DATA SHEET

FortiSandbox

Available in:

Appliance | Virtual Machine | PaaS | Cloud

Third Generation Malware Sandbox

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.

Feature Benefits

Simple

Easily integrates with existing security infrastructure to automate the submission of objects from existing security controls, and the sharing of threat intelligence in real time for immediate threat response and reduction on the reliance on scarce security resources.

Powerful

Built-in next-generation Machine Learning (ML) and Deep Learning (DL) engines that detect new malware and ransomware techniques earlier, improving security efficacy by up to 25% over traditional sandbox detection. Critical to helping organizations elevate their security posture further and reducing business disruption due to new sophisticated ransomware and 0-day threats.

Anywhere

Flexible deployment options for any Information Technology (IT) or Operational Technology (OT) environment to protect networks, emails, web applications, and endpoints from campus to the public cloud, and Industrial Control System (ICS) devices found in industrial facilities. This significantly reduces gaps in the attack surface.

Breach Protection for

- Remote Office
- Branch
- Campus
- Data Center
- Public Cloud (AWS and 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

FEATURE HIGHLIGHTS

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 ML-powered static analysis. Second stage analysis is done in a contained environment to uncover the full attack lifecycle leveraging behavior-based ML 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. Lastly, Deep Learning is applied to analyze the code base for anomalies.

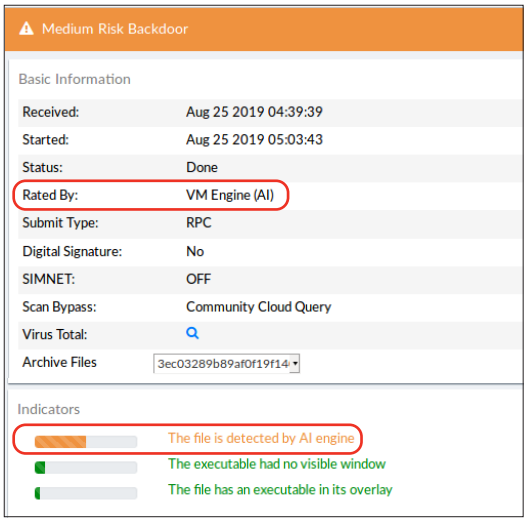

Figure 1 - AI-based dynamic analysis

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 2 steps through the flow on the automated mitigation process.

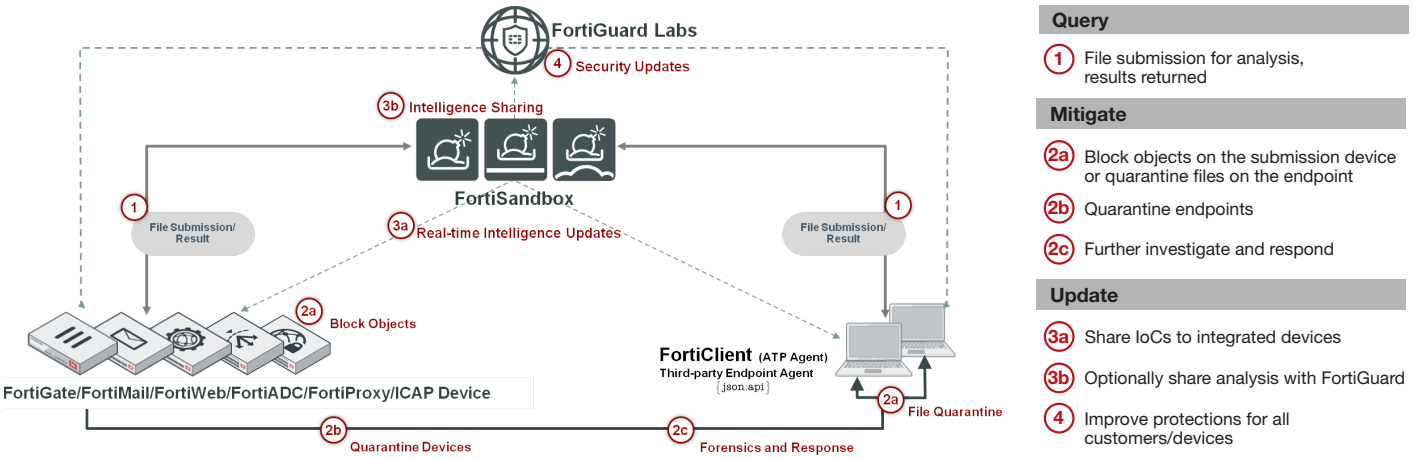

Figure 2 - FortiSandbox threat mitigation workflow

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 3).

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.

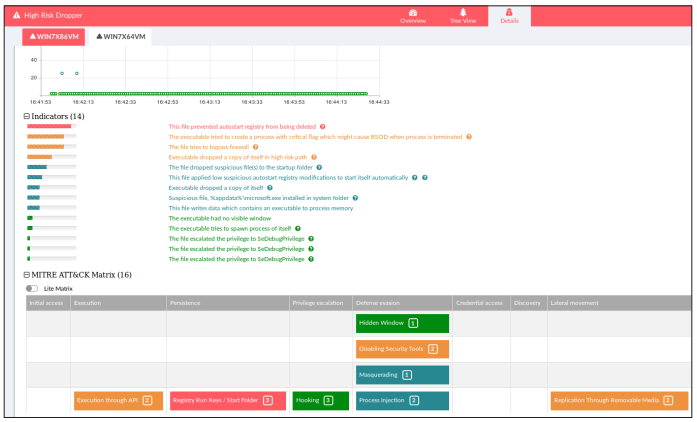

Figure 3 - MITRE ATT&CK matrix with built-in tools

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.

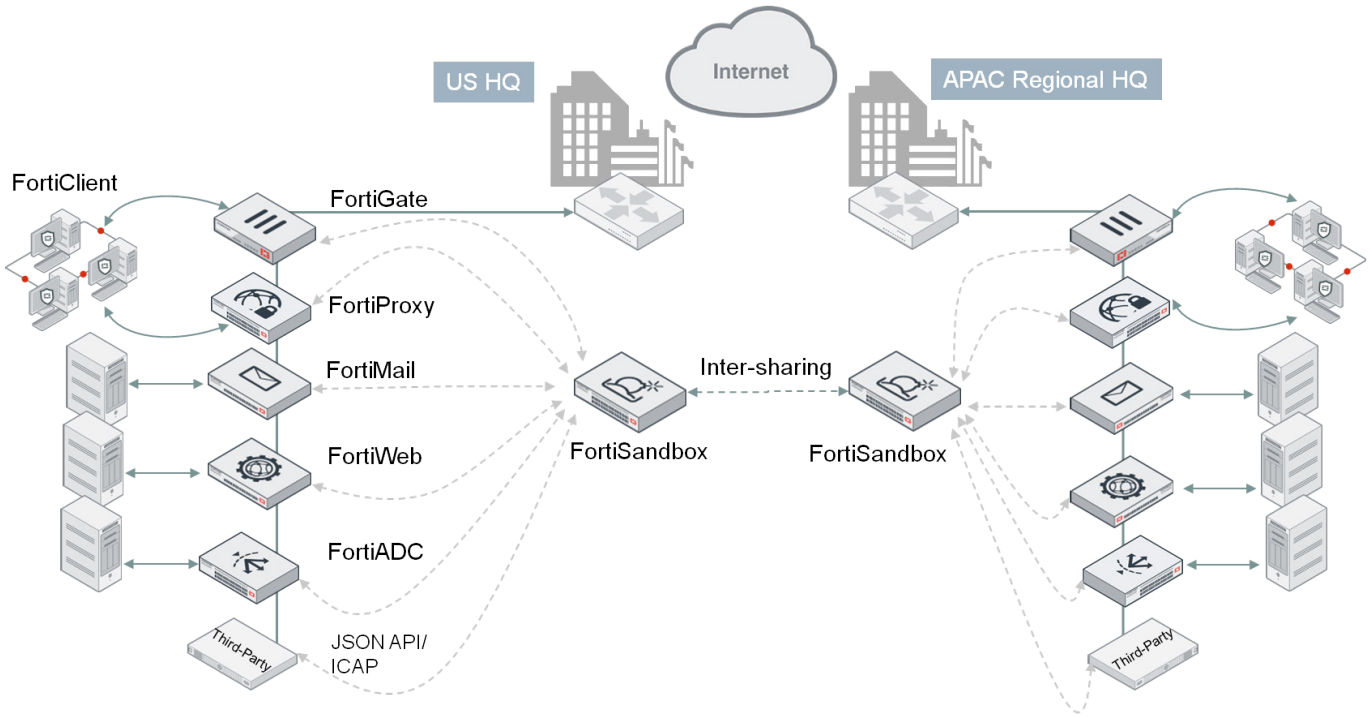

Figure 4 - Integrated deployment

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.

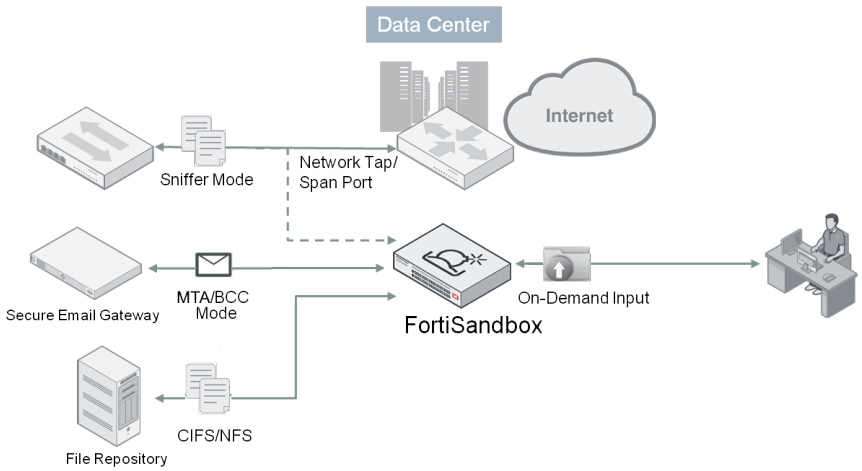

Figure 5 - Standalone deployment

FEATURES SUMMARY

ADVANCED THREAT PROTECTION

Inspection of new threats including ransomware and password protected malware mitigation

Machine Learning (ML) powered Static Code analysis identifying possible threats within non-running code

Virtual OS Sandbox:

- ML-powered behavioral analysis constantly learning new malware and ransomware techniques
- Concurrent instances
- OS type supported: Windows 10, Windows 8.1, Windows 7, macOS, Linux, Android, and ICS systems
- Customize VMs with your own Windows and Linux OS and applications
- 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

Heuristic/ Pattern/ Reputation-based Analysis

Intelligent Adaptive Scan Profile that optimizes sandbox resources based on submissions

VM Scan Ratio for efficient utilization of the VMs

Deep Learning powered Dynamic scan module (Pexbox) for emulating Windows executable codes

Rating Engine Plus that leverages FortiGuard's latest ML rating

Parallel Scan to run multiple distinct VM types

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:

- 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 FortiClient EMS: HTTP, FTP, SMB
- Integrated mode with FortiWeb: HTTP
- Integrated mode with ICAP Client: HTTP
- Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB
- MTA/BCC mode: SMTP

OT services supported: tftp, modbus, s7comm, http, snmp, bacnet, ipmi

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

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

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 for FortiManager

Remote and Secured 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

NETWORKING / DEPLOYMENT

File Input: File submission from integrated device(s). Sniffer mode, on-demand file upload

Large file support (e.g. ISO images, Network Shared Folders)

Air-gapped networks support

High-availability clustering support

Port monitoring for fail-over in a cluster

Aggregate interface for increased bandwidth and redundancy

Static Routing Support

MONITORING AND REPORTING

Dashboard widgets for Connectivity and Services, License Status, Scan Performance, System Resources

Real-Time Monitoring Widgets: 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: MITRE ATT&CK-based report on malware techniques such as file modification, process behaviors, registry behaviors, and network behaviors

Sample file, sandbox tracer logs, PCAP capture and indicators in STIX 2.0 format

Routine logs of system status and performance

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

Cluster Management for administering HA-Cluster

Supports single page upload of any licenses

Alert System for system health check

Supports FortiGuard as NTP server

Consolidated CLI for troubleshooting

SPECIFICATIONS

	FSA-500F	FSA-1000F/-DC	FSA-2000E	FSA-3000E	FSA-3000F
Hardware					
Network Interfaces	4x GE RJ45 ports	4x GE RJ45 ports, 4x GE SFP slots	4x GE RJ45 ports, 2× 10 GE SFP+ slots	4x GE RJ45 ports, 2× 10 GE SFP+ slots	4x GE RJ45 ports, 2× 10 GE SFP+ slots
Storage	1× 1 TB	2× 1 TB	2× 2 TB	4× 2 TB	4× 2 TB
Power Supplies	1x PSU	1x PSU, Optional 2nd PSU for hot-swap	2x Redundant PSU (Hot Swappable)	2x Redundant PSU (Hot Swappable)	2x Redundant PSU (Hot Swappable)
System Performance and Capacity					
Number of VMs	6*	14*	24*	56*	72*
Sandbox Pre-Filter Throughput (Files/Hr)[1]	4,500	7,500	12,000	15,000	18,000
VM Sandboxing Throughput (Files/Hr)	120	280	480	1,120	1,340
Real-world Effective Throughput (Files/Hr)	600[2]	1,400[2]	2,400[2]	5,600[2]	6,720[2]
Sniffer Throughput	500 Mbps	1 Gbps	4 Gbps	8 Gbps	9.6 Gbps
MTA Capacity	5,000 emails/hour	10,000 emails/hour	15,000 emails/hour	35,000 emails/hour	42,000 emails/hour
Dimensions and Power					
Height x Width x Length (inches)	1.73 × 17.24 × 12.63	1.73 × 17.24 × 22.83	3.46 × 17.24 × 20.87	3.5 × 17.2 × 29	3.5 × 17.2 × 23.7
Height x Width x Length (mm)	44 × 438 × 320	44 × 438 × 580	88 × 438 × 530	89 × 437 × 738	88 × 438 × 601
Weight	18.72 lbs (8.5 kg)	25 lbs (11.34 kg)	27 lbs (12.25 kg)	43 lbs (19.52 kg)	44 lbs (20 kg)
Form Factor	1 RU	1 RU	2 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	100–240V AC, 50/60 Hz
Maximum Current (AC/DC)	100V/8A, 240V/4A	100V/5A, 240V/3A / -48VDC/9A	100V/8A, 240V/4A	100V/9.8A, 240V/5A	100V/10A, 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	462.1 / 392.8 W
Heat Dissipation	260.34 BTU/h	397.75 BTU/h	600.17 BTU/h	1,943.82 BTU/h	1,610.81 BTU/h
Environment					
Operating Temperature	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)	50–95°F (10– 35°C)	32–104°F (0– 40°C)
Storage Temperature	-4–158°F (-20–70°C)	-40–158°F (-40–70°C)	-4–158°F (-20–70°C)	-40–158°F (-40–70°C)	-40–158°F (-40–70°C)
Humidity	5–90% non-condensing	5–90% non-condensing	5–90% non-condensing	8–90% (non-condensing)	5–90% (non-condensing)
Compliance					
Certifications	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST				

	FORTISANDBOX-VM		FORTISANDBOX CLOUD
Hardware			
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)		4
Memory Support (Minimum / Maximum)	8 GB / Unlimited		8 GB
Virtual Storage (Minimum / Maximum)	30 GB / 16 TB		200 GB
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**	**Cloud VMs**
Number of VMs	8 VMs/nodes, up to 99 nodes/cluster	5 (up to 200 Windows Cloud VMs)	1 (up to 200 VMs)
VM Sandboxing Throughput (Files/Hour)	Hardware dependent	100 (up to 4,000)	20 (up to 4,000)
Real-world Effective Throughput (Files/Hour)[2]	Hardware dependent	500 (up to 20,000)	100 (up to 20,000)
Compliance			
Certifications	N.A.		SOC2

Note: All performance values are "up to" and vary depending on the environment and system configuration.
* Default Windows VM license(s) included with hardware: FSA-500F (2), FSA-1000F/-DC (2), FSA-2000E (4), FSA-3000E (8), FSA-3000F (8). Additional VM capacity are available as an upgrade license.
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.

FortiSandbox 500F

FortiSandbox 1000F/-DC

FortiSandbox 2000E

FortiSandbox 3000F

INTEGRATION MATRIX

	FORTIGATE	FORTICLIENT	FORTIMAIL	FORTIWEB	FORTIADC	FORTIPROXY
FortiSandbox Appliance and VM	FortiOS V5.6+	FortiClient for Windows OS V5.6+	FortiMail OS V5.4+	FortiWeb OS V5.6+	FortiADC OS V5.0+	FortiProxy OS V1.2.3+
FortiSandbox Cloud	FortiOS V6.4.2+, 6.2.5+	FortiClient for Windows OS V6.4.4+, 7.0+	FortiMail V6.4.3+	--	--	--

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 × 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 × 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 3000F	FSA-3000F	Advanced Threat Protection System - 4 x GE RJ45, 2 × 10GbE SFP+ Slots, redundant PSU, 8 VMs with (6) Win10, (2) Win7 and (1) MS office licenses included. Upgradable to a maximum of 72 licensed VMs, refer to FSA-3000F-UPG-LIC-32 and/or FC-10-SA3KF-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	FC1-10-SACLP-433-01-DD	Cloud VM Service for FortiSandbox Cloud. Expands Cloud VM for Windows/macOS/Linux/Android by 1. Maximum of 200 VMs per FortiSandbox. Requires FortiCloud Premium SKU FC-15-CLDPS-219-02-DD.
	FC2-10-SACLP-433-01-DD	Cloud VM Service for FortiSandbox Cloud. Expands Cloud VMs for Windows/MacOS/Linux/Android by 5. Maximum of 200 VMs per FortiSandbox. Requires FortiCloud Premium SKU FC-15-CLDPS-219-02-DD.
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.

FORTINET

www.fortinet.com