FortiSASE™

Highlights

- Secure SaaS Access
- Secure Internet Access
- Secure Private Access
- AI-Powered Security
- Cloud-Managed

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.

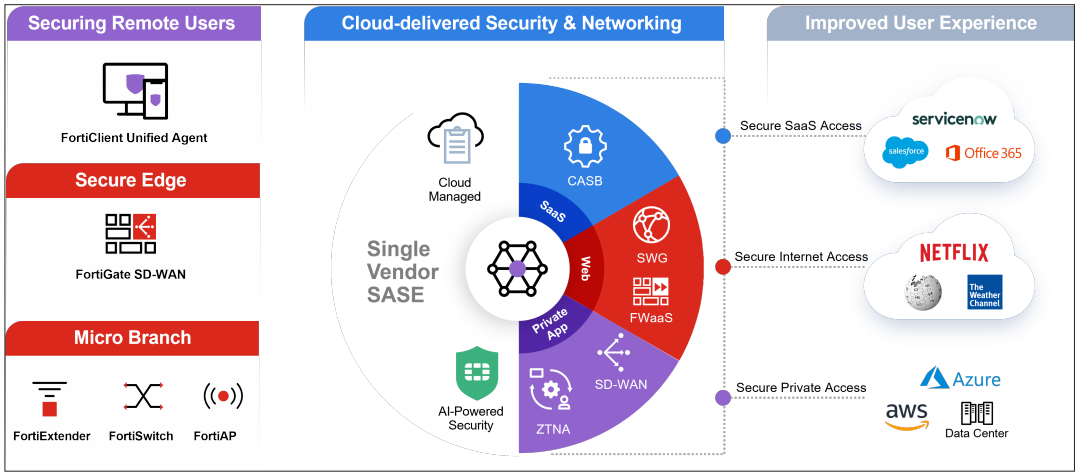
Available in

Cloud

Introduction

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 a hybrid workforce. 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.

Fortinet's Single-Vendor SASE approach empowers organizations to consistently apply enterprise-grade security and superior user experience across all edges converging networking and security across a unified operating system and agent. FortiSASE extends FortiGuard security services across Thin Edge, Secure Edge, and remote users enabling secure access to users both on and off the network.



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.

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 or branch locations 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

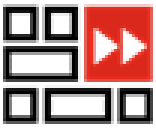
With the rapid increase in SaaS adoption, many organizations struggle with Shadow IT challenges and stopping data exfiltration. FortiSASE Secure SaaS Access, with Next-Generation Dual-Mode CASB using both inline and API-based support, provides comprehensive visibility by identifying key SaaS applications 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 the 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, DLP (data loss 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 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.

Expanding SASE to Secure All Users, Edges, and Devices

Fortinet brings new innovations in its SASE offering. Fortinet SASE is becoming the industry's most comprehensive SASE offering - securing users, access, edges, and devices anywhere while delivering the highest ROI, consistent security posture and improved user experience. Powered by Fortinet's unique security and networking convergence approach, it offers organizations a simple secure networking journey towards SASE.

Fortinet SASE's new innovations enhances the cutting-edge AI-powered solution specifically designed for the hybrid workforce, the power of cloud delivery, unified management and logging, with comprehensive features such as Universal ZTNA, SD-WAN integration, OT/IoT security, LAN/WLAN/5G security, Digital Experience Monitoring, and a flexible licensing model. The new Fortinet SASE solution ensures the utmost security for all edges, devices, and users, whether they are accessing the web, corporate applications, or SaaS 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 the following benefits.

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	BANDS	USER LICENSE
FortiSASE Remote	50-499	FC2-10-EMS05-547-02-DD
	500-1999	FC3-10-EMS05-547-02-DD
	2000-9999	FC4-10-EMS05-547-02-DD
	10 000+	FC5-10-EMS05-547-02-DD

Features List

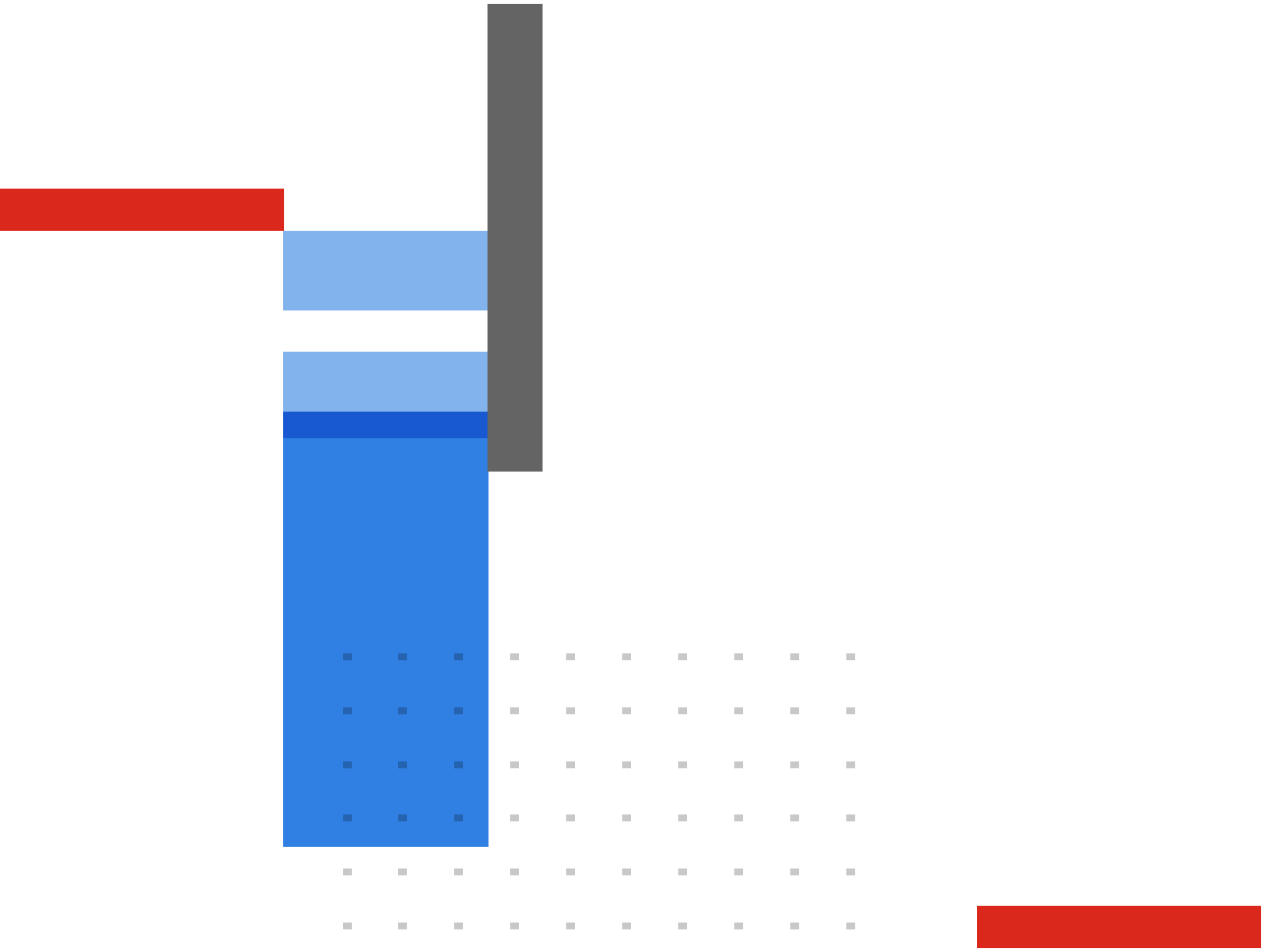
	Features	Description
SECURE SD-WAN	Application Identification and Control	Granular application policies, application SLA based path selection, dynamic bandwidth measurement of SD-WAN paths, active/active and active/standby forwarding, overlay support for encrypted transport, Application session-based steering, probe-based SLA measurements. More than 8000 applications are controlled, including industrial control signatures.
	Advanced Routing	Application aware routing, Static routing, Internal Gateway (iBGP, OSPF v2/v3 , RIP v2), External Gateway(eBGP), VRF, route redistribution, route leaking, BGP confederation, router reflectors, summarization and route-aggregation, route asymmetry
	Network and Security Convergence	Industry's only organically developed, purpose-built, and ASIC-powered SD-WAN enables thin edge (SD-WAN, routing) and WAN Edge (SD-WAN, routing, NGFW) to secure all applications, users, and data in the branch offices and its integration with FortiSASE enables consistent robust security for users everywhere.
	Secure Private Access	Securely connect remote users to private applications (Secure Private Access) by establishing IPSec tunnels from SASE PoP to multiple SD-WAN Hubs
CLOUD-DELIVERED SECURITY	API-CASB	Directly connected to leading SaaS providers to access usage and data stored in the cloud. This enables Administrators the ability to scan provisioned cloud resource configurations for potential threats as well as SaaS application data for threats, proprietary information, or sensitive customer records. This ensures that all users of the organization's SaaS applications are monitored and protected no matter where they are or what device they are on.
	In-line CASB	Protects data in motion and data at rest for cloud applications, create shadow IT report, perform risk assessment, expand visibility into risk trends and events.
	FWaaS	Powered by FortiOS, the FortiSASE FWaaS is a cloud-based service that provides hyperscale, next-generation firewall (NGFW) capabilities, including web filtering, advanced threat protection (ATP), intrusion prevention system (IPS), and Domain Name System (DNS) security. Security efficacy matches that of a FortiGate Firewall.
	SWG	FortiSASE SWG relies on FortiOS explicit web proxy, captive portal, and authentication features to secure customers' web traffic.
	ZTNA	ZTNA is a capability within Zero Trust Access (ZTA) that controls access to applications. It extends the principles of ZTA to verify users and devices before every application session. ZTNA confirms that they meet the organization's policy to access that application.
ADVANCED THREAT DETECTION	AntiVirus (AV)	FortiSASE Antivirus delivers automated updates that protect against the latest polymorphic attacks, viruses, spyware, and other content-level threats. Based on patented Content Pattern Recognition Language (CPRL), the antivirus engine is designed to prevent known and previously unknown virus variants providing 1.8M new AV definitions every week.
	Antispam	FortiGuard Antispam provides a comprehensive and multi-layered approach to detect and filter spam processed by organizations. Dual-pass detection technology can dramatically reduce spam volume at the perimeter, giving you unmatched control of email attacks and infections.
	Application Control	FortiSASE can recognize network traffic generated by well-known applications as well as custom applications. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic, even if the traffic uses non-standard ports or protocols. Quickly create policies to allow, deny, or restrict access to applications or entire categories of applications.
	Data Leak Prevention	DLP allows businesses to identify sensitive information across multiple cloud-based systems, prevent the accidental sharing of data, and monitor and protect data. Offers predefined reports for standards including SOX, GDPR, PCI, HIPAA, NIST, and ISO27001, to provide organizations visibility into policy violations so they can be tracked and remediated.
	DNS Filtering	DNS filtering provides full visibility into DNS traffic while blocking high-risk domains including malicious newly registered domains (NRDs) and parked domains. It protects against sophisticated DNS-based threats including DNS over TLS (DoT), DNS over HTTPS (DoH), DNS flood protection, DNS tunneling, DNS infiltration, C2 server identification, and DGAs (Domain Generation Algorithms).
	Intrusion Prevention (IPS)	The AI/ML-powered IPS Service provides near-real-time intelligence with thousands of intrusion prevention rules to detect, and block known and suspicious threats before they ever reach your devices with deep packet inspection of network traffic. The service is augmented by our in-house research team.
	Next Generation AI Powered Sandbox	Utilizes AI/machine learning technology to identify and isolate advanced threats in real-time. Inspects files, websites, URLs and network traffic for malicious activity, including zero-day threats, and uses sandboxing technology to analyze suspicious files in a secure virtual environment.
	SSL Inspection / Decryption	Using deep inspection, FortiSASE impersonates the recipient of the originating SSL session, then decrypts and inspects the content to find threats and block them. It then re-encrypts the content and sends it to the real recipient. Deep inspection not only protects you from attacks that use HTTPS, but it also protects you from other commonly used SSL-encrypted protocols such as SMTPS, POP3S, IMAPS, and FTPS.
	Web Filtering	Web Filtering leverages a database of hundreds of millions of URLs classified into 90+ categories to enhance granular web controls and reporting. TLS 1.3 support extends analysis to encrypted traffic. It also blocks unknown malicious URLs almost immediately. Cloud-enabled; provides complete protection to web-borne threats, AI-driven detection, analysis and enforcement for real-time protection against known and unknown threats.
	OutBreak Alerts	Receive communication on latest cybersecurity attacks with comprehensive details of the attack including timeline, technology affected, and where applicable patches/ mitigation recommendations can be found. Including recommended Fortinet products that would break the attack sequence, and threat hunting tools to help you determine if you were affected

Features List (continued)

	Features	Description
CONNECTIVITY	Unified Agent	One unified agent supports multiple use cases. The FortiClient agent can be used for ZTNA, traffic redirection to SASE, and Endpoint protection without requiring multiple agents for each use case.
	Agentless Connectivity	Agentless security is available for BYOD devices or devices where an agent cannot be downloaded (eg. Chromebooks), with the use of PAC files.
	Endpoint Protection	Fortinet's FortiClient offers security, compliance, and authorized access controls in a single client. FortiClient gives you endpoint protection software that runs directly on an endpoint, such as a smartphone or tablet. FortiClient then connects to the Fortinet Security Fabric and feeds the devices to the rest of your system. This provides you with endpoint security information, visibility, and the ability to control who and what accesses each device. FortiSASE supports management and integration of a FortiExtender configured as a LAN extension. By relying on FortiExtender instead of FortiClient to handle secure connectivity to FortiSASE, this solution essentially extends the single-user single-device FortiClient endpoint case to a multiuser, multidevice LAN environment.
	Thin Edge	Our family of industry-leading, secure WLAN/LAN products, also integrate with Fortinet Single-Vendor SASE solution. This enables secure micro-branches where LAN solutions are deployed to send traffic to a FortiSASE solution and ensure comprehensive security of all devices at the site, with single management console.
	Secure Edge	To optimize user experience, FortiSASE lets you choose to perform security with your local FortiGate or connect branch offices to FortiSASE for security inspection in the cloud through FortiGate NGFW and Fortinet Secure SD-WAN.
	API Connectivity	FortiSASE integrates seamlessly with FortiAnalyzer (Analytics), FortiMonitor (DEM), FortiSIEM (threat detection). Open REST APIs are available to be leveraged and used for inbound API integrations.
	Authentication	Support for SAML based authentication and seamless integration with 3rd party identity providers such as Microsoft Entra ID and Okta can be integrated along with support for native FortiTrust ID.
	Dedicated IPs Support	With an additional license, FortiSASE can support dedicated public IPs for customers enabling IP reputation and Geo-Location services with source IP anchoring.
AI-POWERED SERVICES	FortiGuard Security Services	FortiSASE provides botnet-protection by default and all the security services like AV, IPS, web Filtering, DLP are enabled by the FortiGuard AI/ML powered security. All the signature updates and definitions are updated in near--real time. Fortinet has massive customer base of 630,000+ and we are able to leverage this intelligence from this install base to deliver updates to FortiGuard threat intelligence labs; which in turn allows us to propagate any new day-0 threat signatures to all customers on a real time basis.
MONITORING AND MANAGEMENT	Single Console	With the SASE Console, administrators gain a centralized management platform for a single dashboard for all-in-one configuration and visibility for all use cases (web, private and SaaS security). Through a single pane of glass, they can efficiently deploy and manage security services, monitor network performance, and analyze security events. Actionable insights and customizable reports enable informed decision-making and continuous optimization of security and networking strategies.
	MSSP Portal	The portal offers centralized management and configuration capabilities, enabling MSSPs to efficiently deploy and manage SASE services across their client base. From a single pane of glass, MSSPs can configure security policies, network settings, and user access, ensuring consistent and unified security across multiple client environments. With the FortiSASE solution, customers can generate reports and view logs. Reports and logs are useful components to help you understand what is happening on your network, and to inform you about network activities, such as a virus detection, visit to an invalid website, intrusion, failed login attempt, and others.
	Reporting	You can generate data reports from logs by using the Reports feature. You can configure FortiSASE to regularly run reports at scheduled intervals, and manually run reports when desired. Logging and monitoring are also useful components to help you understand what is happening on your network, and to inform you about network activities, such as a virus detection, visit to an invalid website, intrusion, failed login attempt, and others.
	Analytics	You can generate data reports from logs by using the Reports feature. You can configure FortiSASE to regularly run reports at scheduled intervals, and manually run reports when desired.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

August 28, 2023

FSI-DAT-R13-20230828