CHECKLIST

Essential SASE Must-haves

Cloud-delivered Security for the Hybrid Workforce

Over the past few years, organizations have been engaged in constantly expanding their multi-edge networking strategies to not only enable new work-from-home realities but also support workers as they become increasingly dependent on cloud applications and environments to do their jobs. But as these networks expand to meet new business demands, the attack surface increases. And unfortunately, most legacy security solutions in place have been unable to keep pace with cloud-based networking innovations.

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 conventional, virtual private network (VPN)-only solutions to access the network. This is usually because all of their application traffic still needs to be backhauled through the network to receive security protections and access controls.

Secure access service edge (SASE) has 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.

Because 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 of 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—which translates to increased 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

To avoid these and similar challenges, organizations should insist on these four must-haves when considering the adoption of any SASE solution.

☑ SASE must function as part of an integrated security platform.

SASE is designed to deliver secure, cloud-based connectivity. However, very few enterprise networks are cloud-only. Even though more than 93% of enterprises have a multi-cloud strategy,[1] the vast majority also 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. Because of this, most SASE-only vendors are limited in their ability to address security

issues holistically since they only solve for cloud access security. Instead, organizations need to insist on SASE services that are integrated with, or can be deployed as a seamless extension of, the extended network, including wide-area network (WAN) security. The resulting unified security framework will lower total cost of ownership (TCO) and improve the net utility of SASE.

☑ Enterprise-grade security

When assessing any SASE service, the functionality and performance of its security elements need to be effective. 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 be able to automatically block threats, even those embedded in encrypted traffic—including TLS 1.3—with high-performance SSL inspection.
- **Zero-Trust Network Access (ZTNA) and Virtual Private Network (VPN).** Enterprise-grade security should be added on top of VPN and extend ZTNA to remote users. This allows the SASE solution to inherently integrate with preexisting VPN solutions and extend zero-trust application access to remote off-network users.
- **Sandboxing.** Whether sandboxing is executed in the cloud or on an appliance, it provides crucial protection, especially against previously unknown threats.

☑ Third-party validated research and services

In addition to needing a unified security framework, a SASE service is also only as good as the threat intelligence that informs it. Any SASE vendor being considered should have a track record of advanced security research and innovation, not just networking experience. This helps ensure that not only is the security being deployed and consumed through their SASE solution world-class but that it is also being continuously updated to counter the latest threat techniques and technologies.

From threat intelligence to protection, SASE vendors that offer Technology-as-a-Service (TaaS) naturally need to provide reliable solution maintenance and upgrades for their SASE services and capabilities. But that's just the start. Any serious TaaS offering also needs to include advanced threat detection against both known and zero-day threats. So, before an organization embarks on their SASE journey, they should verify that any vendor under consideration is invested in threat research and the continuous improvement of their SASE security offering.

Make Sure SASE Security Is Part of a Holistic Security Strategy

Security is a foundational, fundamental function of any SASE solution. Every element must operate as an enterprise-grade solution. Things like third-party testing and validation, and a history of delivering world-class security solutions, are ways to guarantee those results. And just as importantly, those 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.

[1] Janakiram MSV, "10 Key Takeaways From RightScale 2020 State Of The Cloud Report From Flexera," Forbes, May 2, 2020.

FORTINET

www.fortinet.com

March 5, 2021 5:48 AM

D:\Fortinet\2021 Rebranded templates\Checklist\February\SASE checklist\cl-FA-essential-sase-must-haves-342021\cl-FA-essential-sase-must-haves-342021

914297-0-0-EN