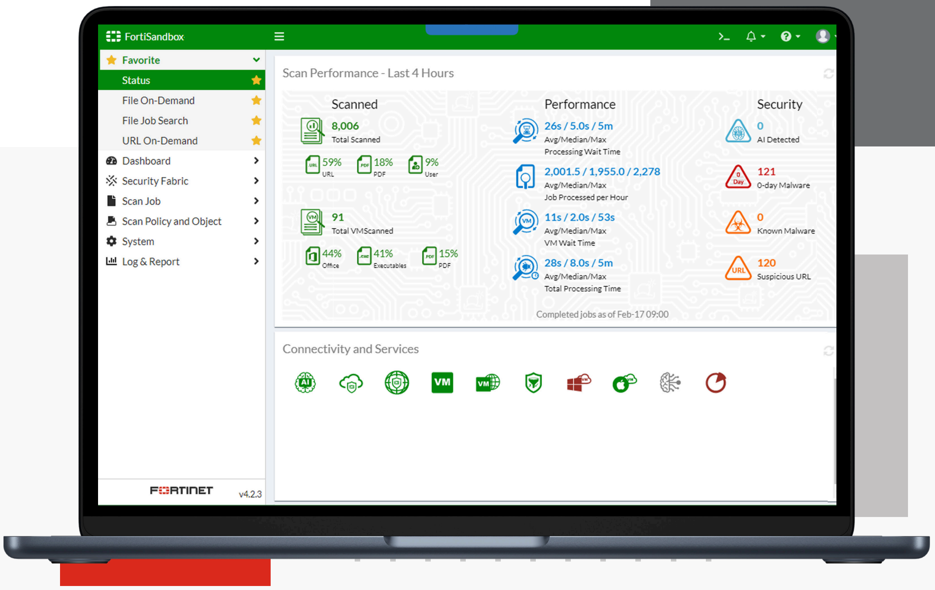
Data Sheet

FortiSandbox and FortiGuard Sandbox Services



Scan Performance - Last 4 Hours

Scanned

8,006 Total Scanned

59% URL, 18% PDF, 9% User

91 Total VMScanned

44% Office, 41% Executables, 15% PDF

Performance

26s / 5.0s / 5m Avg/Median/Max Processing Wait Time

2,001.5 / 1,955.0 / 2,278 Avg/Median/Max Job Processed per Hour

11s / 2.0s / 53s Avg/Median/Max VM Wait Time

28s / 8.0s / 5m Avg/Median/Max Total Processing Time

Security

0 AI Detected

121 0-day Malware

0 Known Malware

120 Suspicious URL

Completed jobs as of Feb-17 09:00

Connectivity and Services

Highlights

REAL-TIME VERDICTS
Prevent delays and unknown files from entering the network with real-time analysis and filtering

INTEGRATION AT EVERY STAGE
Extend zero-day threat protection to NGFWs and other major areas of your infrastructure

ACCELERATED THREAT INVESTIGATION
Speed investigation with built-in MITRE ATT&CK® matrix to identify a variety of malware

REDUCE SECURITY OVERHEAD
Block unknown files and experience fewer incidents and less investigation and mitigation time

Third Generation Malware Sandbox

FortiSandbox is a high-performance security solution that utilizes machine learning technology to identify and isolate advanced threats in real-time. It inspects network traffic, files, and URLs for malicious activity, including zero-day threats, and uses sandboxing technology to analyze suspicious files in a secure virtual environment.

The solution supports multiple operating systems and file types, and provides reporting capabilities for quick threat identification and response. FortiSandbox is a flexible option suitable for organizations of any size and can be deployed on-premises, in the cloud, or as a hosted service, and integrates natively with the Security Fabric and other tools to evaluate suspicious content.

Feature Benefits

Integrated

FortiSandbox easily integrates with existing infrastructure to automate the submission of objects from existing security controls and share threat-intelligence in real time. This automation enables immediate threat response and reduces reliance on security resources.

Inline

With FortiOS 7.2, we introduced the industry's first inline blocking where the FortiGate NGFW holds suspicious files while maintaining user experience. It does this action by leveraging an AI-powered malware analysis environment. Only files that have been analyzed and determined to be safe are let into the network.

Anywhere

Ideal for IT and OT environments to protect networks, email, web applications, and endpoints from the campus to the public cloud, plus industrial control system (ICS) devices found in industrial facilities. This structure significantly reduces gaps in the attack surface.

Feature Highlights

AI-Powered Sandbox Malware Analysis, Automated, Inline Breach Protection

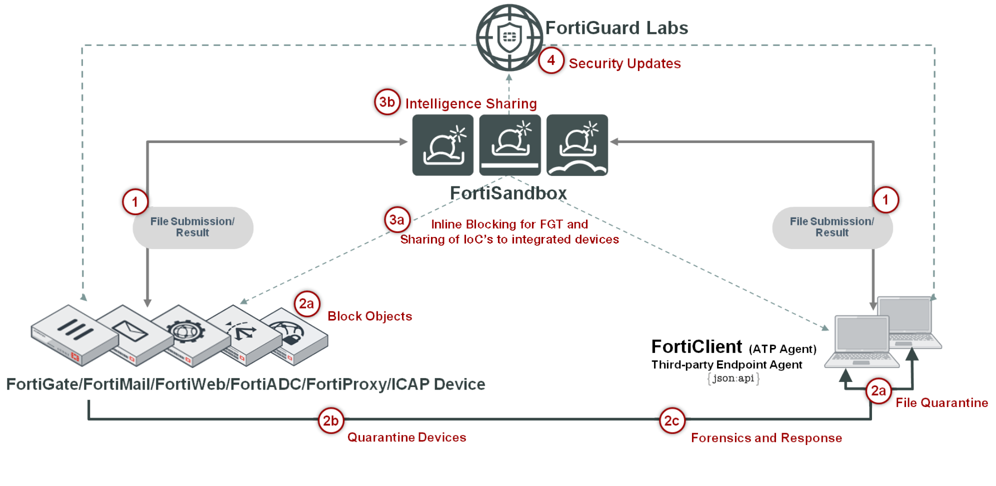
Complement your established defenses with a two-step AI-based sandboxing approach. Suspicious and at-risk files are subjected to the first stage of analysis that quickly identifies known and emerging malware through FortiSandbox's ML-powered static analysis. Second stage analysis is done in a contained environment to uncover the full attack lifecycle leveraging behavior based ML that is constantly learning new malware techniques and automatically adapting malware behavioral indicators. This approach makes the FortiSandbox dynamic analysis detection engine more efficient and effective against zero-day threats. Lastly, deep learning is applied to analyze the code base for anomalies.

Starting with FortiOS 7.2, FortiGate Next-Generation Firewalls can hold suspicious files, without noticeable business impact, by leveraging our AI-powered sandbox for malware analysis. Only files that have been analyzed and determined to be safe are let into the network. This feature is supported with the FortiGuard AI-based Inline Sandbox Service (IL SBX) and FortiSandbox offerings running version 4.2+.

Threat Mitigation

Our ability to uniquely integrate various products with FortiSandbox through the Security Fabric platform automates your breach protection strategy with an incredibly simple setup. Once malicious code is identified, FortiSandbox will return risk ratings and the local intelligence is shared in real time with Fortinet, Fabric-Ready Partners, and third-party security solutions to mitigate and immunize against new advanced threats. The local intelligence can optionally be shared with the Fortinet threat research team, FortiGuard Labs, to help protect organizations globally. Figure 1 steps through the flow on the automated mitigation process.

Feature Highlights


FortiGuard Labs
4 Security Updates
3b Intelligence Sharing
FortiSandbox
1 File Submission/ Result
3a Inline Blocking for FGT and Sharing of IoC's to integrated devices
1 File Submission/ Result
2a Block Objects
FortiGate/FortiMail/FortiWeb/FortiADC/FortiProxy/ICAP Device
FortiClient (ATP Agent)
Third-party Endpoint Agent
{json:api}
2a File Quarantine
2b Quarantine Devices
2c Forensics and Response

Query

1. File submission for analysis, results returned

Mitigate

- 2a Block objects on the submission device or quarantine files on the endpoint
- 2b Quarantine endpoints
- 2c Further investigate and respond

Update

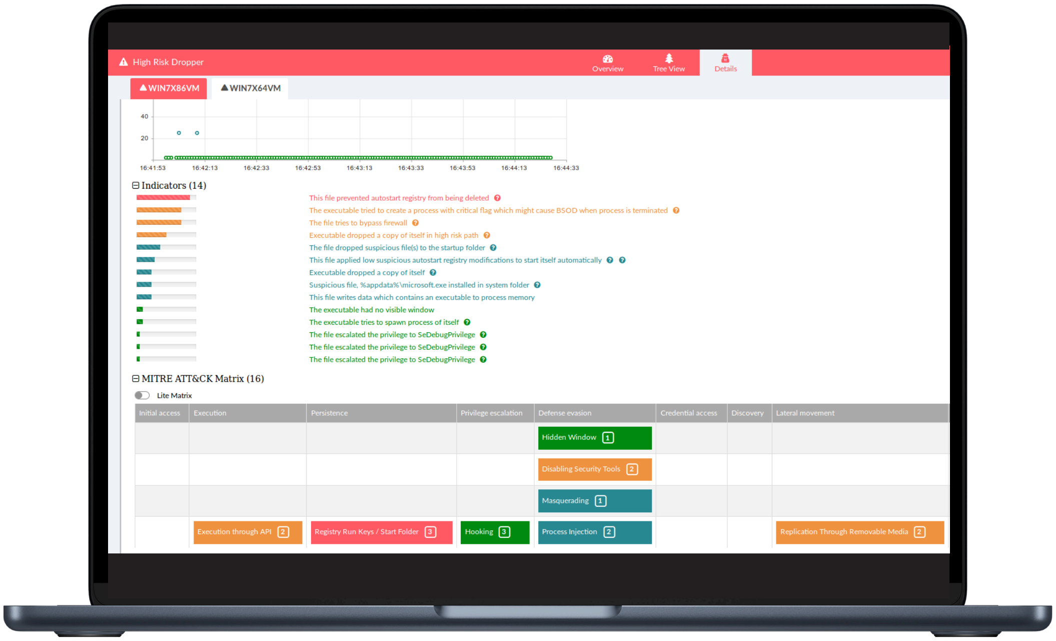
- 3a Share IoCs to integrated devices
- 3b Optionally share analysis with FortiGuard
- 4 Improve protections for all customers/devices

Figure 1 - FortiSandbox Threat Mitigation Workflow

MITRE ATT&CK-based Reporting and Investigative Tools

FortiSandbox provides a 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, malware screenshot, and is 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.



⊟ Indicators (14)

This file prevented autostart registry from being deleted
The executable tried to create a process with critical flag which might cause BSOD when process is terminated
The file tries to bypass firewall
Executable dropped a copy of itself in high risk path
The file dropped suspicious file(s) to the startup folder
This file applied low suspicious autostart registry modifications to start itself automatically
Executable dropped a copy of itself
Suspicious file, %appdata%\microsoft.exe installed in system folder
This file writes data which contains an executable to process memory
The executable had no visible window
The executable tries to spawn process of itself
The file escalated the privilege to SeDebugPrivilege
The file escalated the privilege to SeDebugPrivilege
The file escalated the privilege to SeDebugPrivilege

⊟ MITRE ATT&CK Matrix (16)

Lite Matrix

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement
				Hidden Window 1			
				Disabling Security Tools 2			
				Masquerading 1			
	Execution through API 2	Registry Run Keys / Start Folder 3	Hooking 3	Process Injection 2			Replication Through Removable Media 2

Figure 2 - MITRE ATT&CK Matrix with Built-in Tools

Deployment Options

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

FortiSandbox is the most flexible threat-analysis appliance available as it offers various deployment options for unique configurations and requirements. In addition, organizations can choose to combine these deployment options.

Integrated

FortiSandbox natively integrates with FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy, FortiClient (ATP agent), 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 instantaneous sharing of real-time intelligence. This feature 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

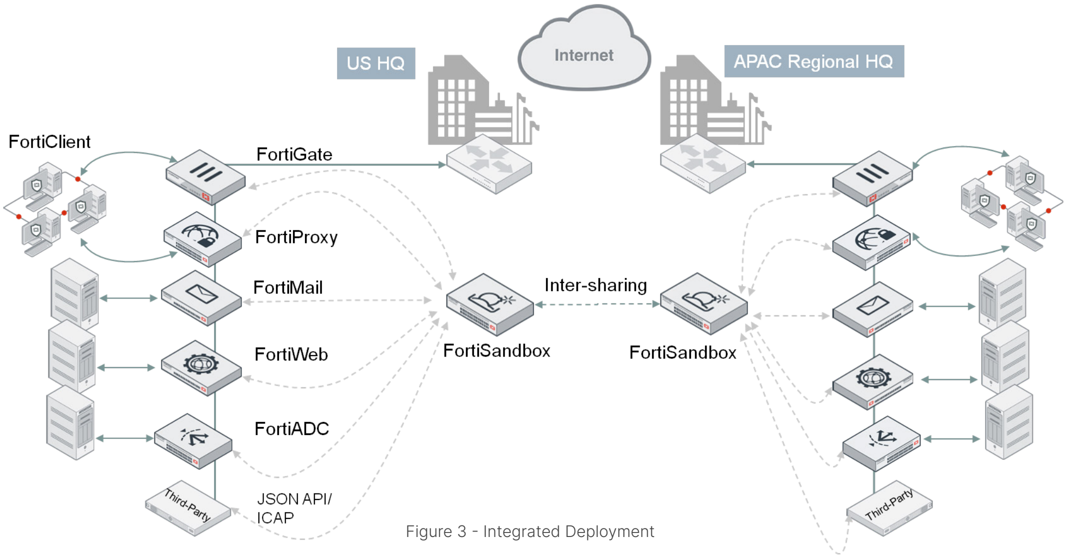


Figure 3 - Integrated Deployment

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 for enhancing an existing multi-vendor threat protection approach.

Platform as a Service (PaaS)

Hosted FortiSandbox services offer the same Fortinet Security Fabric integration as FortiSandbox appliances. FortiSandbox (PaaS) can easily scale to facilitate current and future business needs without big upfront investments and with lower operational costs. Fortinet will maintain, update, and operate this service on your behalf.

Features Summary

ADVANCED THREAT PROTECTION

Inline blocking with FortiOS 7.2 and up.

Inspection of new threats including ransomware and password-protected malware mitigation

ML-powered static code analysis identifying possible threats within non-running code

Intelligent adaptive scan profile that optimizes sandbox resources based on submissions

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
- Customizable VMs with Windows and Linux OS and applications
- Anti-evasion detection. Sleep calls, process identification, registry queries, and more. Plus, simulates bare metal behavior for evasion techniques
- Callback detection. Malicious URL visit, botnet C&C communication, and attacker traffic from activated malware
- Download captured packets, tracer logs, and screenshots
- Sandbox interactive mode
- Video-recording of malware interaction

Heuristic/pattern/reputation-based analysis

Configurable internet browser on dynamic scan

Deep learning powered dynamic scan module (pexbox) for emulating Windows executable codes

VM scan ratio for efficient utilization of VMs

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

User-defined extensions

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 visits

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

File checksum whitelist and blacklist options

URL submission for scan and query from emails and files

SYSTEM 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. Carbon Black, Ziften, SentinelOne

Sharing of IOCs between FortiSandboxes

NETWORKING / DEPLOYMENT

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

Supports sending TCP RST on sniffer mode deployment

Large file support (e.g., ISO images, network shared folders)

Multiple ICAP adapter profile for multi-tenancy support

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

Scan performance page for tracking historical usage

Generates periodic log of scan statistics

Generates periodic log of system resource usage

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 clusters

Supports single-page upload of any licenses

Alert system for system health check

Supports FortiGuard as NTP server

Consolidated CLI for troubleshooting

Supports backup, restore, and revision of the configuration

Specifications

FEATURE	CLOUD			ON PREMISE				
	FortiSandbox SaaS[1]	FortiSandbox PaaS	FortiSandbox Public Cloud	FSA-VM	FSA-500F	FSA-1000F/DC	FSA-2000E	FSA-3000F
Deployment	Fortinet-Hosted	Fortinet-Hosted	Azure, AWS, GCP, OCI	VM Appliance	Hardware Appliance	Hardware Appliance	Hardware Appliance	Hardware Appliance
FortiGate Capabilities								
Detection (Visibility and Log Enrichment)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Accelerated AI Pre-filter	Yes[1]	Yes[2]	Yes[2]	Yes[2]	Yes[2]	Yes[2]	Yes[2]	Yes[2]
Prevention (Inline Blocking)	Yes[1]	coming in Q2	Yes	Yes	Yes	Yes	Yes	Yes
Security Services								
Fortinet Security Fabric Integration	Centralized	Centralized	Centralized	Centralized	Centralized	Centralized	Centralized	Centralized
Fabric Partners		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Adapters, API, Network Share, and Sniffer		Via API only	Yes	Yes	Yes	Yes	Yes	Yes
AI-based Static Behavior Analysis	Yes[1]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dynamic Analysis Time	up to 60 minutes (1-3 minutes)[1]	1-3 minutes	1-3 minutes	1-3 minutes	1-3 minutes	1-3 minutes	1-3 minutes	1-3 minutes
Anti-evasion Detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
C & C Detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AV, IPS, Web Filtering	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System Performance								
Effective Sandboxing Throughput[3] (Files/Hr)		20 – 4000	100 – 1000	100 – 1000	1000	1400	2400	6720
Static Analysis Throughput[4] (Files/Hr)					6000	10 000	16 000	75 000
Dynamic Analysis Throughput[5] (Files/Hr)					250	500	800	1600
FortiMail Throughput[6] (Emails/Hr)		200 – 40 000	1000 – 10 000	1000 – 10 000	10 000	14 000	24 000	67 200
Number of Users[7]		8 – 1600	40 – 400	40 – 400	400	560	960	2688
MTA Adapter Throughput (Emails/Hr)					5000	10 000	15 000	60 000
Sniffer Mode Throughput (Gbps)			1	1	0.5	1	4	9.6
Sandboxing VMs								
Default Local VMs			0	0	2	2	4	+8
Local or Custom VM Expansion Capacity			+8	8	+4	+12	+20	+64
Cloud VM Expansion Capacity		1 - 200	5 - 200	5 - 200	5 - 200	5 - 200	5 - 200	5 - 200
Supported OS								
Windows	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MacOS, Linux, Android		Yes[8]	Yes	Yes	Yes	Yes	Yes	Yes
Custom OS			Yes	Yes	Yes	Yes	Yes	Yes
OT Simulation					Yes	Yes	Yes	Yes

1. Supported on FortiGate as add-on AI-Based Inline Sandbox Prevention Service.
2. Integration support with FortiNDR's Artificial Neural Network capability for fast pre-filtering
3. Tested based on files with 80% documents and 20% executables. Includes both static and dynamic analysis with pre-filtering enabled; measured based on v4.2.2
4. Includes receiving, job handling, AV engine, Yara engine, Cloud Query; measured based on v4.2.2
5. Previously called "Sandboxing VM Throughput"; measured based on v4.2.2 with Pipeline mode enabled
6. Based on a ratio of one email with attachment to 10 emails
7. Based on a ratio of one user per 25 emails
8. Limited to static analysis only

Specifications

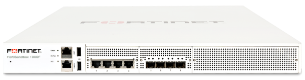
FEATURE	CLOUD			ON PREMISE				
	FortiSandbox SaaS[1]	FortiSandbox PaaS	FortiSandbox Public Cloud	FSA-VM	FSA-500F	FSA-1000F/DC	FSA-2000E	FSA-3000F
System Information								
Form	Virtual Machine	Virtual Machine	Virtual Machine	Virtual Machine	1RU Appliance	1RU Appliance	2RU Appliance	2RU Appliance
Network Interfaces			4	4	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
1G RJ45					Yes	Yes	Yes	Yes
1G SFP					No	Yes	Yes	Yes
10G SFP+					No	No	Yes	Yes
Storage		200 GB	200 GB (min)	200 GB (min)	1× 1 TB	2× 1 TB	2× 2 TB	4× 2 TB
Hot Swappable							Yes	Yes
Trusted Platform Module (TPM)					No	No	No	No
Hypervisor Support[1]	No	No	Yes	Yes				
Dimensions and Power								
Height x Width x Length (inches)					1.73 × 17.24 x 12.63	1.73 × 17.24 x 22.83	3.46 × 17.24 x 20.87	3.5 × 17.2 × 23.7
Height x Width x Length (mm)					44 × 438 × 320	44 × 438 × 580	88 × 438 × 530	88 × 438 × 601
Weight					18.72 lbs (8.5 kg)	25 lbs (11.34 kg)	27 lbs (12.25 kg)	44 lbs (20 kg)
Form Factor					1 RU	1 RU	2 RU	2 RU
Power Supplies					1x PSU	1x PSU, Optional 2nd PSU for hot-swap	2x Redundant PSU (Hot Swappable)	2x Redundant PSU (Hot Swappable)
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)					100V/8A, 240V/4A	100V/5A, 240V/3A / -48VDC/9A	100V/8A, 240V/4A	100V/10A, 240V/5A
Power Consumption (Average/Maximum)					30.1 / 76.3 W	66.93 / 116.58 W	164.7 / 175.9 W	392.8 / 462.1 W
Heat Dissipation					260.34 BTU/h	397.75 BTU/h	600.17 BTU/h	1610.81 BTU/h
Forced Airflow					Front to Back	Front to Back	Front to Back	Front to Back
Environment								
Operating Temperature					32°–104°F (0°–40°C)	32°–104°F (0°–40°C)	32°–104°F (0°–40°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)
Humidity					5%–90% non-condensing	5%–90% non-condensing	5%–90% non-condensing	5%–90% (non-condensing)
Compliance								
Certifications					FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST			
Compute / DC Locations								
Hosted Regions	USA, Germany, Japan, and Canada	USA, Germany, and Canada						
Additional Services								
24 × 7 Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

[1] Hypervisor support includes VMware ESXi, Linux KVM CentOS, Microsoft Hyper-V, Nutanix, AWS, Azure, GCP, and OCI

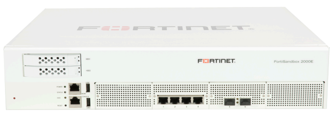
Integration Matrix

	CLOUD				APPLIANCES
Product	SaaS	Inline Sandbox	FortiSandbox Cloud (PaaS)	Private/Public Cloud	*
FORTIGATE	FortiOS V6.2+	FortiOS V7.2.1+	FortiOS V6.4.2+, 6.2.5+	FortiOS V5.6+	
FORTICLIENT	FortiClient for Windows OS V6.2+		FortiClient for Windows OS V6.4.4+, 7.0+	FortiClient for Windows OS V5.6+	
FORTIMAIL	FortiMail OS V6.2+		FortiMail V6.4.3+	FortiMail OS V5.4+	
FORTIWEB	FortiWeb OS V6.2+			FortiWeb OS V5.6+	
FORTIADC				FortiADC OS V5.0+	
FORTIPROXY				FortiProxy OS V1.2.3+	

FortiSandbox 500F



FortiSandbox 1000F/-DC



FortiSandbox 2000E

FortiSandbox 3000F

Ordering Information

Product	SKU	Description
FortiSandbox SaaS for FortiGate		
Cloud Sandbox (FGT-200F)	FC-10-F200F-100-02-DD	Advanced Malware Protection (AMP) Bundle including Antivirus, Mobile Malware and FortiGate Cloud Sandbox Service.
Inline Sandbox (IL SBX) (FGT-200F)	FC-10-F200F-577-02-DD	FortiGuard AI-based Inline Sandbox Service. Requires AMP Bundle for the Antivirus engine.
FortiSandbox SaaS for Security Fabric		
Cloud Sandbox for FortiMail (FML-200F)	FC-10-FE2HF-123-02-DD	FortiMail Cloud Sandbox - Cloud Sandbox for FortiMail.
Cloud Sandbox for FortiWeb (FWB-100E)	FC-10-W01HE-123-02-DD	FortiWeb Cloud Sandbox - Cloud Sandbox for FortiWeb.
Cloud Sandbox for FortiProxy (FPX-400E)	FC1-10-XY400-514-02-DD	SWG Protection Bundle which includes Sandbox Cloud.
Cloud Sandbox for FortiADC (FAD-220F)	FC-10-AD2AF-123-02-DD	FortiADC Cloud Sandbox - Cloud Sandbox for FortiADC.
FortiSandbox PaaS		
FortiSandbox Cloud 1 VM	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.
FortiSandbox Cloud 5 VMs	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 subscription SKU FC-15-CLDPS-219-02-DD.
FortiCloud Premium Account License	FC-15-CLDPS-219-02-DD	Access to advanced account and platform features. Per account license. See datasheet/online resources for included feature/license details.
FortiSandbox Pub Cloud / FortiSandbox VM Appliance		
FortiSandbox-VM	FSA-VM00	Sandboxing Virtual Appliance - No Windows/Office license included. For upgrades with local VMs up to 8, refer to FSA-VM-WIN10-1 or FSA-VM00-UPG-LIC-BYOL. For upgrade with Cloud VM up to 200, refer to FC-10-FSA01-195-02-DD. For Threat Intelligence subscription, refer to FC-10-FSV00-500-02-DD.
FortiSandbox Windows Cloud VM	FC-10-FSA01-195-02-DD	Expands FSA (Appliance/VM) Windows Cloud VM Clone capacity by 5. Supports Windows 10 with Office 2016. Maximum expansion limits to 200.
FortiSandbox MacOS Cloud VM	FC-10-FSA01-192-02-DD	Expands FSA (Appliance/VM) MacOS Cloud VM Clone capacity by 2. Supports MacOS X. Maximum expansion limits to 8.
FortiSandbox Hardware Appliance		
FortiSandbox 500F	FSA-500F	Sandboxing Appliance - 4 x GE RJ45, 1 Win10, 1 Win7, 1 Office16. Upgradable to max 6 VMs. For upgrades, refer to FSA-500F-UPG-WIN-LIC-4 or FSA-500F-UPG-LIC-BYOL. For Threat Intelligence subscription, refer to FC-10-FS5HF-499-02-DD.
FortiSandbox 1000F/-DC	FSA-1000F/FSA-1000F-DC	Sandboxing Appliance - 4 x GE RJ45, 4 x GE SFP slots, redundant PSU optional, 1 Win10, 1 Win7, 1 Office16. Upgradable to max 14 VMs. For upgrades, refer to FSA-1000F-UPG-WIN-LIC-6 or FSA-1000F-UPG-LIC-BYOL. For redundant PSU, refer to SP-FSA1000F-PS SKU. For Threat Intelligence subscription, refer to FC-10-FS1KF-499-02-DD.
FortiSandbox 2000E	FSA-2000E	Sandboxing Appliance - 4 x GE RJ45, 2 × 10GbE SFP+ Slots, redundant PSU, 1 Win10, 1 Win8, 2 Win7, 1 Office16. Upgradable to max 24 VMs. For upgrades, refer to FSA-2000E-UPG-WIN-LIC-10 or FSA-2000E-UPG-LIC-BYOL. For Threat Intelligence subscription, refer to FC-10-SA20K-499-02-DD.
FortiSandbox 3000F	FSA-3000F	Sandboxing Appliance - 4 x GE RJ45, 2 × 10GbE SFP+ Slots, redundant PSU, 6 Win10, 2 Win7, 1 Office19. Upgradable to max 72 VMs. For upgrades, refer to FSA-3000F-UPG-LIC-32 or FSA-3000F-UPG-LIC-BYOL. For Threat Intelligence subscription, refer to FC-10-SA3KF-499-02-DD.
Optional Accessories		
1 GE SFP SX Transceiver Module	FR-TRAN-SX	1 GE SFP transceiver module, short range. Compatible to FSA-1000F and FSA-2000E.
1 GE SFP LX Transceiver Module	FR-TRAN-LX	1 GE SFP transceiver module, long range. Compatible to FSA-1000F and FSA-2000E.
10 GE SFP+ SR Transceiver Module	FG-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range. Compatible to FSA-2000E and FSA-3000F.
10 GE SFP+ LR Transceiver Module	FG-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range. Compatible to FSA-2000E and FSA-3000F.
FSA-1000F AC Power Supply	SP-FSA1000F-PS	AC power supply for FSA-1000F, FDC-1000F, and FIS-1000F modules only.
FSA-1000F DC Power Supply	SP-FSA1000F-DC-PS	DC power supply for FSA-1000F-DC module only.
FSA-3000F AC Power Supply	SP-FSA3000F-PS	AC power supply for FSA-3000F and FAC-3000F modules only.

www.fortinet.com

April 17, 2023