Fortinet FortiSASE
Overview

Telesystem IT's About Trust

Scalable Cloud-Delivered Security and Networking for Hybrid Workforce

A hybrid workforce has become the new reality for most organizations. This situation 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.

Organizations are tasked to secure employees who access the network and applications from on-site and off-site locations. To summarize, the shift to hybrid workforce has expanded the attack surface, created security gaps, and increased the complexity of network and application protection.

Additionally, there is a huge uptick in usage of SaaS applications to improve business productivity. Security teams require visibility into SaaS applications leading to the problem of shadow IT.

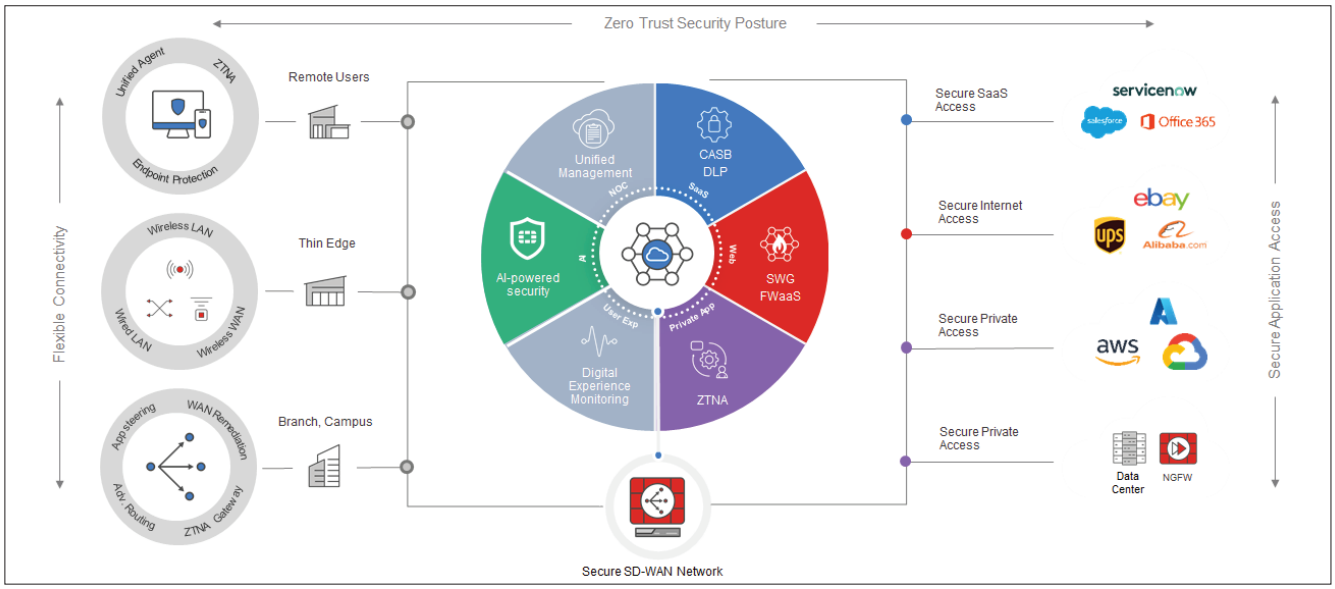
Solution Highlights

- **Flexible Secure Private Access solution** either utilizing ZTNA or via SD-WAN integration.
- **Unified Management**, cloud hosted, includes protections to private and cloud applications.
- **Enterprise Security** with consolidated AI/ML-Powered FortiGaurd threat services
- **Global Coverage** protects users anywhere with an ever-expanding footprint of SASE PoPs
- **Unified Agent combines EPP, ZTNA, CASB, DEM, and VPN** into a single SASE agent

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 Unified SASE approach empowers organizations to consistently apply enterprise-grade security and superior user experience across all edges converging networking and security leveraging a unified operating system and agent. FortiSASE extends FortiGuard AI/ML powered threat intelligence security services across Thin Edge (such as wireless APs), Secure SD-WAN, and client agents 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 the FortiGuard 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), Data Loss Prevention (DLP), 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 can meet diverse compliance requirements. Fortinet delivers 99.999% SLA with latency guarantee for security inspection, which is possible because of global reach with hundreds of security PoPs.

Key Use Cases

Secure Internet Access

- Comprehensive Secure Web Gateway (SWG), Advanced Threat Protection and Firewall-as-a-Service (FWaaS) capabilities for both managed and unmanaged devices by supporting an agent and agentless approach
- FortiGuard Labs suite of AI-powered security services—natively integrated into FortiSASE—secures web, content, and users with protection from ransomware and sophisticated attacks
- Real-time SSL inspection (including TLS 1.3) provides deep inspection of web activity for threats without any drastic performance impact

Secure Private Access

- Secure anywhere access to corporate applications in datacenter and cloud with deep security inspection
- User Identity and device context based zero-trust access to explicit applications with continuous device posture re-assessment from remote or on-premises locations
- Superior experience with full integration with Fortinet SD-WAN architecture allowing fast access to applications even for remote users accessing private applications

Secure SaaS Access

- Safe cloud application access with blocking of malicious applications with in-line CASB feature
- Control over application content and files with API based CASB and DLP for threat protection
- Detect and quarantine malicious files that aren't covered by endpoint security and from unmanaged devices

Secure Thin Edge Access

- Secure thin edge locations that don't have on-prem firewall to block ransomware and malware
- Secure access using built-in hardware agent in FortiAP and FortiExtender without any client agents
- Cloud delivered management of FortiAP with zero-touch provisioning support

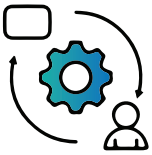
Key FortiSASE Features

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, anti-malware, file filtering, 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, Sandbox, 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.

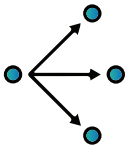


Universal ZTNA

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, context validation, integration with third party IAM, 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 applications to trusted endpoints, and enables ZTNA posture checks for application access.



Software-Defined WAN (SD-WAN)

Fortinet 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.

Data Loss Prevention (DLP)

Identify, monitor, and protect organization data at rest and in motion. DLP engine backed by FortiGuard AI feeds with over hundreds of pre-defined data patterns, updated to protect from day zero.

Thin Edge Extension *(coming soon)*

Secure thin edge locations (Access points and Extenders) that don't have on-premises firewall to block ransomware and malware with full cloud delivered management of thin edges

End-to-End Digital Experience Monitoring (DEM)

To assist administrators with troubleshooting remote user connectivity slowness with enhanced health check visibility of SaaS applications, endpoint device, network path, LAN health, reducing resolution times and ensuring positive user experience

The Fortinet Advantage

One Operating System

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.

Unified Management Plane

Comprehensive cloud hosted unified management which includes all elements of SSE, DEM, WLAN, SD-WAN integration leveraging a single analytics engine—FortiAnalyzer (data lake).

Single Unified Endpoint Agent

FortiClient (SASE agent) supports EndPoint Protection (EPP), ZTNA, SSE, CASB, DEM, Sandbox, vulnerability management and USB device control.

Flexible SASE Enforcement to all locations

Full support available for both agent and agentless based users. FortiSASE also extends to thin edges delivering holistic security to all users across all locations. Only SASE cloud with built-in SD-WAN and ADVPN (dynamic tunnels) functionality.

AI/ML Driven FortiGuard Services

Best in class security efficacy and zero-day threat protection derived from years of experience backed from AI powered FortiGuard threat intelligence irrespective of user location.

License Information

FortiSASE is delivered with a simple user-based licensing model which enables access to all SASE capabilities with industry's lowest Minimum Orderable Quantity of 50 users (MoQ).

Features List

Feature	Description
CORE SSE CAPABILITIES	
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.
API-CASB	Directly connected to leading SaaS providers to access usage and data stored in the cloud. This connection 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 ability 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.
Inline-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.
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.
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 730,000+ and we are able to leverage intelligence from this install base to deliver updates to FortiGuard threat intelligence labs, which in turn allows us to propagate any new day-zero threat signatures to all customers on a real time basis.
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.

Features List (continued)

Feature	Description
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.
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)

Feature	Description
External Threat Feeds	Support for creating external threat feeds of types such as threat hosts, DNS filter domains, and web filter FQDNs. Supported for both secure Internet access as well as secure private access use cases.
Endpoint Forensics Service	FortiGuard Forensics service to investigate potentially compromised endpoints for incident triage, investigation and response. Submit Endpoints for analysis directly from the FortiSASE portal with a downloadable report of verdict.
SOCaaS Integration	Ingest FortiSASE logs to Fortinet SOCaaS to help existing SOC teams analyze security events generated from FortiSASE, perform alert triage, and escalate confirmed threat notifications for appropriate expert response.
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. Support is available for wide range of OS including Windows, macOS, Linux, Android, and iOS.
Agentless connectivity	Agentless security is available for BYOD devices or devices where an agent cannot be downloaded such as Chromebooks, with the use of PAC files.
Endpoint protection	The Fortinet 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 approach provides you with endpoint security information, visibility, and the ability to control who and what accesses each device.
Thin Edge *(coming soon)*	FortiSASE supports management and integration of a FortiExtender and FortiAP (access point) configured as a LAN extension. By relying on FortiExtender or FortiAP instead of FortiClient to handle secure connectivity to FortiSASE, this solution essentially extends the single-user single-device FortiClient endpoint case to a multiuser, multi-device LAN environment. This feature 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), FortiIsolator (RBI), 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 third party identity providers such as Microsoft Entra ID and Okta can be integrated along with support for native FortiTrust ID. Support is also available for local, LDAP, and RADIUS.
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.

Features List (continued)

Feature	Description
MONITORING AND MANAGEMENT	
Single console	With the Unified SASE Console, administrators gain a centralized management platform with] 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.
Digital Experience Monitoring (DEM)	End to End Digital Experience Monitoring includes Last-mile monitoring to ensure fastest connection from each cloud location, and first mile monitoring to easily pinpoint issues down to the user's local network. Monitor endpoint information such as CPU, memory, hard drive, and network usage in real time.
Reporting and Analytics	You can generate data reports from logs by using the Reports feature. You can configure FortiSASE to regularly run reports at scheduled intervals, send as email attachments to select recipients, 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.
Assisted On-Boarding	Service delivery assistance to onboard users easily and have FortiSASE solution up and running quickly.