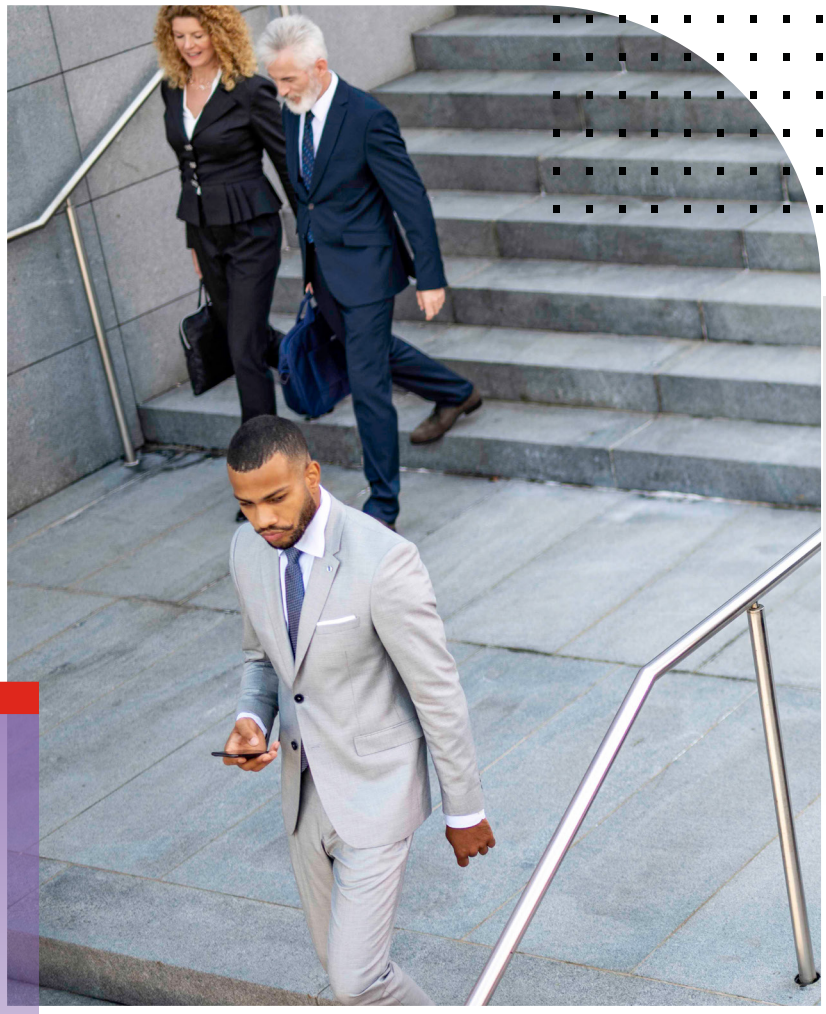
WHITE PAPER

SASE—Ensuring Cloud-Delivered Security Everywhere for Users Anywhere



Executive Summary

Enterprise networks are increasingly reliant on cloud-based applications. They use them to run their businesses and support distributed workflows for remote and mobile users. To support the rapid growth of users looking to access these cloud services—whether from the traditional core network, or from new home, branch office, and other remote location edges—organizations have had to rapidly expand the conventional enterprise network.

This hybrid workforce, accessing critical resources from a variety of devices and locations, has redefined the network, and as a result, infrastructure teams have been challenged to manage and secure the resulting expanded attack surface. Secure access service edge (SASE) solutions are designed to converge networking and cloud-delivered security services into a single, integrated package to enable flexible, secure, anytime and anywhere access between all network edges and remote users.

However, SASE solutions must also be able to function as part of the extended network. Cloud-only solutions only address part of the challenge organizations face, which means that SASE must be designed and delivered as part of a larger, converged, and integrated security framework.

"Customer demands for simplicity, scalability, flexibility, low latency, and pervasive security force convergence of the secure tools for hybrid workforce."[1]

"The need for enhanced business agility and secure remote access to support digital transformation has led to the adoption of the secure access service edge, or SASE, model."[2]

Defining SASE

SASE is specifically designed to support cloud-first initiatives for business applications, especially for those employees who are increasingly working off-network. SASE solutions enable digital innovation by ensuring business continuity in constantly evolving environments while delivering consistent security capabilities across distributed networks and a dispersed workforce. The result is improved business continuity, consistently secure access to cloud applications, and enhanced user experience.

In addition to providing secure and flexible connectivity, SASE is also designed to help organizations control capital expenditures and reduce security infrastructure complexity resulting from digital innovation. It also helps address the gaps in connectivity and security created by many traditional software-defined wide-area networking (SD-WAN) solutions by providing proven and integrated security for the WAN and cloud edges.

A proper SASE solution should also enable infrastructure leaders to extend the value of their existing investments in security infrastructure by providing those same security solutions in the cloud. To achieve this, SASE solutions should be built around a common set of security solutions and an expansive architecture that can be deployed at every edge to extend the protections used to secure traditional environments out to remote workers and to secure the thin edge of the network. And cloud-delivered access control should also be consistent and integrated within a larger access strategy.

Because the environments in which people work span the entire network, a cloud-based solution alone is rarely enough. SASE is generally described in terms of cloud-delivered services. But for SASE to be truly effective, it also needs to support those network environments that rely on the integration between cloud-based solutions and the physical network. To achieve consistent and seamless functionality and policy enforcement end to end, SASE cloud connectivity needs to be combined with network access controls, wireless local-area network (LAN) controllers, Wi-Fi access points at branch offices, and the variety of security tools deployed across the network's evolving edges.

This means that, in addition to its essential cloud-based protections, a robust SASE solution also needs to interoperate with such things as universal access, network segmentation, and compliance requirements. A cloud-based security solution alone can't address these without shuttling local traffic on the physical network out to the cloud for inspection.

Key Elements of a SASE Solution

While most network solutions have been able to evolve rapidly enough to support the workflows of remote users, offices, and endpoints, most security tools and solutions have not kept pace, failing to offer consistent security and ensure optimal user experience for on-premises and remote users.

For example, virtual private network (VPN)-only solutions only offer minimal protections, leaving organizations exposed to the risk of lateral threat movement by threat actors and malware when compromised users and devices access the network. This issue is equally profound when potentially compromised users attempt to directly access cloud-based applications. Unfortunately, enterprise security stakeholders face the challenge of trying to secure their distributed networks using a loose collection of distributed tools often completely isolated from the network and from each other. Vendor and solution sprawl, resulting from rapid digital innovation, is typified by siloed point security products. This adds another layer of management and control complexity.

Managing and correlating these distributed and disconnected solutions is overwhelming already overburdened security teams, making the enforcement of a uniform security policy for a hybrid workforce—one that has been split between on-net and off-net users—nearly impossible. For organizations to remain competitive, while addressing the evolving threat landscape, all endpoints must be secured and managed using consistent and integrated security and networking policies that can be applied to all network users, wherever they're located.

The typical enterprise has an average of 45 security solutions deployed across its distributed environment.[3]

Too Few Qualified Vendors

Conceptually, SASE was designed to address the security challenges caused by a lack of consistent security for remote off-network and on-network thin edge users. The challenge is that SASE is intended to address the control and security needs of distributed and dynamic networks—whether on-premises or remote. However, very few SASE vendors are qualified to provide a comprehensive solution designed to provide the level of security and WAN integration organizations actually need.

Trying to build a comprehensive security strategy using a SASE-only vendor, for example, often results in a solution that has been cobbled together using disparate tools from different security vendors—and worse, they are usually different from those deployed across the rest of the network. Such an approach is not only expensive but also negates the core intent of SASE, which is to provide consistent security everywhere while simplifying deployment and management.

To avoid this challenge, a SASE solution must function as an extension of existing WAN security functionality even though it is delivered via the cloud. Proven and certified security solutions deployed at the WAN edge, designed to natively interoperate with the rest of an organization's security framework, are required. Otherwise SASE only solves half of the challenges facing today's hybrid workforce, enabling access while isolating users and services and preventing universal visibility and control across the network.

[1] Frank Marsala, "The Future of Network Security Is in the Cloud," Gartner, September 13, 2019.

[2] Geetha Nandikotkur, "The SASE Model: What's Driving Adoption?" Data Breach Today, August 31, 2020.

[3] Charlie Osborne, "The more cybersecurity tools an enterprise deploys, the less effective their defense is," ZDNet, June 30, 2020.

FORTINET

www.fortinet.com

March 3, 2021 2:45 AM

D:\Fortinet\2021 Rebranded templates\White paper\March\FortiSASE\wp-FA-sase-ensuring-cloud-delivered-security-everywhere-332021\wp-FA-sase-ensuring-cloud-delivered-security-everywhere-332021

123456-0-0-EN