SOLUTION BRIEF

FortiSASE: Comprehensive SASE Solution Provides Cloud-Delivered Security and Networking for WFA Users

Executive Summary

Most businesses now have a hybrid workforce that spends at least part of their week working off-premises. The resulting expanded attack surface—including home offices and mobile workers—has made it more challenging to secure the network, its applications, and digital resources. Organizations with large numbers of remote offices and hybrid workers often struggle to ensure that security policies are being applied and enforced consistently and that users have an optimal work experience, whether on or off the network.

Part of the challenge is that these changes happened organically rather than as part of a carefully planned strategy. The rapid growth of new network edges and work-from-anywhere (WFA) users, often implemented as discrete projects, has left gaps in security that cybercriminals have been eager to exploit.

A secure access services edge (SASE) architecture helps address these issues by extending secure access and high-performance connectivity to users anywhere. However, many SASE solutions only solve part of the problem, either failing to provide enterprise-grade cybersecurity to WFA users or being unable to seamlessly integrate with the range of physical and virtual network and security tools deployed at the network edge. Or both. The result is an inability to deliver a consistent security posture and optimal user experience everywhere.

FortiSASE, driven by the Fortinet single-vendor SASE approach, delivers a comprehensive SASE solution by integrating cloud-delivered software-defined wide-area network (SD-WAN) connectivity with a cloud-delivered security service edge (SSE) to extend the convergence of networking and security from the network edge to WFA users.

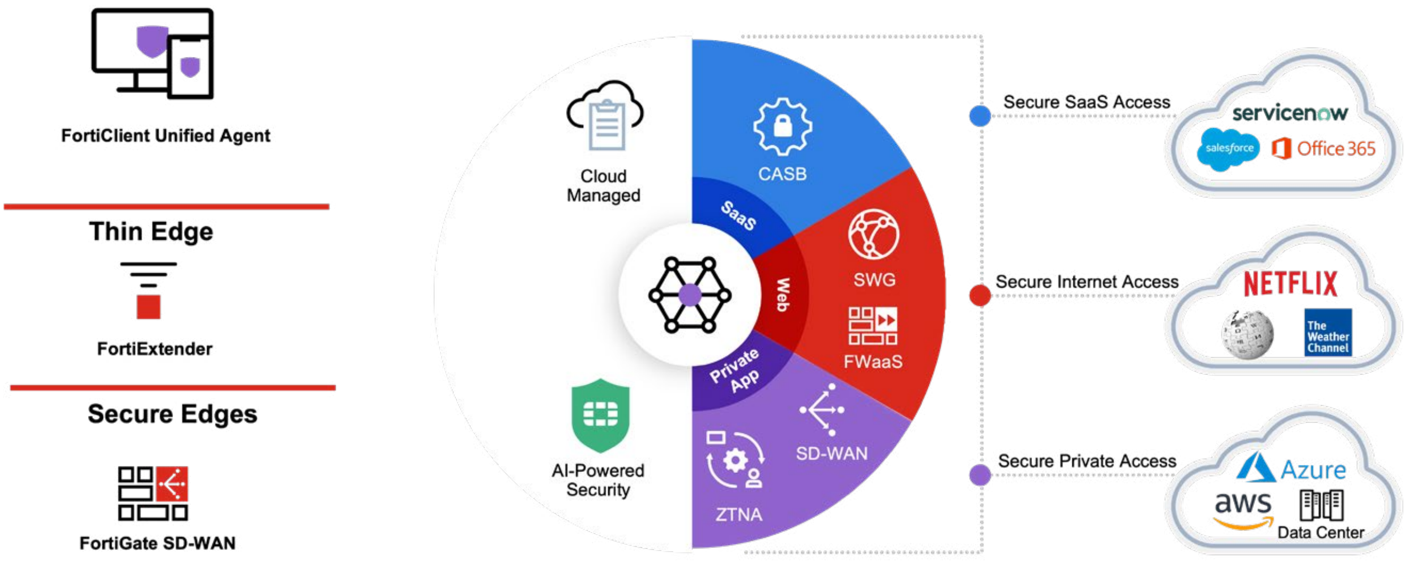

Figure 1: Consistent security posture and superior experience for WFA users anywhere, powered by FortiOS.

FortiSASE has been specifically engineered to converge networking and security into an integrated and adaptive solution to ensure optimal and secure connectivity from any network edge to WFA users. Powered by 20+ years of organic innovation, FortiSASE delivers secure web gateway (SWG), zero-trust network access (ZTNA), next-generation cloud access security broker (CASB), Firewall-as-a-Service (FWaaS) as a cloud-based service, and Secure SD-WAN, allowing organizations to shift from a CapEx to an OpEx business model.

Organizations have the flexibility to perform security locally on their FortiGate or to connect branch offices to FortiSASE over an IPSec tunnel to perform security inspection in the cloud (via the FortiSASE POP) through their FortiGates (SD-WAN/NGFW). This allows for consistent security posture for WFA users and simplifies security policy management. This uses the FortiGate Secure Edge Connector. Additionally, organizations can benefit from simplified Thin Edge deployments (with FortiExtender) with enhanced Zero Touch Provisioning from the SASE interface.

Our unique Security-Driven Networking strategy, powered by a single operating system, FortiOS, and enhanced with FortiGuard AI-powered Security Services, enables us to weave security and networking functionality into a single, integrated system to deliver consistent security and user experience to any user anywhere. FortiSASE uniquely empowers organizations to enable secure access to web, cloud, and applications anywhere with enterprise-grade cybersecurity and superior user experience built in.

FortiSASE, powered by FortiOS and FortiGuard AI-powered Security Services, provides simple and scalable cloud-delivered security for consistent security and superior user experience for WFA users.

FortiSASE: Simple, Seamless, and Scalable Cloud-Delivered Security

FortiSASE provides simple cloud-based management with a self-service design, easy user onboarding, and the industry's most flexible tiered user-based licensing model. This allows organizations to transition from CapEx to OpEx business models to keep the costs of today's highly dynamic networks and infrastructures predictable.

FortiSASE is also Service Organization Control (SOC 2) certified, which provides independent validation that its solution security controls operate in accordance with the American Institute of Certified Public Accountants (AICPA) applicable Trust Services Principles and Criteria. This SOC 2, Type II standard certification demonstrates the Fortinet commitment to ensuring that our customers can meet diverse compliance requirements. FortiSASE also offers a comprehensive set of enterprise-class security capabilities already fully integrated into the solution, including SWG, universal ZTNA, next-generation dual-mode CASB, FWaaS, and advanced threat protection capabilities enabling three critical use cases:

- **Secure internet access:**

  For WFA users operating outside the corporate perimeter, direct internet access expands their attack surface—and risk. FortiSASE offers comprehensive SWG and FWaaS capabilities to secure both managed and unmanaged devices by supporting agent and agentless approaches.

- **Secure private access:**

  With hybrid work being the new norm, traditional VPNs struggle to scale. And because they do not include integrated inspection or advanced protections, compromised VPN tunnels can end up opening access to every application, expanding the attack surface and increasing the risk of lateral threat movement. FortiSASE Secure Private Access offers the industry's most flexible and secure connectivity to corporate applications. Organizations can implement granular application access using a universal ZTNA approach. Enabling explicit, per-application access helps shift security strategies from an implicit trust model to a more secure explicit trust strategy. FortiSASE Secure Private Access also integrates seamlessly with SD-WAN networks to automatically find the shortest path to corporate applications, powered by the intelligent steering and dynamic routing capabilities available in FortiSASE.

- **Secure SaaS access:**

  Given the rapid increase in SaaS adoption, organizations continue to struggle with shadow IT challenges and stopping data exfiltration. FortiSASE Secure SaaS Access with next-generation dual-mode CASB, using both inline and API-based support, provides comprehensive visibility by identifying key SaaS applications and reporting risky applications to overcome shadow IT challenges. Next-generation CASB also offers granular control of the applications to secure sensitive data and detect and remediate malware in applications across both managed and unmanaged devices.

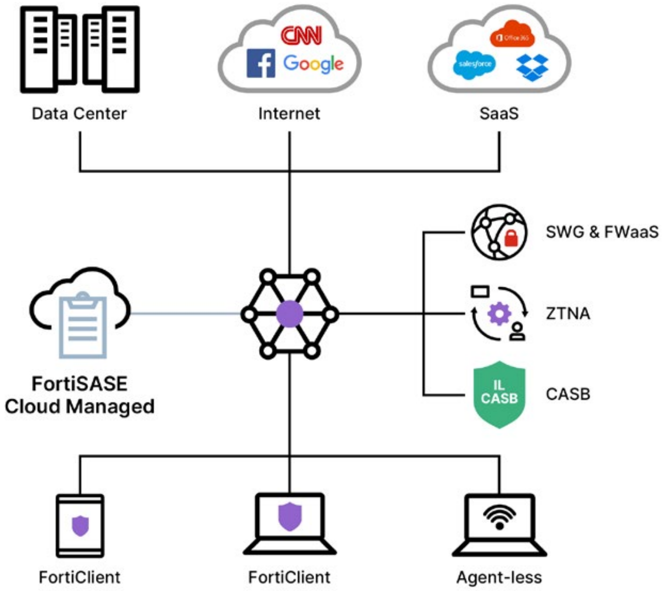

Figure 2: FortiSASE provides secure, reliable clopud-based connectivity to any application

Delivering Comprehensive Security Capabilities at Scale

FortiSASE offers a comprehensive set of security capabilities to secure traffic destined to the internet, private data centers, and SaaS applications:

Secure Web Gateway: Protects against most advanced web threats with a broad set of capabilities for securing web traffic, including encrypted traffic. Its web filtering, antivirus, file filtering, data leak prevention, and more, work together to enable a defense-in-depth strategy for both managed and unmanaged devices.

Firewall-as-a-Service: Leveraging the independently certified capabilities of FortiOS—the core of the Fortinet industry-leading security fabric strategy—enables high-performance SSL inspection and advanced threat detection techniques for cloud traffic, applications, and services. The Fortinet FWaaS solution establishes and maintains secure connections for remote users while analyzing inbound and outbound traffic—without impacting user experience.

Universal ZTNA: ZTNA allows IT teams to authenticate, secure, and monitor per-user and per-session access to business-critical applications. Universal ZTNA allows this functionality to be applied everywhere for all users and devices, regardless of location, shifting security from an implicit access approach to a more secure explicit access strategy, per application, based on continuous identity and context validation.

Next-generation dual-mode CASB: With both inline and API-based CASB support, FortiSASE can identify key SaaS applications, report shadow IT applications, secure access to sanctioned SaaS applications, and restrict access to SaaS apps from trusted endpoints—all while enabling ZTNA posture checks for application access.

Domain Name System (DNS): Protect against sophisticated DNS-based threats, including DNS tunneling, DNS protocol abuse, DNS infiltration, C2 server identification, and domain generation algorithms (DGAs). Gain complete visibility into DNS traffic while blocking high-risk domains, including malicious newly registered domains (NRDs), parked domains, and more.

Intrusion prevention (IPS): Protect against new and existing vulnerabilities with real-time threat intelligence and minimal performance impact.

Sandboxing: Ensure files are safe from previously unknown advanced threats by safely identifying, triggering, and analyzing threats for real-time prevention and detection.

The Fortinet Advantage

Rather than providing an isolated, cloud-only approach, FortiSASE offers services built into the Fortinet Security Fabric. By extending and leveraging the power of FortiOS, the Fortinet Security Fabric provides broad visibility, granular control, and consistent, and even proactive, protection everywhere.

Consistent cybersecurity for users, whether on- or off-network: FortiSASE provides comprehensive cloud-delivered security with natively integrated ZTNA, to provide consistent protection for WFA users.

A unified agent: Our unified agent, FortiClient, supports multiple uses cases, including ZTNA, traffic redirection to SASE, dual-mode next-generation CASB, and robust endpoint protection—eliminating the need for a separate agent for each use case.

Simple management and consumption: Simple deployment, onboarding, and management—with a self-service design and the most flexible tiered user-based licensing model in the industry—allow IT teams to implement comprehensive and consistent security for their hybrid workforce. And it does this without compounding efforts to manage, monitor, orchestrate, and optimize systems deployed across different network ecosystems that can overwhelm already overburdened IT teams. FortiSASE also integrates with Fortinet FortiManager, allowing unmatched visibility and management across on-premises and remote users.

These technologies, powered by a single FortiOS operating system, provide an integrated, cloud-based SASE solution that protects users, applications, and endpoint devices while seamlessly interoperating with the rest of the distributed network. This seamless, end-to-end approach to converging networking and security enables the sort of adaptive strategy organizations require in today's rapidly evolving digital marketplace.

www.fortinet.com

March 3, 2023 1:10 PM

1675117-A-0-EN