HUGHES
An EchoStar Company

FORTINET

Choosing the Best SASE Solution for Your Hybrid Workforce

Table of Contents

Executive Summary

Today, organizations must provide their work-from-anywhere (WFA) employees with secure, authenticated access to critical applications and resources. Many organizations are turning to secure access service edge (SASE), a reliable and flexible security solution to protect their networks, data, and hybrid workforce.

A strong SASE solution combines secure remote access, advanced per-session and per-application authentication, and enterprise-grade security into a single cloud-based solution. SASE can be leveraged from anywhere and extend the same protections and performance to WFA staff that they experience when working from a traditional on-premises office.

Unfortunately, not all SASE solutions are effective. Application-specific access, security features, and security efficacy can vary widely. And organizations with hybrid networks, adding yet another set of technologies to manage, can overwhelm limited IT resources. This is especially difficult when trying to manage environments end to end to detect issues and optimize user experience. IT leadership must carefully consider several critical capabilities across some core use cases when evaluating SASE for their environments.

How Today's WFA Users Impact Cybersecurity

A hybrid workforce is challenging for most organizations. Adding to the difficulty is the number of applications and services steadily moving to the cloud for greater efficiency, cost savings, and elasticity.

The evolution of how business operates today has created issues for cybersecurity teams. A recent survey reveals that 73% of security and business leaders feel their organizations are more exposed to risk due to remote work.[1]

These growing problems are often the result of outdated or insufficient security that was never designed to address today's challenges.

For example, many businesses discovered in the first weeks of the COVID-19 pandemic that their traditional virtual private networks (VPNs) were not an ideal connectivity strategy for their sudden increase in WFA users. VPNs were never intended to operate at scale, ultimately creating security problems.[2]

Protecting rapidly evolving hybrid work environments calls for robust, purpose-built security such as a SASE solution strategy.

New requirements associated with expanding attack surfaces are driving demand for emerging technologies that identify and help prioritize threat exposures across internal and external environments.[3]

Taking a Single-Vendor SASE Approach

To ensure consistent connectivity and security for WFA users, networking and security solutions must converge at the edges and in the cloud. At its most basic level, SASE combines multiple Networking-as-a-Service (NaaS) and Security-as-a-Service (SaaS) functions into a single solution.

This can be difficult to achieve when integrating solutions from different vendors. However, a platform-centric, single-vendor SASE solution consolidates technologies and converges networking and security functions to drive operational efficiency. But SASE solutions don't exist in a vacuum. So, it is also critical for organizations to look for SASE solutions that can be seamlessly integrated into their larger networking and security architectures to ensure secure and reliable connectivity and deliver superior user experience wherever needed.

As with any new opportunity, vendors invariably materialize, looking to fill an urgent need and capture a piece of the new market. However, many of these solutions fall short of their promised benefits.

Some rely on immature technologies or inadequate capabilities. Many operate as isolated, standalone solutions that don't integrate with existing security technologies or the expanding hybrid network. Few enable organizations to build a seamless solution that reduces rather than complicates solution sprawl.

For those organizations trying to manage a rapidly expanding and highly dynamic hybrid network, adding yet another set of technologies to manage can overwhelm limited IT resources. The manual controls, scripts, and limited threat intelligence used by many SASE vendors cannot keep up with today's rapidly evolving threat landscape, leaving organizations vulnerable.

No matter why an organization starts its SASE journey, it ultimately experiences multiple benefits through improving security efficacy and increasing performance.[4]

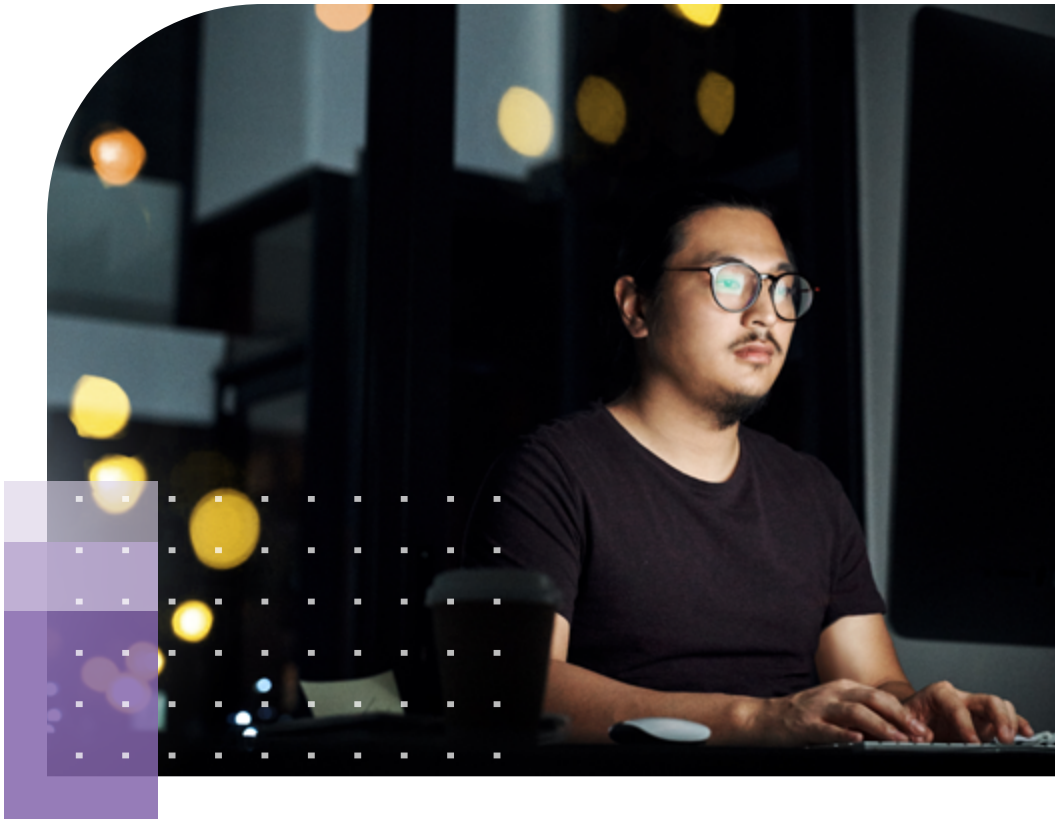
Choosing Your Solution

When it comes to evaluating critical capabilities and selecting the best SASE solution to protect your remote workforce, there are eight core considerations to look for:

1. A single-vendor SASE approach

Trying to get solutions from different vendors to work together as a unified SASE architecture is difficult to build and can be time-consuming to maintain and troubleshoot. A single-vendor SASE approach converges networking and security, so management, optimization, and policy enforcement are all controlled through a single interface.

Ideally, single-vendor solutions also interoperate across the distributed network, seamlessly handing off connections between the cloud and on-premises devices. This allows access and security policies to follow users and applications end to end rather than terminating connectivity and control at either edge of the network.



Organizations can implement a comprehensive zero-trust architecture that delivers consistent security and superior user experience everywhere by truly converging networking and security across the entire IT environment.

2. A unified agent for multiple use cases

Onboarding different agents for every use case can quickly become too complex and expensive to maintain. An effective SASE solution offers a single agent that supports multiple use cases, including zero-trust network access (ZTNA), cloud access security broker (CASB), and endpoint protection, while automatically redirecting traffic to protect assets and applications through cloud-delivered security.

3. Secure internet access

With remote work becoming the new normal, users with direct internet access greatly expand the organization's potential attack surface. An effective solution must follow, enable, and protect users no matter where they (or their applications) are located.

A cloud-delivered security solution should offer more than just an encrypted tunnel (such as traditional VPNs). It should include a portfolio of enterprise-grade security solutions designed to inspect traffic and detect and respond to known and unknown attacks. With this in mind, a successful SASE solution includes secure web gateway capabilities to monitor and protect data and applications against web-based attack tactics along with other features, such as URL filtering, DNS security, antiphishing, antivirus, anti-malware, sandboxing, and deep-SSL inspection.

4. Flexible, secure private access

A flexible SASE solution provides secure connectivity to corporate applications, whether deployed in a private data center or the public cloud.

Integrated ZTNA provides explicit per-application access to authenticated users without requiring a persistent tunnel. ZTNA grants access based on identity and context, combined with continuous validation, and ensures effective control over who and what is on the network.

Your ideal SASE solution should seamlessly integrate with SD-WAN and next-generation firewall (NGFW) solutions to provide intelligent steering and dynamic routing capabilities through the SASE POP, ensuring superior user experience by automatically finding and securing the shortest path to corporate applications. Ideally, it should provide all this through a single agent for ZTNA, traffic redirection, CASB, and endpoint protection.

5. Secure SaaS access

An effective SASE solution must enable secure access regardless of where applications, devices, users, and workloads are located—a function vital to WFA users that regularly move between campus, branch, home office, and mobile environments. And with growing enterprise dependence on SaaS applications, an effective cloud-delivered security solution must also protect mission-critical data and safeguard cloud-based information with the same enterprise-grade security whether users are on or off-premises. It should also support dual-mode CASB, with support for both inline and API-based capabilities, to identify and overcome shadow IT challenges while securing critical data.

In summary, organizations should look for a SASE solution that offers:

- Visibility into key SaaS applications
- Reports on risky applications
- Granular control of applications to secure sensitive data
- Detection and remediation of malware in applications across both managed and unmanaged devices

6. Flexible consumption with simplified onboarding

Considerations for selecting a SASE solution should go beyond just the technology. They should also include how you pay for it. The right SASE can help organizations shift their business consumption from a capital expenditure to an operating expenditure model. To do this effectively, it should offer simple tiered licensing that enables organizations to predict a cost-to-business growth correlation and use of security rather than tying up capital in excess hardware.

Ongoing cost controls can also be tied to simplified onboarding and consolidated endpoint management systems. Centralized management should also combine efficient operations with granular analytics and include pre-generated and on-demand reports, including logging and events across user, endpoint, and VPN events for efficient troubleshooting.

7. Simple cloud-based management and visibility

A cloud-based SASE management system should provide comprehensive visibility, reporting, logging, and analytics. This helps ensure efficient security operations while reducing mean time to detection and remediation. The challenge is that SASE security elements that operate as siloed point solutions can place unnecessary burdens on security teams, especially for organizations managing a hybrid environment with limited IT resources.

This integration can be even more effective if the SASE components deployed in the cloud seamlessly interoperate with on-premises security solutions for consistent policy orchestration and enforcement.

Digital experience monitoring (DEM) for proactive troubleshooting and end-to-end visibility is also key to any SASE solution. DEM empowers organizations with unified visibility into users' experiences as they interact with applications and devices. DEM encompasses endpoint devices, on-premises networking, users, and applications. It allows organizations to comprehensively view the end-user experience and translate it into measurable business outcomes.

8. Deployment flexibility to cater to all configurations

A SASE solution should adapt to organizations' architecture and include expanded integrations to WLAN and LAN extenders to support organizations securing microbranches and related devices. This presents organizations with a new approach to cloud-based security by extending enterprise-grade protection, such as sandboxing, intrusion prevention systems, and URL filtering, to microbranches without additional security appliances or services.

Working from Anywhere without Worry

With an estimated 66% of the U.S. workforce continuing to work remotely,[5] the challenges of securing a hybrid workforce appear to be a permanent reality that security teams must address. When implemented correctly with the requisite capabilities to solve core use cases, the right SASE solution can deliver secure and reliable access to disparate workforces while providing enterprise-grade, cloud-delivered security to harden remote connections.

A well-chosen solution can also help your organization focus on core business tasks while removing the need to manually manage complex integrations, delivering a consistent security posture across your organization's evolving hybrid IT environments end to end.

[1] "Zero Trust Security in the Age of Remote Work," i4DM, LinkedIn, September 6, 2023.

[2] Andrew Froehlich, West Gate Network, "Hybrid workforce model needs long-term security roadmap," TechTarget, June 25, 2021.

[3] Ruggero Contu, Elizabeth Kim, Jonathan Nunez, "Emerging Tech: Security — The Future of Attack Surface Management Supports Exposure Management," Gartner, April 19, 2023.

[4] Dave Abbott, "As SASE Evolves, Organizations Can Choose the Best Model to Meet Their Needs," CDW, April 24, 2023.

[5] Jack Flynn, "25 Trending Remote Work Statistics [2023]: Facts, Trends, and Projections," Zippia, June 13, 2023.

FORTINET

www.fortinet.com

January 2, 2024 3:38 PM

1777526-A-0-EN