FORTINET

Unified SASE Buyer's Guide

The Criteria for Selecting the Best Unified SASE Solution for Your Hybrid Workforce

What Is Unified SASE?

Unified SASE (secure access service edge) is a cloud-delivered architecture that converges networking and security into a single, integrated platform. It combines capabilities such as SD-WAN, secure web gateway (SWG), cloud access security broker (CASB), Firewall-as-a-Service (FWaaS), and zero-trust network access (ZTNA) under one unified framework. This approach enables consistent policy enforcement, centralized management, and seamless user experiences across branch offices, remote users, and cloud environments.

Unified SASE is needed because traditional, fragmented security and networking tools cannot keep up with today's hybrid workforce, distributed applications, and evolving threat landscape. Organizations face increased complexity, higher operational costs, and inconsistent security when relying on multiple point solutions. By unifying these functions, SASE reduces complexity, improves visibility, lowers total cost of ownership, and delivers scalable, high-performance connectivity with built-in security. This ensures users can securely access applications from anywhere without compromising performance or protection.

Key Considerations

Choose a truly unified platform

Converged SD-WAN and secure service edge (SSE) delivered on a single operating system and management plane reduces operational complexity, simplifies licensing, and significantly lowers total cost of ownership (TCO). A unified architecture ensures consistent policy enforcement everywhere while eliminating the cost and overhead of managing multi-point solutions.

Universal ZTNA must be built in

Modern SASE must deliver consistent zero-trust access across all users, devices, locations, and application types, whether SaaS, private applications, or internet resources, ensuring secure access with the same policies everywhere while replacing legacy VPN approaches.

AI must be built in and not bolted on

SASE must leverage AI to detect and stop advanced threats while also governing generative AI (GenAI) usage. This includes preventing data leakage, controlling shadow AI, and protecting organizations from misuse of AI-powered tools.

Performance and inspection at scale are essential

High-performance SASE architectures should deliver low latency, high throughput, and full security inspection at scale. Integrated SD-WAN ensures optimal traffic routing while maintaining consistent protection without performance trade-offs.

Operational efficiency is critical

AI-assisted operations, unified agents, and centralized visibility streamline management, reduce administrative overhead, and accelerate threat detection and response across distributed environments.

Global consistency and sovereignty are essential

Organizations need strong global points of presence (POP) coverage, consistent services everywhere, flexible data sovereignty options, and licensing models that scale easily as the business grows.

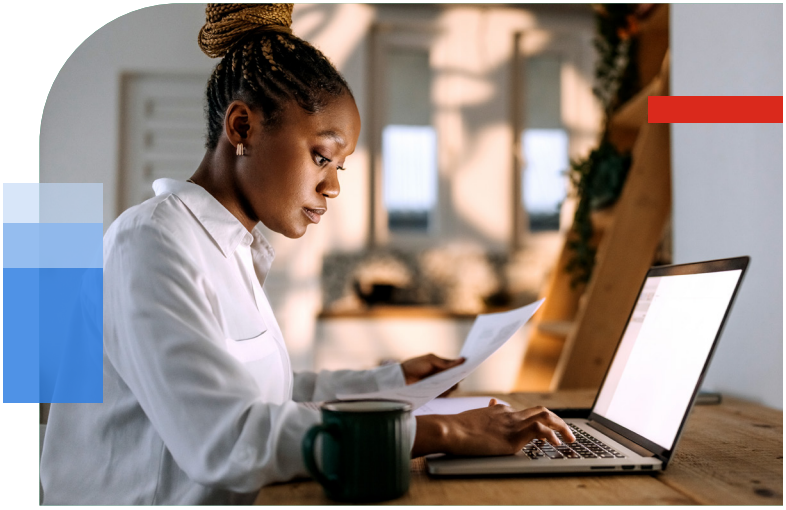
SASE Challenges

Hybrid workforce security requires a unified approach

The rise of hybrid work has fundamentally reshaped enterprise connectivity. Employees now access applications and data from corporate campuses, branch offices, home networks, and mobile devices—dramatically expanding the attack surface. This hybrid workforce model introduces inconsistent policy enforcement, reduced visibility, increased exposure to compromised devices, and growing operational complexity across networking and security teams.

Traditional VPN-based remote access is no longer sufficient for modern hybrid environments. VPNs typically grant broad network-level access rather than application-specific access, increasing the blast radius if credentials are stolen. Once connected, users often have implicit trust within the network, enabling lateral movement during a breach. VPNs also lack continuous posture verification and inline inspection, allowing compromised endpoints or hijacked sessions to introduce significant risk. In addition, centralized VPN gateways create latency and performance bottlenecks for remote users accessing Software-as-a-Service (SaaS) and cloud applications.

Also, cloud-only SSE solutions attempt to modernize access but introduce new challenges. Many rely on centralized inspection points, forcing traffic hair-pinning and increasing latency for on-net users and branch locations. They often operate separately from SD-WAN, resulting in fragmented policy management, inconsistent enforcement, and limited visibility across distributed environments. Without integrated networking and security, organizations are left stitching together multiple tools to secure hybrid access.



Modern hybrid work requires a unified approach that combines zero trust, integrated SD-WAN, consistent inline inspection, and centralized management to deliver secure, high-performance access—everywhere users connect.

Distributed applications and SaaS are expanding risk

Users are increasingly accessing SaaS and other distributed cloud applications from anywhere, accelerating productivity but also expanding organizational risk. At the same time, the rise of unauthorized applications, commonly referred to as shadow IT, reduces visibility and weakens control over sensitive data. Security teams must understand which SaaS and GenAI applications are in use, who is accessing them, and how data is being shared or stored.

Modern SASE platforms must go beyond basic visibility to provide comprehensive SaaS security posture management (SSPM) capabilities. SSPM continuously assesses SaaS configurations, permissions, and security settings to identify misconfigurations, excessive privileges, compliance gaps, and risky third-party integrations. By combining dual-mode CASB controls with SSPM visibility, organizations can enforce granular data protection policies, monitor user behavior, prevent sensitive data exposure, and maintain compliance across sanctioned and unsanctioned SaaS environments.

As SaaS ecosystems grow more complex and interconnected, integrating CASB, DLP, and SSPM into a unified SASE architecture ensures consistent enforcement, continuous posture monitoring, and centralized management. This reduces risk while enabling secure, distributed application access at scale.

The rapid proliferation of new network edges creates many new risks

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 hybrid work users, often implemented as independent projects, have created vulnerabilities that cybercriminals eagerly exploit.

How SASE Addresses Modern Access Challenges

A SASE architecture addresses the complexities of securing hybrid and remote users by delivering both high-performance connectivity and consistent security regardless of location. Whether users are in large branches, small offices, home environments, or mobile, SASE ensures secure, optimized access to applications and data.

SASE converges secure SD-WAN with cloud-delivered SSE capabilities to provide fast, secure access to internet, SaaS, private, and GenAI applications from anywhere. By integrating networking and security, organizations eliminate backhauling, reduce latency, and maintain consistent policy enforcement across distributed environments.

SSE services include ZTNA, FWaaS, SWG, CASB, data loss prevention (DLP), SaaS SSPM, and built-in GenAI security. They are all delivered as cloud services and enforce identity-based and posture-based access controls.

Integrated GenAI governance provides visibility into sanctioned and unsanctioned AI usage, prevents sensitive data leakage into AI prompts, and detects AI-driven threats such as automated phishing and exploit generation. Continuous verification, real-time contextual analysis, and compliance-driven policies ensure granular inline protection across users, devices, and applications.

Unified SASE extends beyond security enforcement by incorporating end-to-end digital experience monitoring (DEM), delivering visibility from the endpoint to the application and SASE POP. This enables rapid root cause identification, improved user experience, and faster mean time to resolution.

Operational efficiency is further enhanced through GenAI assistants, which embeds generative AI directly into the management experience. They accelerate policy creation, automate troubleshooting across network and security domains, and speed root cause analysis through correlated telemetry, reducing operational overhead and enabling teams to scale securely.

Built on a common operating system, unified policy engine, and centralized management plane, Unified SASE supports flexible deployment across secure SD-WAN branches, thin edges (such as wireless access points), client-based and agentless devices (including Chromebooks), and hybrid cloud environments—all governed by a single policy framework.

The result is a simplified, AI-ready security architecture that lowers TCO, preserves existing infrastructure investments, and delivers consistent, high-performance protection and visibility everywhere users connect.

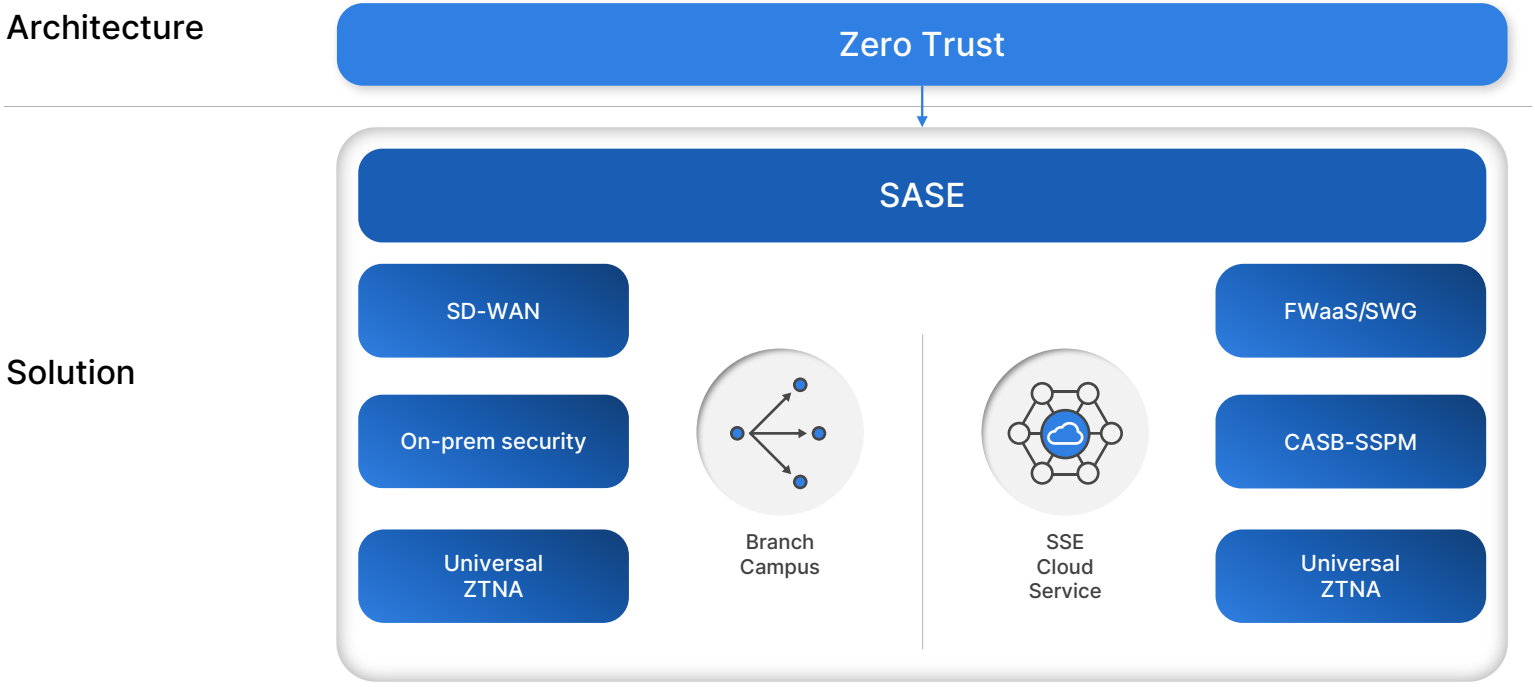


Figure 1: The SASE framework enables secure access.

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:

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

Choosing the Right SASE Solution

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 for an enterprise SASE solution

Many SASE solutions only solve part of the problem. They either fail to provide consistent enterprise-grade cybersecurity to their hybrid workforce 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.

Furthermore, not all SASE solutions are equal regarding scalability, security, data sovereignty, 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.

Secure Hybrid Access

Consistent zero trust everywhere
GenAI aware visibility and control
Consistent policies

Converged Networking and Security

Eliminate tool sprawl
Flexible deployment
Lower TCO

Sovereign and Compliant Access

Meet regulatory requirements
Local data enforcement
Broad sovereignty options

Figure 2: Key use cases for SASE adoption

FORTINET

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

Secure Remote Access to Corporate Applications and VPN Replacement

Zero-trust access 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 real-time 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?

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.

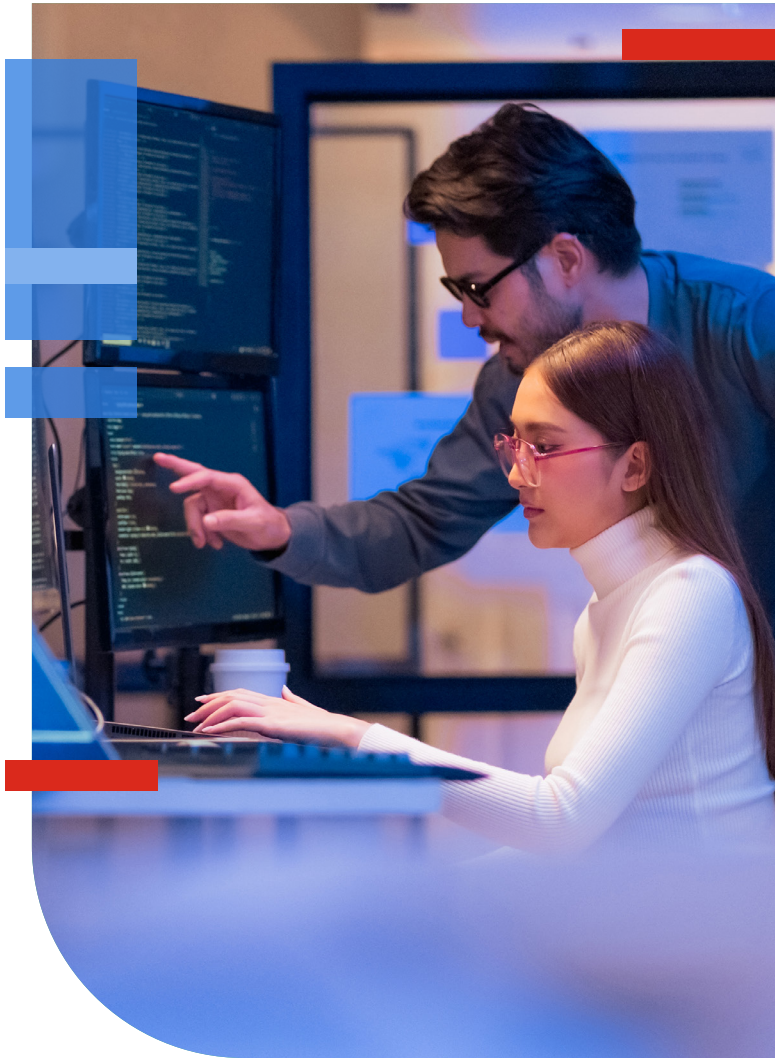
AI-powered security services

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?



Secure SaaS Access

With the rapid adoption of SaaS applications, organizations face increasing challenges from shadow IT, misconfigured applications, and data exfiltration. A modern SASE platform must include advanced SSE capabilities to secure SaaS access while providing visibility, control, and compliance.

Next-generation dual-mode CASB

Dual-mode CASB, combining inline and API-based (out-of-band) enforcement, provides comprehensive visibility into sanctioned and unsanctioned SaaS applications. It detects shadow IT usage, reports risky or unauthorized applications, and enforces granular access policies to protect sensitive data. CASB also monitors for malware, enforces DLP policies, and applies controls across both managed and unmanaged devices, ensuring consistent security across the hybrid workforce.

SaaS SSPM

SSPM continuously assesses SaaS configurations, permissions, and risk exposure, identifying misconfigurations, excessive privileges, and compliance gaps. By integrating SSPM with CASB and DLP, organizations gain unified visibility into application posture, ensure data protection, and remediate risks in real time, providing stronger governance over both sanctioned and unsanctioned SaaS applications.

Data protection and enhanced DLP support

A robust SASE solution must include an advanced, highly customizable data protection suite. This includes broad DLP signatures, EDM, a flexible pattern and policy engine, and precise content analysis to prevent data breaches. Predefined reporting and compliance dashboards simplify adherence to standards such as SOX, GDPR, PCI, HIPAA, NIST, and ISO 27001, enabling organizations to maintain a strong data security posture while securing SaaS usage at scale.

GenAI access security

With growing AI-driven workflows within SaaS applications, built-in GenAI governance ensures sensitive data is protected when interacting with AI models, prevents unauthorized AI usage, and provides visibility and control over AI-assisted actions across SaaS platforms.

By combining CASB, SSPM, DLP, and GenAI security in a unified SASE framework, organizations gain comprehensive SaaS protection, visibility, and compliance while reducing operational complexity and risk.

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 SSPM capabilities?
- 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?

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? Will performance be impacted when inspecting encrypted traffic?
- Is your SD-WAN capability validated with industry certifications, such as Mplify?
- Does your SD-WAN solution optimize connections when links are impaired? Can it remediate connections using FEC and packet duplication techniques?

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, a 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?
- What management visibility exists for WLAN users in SASE dashboards?

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 select a SASE vendor that can provide low latency and 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?
- How does the SASE vendor show past outage details and information?

A Variety of SASE Approaches

The market offers a variety of SASE approaches, each with differing levels of integration, functionality, and operational complexity. Understanding these differences is critical for selecting a solution that aligns with an organization's security, networking, and operational needs.

Dual-vendor SASE

Dual-vendor SASE solutions combine SD-WAN and SSE capabilities (ZTNA, SWG, FWaaS, CASB, DLP) from separate vendors. Typically, networking teams select the

SD-WAN solution while security teams choose the SSE component. While this approach offers flexibility to mix and match technologies, it increases deployment complexity, operational overhead, licensing costs, and integration challenges. Enterprises must manage multiple consoles, policy engines, and agents, making consistent enforcement and troubleshooting more difficult.

Single-vendor SASE

Single-vendor SASE platforms consolidate SD-WAN and SSE capabilities, such as SWG, CASB, ZTNA, FWaaS, and DLP, under one vendor with a common management console. Cloud-centric by design, these solutions simplify deployment, reduce cost, and provide easier management than dual-vendor approaches. However, not all single-vendor solutions are built on a unified platform; some rely on stitching together acquired products or third-party OEM technologies, which can introduce complexity, require multiple agents, and limit operational efficiency.

Unified SASE

True unified SASE goes beyond single-vendor consolidation by integrating all networking and security components on a common operating system, policy engine, and management plane. Unified SASE delivers seamless, high-performance connectivity with SD-WAN, ZTNA, FWaaS, SWG, CASB, DLP, SSPM, on-net and off-net detection, and built-in GenAI security—all governed by a single policy framework. End-to-end DEM provides full visibility from endpoint to application, while GenAI assistance embeds AI-driven automation for policy creation, and root cause analysis, reducing operational overhead.

Unified SASE eliminates the need for multiple agents, separate consoles, or fragmented inspection points, providing consistent zero-trust enforcement, simplified management, and lower TCO. It enables organizations to secure hybrid and cloud-first environments, including AI-enabled workflows, while maintaining flexibility, performance, and compliance at scale.

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

- Do you provide a unified 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?

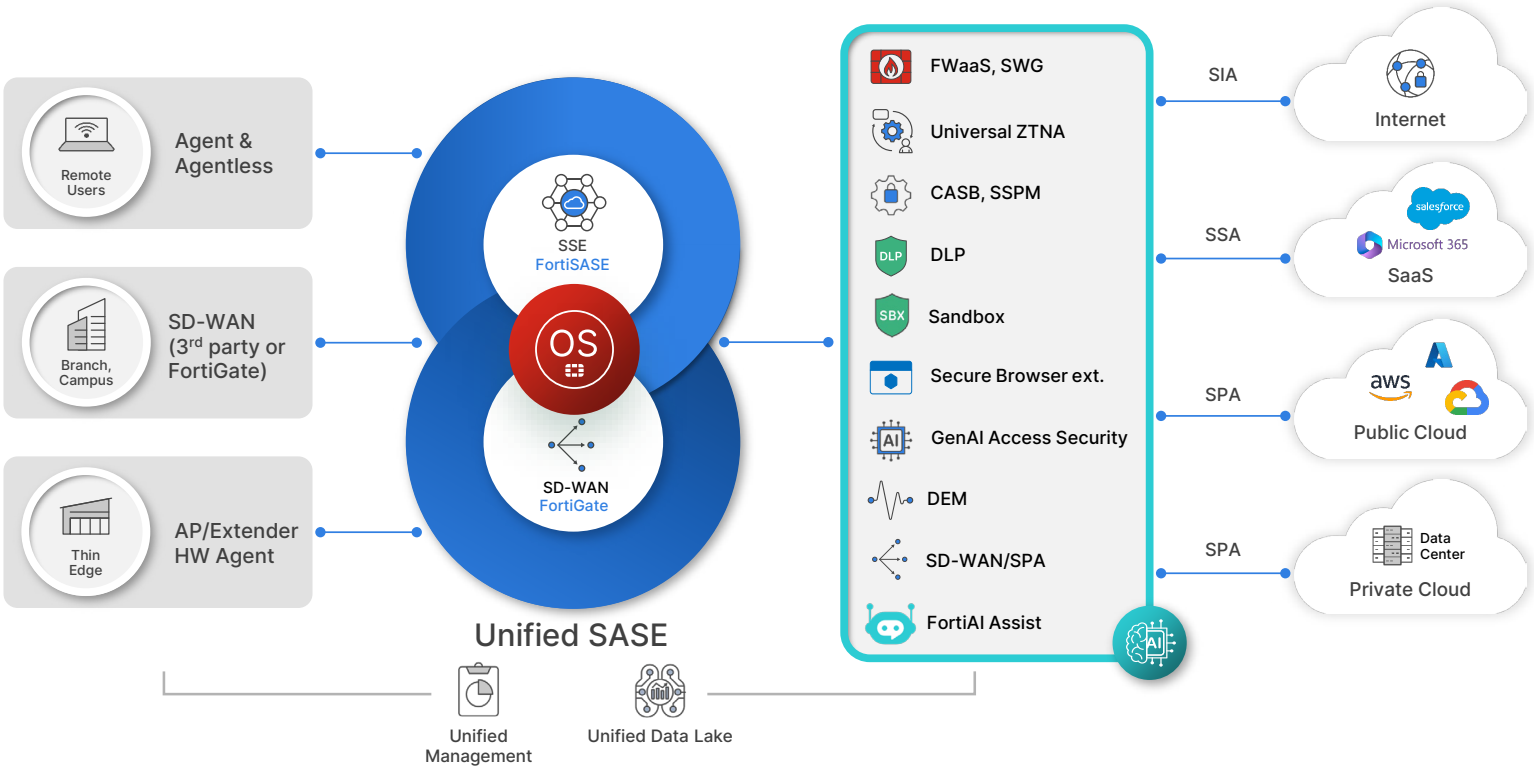


Figure 3: Example of a unified SASE solution design

End-to-End DEM

SASE solutions must support 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 and the user's LAN network?
- How far back can DEM analyze historical experience data?
- Is DEM available as part of the same SASE agent or is a separate agent required?
- Does DEM work across branch, remote users, and mobile devices?

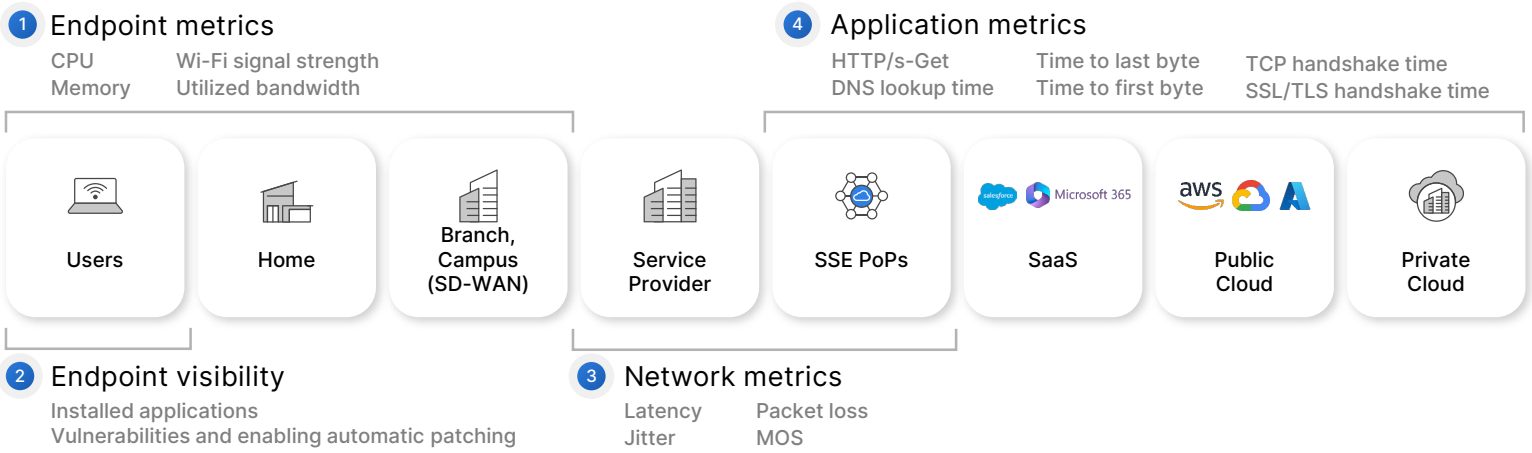


Figure 4: How end-to-end DEM works as part of a SASE solution.

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 be integrated 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 GenAI applications?

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?

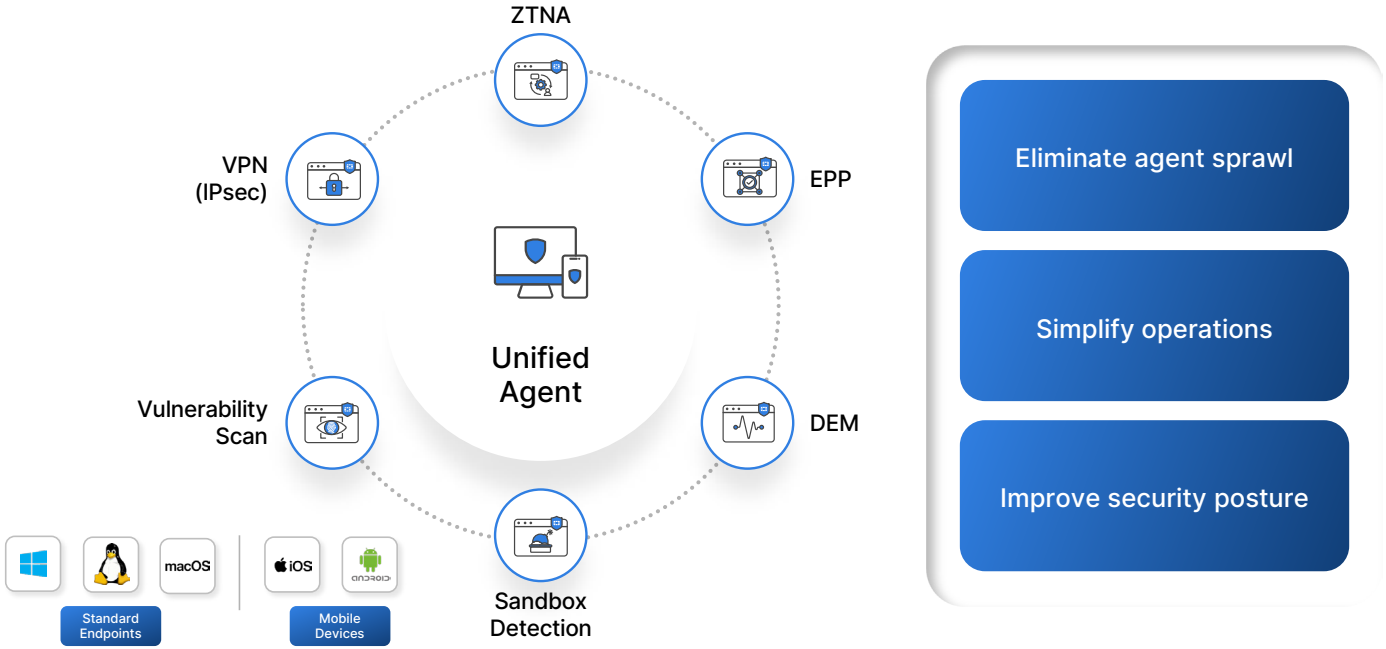


Figure 5: A unified client agent eliminates sprawl, simplifies operations, and improves security.

GenAI Agent and Assistant

Some SASE solutions include an AI-powered operational engine embedded directly into the unified SASE solution, designed to accelerate security and networking management. It translates natural language into security and access policies, automates troubleshooting across network and security domains, and summarizes alerts and incidents with contextual risk insights. By correlating telemetry from endpoints, networks, and applications, it speeds root cause analysis, reduces manual investigation, and lowers operational overhead, enabling lean IT teams to operate at scale while maintaining consistent, high-performance protection.

Questions to ask the SASE vendor about GenAI assistance:

- What telemetry sources and data feed its AI-driven insights?
- How quickly can it help your team identify and resolve security incidents?
- How does it reduce operational overhead while maintaining consistent protection?

Deployment Flexibility

Enterprises rarely modernize networking and security everywhere at once. A SASE platform should support multiple deployment models (cloud-delivered, on-premises, virtual, and hybrid) so organizations can adopt new capabilities at their own pace while maintaining consistent policy, visibility, and user experience. Deployment flexibility should also extend to how enforcement is delivered (branch, thin edge, endpoint agent, and cloud) and how solutions coexist during migration to avoid forced rip-and-replace projects.

Questions to ask the SASE vendor about deployment flexibility:

- What deployment models do you support (cloud-delivered, on-premises appliances, virtual/VM, and hybrid), and are feature sets consistent across them?
- Can we apply and audit a single policy framework across on-net and off-net users, branches, cloud workloads, and thin edges?
- What form factors are available for branch and data center (hardware, virtual, cloud marketplace images), and how do you scale performance?
- How do you support phased migration and coexistence with existing firewalls, SD-WAN, proxies, and identity providers without disrupting users?

Data Sovereignty and Flexibility in Sovereignty Deployment Levels

Data sovereignty is a critical consideration in modern SASE deployments, as organizations must comply with regional regulations governing where data is processed, inspected, and stored. A robust SASE solution should provide flexible sovereignty options, enabling enterprises to control data residency, operational access, and administrative domains based on geographic, regulatory, or organizational requirements. This includes:

- The ability to restrict traffic inspection to specific in-country or regional POPs
- Segment management access by jurisdiction
- Logical and physical separation of customer data
- A full SASE sovereign solution that provides a turnkey solution to build your own private SASE network when needed

A multilevel sovereignty offering helps organizations meet compliance mandates, reduce regulatory risk, and maintain operational control that adapts to their specific needs.

Questions to ask the SASE vendor about data sovereignty:

- Can traffic inspection, logging, and data storage be restricted to specific countries or regions?
- Do you offer multiple levels of sovereignty (data, operational, and administrative)?
- How do you support compliance with regional regulations or other local data protection laws?

Choose a Vendor that Offers Flexibility, Seamless Integration, and Reliable Tech Support

The SASE market is diverse and a complete solution often requires multiple components. If these components aren't designed to work as a single system, integration can be complex, costly, and diminish the benefits of converged networking and security. SASE is a journey, not a single-step transformation.

Evaluate your business needs and use cases to select a unified, single-vendor SASE platform that provides the capabilities you need today and can scale for the future. Choose a vendor that offers flexibility, seamless integration, and reliable technical support to minimize downtime, accelerate deployment, and maintain consistent, high-performance security across your organization.

www.fortinet.com

April 7, 2026 10:49 AM / MKTG-3121-0-0-EN