CHECKLIST

Essential SASE Must-haves

Cloud-delivered Security for the Hybrid Workforce

Over the past several years, organizations have been engaged in expanding their multi-edge networking strategies to not only enable new work-from-anywhere (WFA) realities but also support workers as they become increasingly dependent on cloud applications and environments to do their jobs. However, as these networks grow to meet new business demands, the attack surface increases.

The result is a growing gap between network functionality and security coverage that not only inherently exposes organizations to more points of compromise but also degrades the user experience of those remote workers that still rely on the conventional, virtual private network (VPN)-only solutions to access the network. This is usually because all their application traffic still needs to be backhauled through the network to receive security protections and access controls.

Secure access service edge (SASE) solutions have been developed to address these issues, enabling organizations to rapidly converge and scale out their security and networking strategies. With SASE, they can securely deliver an expanding and dynamic set of new network edges as well as meet the new demands of a hybrid workforce—distributed between on- and off-network users.

Supporting this new distributed and performance-heavy strategy is now fundamental to succeeding in today's digital marketplace. Selecting the right SASE vendor to partner with can mean the difference between operational success and struggling to keep all the essential elements working together. In theory, SASE provides secure access to the cloud for users anywhere. However, not all SASE solutions are equal in terms of scalability, security, and orchestration. The best SASE solution should not increase overhead—both in terms of the technologies that need to be implemented and the IT staff needed to get them to work as an integrated system.

Top Four Requirements of a SASE Solution

Organizations should insist on these four must-haves when considering the adoption of any SASE solution:

☑ Look for single-vendor SASE vendors for flexible deployments

SASE is designed to deliver secure, cloud-based connectivity. However, very few enterprise networks are cloud only. Even though many enterprises have a multi-cloud strategy, most still have physical networks. This means that cloud-only security is, by definition, incomplete security. The data center and other on-premises resources not only need to be protected, but they also need their policies to be deployed and orchestrated as part of a unified security strategy, using the same security products and services applied elsewhere, including those that come with SASE.

Consequently, most SSE-only vendors are limited in their ability to address security issues holistically since they only solve for cloud access security. Organizations need to insist on SASE services that are integrated with—or can be deployed as a seamless extension of—the extended network, including SD-WAN security. This is called the single-vendor SASE approach. The resulting unified security framework will lower total cost of ownership (TCO) and improve the net utility of SASE.

☑ Enterprise-grade security everywhere

When assessing any SASE solution, the functionality and performance of its security elements need to be effective. Questions to ask before selecting an SASE:

- Can its Firewall-as-a-Service (FWaaS) solution support both stateful and proxy protocols?
- Does it support SSL inspection at application speeds?
- Does it provide a full suite of tested and validated solutions, rather than forcing customers to settle for off-brand technologies?

Answering these and similar questions will help assure that your SASE selection can provide the security at scale that your enterprise demands.

A truly secure SASE solution should include the following stack of security capabilities and tools:

- **Firewall-as-a-Service (FWaaS).** Any SASE solution should include a next-generation firewall (NGFW) that:
  - Delivers high-performance secure sockets layer (SSL) inspection and advanced threat detection techniques via the cloud
  - Establishes and maintains secure connections for distributed users
  - Analyzes inbound and outbound traffic without impact on user experience
- **Domain Name System (DNS).** DNS identifies and isolates malicious domains to prevent malicious threats from entering the network.
- **Intrusion Prevention System (IPS).** IPS should be used to actively monitor the network, looking for malicious activities attempting to exploit known vulnerabilities.
- **Data Loss Prevention (DLP).** DLP functionality is needed to prevent end-users from moving key information outside the network to ensure that the network and data are both secure.
- **Secure Web Gateway (SWG).** An SWG solution secures web access against both internal and external risks. It also needs to automatically block threats, even those embedded in encrypted traffic—including TLS 1.3—with high-performance SSL inspection.
- **Zero-Trust Network Access (ZTNA).** Enterprise-grade security should be added on top of VPN and extend ZTNA to WFA users. This allows the SASE solution to inherently integrate with preexisting VPN solutions and extend zero-trust application access to off-network users.
- **Sandboxing.** Whether sandboxing is executed in the cloud or on an appliance, it provides crucial protection, especially against previously unknown threats.
- **Cloud Access Security Broker (CASB).** A solution designed to provide visibility, compliance, data security, and threat protection for cloud-based services employed by an organization. It provides policy-based insights into users, behaviors, and data stored in major SaaS applications.

☑ Unified architecture with a unified agent

Simplifying user experience is always key in any security or networking solution. Look for a SASE solution that uses a unified agent for all endpoint security features and secure connection to the cloud and the applications. A unified agent simplifies operations and improves overall user experience.

☑ Full convergence between networking and security

Security is a foundational and fundamental function of any SASE solution. The SASE elements need to interoperate as part of a seamlessly integrated security strategy, both as part of a unified SASE solution and as part of a single, holistic security fabric designed to span the entire distributed network.

Legacy equipment is here to stay and SASE integration with on-premises solutions is essential for streamlined operations and to facilitate change. Seamless integration between on-premises security (SD-WAN and/or NGFW) and cloud security is key for operations simplification, compliance requirements, and consistent security posture among all users.

January 19, 2023 7:19 PM

1924210-0-0-EN