DATA SHEET

FortiSandbox™

FortiSandbox 500F, 1000F/-DC, 2000E, 3000E, VM, Cloud Hosted, and Public Cloud

Top-rated AI-powered FortiSandbox is part of Fortinet's breach protection solution that integrates with Fortinet's Security Fabric platform to address the rapidly evolving and more targeted threats including ransomware, crypto-malware, and others across a broad digital attack surface. Specifically, it delivers real-time actionable intelligence through the automation of zero-day, advanced malware detection and response.

Broad Coverage of the Attack Surface with Security Fabric

Effective defense against advanced targeted attacks through a cohesive and extensible architecture working to protect networks, emails, web applications, and endpoints from campus to the public cloud, and Industrial Control System (ICS) devices found in an OT (Operational Technology) environment.

Automated Zero-day, Advanced Malware Detection and Response

Native integration and open APIs automate the submission of objects from Fortinet and third-party vendor protection points, and the sharing of threat intelligence in real time for immediate threat response and reduction on the reliance on scarce security resources.

Certified and Top Rated

Constantly undergoes rigorous, real-world independent testing such as NSS Labs Breach Detection Systems (BDS) and Breach Prevention Systems (BPS), and ICSA Labs Advanced Threat Defense (ATD), and consistently earns top marks in dealing with known and unknown threats.

Provides Breach Protection for

- Remote office
- Branch
- Campus
- Data Center
- Public cloud (AWS, Azure)

Third-Party Certifications

NSS LABS RECOMMENDED

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

FortiGuard Security Services

www.fortiguard.com

FortiCare Worldwide 24/7 Support

support.fortinet.com

Features

AI-powered Sandbox Malware Analysis

Complement your established defenses with a two-step AI-based sandboxing approach. Suspicious and at-risk files are subjected to the first stage of analysis that quickly identifies known and emerging malware through FortiSandbox's AI-powered static analysis. Second stage analysis is done in a contained environment to uncover the full attack lifecycle leveraging behavior-based AI that is constantly learning new malware techniques and automatically adapting malware behavioral indicators making FortiSandbox's dynamic analysis detection engine more efficient and effective against new zero-day threats. Figure 1 depicts new threats discovered via AI-based dynamic analysis.

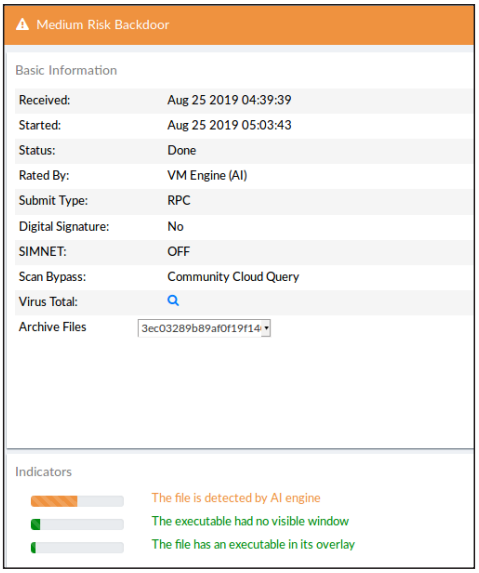

Figure 1: AI-based Dynamic Analysis

Mitre ATT&CK-based Reporting and Investigative Tools

FortiSandbox provides detailed analysis report that maps discovered malware techniques to Mitre ATT&CK framework with built-in powerful investigative tools that allows Security Operations (SecOps) team to download captured packets, original file, tracer log, and malware screenshot, and STIX 2.0 compliant IOCs that not only provides rich threat intelligence but actionable insight after files are examined (see Figure 2).

In addition, SecOps team can choose to record a video of the entire malware interaction or manually interact with the malware in a simulated environment.

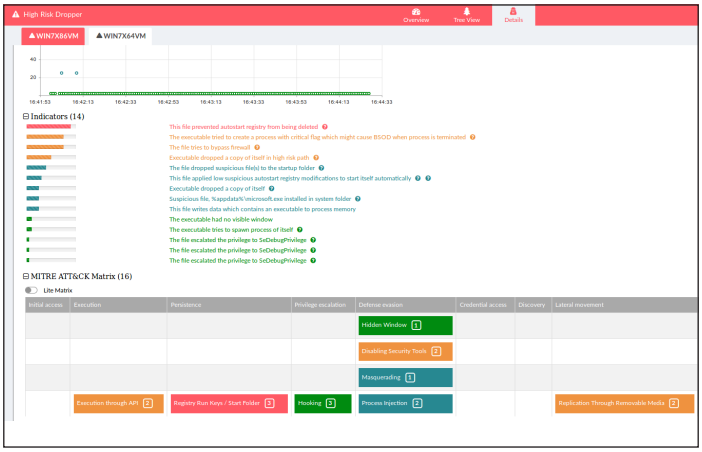

Figure 2: Mitre ATT&CK matrix with built-in tools

Automated Breach Protection

Fortinet's ability to uniquely integrate various products with FortiSandbox through the Security Fabric platform automates your breach protection strategy with an incredibly simple setup. Once a malicious code is identified, the FortiSandbox will return risk ratings and the local intelligence is shared in real time with Fortinet, Fabric-Ready Partner, and third-party security solutions to mitigate and immunize against new advanced threats. The local intelligence can optionally be shared with Fortinet threat research team, FortiGuard Labs, to help protect organizations globally. Figure 3 steps through the flow on the automated mitigation process.

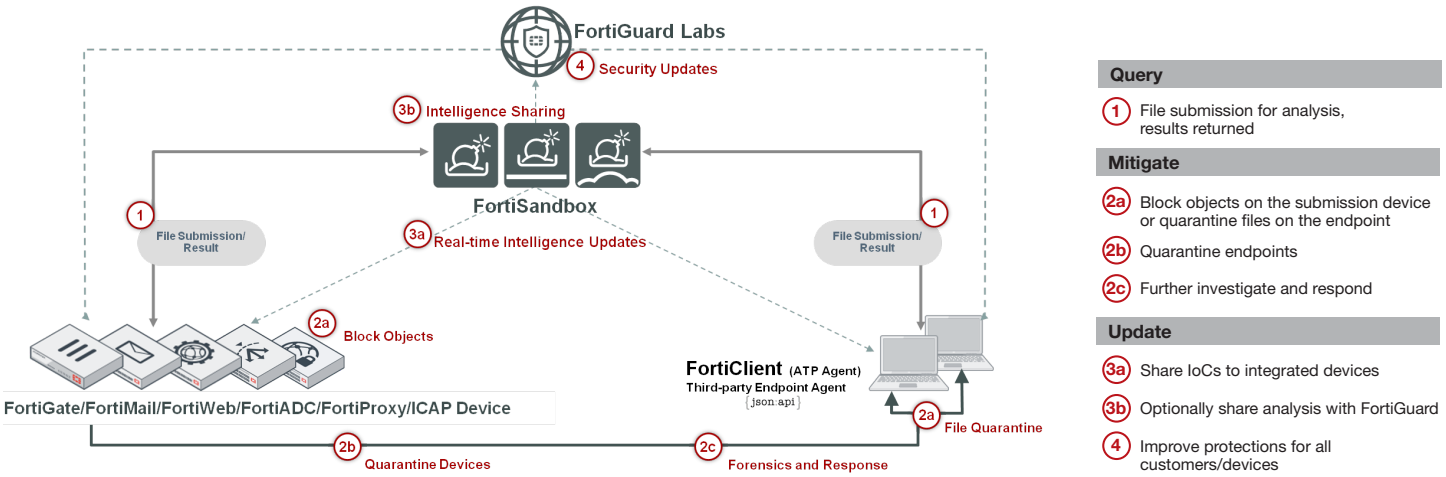

Figure 3: FortiSandbox threat mitigation workflow

Deployment Options

Easy Deployment

FortiSandbox supports inspection of many protocols in one unified solution, thus simplifying both network and security, infrastructure and operations while reducing overall Total Cost of Ownership. Further, it integrates within the Security Fabric platform, adding a layer of advanced threat protection to your existing security architecture.

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 choose to combine these deployment options.

Integrated

FortiSandbox natively integrates with FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy, FortiClient (ATP agent), and Fabric-Ready Partner solutions, and via JSON API or ICAP with third-party security vendors to intercept and submit suspicious content to FortiSandbox. The integration will also provide timely remediation and reporting capabilities to those devices.

This integration extends to other FortiSandboxes to allow instantaneously sharing of real-time intelligence. This benefits large enterprises that deploy multiple FortiSandboxes in different geo-locations. This zero-touch automated model is ideal for holistic protection across different borders and time zones.

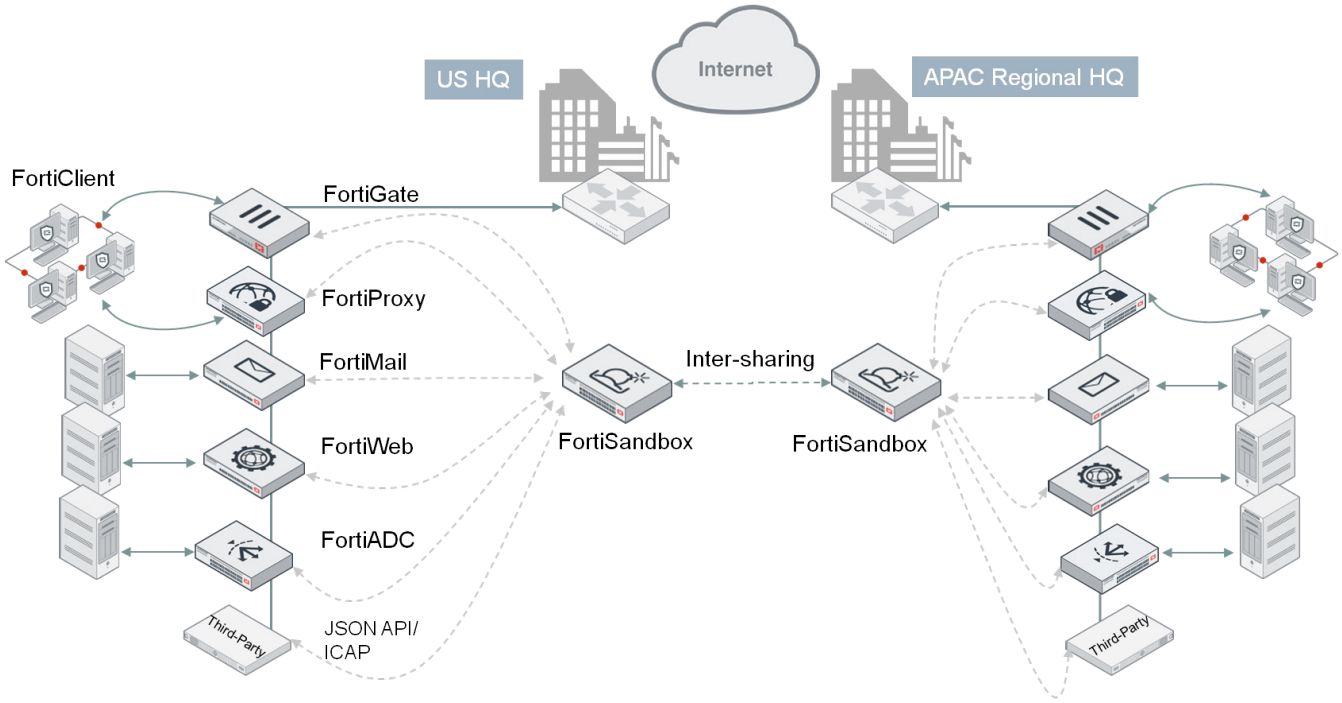

Figure 4: Integrated Deployment

Standalone

This FortiSandbox deployment mode accepts inputs from spanned switch ports or network taps, and emails via MTA or BCC mode. It may also include SecOps analyst on-demand file uploads or scanning of file repositories via CIFs, NFS, AWS S3 and Azure Blob through the GUI. It is the ideal option to enhancing an existing multi-vendor threat protection approach.

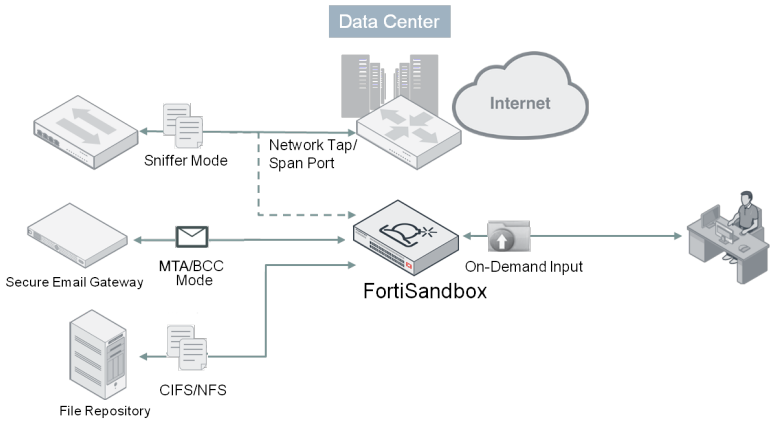

Figure 5: Standalone Deployment

Features Summary

ADMINISTRATION

- ✓ Supports GUI and CLI configurations
- ✓ Multiple administrator account creation
- ✓ Configuration file backup and restore
- ✓ Notification emails when a malicious file is detected
- ✓ Weekly reports to global email lists and FortiGate administrators
- ✓ Centralized search page allowing administrators to build customized search conditions
- ✓ Frequent signature auto-updates
- ✓ Automatic check and download of 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 a 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, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent)
- ✓ File Status Feedback & Report:
  - FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent)
- ✓ Dynamic Threat DB update:
  - FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent)
  - Periodically push dynamic DB to registered entities
  - File checksum and malicious URL DB
- ✓ Update Database proxy for FortiManager
- ✓ Remote Logging: FortiAnalyzer, FortiSIEM, syslog server
- ✓ JSON API to automate uploading samples and downloading actionable malware indicators to remediate
- ✓ Certified third-party integration:
  - CarbonBlack, Ziften, SentinelOne
- ✓ Inter-sharing of IOCs between FortiSandboxes

ADVANCED THREAT PROTECTION

- ✓ Inspection of new threats including ransomware and password protected malware mitigation
- ✓ AI-based Static Code analysis identifying possible threats within non-running code
- ✓ Heuristic/Pattern/Reputation-based analysis
- ✓ Virtual OS Sandbox:
  - AI-based behavior analysis
  - Concurrent instances
  - OS type supported: Windows 7, Windows 8.1, Windows 10, macOS, Linux, Android, and ICS systems
  - Anti-evasion techniques: sleep calls, process, registry queries, and more
  - Callback Detection: malicious URL visit, botnet C&C communication, and attacker traffic from activated malware
  - Download Capture packets, Original File, Tracer log, and Screenshot
  - Sandbox Interactive Mode
  - Video-recording of malware interaction
- ✓ File type support: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .elf, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, .rl, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
- ✓ Protocols/applications supported:
  - Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB
  - MTA/BCC mode: SMTP
  - 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
  - Integrated mode with ICAP Client: HTTP
- ✓ OT services supported: tftp, modbus, s7comm, http, snmp, bacnet, ipmi
- ✓ Customize VMs for supporting various file types
- ✓ Isolate VM image traffic from system traffic
- ✓ Network threat detection in Sniffer Mode: Identify Botnet activities and network attacks, malicious URL visit
- ✓ Manual or scheduled scan SMB/NFS, AWS S3 and Azure Blob storage shares and quarantine of suspicious files.
- ✓ Scan embedded URLs inside document files
- ✓ Option to integrate with 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
- ✓ Reports and Logging—GUI, download pdf and raw log file
- ✓ Report generation for malicious files:
  - Mitre ATT&CK-based report on malware techniques such as file modification, process behaviors, registry behaviors, and network behaviors.
- ✓ Further Analysis: Downloadable files—sample file, sandbox tracer logs, PCAP capture and indicators in STIX 2.0 format

Specifications

	FSA-500F	FSA-1000F/-DC	FSA-2000E	FSA-3000E
Hardware				
Network Interfaces	4x GE RJ45 ports	4x GE RJ45 ports, 4x GE SFP slots	4x GE RJ45 ports, 2x 10 GE SFP+ slots	4x GE RJ45 ports, 2x 10 GE SFP+ slots
Storage	1x 1 TB	2x 1 TB	2x 2 TB	4x 2 TB
Power Supplies	1x PSU	1x PSU, Optional 2x PSU	2x Redundant PSU	2x Redundant PSU (Hot Swappable)
System Performance and Capacity				
Number of VMs	6*	14*	24*	56*
Sandbox Pre-Filter Throughput (Files/Hour)[1]	4,500	7,500	12,000	15,000
VM Sandboxing Throughput (Files/Hour)	120	280	480	1,120
Real-world Effective Throughput (Files/Hour)	600[2]	1,400[2]	2,400[2]	5,600[2]
Sniffer Throughput	500 Mbps	1 Gbps	4 Gbps	8 Gbps
MTA Capacity	5,000 emails/hour	10,000 emails/hour	15,000 emails/hour	35,000 emails/hour
Dimensions and Power				
Height x Width x Length (inches)	1.73 x 17.24 x 12.63	1.73 x 17.24 x 22.83	3.46 x 17.24 x 20.87	3.5 x 17.2 x 29
Height x Width x Length (mm)	44 x 438 x 320	44 x 438 x 580	88 x 438 x 530	89 x 437 x 738
Weight	18.72 lbs (8.5 kg)	25 lbs (11.34 kg)	27 lbs (12.25 kg)	43 lbs (19.52 kg)
Form Factor	1 RU	1 RU	2 RU	2 RU
Power Supply (AC/DC)	100–240V AC, 50/60 Hz	100–240V AC, 50/60 Hz / -48VDC	100–240V AC, 50/60 Hz	100–240V AC, 50/60 Hz
Maximum Current (AC/DC)	100/8A, 240V/4A	100V/5A, 240V/3A / -48VDC/9A	100V/8A, 240V/4A	100V/9.8A, 240V/5A
Power Consumption (Average/Maximum)	30.1 / 76.3 W	66.93 / 116.58 W	164.7 / 175.9 W	538.6 / 549.6 W
Heat Dissipation	260.34 BTU/h	397.75 BTU/h	600.17 BTU/h	1,943.82 BTU/h
Environment				
Operation Temperature Range	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)	50–95°F (10– 35°C)
Storage Temperature Range	-4–158°F (-20–70°C)	-40–158°F (-40–70°C)	-4–158°F (-20–70°C)	-40–158°F (-40–70°C)
Humidity	5–90% non-condensing	5–90% non-condensing	5–90% non-condensing	8–90% (non-condensing)
Compliance				
Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST			

	FORTISANDBOX-VM		FORTISANDBOX CLOUD
Hardware Requirements			
Hypervisor Support	VMware ESXi, Linux KVM CentOS, Microsoft Hyper-V, Nutanix, AWS, and Azure		N.A
Virtual CPUs (Minimum / Maximum)	4 / Unlimited (Fortinet recommends that the number of vCPUs match the number of Windows VM +4)		N.A
Memory Support (Minimum / Maximum)	8 GB / Unlimited		N.A
Virtual Storage (Minimum / Maximum)	30 GB / 16 TB		N.A
Total Virtual Network Interfaces (Minimum)	6		N.A
System Performance			
Sniffer Throughput	1 Gbps		N.A
Sandbox Pre-filter Throughput (Files/Hour)[1]	Hardware dependent		**
	Local VMs	**Cloud VMs**	
Number of VMs	8 VMs/nodes, up to 99 nodes/cluster	5 (up to 200 Windows Cloud VMs)	**
VM Sandboxing Throughput (Files/Hour)	Hardware dependent	100 (up to 4,000)	**
Real-world Effective Throughput (Files/Hour)[2]	Hardware dependent	500 (up to 20,000)[2]	**

Note: All performance values are "up to" and vary depending on the environment and system configuration.

[1] FortiSandbox pre-filtering is powered by FortiGuard Intelligence.

[2] Measured based on real-world web and email traffic when both pre-filter and dynamic analysis are working consecutively.

* 2(FSA-500F)/2(FSA-1000F/-DC)/4(FSA-2000E)/8(FSA-3000E) Windows VM licenses included with hardware, remaining are sold as an upgrade license.

** Please refer to FortiSandbox Cloud Service description.

FortiSandbox 500F

FortiSandbox 1000F/-DC

FortiSandbox 2000E

FortiSandbox 3000E

Integration Matrix

		FORTIGATE	FORTICLIENT	FORTIMAIL	FORTIWEB	FORTIADC	FORTIPROXY
FSA Appliance and VM	File Submission	*FortiOS V5.0.4+	FortiClient for Windows OS V5.4+	FortiMail OS V5.1+	FortiWeb OS V5.4+	FortiADC OS V5.0+	FortiProxy OS V1.0+
	File Status Feedback	*FortiOS V5.0.4+	FortiClient for Windows OS V5.4+	FortiMail OS V5.1+	FortiWeb OS V5.4+	FortiADC OS V5.0+	FortiProxy OS V1.0+
	File Detailed Report	*FortiOS V5.4+	FortiClient for Windows OS V5.4+	FortiMail OS V5.1+	–	FortiADC OS V5.0+	FortiProxy OS V1.0+
	Dynamic Threat DB Update	*FortiOS V5.4+	FortiClient for Windows OS V5.4+	FortiMail OS V5.3+	FortiWeb OS V5.4+	FortiADC OS V5.0+	FortiProxy OS V1.0+
FortiSandbox Cloud	File Submission	*FortiOS V5.2.3+	FortiClient for Windows OS V6.2+	FortiMail OS V5.3+	FortiWeb OS 5.5.3+	–	FortiProxy OS V1.0+
	File Status Feedback	*FortiOS V5.2.3+	FortiClient for Windows OS V6.2+	FortiMail OS V5.3+	FortiWeb OS 5.5.3+	–	FortiProxy OS V1.0+
	File Detailed Report	*FortiOS V5.2.3+	–	–	–	–	FortiProxy OS V1.0+
	Dynamic Threat DB Update	*FortiOS V5.4+	FortiClient for Windows OS V6.2+	FortiMail OS V5.3+	FortiWeb OS 5.5.3+	–	FortiProxy OS V1.0+

*some models may require CLI configuration

Order Information

Product	SKU	Description
FortiSandbox 500F	FSA-500F	Advanced Threat Protection System - 4 x GE RJ45, 2 licensed Windows/Linux/Android VMs with Win7, Win10 and (1) MS office licenses included. Upgradable to a maximum of 6 VMs, refer to FSA-500F-UPG-LIC-4 and/or FC-10-FS5HF-176-02-DD SKU.
FortiSandbox 1000F/-DC	FSA-1000F FSA-1000F-DC*	Advanced Threat Protection System - 4 x GE RJ45, 4 x GE SFP slots, 2 licensed Windows/Linux/Android VMs with Win7 , Win10 and (1) MS office licenses included. Upgradable to a maximum of 14 licensed VMs, refer to FSA-1000F-UPG-LIC-6 and/or FC-10-FS1KF-176-02-DD SKU. Redundant PSU (optional), refer to SP-FSA1000F-PS SKU.
FortiSandbox 2000E	FSA-2000E	Advanced Threat Protection System - 4 x GE RJ45, 2 x 10GbE SFP+ Slots, redundant PSU, 4 licensed Windows/Linux/Android VMs with Win7 , Win8 , Win10 and (1) MS office licenses included. Upgradable to a maximum of 24 VMs, refer to FSA-2000E-UPG-LIC-10 and/or FC-10-SA20K-176-02-DD SKU
FortiSandbox 3000E	FSA-3000E	Advanced Threat Protection System - 4 x GE RJ45, 2 x 10GbE SFP+ Slots, redundant PSU, 8 licensed Windows/Linux/Android VMs with Win7 , Win8 , Win10 and (1) MS office licenses included. Upgradable to a maximum of 56 VMs, refer to FSA-3000E-UPG-LIC-16 and/or FC-10-SA30K-176-02-DD SKU.
FortiSandbox-VM	FSA-VM-00	FortiSandbox-VM Virtual Appliance with 0 VMs included and maximum expansion limited to 8 total VMs per node, up to 99 nodes per cluster.
FortiSandbox Windows Cloud VM	FC-10-FSA01-195-02-DD	FortiSandbox Windows Cloud VM Service for (5) Windows VMs and maximum expansion limited to (200) Windows Cloud VMs per FortiSandbox VM.
FortiSandbox macOS Cloud VM	FC-10-FSA01-192-02-DD	macOS Cloud VM Service for (2) macOS X VMs and maximum expansion limited to (8) macOS X VMs per FortiSandbox (Appliance / VM).
FortiSandbox Cloud Service	FC-10-XXXXX-100-02-DD	FortiGuard Advanced Malware Protection (AMP) including Antivirus, Mobile Malware and FortiSandbox Cloud Service. (SKU varied by FortiGate models).
	FC-10-XXXXX-123-02-12	FortiSandbox Cloud Service Subscription (SKU varied by FortiMail/FortiWeb models).
	FC1-15-EMS01-298-02-DD	FortiSandbox Cloud license subscription for 25 endpoints. Includes Sandbox Agent with On-Prem/Cloud Sandbox subscription, Central Management and 24x7 Support. (SKU for FortiClient).
	FC1-10-XXXXX-620-02-DD	SWG Protection - Web Filtering, DNS Filtering, Application Control, DLP, AV, Botnet (IP/Domain), Sandbox Cloud. (SKU varied by FortiProxy 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.
AC Power Supply	SP-FSA1000F-PS	AC power supply for FDC-1000F, FIS-1000F, FSA-1000F modules only.
DC Power Supply	SP-FSA1000F-DC-PS	DC power supply for FSA-1000F-DC module only.

* Available in Q3 2020

FORTINET®

www.fortinet.com