DATA SHEET

FortiSASE SIA™

Available in:

Appliance | Virtual Machine | Hosted | Cloud

Cloud-Delivered Security for Off-Net Clients

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, DNS, SWG, and sandboxing to Off-Net users. 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 anywhere.

FortiSASE SIA simplifies the challenges of managing and securing users who are out of the office by providing the same security policy protection whether On-Net or Off-Net via simple FortiClient Agent.

Off-Net Security Challenges

Problem

Off-Net users, overly reliant on VPN, access the Internet from home or from public places on the road without the firewall and security available in the office. Threats acquired at home or on the road are then traverse location and threaten the corporate network.

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 and zero trust access while Off-Net

HIGHLIGHTS

FortiOS

Accelerates network and user experience with continuous innovation and real-time application optimization for consistent application experience and advanced next generation firewall protection and prevention.

Broad Coverage of the Attack Surface

Covers the entire Security Fabric with an effective defense against advanced targeted attacks.

Built on a cohesive and extensible architecture working to protect network application layers and endpoint devices.

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.

Multi-Tenancy

Support for MSSP multi-tenancy deployment.

Delegated access for end-customers.

Centralized visibility and management.

World-Class Protection

Fortinet is a recognized leader in Next-Generation Firewall technology

FortiSASE SIA provides that same technology, backed by the same award winning FortiGuard Service in a cloud-based, easy-to-manage service.

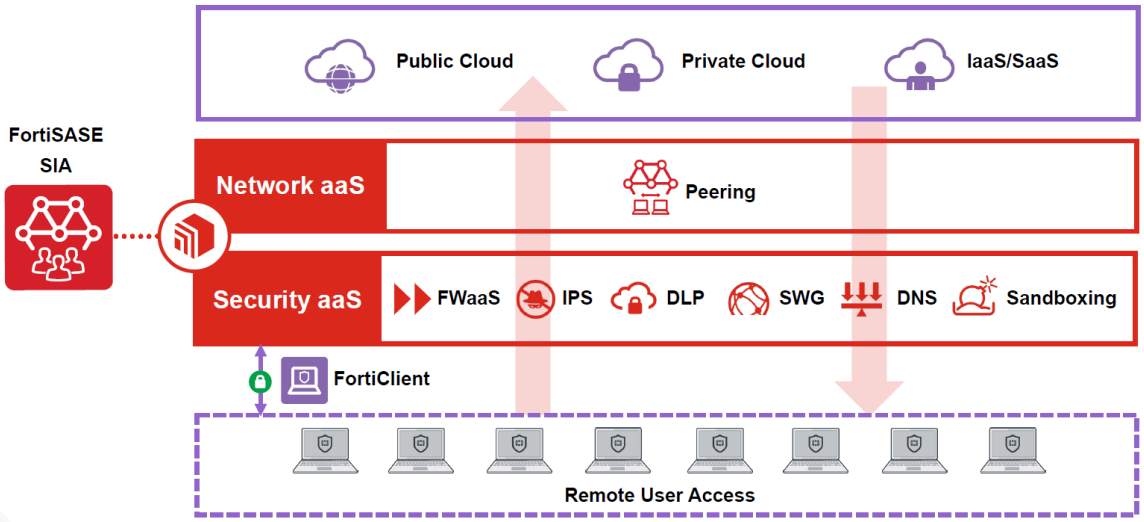
OVERVIEW

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 Off-Net as when they are within the organizational network.

Optimized Off-Net Security

FortiSASE SIA for Off-Net users provides security-as-a-service for users while they are outside of the protection of the corporate network. FortiClient can detect that the user is outside of the network and enforce that traffic is tunneled 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 Detection

Antivirus with automated content updates and latest malware and heuristic detection engines, 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.

Zero-Day Protection

Virus Outbreak Protection Service (VOS) closes the gap between antivirus updates with FortiSandbox Cloud analysis to detect and stop malware threats discovered between signature updates before they can spread throughout an organization, with real-time look-up to our Global Threat Intelligence database, providing you with the latest in malware protection.

Filtering Services

Web Filtering blocks and monitors web activities to assist customers with government regulations enforcement of corporate internet usage policies. FortiGuard's massive web-content rating databases power one of the industry's most accurate web-filtering services. Granular blocking and filtering provide web categories to allow, log, or block Comprehensive URL database provides rapid and comprehensive protection.

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.

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 blacklist and white list approaches can allow or deny traffic. Traffic shaping can be used to prioritize applications and flexible policies enable full control of attack detection methods.

Encrypted Traffic Analysis

SSL Inspection is the ability to look inside an SSL-encrypted traffic to inspect the contents. Using industry-mandated ciphers, FortiSASE SIA can apply all the standard traffic protections against SSL-encrypted traffic, which is now a majority of the traffic on the Internet.

FEATURES

Automated Rapid Detection

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.

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 proved by NSS Labs.

Malicious Code Removal

Content Disarm & Reconstruction (CDR) strips active content from files in real-time, creating a sanitized file and active content is treated as suspect and removed. CDR processes incoming files, deconstructs them, and removes any possibility of malicious content in your files that do not match firewall policies, fortifying your zero-day protection strategy.

Event Log Management

Real-time Logging & Audit trail is part of the FortiSASE SIA capabilities, providing a record of what happened that enables an audit team to evaluate and assess events within the cloud. This integrates with FortiSASE SIA's portal service configuration which provides logging analytics.

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-R02-20210310