# FortiSandbox™

FortiSandbox 1000D, 2000E, 3000E, 3500D, FortiSandbox-VM, and FortiSandbox Cloud

Fortinet's top-rated FortiSandbox is at the core of the Advanced Threat Protection (ATP) solution that integrates with Fortinet's Security Fabric to address the fast moving and more targeted threats across a broad attack surface. Specifically, it delivers real-time actionable intelligence through the automation of zero-day, advanced malware detection and mitigation.

## Broad Coverage of the Attack Surface with Security Fabric

Effective defense against advanced targeted attacks through a cohesive and extensible architecture working to protect network, application layers and endpoint devices.

## Automated Zero-day, Advanced Malware Detection and Mitigation

Native integration and open APIs automate the submission of objects from Fortinet and third-party vendor protection points, and the sharing of threat intelligence in real time for immediate threat response.

## Certified and Top Rated

Constantly undergoes rigorous, real-world independent testing and consistently earns top marks.

### Deployment Modes

Standalone
Integrated

### FortiGuard Security Services

www.fortiguard.com

### FortiCare Worldwide 24/7 Support

support.fortinet.com

### Third-Party Certifications

NSS LABS RECOMMENDED

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

DATA SHEET

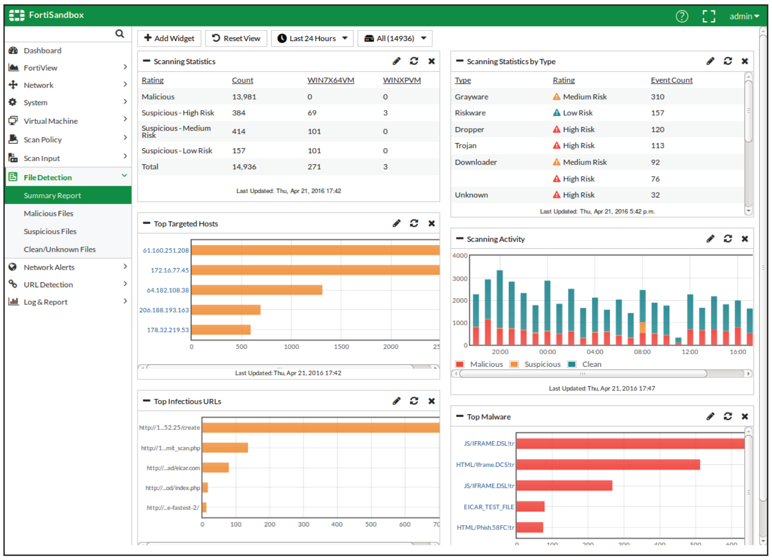
# FEATURES

## Sandbox Malware Analysis

Complement your established defenses with a two-step sandboxing approach. Suspicious and at-risk files are subjected to the first stage of analysis with Fortinet's award-winning AV engine, FortiGuard global intelligence query*, and code emulation. Second stage analysis is done in a contained environment to uncover the full attack lifecycle using system activity and callback detection. Figure 1 depicts new threats discovered in real time.

In addition to supporting FortiGate, FortiMail, FortiWeb, and FortiClient (ATP Agent) file submission, third-party security vendor offerings are supported through a well-defined open API set.

* a real time IoC check for emerging threats (known good and bad) within the Sandbox community



Scanning Statistics

| Rating | Count | WIN7X64VM | WINXPVM |
|---|---|---|---|
| Malicious | 13,981 | 0 | 0 |
| Suspicious - High Risk | 384 | 69 | 3 |
| Suspicious - Medium Risk | 414 | 101 | 0 |
| Suspicious - Low Risk | 157 | 101 | 0 |
| Total | 14,936 | 271 | 3 |

Last Updated: Thu, Apr 21, 2016 17:42

Scanning Statistics by Type

| Type | Rating | Event Count |
|---|---|---|
| Grayware | Medium Risk | 310 |
| Riskware | Low Risk | 157 |
| Dropper | High Risk | 120 |
| Trojan | High Risk | 113 |
| Downloader | Medium Risk | 92 |
|  | High Risk | 76 |
| Unknown | High Risk | 32 |

Last Updated: Thu, Apr 21, 2016 5:42 p.m.

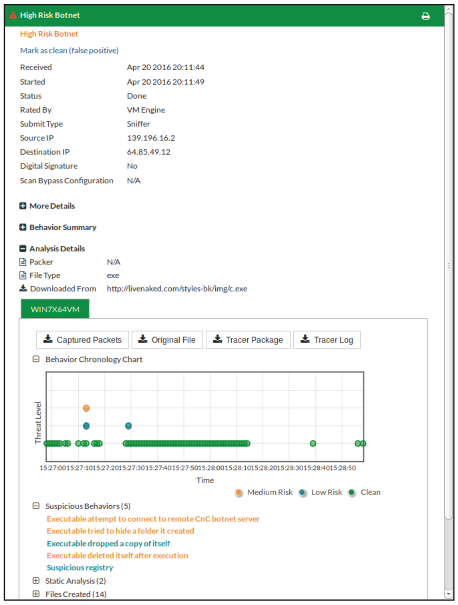
Figure 1: Widget-based real-time threat status dashboard

## Reporting and Investigative Tools

Reports with captured packets, original file, tracer log, and screenshot provide rich threat intelligence and actionable insight after files are examined (see Figure 2). This is to speed up remediation.

## Threat Mitigation

Fortinet's ability to uniquely integrate various products with FortiSandbox offers automatic protection with incredibly simple setup. Once a malicious code is identified, the FortiSandbox will return risk ratings and the local intelligence is shared in real time with Fortinet and third-party vendor-registered devices and clients to remediate and immunize against new advanced threats. The local intelligence can optionally be shared with Fortinet threat research team, FortiGuard Labs, to help protect organizations globally. Figure 3 steps through the flow on the automated mitigation process.



High Risk Botnet

High Risk Botnet

Mark as clean (false positive)

| | |
|---|---|
| Received | Apr 20 2016 20:11:44 |
| Started | Apr 20 2016 20:11:49 |
| Status | Done |
| Rated By | VM Engine |
| Submit Type | Sniffer |
| Source IP | 139.196.16.2 |
| Destination IP | 64.85.49.12 |
| Digital Signature | No |
| Scan Bypass Configuration | N/A |

More Details

Behavior Summary

Analysis Details

| | |
|---|---|
| Packer | N/A |
| File Type | exe |
| Downloaded From | http://livenaked.com/styles-bk/img/c.exe |

WIN7X64VM

Captured Packets | Original File | Tracer Package | Tracer Log

Behavior Chronology Chart

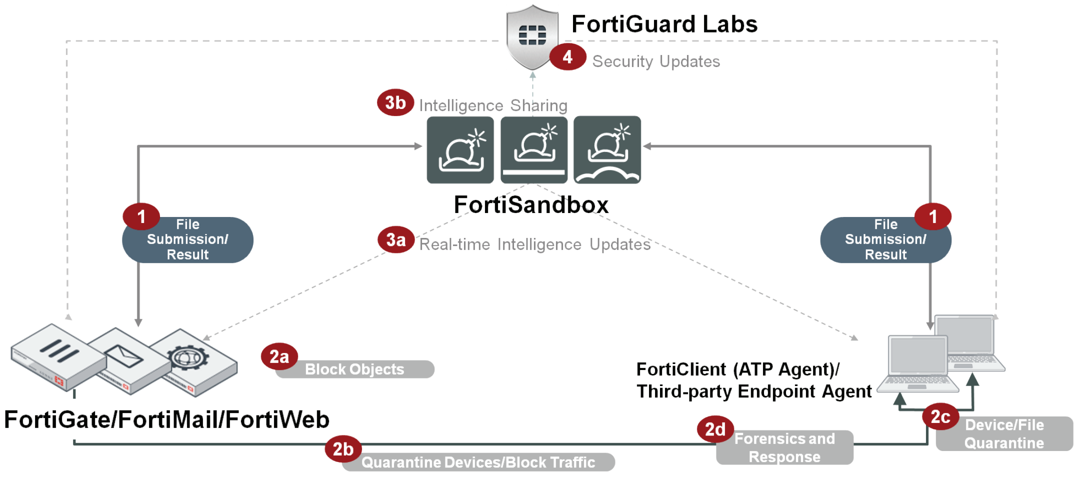
Suspicious Behaviors (5)

Executable attempt to connect to remote CnC botnet server
Executable tried to hide a folder it created
Executable dropped a copy of itself
Executable deleted itself after execution
Suspicious registry

Static Analysis (2)

Files Created (14)

Figure 2: Detailed malware report with built-in tools


FortiGuard Labs
4 Security Updates
3b Intelligence Sharing
FortiSandbox
1 File Submission/ Result
3a Real-time Intelligence Updates
1 File Submission/ Result
2a Block Objects
FortiGate/FortiMail/FortiWeb
FortiClient (ATP Agent)/ Third-party Endpoint Agent
2b Quarantine Devices/Block Traffic
2d Forensics and Response
2c Device/File Quarantine

**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

Figure 3: FortiSandbox threat mitigation workflow

# DEPLOYMENT OPTIONS

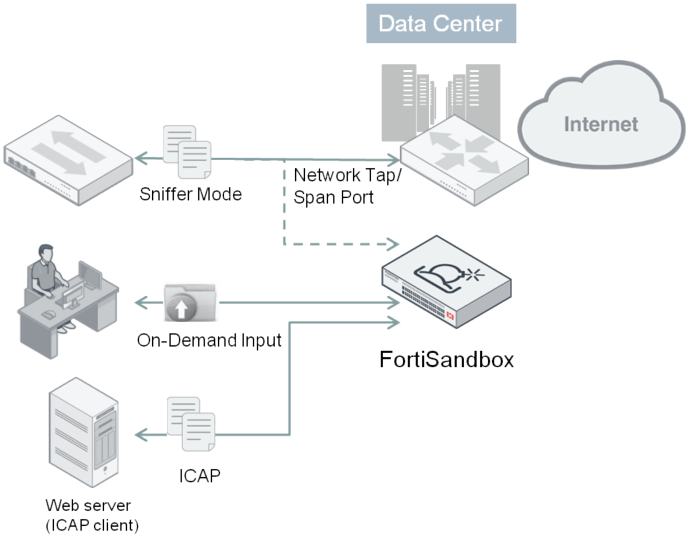
## Easy Deployment

FortiSandbox supports inspection of many protocols in one unified solution, thus simplifies network infrastructure and operations. Further, it integrates within the Security Fabric adding a layer of advanced threat protection to your existing security architecture.

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 choose to combine these deployment options.

### Standalone

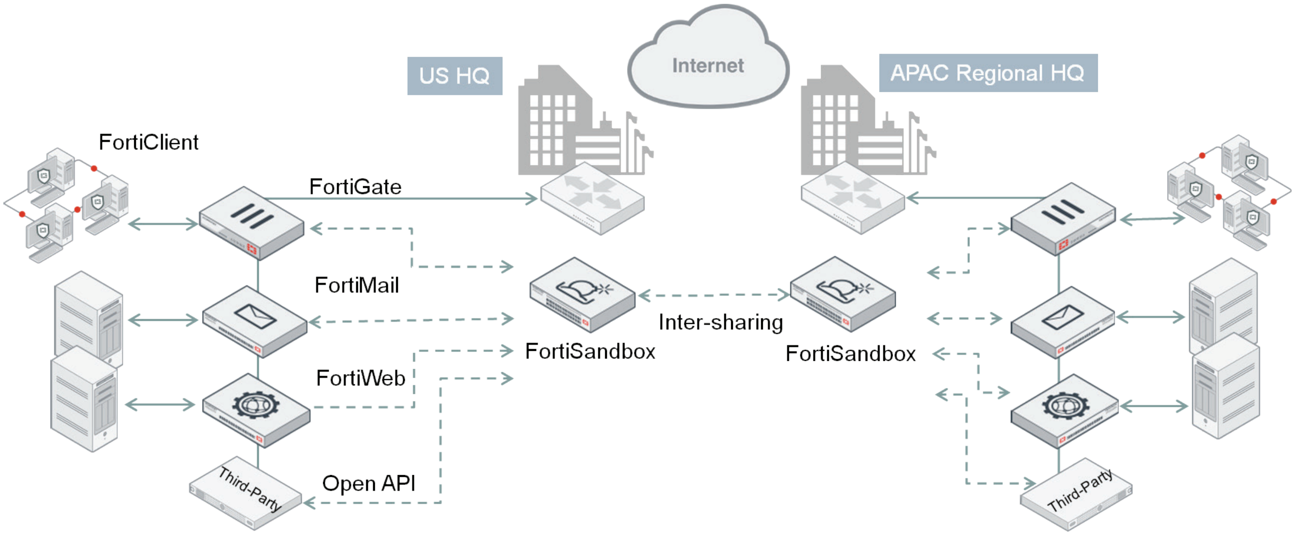
This FortiSandbox deployment mode accepts inputs as an ICAP server or from spanned switch ports or network taps. It may also include administrators' on-demand file uploads using the GUI. It is the most suitable infrastructure for adding protection capabilities to existing threat protection systems from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



### Integrated

Fortinet products, such as FortiGate, FortiMail, FortiWeb, FortiClient (ATP Agent) and third-party security vendors 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.

This integration extends to other FortiSandboxes to allow instantaneous sharing of real-time intelligence. This 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.



# 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 (ATP agent), 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

JSON API to automate the process of uploading samples and downloading actionable malware indicators to remediate

Certified third-party integration: CarbonBlack, Ziften

Inter-sharing of IOCs between FortiSandboxes

## ADVANCED THREAT PROTECTION

Inspection of new threats including ransomware and password protected malware mitigation

Static Code analysis identifying possible threats within non-running code

Heuristic/Pattern/Reputation-based analysis

Virtual OS Sandbox:
– Concurrent instances
– OS type supported: Windows XP*, Windows 7, Windows 8.1, Windows 10, macOS, 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, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .exe, .gz, .htm, html, .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, 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 for supporting various file types

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-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

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

* Supported in a custom VM

# SPECIFICATIONS

| | FSA-1000D | FSA-2000E | FSA-3000E | FSA-3500D |
|---|---|---|---|---|
| **Hardware** | | | | |
| Form Factor | 2 RU | 2U | 2 RU | 3 RU (with default 5 nodes, up to 8 maximium) |
| Total Network Interfaces | 6x GE RJ45 ports,<br>2x GE SFP slots | 4x GE RJ45 ports,<br>2x 10 GE SFP+ slots | 4x GE RJ45 ports,<br>2x 10 GE SFP+ slots | 20x GE RJ45 ports,<br>10x 10 GE SFP+ slots<br>(4x GE RJ45 ports, 2x 10 GE SFP+ slots per node) |
| Storage | 2x 2 TB | 2x 2 TB | 4x 2 TB | 5x 2 TB (2 TB per node) |
| Power Supplies | 2x Redundant PSU | 2x Redundant PSU | 2x Redundant PSU | 2x Redundant PSU |
| **System Performance** | | | | |
| Number of VMs | 8 | 24*** | 56*** | 36* (Upgradable** to 60) (8 per node) |
| Sandbox Pre-Filter Throughput (Files/Hour) [1] | 6,000 | 12,000 | 15,000 | 30,000* (Upgradable** to 48,000) (6,000 per node) |
| VM Sandboxing Throughput (Files/Hour) | 160 | 480 | 1,120 | 720* (Upgradable** to 1,200) (160 per node) |
| Real-world Effective Throughput (Files/Hour) [2] | 480 | 1,440 | 3,360 | 2,160 (Upgradable** to 3,600) (480 per node) |
| Sniffer Throughput | 1 Gbps | 4 Gbps | 8 Gbps | 2 Gbps |
| **Dimensions** | | | | |
| Height x Width x Length (inches) | 3.5 x 17.2 x 14.5 | 3.46 x 17.24 x 20.87 | 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 | 88 x 438 x 530 | 89 x 437 x 647 | 133 x 445 x 749 |
| Weight | 27.60 lbs (12.52 kg) | 27 lbs (12.25 kg) | 43 lbs (19.52 kg) | 88 lbs (39.92 kg) |
| **Environment** | | | | |
| Power Consumption (Average / Maximum) | 115 / 138 W | 164.7 / 175.9 W | 538.6 / 549.6 W | 625 / 735.6 W |
| Maximum Current | 100V/5A, 240V/3A | 100V/8A, 240V/4A | 100V/9.8A, 240V/5A | 12A@100V/12A, 240V/8A |
| Heat Dissipation | 471 BTU/h | 600.17 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 | 100–240V AC, 60–50 Hz |
| Humidity | 5–95% non-condensing | 5–90% non-condensing | 8–90% (non-condensing) | 8–90% (non-condensing) |
| Operation Temperature Range | 32–104°F (0–40°C) | 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) | -4–158°F (-20–70°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.

*** 4(FSA-2000E)/8(FSA-3000E) Windows VM licenses included with hardware, remaining are sold as an upgrade license.

[1] FortiSandbox pre-filtering is powered by FortiGuard Intelligence.

[2] Measured based on real-world data when both pre-filter and dynamic analysis are working consecutively

FortiSandbox 1000D

FortiSandbox 2000E

FortiSandbox 3000E

FortiSandbox 3500D

| | FORTISANDBOX-VM | FORTISANDBOX CLOUD |
|---|---|---|
| **Hardware Requirements** | | |
| Hypervisor Support | VMware ESXi version 5.1 or later, Linux KVM CentOS 7.2 or later, Amazon Web Services (On-Demand) | N.A |
| Virtual CPUs (Minimum / Maximum) | 4 / Unlimited<br>(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 Performance** | | |
| VM Sandboxing (Files/Hour) | Hardware dependent | * |
| AV Scanning (Files/Hour) | Hardware dependent | * |
| Number of VMs | 8 VMs/node, up to a maximum of 99 nodes per cluster | * |
| Sniffer Throughput | 1 Gbps | N.A |

* Please refer to FortiCloud Sandbox Service Description

Note: All performance values are "up to" and vary depending on the environment and system configuration.

## 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 VMs with Win7 and (1) MS Office license included. |
| FortiSandbox 2000E | FSA-2000E | Advanced Threat Protection System — 4x GE RJ45, 2x 10 GE SFP+ slots, redundant PSU, 4 VMs with Win7, Win8, Win10 and (1) MS Office license included. Upgradable to a maximum of 24 licensed VMs. |
| FortiSandbox 3000E | FSA-3000E | Advanced Threat Protection System — 4x GE RJ45, 2x 10 GE SFP+ slots, redundant PSU, 8 VMs with Win7, Win8, Win10 and (1) MS Office license included. Upgradable to a maximum of 56 licensed VMs. |
| FortiSandbox 3500D | FSA-3500D | Advanced Threat Protection System — 3U 8-slot chassis with redundant PSU, 5x SAM-3500D blades with 20x GE RJ45, 10x 10 GE SFP+ slots, 36 VMs with WIn7, Win8, Win10 and (5) MS Office licenses included. Upgradable to a maximum of 60 licensed VMs. |
| SandboxModule 3500D | SAM-3500D | Advanced Threat Protection Blade: 4x GE RJ45, 2x 10 GE SFP+ slots, 8 VMs with WIn7, Win8, Win10 and (1) MS Office license included. |
| 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 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 | FC-10-XXXXX-123-02-12 | FortiSandbox Cloud Service Subscription (SKU varied by FortiGate/FortiMail/FortiWeb 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. |

FORTINET®
SILVER PARTNER

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