FortiSASE™

Highlights

- **Unified Management**, cloud hosted, includes protections to private and cloud applications.
- **Enterprise Security** with consolidated AI/ML-Powered FortiGuard 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
- **Expand SASE to Thin Edges**, only SASE vendor to support SASE integration with Wireless Access Points, Extenders

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.

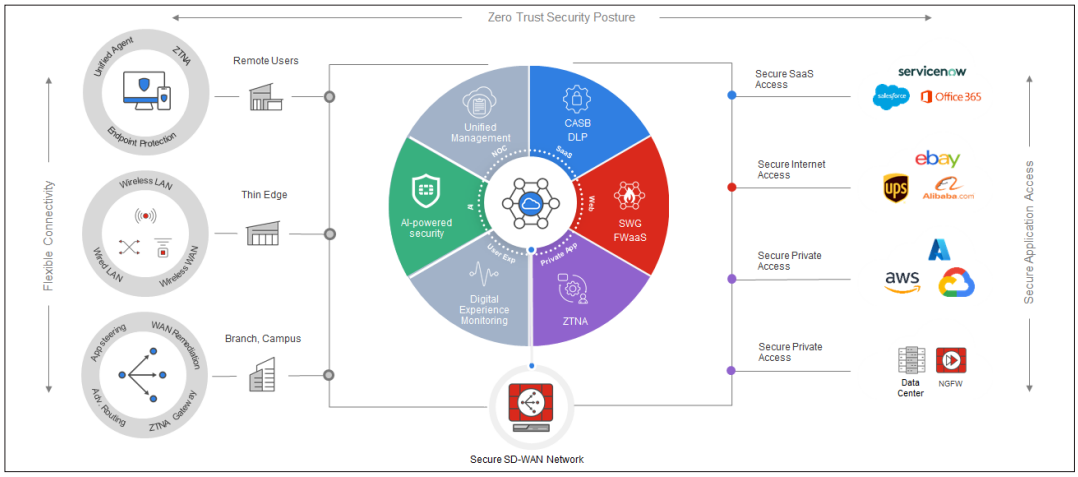
Available in

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 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, client agents and agentless (such as Chromebooks) 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)

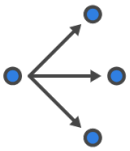
Leveraging the independently certified and acclaimed capabilities of FortiOS, our FWaaS technology enables high-performance SSL inspection, Sandbox, and advanced threat detection techniques from the cloud. It also establishes and maintains secure connections and analyzes in-bound and out-bound traffic 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

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). FortiSASE also supports applying FortiFlex entitlements generated from within the FortiFlex portal.

Additional details can be found at the FortiSASE and Zero Trust ordering guide here.