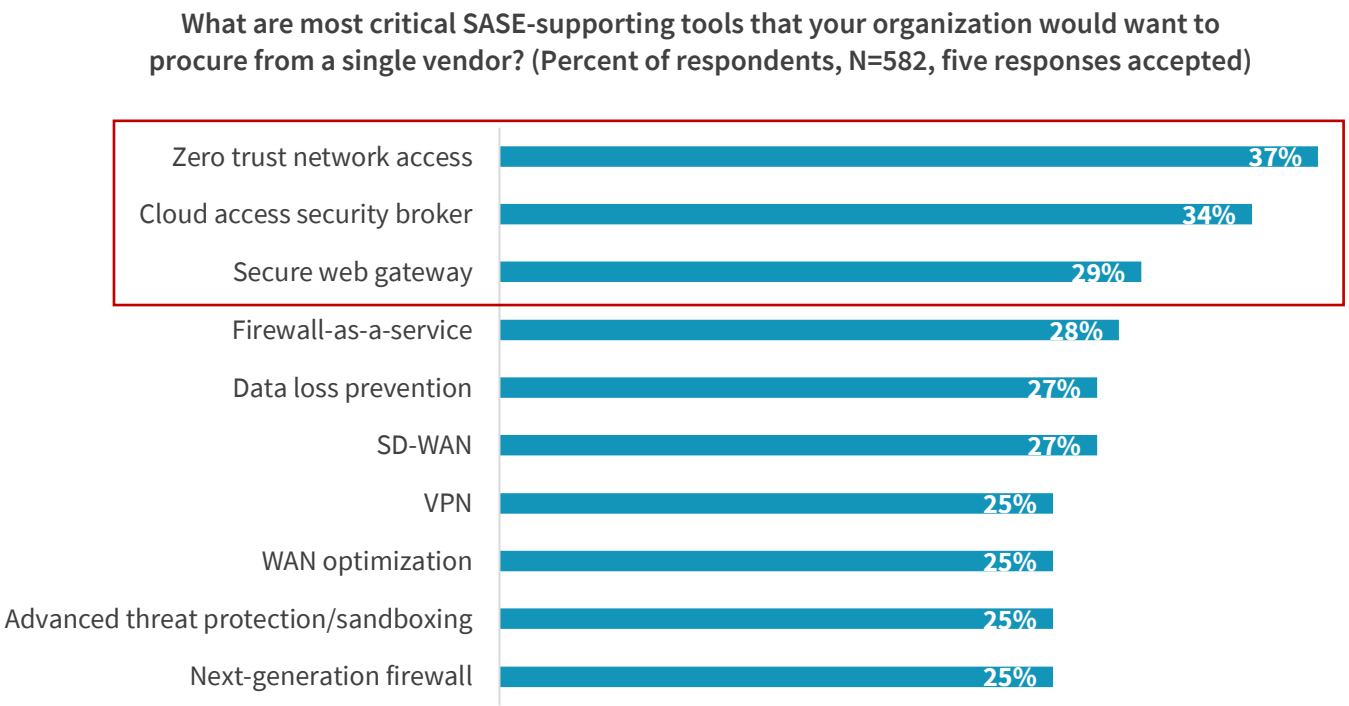
Broad and Flexible Functionality

While ease of use is critical for smaller organizations, this does not mean that functionality can be sacrificed. There is a long list of capabilities that SASE platforms must support across both security and networking. Yet with the focus often on securely connecting users to resources, and the increasing functional overlap of the tools supporting this use case, a common starting point for SASE is converging secure access to the internet, private applications, and public SaaS applications. Highlighting this, ESG research has found that ZTNA, CASB, and SWG are the most likely tools to be procured from a single vendor (see Figure 2).[6] The convergence of these tools provides more consistent security coverage across multiple attack vectors and can help improve efficiency through streamlined policy management.

These tools are important for enforcing acceptable use policies, protecting users from malicious downloads, and preventing data loss. However, the increase in stealthy attacks leveraging zero-day web threats, advanced phishing techniques and ransomware, and ephemeral URLs and domains can limit the effectiveness of these tools. As a result, remote browser isolation (RBI) is increasingly viewed as a key SASE platform component that ensures users are fully protected from sophisticated threats. In fact, ESG has found that 90% of organizations say RBI is a consideration for SASE.[7]

Finally, the increasing intersection of SASE with zero trust highlights the importance of identity. Multifactor authentication is a foundational element of both SASE and zero trust to ensure users are who they say they are and protects against stolen credential abuse. With identity specifically and SASE overall, the flexibility to either provide an all-in-one approach or seamlessly integrate with existing tool deployments to fill gaps is an important attribute to address both short- and long-term needs. Solutions that can deliver on the majority of these points and support a variety of use cases at the outset of the project can enable organizations to seamlessly expand over time.

Figure 2. Critical SASE Tools to Procure From a Single Vendor



Source: ESG, a division of TechTarget, Inc.

[6] Ibid.
[7] Ibid.

Performance

While management and functionality are often front and center considerations for SASE, the underlying network that the platform is built upon can be overlooked. With highly distributed users and resources, it is critical that SASE solutions provide a performant, consistent user experience at all times and in all locations. Further, as more capabilities are added, especially computationally intensive controls such as RBI, the platform must be able to scale to provide performance on demand. This requires a global network footprint with strong peering relationships and redundant points of presence. While availability SLAs are important to ensure uptime, latency guarantees are also critical to ensure that users enjoy consistent application performance.

Introducing ZTEdge by Ericom Software

ZTEdge is a zero trust SASE platform specifically designed for the midsize enterprise. The platform protects users, applications, networks, and devices while helping customers reduce complexity, limit risk, and improve performance. Powered by a global network hosted by top-tier providers including AWS, Google, and Oracle, ZTEdge provides strong uptime SLAs and has peering relationships with major IaaS and SaaS providers to deliver high performance.

The platform natively integrates Ericom's remote browser isolation (RBI) technology to provide advanced protection from zero-day threats and sophisticated malware, phishing, and credential theft. RBI can also be used to protect private web applications from cyberattacks. The platform was designed to be delivered by certified managed security service provider (MSSP) partners to help midsize organizations reap the benefits of SASE without the need to self-manage the platform. ZTEdge is priced with the budget realities of midsize enterprises in mind, at price points that are approximately half that of alternative solutions on the market. Customers can license the full ZTEdge platform to cover a variety of use cases, or sub-modules, such as ZTEdge Web Security, can be licensed to meet specific security requirements. Several of the top use cases that ZTEdge supports include:

- Ransomware and phishing protection. ZTEdge's secure web gateway with built-in remote browser isolation provides essential functionality to manage user access to specific websites or web categories based on threat profiles or acceptable use policies. Additional capabilities such as antivirus scanning, file sanitization, and encrypted traffic visibility offer protection from web-based attacks. The solution is also able to scan attachments in end-to-end encrypted traffic (such as WhatsApp) and can render suspected phishing sites in "read-only" mode to prevent users from handing their credentials over to hackers.

- SaaS application access and data security. Organizations can require that users access corporate SaaS applications like Salesforce.com and O365 only through the ZTEdge cloud to prevent unauthorized access and data loss from stolen credentials. Contextual-based policies based on location, device, destination, and other factors can also be applied to reduce risk. Browser isolation is used to control browser-based data sharing functions such as copy/paste and printing while built-in DLP can be used to enforce information security policies. The solution also protects the use of meeting apps like Zoom and Teams through its patent-pending Virtual Meeting Isolation capabilities.

- Secure private application access. ZTNA is a key part of the ZTEdge platform that provides users with secure access to private applications, either in the cloud or on-premises. Policies can be applied to entire groups, or specific users, and recommended automatically through patent-pending ML-powered behavioral-based analytics.

- East-west access control. In addition to ZTEdge's ZTNA secure remote access capabilities, the platform can control east-west movement in the network. Each individual is granted access on a per-application basis to prevent users from accessing more than they are entitled to. This helps to limit lateral movement in the event of a compromise.

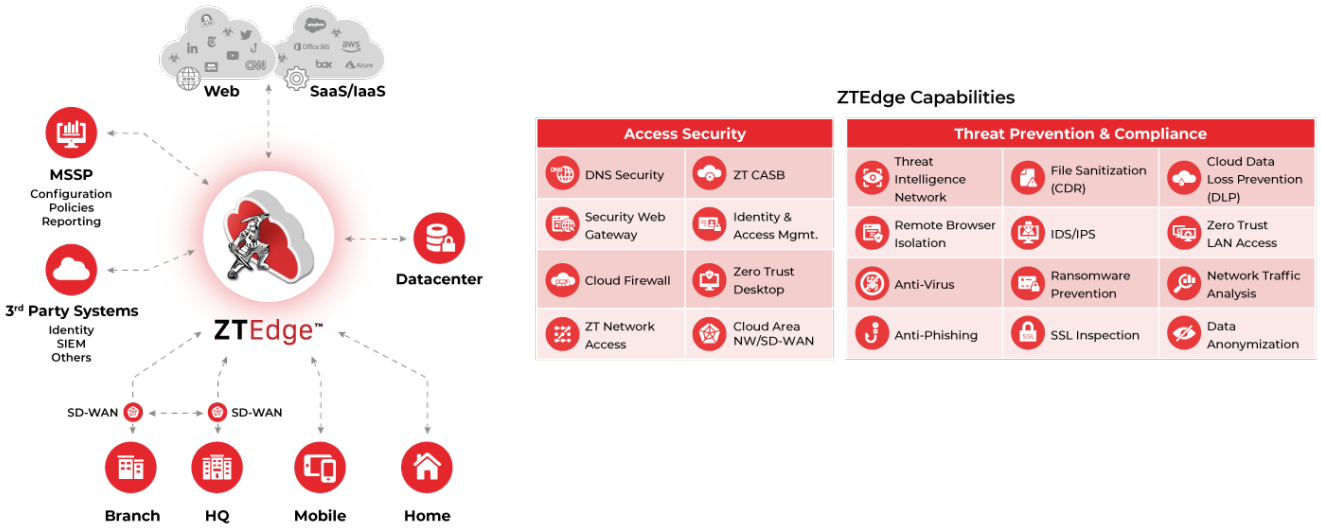
- **Network protection and monitoring.** Foundational network security components such as firewall and intrusion prevention are included as part of ZTEdge to monitor network traffic and provide inbound and outbound threat protection.

- **Connecting distributed branches and users.** ZTEdge's cloud-based SD-WAN and Cloud Area Network capabilities help customers transition from a reliance on costly and complicated corporate LAN and hub-and-spoke network connectivity architectures to a simplified, cost-effective model for quickly connecting users to any IT resource, regardless of location, as well as connecting distributed brand environments.

- **User and device authentication.** Unlike most SASE platforms, ZTEdge includes IAM and MFA natively in the platform for no additional cost—providing organizations with savings since they no longer must pay for subscriptions to additional identity solution providers. If needed, ZTEdge can also integrate with other SAML supported identity solutions.

Customers can license the full ZTEdge platform to cover all of these use cases, or sub-modules, such as ZTEdge Web Security, can be licensed to meet specific security requirements.

Figure 3. Ericom's ZTEdge



Source: Ericom

The Bigger Truth

At its core, SASE seeks to both modernize and simplify what has become an overly complex and fundamentally flawed network and security model. The derivative goals of that modernization and simplification are better security effectiveness, improved operational efficiency, and a stronger user experience. Unfortunately, large enterprise realities have prevented many current solutions from fully delivering on these tenets, especially for midmarket organizations. ZTEdge from Ericom represents a purpose-built SASE platform designed specifically with the requirements of the midsized enterprise in mind.

Smaller organizations—especially those seeking to move to a service-based model—that have been hesitant to adopt SASE due to perceived complexity or cost would be well served to consider ZTEdge.

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