

SOLUTION BRIEF

Secure Your Hybrid Workforce with Fortinet Unified SASE

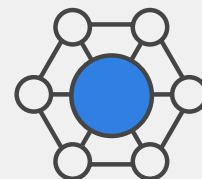
Executive Summary

The rise of the hybrid workforce has significantly expanded the attack surface, extending beyond traditional offices to include home networks, mobile users, and distributed locations. This expanded perimeter makes it increasingly difficult for IT teams to consistently secure networks, applications, and data.

Secure access service edge (SASE) addresses this challenge by converging networking and security into a cloud-delivered architecture that protects users wherever they work. SASE solutions provide secure access and high-performance connectivity for branches, remote offices, and mobile users of any size. However, many offerings only solve part of the problem, delivering either networking or security capabilities that are loosely integrated.

Fortinet Unified SASE addresses the full scope of hybrid workforce security through a comprehensive, single-vendor approach that tightly integrates software-defined wide area networking (SD-WAN) with cloud-delivered security service edge (SSE), simplifying operations while ensuring consistent protection from the network edge to remote users.

Fortinet Unified SASE further streamlines operations with unified management, a single agent, and integrated GenAI capabilities, along with end-to-end digital experience monitoring (DEM). Together, these capabilities provide greater visibility, faster troubleshooting, and stronger protection while simplifying how organizations secure and connect their distributed workforce.



According to Gartner, by 2028, 50% of new SASE deployments will be based on a single-vendor SASE platform offering, up from 30% in 2025.¹

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 access the web, corporate applications, or Software-as-a-Service (SaaS) applications. The solution includes a high-performance, scalable cloud network with more than 170 locations globally, providing 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), SaaS security posture management (SSPM), data loss prevention (DLP), universal zero-trust network access (ZTNA), 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), giving organizations access to our SOC expertise and advanced technology without building and maintaining an in-house SOC. In addition to SOCaaS integration, FortiSASE also supports forensic 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, including native SD-WAN integrations, support for thin edge locations, agent-based and agentless access, and flexible point-of-presence (POP) selection. 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, AWS, 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 ever-evolving threat landscape, Unified SASE security measures are no longer sufficient. SASE solutions must leverage AI to detect and mitigate threats in real time proactively.

AI is fundamental to Unified SASE, 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, FortiAI-Assist can be added to Unified SASE to transform troubleshooting and operations by replacing manual, time-consuming tasks with AI-driven workflows and agentic AI capabilities. It can enable initial configuration and provisioning on the one hand, and, combined with DEM, automatically check SD-WAN health, application availability, endpoint performance, and connectivity paths, pinpointing and resolving issues within minutes. This reduces mean time to resolution (MTTR), enforces compliance, and allows smaller IT teams to deliver faster, more reliable user experiences.

Beyond reactive support, FortiAI-Assist also provides automated diagnostics and continuous anomaly detection to prevent issues before they escalate. 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 to configure each ZTNA application destination manually.

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, leveraging a combination of web filtering, antivirus, file filtering, and DLP to provide a robust defense-in-depth across all devices.



CASB, SSPM, 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.

The integration of SSPM capabilities in FortiSASE strengthens SaaS security with a comprehensive set of innovations. Organizations lack the resources to continuously monitor SaaS configurations across tools such as Microsoft 365 and Salesforce. Misconfigurations create costly compliance risks and open the door to data leaks. With SSPM built into FortiSASE, organizations can get SSPM capabilities by automatically detecting, reporting, and remediating SaaS misconfigurations. This comprehensive SSPM solution complements our existing CASB capability in our Unified SASE solution and can be managed through our unified FortiSASE console.

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.

Universal ZTNA can be enforced by an application gateway, which can be either a FortiOS-based product deployed close to the applications or a lightweight connector, integrated in FortiSASE. The ZTNA connector serves as the native enforcement point within FortiSASE. It simplifies deployment, reduces infrastructure dependencies, and ensures consistent ZTNA enforcement everywhere, even in locations without a FortiGate firewall. Applications remain hidden from direct internet exposure, while the lightweight connector provides easy-to-deploy protection that can run seamlessly in any cloud or on-premises environment. It gives users an additional option for connecting their applications to the cloud for remote access, for even more flexibility.

Secure Browser

The Secure Browser is a browser extension that provides an additional layer of security while allowing users to continue using the browser they have always used. With the browser extension, security controls are added to provide conditional access to both private and SaaS applications, enforcing DLP policies with strict controls to deny copy/paste, print, download, upload, and watermarking, along with controls for GenAI applications. An extension delivers enterprise-grade SASE protection without disrupting user choice or IT operations, unlike a full enterprise browser, which often adds cost, complexity, and adoption barriers.

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.

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 three remote workers.



Key Use Cases

Secure internet access

The comprehensive FWaaS and SWG capabilities secure managed and unmanaged devices, supporting both agent-based 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, enabled by unique SD-WAN integration, provides low-latency access. ZTNA eliminates vulnerabilities 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 over applications to secure sensitive data and detect and remediate malware 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 across 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 networks. It provides real-time application optimization for a consistent and resilient experience and advanced next-generation firewall 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 tools to overcome the challenges of hybrid work, including visibility, protection, and end-user experience optimization. Fortinet Unified SASE provides a single console to manage all SSE capabilities, including FWaaS, SWG, ZTNA, CASB, SSPM, DLP, Secure Browser, and DEM.

Superior user experience

Productivity and quality of experience for the hybrid workforce are ensured through cloud-delivered SD-WAN capabilities, including 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, an 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, FortiBranch SASE devices, and FortiExtenders. This enables secure access to operational technology and Internet-of-Things (IoT) 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.

Fortinet Unified SASE Improves ROI and Reduces Complexity

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 to zero-trust access, where continuous verification ensures robust security across all connections, even when software agents cannot be deployed.

Learn more about solving today's hybrid workforce challenges with [Fortinet Unified SASE](#).

¹ Gartner, "Magic Quadrant for SASE Platforms," Jonathan Forest, Neil MacDonald, Dale Koeppen, 9 July 2025, <https://www.fortinet.com/resources/analyst-reports/gartner-magic-quadrant-sase>.

