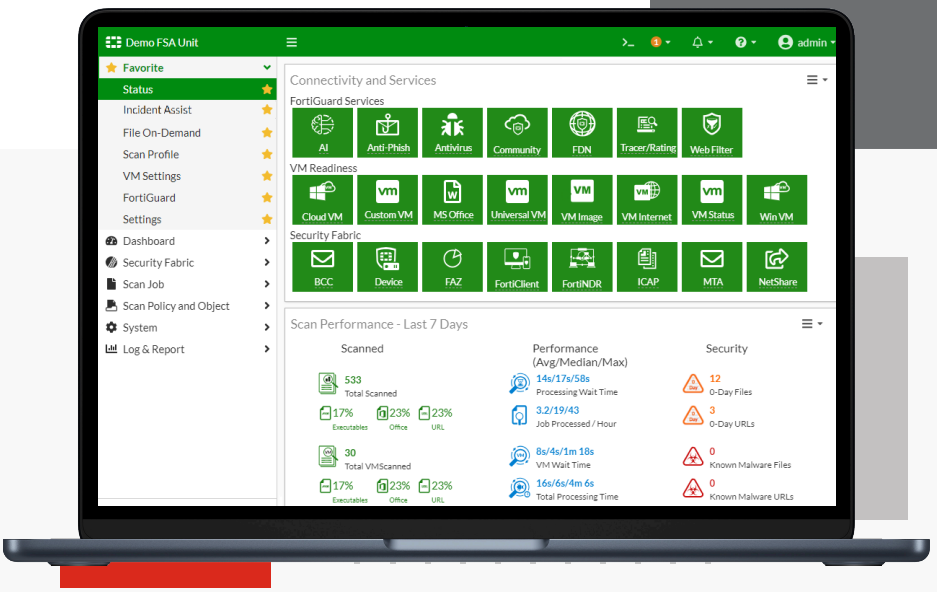
FortiSandbox and FortiGuard Sandbox Services



New FortiSandbox is built with Advanced AI to defend against new threats in real-time.

Highlights

10X Effective Throughput
over traditional Sandboxes, allowing for ultra-scalable operations with no impact on performance

10X Faster Real-Time Verdicts
Accelerate incident handling, increase productivity, reduce exploit windows and reduce downtime and costs while blocking unknown files from entering the network with real-time analysis and filtering

3X Improved Detection and Accuracy
Detect 3X more malware accurately and eliminate false positives

3X More Universal VMs for Scalability and Flexibility
Choose any local, cloud, or custom virtual machine (VM) types and operating systems (OSs)

SOC assistance
FortiSandbox features a single pane of glass view of all threats for analysis and response

FortiSandbox 5.0. Faster, Smarter, and more Scalable

FortiSandbox 5.0 is a fast and smart security solution that utilizes a combination of AI/ML, static, and dynamic analysis, inline blocking, and scalable virtual environments to identify, analyze, contextualize, prioritize, and protect against advanced threats in real-time. Using an advanced AI engine running on a purpose built ML, FortiSandbox 5.0 is 10X faster and provides 3X more detection and accuracy than before with 3X more universal VMs for expansion than before to protect against malicious activity, including zero-day threats and advanced AI-powered sophisticated threats across a broad attack surface of Cloud, IT, Edge, hybrid, and OT.

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 and protect against malicious content.

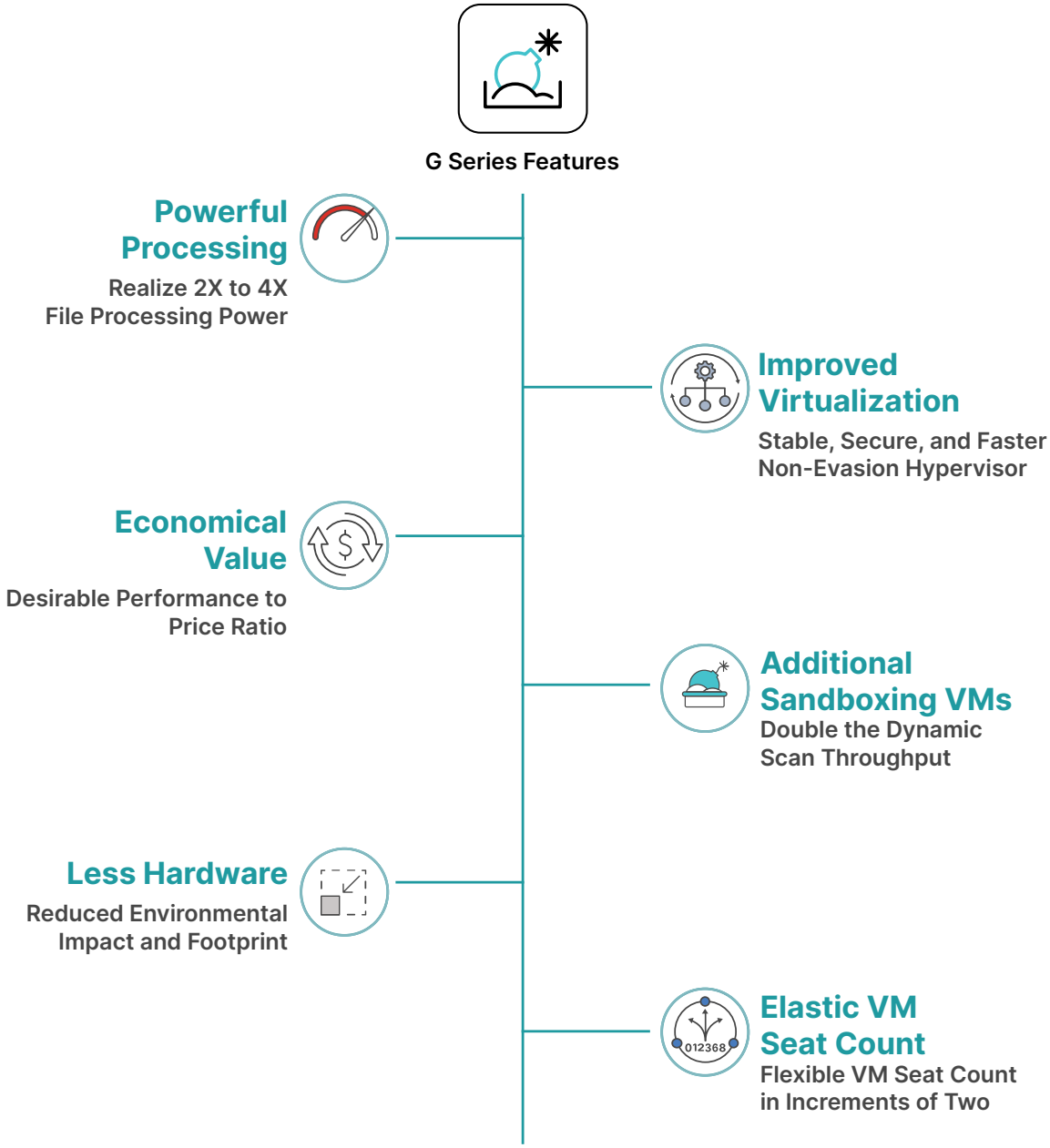
Platform Evolution

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.



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

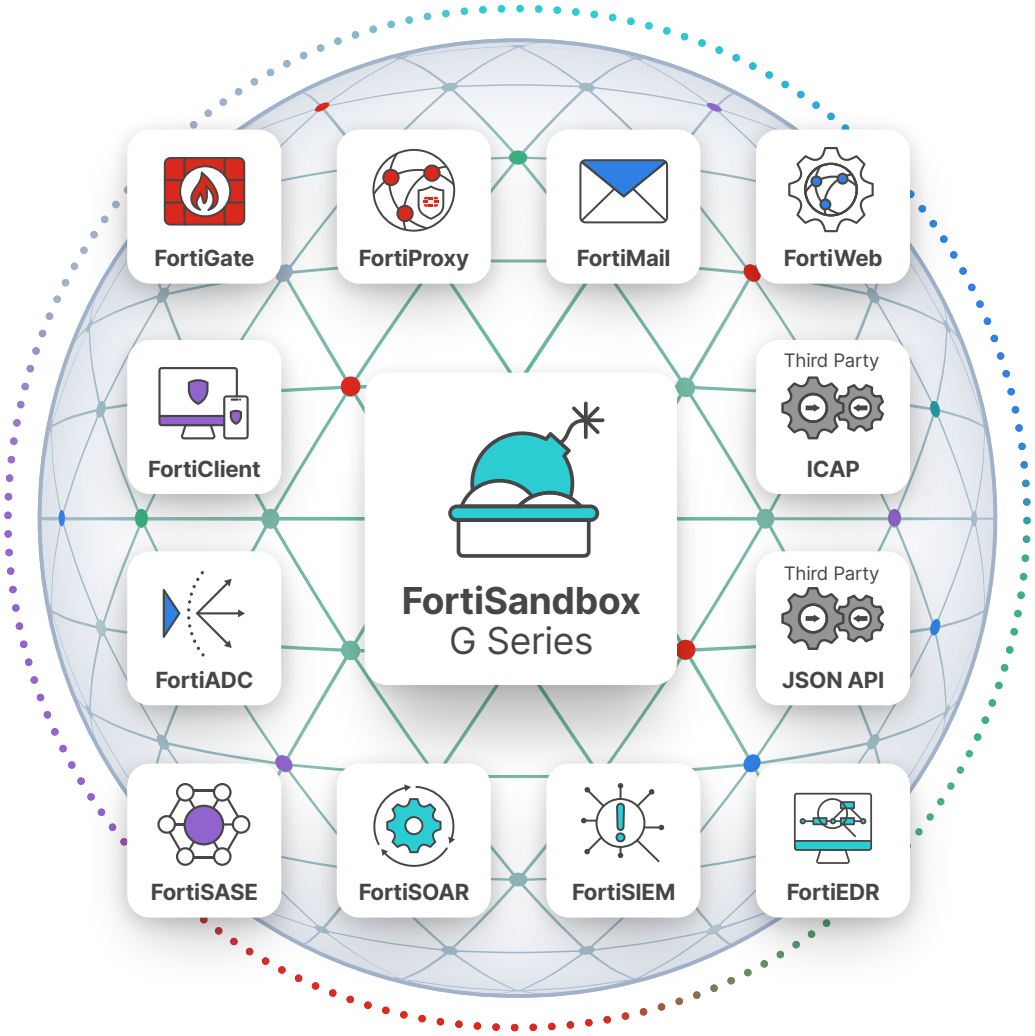
Features

FortiSandbox is the most flexible threat-protection 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.



Advanced AI Engine

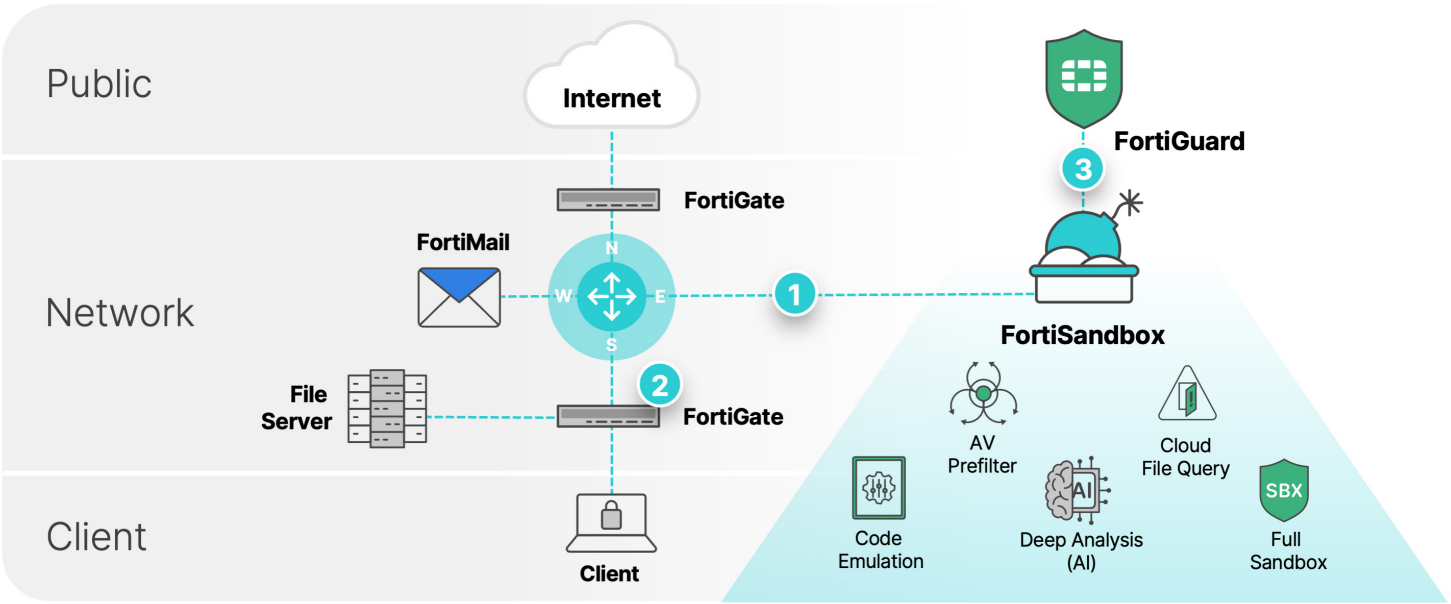
With FortiSandbox 5.0 we have moved the power of AI/ML within FortiSandbox. This advanced AI engine with purpose built ML allows FortiSandbox to detect, analyze, and protect against all types of malicious content faster, in real-time without any latency/delays so that organizations are protected against new and emerging threats without adding more resources or cybersecurity controls.

Real-Time Anti-Phishing

The FortiSandbox 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.

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.

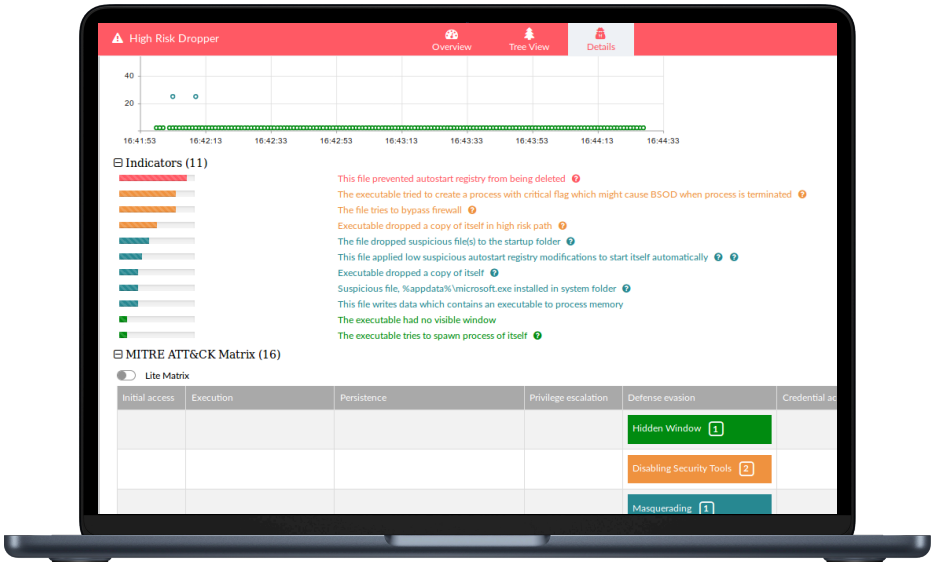


1. Submit file and URL for analysis from the FortiGate, FortiMail, client or file server.
2. Block suspicious file and URL inline on the device or quarantine on the client.
3. Share IoCs to the FortiGate devices (optional to FortiGuard) for intelligence sharing.

Incident Assist for Threat Investigation with MITRE ATT&CK-based Reporting and Tools

FortiSandbox provides a comprehensive Job Detail Report for threat analysis and intelligence for Virtual Security Analyst. The report maps discovered malware techniques to MITRE ATT&CK framework with built-in powerful investigative tools that allow Security Operations (SecOps) teams to download captured packets, original file, tracer log, and 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

Universal VM

Universal VM is an all-in-one license for the flexibility to choose any local, cloud, or custom virtual machine (VM) type and operating system. It detaches VM licenses from the OS licenses to reduce licensing complexity.

NetShare Scan

The FortiSandbox facilitates scanning of file repositories via FTP, sFTP, CIFs, NFS, OneDrive, AWS S3 Buckets, Azure Blob, and Google Cloud storage. 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 provides redundancy for uninterrupted critical operation and supports clustering to expand the throughput capacity of up to 99 worker nodes.

Platform as a Service (PaaS)

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.

Features Summary

Advanced Threat Protection

- Advanced AI to identify zero-day threats faster and better detection
- Inline blocking to detect and protect against Zero-day Malware including ransomware; blocks and holds malicious content at the FortiGate and sends to the sandbox for analysis/verdict
- Real-time identification of Zero-day Phishing sites including spam and malware-hosted sites
- Network threat detection in sniffer mode. Identify botnet activities and network attacks, malicious URL visits
- Threat enrichment through FortiGuard IOC
- 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 FTP, sFTP, CIFs, NFS, OneDrive, AWS S3 Buckets, Azure Blob, and Google Cloud storage.
- 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 AI Scan (Static AI Scan) Features

- Integrated with the new Advanced AI engine and model
- 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 and scan files embedded in documents
- Extracts and scan URLs embedded in documents and QR Code
- Extracts and scan images in documents using OCR
- 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 VM (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 and VM screenshots
- Nested VMs on premise and cloud deployment
- 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, .vbe, wsf
    - Microsoft Office: .doc, .docm, .docx, .dot, .dotm, .dotx, .ics, .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, .sh, ObjectFiles
    - MacOS files: .app, .dmg, Mach-O
    - Web files: .asp, .hta, .htm, html, .lnk, .js, .lnk, .url, WEBLink
    - Compress files: .7z, .ace, .arj, .bz2, .gz, .iso, .jar, .kgb, .lzh, .rar, .swf, .tar, .tgz, .udf, .upx, .xz, .z, .zip
- User-defined extensions

Features Summary continued

Monitoring and Reporting

- AI-based Threat Summary using the collected indicators and results
- 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, performance, 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
- TAC-report for comprehensive snapshot of system configuration and status

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			
	FSA SaaS	FSA IL MPS	FSA PaaS	FSA Public Cloud	FSA VM	FSA 500G	FSA 1500G	FSA 3000F
Deployment and Integration								
Deployment Type	Fortinet Hosted	Fortinet Hosted	Fortinet Hosted	Azure, AWS, GCP, OCI	On Premise	On Premise	On Premise	On Premise
Hosting Type	Shared	Shared	Dedicated	Dedicated	Dedicated	Dedicated	Dedicated	Dedicated
Security Fabric Integration	Centralized	Centralized	Centralized	Centralized	Centralized	Centralized	Centralized	Centralized
Fabric Partner Integration	—	—	✓	✓	✓	✓	✓	✓
API, BCC Adapter, MTA Adapter, NetShare Scan, and Sniffer Mode	—	—	only API	✓	✓	✓	✓	✓
FortiGate Capabilities								
Detection (Visibility and Log Enrichment)	✓	✓	✓	✓	✓	✓	✓	✓
Prevention (Inline Blocking)	—	✓[3]	✓	✓	✓	✓	✓	✓
Security Services								
Static Analysis								
Advanced AI[1]				Add-on	Add-on	Add-on	Add-on	Add-on
Static AI Engine[3]	✓	✓	✓	✓	✓	✓	✓	✓
Accelerated AI Pre-filter[2]		✓	Add-on	Add-on	Add-on	Add-on	Add-on	Add-on
Antivirus Extended DB	✓	✓	✓	✓	✓	✓	✓	✓
Web Filtering	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic Analysis								
Dynamic AI Engine[3]	✓	✓	✓	✓	✓	✓	✓	✓
Analysis Time	up to 60 mins	1-5 minutes	1-3 minutes	1-3 minutes	1-3 minutes	1-3 minutes	1-3 minutes	1-3 minutes
Universal VM[4]				✓	✓	✓	✓	✓
Local VM Capacity				0-8	0-8	2-14	2-28	8-72
Cloud VM Expansion[5]			1-200	1-200	1-200	1-80	1-120	1-200
Real-Time Anti-Phishing		✓	Add-on	Add-on	Add-on	Add-on	Add-on	Add-on
Anti-Evasion Detection	✓	✓	✓	✓	✓	✓	✓	✓
IPS and C&C Detection	✓	✓	✓	✓	✓	✓	✓	✓
Performance and Capacity								
Effective Sandboxing Throughput[6] (Files/Hr)	—	—	5000[7]	100 – 1000	7500[8]	10 000	32 000	68 000
Static Analysis Throughput[9] (Files/Hr)	—	—	10 000[7]	TBD	15 000[8]	20 000	80 000	160 000
Dynamic Analysis Throughput[10] (Files/Hr)	—	—	160[7]	TBD	160[8]	500	1000	1600
FortiMail Throughput[11] (Emails/Hr)	—	—	50 000	1000 – 40 000	75 000	100 000	320 000	680 000
MTA Adapter Throughput (Emails/Hr)	—	—	—	—	—	10 000	32 000	68 000
Sniffer Mode Throughput (Gbps)	—	—	—	1	1	0.5	4	9.6
Number of Users[12]	—	—	650	40 – 1600	1000	1400	4000	6400
Supported OS								
Windows	✓	✓	✓	✓	✓	✓	✓	✓
MacOS, Linux, Android	—	✓[13]	✓[13]	✓	✓	✓	✓	✓
Custom VM	—	—	—	✓	✓	✓	✓	✓
OT Simulation	—	—	—	✓/—	✓	✓	✓	✓

1. Available as part of "Advanced Sandbox Threat Intelligence" subscription running on firmware version 5.0.
2. Add-on integration with FortiNDR appliance for fast pre-filtering.
3. AI-powered content and behavioral analysis through Machine Learning Model updated via Sandbox Threat Intelligence subscription supported up to firmware version 5.0.
4. Supported on firmware version 5.0.
5. The ranges reflect Universal VM support through firmware version 5.0.
6. Tested based on files with 80% documents and 20% executables; measured based on v5.0. Includes both static and dynamic analysis with pre-filtering enabled.
7. Tested on default Flavor-1 VM (with 4 CPUs and 8GB RAM) and 8 VMs. A higher VM flavor can be provided with 20 or more VM subscriptions for higher capacity. To inquire about VM flavors contact your account representative.
8. Tested on a Hyper-V (with 12 CPUs and 32GB RAM) and 8 VMs.
9. Includes receiving, job handling, AV engine, Yara engine, Cloud Query; measured based on v5.0.
10. Tested with Static Analysis and all files are forwarded to Dynamic Analysis.
11. Based on a ratio of one email with attachment to 10 emails.
12. Based on a ratio of one user per 25 emails on 10 hour period with 10% on Dynamic Scan.
13. MacOS and Linux are limited to static analysis only.

Specifications

FEATURE	CLOUD				ON PREMISE			
	FSA SaaS	FSA IL MPS	FSA PaaS	FSA Public Cloud	FSA VM	FSA 500G	FSA 1500G	FSA 3000F
System Information								
Form Factor	Virtual Machine	Virtual Machine	Virtual Machine	Virtual Machine	Virtual Machine	1RU Appliance	1RU Appliance	2RU Appliance
Network Interfaces	—	—	—	—	—	4x GE RJ45 ports	4x GE RJ45 ports, 2× 10 GE SFP+ slots	4x GE RJ45 ports, 2× 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	—	—	—	—	—	—	✓	✓
Trusted Platform Module (TPM)	—	—	—	—	—	✓	✓	—
Hypervisor Support[1]	—	—	—	✓	✓	—	—	—
Dimensions								
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 (lbs/kg)	—	—	—	—	—	11.42 lbs (5.18 kg)	24.92 lbs (11.30 kg)	44 lbs (20 kg)
Power								
Number of Power Supplies	—	—	—	—	—	1x	2x	2x
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 W / 87.8 W	238.1 W / 291.06 W	418.3 W / 511.3 W
Redundancy	—	—	—	—	—	—	Yes	Yes
Hot Swappable	—	—	—	—	—	—	Yes	Yes
Environment								
Forced Airflow	—	—	—	—	—	Front to Back	Front to Back	Front to Back
Heat Dissipation	—	—	—	—	—	333.63 BTU/h	1027.22 BTU/h	1778.61 BTU/h
Operating Temperature	—	—	—	—	—	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature	—	—	—	—	—	-40°F to 158°F (-40°C to 70°C)	-4°F to 158°F (-20°C to 70°C)	-40°F to 158°F (-40°C to 70°C)
Humidity	—	—	—	—	—	10% to 90% non-condensing	10% to 90% non-condensing	10% to 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	✓	✓	✓		✓	✓	✓	✓

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 V7.0+	FortiOS V7.2.1+, FortiOS V7.4.1+ (PaaS)	FortiOS V7.0+	FortiOS V7.0+	
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 V7.0+			FortiWeb OS V7.0+	
FORTIADC				FortiADC OS V6.0+	
FORTIPROXY				FortiProxy OS V2.0+	

Hardware Appliances

FortiSandbox 500G

FortiSandbox 1500G

FortiSandbox 3000F

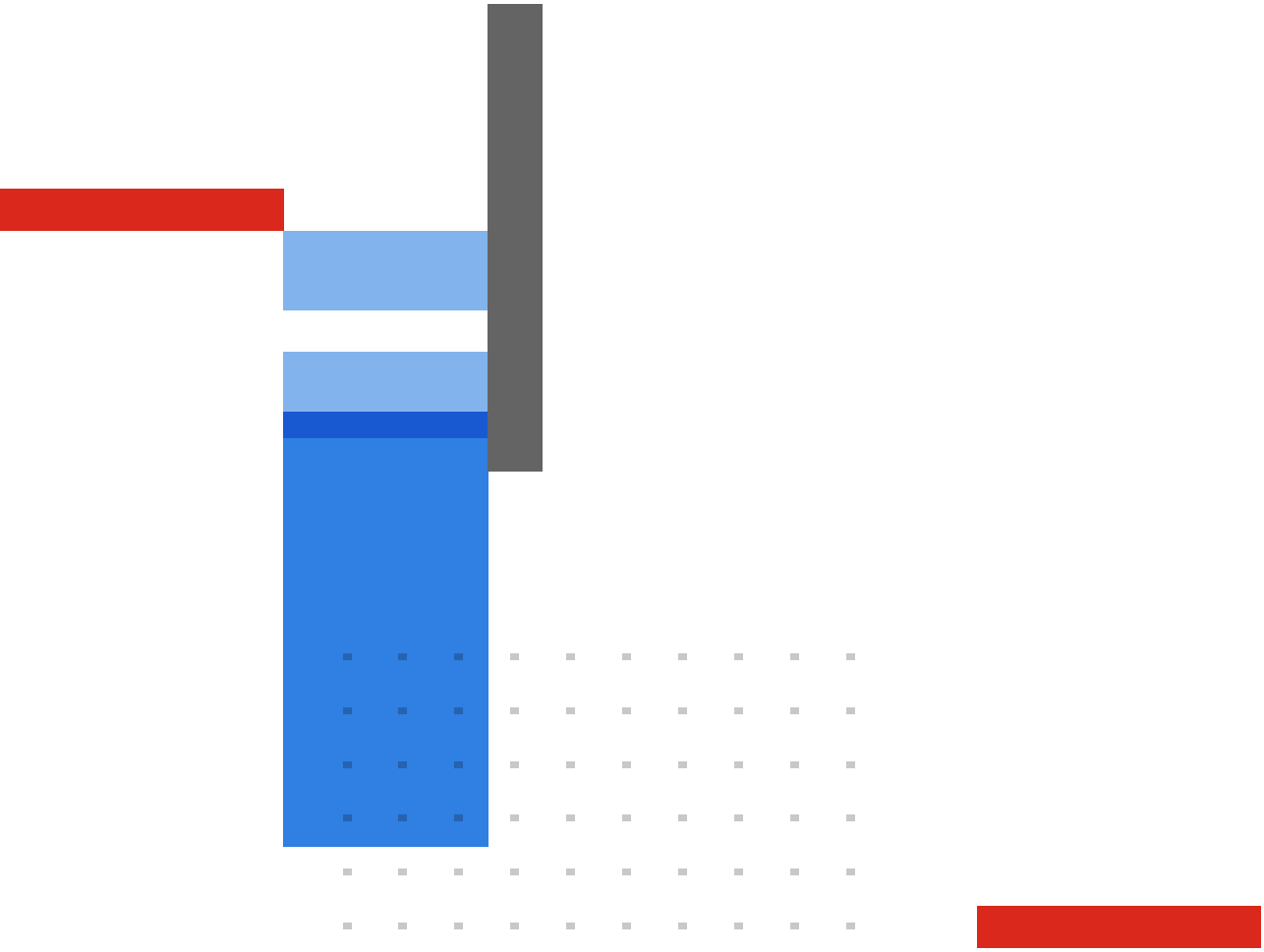
Ordering Information

The following SKU list outlines the primary Sandbox deployment options. For full guidance, please refer to the related ordering guides at https://www.fortinet.com/resources/ordering-guides.

Product	SKU	Description
FortiSandbox SaaS for FortiGate		
Enterprise Protection (includes IL MPS) (FGT-60F)	FC-10-0060F-809-02-DD	Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium)
Inline Malware Prevention Service (IL MPS) (a la carte SKU) (FGT-60F)	FC-10-0060F-577-02-DD	FortiGuard AI-based Inline Malware Prevention Service. (Also available as part of the Enterprise Bundle)
Cloud Sandbox (FGT-60F)	FC-10-0060F-100-02-DD	Advanced Malware Protection (AMP) Bundle including Antivirus, Mobile Malware and FortiGate Cloud Sandbox Service.
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 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 FortiCloud datasheet for included feature and license details.)
FortiSandbox Pub Cloud / FortiSandbox VM Appliance		
FortiSandbox-VM	FSA-VM00	Sandboxing Virtual Appliance. No Universal VM count included. Available VM count expansion up to max 8 Local and 200 Cloud. No Microsoft licenses included.
FortiSandbox On Premise Hardware		
FortiSandbox 500G	FSA-500G	Sandboxing Hardware Appliance for SMB. Includes two Universal VM count. Available VM count expansion up to max 14 Local and 80 Cloud. Includes 1xWin11, 1xWin10, 1xOffice21 Licenses.
FortiSandbox 1500G	FSA-1500G	Sandboxing Hardware Appliance for Mid-Range. Includes two Universal VM count. Available VM count expansion up to max 28 Local and 120 Cloud. Includes 1xWin11, 1xWin10, 1xOffice21 Licenses.
FortiSandbox 3000F	FSA-3000F	Sandboxing Hardware Appliance for Enterprise. Includes eight Universal VM count. Available VM count expansion up to max 72 Local and 200 Cloud. Includes 6xWin10, 2xWin7, 1xOffice19 Licenses.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

November 13, 2024

FSA-DAT-R62-20241113