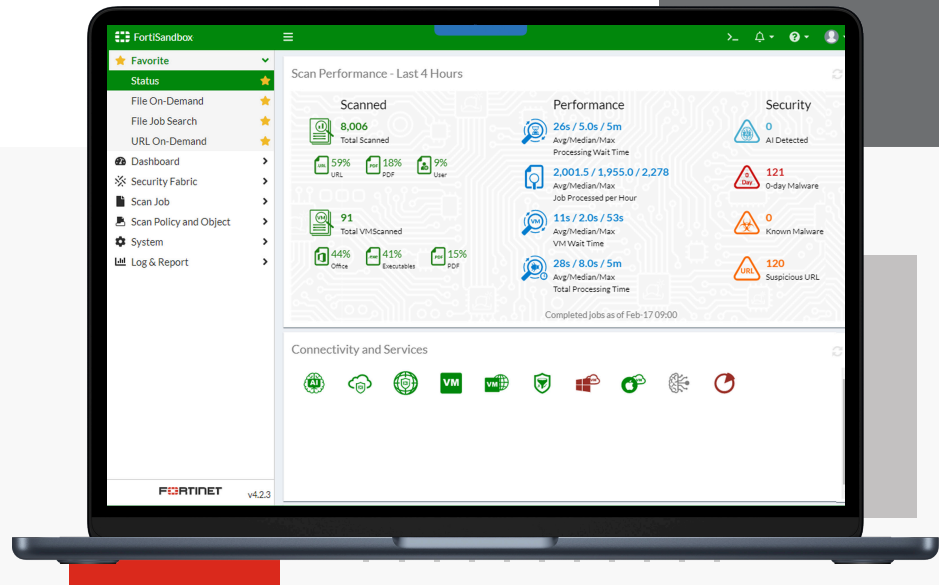# FortiSandbox and FortiGuard Sandbox Services

## 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.
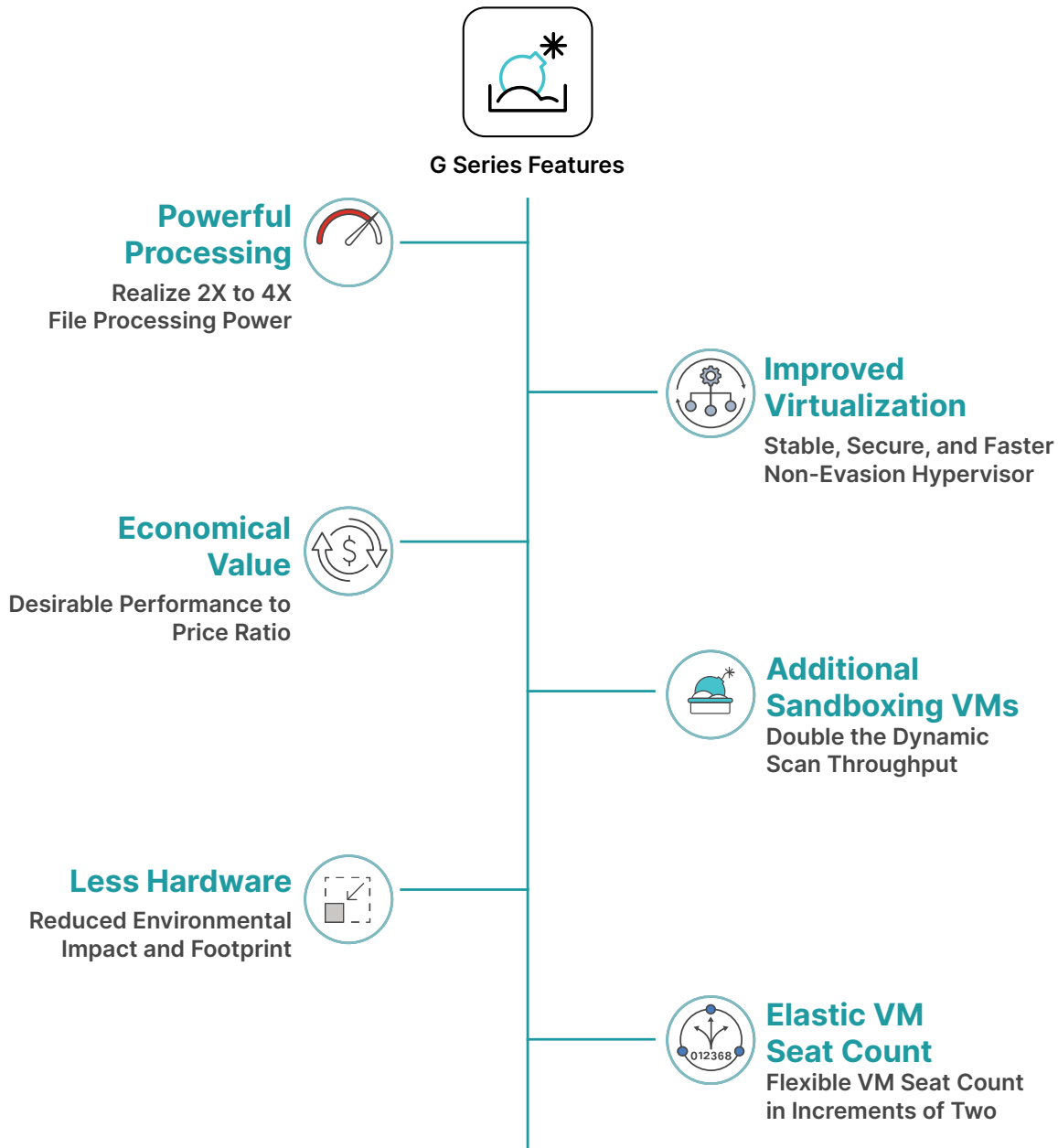
# Platform Evolution

### FortiSandbox G Series

Leveraging on our previous F and E models*, FortiSandbox 1500G and 500G provide cutting edge technological advancements performance, real-time sharing of threat intelligence across multiple geographical locations, and integrating Fortinet's Security Fabric and third party providers.

### Performance Optimization

With twice the VM capacity and file processing capabilities, our G Series delivers unparalleled stability, the highest detection accuracy, and best-breed throughput, while offering flexible and cost-effective deployment solutions.

**G Series Features**

**Powerful Processing**
Realize 2X to 4X File Processing Power

**Improved Virtualization**
Stable, Secure, and Faster Non-Evasion Hypervisor

**Economical Value**
Desirable Performance to Price Ratio

**Additional Sandboxing VMs**
Double the Dynamic Scan Throughput

**Less Hardware**
Reduced Environmental Impact and Footprint

**Elastic VM Seat Count**
Flexible VM Seat Count in Increments of Two

*The 500G replaces the 500F, and the 1500G replaces the 1000F and 2000E.

## Features

FortiSandbox is the most flexible threat-analysis appliance available as it offers various deployment options for unique configurations and requirements. Organizations can choose to combine these options.

### Security Fabric Integration

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 FortiSandbox solutions allowing instantaneous sharing of real-time intelligence. This feature benefits large enterprises that deploy multiple FortiSandbox solutions in different geo-locations. This zero touch automated model is ideal for holistic protection across different borders and time zones.
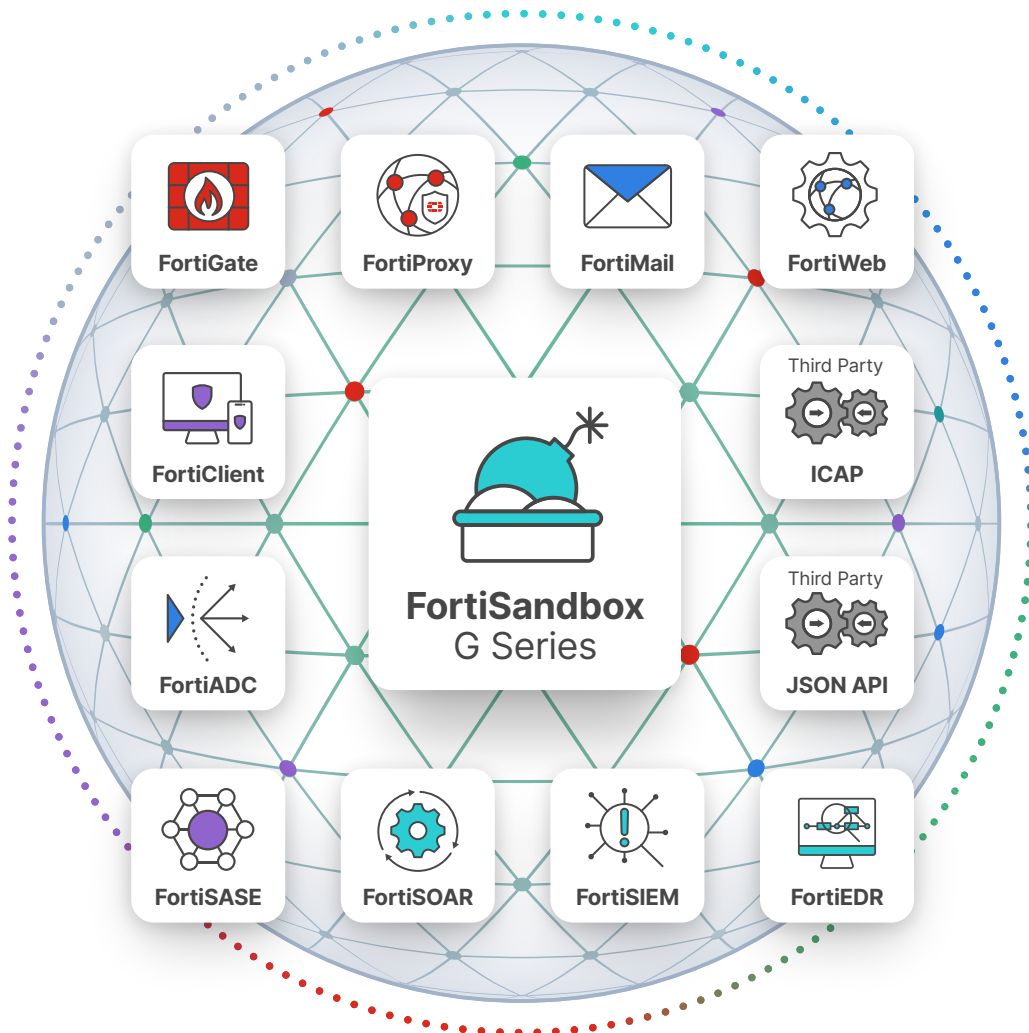
**Threat Mitigation**

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. The diagram following describes the automated mitigation process flow.
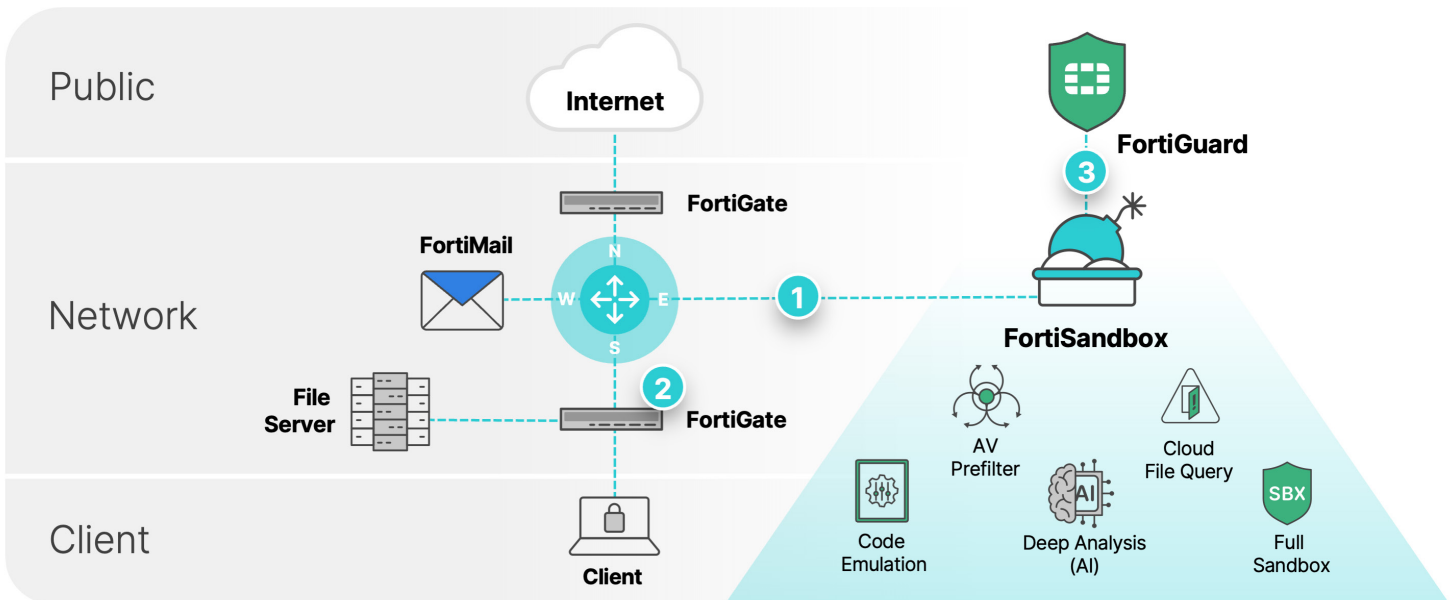


1. Submit file and URL for analysis from the FortiGate, FortiMail, client or file server.
2. Block suspicious file and URL inline on the device or quarantine on the client.
3. Share IoCs to the FortiGate devices (optional to FortiGuard) for intelligence sharing.

### 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 image below).

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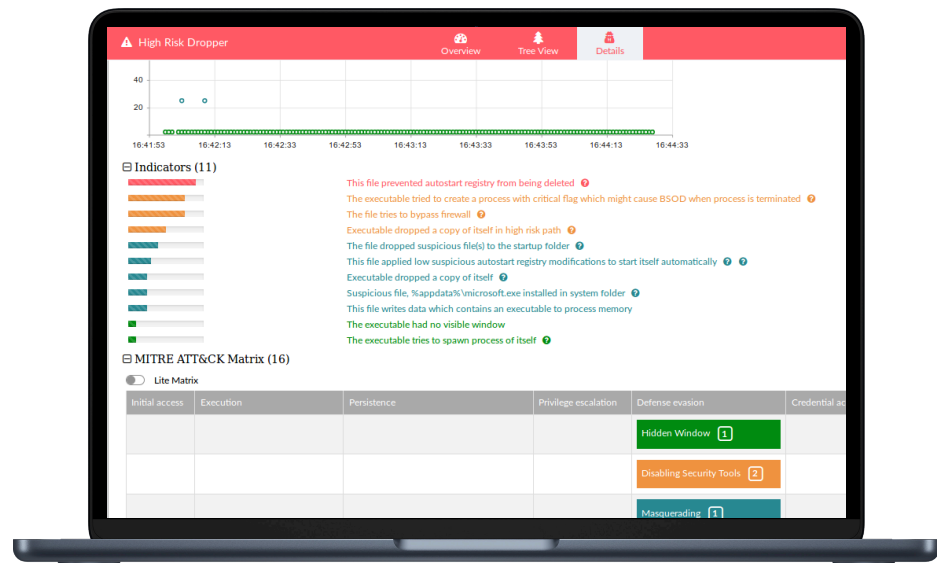


MITRE ATT&CK Matrix with Built-in Tools

### NetShare Scan

The FortiSandbox facilitates scanning of file repositories via CIFs, NFS, AWS S3 Buckets, and Azure Blob. This feature allows system admin and web hosting to sanitize any file sharing. It is the ideal option for enhancing an existing multi-vendor threat protection approach.

### HA-Cluster

The FortiSandbox natively supports clustering to expand the throughput capacity of up to 99 worker nodes. The HA feature provides redundancy for uninterrupted critical operation.

### 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 platform on your behalf.

### Real Time Anti-Phishing

The FortiSandbox v4.4 provides protection against zero-day phishing. The URLs extracted from emails and embedded from documents are processed in the FortiGuard cloud. The web pages are downloaded in real-time and analyze using patented technologies to determine any phishing signs.

## 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 the full FortiGuard 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-500G | FSA-1500G | FSA-3000F |
| Deployment | Fortinet-Hosted | Fortinet-Hosted | Azure, AWS, GCP, OCI | VM Appliance | Hardware Appliance | Hardware Appliance | Hardware Appliance |
| **FortiGate Capabilities** | | | | | | | |
| Detection (Visibility and Log Enrichment) | 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] |
| Prevention (Inline Blocking) | Yes[1] | Yes[9] | Yes | Yes | Yes | Yes | Yes |
| **Security Services** | | | | | | | |
| Fortinet Security Fabric Integration | Centralized | Centralized | 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 |
| AI-based Static Behavior Analysis | Yes[1] | 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 |
| 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 |
| **System Performance** | | | | | | | |
| Effective Sandboxing Throughput[3] (Files/Hr) | | 20 – 4000 | 100 – 1000 | 100 – 1000 | 10 000 | 32 000 | 68 000 |
| Static Analysis Throughput[4] (Files/Hr) | | | | | 20 000 | 80 000 | 160 000 |
| Dynamic Analysis Throughput[5] (Files/Hr) | | | | | 500 | 1000 | 1600 |
| FortiMail Throughput[6] (Emails/Hr) | | 200 – 40 000 | 1000 – 40 000 | 1000 – 40 000 | 100 000 | 320 000 | 680 000 |
| Number of Users[7] | | 8 – 1600 | 40 – 1600 | 40 – 1600 | 1400 | 4000 | 6400 |
| MTA Adapter Throughput (Emails/Hr) | | | | | 10 000 | 32 000 | 68 000 |
| Sniffer Mode Throughput (Gbps) | — | — | 1 | 1 | 0.5 | 4 | 9.6 |
| **Sandboxing VMs** | | | | | | | |
| Default Local VMs | | | 0 | 0 | 2 | 2 | +8 |
| Local or Custom VM Expansion Capacity | | | +8 | 8 | +12 | +26 | +64 |
| Cloud VM Expansion Capacity | | 1 - 200 | 5 - 200 | 5 - 200 | 5 - 200 | 5 - 200 | 5 - 200 |
| **Supported OS** | | | | | | | |
| Windows | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| MacOS, Linux, Android | | Yes[8] | Yes | Yes | Yes | Yes | Yes |
| Custom OS | | | Yes | Yes | Yes | Yes | Yes |
| OT Simulation | | | | | Yes | Yes | Yes |

1. Supported on FortiGate as add-on AI-Based Inline Sandbox Prevention Service
2. Integration support with FortiNDR 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 v4.4.2
4. Includes receiving, job handling, AV engine, Yara engine, Cloud Query; measured based on v4.4.2
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 on 10 hour period with 10% on Dynamic Scan
8. Limited to static analysis only
9. Supported on FortiGate FortiOS v7.4.1

# Specifications

| FEATURE | CLOUD | | | ON PREMISE | | | |
|---|---|---|---|---|---|---|---|
| | FortiSandbox SaaS[1] | FortiSandbox PaaS | FortiSandbox Public Cloud | FSA-VM | FSA-500G | FSA-1500G | FSA-3000F |
| **System Information** | | | | | | | |
| Form | Virtual Machine | Virtual Machine | Virtual Machine | Virtual Machine | 1RU Appliance | 1RU Appliance | 2RU Appliance |
| **Network Interfaces** | | | 4 | 4 | 4x GE RJ45 ports | 4x GE RJ45 ports, 2x 10 GE SFP+ slots | 4x GE RJ45 ports, 2x 10 GE SFP+ slots |
| Storage | | 200 GB | 200 GB (min) | 200 GB (min) | 1× 960 GB | 2× 960 GB RAID1 | 4× 2 TB RAID-10 |
| Hot Swappable | | | | | No | Yes | Yes |
| **Trusted Platform Module (TPM)** | | | | | Yes | Yes | No |
| Hypervisor Support[1] | No | No | Yes | Yes | | | |
| **Dimensions and Power** | | | | | | | |
| **Height x Width x Length (inches)** | | | | | 1.73 × 17.24 × 14.96 | 1.73 × 17.24 × 24.02 | 3.5 × 17.2 × 23.7 |
| **Height x Width x Length (mm)** | | | | | 44 × 438 × 380 | 44 × 438 × 610 | 88 × 438 × 601 |
| Weight | | | | | 11.42 lbs (5.18 kg) | 24.92 lbs (11.30 kg) | 44 lbs (20 kg) |
| Form Factor | | | | | 1 RU | 1 RU | 2 RU |
| Power Supplies | | | | | 1x PSU | 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 | 100–240V AC, 50/60 Hz |
| **Maximum Current (AC/DC)** | | | | | 100V/6A, 240V/3A | 100V/7.5A, 240V/3.9A | 100V/10A, 240V/5A |
| **Power Consumption (Average/Maximum)** | | | | | 71.8 / 87.8 W | 238.1 W / 291.06 W | 418.3 W / 511.3 W |
| Heat Dissipation | | | | | 333.63 BTU/h | 1027.22 BTU/h | 1778.61 BTU/h |
| Forced Airflow | | | | | 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) |
| Storage Temperature | | | | | -40°–158°F (-40°–70°C) | -4°–158°F (-20°–70°C) | -40°–158°F (-40°–70°C) |
| Humidity | | | | | 10%–90% non-condensing | 10%–90% non-condensing | 10%–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 |

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

| Product | CLOUD | | | | APPLIANCES |
| | 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 V6.2+ | |
| **FORTIWEB** | FortiWeb OS V6.2+ | | | FortiWeb OS V6.2+ | |
| **FORTIADC** | | | | FortiADC OS V5.0+ | |
| **FORTIPROXY** | | | | FortiProxy OS V1.2.3+ | |

## Hardware Appliances



FortiSandbox 500G



FortiSandbox 1500G



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 Malware Prevention Service (IL MPS) (FGT-200F)** | FC-10-F200F-577-02-DD | FortiGuard AI-based Inline Malware Prevention Service. Also available as part of the ENTERPRISE Bundle. |
| **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 one. 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 five. 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 eight, 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 five. 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 two. Supports MacOS X. Maximum expansion limits to eight. |
| **FortiSandbox Hardware Appliance** | | |
| **FortiSandbox 500G** | FSA-500G | Sandboxing Appliance - 4 GE RJ45, 1 Win11, 1 Win10, 1 Office21. Upgradable to max 14 VMs. |
| **FortiSandbox 1500G** | FSA-1500G | Sandboxing Appliance - 4 x GE RJ45, 2 × 10GbE SFP+ Slots, redundant PSU, 1 Win11, 1 Win10, 1 Office21. Upgradable to max 28 VMs. |
| **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. |

**FURTINET**

November 30, 2023

FSA-DAT-R53-20231130