POINT OF VIEW

Critical Considerations When Evaluating SASE Solutions

Executive Summary

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

Today's hybrid networks are only as secure as the weakest link. 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 those often poorly secure home offices. These attacks were then able to successfully burrow into the network through encrypted VPN tunnels.

Organizations need a more advanced solution. Secure Access Services Edge (SASE) combines secure remote access, advanced per-session/per-application authentication, and enterprise-grade security in a single cloud-based solution that can be leveraged from anywhere. It extends the same protections and performance to remote workers they experience when working from their traditional on-premises office. It has quickly become a vital tool in the arsenal of IT teams needing a more reliable solution for what has now become a permanent transition to a 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 organizations with a hybrid network strategy, adding yet another set of technologies to manage can overwhelm limited IT resources.

Buyers Should Look Carefully Before Investing

Much of the 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 of the information.

As with many new markets, there are a lot of vendors popping up looking to capture a piece of the SASE market. But many solutions fall short of their promised benefits. They have immature or inadequate security technologies. They often operate as isolated stand-alone solutions that don't work with any of the other technologies across the organization, especially when integrating with the rest of the hybrid network. 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:

User access controls: Zero-trust network access (ZTNA) has emerged as one of the most essential tools for protecting today's distributed resources. A complete ZTNA solution must authenticate users, grant explicit access to specific applications, provide constant monitoring, and be able to take countermeasures if something unexpected occurs.

Not all SASE solutions are alike. Application performance, access, and security can vary widely between solutions. And for organizations with a hybrid network 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.

Consistent policy: Rather than working as a one-off solution, SASE technologies should be easily integrated into the organization's larger network and security architecture. Ideally, the security protocols and policies within the SASE solution should be identical to those being used elsewhere in the network. Systems managers should also be able to integrate their SASE solution with their existing technologies to ensure they interoperate smoothly to help optimize their security and network operations.

Network and security convergence: The vast majority of organizations will continue to operate a hybrid network that includes a traditional infrastructure well into the future. A SASE solution must be able to seamlessly handoff connections between the cloud and on-premise devices, while access and security policies must follow the user rather than terminate at the edge of the network. Only by converging networking and security end-to-end, from on-premises to the cloud to the remote user, can organizations truly implement a comprehensive zero-trust edge strategy. Extending the unique approach of security-driven networking to the cloud edge delivers consistent security and connectivity everywhere.

Purpose-built PoP: Relying on generic technologies to solve unique challenges inevitably compromises the performance and reliability of a solution. Purpose-built points of presence (PoP) combined with tightly integrated security and connectivity technologies provide higher scalability, lower latency, and more responsive and consistent security enforcement. This is why cloud providers design and build their own servers and switches rather than using off-the-shelf technology. SASE services have specific needs for performance and interoperability and services that generic systems and solutions simply can't provide.

AI-powered threat intelligence: Keeping users and applications safe requires keeping the security components of the SASE solution constantly tuned to the latest threats. 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. In addition to enterprise-class security components, a SASE solution must also leverage an AI-powered threat intelligence system built using supervised and unsupervised learning models and trained on a large and diverse set of billions of cyber events to prevent 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 sales people 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 a solution should be able to address is a valuable way to refine your search. Here are four basic use cases that need to be considered when evaluating a SASE solution.

Secure internet access: As remote and hybrid work becomes the status quo, direct internet access expands the potential attack surfaces that 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 need 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 attacks. The list should include such essentials as a secure web gateway (SWG) solution to monitor and protect data and applications against web-based attack tactics, ZTNA, URL filtering, DNS security, antiphishing, antivirus, antimalware, sandboxing, and more.

Secure private access: For many reasons, not all applications can be ported to the cloud. But as the volume of remote users trying to access applications deployed at the corporate data center continues to grow, traditional VPNs do not address critical security concerns. That's because VPNs rely on implicit trust that assumes that anyone using an encrypted tunnel can be trusted. Giving broad access to every application and then allowing lateral threat movement led to the recent spike in cybercriminals breaking into under-protected home networks and hijacking their VPN tunnels to inject ransomware payloads into the network.

A SASE solution with integrated ZTNA provides explicit per-application access to authenticated users without requiring a persistent tunnel to be established. Granting access based on identity and context combined with continuous validation enables effective control over who and what is on the network. And ideally, only one agent should be needed for ZTNA, combining traffic redirection and endpoint protection into a single tool.

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. 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 looking to manage a hybrid environment, SASE management should also be able to work with on-premises management. This consolidation effort can be even more effective when the components deployed in the SASE cloud can interoperate with on-premises solutions, ensuring consistent policy orchestration and enforcement.

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.

June 16, 2022 6:03 PM
16374812-0-0-EN