POINT OF VIEW

Critical Guidance for Evaluating SASE Solutions

Executive Summary

Providing secure, reliable, and consistent access to corporate assets and applications to today's hybrid world is one of the biggest challenges facing IT teams. Secure, authenticated access to critical applications and resources combined with consistent enterprise-grade protection, whether workers are on-premises, working from home, or somewhere in between, is crucial in today's marketplace.

Today's hybrid networks are only as secure as their weakest link. So, when workers suddenly shifted to home offices, organizations experienced a spike in malware, particularly ransomware. Cybercriminals quickly moved their efforts from attacking the corporate network to targeting often poorly secured home offices. They were then able to burrow into the network by hijacking encrypted VPN tunnels.

Organizations need a more advanced solution. Secure Access Service Edge (SASE) is an architecture that converges networking and security—combining cloud-delivered security and SD-WAN—to ensure consistent and secure access to critical resources for remote workers. An effective SASE solution should include enterprise-class security elements, like a secure web gateway (SWG), zero-trust network access (ZTNA), and a next-generation dual-mode cloud access security broker (CASB) to ensure consistent and secure access to web, cloud, and private applications. And its integrated SD-WAN should provide keep together access to business-critical applications. If done right, SASE should extend the same protections and performance to remote workers they experience when working from their traditional on-premises office.

SASE has quickly become a vital tool in the arsenal of IT teams needing a more reliable solution for their now permanent hybrid, work-from-anywhere (WFA) model. However, not all SASE solutions are alike. Application performance, access, and security can vary widely between solutions. And for those organizations with a dynamic and evolving hybrid network, adding yet another set of technologies to manage can overwhelm limited IT resources.

Buyers Should Look Carefully Before Investing

Much of SASE adoption near the end of the pandemic was spurred by a sense of urgency. Organizations were looking to replace their temporary and resource-intensive WFA solutions with something more reliable. However, it is easy to get caught up in the enthusiasm of a new market trend and make purchases before having all the information.

As with many new markets, vendors have popped up looking to capture a piece of the SASE market. But many of these solutions fall short of their promised benefits. They have immature or inadequate security technologies. They often operate as isolated standalone solutions that don't work with any other technologies across the organization, especially when integrating with the rest of the hybrid network. And they can only address a limited number of use cases. As a result, they often contribute to vendor and solution sprawl rather than reducing it, adding an additional management burden to already overtaxed IT teams.

Rather than blindly jumping on the SASE bandwagon, organizations are urged to carefully consider the following issues before opening their wallets:

Not all SASE solutions are alike. Application performance, access, and security can vary widely between solutions. And for organizations with a hybrid networking strategy, adding yet another set of technologies to manage can overwhelm limited IT resources.

The manual controls, scripts, and limited threat intelligence used by most SASE vendors cannot keep up with today's rapidly evolving threat landscape, leaving organizations vulnerable.

A single-vendor SASE approach

Most organizations will continue to operate a hybrid network that combines a traditional infrastructure with a cloud-based system well into the future. The challenge is that vendor sprawl within these environments reduces visibility and control. Security and networking components that operate in siloes cannot be automated, and SASE solutions that don't work with the rest of the network mean that IT teams cannot track and secure transactions end to end. Rather than trying to build a multi-vendor SASE solution, with its attendant challenges for implementation and management, SASE should be a single-vendor solution that converges networking and security into a unified solution out of the box. A SASE solution must also seamlessly hand off connections between the cloud and on-premises devices, allowing access and security policies to follow the user rather than terminating at the edge of the network. Only by converging networking and security end to end can organizations implement a comprehensive zero-trust architecture. Extending the unique approach of security-driven networking to the cloud edge ensures consistent security and superior user experience everywhere.

Flexible, secure private access to corporate applications

Today's organizations are rapidly evolving. Their needs require a flexible SASE solution that can meet—and adapt to—their unique business environment. An adaptive SASE solution that can provide secure connectivity to corporate applications, whether in a private data center or the public cloud, is vital for meeting today's dynamic organizational requirements. It should also offer secure access to corporate applications using ZTNA for granular control and seamlessly integrate with SD-WAN and NGFW solutions to ensure an optimal user experience when accessing corporate applications. Powered by intelligent steering and dynamic routing capabilities through its cloud-based PoPs, a SASE solution should also automatically find and maintain the shortest path to critical resources to ensure a consistent user experience for today's hybrid workforce.

Unified agent for multiple use cases

Onboarding a different agent for each use case can quickly become complex and expensive to maintain. A SASE solution should provide a single agent that can be used for multiple use cases, including ZTNA, CASB, and endpoint protection, while automatically redirecting traffic to protect assets and applications through cloud-delivered security.

User access controls

ZTNA has emerged as an essential tool for protecting today's distributed resources and hybrid workers. A Universal ZTNA solution must authenticate users everywhere, grant explicit access to specific applications, provide constant monitoring, and take countermeasures when something unexpected occurs.

Consistent policy enforcement and superior user experience

SASE technologies should be easily integrated into the organization's larger network and security architecture rather than working as a one-off solution. Ideally, the security protocols and policies within the SASE solution should be identical to those used elsewhere in the network. Systems managers should also be able to integrate their SASE solution with existing technologies to optimize their security and network operations through seamless interoperability. And consistent network operations enable superior user experience for workers, whether on or off the network.

AI-powered threat intelligence

Keeping users and applications safe requires keeping the security components of the SASE solution constantly tuned to the latest threats. However, the manual controls, scripts, and limited threat intelligence used by most SASE vendors cannot keep up with today's rapidly evolving threat landscape, leaving organizations vulnerable. So, in addition to enterprise-class security components, a SASE solution must also leverage AI-powered threat intelligence, built using supervised and unsupervised learning models and trained on a large and diverse set of billions of cyber events, to prevent today's sophisticated and evasive zero-day threats.

Essential Use Cases Your SASE Solution Should Address

On the surface, it may seem like a SASE deployment is straightforward. Purchase a SASE solution, point your users at it, and forget about it. In fact, that's what many SASE salespeople will tell you. But as anyone with any IT experience knows, nothing is ever as easy as it seems. For even the most straightforward solutions, the devil is often in the details.

Understanding the primary use cases your SASE solution needs to address is a valuable way to refine your search. Here are five primary use cases that need to be considered:

1. **Secure internet access:** With remote and hybrid work now the status quo, direct internet access expands the potential attack surface organizations must address. And because cybercriminals will continue to target this expanding attack surface, organizations need a solution capable of following, enabling, and protecting users no matter where they or the applications they use are located.

   SASE security must provide more than an encrypted tunnel to address today's advanced threats. It must also include a portfolio of enterprise-grade security solutions designed to inspect traffic and detect and respond to known and unknown threats. The list includes such essentials as a SWG solution to monitor and protect data and applications against web-based attack tactics, ZTNA, URL filtering, DNS security, antiphishing, antivirus, antimalware, and sandboxing.

2. **Secure private access:** A flexible SASE solution that offers fast and secure connectivity to corporate applications, whether deployed at a private data center or in the public cloud, is essential for meeting today's dynamic organizational requirements. A SASE solution with integrated ZTNA provides explicit per-application access to authenticated users without requiring a persistent tunnel. Granting access based on identity and context, combined with continuous validation, enables effective control over who and what is on the network. At the same time, a SASE solution should offer the benefit of seamless integration with SD-WAN and NGFW solutions to enable superior user experience for corporate applications by automatically finding the shortest path to those resources—powered by intelligent steering and dynamic routing capabilities from the SASE PoPs. And ideally, only one agent should be needed, combining traffic redirection, ZTNA, CASB, and endpoint protection into a single tool.

3. **Secure SaaS access:** A SASE solution must enable secure access to critical resources regardless of where applications, devices, users, and workloads are located. With growing enterprise dependence on SaaS applications, an effective cloud-delivered security solution must protect mission-critical data and secure and safeguard cloud-based information. An effective solution should support next-generation dual-mode CASB, supporting both in-line and API-based capabilities to

overcome shadow IT challenges and secure critical data. With this in mind, look for a SASE solution that offers visibility into key SaaS applications, provides reports of risky applications, ensures granular control of applications to secure sensitive data, and detects and remediates application malware across both managed and unmanaged devices.

4. **Cloud-based management:** A cloud-based SASE management system should provide comprehensive visibility, reporting, logging, and analytics to ensure efficient web security operations and reduce mean time to detect and respond (MTTD and MTTR). However, having yet another management console to monitor may place unnecessary burdens on IT teams, especially when SASE security elements operate as siloed point solutions. For organizations managing a hybrid environment, SASE management should interoperate with on-premises management. Such consolidation can be even more effective when components deployed in the SASE cloud can interoperate with on-premises solutions, ensuring consistent policy orchestration and enforcement.
5. **Simplified onboarding and flexible consumption:** SASE considerations should not just focus on how it is used but also on how you pay for it. Simple tiered licensing enables organizations to predict a cost-to-business growth correlation and use of security rather than tying up capital in excess hardware. Simplified onboarding and endpoint management should combine efficient operations with granular analytics and include pre-generated and on-demand reports—including granular logging and events across user, endpoint, and VPN events for efficient troubleshooting.

October 14, 2022 7:12 AM
1800654-0-0-EN