

DATA SHEET

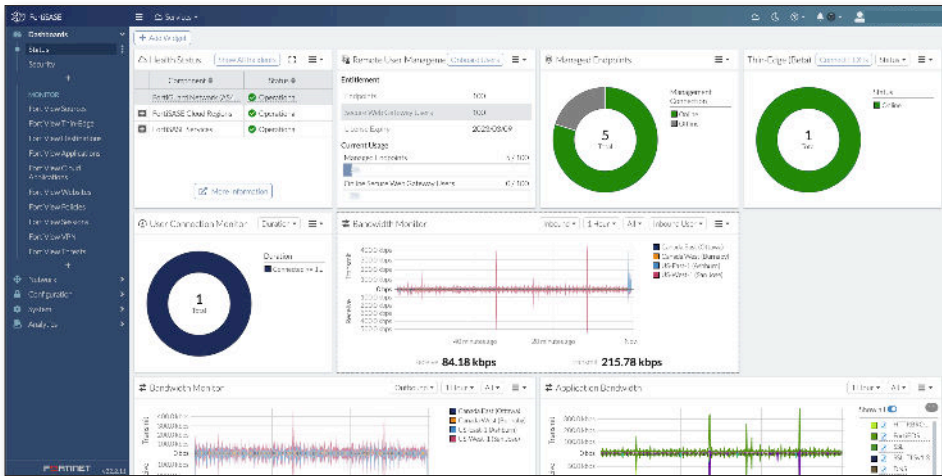
FortiSASE™

Available in:



Cloud

Scalable, Simple, and Secure Access for Remote Workforce



FortiSASE is a cloud-delivered security service designed for securing remote users. This highly-scalable cloud-based platform is powered by FortiOS allowing customers to extend FWaaS, SWG, IPS, DLP, and ZTNA to remote workforce.

FortiSASE simplifies the challenges of securing remote users with flexible deployment options with best-in-class cloud-delivered security service. You can forward traffic from FortiClient agent or use PAC file with explicit proxy for Secure Web Gateway usecase to redirect traffic to the nearest FortiSASE datacenter.

FortiSASE offers simple onboarding process and endpoint management. It enables efficient operations with Granular analytics, pre-generated and on-demand reports, including granular logging and events across user, endpoint, and VPN events for efficient troubleshooting.

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.

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 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 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.



Flexible and Scalable OPEX Pricing Models

Based on a per device or per user, 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.

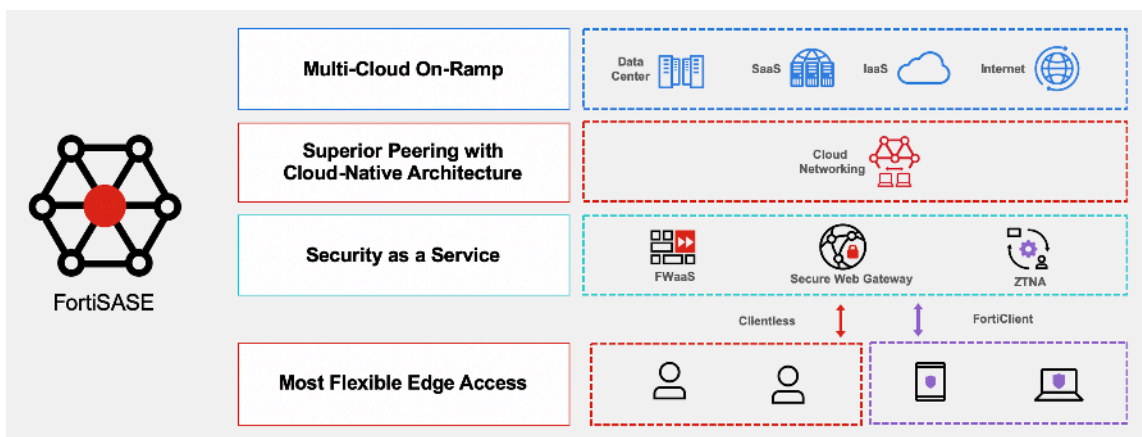
OVERVIEW

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 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 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 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 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.

ZTNA

With integrated ZTNA, FortiSASE offers secure private access to applications—whether they are in private datacenter or public clouds. Each session is initiated with an automatic, encrypted tunnel to FortiSASE for user and device posture check enabling granular policies based on specific user and application. It integrates with popular identity providers such as Azure AD and Okta, and you can also use multifactor authentication to provide an additional layer of security.



ORDER INFORMATION

| UNIT | SKU | DESCRIPTION |
|--|------------------------|---|
| FortiSASE Remote - Device License | | |
| FortiSASE Remote - Device License | FC1-10-EMS05-434-01-DD | FortiSASE Remote Agent for 25 endpoints (includes ZTNA Agent, EPP/APT and FortiSASE Remote Agent Subscriptions with EMS hosted by FortiCloud) and 24x7 FortiCare. |
| | FC2-10-EMS05-434-01-DD | FortiSASE Remote Agent for 500 endpoints (includes ZTNA Agent, EPP/APT and FortiSASE Remote Agent Subscriptions with EMS hosted by FortiCloud) and 24x7 FortiCare. |
| | FC3-10-EMS05-434-01-DD | FortiSASE Remote Agent for 2000 endpoints (includes ZTNA Agent, EPP/APT and FortiSASE Remote Agent Subscriptions with EMS hosted by FortiCloud) and 24x7 FortiCare. |
| | FC4-10-EMS05-434-01-DD | FortiSASE Remote Agent for 10 000 endpoints (includes ZTNA Agent, EPP/APT and FortiSASE Remote Agent Subscriptions with EMS hosted by FortiCloud) and 24x7 FortiCare. |
| FortiSASE Remote User License | | |
| FortiSASE Remote - User License | FC1-10-EMS05-488-01-DD | FortiSASE Remote - User Subscription for 25 Users (includes agentless Secure Web Gateway plus 10Mbps per user) and 24x7 FortiCare. |
| | FC2-10-EMS05-488-01-DD | FortiSASE Remote - User Subscription for 500 Users (includes agentless Secure Web Gateway plus 10Mbps per user) and 24x7 FortiCare. |
| | FC3-10-EMS05-488-01-DD | FortiSASE Remote - User Subscription for 2000 Users (includes agentless Secure Web Gateway plus 10Mbps per user) and 24x7 FortiCare. |
| | FC4-10-EMS05-488-01-DD | FortiSASE Remote - User Subscription for 10 000 Users (includes agentless Secure Web Gateway plus 10Mbps per user) and 24x7 FortiCare. |


www.fortinet.com

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full all covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

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 (<https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf>) and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy (https://secure.ethicspoint.com/domain/media/en/gui/19775/Whistleblower_Policy.pdf).