Corporate Armor
sales@corporatearmor.com
877.449.0458

DATA SHEET

FortiSASE™

Available in:

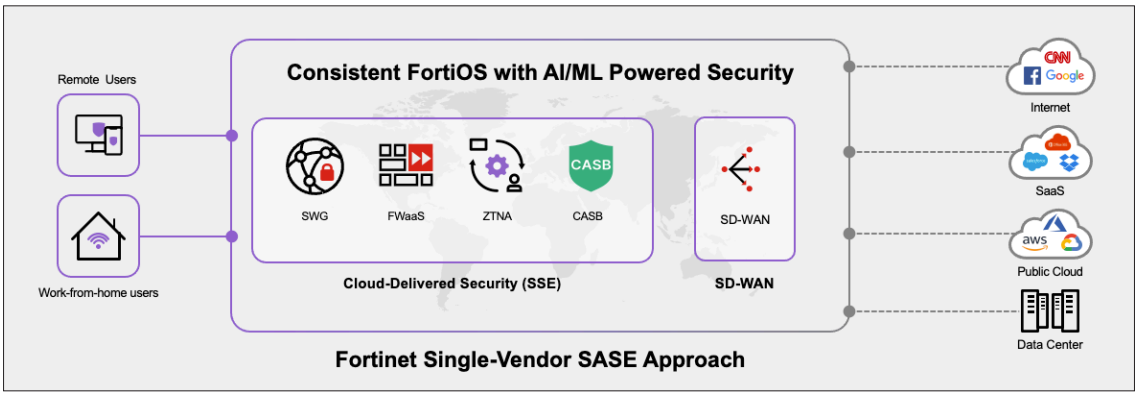
Cloud

Scalable Cloud-Delivered Security and Networking for Hybrid Workforce

A hybrid workforce has become the new reality for most organizations. This has created new challenges by expanding the attack surface while making it more challenging to secure remote users. The growing number of new network edges and remote users, often implemented as discrete projects, leave gaps in security that cybercriminals are all too anxious to exploit. At the same time, organizations with large numbers of remote offices and a hybrid workforce often struggle to ensure that security policies are being applied and enforced consistently for users both on and off the network while delivering superior user experience to everyone.

A Secure Access Services Edge (SASE) architecture converges networking and security, enabling secure access and high-performance connectivity to users anywhere. However, many cloud-delivered security solutions fail to provide enterprise-grade security to remote users. They are also unable to seamlessly integrate with the range of physical and virtual network and security tools deployed at the network edge to deliver consistent security posture and superior user experience everywhere.

FortiSASE, driven by Fortinet's single-vendor SASE approach, delivers a comprehensive SASE solution that seamlessly integrates cloud-delivered SD-WAN connectivity with cloud-delivered Security (SSE) to extend the convergence of networking and security from the edge to remote users. FortiSASE's cloud-delivered security and networking capabilities deliver enterprise grade security and superior user experience to remote workers in a single, integrated solution.



Fortinet Single-Vendor SASE Approach

Powered by 20+ years of organic innovations, a common FortiOS operating system, and FortiGuard's AI-powered security services, FortiSASE enables Secure Web Gateway (SWG), Universal Zero Trust Network Access (ZTNA), next-generation dual-mode Cloud Access Security Broker (CASB), Firewall-as-a-Service (FWaaS), and cloud-delivered SD-WAN connectivity that allows organizations to shift from a CAPEX to an OPEX business model while significantly lowering overhead and improving user experience and protection. FortiSASE empowers organizations to grant per-user and per-session secure access to web, cloud, and applications regardless of where they have been deployed, combined with fully-integrated enterprise-grade security. With seamless convergence between security and networking, FortiSASE ensures that the same level of protection, visibility, and user experience is extended to every user, anywhere.

For those who are compliance-conscious, FortiSASE is Service Organization Control (SOC2) Certified, which provides independent validation that the 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 our commitment to ensuring that our customers are able to meet diverse compliance requirements.

HIGHLIGHTS

FortiOS

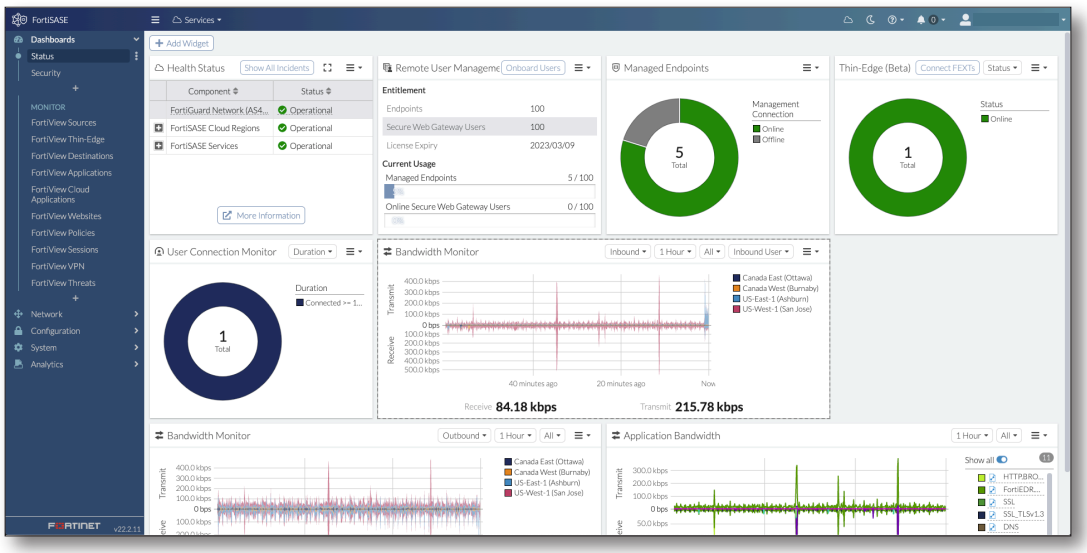
Fortinet's unified operating system, FortiOS, is the culmination of over 20 years of industry-leading innovation. It powers our unique security-driven approach to seamlessly converge networking and security from the cloud.

FortiGuard AI-powered Security Services

Our AI-powered security services, applied across application, content, web traffic, devices, and users, provide consistent real-time protection against the latest attacks while ensuring rapid, real-time detection and response.

Cloud-Based Management

Simple cloud-based management provides centralized visibility and control across distributed users and applications, all backed by our industry-leading SLAs.



KEY BUSINESS OUTCOMES

Consistent Security Posture Everywhere

Overcome security gaps and minimize your attack surface with consistent security posture powered by the same FortiOS at the edge as in the cloud for remote users.

Superior User Experience

With intelligent application steering and dynamic routing, our Secure SD-WAN capabilities natively available deliver superior user experience for your remote users.

Operational Efficiency

Simplify operations with simple cloud-delivered management combined with enhanced security and networking analytics.

Shift to an OPEX Business Model

Simple user-based license model allows organizations to shift from upfront capital investments.

KEY USE CASES

Secure Internet Access

For remote users no longer protected by the corporate perimeter, direct internet access expands the attack surface and related risks. FortiSASE offers comprehensive Secure Web Gateway (SWG) and Firewall-as-a-Service (FWaaS) capabilities for both managed and unmanaged devices by supporting an agent and agentless approach.

Secure Private Access

Traditional VPNs cannot address the challenges faced by today's hybrid workforce. Because they do not inspect connections, they inadvertently expand the attack surface and increase the risk of lateral threat movement. FortiSASE Secure Private Access offers the industry's most flexible secure connectivity to corporate applications. Organizations can enforce granular access to applications with Universal ZTNA, enabling explicit per-application access and enabling the critical shift from implicit to explicit trust. FortiSASE Secure Private Access also offers organizations the benefits of seamless integration with SD-WAN networks and access to corporate applications by automatically finding the shortest path—powered by the intelligent steering and dynamic routing capabilities available in FortiSASE.

Secure SaaS Access

With the rapid increase in SaaS adoption, many organizations 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 applications to secure sensitive data and detect and remediate malware in applications across both managed and unmanaged devices.

KEY FEATURES

SECURITY AS A SERVICE

Secure Web Gateway (SWG)

Protects against most advanced web threats with a broad set of capabilities for securing web traffic, including encrypted traffic. SWG enables defense-in-depth strategy with web filtering, anti-virus, file filtering, data leak prevention, and more for both managed and unmanaged devices.

Firewall-as-a-Service (FWaaS)

Leveraging the independently certified and acclaimed capabilities of FortiOS, our FWaaS technology enables high-performance SSL inspection and advanced threat detection techniques from the cloud. It also establishes and maintains secure connections for remote users and analyzes in-bound and out-bound traffic without impacting user experience.

Universal ZTNA

Applying ZTNA everywhere for all users and devices, regardless of location, shifts implicit access to explicit control. Granular controls, applied per application, combine user authentication, continuous identity and context validation, and monitoring.

Next-Generation Dual-mode CASB

With both inline and API-based support, next-gen CASB identifies key SaaS applications and reports shadow IT applications, provides secure access to sanctioned SaaS applications, restricts access to SaaS apps to trusted endpoints, and enables ZTNA posture checks for application access.

NETWORKING AS A SERVICE

Software-Defined WAN (SD-WAN)

Fortinet's cloud-delivered SD-WAN capabilities include application steering and dynamic routing to help identify the shortest path to corporate applications—and then make corrections as the integrity of those connections changes—delivering and maintaining a superior user experience to remote workers.

Application Visibility and Control

FortiSASE includes over 5000 application signatures, first packet identification, deep packet inspection, custom application signatures, SSL decryption, TLS1.3 with mandated ciphers, and deep inspection to ensure and maintain deep visibility and granular control over applications.

THE FORTINET ADVANTAGE

Rather than providing an isolated, cloud-only approach, FortiSASE functions as an extension of the Fortinet Security Fabric, extending and leveraging the power of FortiOS—the common operating system that ties the entire portfolio of Fortinet security solutions—everywhere. This solution includes

Consistent Security and Superior User Experience

Comprehensive cloud-delivered security and networking combined with universal ZTNA for users anywhere.

One Unified Agent

Our unified agent supports multiple use cases. FortiClient can be used for ZTNA, traffic redirection to SASE, CASB, and endpoint protection without the multiple agents for each use case other solutions require.

Simple Management and Consumption

Simple onboarding and management with a unique self-service design includes the industry's most flexible tiered user-based licensing model.

LICENSE INFORMATION

REMOTE USERS AND DEVICES	BANDS	FORTITRUST USER LICENSE	PACKS	USER LICENSE
FortiSASE Remote	**100-499**	FC2-10-EMS05-547-02-DD	**25-pack**	FC1-10-EMS05-553-01-DD
	500-1999	FC3-10-EMS05-547-02-DD	**500-pack**	FC2-10-EMS05-553-01-DD
	2000-9999	FC4-10-EMS05-547-02-DD	**2000-pack**	FC3-10-EMS05-553-01-DD
	10 000+	FC5-10-EMS05-547-02-DD	**10 000 pack**	FC4-10-EMS05-553-01-DD

FSI-DAT-R09-20221020