DATA SHEET

FortiSandbox™

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

Fortinet's top-rated FortiSandbox is at the core of the Advanced Threat Protection (ATP) solution that integrates with Fortinet's Security Fabric to address the rapidly evolving and more targeted threats across a broad digital attack surface. Specifically, it delivers real-time actionable intelligence through the automation of zero-day, advanced malware detection and mitigation.

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 cloud.

Automated Zero-day, Advanced Malware Detection and Mitigation

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 and consistently earns top marks in dealing with known and unknown threats.

Deployment Modes

Standalone
Integrated

FortiGuard Security Services

www.fortiguard.com

FortiCare Worldwide 24/7 Support

support.fortinet.com

Third-Party Certifications

Features

Sandbox Malware Analysis

Complement your established defenses with a two-step sandboxing approach. Suspicious and at-risk files are subjected to the first stage of analysis with Fortinet's award-winning AV engine, FortiGuard global intelligence query*, and code emulation. Second stage analysis is done in a contained environment to uncover the full attack lifecycle using system activity and callback detection. Figure 1 depicts new threats discovered in real time.

In addition to supporting FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy, FortiClient (ATP agent) and Fabric-Ready Partner submission, third-party security vendor offerings are supported through a well-defined open API set.

* a real time IoC check for emerging threats (known good and bad) within the FortiGuard intelligence community

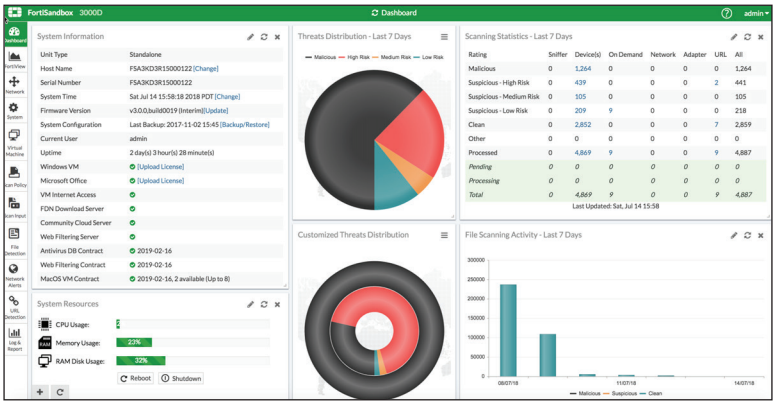

Figure 1: Widget-based real-time threat status dashboard

Reporting and Investigative Tools

Reports with captured packets, original file, tracer log, and screenshot provide rich threat intelligence and actionable insight after files are examined (see Figure 2). This is to speed up remediation.

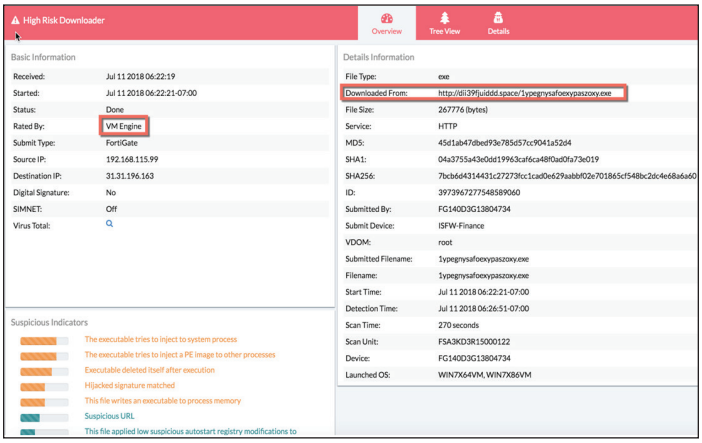

Figure 2: Detailed malware report with built-in tools

Threat Mitigation

Fortinet's ability to uniquely integrate various products with FortiSandbox through the Security Fabric offers automatic protection with 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 and third-party vendor-registered devices and clients to remediate 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.

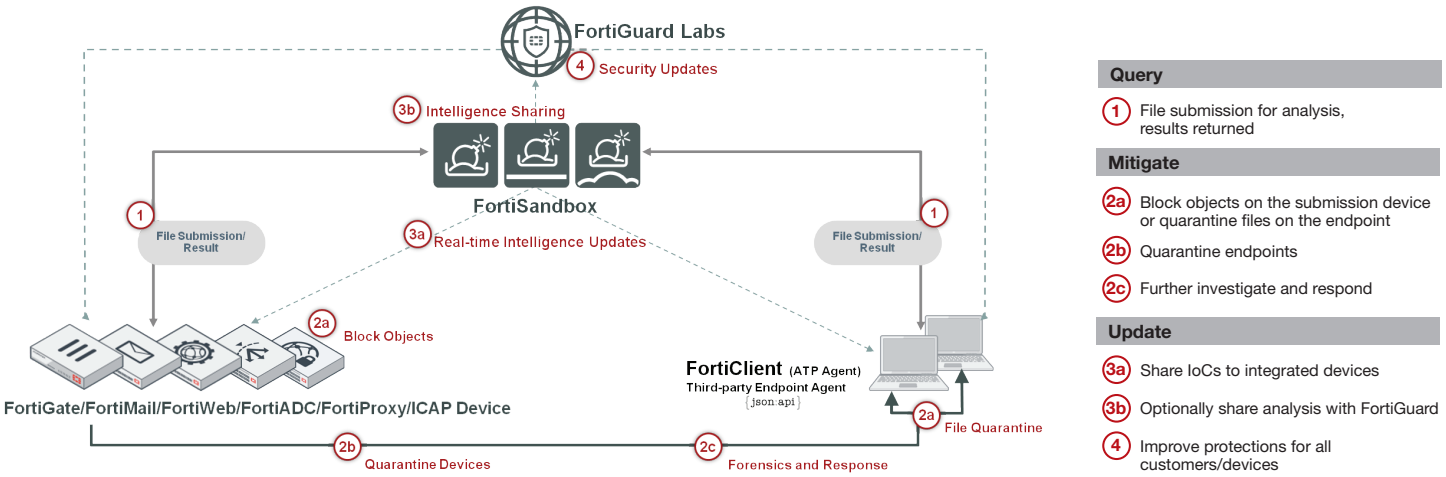

Figure 3: FortiSandbox threat mitigation workflow

Deployment Options

Easy Deployment

FortiSandbox supports inspection of many protocols in one unified solution, thus simplifies network infrastructure and operations. Further, it integrates within the Security Fabric adding a layer of advanced threat protection to your existing security architecture.

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 choose to combine these deployment options.

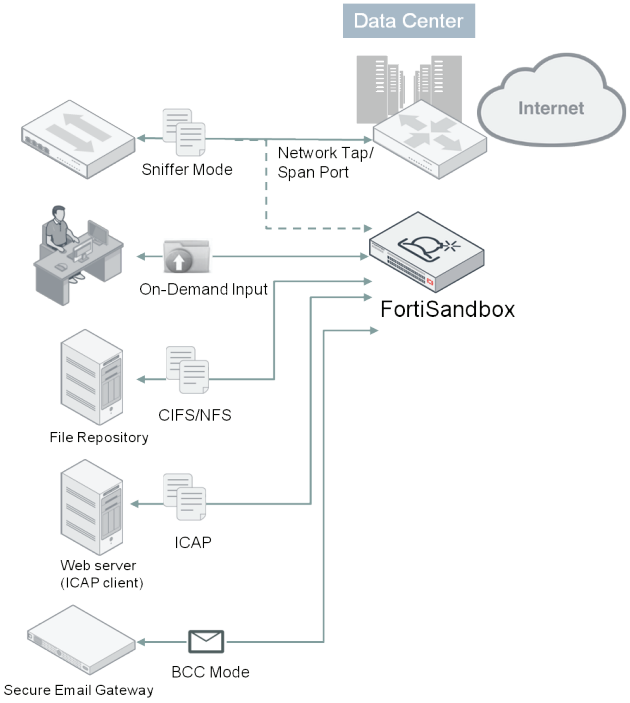

Figure 4: Standalone Deployment

Standalone

This FortiSandbox deployment mode accepts inputs as an ICAP server or from spanned switch ports or network taps. It may also include administrators' on-demand file uploads or scanning of file respositories via CIFs or NFS through the GUI. It is the ideal option to enhancing an existing multi-vendor threat protection approach.

Integrated

Fortinet products, such as FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent) and third-party security vendors 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.

This integration extends to other FortiSandboxes to allow instantaneous 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.

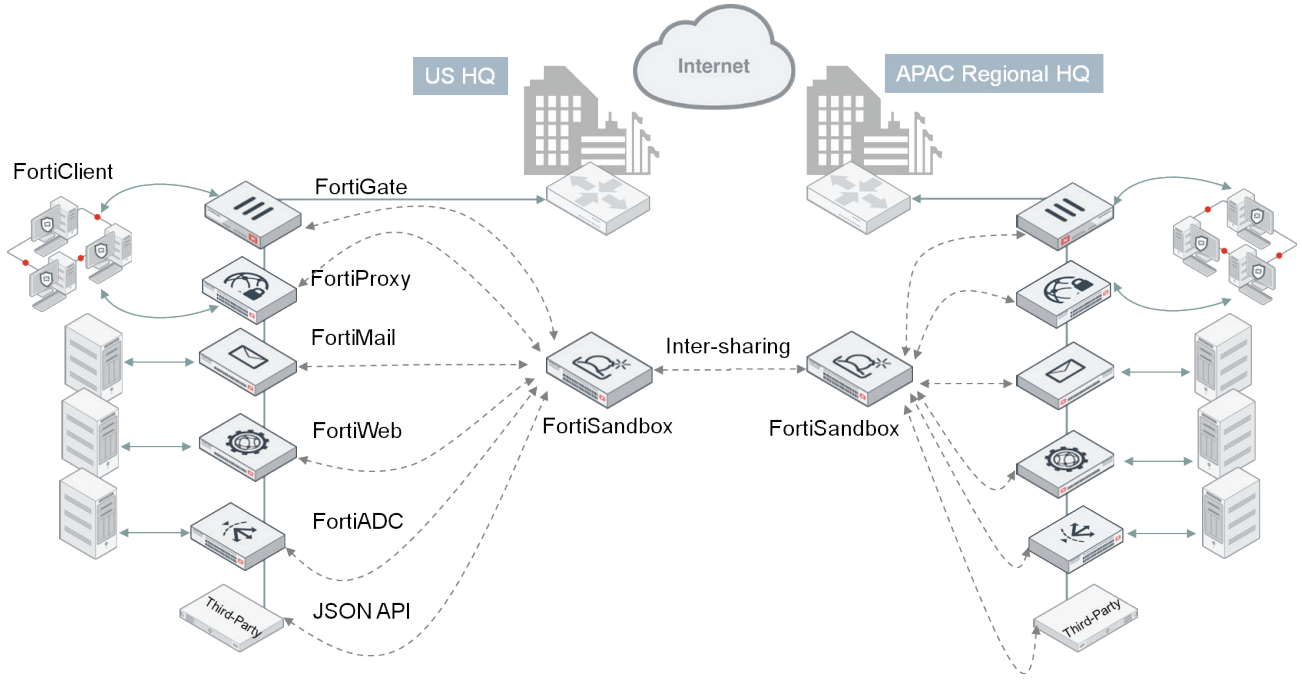

Figure 5: Integrated Deployment

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, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent)
File Status Feedback and 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: FortiManager
Remote Logging: FortiAnalyzer, syslog server
JSON API to automate the process of 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
Static Code analysis identifying possible threats within non-running code
Heuristic/Pattern/Reputation-based analysis
Virtual OS Sandbox: – Concurrent instances – OS type supported: Windows XP*, Windows 7, Windows 8.1, Windows 10, macOS, 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 – Sandbox Interactive Mode

* Supported in a custom VM

File type support: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .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, url, .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 – 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
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
Scan SMB/NFS network share and quarantine suspicious files. Scan can be scheduled
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
Logging — GUI, download RAW log file
Report generation for malicious files: Detailed reports on file characteristics and behaviors – file modification, process behaviors, registry behaviors, network behaviors, vm snapshot, behavior chronology chart
Further Analysis: Downloadable files — sample file, sandbox tracer logs, PCAP capture and indicators in STIX format

Specifications

	FSA-500F	FSA-1000F	FSA-2000E	FSA-3000E
Hardware				
Form Factor	1 RU	1 RU	2U	2 RU
Total 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
System Performance				
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] 360[3]	1,400[2] 840[3]	2,400[2] 1,440[3]	5,600[2] 3,360[3]
Sniffer Throughput	500 Mbps	1 Gbps	4 Gbps	8 Gbps
Dimensions				
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)
Environment				
Power Consumption (Average / Maximum)	30.1 / 76.3 W	66.93 / 116.58 W	164.7 / 175.9 W	538.6 / 549.6 W
Maximum Current	100/8A, 240V/4A	100V/5A, 240V/3A	100V/8A, 240V/4A	100V/9.8A, 240V/5A
Heat Dissipation	260.34 BTU/h	397.75 BTU/h	600.17 BTU/h	1,943.82 BTU/h
Power Source	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz
Humidity	5–90% non-condensing	5–90% non-condensing	5–90% non-condensing	8–90% (non-condensing)
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)
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 version 5.1 or later, Linux KVM CentOS 7.2 or later, AWS (On-Demand and BYOL)		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], 300 (up to 12,000)[3]	**

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

* 2(FSA-500F)/2(FSA-1000F)/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

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+	–	FortiMail OS V5.3+	FortiWeb OS 5.5.3+	–	FortiProxy OS V1.0+
	File Status Feedback	*FortiOS V5.2.3+	–	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+	–	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 — 4x GE RJ45, 2 licensed VMs with Win7, Win10 and (1) MS Office license included. Upgradable to a maximum of 6 VMs.
FortiSandbox 1000F	FSA-1000F	Advanced Threat Protection System — 4x GE RJ45, 2x GE SFP slots, 2 VMs with Win7, Win10 and (1) MS Office license included. Upgradable to a maximum of 14 licensed VMs. Refer to FSA-1000F-UPG-LIC-6 or FC-10-FS1KF-176-02-DD SKU.
FortiSandbox 2000E	FSA-2000E	Advanced Threat Protection System — 4x GE RJ45, 2x 10 GE SFP+ slots, redundant PSU, 4 VMs with Win7, Win8, Win10 and (1) MS Office license included. Upgradable to a maximum of 24 licensed VMs.
FortiSandbox 3000E	FSA-3000E	Advanced Threat Protection System — 4x GE RJ45, 2x 10 GE SFP+ slots, redundant PSU, 8 VMs with Win7, Win8, Win10 and (1) MS Office license included. Upgradable to a maximum of 56 licensed VMs. TAA-Compliant.
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-123-02-12	FortiSandbox Cloud Service Subscription (SKU varied by FortiGate/FortiMail/FortiProxy/FortiWeb 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.

FORTINET®

www.fortinet.com