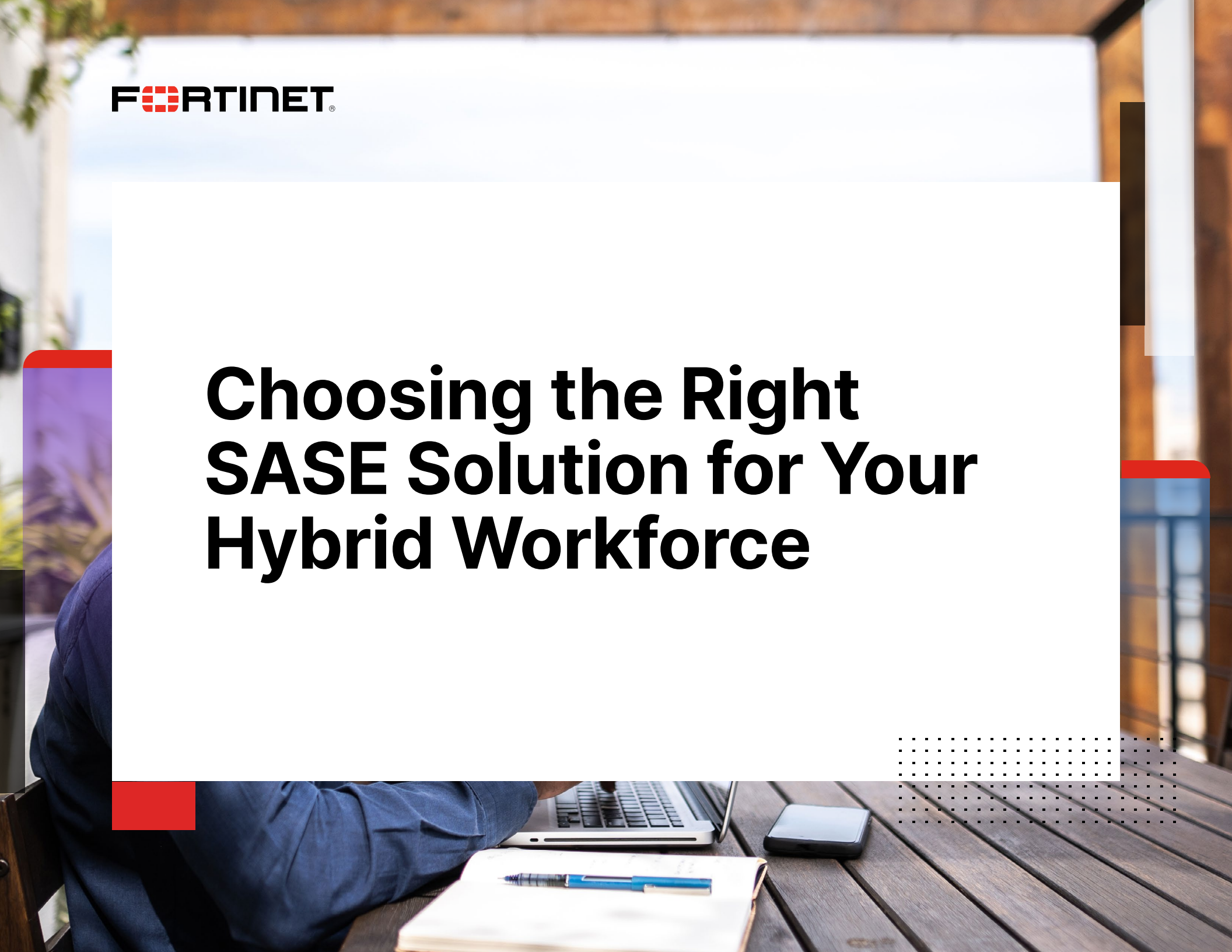


Choosing the Right SASE Solution for Your Hybrid Workforce

Table of Contents

Executive Overview	3
How Today’s Hybrid Workforce Impacts Cybersecurity	4
Taking a Single-Vendor SASE Approach	6
Choosing Your Solution: What to Look for	8
Working from Anywhere Without Worry	12

Executive Overview

Providing secure, authenticated access to critical applications and resources—whether workers are on-premises, working from home, or somewhere between—is now a permanent requirement for most organizations. Secure Access Service Edge (SASE) solutions offer a reliable and flexible solution for the now permanent transition to a hybrid, work-from-anywhere (WFA) model. SASE solutions should combine secure remote access, advanced per-session and per-application authentication, and enterprise-grade security in a single cloud-based solution that can be leveraged from anywhere, extending the same protections and performance to remote workers they experience when working from a traditional on-premises office.

However, not all SASE solutions are alike—application-specific access, security features, and security efficacy can vary widely. And for organizations with a hybrid network, adding yet another set of technologies to manage can overwhelm limited IT resources, especially when trying to manage their environment end to end to detect issues and optimize user experience. Organizations must carefully consider several critical capabilities across a number of core use cases when evaluating SASE for their environment.

How Today's Hybrid Workforce Impacts Cybersecurity

A hybrid workforce is the new reality for most businesses. The percentage of workers worldwide that now permanently work from home doubled last year.[1] One survey shows that 83% of business and IT leaders see hybrid work as a mainstay of future operations, and 42% think that more than half of their workforce will remain permanently hybrid now that the pandemic is behind us.[2]

Another fact of modern business is the number of applications and services moving to the cloud for greater efficiency, cost-savings, and elasticity. As much as half of all spending across applications, infrastructure software, business process services, and system infrastructure markets will have shifted to the cloud by 2025.[3]

But these rapid changes to how businesses operate have created new problems for cybersecurity teams. A recent survey reveals that 80% of security and business leaders feel their organizations are more exposed to risk due to remote work.[4] This is borne out by data showing that the overall volume of attacks increased by 31% last year, fueled by cybercriminals trying to exploit rapid changes to business networks.[5] The number of successful data breaches also grew last year, eclipsing the previous annual record by 23%.[6]

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 expanded remote workforce. VPNs were never intended to operate at scale, ultimately creating security problems.[7] They also carry numerous risks, especially if the network is poorly configured (the Colonial Pipeline attack was administered via just such a VPN).[8] Still, other security gaps arise due to a lack of cloud awareness and security circumvention.[9]

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

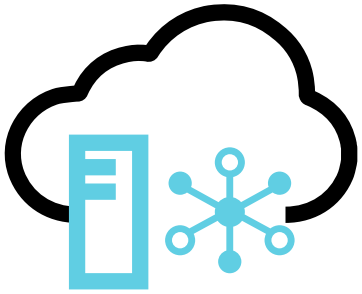
Every organization has a rapidly expanding attack surface due to more hybrid environments, new connectivity options, and additional business-critical applications deployed into the cloud.[10]

Taking a Single-Vendor SASE Approach

To ensure consistent connectivity and security for users everywhere, 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 trying to integrate solutions from different vendors. However, a platform-centric, single-vendor SASE solution enables the consolidation of 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 pop up 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.



What SASE really stands for is a better way to deliver cybersecurity technologies using a convergence of cloud software and networking tools.[11]

Choosing Your Solution: What to Look for

When it comes to evaluating critical capabilities and selecting the best SASE solution to protect your remote workforce, there are seven 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 not just difficult to build but 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. And ideally, that single-vendor solution should 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. Only by truly converging networking and security across the entire business environment can organizations implement a comprehensive zero-trust architecture that delivers consistent security and superior user experience everywhere.

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 should offer a single agent that supports multiple use cases, including 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 be able to 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 offer 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 will include secure web gateway (SWG) 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 should provide 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's ability to grant access based on identity and context, combined with continuous validation, ensures effective control over who and what is on the network. Your SASE solution should also seamlessly integrate with SD-WAN and 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. And ideally, it should provide all of 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 a hybrid workforce that regularly moves 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 in-line and API-based capabilities, to identify and overcome shadow IT challenges while securing critical data. With all this in mind, organizations should look for a SASE solution that offers visibility into key SaaS applications, reports on risky applications, provides granular control of applications to secure sensitive data, and can detect and remediate 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 (CapEx) to an operating expenditure (OpEx) 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 such things as 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

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 (MTTD) and remediation (MTTR). 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.

Working from Anywhere Without Worry

With an estimated 50% of the U.S. workforce continuing to work from home long term,[12] the challenges of securing a hybrid workforce appear to be a permanent reality that security teams must address in the near term. 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. But more, 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 evolving hybrid IT environments end to end.

[1] "Securing the hybrid workforce," Security Magazine, January 7, 2022.

[2] "83% of IT leaders believe the hybrid workforce is here to stay," Tech Republic, November 3, 2021.

[3] "What is cloud computing? Everything you need to know about the cloud explained," ZD Net, February 25, 2022.

[4] "Corporate attack surface exploding as a result of remote work," Help Net Security, September 27, 2021.

[5] "Cybersecurity Still A Challenge, And Improving Resiliency Is Essential," Forbes, December 15, 2021.

[6] "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," ITRC, January 24, 2022.

[7] "Hybrid workforce model needs long-term security roadmap," Tech Target, June 25, 2021.

[8] "The Cybersecurity Challenges Of Working From Anywhere," Forbes, March 2, 2022.

[9] "Misconfigurations: Still the Biggest Threat to Cloud Security," Network Computing, August 25, 2021.

[10] "Predictions for 2022: Tomorrow's Threats Will Target the Expanding Attack Surface," Fortinet, November 16, 2021.

[11] "What's Driving The SASE Boom," Forbes, November 11, 2021.

[12] "83% of IT leaders believe the hybrid workforce is here to stay," Tech Republic, November 3, 2021.

FORTINET®

www.fortinet.com

October 17, 2022 10:17 AM
1777526-0-0-EN