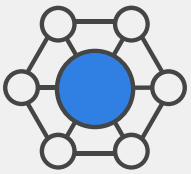
SOLUTION BRIEF

Secure Your Hybrid Workforce with Fortinet Unified SASE

Executive Summary

The rise of the hybrid workforce has significantly expanded the attack surface, now including home offices and mobile employees. This enlarged perimeter complicates the securing of networks, applications, and resources. Secure access service edge (SASE) simplifies this challenge by providing IT teams with an effective way to safeguard the hybrid workforce.

SASE solutions offer secure access and high-performance connectivity for branches and remote locations of any size. However, many solutions only address part of the issue. Fortinet Unified SASE tackles all hybrid workforce security challenges through a comprehensive, single-vendor approach. It integrates software-defined wide area networking (SD-WAN) with cloud-delivered security service edge (SSE), streamlining networking and security from the network edge to remote users. Additionally, Fortinet Unified SASE features unified management, a single agent, and end-to-end digital experience monitoring (DEM) to further simplify and enhance protection.



By 2027, 45% of new SASE deployments will be based on a single-vendor SASE offering, up from about 20% in 2023.[1]

Hybrid Workforce Challenges

Securing the hybrid workforce presents unique challenges as the rapid expansion of new network edges and the increase in remote employees have created vulnerabilities that cybercriminals now readily exploit. Security policies must be consistently applied and enforced, and an optimal work experience must be provided for all users.

Fortinet Unified SASE provides consistent security and user experience, whether users are accessing the web, corporate applications, or Software-as-a-Service (SaaS) applications. The solution includes a high-performance and scalable cloud network with more than 140 locations globally, enabling broad coverage, scalability, and proven security controls. Fortinet Unified SASE stands out as the most integrated, flexible, and intelligent SASE solution, continuously evolving to meet all use cases with innovative advancements.

A Truly Unified Solution

Our single-vendor SASE solution integrates Fortinet's premier Secure SD-WAN with our cloud-delivered SSE, known as FortiSASE. This unified approach offers the convenience of a single operating system, agent, and management platform.

FortiSASE features a cloud-based management console that includes features such as secure web gateway (SWG), Firewall-as-a-Service (FWaaS), cloud access security broker (CASB), data loss prevention (DLP), universal zero-trust network access (ZTNA), remote browser isolation (RBI) and much more. FortiSASE eliminates the need to navigate multiple consoles. It also uses a single data lake and unified data model for consistent policy enforcement and event tracking, with a regional log storage option to ensure compliance.

FortiSASE is a comprehensive solution that enables the deployment of a unified security policy, encompassing thorough malware and sensitive data inspection. The integrated user agent provides full functionality and embedded DEM, delivering end-to-end performance insights focused on users and applications, along with detailed troubleshooting capabilities. It also allows extending SASE logs to Fortinet SOC-as-a-Service (SOCaaS), offering organizations access to our SOC expertise and advanced technology without needing to build and maintain an in-house SOC. On top of SOCaaS integration, FortiSASE also supports forensics integration to provide in-depth analysis and investigation capabilities to help organizations respond to security incidents.

Flexible Deployment

Fortinet Unified SASE provides the industry's most adaptable deployment options, featuring native SD-WAN integrations, support for thin edge locations, agent-based and agentless access, and flexible point of presence (POP) selection options. This all-encompassing approach ensures a customized fit for various network environments and business requirements.

Our solution also supports third-party SD-WAN connectivity, making it ideal for large enterprises and managed service providers with diverse networking needs. It offers flexible POP connectivity, enabling the integration of Google Cloud and Fortinet POPs within a single deployment.

An enhanced system for cross-domain identity management support simplifies user management, streamlining IT administration. Additionally, Fortinet Universal ZTNA provides versatile access options and integration for agentless access from unmanaged devices, while improvements in Fortinet Secure SD-WAN enhance multicast routing, orchestration, and network visibility for latency-sensitive applications.

Integrated Intelligence with Native AI

In today's evolving threat landscape, reactive security measures are no longer sufficient. SASE solutions must utilize AI to proactively detect and mitigate threats in real time.

AI is fundamental to FortiSASE, with all security services powered by FortiGuard Labs AI-driven threat intelligence. FortiGuard Labs provides real-time threat intelligence feeds that continuously update our FortiSASE architecture with the latest information on emerging threats and attack patterns.

Additionally, incorporated generative AI (GenAI) tools serve as a virtual assistant, simplifying deployment, operations, and troubleshooting. Analysts highlight that integrating AI into SASE solutions significantly enhances proactive security capabilities, leading to a stronger security posture and improved operational efficiency.

Fortinet leverages AI-powered security to deliver complete visibility and streamlined troubleshooting. Integrating FortiAI with FortiManager and FortiAnalyzer streamlines and accelerates configuration, management, and troubleshooting for Day 0, Day 1, and Day 2 operations.

Unified SASE intelligence can also be found in Fortinet Universal ZTNA. The universal ZTNA application catalog automates ZTNA application configurations, integrating with the ZTNA application gateway fabric connector and management server. This eliminates the need for manual configuration of each ZTNA application destination.

Additionally, enhancements to SD-WAN include self-healing networks that address issues in real time and support autonomous mesh networking for improved resilience and performance.

Key Capabilities Under a Unified Console

FWaaS and SWG

FWaaS delivers high-performance SSL inspection and AI-driven threat detection for cloud traffic, applications, and services, ensuring secure connections for remote users while preserving user experience. SWG enhances web security by protecting against advanced threats and securing both web and encrypted traffic, using a combination of web filtering, antivirus, file filtering, and DLP to provide a robust defense-in-depth strategy for all devices.

CASB and DLP

The FortiGuard CASB Service offers extensive visibility, control, and security for SaaS applications, including the ability to block malicious applications with inline CASB. Additionally, the FortiGuard Data Loss Prevention Service safeguards sensitive data from breaches, insider threats, and exfiltration across hybrid environments.

Universal ZTNA

Fortinet Universal ZTNA provides flexible zero-trust access control for applications, regardless of user or application location. It enables IT teams to authenticate, secure, and monitor access to critical applications on a per-user and per-session basis. The solution offers continuous, near-real-time device posture verification and promptly blocks noncompliant devices and sessions.

RBI

RBI is available natively within FortiSASE unified management, enhancing web security by isolating potentially harmful web content infecting end users' devices. Risky web content is isolated in a secure, remote environment within FortiSASE POPs, protecting end-users against malware, phishing attacks, and malicious downloads without hindering user experience.

DEM

Fortinet DEM functionality streamlines troubleshooting and monitors the end-to-end user experience, offering insights into performance and business impact. It provides comprehensive coverage from endpoint devices to applications, with monitoring that addresses both cloud connections and local network issues to reduce resolution time.

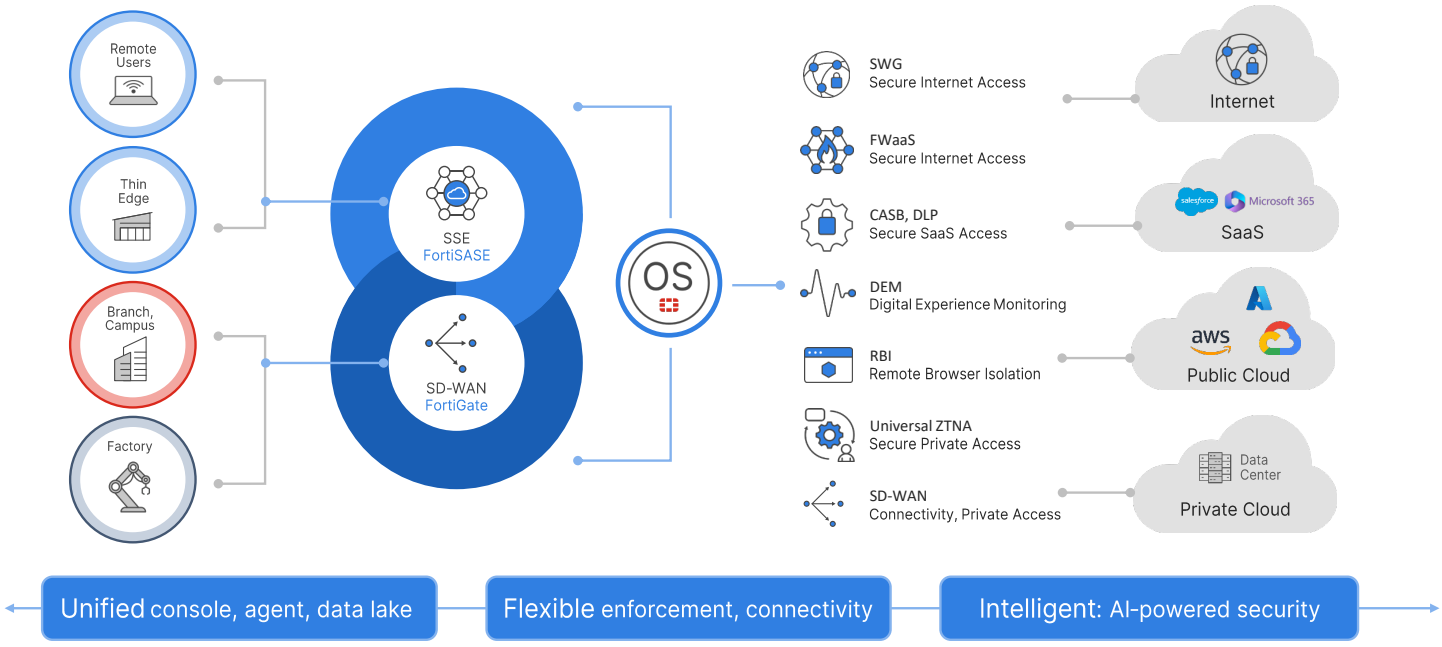


Figure 1: Fortinet Unified SASE with FortiGuard AI-Powered Security Services

SD-WAN

Cloud-delivered SD-WAN features, such as application steering and dynamic routing, ensure the shortest path to corporate applications. It adjusts connections in real time to maintain high-quality performance, enhancing the user experience for remote workers.

Key Use Cases

Secure internet access

The comprehensive FWaaS and SWG capabilities secure managed and unmanaged devices by supporting agent and agentless approaches. Natively integrated FortiGuard AI-Powered Security Services protect content and users from ransomware and other sophisticated attacks.

Secure private access

Zero-trust connectivity to corporate applications with unique SD-WAN integration provides low-latency access. ZTNA eliminates points of vulnerability by restricting network access. With Fortinet Universal ZTNA, you can implement granular application access to enable explicit, per-application access and help shift security strategies from an implicit trust model to a more secure explicit trust strategy. Fortinet Universal ZTNA provides continuous near-real-time device posture verification and blocks noncompliant devices and sessions.

Secure SaaS access

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

Secure access from thin edge locations

Fortinet Unified SASE secures internet and corporate application access from the thin edge with cloud-delivered AI-powered security to protect against malware, ransomware, and zero-day cyberthreats without endpoint agents.

FortiAP wireless access points intelligently offload traffic from thin edge locations to a SASE point of presence for comprehensive security inspection at scale for all devices. This integration also means you can manage the Fortinet WLAN portfolio from the same management console being used for SASE. Our solution also offers cloud-delivered management of FortiAP devices with zero-touch provisioning, removing the need for local on-site administrative staff and reducing management costs.

Secure SD-WAN for branch and campus locations

Fortinet Unified SASE includes the industry's only organically developed software complemented by an ASIC-accelerated platform to deliver the most comprehensive secure SD-WAN solution for branch and campus. It provides real-time application optimization for a consistent and resilient experience and advanced NGFW protection. Transitioning from MPLS to broadband via SD-WAN reduces cost and enhances application performance. This shift optimizes user experience and provides security for direct internet access.

The Fortinet Advantage

Rather than providing an isolated, cloud-only approach, Fortinet Unified SASE is integrated with the Fortinet Security Fabric platform. Using one operating system, FortiOS, across security controls, the Fortinet Security Fabric provides broad visibility, granular control, and consistent, proactive protection everywhere.

Additional benefits achieved with Fortinet Unified SASE include:

Reduced complexity and full visibility

Unified management equips you with the necessary tools to overcome the challenges associated with hybrid work, including visibility, protection, and optimization of the end-user experience. Fortinet Unified SASE provides a single console to manage all SSE capabilities, including FWaaS, SWG, ZTNA, CASB, DLP, RBI, and DEM.

Superior user experience

Productivity and quality of experience for the hybrid workforce are ensured with cloud-delivered SD-WAN capabilities such as intelligent application steering and dynamic routing.

Agentless connectivity

Agentless security is available for BYOD devices or devices where an agent cannot be downloaded, such as Chromebooks, with proxy auto-configuration files, agentless web portal, and thin edge devices.

Thin edge security

Our thin edge SASE solution provides comprehensive, agentless protection and simplified management for thin edges delivered via FortiAPs and FortiExtenders. This enables secure access to operational technology and Internet-of-Things devices and simplifies access in home offices and small office locations using Wi-Fi. This unique capability lets you extend enterprise-grade protection to thin edge locations without additional appliances, agents, or services.

Conclusion

Powered by a single operating system, Fortinet Unified SASE is an integrated, flexible, and intelligent cloud-delivered solution that protects users, applications, and endpoint devices while seamlessly interoperating with the rest of the distributed network. Our unique solution provides unified network and security visibility and is easy to configure via its intuitive cloud-hosted user interface. Its single management console for all SSE capabilities and DEM simplifies operations, improves return on investment, and facilitates the transition to hybrid workforce security.

Our commitment to reducing complexity and offering flexible solutions is demonstrated by our diverse use-case offerings, which range from traditional remote access to microbranch deployments and SD-WAN integrations. This adaptability extends zero-trust access, where continuous verification ensures robust security postures across all connections, even where software agents cannot be deployed.

Learn more about solving today's hybrid workforce challenges with Fortinet Unified SASE.

[1] Nat Smith, Neil MacDonald, Christian Canales, Andrew Lerner, Jonathan Forest, John Watts, Shailendra Upadhyay, Charlie Winckless, Forecast Analysis: Secure Access Service Edge (SASE), Gartner, October 10, 2023.

August 26, 2024 4:53 PM / 2845117-0-0-EN