CHECKLIST

5 Essential SASE Must-Haves

Cloud-Delivered Security for the Hybrid Workforce

Over the past several years, organizations have been expanding their multi-edge networking strategies to enable new hybrid work realities and support work-from-anywhere (WFA) users 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 inherently exposes organizations to more points of compromise and degrades the user experience of those remote workers who still rely on the conventional, virtual private network–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 their security and networking strategies. With SASE, they can securely deliver an expanding and dynamic set of new network edges and 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 can mean the difference between operational success and struggling to keep all the essential elements working together. In theory, SASE provides WFA users with secure access to the cloud no matter where they are. However, not all SASE solutions are equal when it comes to scalability, security, and orchestration. The best SASE solution won't increase overhead by adding the technologies that need to be implemented and the IT staff required to get them to work as an integrated system.

Top Five Requirements of a SASE Solution

Organizations should insist on these five 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 incomplete security. The data center and other on-premises resources need to be protected, and their policies need 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 vendors that just provide security service edge (SSE) are limited in addressing security issues holistically as they only solve for cloud-access security. Organizations must insist on SASE services that are integrated with or can be deployed as a seamless extension of the extended network, including SD-WAN security or even integration with LAN networks to address smaller locations. This can be solved with a single-vendor SASE approach, where the same vendor builds the networking and security components from the ground up. The resulting unified security framework will lower the total ownership cost and improve SASE's net utility.

☑ Enterprise-grade security everywhere

Effective security is the cornerstone of any SASE solution. Organizations must look for features such as Firewall-as-a-Service capable of supporting diverse protocols and high-speed SSL inspection. Additionally, a comprehensive suite of security components is essential to safeguard against a wide range of cyberthreats. The components should include:

- Domain Name System
- Intrusion prevention system
- Data loss prevention
- Secure web gateway
- Zero-trust network access
- Sandboxing
- Cloud access security broker

These security measures should be scalable and provide robust protection without compromising performance or user experience.

☑ Unified architecture with a unified agent

Simplifying user experience ensures widespread adoption and adherence to security protocols. A unified agent that consolidates endpoint security features and facilitates secure connections to cloud applications streamlines operations and enhances user satisfaction. A unified approach reduces complexity and ensures consistent security enforcement across all endpoints, regardless of their location or access method.

☑ Full convergence between networking and security

The integration of networking and security functionalities is critical for the seamless operation of a SASE solution. Organizations should prioritize solutions that offer seamless interoperability between on-premises security infrastructure, such as SD-WAN, next-generation firewalls, and cloud-based security components. This convergence facilitates operational efficiency, compliance adherence, and consistent security posture across distributed networks.

☑ Digital experience monitoring for performance optimization

In addition to security considerations, organizations must prioritize the monitoring and optimization of digital experiences for end-users. Digital experience monitoring encompasses real-time performance monitoring, end-user experience tracking, and application performance analytics. Organizations can proactively identify and address performance bottlenecks to ensure optimal user productivity and satisfaction across all network environments.

FORTINET

www.fortinet.com

March 26, 2024 4:03 PM

2633753-0-0-EN