



FortiSandbox™

Multi-layer proactive threat mitigation



FortiSandbox

FortiSandbox 1000D, 3000D, FortiSandbox-VM and FortiSandbox Cloud

Multi-layer proactive threat mitigation

Today's most sophisticated cybercriminals are increasingly bypassing traditional antimalware solutions and inserting advanced persistent threats deep within networks. These highly targeted attacks evade established signature-based detection by masking their malicious nature in many ways — compression, encryption, polymorphism, the list of techniques goes on. Some have even begun to evade virtual “sandbox” environments using VM detection, “time bombs” and more. Fighting today's attacks requires a comprehensive and integrated approach — more than antimalware. More than a virtual sandbox. More than a separate monitoring system.

FortiSandbox offers a robust combination of proactive detection and mitigation, actionable threat insight and integrated and automated deployment. At its foundation is a unique, dual-level sandbox which is complemented by Fortinet's award-winning antimalware and optional integrated FortiGuard threat intelligence. Years of Fortinet threat expertise is now packaged up and available on site or in the cloud via FortiSandbox.

Proactive Detection and Mitigation

Suspicious codes are subjected to multi-layer pre-filters prior to execution in the virtual OS for detailed behavioral analysis. The highly effective pre-filters include a screen by our AV engine, queries to cloud-based threat databases and OS-independent simulation with a code emulator, followed by execution in the full virtual runtime environment. Once a malicious code is detected, granular ratings along with key threat intelligence is available, a signature is dynamically created for distribution to integrated products and full threat information is optionally shared with FortiGuard Labs for the update of global threat databases.

Actionable Insight

All classifications — malicious and high/medium/low risk — are presented within an intuitive dashboard. Full threat information from the virtual execution — including system activity, exploit efforts, web traffic, subsequent downloads, communication attempts and more — is available in rich logs and reports.

The ultimate combination of proactive mitigation, advanced threat visibility and comprehensive reporting.

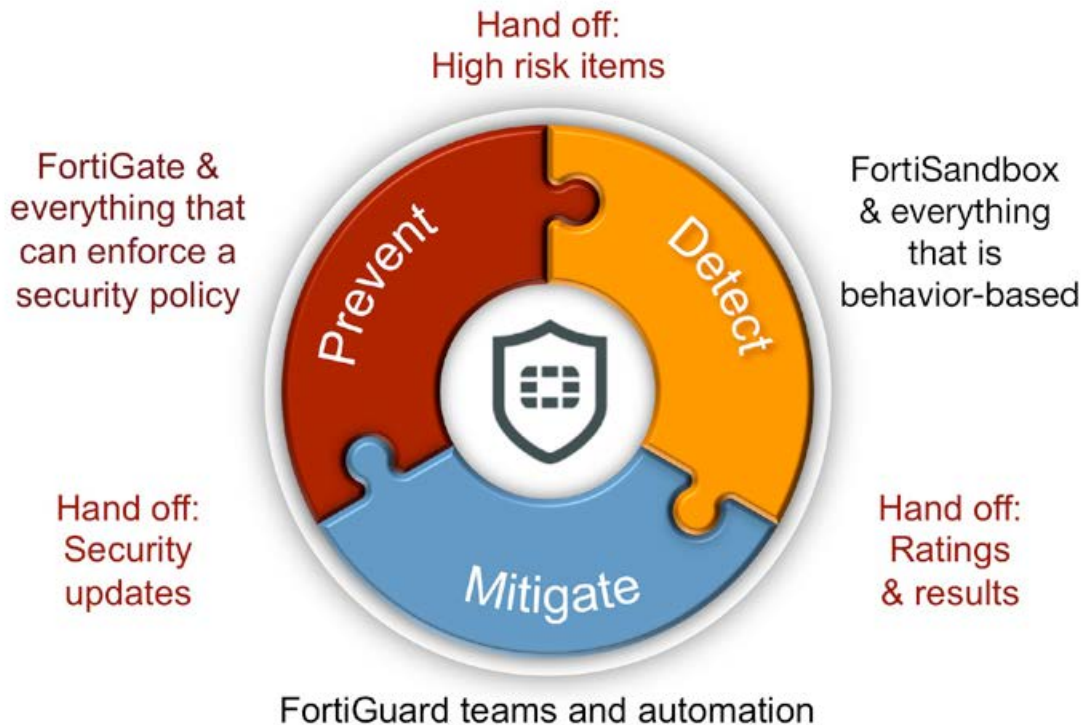
- Secure virtual runtime environment exposes unknown threats
- Unique multi-layer prefilters aid fast and effective threat detection
- Rich reporting provides full threat lifecycle visibility
- Inspection of many protocols in one appliance simplifies deployment and reduces cost
- Integration and automation with Fortinet threat prevention products enhances rather than duplicates security infrastructure
- Independent testing and certification validates effectiveness



ADVANCED THREAT PROTECTION FRAMEWORK

The most effective defense against advanced targeted attacks is founded on a cohesive and extensible protection framework. The Fortinet framework uses security intelligence across an integrated solution of traditional and advanced security tools for network, application and endpoint security, and threat detection to deliver actionable, continuously improving protection.

Fortinet integrates the intelligence of FortiGuard Labs into FortiGate next generation firewalls, FortiMail secure email gateways, FortiClient endpoint security, FortiSandbox advanced threat detection, and other security products to continually optimize and improve the level of security delivered to organizations with a Fortinet solution.



Prevent Attacks

Fortinet next generation firewalls, secure email gateways, web application firewalls, endpoint security and similar solutions use security such as antivirus, web filtering, IPS, and other traditional security techniques to quickly and efficiently prevent known threats from impacting an organization.

Detect and Analyze Threats

FortiSandbox and other advanced detection techniques step in to detect “Zero-day” threats and sophisticated attacks, delivering risk ratings and attack details necessary for remediation.

Mitigate Impact and Improve Protection

In a Fortinet solution, detection findings can be used to trigger prevention actions to ensure the safety of resources and data until remediation is in place. Finally, the entire security ecosystem updates to mitigate any impact from future attacks through the strong, integrated threat intelligence research and services of FortiGuard Labs.

DEPLOYMENT OPTIONS

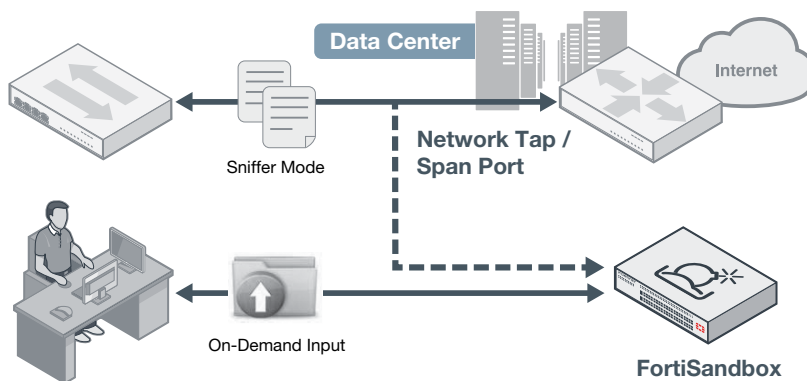
Easy Deployment

FortiSandbox supports inspection of many protocols in one unified solution, thus simplifies network infrastructure and operations. Further, it integrates with FortiGate as a new capability within your existing security framework.

The FortiSandbox is the most flexible threat analysis appliance in the market as it offers various deployment options for customers' unique configurations and requirements. Organizations can also have all three input options at the same time.

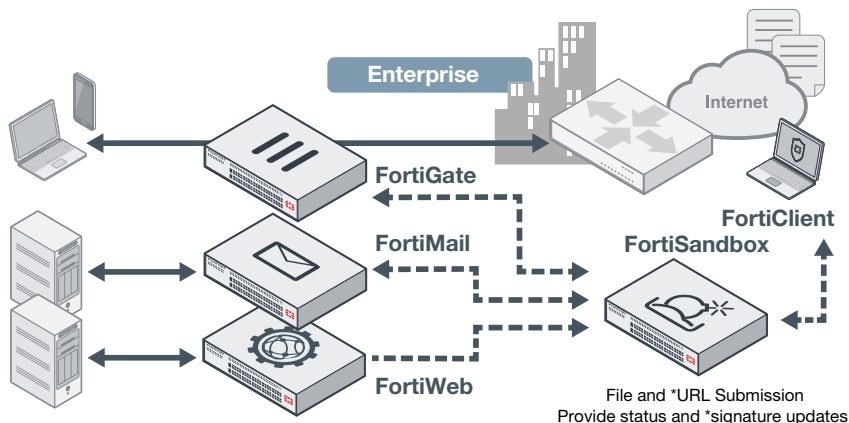
Standalone

This deployment mode relies on inputs from spanned switch ports or network taps. It may also include administrators' on-demand file uploads using the GUI. It is the most suitable infrastructure for adding protection capabilities to existing threat protection systems from various vendors.



Integrated

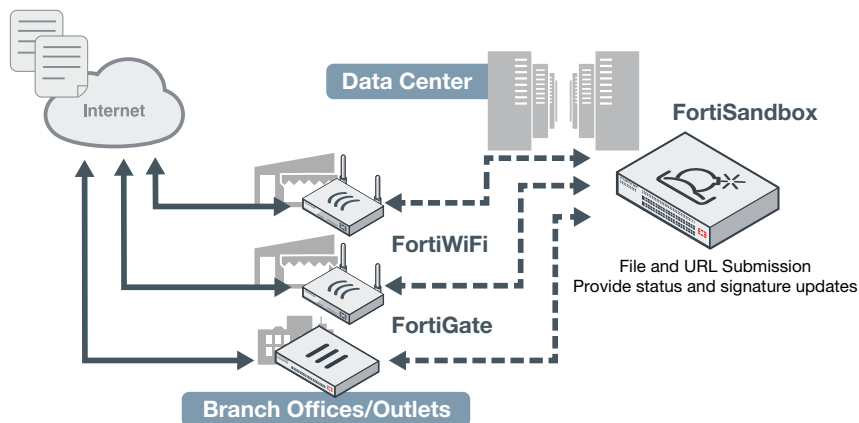
Various Fortinet products, namely FortiGate, FortiMail, FortiWeb and FortiClient can intercept and submit suspicious content to FortiSandbox when they are configured to interact with FortiSandbox. The integration will also provide timely remediation and reporting capabilities to those devices.



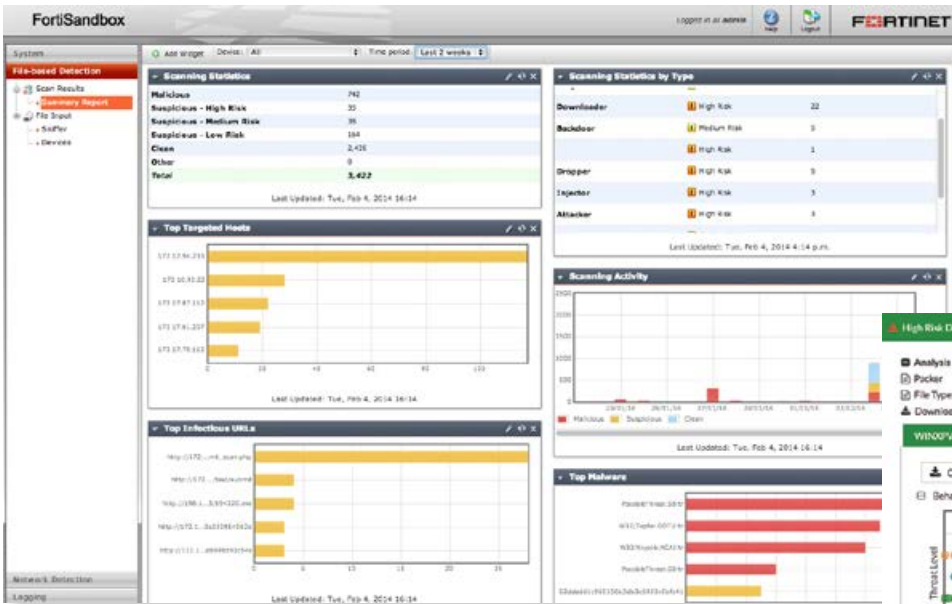
* Not applicable to FortiWeb

Distributed

This deployment is attractive for organizations that have distributed environments, where FortiGates are deployed in the branch offices and submit suspicious files to a centrally-located FortiSandbox. This setup yields the benefits of lowest TCO and protects against threats in remote locations.



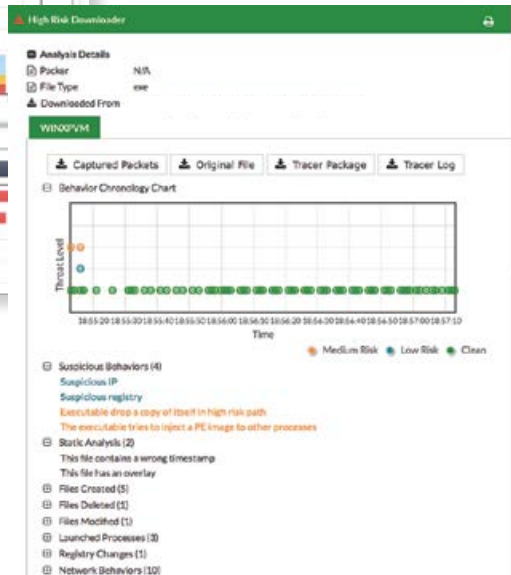
FEATURES



Dashboard widgets — real-time threat status

VM Sandboxing

Complement your established defenses with cutting-edge capability — analyzing suspicious and high-risk files in a contained environment to uncover the full attack lifecycle using system activity and callback detection.

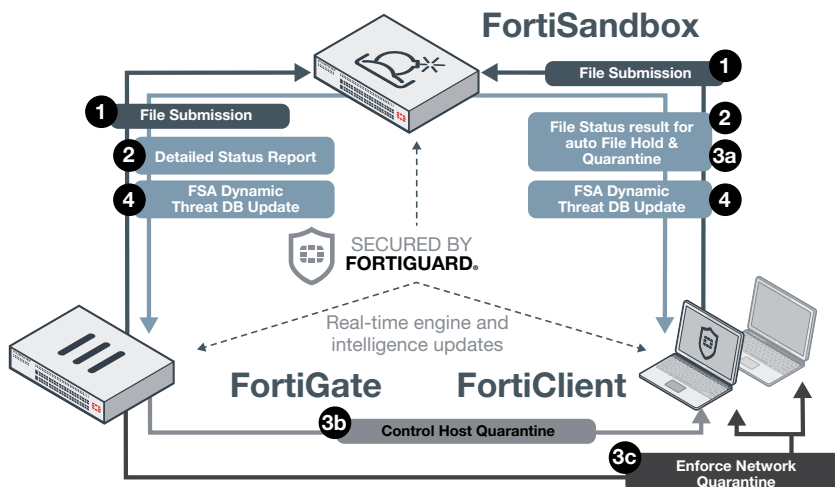


File Analysis Tools

Reports with captured packets, original file, tracer log and screenshot provide rich threat intelligence and actionable insight after files are examined. This is to speed up remediation and updated protection.

Remediation

Fortinet’s ability to uniquely integrate various products with FortiSandbox offers automatic protection with incredibly simple setup. Once a malicious code is determined, the analyzer will develop and forward the dynamically generated signature to all registered devices and clients. These devices then examine subsequent files against the latest DB.



Query

- 1 File submission for Analysis
- 2 Respective analysis results are returned

Remediation

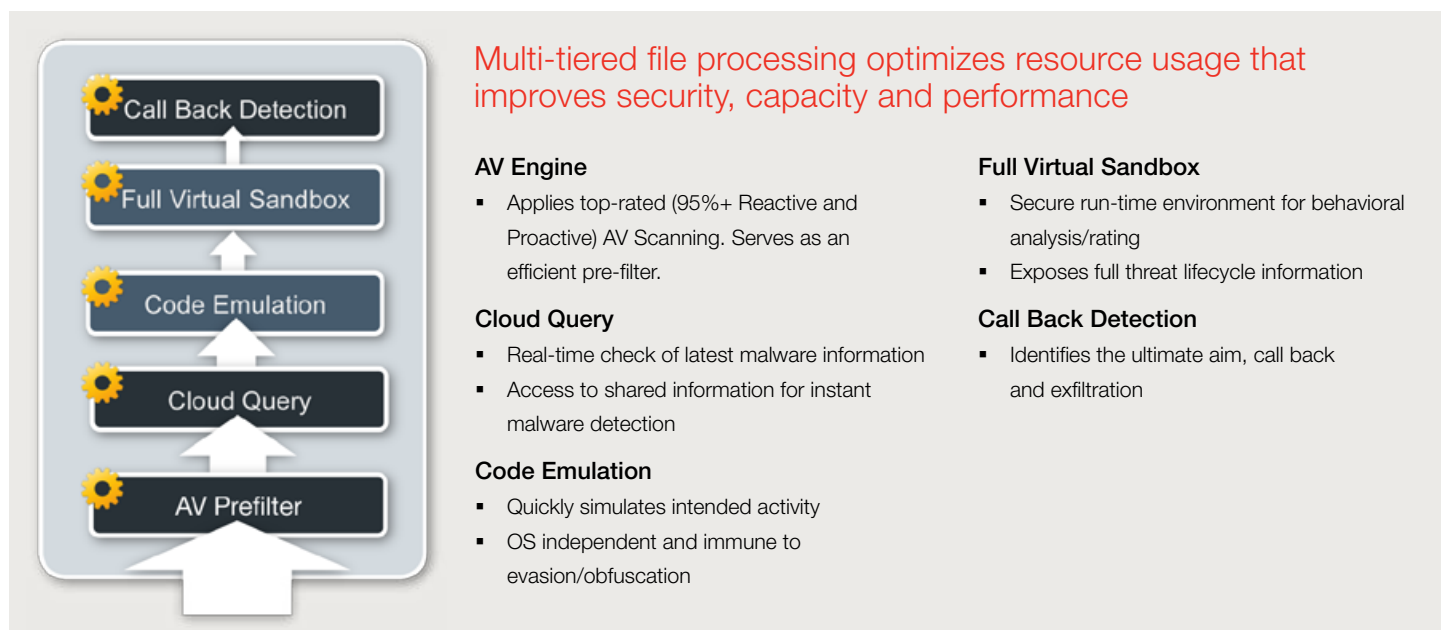
- 3a Auto File Quarantine on Host with option to hold file until result
- 3b Manual Host Quarantine by Admin
- 3c Manual Source IP Quarantine using Firewall

Protection

- 4 Proactive dynamic Threat DB update to gateway and host

Examination and remediation integration between FortiSandbox, FortiGate and FortiClient.

FEATURES



FEATURES SUMMARY

Administration

- Supports WebUI and CLI configurations
- Multiple administrator account creation
- Configuration file backup and restore
- Notification email when malicious file is detected
- Weekly report to global email list and FortiGate administrators
- Centralized search page which allows administrators to build customized search conditions
- Frequent signature auto-updates
- Automatic check and download new VM images
- VM status monitoring
- Radius Authentication for administrators

Networking/Deployment

- Static Routing Support
- File Input: Offline/sniffer mode, On-demand file upload, file submission from integrated device(s)
- Option to create simulated network for scanned file to access in a closed network environment
- High-Availability Clustering support
- Port monitoring for fail-over in a cluster

Systems Integration

- File Submission input: FortiGate, FortiClient, FortiMail, FortiWeb
- File Status Feedback and Report: FortiGate, FortiClient, FortiMail, FortiWeb
- Dynamic Threat DB update: FortiGate, FortiClient, FortiMail
 - Periodically push dynamic DB to registered entities.
 - File checksum and malicious URL DB
- Update Database proxy: FortiManager
- Remote Logging: FortiAnalyzer, syslog server
- Web-based API with which users can upload samples to scan indirectly
- Bit9 end point software integration

Advanced Threat Protection

- Virtual OS Sandbox:
 - Concurrent instances
 - OS type supported: Windows XP, Windows 7, Windows 8.1, Windows 10 and Android
 - Anti-evasion techniques: sleep calls, process and registry queries
 - Callback Detection: malicious URL visit, Botnet C&C communication and attacker traffic from activated malware
 - Download Capture packets, Original File, Tracer log and Screenshot

File type support:

- Archived: .tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj
- Executable files: (eg: .exe, .dll), PDF, Windows Office Document, AdobeFlash and JavaArchive (JAR) files
- Script files: .js, .bat, .vbs, .ps1, .cmd
- Media files: .avi, .mpeg, .mp3, .mp4

Protocols/applications supported:

- Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB
- Integrated mode with FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM and their equivalent SSL encrypted versions
- Integrated mode with FortiMail: SMTP, POP3, IMAP
- Integrated mode with FortiWeb: HTTP

Customize VMs with support file types support

- Isolate VM image traffic from system traffic
- Network threat detection in Sniffer Mode: Identify Botnet activities and network attacks, malicious URL visit
- Scan SMB/NFS network share and quarantine suspicious files. Scan can be scheduled
- Scan embedded URLs inside document files
- Integrate option for third party Yara rules
- Option to auto-submit suspicious files to cloud service for manual analysis and signature creation
- Option to forward files to a network share for further third-party scanning
- Files checksum whitelist and blacklist option
- URLs submission for scan and query from emails and files

Monitoring and Report

- Real-Time Monitoring Widgets (viewable by source and time period options): Scanning result statistics, scanning activities (over time), top targeted hosts, top malware, top infectious urls, top callback domains
- Drilldown Event Viewer: Dynamic table with content of actions, malware name, rating, type, source, destination, detection time and download path
- Logging — GUI, download RAW log file
- Report generation for malicious files: Detailed reports on file characteristics and behaviors — file modification, process behaviors, registry behaviors, vm snapshot, behavior chronology chart
- Further Analysis: Downloadable files — Sample file, Sandbox tracer logs and PCAP capture

SPECIFICATIONS

	FSA-1000D	FSA-3000D
Hardware		
Form Factor	2 RU	2 RU
Total Network Interfaces	6x GE RJ45 ports, 2x GE SFP slots	4x GE RJ45 ports, 2x GE SFP slots 2x 10 GE SFP+ slots
Storage Capacity	4 TB (max. 8 TB)	8 TB (max. 16 TB)
Power Supplies	2x Redundant PSU	2x Redundant PSU
System		
VM Sandboxing (Files/Hour)	160	560
AV Scanning (Files/Hour)	6,000	15,000
Number of VMs	8	28
Dimensions		
Height x Width x Length (inches)	3.5 x 17.2 x 14.5	3.3 x 19.0 x 29.7
Height x Width x Length (mm)	89 x 437 x 368	84 x 482 x 755
Weight	27.60 lbs (12.52 kg)	71.5 lbs (32.5 kg)
Environment		
Power Consumption (Average / Maximum)	15 / 138 W	392 / 614.6 W
Maximum Current	100V/5A, 240V/3A	110V/10A, 220V/5A
Heat Dissipation	471 BTU/h	2131.14 BTU/h
Power Source	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz
Humidity	5–95% non-condensing	20–90% non-condensing
Operation Temperature Range	32–104°F (0–40°C)	50–95°F (10–35°C)
Storage Temperature Range	-13–158°F (-25–70°C)	-40–149°F (-40–65°C)
Compliance		
Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	
FortiSandbox Cloud		
System		
VM Sandboxing (Files/Hour)	Unrestricted	
AV Scanning (Files/Hour)	Unrestricted	
Number of VMs	Not applicable	

FortiSandbox-VM		
Hardware Requirements		
Hypervisor Support	VMware ESXi version 5.1 or later	
Virtual CPUs (Minimum / Maximum)	4 / Unlimited (Fortinet recommends that the number of vCPUs match the number of Windows VM +4.)	
Memory Support (Minimum / Maximum)	8 GB / Unlimited	
Virtual Storage (Minimum / Maximum)	30 GB / 16 TB	
Total Virtual Network Interfaces (Minimum)	6	
System		
VM Sandboxing (Files/Hour)	Hardware dependent	
AV Scanning (Files/Hour)	Hardware dependent	
Number of VMs	4 to 54 (Upgrade via appropriate licenses)	
File Submission		
Manual File Upload for Analysis	Yes	–
Sniffer Mode	Yes	–
FortiGate	All models*, *FortiOS V5.0.4+	All models*, *FortiOS V5.2.3+
FortiClient	Windows only, FortiClient OS V5.4	–
FortiMail	All models, FortiMail OS V5.1+	All models, FortiMail OS V5.3+
FortiWeb	All models, FortiWeb OS V5.4+	–
Status Reporting		
File Status Feedback	Yes, for all supported entities	Yes, for FortiGate and FortiMail only
File Detailed Report	Yes, for all supported entities	Yes, for FortiGate only
Dynamic Threat DB update		
FortiGate	All models*, *FortiOS V5.4+	All models*, *FortiOS V5.4+
FortiClient	Windows only, FortiClient OS V5.4	–
FortiMail	All models, FortiMail OS V5.3+	–

*some may require CLI configuration

ORDER INFORMATION

Product	SKU	Description
FortiSandbox 1000D	FSA-1000D	Advanced Threat Protection System — 6x GE RJ45, 2x GE SFP slots, redundant PSU, 8 Windows licenses and 1 Microsoft Office license included.
FortiSandbox 3000D	FSA-3000D	Advanced Threat Protection System — 4x GE RJ45, 2x GE SFP slots, 2x 10 GE SFP+ slots, redundant PSU, 28 Windows licenses and 3 Microsoft Office licenses included.
FortiSandbox-VM	FSA-VM-BASE	Base license for stackable FortiSandbox-VM. 4 Windows licenses and 1 Microsoft Office license included. FSA-VM maximum expansion limited to 54 total VMs.
FortiSandbox Cloud Service	FC-10-00XXX-123-02-12	FortiSandbox Cloud Service Subscription (SKU varied by FortiGate models).
Optional Accessories		
1 GE SFP SX Transceiver Module	FG-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP LX Transceiver Module	FG-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FG-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FG-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.



GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne 06560
Alpes-Maritimes, France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990