FORTINET

ORDERING GUIDE

FortiSandbox

AI-powered sandbox malware analysis
Inline block breach protection
MITRE ATT&CK-based report

Available in

Hardware Appliance | VM Appliance | Public Cloud | Fortinet-Hosted

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 IT and OT environments.

FortiSandbox is offered from different cloud services and on-premise appliances:

- **Sandbox As-a-service (SaaS):** subscription services for FortiGate (and FortiMail and FortiClient) to support either:
  - **Detection:** out-of-band sandboxing, alerting, reporting, and log enrichment for SOC response.
  - **Detection and Prevention:** prioritized and high capacity to support inline sandboxing plus SOCaaS log ingestion.
- **SOC Platforms:** multiple form factors to aid SOC teams in detection, prevention, and threat hunting:
  - **Fortinet-hosted Cloud:** subscription service (platform as-a-service (PaaS)) FortiSandbox with dedicated VM resource for dedicated performance and centralization of reports and threat intelligence across Fortinet estate.
  - **Public Cloud:** cloud-based FortiSandbox on Azure/AWS/OCI/GCP cloud.
  - **Dedicated Appliance:** on-premise FortiSandbox with guaranteed response time and detection.

	AS-A-SERVICE		SOC PLATFORMS
	ADVANCED MALWARE PROTECTION	INLINE MALWARE PREVENTION	CLOUD/APPLIANCES
FortiGate Integration			
Detection (Visibility and Log Enrichment)	✓	✓	✓
Accelerated AI Prefilter		✓	✓ Supported
Prevention (Inline Blocking)		✓	✓
Security Operations			
SOC Integration	SaaS monitoring of threats plus data (log) enrichment	Inline blocking of detected threats plus data (log) enrichment	Advanced sandbox GUI including MITRE ATT&CK techniques, sandbox execution timelines, and more

PRODUCT OFFERINGS

Flexible FortiGate, FortiClient, and FortiMail Offerings

Sandbox Detection Service is bundled with the FortiGate's Advanced Malware Protection (AMP) service, including antivirus, mobile malware, and other components. This service provides out-of-band sandbox detection and log enrichment with a cloudbased SaaS portal for SOC admins.

Sandbox Detection and Prevention Service is a new a la carte service, which includes inline blocking for sandbox and AI/NDR detections, plus log enrichment for SOC teams.

Both services are currently available in the North America, Europe, and Asia regions. Similar service offerings are available for FortiClient and FortiMail products.

	AS-A-SERVICE	
	ADVANCED MALWARE PROTECTION	**INLINE MALWARE PREVENTION**
FortiGate Integration		
Detection (Visibility and Log Enrichment)	✓	✓
Accelerated AI Prefilter		✓
Prevention (Inline Blocking)		✓
Security Operations		
SOC Integration	SaaS monitoring of threats, plus data (log) enrichment.	Inline blocking of detected threats, plus data (log) enrichment
Detection Capabilities		
AI-based Static Behavior Analysis		✓ Accelerated[1]
Antievasion Detection	✓	✓
C&C Detection	✓	✓
AV, IPS, Web Filtering	✓	✓
Sandboxing VMs		
Cloud VMs	✓	✓ Prioritized[2]
Supported OS		
Windows[3]	✓	✓
Additional Services		
24×7 Support	✓	✓

[1] Integrated with FortiNDR's Artificial Neural Network capability for fast pre-filtering.
[2] Submissions to the shared service are handled with priority and allowed double the capacity.
[3] Based on configured file types on the antivirus profile.

ORDER INFORMATION

The following table shows an example of the a la carte SKUs for the FortiGate-60F. The same SKUs are available for FortiGate models.

	SKU
Hardware and Support	
FG-60F	FG-60F
24×7 FortiCare Support	FC-10-0060F-247-02-DD
A la Carte - FortiGuard Security Services	
FortiGuard Advanced Malware Protection (AMP) Service	FC-10-0060F-100-02-DD
FortiGuard AI-based Inline Malware Prevention Service	FC-10-0060F-577-02-DD

SOC AUGMENTATION

On-Premise, Cloud, and Hosted Options

FortiSandbox PaaS is a Fortinet-hosted platform (FortiCloud) available on a subscription basis, providing the same capabilities as hardware and virtual appliances. The subscription provides a dedicated FortiSandbox VM through FortiCloud and utilizes Cloud VMs for dynamic analysis. It is currently available in the North America and Europe regions.

FortiSandbox Virtual Appliances are available for public cloud and private cloud deployments.

FortiSandbox Hardware Appliances are available in a range of performance levels for different size organizations.

	CLOUD		HARDWARE		
	FORTISANDBOX PAAS	PRIVATE/PUBLIC CLOUD	500G	1500G	3000F
FortiGate Capabilities					
Detection (Visibility and Log Enrichment)	✓	✓	✓	✓	✓
Accelerated AI Prefilter	✓	✓ Supported[1]	✓ Supported[1]	✓ Supported[1]	✓ Supported[1]
Prevention (Inline Blocking)	✓	✓	✓	✓	✓
System Performance					
Effective Sandboxing Throughput (Files/Hr)	5,000[2]	7,500[3]	10,000	32,000	68,000
Static Analysis Throughput (Files/Hr)	10,000[2]	15,000[3]	20,000	80,000	160,000
Dynamic Analysis Throughput (Files/Hr)	160[2]	160[3]	400	1,000	1,600
FortiMail Throughput[4] (emails/hour)	50,000	75,000	100,000	320,000	680,000
Number of Users[5]	650	1,000	1,400	4,000	6,400
MTA Adapter Throughput (emails/hour)			10,000	32,000	68,000
Sniffer Mode Throughput (Gbps)		1	0.5	4	9.6
Detection Capabilities					
AI-based Static Behavior Analysis	✓	✓	✓	✓	✓
Antievasion Detection	✓	✓	✓	✓	✓
C&C Detection	✓	✓	✓	✓	✓
AV, IPS, Web Filtering	✓	✓	✓	✓	✓
Sandboxing VMs					
Default Local VMs		0	2	2	8
Local or Custom VM Expansion Capacity		8 (Private/BYOL) 128 (PAYG)[6]	+12	+26	+64
Cloud VM Expansion Capacity	1 - 200	1 - 200	5 - 200[7]	5 - 200[7]	5 - 200[7]
Supported OS					
Windows	✓	✓	✓	✓	✓
MacOS, Linux, Android	✓ Limited[7]	✓	✓	✓	✓
Custom OS		✓	✓	✓	✓
OT Simulation		✓ / —	✓	✓	✓
System Information					
Type	Cloud Subscription	Virtual Machine	1RU Appliance	1RU Appliance	2RU Appliance
1G RJ45		Hardware Dependent	✓	✓	✓
10G SFP+		Hardware Dependent		✓	✓

[1] Tested based on files with 80% documents and 20% executables; measured based on v4.4.2. Includes both Static and Dynamic analysis with pre-filtering enabled.

[2] Tested on Flavor-1 VM (with 4 CPUs and 8GB RAM) and 8 VMs. A higher VM flavor with more resources will produce higher throughput and is provided on more VM subscriptions. To inquire about VM flavors contact your account representative.

[3] Tested on a Hyper-V (with 12 CPUs and 32GB RAM) and 8 VMs.

[4] Based on a ratio of one email with attachment to 10 emails.

[5] Based on a ratio of one user per 25 emails on 10 hour period with 10% on Dynamic Scan.

[6] Based on number of cores multiplied by 4.

[7] Limited to Static Analysis only.

Note that all form factors include the same set of advanced detection capabilities below:

	CLOUD		HARDWARE		
	FORTISANDBOX PAAS	PRIVATE/PUBLIC CLOUD	500G	1500G	3000F
Security Services					
Fortinet Security Fabric Integration	Centralized	Centralized	Centralized	Centralized	Centralized
Fabric Partners		✓	✓	✓	✓
Adapters, API, Network Share, and Sniffer	Via API only	✓	✓	✓	✓
Dynamic Analysis Time	3-5 minutes	3-5 minutes	3-5 minutes	3-5 minutes	3-5 minutes
AI-based Static Behavior Analysis	✓	✓	✓	✓	✓
Anti-evasion Detection	✓	✓	✓	✓	✓
C&C Detection	✓	✓	✓	✓	✓
AV, IPS, Web Filtering	✓	✓	✓	✓	✓
Additional Services					
24×7 Support	✓	✓	✓	✓	✓

ORDER INFORMATION

The following table shows the SKUs for PaaS, VM subscriptions, and hardware appliances.

PaaS is simply licensed based on the capacity needed:

PAAS	SKU
Base	
+1 Cloud Expansion (all supported OS)	FC1-10-SACLP-433-01-DD
+5 Cloud Expansion (all supported OS)	FC2-10-SACLP-433-01-DD
Real-time Zero-Day Anti-Phishing Service	FC-10-SACLP-682-02-DD
FortiCloud Premium (pre-requirement)	FC-15-CLDPS-219-02-DD

VM licensing is comprised of the base VM license combined with flexible expansion options:

VIRTUAL MACHINE	SKU
Base	
Base License	FSA-VM00
Local VM Expansion and Add-Ons	
+1 Microsoft Windows 10 VM License	FSA-VM-WIN10-1
+1 Microsoft Windows 11 VM License[1]	FSA-UPG-VM-WIN11-1
+1 Microsoft Office 2021 License[2]	FSA-UPG-OFFICE2021-1
+8 Custom VMs License	FSA-VM00-UPG-LIC-BYOL
Cloud VM Expansion	
+5 Cloud Expansion Windows	FC-10-FSA01-195-02-DD
+2 Cloud Expansion MacOS	FC-10-FSA01-192-02-DD
Subscriptions	
Sandbox Threat Intelligence	FC-10-FSV00-500-02-DD
Real-time Zero-Day Anti-Phishing Service	FC-10-FSV00-682-02-DD
FortiCare Premium Support Only[3]	FC-10-FSV00-248-02-DD

[1] Supported by FortiSandbox 4.4.0.

[2] Supported by FortiSandbox 4.4.0.

[3] For HA Cluster deployment setup, configured as a primary or secondary node used as a dispatcher only. Supported by FortiSandbox 4.2.1.

Hardware can be purchased as fully-loaded bundles or customized as needed:

HARDWARE	500G	1500G	3000F
Hardware Bundles			
Local or Custom VM Base + Expansion Capacity	2+12	2+26	8+64
Hardware Bundle with Licensed VMs	FSA-500G FSA-500G-UPG-WIN-LIC-2 (6) FC-10-FS5HG-499-02-DD	FSA-1500G FSA-1500G-UPG-WIN-LIC-2 (13) FC-10-FS15G-499-02-DD	FSA-3000F FSA-3000F-UPG-LIC-32 (2) FC-10-SA3KF-499-02-DD
Hardware Bundle with Custom VMs	FSA-500G FSA-500G-UPG-LIC-BYOL FC-10-FS5HG-499-02-DD	FSA-1500G FSA-1500G-UPG-LIC-BYOL FC-10-FS15G-499-02-DD	FSA-3000F FSA-3000F-UPG-LIC-BYOL FC-10-SA3KF-499-02-DD
Cloud VM Expansion			
+5 Cloud Expansion Windows	FC-10-FSA01-195-02-DD		
Add-on Licenses			
+1 Microsoft Windows 11 License[1]	FSA-UPG-HW-WIN11-1		
+1 Microsoft Office 2021 License[2]	FSA-UPG-OFFICE2021-1		
100-1000 Mailbox MTA License	FC1-10-FSA01-321-02-DD		
1001-5000 Mailbox MTA License	FC2-10-FSA01-321-02-DD		
5000+ Mailbox MTA License	FC3-10-FSA01-321-02-DD		
Subscription			
Renewal (Sandbox Threat Intelligence)[3]	FC-10-FS5HG-499-02-DD	FC-10-FS15G-499-02-DD	FC-10-SA3KF-499-02-DD
Real-time Zero-Day Anti-Phishing Service	FC-10-FS5HG-682-02-DD	FC-10-FS15G-682-02-DD	FC-10-SA3KF-682-02-DD

[1] Supported by FortiSandbox 4.4.0.

[2] Supported by FortiSandbox 4.4.0.

[3] Sandbox Threat Intelligence is a subscription service for Antivirus, IPS, Web Filtering, File Query, Industrial Security, Sandbox engine, plus 24×7 FortiCare.

FREQUENTLY ASKED QUESTIONS

What is the best strategy for sizing a sandbox deployment?

Following are suggested approaches when sizing the file throughput (files per hour):

- **Estimate:** based on FortiGate, FortiMail and FortiClient platform using average of actual customer submission count. See local Fortient partner and sales representative for a sizing report.
- **Ideal:** determined during POC.

For best results, engage your regional CSEs. FortiSandbox supports clustering up to 99 devices to further increase VM capacity. See the FortiSandbox Administration Guide.

FORTINET TRAINING

FortiSandbox Training

Learn how to protect your organization and improve its security against advance threats that bypass traditional security controls. You will learn about how FortiSandbox detects advanced threats. You will also learn about how FortiSandbox dynamically generates local threat intelligence, and how the advanced threat protection (ATP) components leverage this threat intelligence information to protect organizations from advanced threats. This course does not have a certification exam.

Course Description

For more information about prerequisites, agenda topics and learning objectives, please refer to the course description at https://training.fortinet.com/local/staticpage/view.php?page=library_fortisandbox

Ordering Information

SKU	DESCRIPTION
FT-FSA	Instructor-led Training - 2 full days or 4 half days
FT-FSA-LAB	On-demand Labs (self-paced)

Visit www.fortinet.com for more details

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.