FORTINET

Buyer’s Guide to Unified SASE

Considerations for Selecting the Best Single-Vendor SASE Solution for Your Hybrid Workforce

Challenges

With the rise of the hybrid workforce, organizations need to secure employees who access the network and applications from on-site and off-site locations. This shift to work-from-anywhere (WFA) has significantly expanded the attack surface, created security gaps, and increased the complexity of network and application protection.

Virtual private networks (VPNs) for securing remote access are no longer sufficient to effectively secure hybrid workforce access to enterprise applications. VPNs often provide more access than a user needs to an organization's network. This expands the attack surface, making it easier for an attacker with stolen credentials to access critical resources. Because VPNs do not inspect connections, they can inadvertently expand the attack surface through a hijacked connection or compromised endpoint device, increasing the risk of lateral threat movement. In addition, VPNs are usually aggregated at a central location, adding latency issues for people working from home or other remote locations.

Users are not only increasingly accessing SaaS and other distributed applications in the cloud, but there has been a significant rise in the use of unauthorized applications, known as shadow IT. Security teams need visibility into which SaaS applications are being used and to control what type of data is stored or accessed through these applications.

Further, securing the modern hybrid workforce environment can be a unique challenge because many of these changes have occurred organically rather than through a carefully planned strategy. The rapid proliferation of new network edges with multiple network and security products and the inclusion of WFA users, often implemented as independent projects, have created vulnerabilities that cybercriminals eagerly exploit.

Figure 1: Trends and drivers for SASE

SASE Addresses the Challenges

A secure access service edge (SASE) architecture addresses the challenges of securing WFA users by providing secure access and high-performance connectivity to users in large and small branches or other off-site locations.

SASE architecture converges SD-WAN with cloud-delivered security service edge (SSE) capabilities to provide users with secure and fast access to the internet, SaaS, and private applications from any location.

SSE capabilities, including zero-trust network access (ZTNA), Firewall-as-a-Service (FWaaS), secure web gateway (SWG), and cloud access security broker (CASB), are delivered as a cloud service and enable zero-trust access based on the identity of a device or entity. With real-time context and security and compliance policies, SSE helps ensure consistent monitoring and enforcement.

Unified SASE is a single-vendor SASE solution in which all SASE components are tightly integrated based on a common OS engine with unified management and agent. It enables flexible deployment with a unified policy that supports on-premises connectivity from the branch using secure SD-WAN, thin edges (such as wireless APs), client agents, and agentless support (such as Chromebooks). The resulting unified security framework lowers the total cost of ownership (TCO), providing deployment flexibility rather than replacing the current on-premises infrastructure and providing consistent security everywhere.

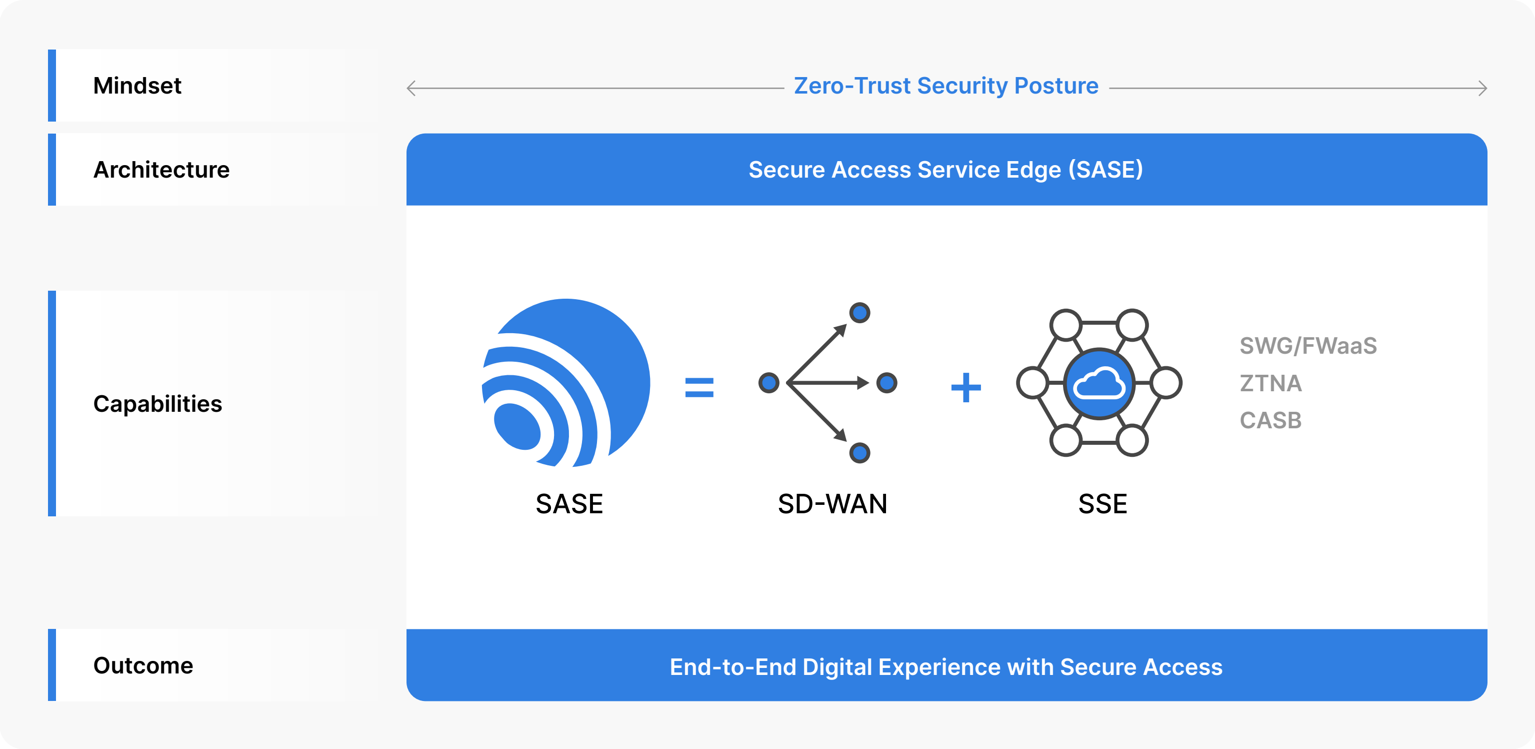

Mindset
Zero-Trust Security Posture
Architecture
Secure Access Service Edge (SASE)
Capabilities
SASE
=
SD-WAN
+
SSE
SWG/FWaaS
ZTNA
CASB
Outcome
End-to-End Digital Experience with Secure Access

Figure 2: SASE framework to enable secure access

SASE Use Cases

For most organizations, SASE is a journey that needs to scale and adapt as your business requirements evolve. To ensure you have the right solution, identify your organization's key drivers and use cases before evaluating a SASE solution.

The most common use cases and drivers for SASE include:

- Replacing legacy VPN with ZTNA secure remote access
- Securing SaaS access with shadow IT visibility and SaaS data protection (CASB)
- Consistent, secure internet access for your hybrid workforce (SWG and FWaaS)
- Network modernization for WAN edge (SD-WAN)
- Consolidation of multiple network and security products to reduce complexity and overhead
- Cloud-delivered security

Identifying your critical business drivers and use cases will help you choose the right SASE solution for your current and future needs. Once you have identified your use cases, you must define your requirements holistically to meet your functional requirements while enabling seamless integration with your existing network and security infrastructure. SASE should be deployed as something other than a standalone solution. Selecting a SASE solution designed to interoperate with your network and security infrastructure helps simplify deployment and operational overhead to meet your budget constraints and implementation timelines.

Main Considerations When Choosing an Enterprise SASE Solution

Many SASE solutions only solve part of the problem. They either fail to provide consistent enterprise-grade cybersecurity to their WFA users or cannot seamlessly integrate with the range of physical and virtual network and security tools deployed at the network edge. The result is an inability to deliver consistent cybersecurity and optimal user experiences. In addition, not all SASE solutions are equal regarding scalability, security, and orchestration. The best SASE solution should not increase overhead regarding the technologies that must be implemented or the IT staff required to get it to work as an integrated system.

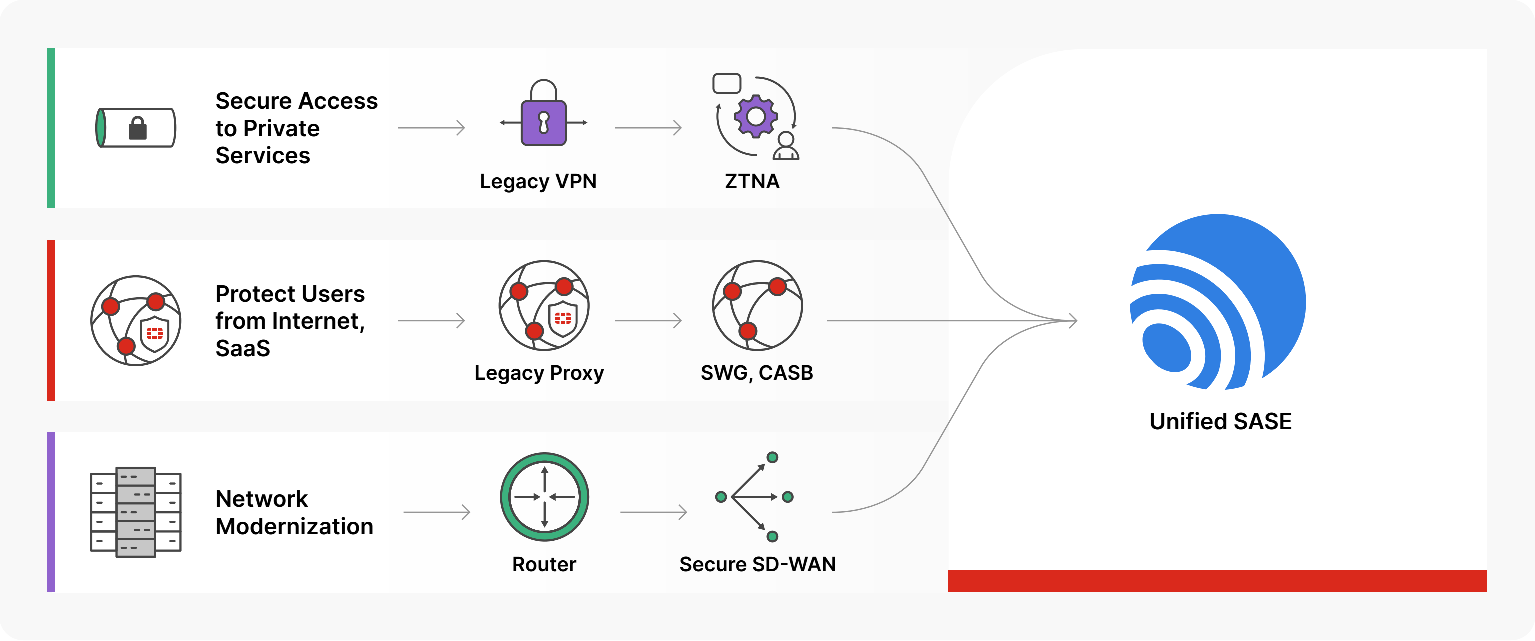


Figure 3: Key enterprise initiatives and use cases for SASE adoption

Key Requirements and Questions to Ask Your SASE Vendor to Support Your SASE Use Cases

1 Secure Remote Access to Corporate Applications and VPN Replacement

Zero trust does not grant implicit trust to user accounts or assets based solely on their network or physical locations. Applying a zero-trust security model to secure application access allows organizations to move away from a traditional VPN tunnel that provides unrestricted remote access.

However, an effective ZTNA solution must grant access to individual applications per session based on user identity and provide continuous near-real-time device posture verification. Your ZTNA solution must also support the following core requirements:

- Explicit and granular access control per application based on user identity and continuous near-real-time device posture validation and monitoring
- Noncompliant devices and sessions blocked in near real time
- Endpoint security and vulnerability management as a part of a unified agent to simplify deployment and management
- Security inspection for application traffic and blocking malicious traffic
- All common enterprise device types, including Windows, Mac, and Chromebooks
- Support for secure access to all your corporate applications
- Universal enforcement of ZTNA policies, even when users are on the corporate network

You want to provide the same zero-trust model no matter the user's location. This extends ZTNA beyond remote access to anywhere in the organization.

Questions to ask a SASE vendor regarding secure private access and a ZTNA use case:

- How often does your ZTNA solution continuously check for device posture? It is vital that your ZTNA solution checks for device posture in near realtime rather than every 10–15 minutes to avoid the risk of exposure from compromised or malicious users or devices.

- How does your ZTNA solution handle a user's session that fails device posture checks while the user is accessing a corporate application? Does the ZTNA solution block user sessions in real time if they fail the device posture checks and are no longer compliant?
- Does your ZTNA client include endpoint protection and vulnerability management? Do you need to install multiple agents for these capabilities, or are they supported via a unified agent?
- Does the ZTNA solution provide inline security inspection for authenticated user sessions to block malware propagation?
- What application protocols are supported by the ZTNA solution?

2 Secure Internet Access

For remote users or branch locations outside the protection of the corporate perimeter, direct internet access expands the attack surface and increases related risks. To address this, the SASE solution must include enterprise-grade FWaaS with IPS and web filtering, SWG, and deep SSL inspection capabilities. It should also include advanced threat protection, including inline antivirus and sandbox capabilities, as a part of its SSE cloud-delivered service to provide consistent, secure internet access from any location.

FWaaS with IPS and web filtering

The FWaaS must support next-gen firewall (NGFW) capabilities delivered from the cloud as a service. It must secure all connections and analyze inbound and outbound traffic without impacting user experience. FWaaS should support L7 application visibility and control, web filtering, SSL inspection, DNS security, intrusion prevention system (IPS), and advanced threat protection (ATP).

SWG with high-performance SSL inspection

The SWG should protect internet users and devices from the most advanced web threats. It should include a broad set of capabilities for securing web traffic, including SSL-encrypted web traffic, without significant performance degradation.

SWG should support deep security inspection capabilities, including web filtering, antivirus, and file filtering, for managed and unmanaged devices using agent or agentless mode. Its web filtering capability must support predefined common web categories for URLs and web content to block access to malware, phishing sites, and inappropriate content.

ATP with inline antivirus and real-time sandboxing

The antivirus engine should detect and prevent known and previously unknown virus variants. Inline antivirus should include automated updates that protect against the latest viruses, spyware, and other content-level threats.

Sandboxing must offer high-performance security solutions utilizing artificial intelligence (AI) and machine learning (ML) technology to identify and isolate advanced threats in real time. It should also inspect files, websites, URLs, and network traffic for malicious activity, including zero-day threats, and use sandboxing technology to analyze suspicious files in a secure virtual environment.

AI-powered security services

Your solution should also include AI-powered security services for FWaaS, web filtering, DNS security, antivirus, anti-malware, sandbox, and IPS to ensure comprehensive and up-to-date protection from the latest known and zero-day threats. It is important to validate the efficacy of SWG and FWaaS components, including IPS, based on leading industry security certifications.

Questions to ask a SASE vendor for a secure internet access use case:

- Does your solution support deep SSL inspection for encrypted web traffic? Is there a significant performance impact when you turn SSL inspection on?
- Is the security efficacy of your solution certified for capabilities such as FWaaS, IPS, antivirus, anti-malware, and web filtering?
- Is your solution based on OEMs for its core technology components, such as SWG or FWaaS?
- Do you have internal threat research expertise? Or do you solely rely on third-party OEMs for threat intelligence?
- Do you offer AI-powered security intelligence to detect and respond to zero-day threats?
- Do you offer inline antivirus and sandboxing support to deliver advanced threat protection from known and previously unknown threats?

3 Secure SaaS Access

Given the rapid increase in SaaS adoption, organizations struggle with shadow IT and stopping data exfiltration. SSE must include the following core capabilities to provide secure SaaS access for users:

Next-generation dual-mode CASB

Next-generation dual-mode CASB, using both inline and out-of-band support, should provide comprehensive visibility by identifying key SaaS applications and reporting risky unsanctioned applications to overcome shadow IT challenges. Next-gen CASB should also offer granular control of applications to secure sensitive data and detect and remediate malware in applications across both managed and unmanaged devices.

Data protection and enhanced DLP support

A SASE solution must support a highly customizable suite of data protection capabilities that help safeguard from data-related breaches and compromises by providing a granular data protection policy engine. It should offer a broad set of DLP signatures, a customizable pattern and policy engine, and an advanced and accurate DLP content analysis engine to help achieve the best possible data security posture. It should also provide a rich set of predefined reports on DLP activities and compliance standards, such as SOX, GDPR, PCI, HIPAA, NIST, and ISO 27001.

Questions to ask a SASE vendor for secure SaaS access use case:

- Does your solution support both inline and API-based CASB?
- Does your solution support visibility into all SaaS applications—sanctioned and un-sanctioned—to address shadow IT?
- Does your solution support predefined reports for compliance standards, including SOX, GDPR, PCI, HIPAA, and NIST?
- Does your solution offer DLP capabilities for SaaS applications?
- Does your DLP solution support advanced data matching techniques to prevent accidental data breaches?

4 Secure SD-WAN for Branch Connectivity

Many SASE solutions only provide SSE capabilities or deliver lightweight SD-WAN capabilities to forward branch traffic to their SSE cloud. This leaves a gap in providing fast and secure access from branch locations.

The best SD-WAN solutions offer converged networking and security managed by one centralized management system, allowing sites to be brought on quickly without requiring networking or security experts to be on-site for installation. An effective and scalable SASE solution must offer secure SD-WAN devices at branch locations that consolidate core WAN edge networking and branch security capabilities to provide fast and secure access to the internet, SaaS, and private applications from branch locations.

Secure SD-WAN should support the following core capabilities:

- **Transport independence:** Secure SD-WAN supports multiple kinds of uplinks, including internet, MPLS, 4G, LTE, and 5G.
- **Path control:** The SD-WAN must be able to utilize active paths for bandwidth efficiency, failover, and resiliency.
- **Security:** SD-WAN must ensure security across each branch location, including an integrated, NGFW that offers antivirus, anti-malware, data loss prevention, IPS, IDS, sandboxing, and URL and content filtering.
- **Application optimization:** The SD-WAN solution must optimize applications, including video and voice traffic and SaaS applications. Also, it must be intelligently able to identify thousands of applications and steer them dynamically on the appropriate link.
- **Encryption:** SD-WAN must support the creation of an end-to-end encrypted tunnel over the broadband between headquarters and branch locations. Companies must use SD-WAN to encrypt WAN traffic and ensure it encrypts it effectively.
- **Zero-touch provisioning:** The solution must optimize branch SD-WAN device onboarding.
- **Automation and orchestration:** All functions must be supported by a centralized, single-pane-of-glass management system.

Questions to ask the SASE solution vendor regarding Secure SD-WAN support:

- How many application signatures does your SD-WAN solution support for application traffic steering?
- What application optimization capabilities are supported by your SD-WAN solution?
- What security capabilities are included in your SD-WAN to inspect and block malicious traffic from propagating to your corporate network?
- Is your SD-WAN capability validated with industry certifications, such as MEF?
- Does your SD-WAN solution optimize connections when links are impaired? Can it remediate connections using FEC and packet duplication techniques?

5 Securing Thin Edges with Cloud-Based SSE

A SASE solution should provide flexible connectivity to locations and endpoints beyond remote user devices and branch sites. Cloud-delivered SSE capabilities are a cost-effective choice to secure thin edges to secure LAN, wireless LAN, and OT environments that may not be able to deploy a full NGFW on-premises or install clients on the endpoints.

Many enterprises deploy wireless APs to provide connectivity at remote locations (such as retail stores). These APs require the same level of security as larger branch sites to secure communications with the internet, SaaS, and private applications from within the thin edge. A SASE solution that can offer cloud-delivered SSE capabilities by integrating directly with wireless APs without deploying an NGFW or client at each endpoint provides enterprise-class security and reduces complexity and costs. In addition, the SASE solution can extend zero-touch provisioning beyond branch SD-WAN devices and offer similar capabilities for wireless APs at thin edges.

Questions to ask the SASE vendor about support for wireless LAN and thin edge:

- Does your SASE solution provide direct secure connectivity to an SSE POP from wireless APs in the thin edge?
- Does your SASE solution offer SSE capabilities to secure access to the internet, SaaS, and private applications from wireless APs at the thin edge?
- Does your SASE solution provide cloud-based onboarding for wireless APs connecting from the thin edge?

6 Geographic SASE POP Coverage and Latency

Organizations need to identify where their users are working from and where the applications they access are located. This helps ensure they pick a SASE vendor that can provide low latency and points of presence (POPs) closer to where users are located.

In addition, not all SASE vendors provide the full stack of SSE security capability at each POP. It is important to understand:

- What capabilities are provided in each SASE POP
- Any mechanisms the SASE vendor has in the POP to optimally steer traffic through their cloud network
- The SLA offered by the vendor for SSE inspection, rather than just going with the total number of POPs claimed by the vendor

Questions to ask the SASE vendor related to geographic POP coverage and latency:

- Can I see a complete list of your SASE POPs?
- Do you provide a full stack of SSE capabilities at each POP?
- What SLA do you offer for latency at each SSE POP for security inspection?
- Does your SASE POP include intelligent application steering based on SD-WAN to provide fast, low-latency path selection to applications?
- What is the disaster recovery mechanism for POPs?
- Is data between multiple customers segregated in a POP?

7 Unified SASE

There are many approaches to SASE in the market, with varying levels of functionality and integration required for SASE deployments. Enterprises must be aware of the differences to identify the right SASE solution for their needs.

Dual-vendor SASE

Dual-vendor SASE solutions are typically based on SD-WAN and SSE functionality (ZTNA, SWG, FWaaS, CASB, DLP) from two different vendors. The enterprise networking team normally leads the selection of SD-WAN technology, while the enterprise security team typically leads the selection of the SSE functionality. While dual-vendor SASE provides the flexibility to choose different vendors for networking and security as a service, it leads to increased complexity and costs. It is not simple to deploy or operate.

Single-vendor SASE

Single-vendor SASE solutions offer SD-WAN and SSE capabilities, including SWG, CASB, network firewalling, and ZTNA. Such offerings use a cloud-centric architecture and are delivered by a single vendor through a common management console. Single-vendor SASE solutions are simpler to manage, more cost-effective, and easier to deploy than dual-vendor SASE solutions that attempt to combine SD-WAN and SSE capabilities from two different vendors.

Unified SASE

Not all single-vendor SASE solutions are based on a common platform or operating system (OS), as some vendors have chosen to offer single-vendor SASE based on integrating multiple products or using third-party OEM technologies for several of their SASE components. They also often require numerous deploying client agents, which adds to complexity and costs.

Questions to ask the SASE vendor about their SASE approach and deployment:

- Do you provide a single-vendor SASE solution with enterprise-class SD-WAN and SSE cloud-delivered security?
- Do you offer centralized management of your SSE capabilities from a common console?
- Is your SASE solution based on integrating multiple products with different operating systems, or is it based on a common OS platform?
- Is your SASE solution flexible enough to integrate with your existing on-premises network security infrastructure and provide consistent policy enforcement across on-premises and SSE?

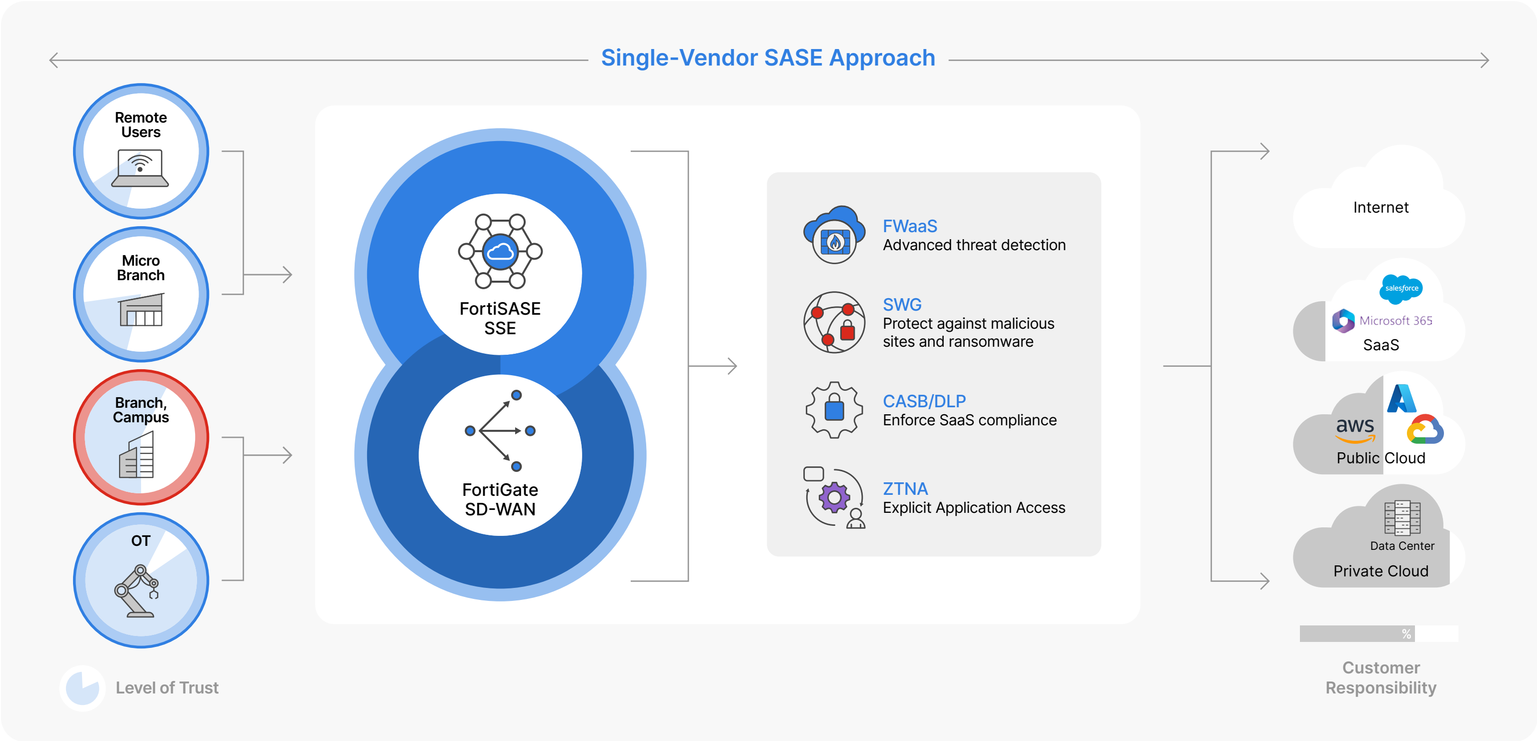


Figure 4: Unified SASE

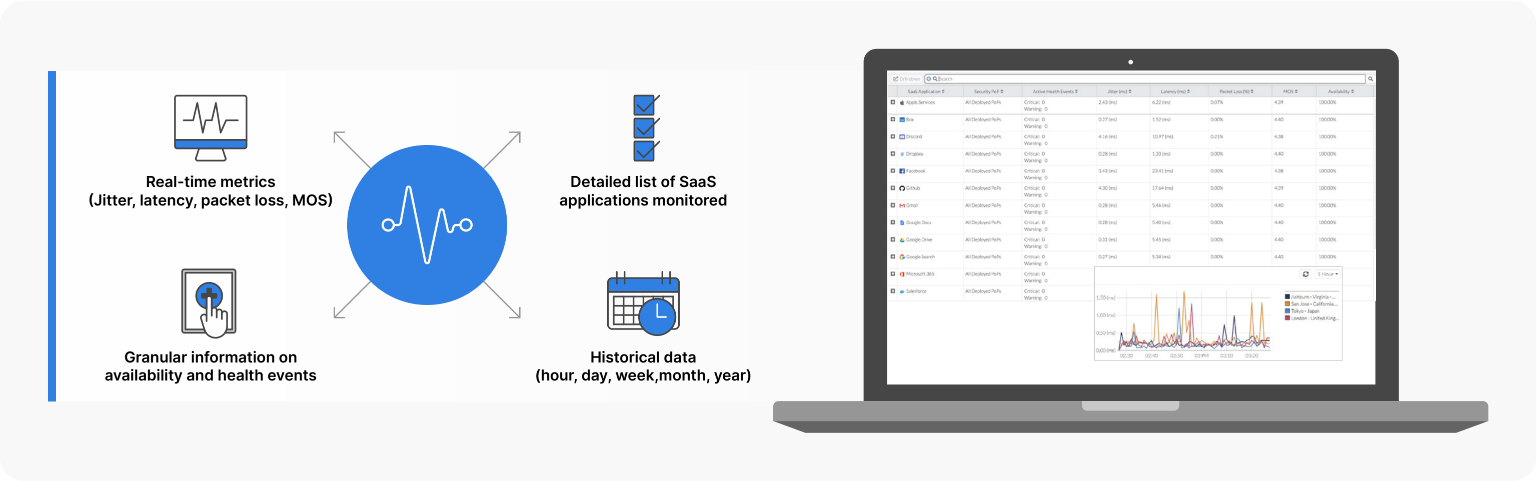
8 End-to-End Digital Experience Monitoring

SASE solutions must support digital experience monitoring (DEM) to provide end-to-end visibility. This provides IT teams with the data they need to decrease resolution times and ensure and maintain an optimal user experience.

DEM should offer insights across users and global SASE POPs and provide comprehensive visibility into the performance of common SaaS applications based on typical metrics, such as latency, jitter, packet loss, and mean opinion scores. DEM should also provide end-to-end monitoring of performance metrics, from user to common SaaS applications, and performance from each SASE POP to the SaaS applications to help troubleshoot issues and reduce mean time to resolution.

Questions to ask the SASE vendor about DEM:

- Does your SASE solution offer DEM?
- What SaaS applications and performance metrics are supported by your DEM capability?
- Does your DEM capability provide insight into performance from users?



	SaaS Application	Security PoP	Active Health Events	Jitter (ms)	Latency (ms)	Packet Loss (%)	MOS	Availability
⊞	Apple.Services	All Deployed PoPs	Critical: 0 Warning: 0	2.43 (ms)	6.22 (ms)	0.07%	4.39	100.00%
⊞	Box	All Deployed PoPs	Critical: 0 Warning: 0	0.27 (ms)	1.52 (ms)	0.00%	4.40	100.00%
⊞	Discord	All Deployed PoPs	Critical: 0 Warning: 0	4.16 (ms)	10.97 (ms)	0.21%	4.38	100.00%
⊞	Dropbox	All Deployed PoPs	Critical: 0 Warning: 0	0.28 (ms)	1.33 (ms)	0.00%	4.40	100.00%
⊞	Facebook	All Deployed PoPs	Critical: 0 Warning: 0	3.43 (ms)	23.41 (ms)	0.00%	4.38	100.00%
⊞	Github	All Deployed PoPs	Critical: 0 Warning: 0	4.30 (ms)	17.64 (ms)	0.00%	4.39	100.00%
⊞	Gmail	All Deployed PoPs	Critical: 0 Warning: 0	0.28 (ms)	5.46 (ms)	0.00%	4.40	100.00%
⊞	Google.Docs	All Deployed PoPs	Critical: 0 Warning: 0	0.28 (ms)	5.40 (ms)	0.00%	4.40	100.00%
⊞	Google.Drive	All Deployed PoPs	Critical: 0 Warning: 0	0.31 (ms)	5.45 (ms)	0.00%	4.40	100.00%
⊞	Google.Search	All Deployed PoPs	Critical: 0 Warning: 0	0.27 (ms)	5.34 (ms)	0.00%	4.40	100.00%
⊞	Microsoft.365	All Deployed PoPs	Critical: 0 Warning: 0					
⊞	Salesforce	All Deployed PoPs	Critical: 0 Warning: 0					

Figure 5: Digital Experience Monitoring Report for SaaS applications

9 AI-Powered Security and SOC-as-a-Service

Enterprises need a SASE solution that delivers high-security efficacy to combat modern zero-day threats and support 24×7 monitoring of security threats. However, many SASE solutions are limited to threat prevention and detection of known threats based on signature-based IPS. They require additional investment in in-house security, SOC staff, and technology to maintain ongoing security monitoring.

AI-powered security enables prevention, detection, and automated response to zero-day threats. However, not all SASE vendors have the breadth of deployments nor the ability to gather the large volumes of security data needed to effectively support AI and ML for detecting zero-day threats. Enterprises should look for SASE solutions that can gather a sufficiently large breadth and volume of telemetry data to support the AI-powered functions augmenting essential SSE capabilities, such as a SWG, FWaaS, ZTNA, CASB, and DLP, to maintain protection from a wide range of security threats.

In addition, SASE solutions should integrate with existing systems to minimize investments in SOC technology and personnel to monitor and respond to security threats in near real time.

Questions to ask the SASE vendor about AI-powered security and SOC-as-a-Service:

- What is the scope and volume of your datasets used for AI and ML?
- How much data do you collect from endpoints, networks, and applications, and how often do you collect that data?
- What SLAs do you offer as a part of your SOC-as-a-Service? How quickly can you notify the enterprise in case of a security event?
- How does your solution protect your organization from users who input sensitive data into ChatGPT?

10 Unified Client Agent

Many SASE solutions require additional third-party clients for endpoint protection, vulnerability management, DEM, ZTNA, and SSE connectivity. This increases deployment and operational complexity as well as the TCO.

Unified SASE solutions consolidate security capabilities in the cloud and at the endpoints to reduce complexity and costs.

Questions to ask the SASE vendor about unified client support:

- Does your SASE client support vulnerability management and endpoint protection, or do you rely on third-party endpoint security vendors?
- Does your SASE client include DEM support, or do you rely on a separate third-party client?
- What client capabilities are included in your SASE license?

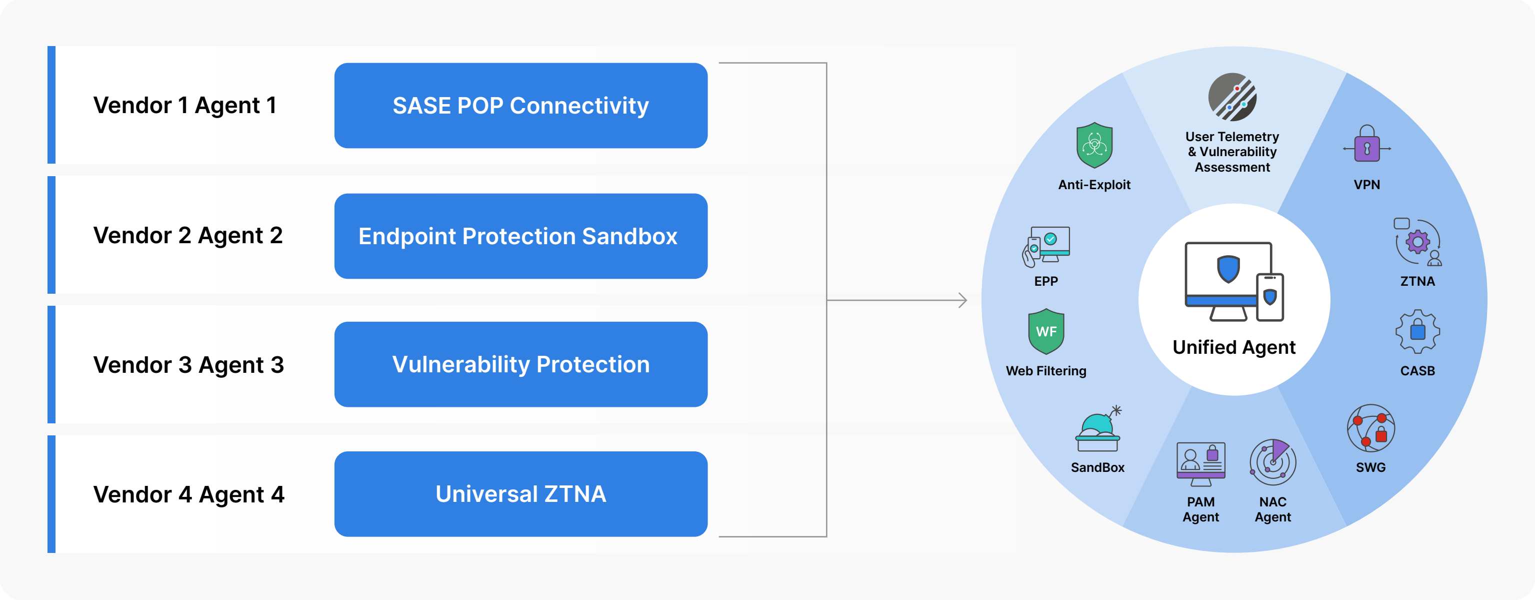


Figure 6: Unified client agent

Conclusion

There are numerous SASE vendors in the market. A robust SASE solution requires multiple products to provide full functionality. Unless these components are designed to operate as a single system, they can be complex and costly to integrate and operate. This negates the benefits of converged networking and security that SASE promises.

SASE is a journey and not a transformation in a single step. You should evaluate your business needs and use cases to identify a SASE vendor that aligns with your requirements. In most cases, that means looking for a unified single-vendor SASE solution that offers the breadth of capabilities needed to address your current and future needs. You won't regret partnering with a SASE vendor that gives you flexibility, meets you where you are on your SASE implementation, and supports you throughout the journey.

In the realm of SASE solutions, quick and reliable technical support, including faster response times, is crucial. Prioritizing providers who offer prompt assistance ensures minimal downtime and uninterrupted operations. Look for a dedicated vendor with deep expertise in swiftly resolving issues, providing peace of mind, and keeping your business running smoothly.

www.fortinet.com

July 31, 2024 12:54 PM

2613421-A-0-EN