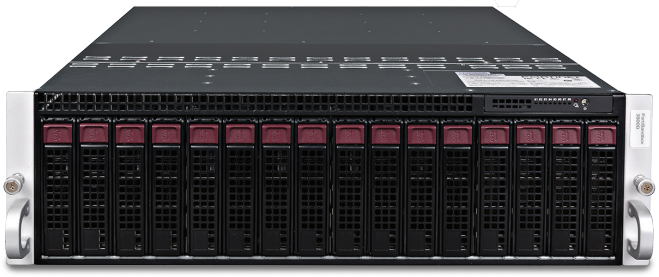
FortiSandbox™

FortiSandbox 1000D, 3000E, 3500D, FortiSandbox-VM and FortiSandbox Cloud

Today's most sophisticated cybercriminals are increasingly bypassing traditional antimalware solutions and inserting advanced persistent threats deep within networks. These highly targeted attacks evade established signature-based detection by masking their malicious nature in many ways — compression, encryption, polymorphism, the list of techniques goes on.



Some have even begun to evade virtual "sandbox" environments using VM detection, "time bombs" and more. Fighting today's attacks requires a comprehensive and integrated approach — more than antimalware. More than a virtual sandbox. More than a separate monitoring system.

FortiSandbox offers a robust combination of proactive detection and mitigation, actionable threat insight and integrated and automated deployment. At its foundation is a unique, dual-level sandbox which is complemented by Fortinet's award-winning antimalware and optional integrated FortiGuard threat intelligence. Years of Fortinet threat expertise is now packaged up and available on site or in the cloud via FortiSandbox.

Proactive Detection and Mitigation

Suspicious codes are subjected to multi-layer pre-filters prior to execution in the virtual OS for detailed behavioral analysis. The highly effective pre-filters include a screen by our AV engine, queries to cloud-based threat databases and OS-independent simulation with a code emulator, followed by execution in the full virtual runtime environment. Once a malicious code is detected, granular ratings along with key threat intelligence is available, a signature is dynamically created for distribution to integrated products and full threat information is optionally shared with FortiGuard Labs for the update of global threat databases.

Actionable Insight

All classifications — malicious and high/medium/low risk — are presented within an intuitive dashboard. Full threat information from the virtual execution — including system activity, exploit efforts, web traffic, subsequent downloads, communication attempts and more — is available in rich logs and reports.

Highlights

- Unique multi-layer prefilters aid fast and effective threat detection
- Rich reporting provides full threat lifecycle visibility
- Inspection of many protocols in one appliance simplifies deployment and reduces cost
- Integration and automation with Fortinet threat prevention products enhances rather than duplicates security infrastructure

FortiCare Worldwide 24/7 Support

support.fortinet.com

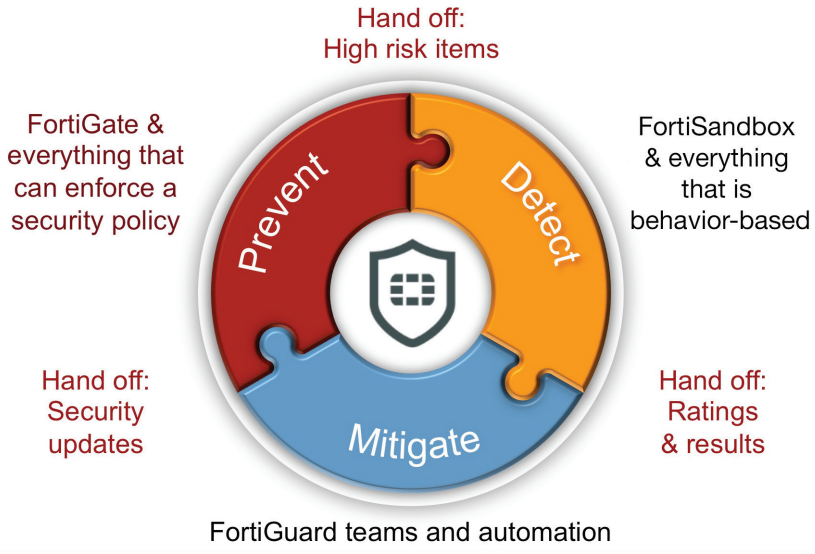
FortiGuard Security Services

www.fortiguard.com

ADVANCED THREAT PROTECTION FRAMEWORK

The most effective defense against advanced targeted attacks is founded on a cohesive and extensible protection framework. The Fortinet framework uses security intelligence across an integrated solution of traditional and advanced security tools for network, application and endpoint security, and threat detection to deliver actionable, continuously improving protection.

Fortinet integrates the intelligence of FortiGuard Labs into FortiGate next generation firewalls, FortiMail secure email gateways, FortClient endpoint security, FortiSandbox advanced threat detection, and other security products to continually optimize and improve the level of security delivered to organizations with a Fortinet solution.



Prevent Attacks

Fortinet next generation firewalls, secure email gateways, web application firewalls, endpoint security and similar solutions use security such as antivirus, web filtering, IPS, and other traditional security techniques to quickly and efficiently prevent known threats from impacting an organization.

Detect and Analyze Threats

FortiSandbox and other advanced detection techniques step in to detect “Zero-day” threats and sophisticated attacks, delivering risk ratings and attack details necessary for remediation.

Mitigate Impact and Improve Protection

In a Fortinet solution, detection findings can be used to trigger prevention actions to ensure the safety of resources and data until remediation is in place. Finally, the entire security ecosystem updates to mitigate any impact from future attacks through the strong, integrated threat intelligence research and services of FortiGuard Labs.

FORTINET SECURITY FABRIC

Fortinet is the only company with security solutions for network, endpoint, application, data center, cloud, and access designed to work together as an integrated and collaborative security fabric.

Simply deploying security end to end is not enough. These solutions must work together to form a cooperative fabric that can scale to cover the entire network, with different security sensors and tools that are aware of each other and operate as a single entity, even when sourced from multiple vendors. Further components must collect, coordinate, and respond to any potential threat in real-time with actionable intelligence. This is where FortiSandbox and the broader Advanced Threat Protection solution set fits.

DEPLOYMENT OPTIONS

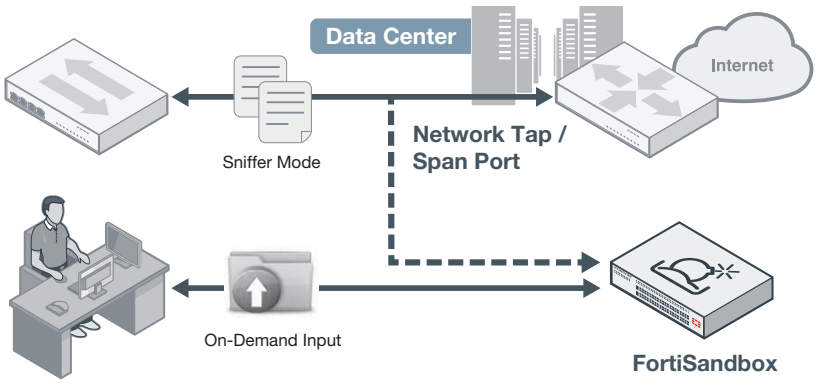
Easy Deployment

FortiSandbox supports inspection of many protocols in one unified solution, thus simplifies network infrastructure and operations. Further, it integrates with FortiGate as a new capability within your existing security framework.

The 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 also have all three input options at the same time.

Standalone

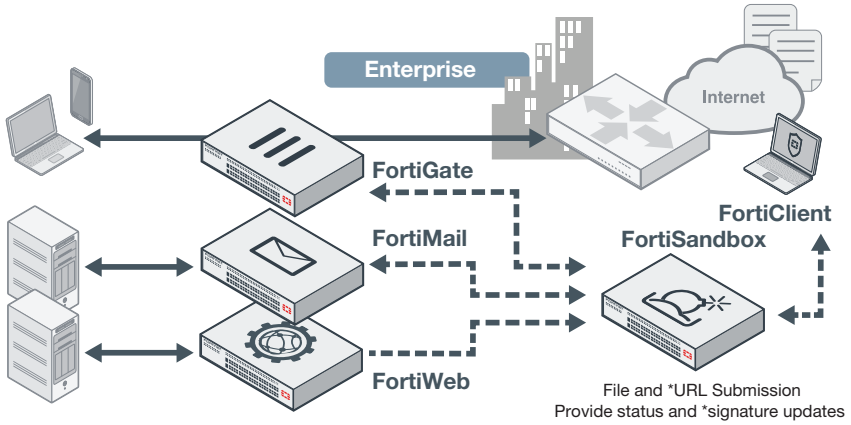
This deployment mode relies on inputs from spanned switch ports or network taps. It may also include administrators' on-demand file uploads using the GUI. It is the most suitable infrastructure for adding protection capabilities to existing threat protection systems from various vendors.



Integrated

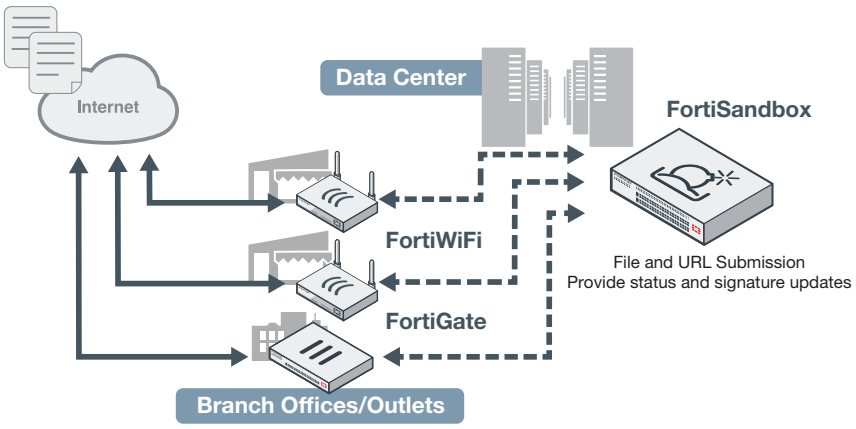
Various Fortinet products, namely FortiGate, FortiMail, FortiWeb and FortiClient can intercept and submit suspicious content to FortiSandbox when they are configured to interact with FortiSandbox. The integration will also provide timely remediation and reporting capabilities to those devices.

* Not applicable to FortIWeb

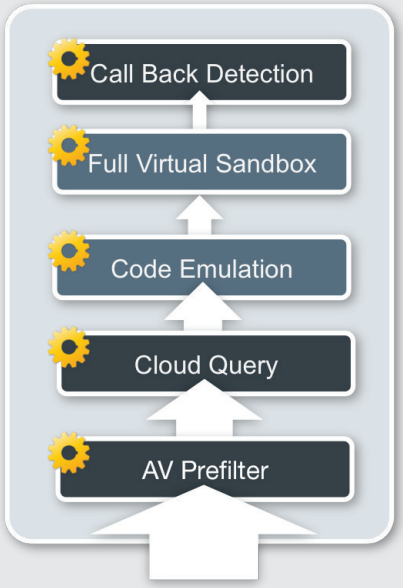


Distributed

This deployment is attractive for organizations that have distributed environments, where FortiGates are deployed in the branch offices and submit suspicious files to a centrally-located FortiSandbox. This setup yields the benefits of lowest TCO and protects against threats in remote locations.



FEATURES



Multi-tiered file processing optimizes resource usage that improves security, capacity and performance

AV Engine
- Applies top-rated (95%+ Reactive and Proactive) AV Scanning. Serves as an efficient pre-filter.

Cloud Query
- Real-time check of latest malware information
- Access to shared information for instant malware detection

Code Emulation
- Quickly simulates intended activity
- OS independent and immune to evasion/obfuscation

Full Virtual Sandbox
- Secure run-time environment for behavioral analysis/rating
- Exposes full threat lifecycle information

Call Back Detection
- Identifies the ultimate aim, call back and exfiltration

FEATURES SUMMARY

ADMINISTRATION

Supports WebUI and CLI configurations

Multiple administrator account creation

Configuration file backup and restore

Notification email when malicious file is detected

Weekly report to global email list and FortiGate administrators

Centralized search page which allows administrators to build customized search conditions

Frequent signature auto-updates

Automatic check and download new VM images

VM status monitoring

Radius Authentication for administrators

NETWORKING/DEPLOYMENT

Static Routing Support

File Input: Offline/sniffer mode, On-demand file upload, file submission from integrated device(s)

Option to create simulated network for scanned file to access in a closed network environment

High-Availability Clustering support

Port monitoring for fail-over in a cluster

SYSTEMS INTEGRATION

File Submission input: FortiGate, FortiClient, FortiMail, FortiWeb

File Status Feedback and Report: FortiGate, FortiClient, FortiMail, FortiWeb

Dynamic Threat DB update: FortiGate, FortiClient, FortiMail
– Periodically push dynamic DB to registered entities.
– File checksum and malicious URL DB

Update Database proxy: FortiManager

Remote Logging: FortiAnalyzer, syslog server

Web-based API with which users can upload samples to scan indirectly

Bit9 end point software integration

ADVANCED THREAT PROTECTION

Virtual OS Sandbox:
– Concurrent instances
– OS type supported: Windows XP, Windows 7, Windows 8.1, Windows 10 and Android
– Anti-evasion techniques: sleep calls, process and registry queries
– Callback Detection: malicious URL visit, Botnet C&C communication and attacker traffic from activated malware
– Download Capture packets, Original File, Tracer log and Screenshot

File type support: .7z, .ace, .apk, .arj, .bat, .bz2, .cab, .cmd, .dll, .doc, .docm, .docx, .dot, .dotm, .dotx, .exe, .gz, .htm, html, .jar, .js, .kgb, .lnk, .lzh, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip

Protocols/applications supported:
– Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB
– 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 FortiWeb: HTTP
– Integrated mode with ICAP Client: HTTP

Customize VMs with support file types support

Isolate VM image traffic from system traffic

Network threat detection in Sniffer Mode: Identify Botnet activities and network attacks, malicious URL visit

Scan SMB/NFS network share and quarantine suspicious files. Scan can be scheduled

Scan embedded URLs inside document files

Integrate option for third partyYara 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

MONITORING AND REPORT

Real-Time Monitoring Widgets (viewable by source and time period options): Scanning result statistics, scanning activities (over time), top targeted hosts, top malware, top infectious urls, top callback domains

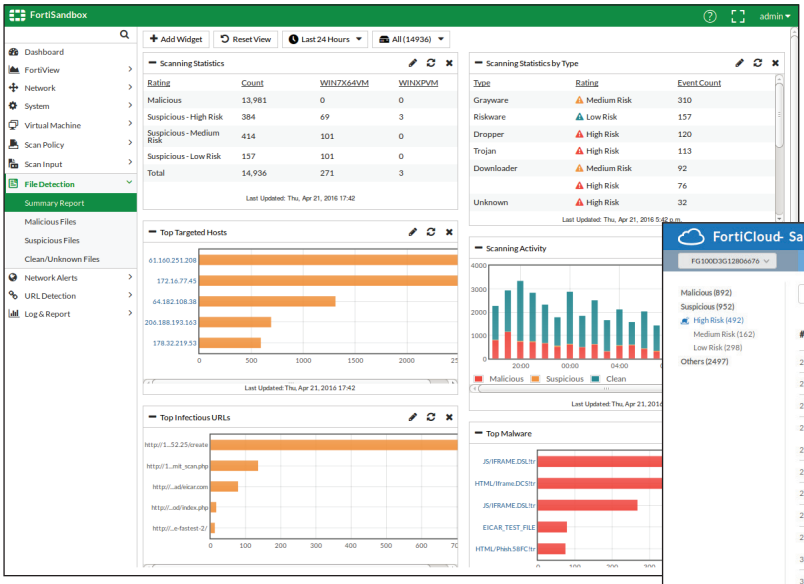
Drilldown Event Viewer: Dynamic table with content of actions, malware name, rating, type, source, destination, detection time and download path

Logging — GUI, download RAW log file

Report generation for malicious files: Detailed reports on file characteristics and behaviors – file modification, process behaviors, registry behaviors, network behaviors, vm snapshot, behavior chronology chart

Further Analysis: Downloadable files — Sample file, Sandbox tracer logs, PCAP capture and Indicators in STIX format

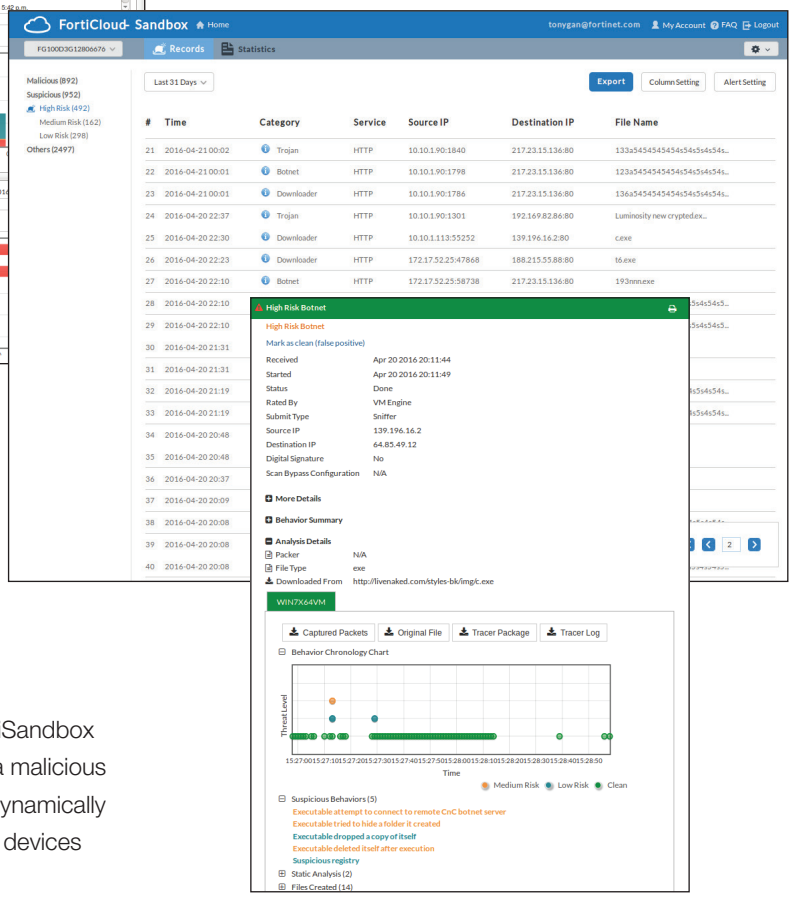
FEATURES



Dashboard widgets — real-time threat status

VM Sandboxing

Complement your established defenses with cutting-edge capability — analyzing suspicious and high-risk files in a contained environment to uncover the full attack lifecycle using system activity and callback detection.

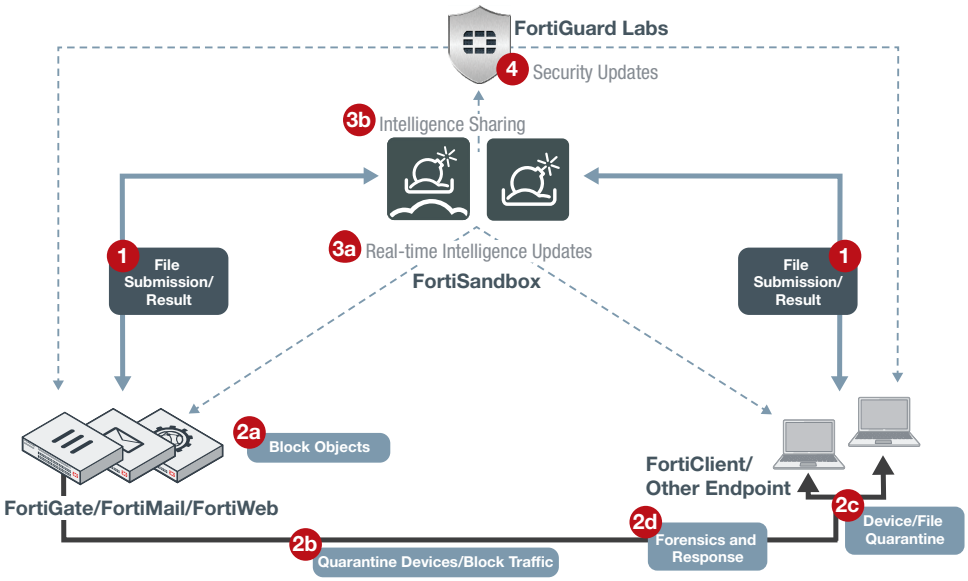


File Analysis Tools

Reports with captured packets, original file, tracer log and screenshot provide rich threat intelligence and actionable insight after files are examined. This is to speed up remediation and updated protection.

Remediation

Fortinet's ability to uniquely integrate various products with FortiSandbox offers automatic protection with incredibly simple setup. Once a malicious code is determined, the analyzer will develop and forward the dynamically generated signature to all registered devices and clients. These devices then examine subsequent files against the latest DB.



Query

1. File submission for analysis, results returned

Mitigate

- 2a Block objects held at mail gateway
- 2b Quarantine devices, block traffic by firewall
- 2c Quarantine file or device by endpoint protection
- 2d Further investigate and respond

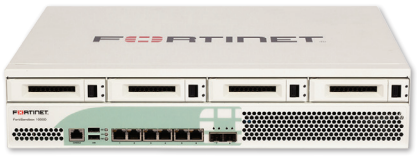
Update

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

SPECIFICATIONS

	FSA-1000D	FSA-3000E	FSA-3500D
Hardware			
Form Factor	2 RU	2 RU	3 RU (with default 5 nodes, up to 8 maximium)
Total Network Interfaces	6x GE RJ45 ports, 2x GE SFP slots	4x GE RJ45 ports, 2x 10 GE SFP+ slots	20x GE RJ45 ports, 10x 10 GE SFP+ slots (4x GE RJ45 ports, 2x 10 GE SFP+ slots per node)
Storage Capacity	4 TB (max. 8 TB)	8 TB HDD (max. 24 TB)	10 TB (2 TB per node) HDD
Power Supplies	2x Redundant PSU	2x Redundant PSU	2x Redundant PSU
System			
VM Sandboxing (Files/Hour)	160	1,120	720* (Upgradable** to 1,200) (160 per node)
AV Scanning (Files/Hour)	6,000	15,000	30,000* (Upgradable** to 48,000) (6,000 per node)
Number of VMs	8	56***	36* (Upgradable** to 60) (8 per node)
Dimensions			
Height x Width x Length (inches)	3.5 x 17.2 x 14.5	3.5 x 17.2 x 25.5	5.2 x 17.5 x 29.5
Height x Width x Length (mm)	89 x 437 x 368	89 x 437 x 647	133 x 445 x 749
Weight	27.60 lbs (12.52 kg)	43 lbs (19.52 kg)	88 lbs (39.92 kg)
Environment			
Power Consumption (Average / Maximum)	115 / 138 W	538.6 / 549.6 W	625 / 735.6 W
Maximum Current	100V/5A, 240V/3A	100–240V / 9.8–5A	12A@100V, 8A@240V
Heat Dissipation	471 BTU/h	1,943.82 BTU/h	2,728.9 BTU/h
Power Source	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz
Humidity	5–95% non-condensing	8–90% (non-condensing)	8–90% (non-condensing)
Operation Temperature Range	32–104°F (0–40°C)	50–95°F (10– 35°C	50–95°F (10– 35°C)
Storage Temperature Range	-13–158°F (-25–70°C)	-40 –158°F (-40–70°C	-40 –158°F (-40–70°C)
Compliance			
Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST		

* Based on the assumption that 1 blade will be used as master in HA-cluster mode.
** By adding 3 more SAM-3500D nodes to the same chassis.
*** 8 Windows VM licenses included with hardware, remaining 48 sold as an upgrade license.



FortiSandbox 1000D

FortiSandbox 3000E

FortiSandbox 3500D

	FORTISANDBOX-VM	FORTISANDBOX CLOUD
Hardware Requirements		
Hypervisor Support	VMware ESXi version 5.1 or later, Citrix XenServer 6.2 or later, Linux KVM CentOS 7.2 or later	N.A
Virtual CPUs (Minimum / Maximum)	4 / Unlimited (Fortinet recommends that the number of vCPUs match the number of Windows VM +4.)	N.A
Memory Support (Minimum / Maximum)	8 GB / Unlimited	N.A
Virtual Storage (Minimum / Maximum)	30 GB / 16 TB	N.A
Total Virtual Network Interfaces (Minimum)	6	N.A
System		
VM Sandboxing (Files/Hour)	Hardware dependent	–
AV Scanning (Files/Hour)	Hardware dependent	–
Number of VMs	4 to 54 (Upgrade via appropriate licenses)	–

INTEGRATION MATRIX

		FORTIGATE	FORTICLIENT	FORTIMAIL	FORTIWEB
FSA Appliance and VM	File Submission	*FortiOS V5.0.4+	FortiClient for Windows OS V5.4+	FortiMail OS V5.1+	FortiWeb OS V5.4+
	File Status Feedback	*FortiOS V5.0.4+	FortiClient for Windows OS V5.4+	FortiMail OS V5.1+	FortiWeb OS V5.4+
	File Detailed Report	*FortiOS V5.4+	FortiClient for Windows OS V5.4+	FortiMail OS V5.1+	–
	Dynamic Threat DB Update	*FortiOS V5.4+	FortiClient for Windows OS V5.4+	FortiMail OS V5.3+	FortiWeb OS V5.4+
FortiSandbox Cloud	File Submission	*FortiOS V5.2.3+	–	FortiMail OS V5.3+	FortiWeb OS 5.5.3+
	File Status Feedback	*FortiOS V5.2.3+	–	FortiMail OS V5.3+	FortiWeb OS 5.5.3+
	File Detailed Report	*FortiOS V5.2.3+	–	–	–
	Dynamic Threat DB Update	*FortiOS V5.4+	–	FortiMail OS V5.3+	FortiWeb OS 5.5.3+

*some models may require CLI configuration

ORDER INFORMATION

Product	SKU	Description
FortiSandbox 1000D	FSA-1000D	Advanced Threat Protection System — 6x GE RJ45, 2x GE SFP slots, redundant PSU, 8 Windows licenses and 1 Microsoft Office license included.
FortiSandbox 3000E	FSA-3000E	Advanced Threat Protection System — 4x GE RJ45, 2x 10 GE SFP+ slots, redundant PSU, 8 VMs with WinXP, Win7, Win8.1, Win10 and 1 Microsoft Office license included.
FortiSandbox 3500D	FSA-3500D	Advanced Threat Protection System — 3U 8-slot chassis with redundant PSU, 5x SAM-3500D nodes with 20x GE RJ45, 5x 10 GE SFP+ slots, 36 VMs with WinXP, Win7, Win8, Win10 and 5 Microsoft Office licenses included.
SandboxModule 3500D	SAM-3500D	Advanced Threat Protection Node — 4x GE RJ45, 2x 10 GE SFP+ slots, 8 VMs with WinXP, Win7, Win8, Win10 and 1 Microsoft Office licenses included.
FortiSandbox-VM	FSA-VM-BASE	Base license for stackable FortiSandbox-VM. 4 Windows licenses and 1 Microsoft Office license included. FSA-VM maximum expansion limited to 54 total VMs.
FortiSandbox Cloud Service	FC-10-00XXX-123-02-12	FortiSandbox Cloud Service Subscription (SKU varied by FortiGate models).
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.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 KIFER ROAD
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990