Evaluating SASE for the Work-From-Anywhere Era

Table of Contents

Executive Overview

Secure authenticated access to critical applications and resources—whether workers are on-premises, working from home, or somewhere between—will be a persistent need for most organizations around the world. Secure access service edge (SASE) offers a reliable solution for what has now become a permanent transition to a hybrid, work-from-anywhere (WFA) model. SASE combines secure remote access, advanced per-session/per-application authentication, and enterprise-grade security in a single cloud-based solution that can be leveraged from anywhere. It extends 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 efficacy, and security features vary. And for organizations with a hybrid network strategy, adding yet another set of technologies to manage can overwhelm limited IT resources. 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 has become the new reality for a majority of businesses. The percentage of workers around the world that permanently work from home doubled last year.[1] A recent survey also shows that 83% of business and IT leaders see hybrid work in their future, and 42% think that more than half of their workforce will be hybrid post-pandemic.[2]

Another fact of modern business today is the number of applications and services that are moving to the cloud for greater efficiency, cost-savings, and elasticity. As much as half of spending across application software, 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 simultaneously created new problems for cybersecurity teams. A recent survey shows that 80% of security and business leaders feel their organizations are more exposed to risk as a result of remote work.[4] The overall volume of attacks increased by 31% last year, as cybercriminals continue to try to take advantage of 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These growing problems are a result of outdated or insufficient security. Many businesses discovered in the first weeks of the COVID-19 pandemic that traditional virtual private networks (VPNs) are not an ideal connectivity strategy for an expanded remote workforce. VPNs were never intended to operate at scale, which ultimately creates problems for security.[7] They 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 **secure access service edge (SASE)**.

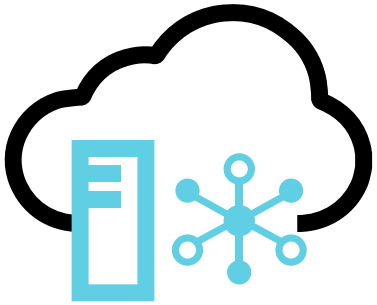
Practically every organization has a rapidly expanding attack surface as a result of more hybrid environments, new connectivity options, and additional business-critical applications deployed into the cloud.[10]

Not All SASE Solutions Are the Same

At its most basic level, SASE combines multiple networking and Security-as-a-Service functions together into a single solution. The convergence of networking and security solutions should occur at edges and in the cloud to ensure consistent security to users. This also allows organizations to seamlessly deploy secure connectivity wherever it's needed.

But as with any cybersecurity innovation, there have been many vendors popping up looking to fill an urgent need and capture a piece of the cloud-delivered security market. But 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 expanding parts of the hybrid network.

And for organizations with a hybrid network strategy, 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 for protecting the remote workforce, there are five core use cases to consider:

Secure internet access

With remote work settling in to be a major feature of the new normal, users with direct internet access greatly expands the organization's potential attack surface. An effective solution will be capable of following, enabling, and protecting 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. Other features to look for include URL filtering, DNS security, antiphishing, antivirus, anti-malware, sandboxing, and deep-SSL inspection.

Secure private access

For many reasons, not all applications can be ported to the cloud. But as the volume of remote users trying to access applications deployed at the corporate data center continues to grow, traditional VPNs do not address critical security concerns. That's because VPNs rely on implicit trust that assumes that anyone using an encrypted tunnel can be trusted. Giving broad access to every application and then allowing lateral threat movement led to the recent spike in cybercriminals breaking into under-protected home networks and hijacking their VPN tunnels to inject ransomware payloads into the network.

A SASE solution with integrated zero-trust network access (ZTNA) provides explicit per-application access to authenticated users without requiring a persistent tunnel to be established. Granting access based on identity and context combined with continuous validation enables effective control over who and what is on the network. And ideally, only one agent should be needed for ZTNA, combining traffic redirection and endpoint protection into a single tool.

Secure Software-as-a-Service (SaaS) access

A SASE solution must enable secure access regardless of where applications, devices, users, and workloads are located—which is vital to remote-based workforces. With growing enterprise dependence on SaaS applications, an effective cloud-delivered security solution must protect virtualized environments, keep mission-critical data secure, and safeguard cloud-based information. User productivity is also an important factor. An effective solution also optimizes performance by leveraging cloud availability, enabling users to quickly access applications, resources, and the internet from any location. With all this in mind, look for a SASE solution with in-line cloud access security broker (CASB) capabilities.

Flexible consumption with simplified onboarding

Considerations should also include how you pay for security. SASE can help organizations shift their business consumption from a capital expenditure (CapEx) to an operating expenditure (OpEx) model. An effective solution will 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.

Simplified onboarding and endpoint management should combine efficient operations with granular analytics and include pre-generated and on-demand reports—including granular logging and events across user, endpoint, and VPN events for efficient troubleshooting.

Simple cloud-based management

A cloud-based SASE management system should provide comprehensive visibility, reporting, logging, and analytics. This helps ensure efficient security operations and reduce mean time to detection (MTTD) and remediation (MTTR) incidents. But SASE security elements that operate as siloed point solutions can place unnecessary burdens on security teams—especially for organizations that are managing a hybrid environment with limited IT resources.

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

It's important to fully understand the different SASE solution functions and what they can offer. A recent survey shows that only 31% of teams could correctly define what SASE is.[12]

Working From Anywhere Without the Worry

With an estimated 50% of the U.S. workforce continuing to work from home long term,[13] 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, SASE offers cloud-delivered security to securing remote connections and deliver secure access to disparate workforces. Even more, a well-chosen solution can help your organization focus on core business tasks while removing the need to manually manage complex integrations and deliver a consistent security posture across hybrid IT environments.

[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] "Benefits of integrating security and networking with SASE," Tech Radar Pro, April 1, 2022.

[13] "83% of IT leaders believe the hybrid workforce is here to stay," Tech Republic, November 3, 2021.

FORTINET®

www.fortinet.com

July 14, 2022 12:18 AM

1639964-0-0-EN