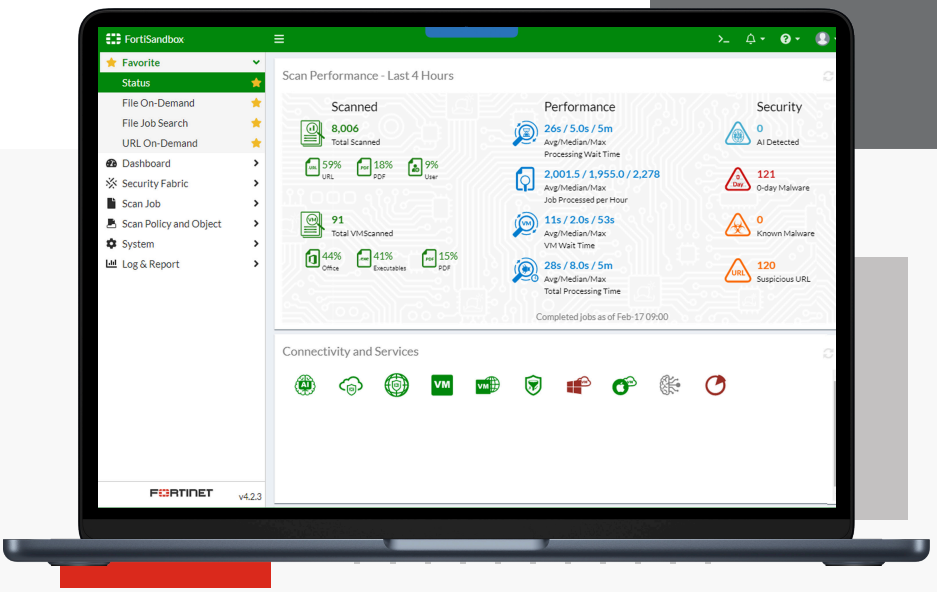
FortiSandbox and FortiGuard Sandbox Services



Highlights

10X EFFECTIVE THROUGHPUT
over traditional Sandboxes, allowing for scaling operations without impacting performance

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

Next Generation AI Powered Sandbox

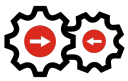
FortiSandbox is a high-performance security solution that utilizes AI/machine learning technology to identify and isolate advanced threats in real-time. FortiSandbox inspects files, websites, URLs and network traffic for malicious activity, including zero-day threats, and uses sandboxing technology to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

FortiSandbox supports multiple operating systems and file types, and provides reporting capabilities for quick threat identification and response. Suitable for organizations of any size and can be deployed on-premises, in the cloud, or as a hosted service, and integrates natively with 11 Security Fabric products and other tools to evaluate suspicious content.

Key Advantages

AI-Powered

FortiSandbox uses AI/ML to enhance its coverage of malware, improve zero-day detection, process large amounts of data, reduce false negatives while rendering quicker verdicts.



Integrated Solution

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 Breach Protection

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 Protection

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.

Unprecedented 10X Performance

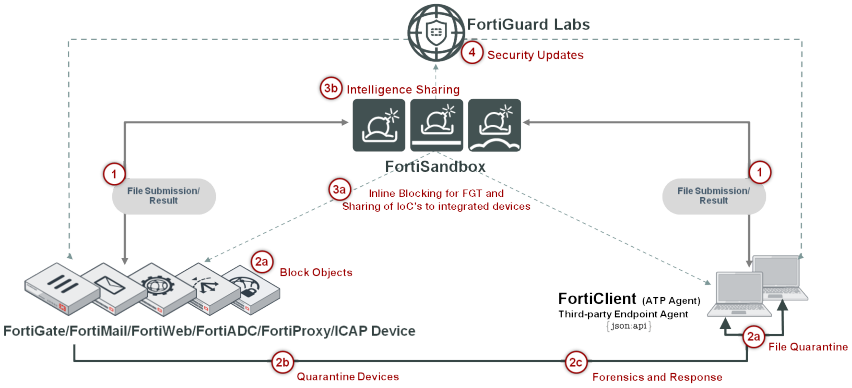
FortiSandbox 4.4 offers up to 10X increase in effective throughput where previously, processing 7,000 files per hour, our solution can now handle a staggering 70,000 files per hour. This monumental boost in performance empowers FortiSandbox customers to scale their security operations and analyze an expanded volume of potential threats in record time.

Real-Time Anti-Phishing Protection

Extra layer of defense against phishing attacks by detecting, blocking, and rating unrated malicious websites, protecting against spam email campaign or a targeted spear-phishing attack in real-time. Now, FortiSandbox customers can proactively safeguard their sensitive information and prevent costly phishing incidents.

Threat Mitigation

FortiSandbox uniquely integrates with various products through the Security Fabric platform that 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 FortiGuard Labs, to help protect organizations globally. Figure 1 describes the automated mitigation process flow.



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) teams to download captured packets, original file, tracer log, malware screenshot. STIX 2.0 compliant IOCs provide rich threat intelligence and actionable insight after files are examined (see Figure 2).

FortiSandbox also allows SecOps teams to optionally record a video or interact with the malware in a simulated environment.

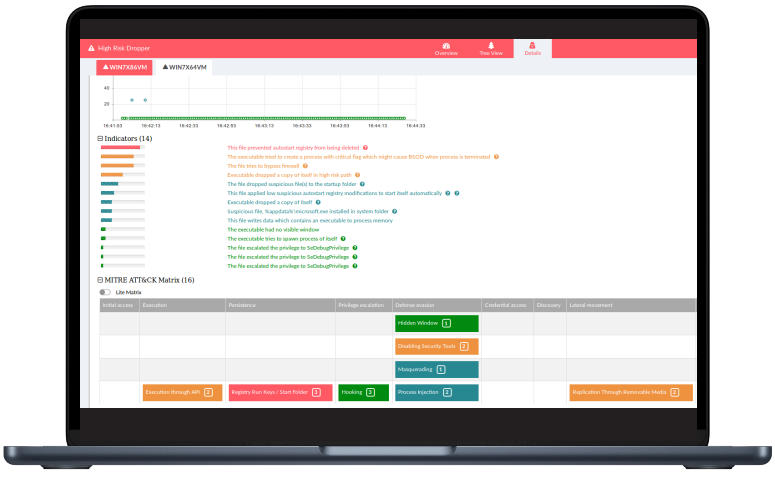


Figure 2 - MITRE ATT&CK Matrix with Built-in Tools

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. The integration provides suspicious content submission, timely remediation, and reporting capabilities.

This integration extends to other FortiSandboxes allowing 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

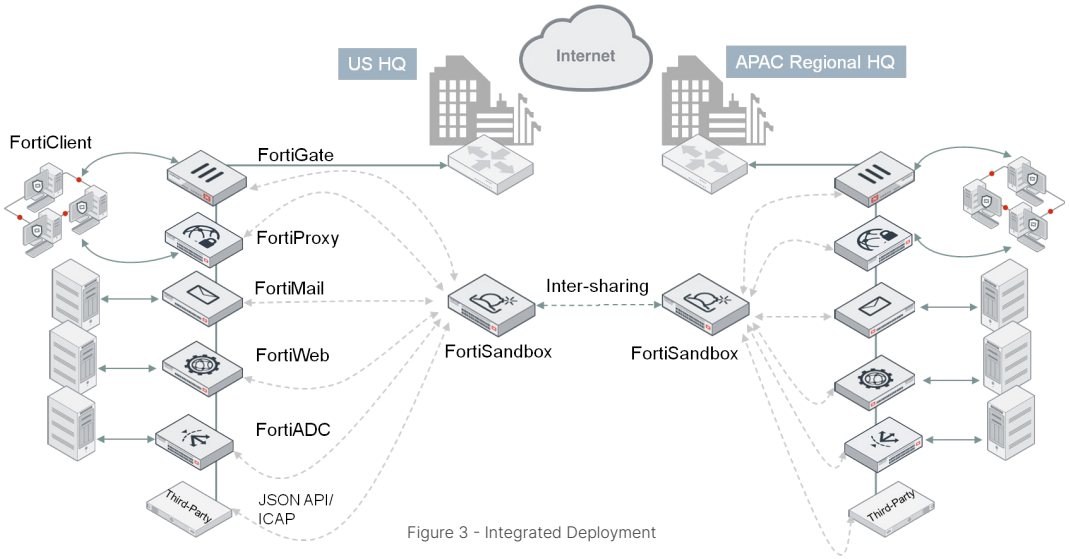


Figure 3 - Integrated Deployment

Standalone

This FortiSandbox deployment mode accepts inputs from spanned switch ports or network taps and emails via MTA or BCC mode. It also facilitates SecOps Analysts on-demand file uploads or scanning of file repositories via CIFs, NFS, AWS S3, and Azure Blob. 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, offering lower operational costs. Fortinet maintains, updates, and operates the service on your behalf.

Features Summary

Advanced Threat Protection

- Inline blocking to detect and protect against Zero-day Malware including ransomware
- Real-time identification of Zero-day Phishing sites including spam and malware-hosted sites
- AI-powered static code analysis identifying possible threats within non-running code
- Deep learning powered VM-Less emulation of Windows executable codes (PEXBox)
- Network threat detection in sniffer mode. Identify botnet activities and network attacks, malicious URL visits
- Sandbox Community Cloud for shared analysis within the worldwide community of FortiSandbox deployments

System Integration Support

- File and URL submission by Security Fabric devices
  - 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
- Sniffer mode. HTTP, FTP, POP3, IMAP, SMTP, SMB
- Proxy inspection via ICAP
- MTA/BCC mode via SMTP
- NetShare Scan mode via CIFs, NFS, AWS S3, and Azure Blob
- Dynamic Threat Intelligence DB update of malicious file checksum and URL
- JSON API to automate uploading samples and downloading actionable malware indicators to remediate
- Remote and secured logging with FortiAnalyzer, FortiSIEM, CEF servers and syslog servers

Deployment

- File submission from integrated device(s)
- Sniffer mode deployment with TCP RST support to reset client's connection with the suspicious server
- Network Share Scan with large file support (e.g., ISO images, network shared folders, SMB/NFS, AWS S3, and Azure Blob)
- Proxy adapter submission with multi-tenancy support
- OT deployment with supported services: BACnet, HTTP, IPMI, Modbus, S7comm, SNMP, TFTP
- High-availability with Primary and Secondary nodes for redundancy
- Port monitoring for cluster fail-over
- Clustering up to 99 worker nodes for higher throughput
- Air-gapped networks support
- Aggregate interface support for increased bandwidth and redundancy
- Isolated administrative traffic from VM image traffic

Features Summary continued

Advanced Scan (Static AI Scan) Features

- Integrated with FortiGuard's full Antivirus database of heuristic and checksum signatures
- Intelligent adaptive scan profile that optimizes sandbox resources based on submissions
- Parallel scan to run multiple distinct VM types simultaneously
- Extracts URLs embedded in QR Code
- Scan URLs embedded inside document files
- Integrate with third-party Yara rules
- Cloud query for latest known Malware and clean files
- File checksum whitelist and blacklist options
- Scan URLs from submitted emails and files
- Rating Engine Plus that leverages the latest FortiGuard ML rating
- VM scan ratio for efficient utilization of VMs

Sandboxing (Dynamic AI Scan) Support

- AI-powered behavioral analysis constantly learning new malware and ransomware techniques
- Concurrent Sandbox instances
- OS type supported: Windows 11/10/8.1/7, macOS, Linux, Android, and ICS systems
- Customizable VMs for Windows and Linux OS
- Configurable internet browser supporting Internet Explorer, Microsoft Edge, Google Chrome, and Mozilla Firefox
- Sandbox interactive mode
- Video-recording of malware interaction
- Anti-evasion detection techniques
    - API Obfuscation
    - Bare-metal Detection
    - Command and Control
    - Direct System Calls
    - Execution Delay
    - Memory Only Payload
    - Process Hollowing/Injection
    - Runtime Encryption/Packing
    - System Fingerprinting
    - Time Bomb
    - User Files Check
    - User Interaction Check
    - VM/Sandbox Detection
- Callback detection. Malicious URL visit, botnet C&C communication, and attacker traffic from activated malware

- Downloadable captured packets, tracer logs, and screenshots
- File Types Support
    - Windows Executables: .bat, .cab, .cmd, .dll, .exe, .js, .msi, .ps1, .vbs, wsf
    - Microsoft Office: .doc, .docm, .docx, .dot, .dotm, .dotx, .iqy, .one, .pot, .potm, .potx, .ppt, .pptm, .pptx, .ppam, .pps, .ppsm, .ppsx, .pub, .rtf, .sldm, .sldx, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, xltx
    - Document/Email files: .eml, .pdf, .rl
    - Android files: .apk
    - Linux files: .elf
    - MacOS files: .app, .dmg, Mach-O
    - Web files: .htm, html, .lnk, WEBLink
    - Compress files: .7z, .ace, .arj, .bz2, .gz, .iso, .jar, .kgb, .lzh, .rar, .swf, .tar, .tgz, .upx, .xz, .z, .zip
- User-defined extensions

Features Summary continued

Monitoring And Reporting

- Dashboard widgets for connectivity and services, license status, scan performance, system resources
- Scan performance page for tracking historical usage
- 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 including actions, malware name, rating, type, source, destination, detection time, and download path
- Reports and logging. GUI, download PDF, and raw log file
- Detailed Job Report generation
- Periodic logs of system status and performance
- Periodic log generation of scan statistics and system resource usage
- MITRE ATT&CK v11 support
- Download tracer logs, PCAP, and indicators in STIX 2.0 format
- Notification emails when a malicious file is detected
- Weekly reports to global email lists and administrators

Administration

- Configuration via GUI and CLI
- Multiple administrator accounts supporting full or view only access
- Radius authentication for administrators
- Single Sign-On via SAML
- Self-Check widget for configurations, connectivity, and services
- Cluster management page for administering the HA and cluster nodes
- Centralized search page allowing administrators to build customized search conditions
- Upload any license from a single convenient page
- VM status monitoring
- Automatic engine and signature updates
- Automatic check for new VM image availability
- System health check alerting system
- NTP via FortiGuard support
- Backup, restore, and revision of system configuration
- Consolidated CLI for troubleshooting
- Option to auto-submit suspicious files to cloud service for manual analysis and signature creation
- Option on NetShare scan mode to prioritize and forward files to a third-party scanning for further scanning

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 FortiOS 7.4.1	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	6000	8000	12 000	68 000
Static Analysis Throughput[4] (Files/Hr)					10 000	18 000	28 000	160 000
Dynamic Analysis Throughput[5] (Files/Hr)					250	500	800	1600
FortiMail Throughput[6] (Emails/Hr)		200 – 40 000	1000 – 40 000	1000 – 40 000	60 000	80 000	120 000	600 000
Number of Users[7]		8 – 1600	40 – 1600	40 – 1600	1000	2000	3200	6400
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 v4.4.0
4. Includes receiving, job handling, AV engine, Yara engine, Cloud Query; measured based on v4.4.0
5. Previously called "Sandboxing VM Throughput"; measured based on v4.4.0 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 with 10% on Dynamic Scan
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	SOC2[2]			FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST				
Data Privacy	Data Privacy Practice[3]							
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.

2 Visit the Fortinet SOC2 certification page here.

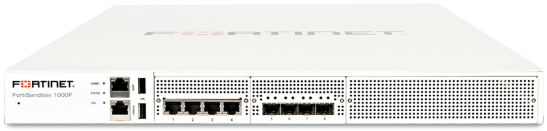
3 Visit the Fortinet Data Privacy Practice Datasheet here.

Integration Matrix

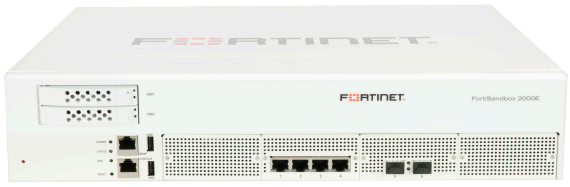
	CLOUD				APPLIANCES
Product	**SaaS**	**Inline Sandbox**	**FortiSandbox Cloud (PaaS)**	**Private/Public Cloud**	**VM / Hardware**
FORTIGATE	FortiOS V6.2+	FortiOS V7.2.1+, FortiOS V7.4.1+ (PaaS)	FortiOS V6.4.2+, 6.2.5+	FortiOS V5.6+	
FORTICLIENT	FortiClient for Windows OS V6.2+		FortiClient for Windows 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+	

Hardware Appliances

FortiSandbox 500F



FortiSandbox 1000F/-DC

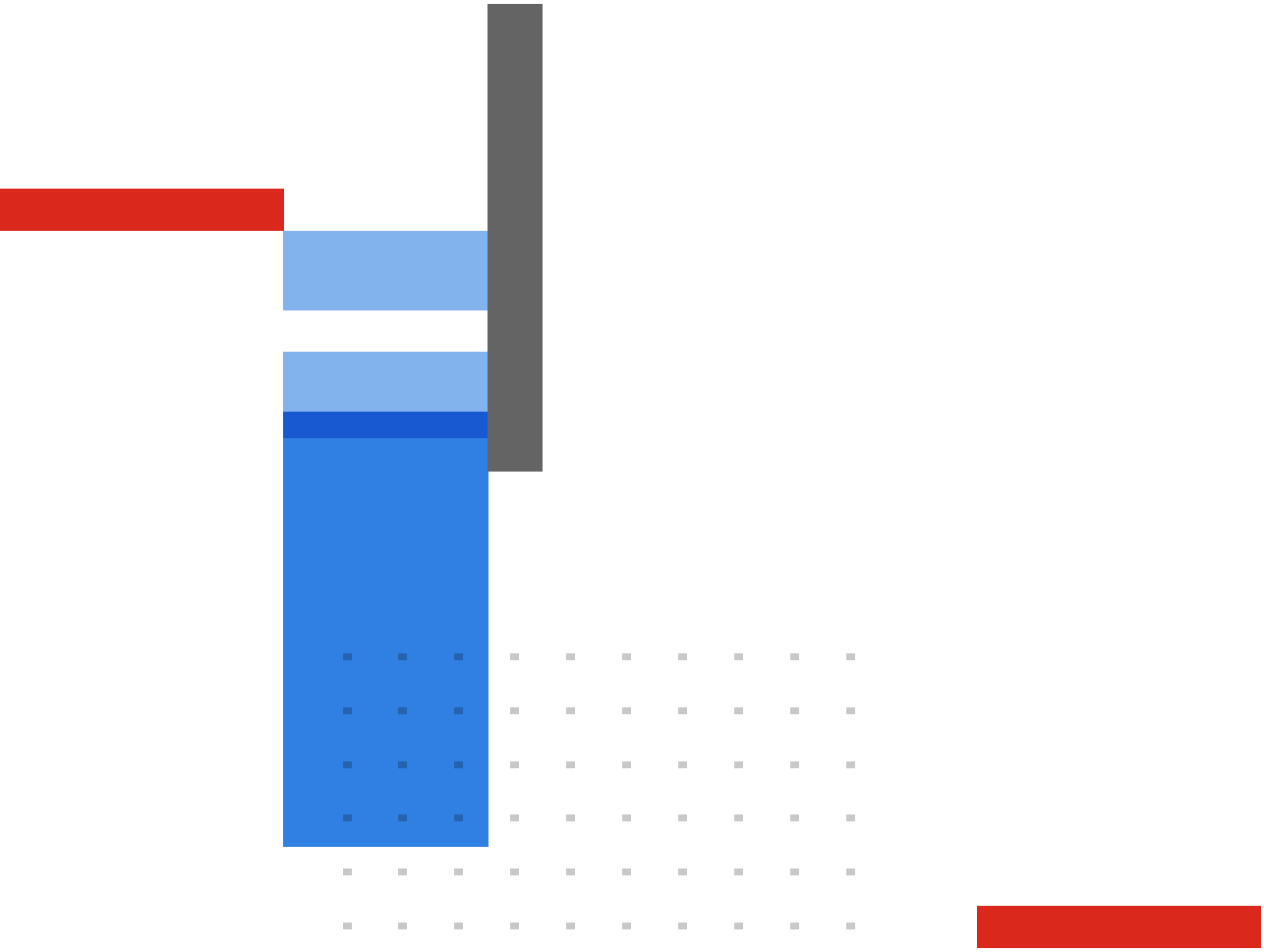


FortiSandbox 2000E

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

August 30, 2023

FSA-DAT-R52-20230830