DATA SHEET

FortiSandbox and FortiGuard Sandbox Services

Available in:

Appliance | Virtual Machine | Public Cloud | PaaS | Inline Sandbox Service

Third-Generation Malware Sandbox

FortiSandbox is a third-generation malware sandbox powered by machine learning and deep learning that integrates to any existing security infrastructure and enables automated protection across both information technology (IT) and operational technology (OT) environments.

Inline Sandboxing

AI-Powered cloud or on-premise sandboxes allow FortiGate Next Generation Firewalls (NGFW) to hold suspicious files. This industry-first inline sandboxing technology keeps malware out with real-time file analysis.

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.

Breach Protection for

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

Third-Party Certifications

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, 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 FortiSandbox's dynamic analysis detection engine more efficient and effective against zero-day threats. Lastly, deep learning is applied to analyze the code base for anomalies.

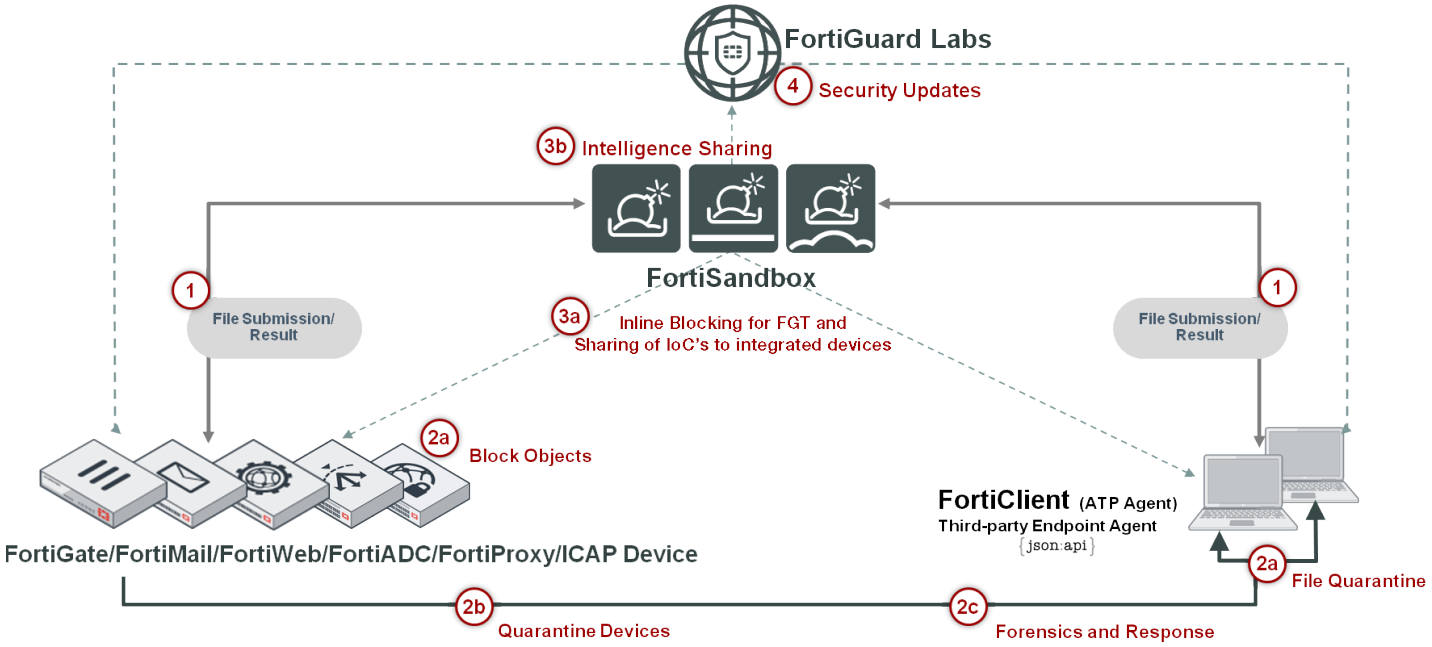

Figure 1 - FortiSandbox Threat Mitigation Workflow

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 and FortiSandbox offerings running version 4.2+.

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.

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 2 - AI-based Dynamic Analysis

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 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.

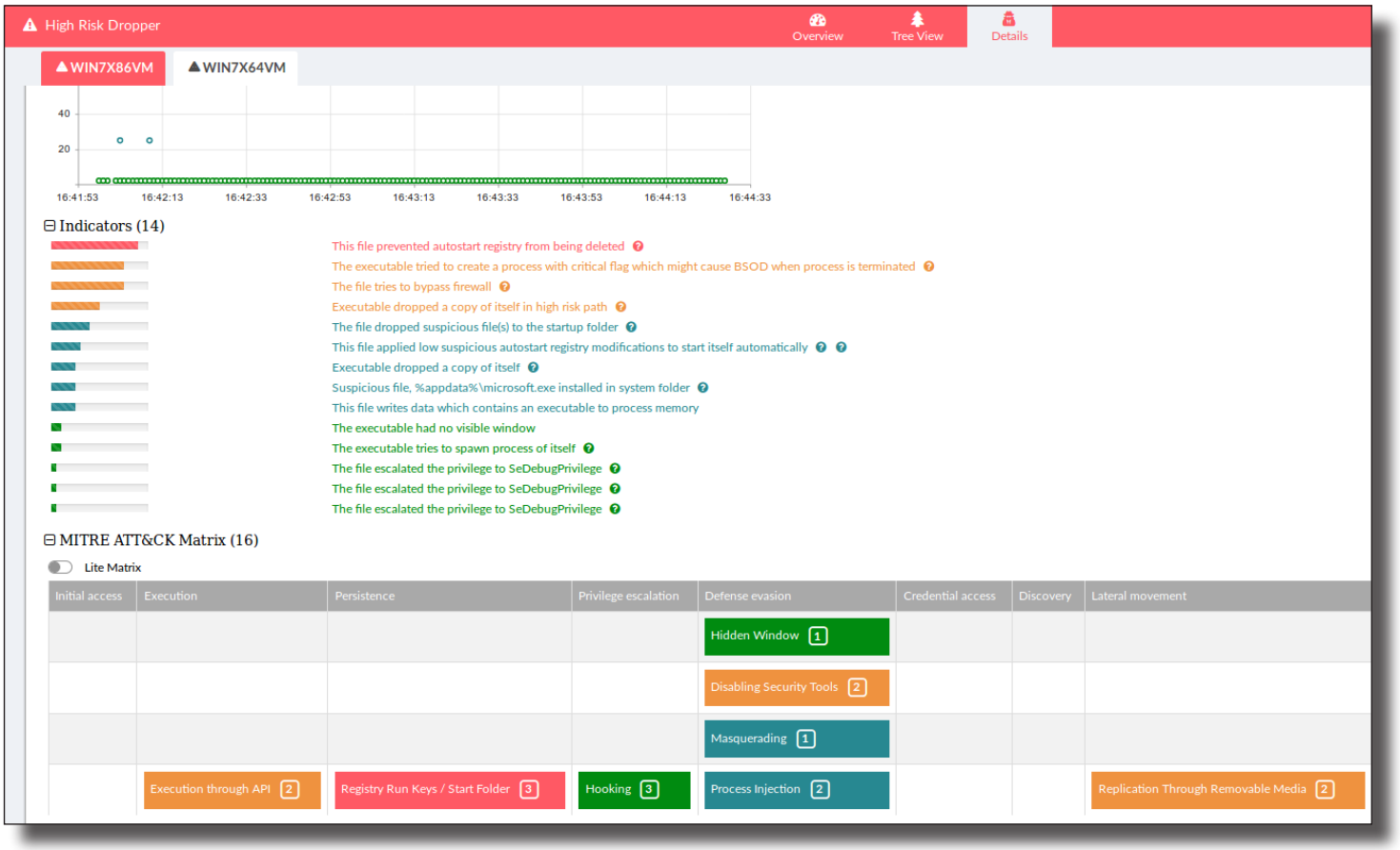

Figure 3 - MITRE ATT&CK Matrix with Built-in Tools

DEPLOYMENT OPTIONS

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.

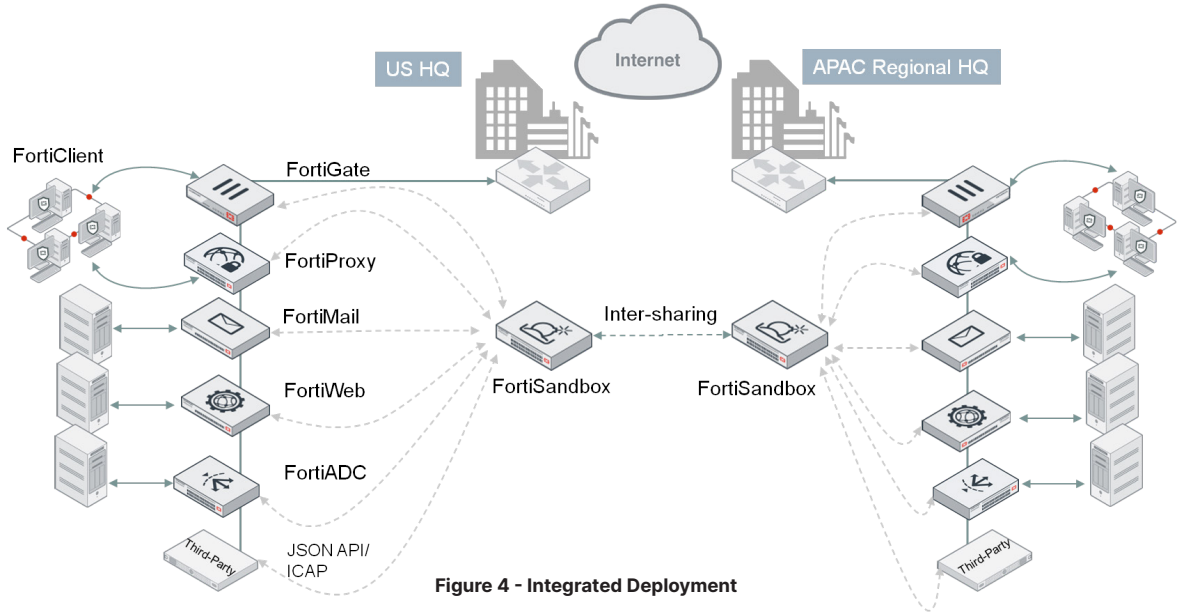

Figure 4 - Integrated Deployment

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 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.

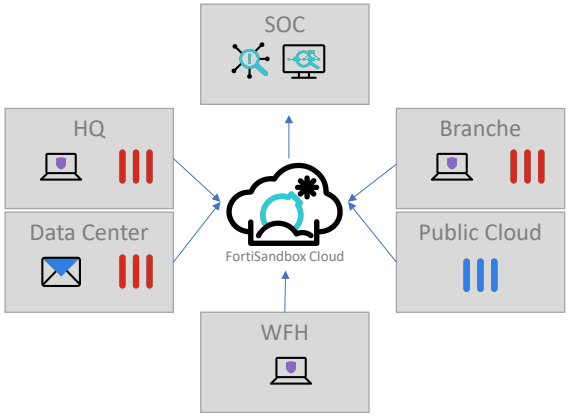

Figure 5 - PaaS Deployment

FEATURES SUMMARY

ADVANCED THREAT PROTECTION

Inline blocking with FortiOS 7.2.

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

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

	AS-A-SERVICE	PAAS	VM	HARDWARE			
	FGD AI-Based Inline SBX Service	FortiSandbox Cloud	Private/Public Cloud	FSA-500F	FSA-1000F/DC	FSA-2000E	FSA-3000F
FortiGate Capabilities							
Detection (Visibility and Log Enrichment)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Accelerated AI Prefilter	Yes[1]	Yes	Yes[1]	Yes[1]	Yes[1]	Yes[1]	Yes[1]
Prevention (Inline Blocking)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security Operations							
SOC Integration	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Data (Log) enrichment	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System Performance							
Effective Sandboxing Throughput[2] (Files/Hr)	20 – 4000	20 – 4000	100 – 4000	600	1400	2400	6720
Static Analysis Throughput[3] (Files/Hr)	—	—	—	5000	7000	10 000	60 000
Dynamic Analysis Throughput[4] (Files/Hr)	—	—	—	180	320	600	2500
Number of Users[5]	10 – 2000	10 – 2000	50 – 2000	500	700	1000	6000
FortiMail Throughput[6] (Emails/Hour)	—	200 – 40 000	1000 – 40 000	10 000	14 000	20 000	120 000
MTA Adapter Throughput (Emails/Hour)	—	—	—	5000	10 000	15 000	60 000
Sniffer Mode Throughput (Gbps)	—	—	1	.5	1	4	9.6
Sandboxing VMs							
Default Local VMs	—	—	0	2	2	4	8
Local or Custom VM Expansion Capacity	—	—	8	+4	+12	+20	+64
Cloud VM Expansion Capacity	—	1 - 200	1 - 200	*Hardware Cloud Expansion (available in Q3 2022)*			
Supported Sandboxing							
Windows VM	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MacOS, Linux, Android VMs	Yes	Yes[7]	Yes	Yes	Yes	Yes	Yes
Custom OS	—	—	Yes	Yes	Yes	Yes	Yes
OT Simulation	—	—	Yes	Yes	Yes	Yes	Yes
System Information							
Type	As-a-Service	Cloud Subscription	Virtual Machine + Cloud Expansion	1RU Appliance	1RU Appliance	2RU Appliance	2RU Appliance
1G RJ45	—	—	Hardware Dependent	Yes	Yes	Yes	Yes
1G SFP	—	—	Hardware Dependent	—	Yes	Yes	Yes
10G SFP+	—	—	Hardware Dependent	—	Yes	Yes	Yes
Security Services							
Fortinet Security Fabric Integration	FortiGate	FortiGate, FortiClient, and FortiMail	Centralized	Centralized	Centralized	Centralized	Centralized
Fabric Partners	—	Yes	Yes	Yes	Yes	Yes	Yes
Adapters, API, Network Share, and Sniffer	—	Via API only	Yes	Yes	Yes	Yes	Yes
Dynamic Analysis Time	3-5 minutes	3-5 minutes	3-5 minutes	3-5 minutes	3-5 minutes	3-5 minutes	3-5 minutes
AI-based Static Behavior Analysis	Yes[1]	Yes	Yes	Yes	Yes	Yes	Yes
Anti-evasion Detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
C & C Detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AV, IPS, Web Filtering	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Additional Services							
24 × 7 Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Compute / DC Locations							
	USA, Germany, Japan, and Canada						

[1] Integrated with FortiNDR's Artificial Neural Network capability for fast pre-filtering
[2] Tested based on files with 80% documents and 20% executables. Includes both static and dynamic analysis with pre-filtering enabled
[3] Includes receiving, job handling, AV engine, Yara engine, Cloud Query
[4] Previously called "Sandboxing VM Throughput"
[5] Based on a ratio of 20 files per user ovre a 10-hour period
[6] Based on a ratio of 1:10 emails with attachment
[7] Limited to static analysis only

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 - PaaS/ Hosted	FortiOS V6.4.2+, 6.2.5+	FortiClient for Windows OS V6.4.4+, 7.0+	FortiMail V6.4.3+			
FortiGuard AI-based Inline Sandbox Service	FortiOS V7.2.1+					

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-1000FUPG-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 × 10 GbE 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 3000F	FSA-3000F	Advanced Threat Protection System - 4 x GE RJ45, 2 × 10 GbE 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-UPGLIC-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
FortiGuard AI-Based Inline Sandbox Service	FC-10-0060F-577-02-DD	A-la-carte service, which includes inline blocking for sandbox and AI/NDR detections, plus log enrichment for SOC teams.
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 FSA-1000F, FDC-1000F, and FIS-1000F modules only.
AC Power Supply	SP-FSA3000F-PS	AC power supply for FSA-3000F and FAC-3000F modules only.
DC Power Supply	SP-FSA1000F-DC-PS	DC power supply for FSA-1000F-DC module only.

FORTINET

www.fortinet.com