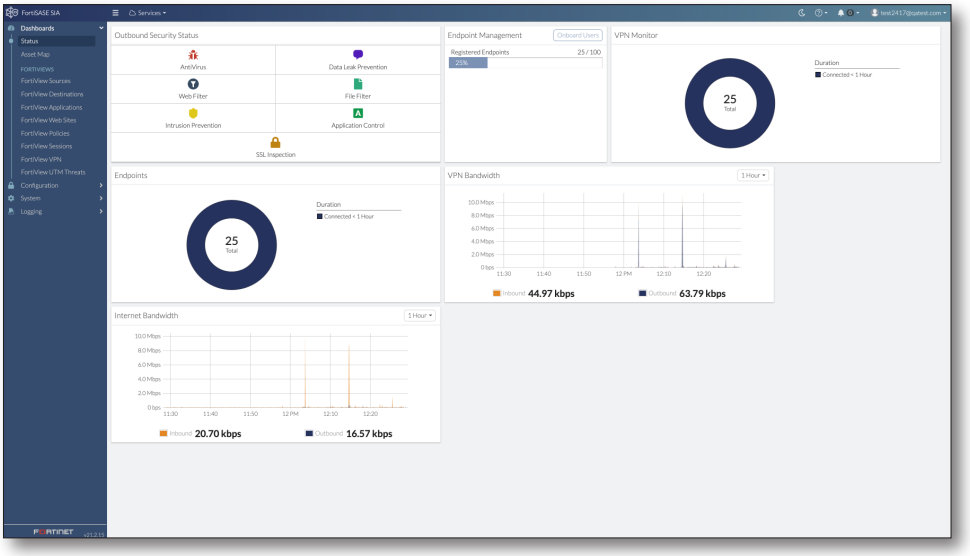
DATA SHEET

FortiSASE Secure Internet Access™

Available in:

Cloud

Cloud-Delivered Security for Remote Workforces



FortiSASE SIA™ is a cloud-delivered service specifically designed for **securing users outside of the corporate network.** This scalable cloud-based platform is powered by FortiOS allowing customers to extend FWaaS, IPS, DLP, SWG, and sandboxing to remote workforces.

FortiSASE SIA offers **up-to-date real-time protection** to terminate client traffic, scan traffic for known and unknown threats, and enforce corporate security policies for users working from anywhere.

FortiSASE SIA **simplifies the challenges** of managing and securing users who are out of the office by providing a best-in-class cloud-delivered threat protection service. FortiClient Agent tunnels user traffic to the nearest FortiSASE SIA datacenter for **security enforcement and protection.**

Security Challenges for Remote Workforces

Challenge

Remote workforces access the internet from home or from anywhere on the road to access business-critical applications without the firewall and security available in the office. These users remain a target of cyberthreats but can provide a greater threat to the corporate network and other users when the device connects by VPN or is brought back into the office.

Solution

Implement and enforce the unified networking and security policies at all network edges by extending on-premise policies to remote users and their devices with FortiSASE SIA.

Benefits

Consistent firewall and security policies at all times, regardless of a user's location.

Prevent corporate network infections by enforcing security policies for remote workforces with better user experience.

HIGHLIGHTS

SASE Delivery Model

FortiSASE SIA is a cloud-delivered security-as-a-service solution provided by Fortinet utilizing components of the Fortinet Security Fabric that allows users, regardless of location, to take advantage of firewall-as-a-service (FWaaS), secure web gateway (SWG), and other security features in an easy-to-consume package.

Powered By FortiOS

The FortiOS operating system is the heart of the Fortinet Security Fabric. It enables multiple security and networking technologies to work together seamlessly across all environments protecting users based on best-in-class threat intelligence along with improving user experience. This holistic approach eliminates security gaps for remote workforces and hastens responses to attacks and breaches.

World-Class Protection

FortiSASE SIA is powered by industry leading FortiGuard Labs research organization, delivering real-time protection to remote workforces. It does this by constantly analyzing real-world threat intelligence gathered from over 5.6 million globally deployed sensors. Advanced AI is then applied to identify abnormalities and suspicious patterns to generate new protections that are automatically distributed via native integration with FortiOS. This fully integrated and automated approach ensures timely and coordinated protection of known and unknown threats across the entire attack life cycle.

Scalable OPEX Model

Based on a per device, per annum pricing model, organizations can now predict a cost-to-business growth correlation and use of security instead of tying up capital in excess hardware.

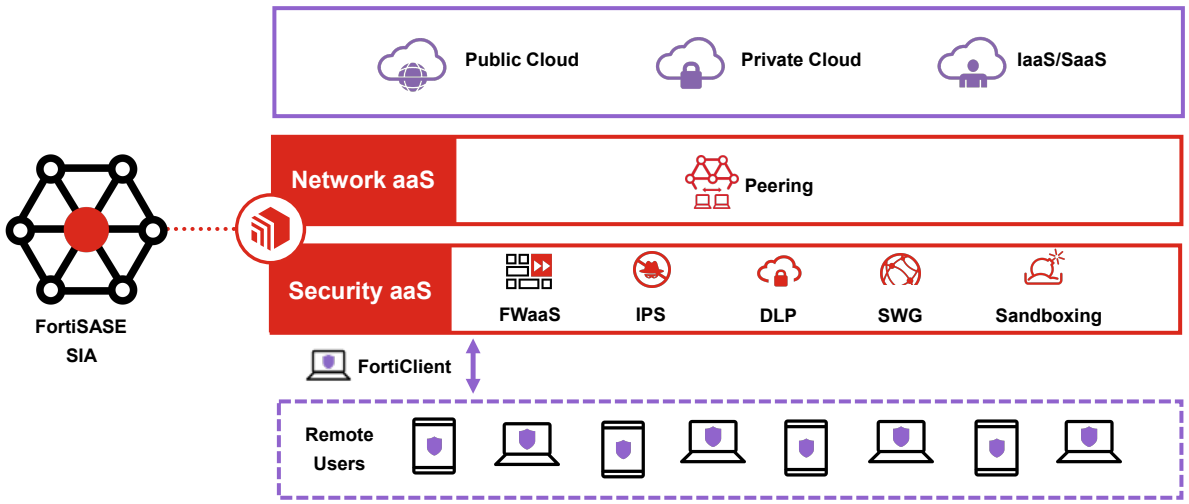
OVERVIEW

Enterprise Grade Security

Web and email are the two most common attack vectors for the delivery of malware into an organization and when users are out of the office, they are not as well protected as when within the organizational network. It is critical to ensure that the same level of security is employed while the user is remote as when they are within the organizational network.

Optimized Remote Workforce Security

FortiSASE SIA provides security-as-a-service for remote users while they are outside of the protection of the corporate network. FortiClient detects that the user is outside of the network and tunnels the traffic to the FortiSASE SIA Service where the corporate security policy can be enforced – removing the risk of corporate managed devices being unprotected on the internet.



FEATURES

Malware and Exploit Prevention

Antivirus with automated content updates, the latest malware and heuristic detection engines, and a proactive threat library protects against all known threats and variants. Content Pattern Recognition Language and new patented code recognition software protects against unknown variants and guaranteed SLAs to address severe malware threats.

FortiSandbox Cloud provides protection against unknown attacks using dynamic analysis and provides automated mitigation. FortiSandbox Cloud is able to take suspicious files and see what they do when executed. If they are malicious, FortiSandbox Cloud will create a new signature so that the firewall can stop future attacks immediately.

Millions of FortiClient and FortiSandbox users worldwide share information about known and unknown malware with FortiGuard's cloud-based threat intelligence platform. FortiGuard automatically shares the intelligence with FortiClient endpoints to protect against emerging threats

FortiClient Anti-Ransomware uses behavioral analytics to detect suspicious, ransomware-like behavior. If such behavior is detected, FortiClient can stop ransomware in its tracks, alerting the administrator and optionally auto-quarantine the infected endpoint so it is disconnected from the network and cannot infect other endpoints.

Encrypted Traffic Analysis

With 95% of Internet application traffic being encrypted, attackers try to take advantage and attempt to slip threats into the network without being detected. **SSL/TLS Inspection** is the ability to look inside encrypted traffic to inspect the contents in order to detect attacks that would otherwise be invisible. Deep inspection certificates are automatically distributed to endpoints to provide simplified management.

Continuous Threat Monitoring

Intrusion Prevention (IPS) FortiGuard Automated updates provide latest defenses against network-based threats. You get the latest defenses against stealthy network-level threats, a comprehensive IPS Library with thousands of signatures, flexible policies that enable full control of attack detection methods to suit complex security applications, resistance to evasion techniques proven by NSS Labs.

Filtering Services

The Internet has become a critical part of conducting business, however inappropriate Internet usage has led to lower productivity, inappropriate use of company resources, harassment, legal liability, and human resource issues. Fortinet's **FortiGuard Web Filtering Service** regulates and provides valuable insight into all web activities allowing customers to meet new Government Regulations, Educational Compliance, HR Policies, and Corporate Internet Usage Policies.

FortiGuard's cloud delivered and continually updated web content rating database with over 80 content categories powers one of the industry's most accurate web-filtering services.

Application Control

FortiGuard's App Control protects managed assets by controlling network application usage. The sophisticated detection signatures identify Apps, DB applications, web applications and protocols, both blocklist and allowlist approaches can allow or deny traffic. Flexible policies enable full control of attack detection methods.

Risk Detection

Data Loss Protection (DLP) monitor network traffic looking for sensitive information that should not leave the network. FortiSASE SIA scans the traffic against file format and content definitions, leveraging both standard data types as well as custom entries by the admin, to identify and stop files from leaking out.

Event Log Management

Real-time Logging and Analytics are provided by FortiSASE SIA which can be used to troubleshoot connectivity problems, investigate an incident, and audit for compliance. To help adhere to local regulations, you can select a specific geographic region in which to store logs. All logs can optionally be forwarded to an external logging service.

ORDER INFORMATION

Product	SKU	Description
FortiSASE SIA – 25 Endpoints	FC1-10-EMS05-372-01-DD	License Subscription for 25 Roaming Endpoints. Includes: FortiClient ZTNA Agent, EPP/APT and FortiSASE SIA Subscriptions (EMS hosted by FortiCloud) and 24×7 FortiCare, plus FortiCare Best Practice Service
FortiSASE SIA – 500 Endpoints	FC2-10-EMS05-372-01-DD	License Subscription for 500 Roaming Endpoints. Includes: FortiClient ZTNA Agent, EPP/APT and FortiSASE SIA Subscriptions (EMS hosted by FortiCloud) and 24×7 FortiCare, plus FortiCare Best Practice Service
FortiSASE SIA – 2,000 Endpoints	FC3-10-EMS05-372-01-DD	License Subscription for 2,000 Roaming Endpoints. Includes: FortiClient ZTNA Agent, EPP/APT and FortiSASE SIA Subscriptions (EMS hosted by FortiCloud) and 24×7 FortiCare, plus FortiCare Best Practice Service
FortiSASE SIA – 10,000 Endpoints	FC4-10-EMS05-372-01-DD	License Subscription for 10,000 Roaming Endpoints. Includes: FortiClient ZTNA Agent, EPP/APT and FortiSASE SIA Subscriptions (EMS hosted by FortiCloud) and 24×7 FortiCare, plus FortiCare Best Practice Service

FSI-DAT-R05-20210706