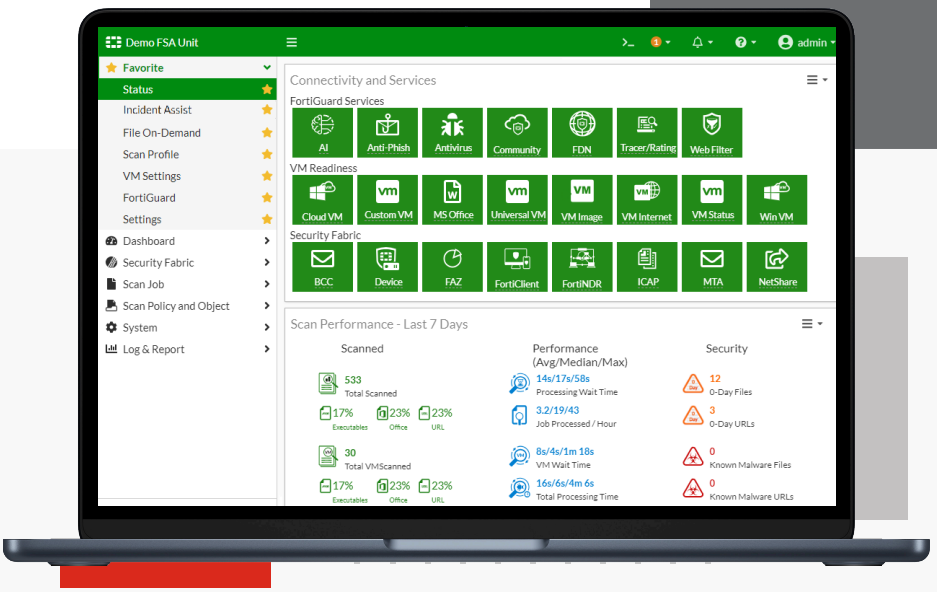
FortiSandbox and FortiGuard Sandbox Services



The new FortiSandbox is built on an advanced AI engine that defends against new, emerging, evasive, and previously unseen 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 with near-zero 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 to assist SOC and IR teams

Next-Level FortiSandbox 5.0: Smarter, Faster, 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 purpose built ML, FortiSandbox 5.0 is 10X faster and offers 3X greater 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. Integrating natively with 12 Security Fabric products and other tools, deployable on-premises, in the cloud, or as a hosted service, FortiSandbox is suitable for organizations of any size.

Sandboxing: a must-have in modern cyber defense

As the modern threat landscape, powered by AI enhanced threats bypass traditional defenses, sandboxing has become a critical layer in detecting the unknown and evasive —especially zero-day or fileless malware. This section highlights why sandboxing is no longer optional but an essential and foundational control in modern security strategies.

Defend against the unknown: why sandboxing is mission-critical.

Framework	Region	Requirement Summary	Primary Industry or Sector
PCI DSS v4.0		Mandates anti-malware and recommends advanced techniques (heuristics/ behavioral analysis).	Retail, E-commerce, Financial Services, Hospitality, Call Centers
CMMC 2.0		Mandates malware protection.	Defense, Aerospace, Government Contractors
Singapore CCoP		Mandates behavior-based detection (such as sandboxing).	Critical Information Infrastructure (Energy, Water, Finance, Healthcare)
EU NIS2		Mandates risk-based cybersecurity at national level.	Critical Infrastructure, Digital Services, Energy, Telecom
NIST CSF v2.0		Recommends malware detection as an outcome (such as malicious code is detected).	Critical Infrastructure, Government, Finance, Healthcare, Enterprise
Japan METI/IPA		Recommends advanced malware detection (such as sandboxing).	Manufacturing, Technology, Energy, Critical Infrastructure
EU CSA		May require advanced malware detection for high assurance levels and certification.	IT Products and Services (EU Market)

Note: The industry sectors under critical infrastructure are energy, finance, health, telecommunications, transport, and water.

Sandboxing solutions like FortiSandbox offer powerful detection and protection. However, some security team members still have some doubts about the performance of sandboxing. Let's clear the air on that.

Sandboxing isn't slow—it's smarter.

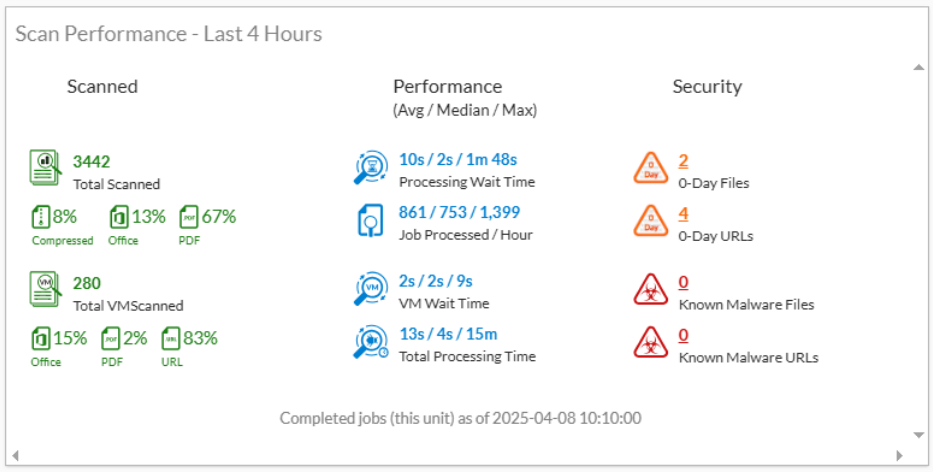
The truth about sandboxing speed

Contrary to outdated beliefs, sandboxing doesn't have to slow things down. FortiSandbox delivers fast, AI-driven threat analysis—proving that high security and high performance can go hand in hand. One of the most common misconceptions about sandboxing is that *it's too slow for real-time protection*. In reality, FortiSandbox is **engineered for speed and efficiency** without compromising on deep threat analysis and protection. It uses a two-tiered AI-powered scanning approach—static and dynamic—to rapidly and accurately assess files.

The Static AI Scan can process up to 50 files per second, immediately identifying known malicious attributes and returning a threat verdict within milliseconds. If a file contains active content (such as embedded URLs, scripts, macros, or executables) but shows no obvious static threats, it is passed to the Dynamic AI Scan, which spins up an isolated virtual environment to detonate and observe the file's behavior—typically within a few seconds.

In a well-resourced production environment, most files are scanned in under a second, with a median scan time of just five seconds. This time-frame is well within acceptable thresholds for network, email, and endpoint solutions to safely hold files during analysis—ensuring high detection efficacy without slowing down operations.

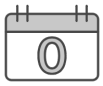
With speed no longer a barrier, it's time to evaluate what really sets sandboxing solutions apart.



The screenshot illustrates the performance of FortiSandbox over the last four hours, highlighting its ability to quickly and efficiently scan a high volume of files and URLs. Over 3000 files and URLs were scanned, with only 8% (280) requiring the more time-intensive Dynamic Scan. The majority of files were processed rapidly, with a median total processing time of just 4 seconds and an average of 13 seconds. Within the efficient scanning process, a handful of suspicious detections were flagged, demonstrating the system ability to balance speed with thorough threat analysis.

A smarter choice: feature-driven evaluation of sandbox technologies

Not all sandboxes are built the same. This section compares key capabilities that matter most—such as AI-driven analysis, deployment flexibility, integration, and automation—to help you choose the right solution for your environment.



Advantage	FortiSandbox	Competitor	Comments
AI/ML Capabilities	✓✓✓	✓✓	FortiSandbox: advanced AI and ML with neural networks available on-premises and cloud, reduce latency. Competitor: AI or ML engine based on cloud-based updates are slower.
Zero-Day Threat Detection	✓✓✓	✓✓	FortiSandbox: Dual analysis (static + dynamic), with fastest Sandbox database creation (e.g. 2 mins) Competitor: High accuracy with rapid signature creation (e.g. 5 mins)
Integration	✓✓✓	✓✓✓	FortiSandbox: Integrates with Fortinet Security Fabric, ICAP, BCC, API. Competitor: Strong integration with their ecosystem.
Deployment Options	✓✓✓	✓✓	FortiSandbox: On-prem, virtual, public-cloud and SaaS cloud. Competitor: Limited selection on-prem, virtual, public-cloud or SaaS cloud.
Forensics Capabilities	✓✓✓	✓✓	FortiSandbox: Full job detailed report. Competitor: Limited to moderate forensic tools.
Automation and Threat Sharing	✓✓✓	✓✓✓	FortiSandbox: Automatic signature distribution. Competitor: Automatic signature distribution.
Cost and Licensing	✓✓✓	✓✓	FortiSandbox: Competitive pricing and simple licensing model. Competitor: Higher tiered pricing and/or per-seat licensing.

Once you understand the features, the next question is: how well does it work across your existing stack?

Better and stronger together: FortiSandbox and the power of coordinated defense

FortiSandbox is designed to integrate deeply across the Fortinet Security Fabric and with third-party products to deliver advanced threat detection and automated response. Here are the most common integrations and use cases.

1. Next-Generation Firewall (NGFW) with Inline Blocking Option

Use Case: Real-time blocking of advanced threats at the network perimeter

When integrated with FortiSandbox, FortiGate NGFW becomes a proactive defense system capable of detecting and blocking sophisticated threats **before they enter the network**. It uses **Inline Scanning**, meaning files and content passing through the firewall (via HTTP, FTP, SMTP) are actively inspected **in real time**.

Suspicious files that cannot be confirmed as safe using static inspection are automatically sent to **FortiSandbox**. If the sandbox determines the file is malicious—through static or dynamic analysis—FortiGate can **immediately block the file**, quarantine the session, or take other actions, all **without delay to users or services**.

With AI-driven detection, high throughput, and tight Security Fabric integration, this setup enables **zero-day threat detection and inline prevention**, offering deep security **without the performance penalty**.

2. Secure Email Gateway (SEG)

Use Case: Prevent phishing, malware, and ransomware via email

Emails with attachments or embedded URLs are scanned through FortiSandbox **to detect hidden malware, phishing and ransomware**. If a threat is confirmed, SEG such as FortiMail can block delivery or strip dangerous content—**stopping email-borne threats before they reach inboxes**.

3. Endpoint Security

Use Case: Endpoint-level detection and response

When Endpoint Security solutions such as FortiClient or FortiEDR, encounter unknown files they forward those to FortiSandbox for analysis. If malware is detected, the endpoint agent can kill the process, isolate the host, or share IOCs with other devices—**creating a fast, coordinated response across users and systems**.

4. Web Proxy

Use Case: Block advanced web threats from downloads and scripts

Proxy devices such as FortiProxy filter web traffic and enforce policies, while FortiSandbox adds deep analysis for suspicious downloads and web content. Together, they detect and block zero-day malware, drive-by downloads, and malicious scripts—**before they ever reach the endpoint**.

5. Shared Storage

Use Case: Analyze files from SMB/NFS shares, cloud storage (e.g. OneDrive), and web uploads

FortiSandbox can scan files from shared folders and upload portals—including SMB, NFS, public shares, and cloud storage like OneDrive. By detecting hidden malware in these locations, it helps **stop lateral movement and insider threats** before they spread.

6. FortiAnalyzer and FortiSIEM

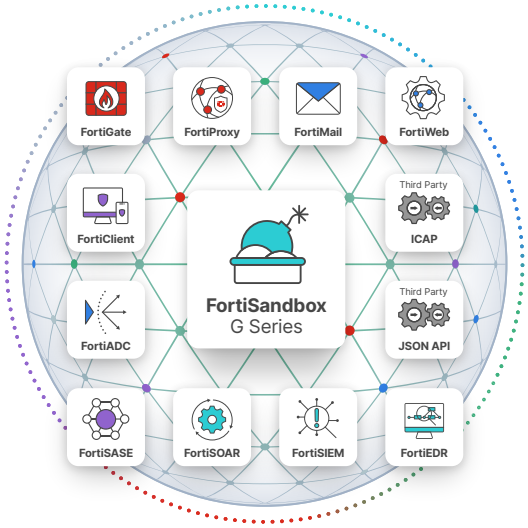
Use Case: Centralized visibility, correlation, and automated response

FortiSandbox shares IOCs and threat intelligence with FortiAnalyzer and FortiSIEM. These platforms correlate events, generate alerts, and trigger workflows—**accelerating detection, triage, and mitigation across the enterprise**.

7. Third Party Integrations (via APIs or ICAP)

Use Case: Extend sandboxing to external products

FortiSandbox supports **ICAP** and **RESTful APIs**, allowing integration with third-party tools like other NGFWs, proxies, SIEMs, or email gateways. This integration enables **sandbox-as-a-service** functionality even outside of Fortinet environments.



FortiSandbox doesn't work in isolation—it integrates deeply across the Fortinet Security Fabric. From firewalls and email to endpoints and storage, see how FortiSandbox delivers maximum threat coverage and protection through intelligent and coordinated defense in real-time.

Now that we've explored the value of sandboxing, addressed common misconceptions, and reviewed real-world use cases, it's time to look under the hood. The following section outlines FortiSandbox's core capabilities and technical specifications—highlighting the features that drive its speed, accuracy, and seamless integration across your security infrastructure.

Feature Summary

FortiSandbox combines advanced threat detection with performance and flexibility, making it a powerful addition to any security stack. This section summarizes key features that define its effectiveness—from AI-driven static and dynamic analysis to flexible deployment models and seamless integration across network, endpoint, email, and cloud environments. Whether you're looking for speed, scalability, or automated response, FortiSandbox delivers where it matters most.

Continuously Evolving AI-Powered Detection

With FortiSandbox 5.0, the Advanced AI Engine is natively integrated into the platform, combining real-time performance with purpose-built machine learning. Trained daily on thousands of newly collected malware samples across various file types, the engine adapts continuously by analyzing undetected samples and refining detection models accordingly. Each model undergoes two weeks of rigorous validation to ensure accuracy and reliability. This process enables FortiSandbox to detect, analyze, and protect against both known and unknown threats—faster and without added latency—helping organizations stay ahead of emerging attacks without the need for additional security controls or resources.

Real-Time Phishing Detection and Prevention

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 are analyzed using patented technologies to determine any phishing signs.

Intelligent Threat Investigation with MITRE-Aligned Insights

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.

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

Flexible and Scalable Universal VM Deployment

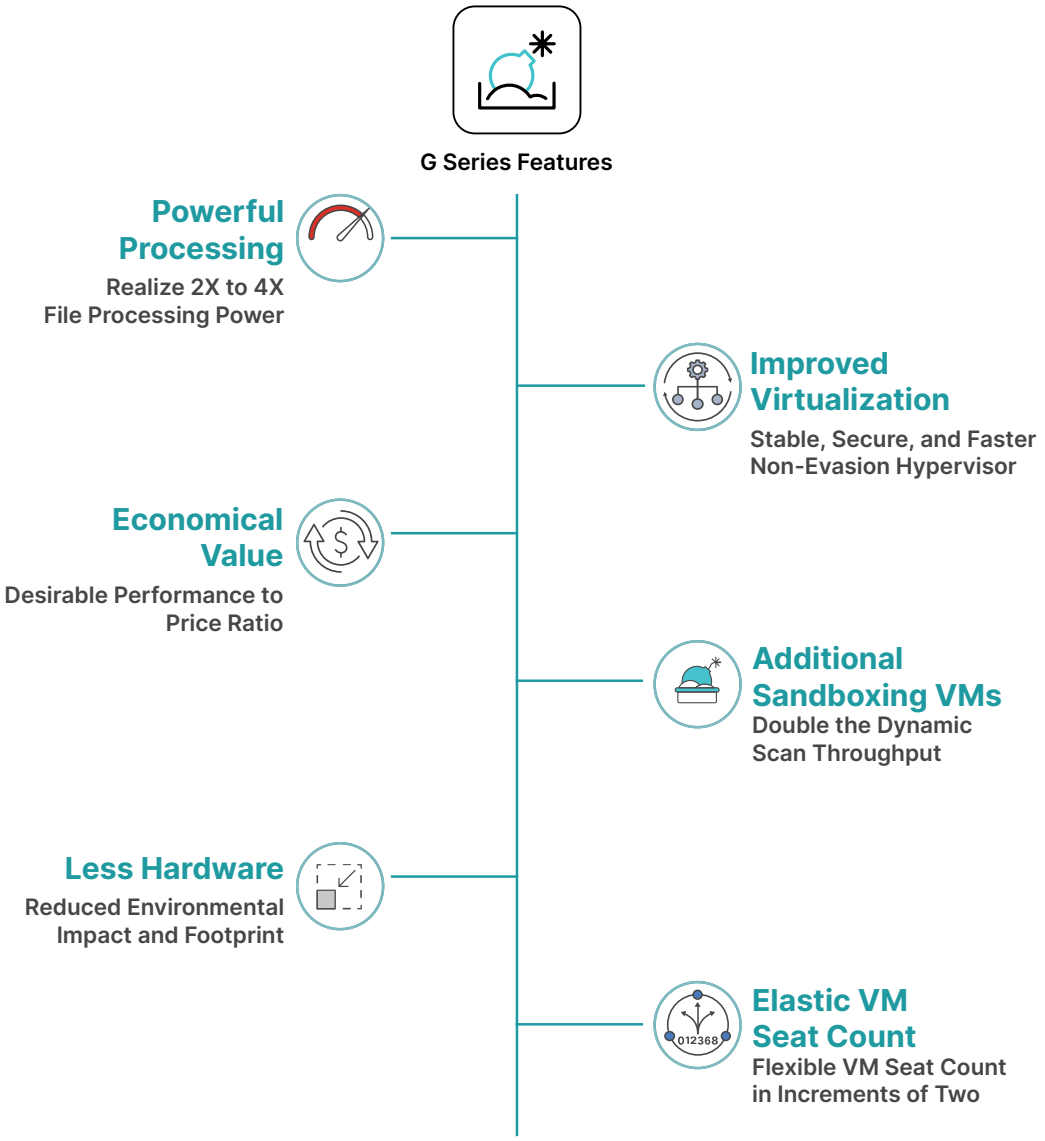
Universal VM is an all-in-one license for the flexibility to choose any local, cloud, or custom virtual machine (VM) type and operating system. It detaches VM licenses from the OS licenses to reduce licensing complexity.

Resilient High-Availability Architecture for Continuous Protection

The FortiSandbox provides native clustering support of up to 99 worker nodes that expands throughput capacity providing uninterrupted critical operations.

Platform Evolution

Leveraging our previous F and E models*, FortiSandbox 3000G, 1500G, and 500G provide cutting edge technological advancements, performance, real-time sharing of threat intelligence across multiple geographical locations, and integration with Fortinet's Security Fabric and third party providers. 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.



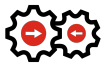
*The 500G replaces the 500F, and the 1500G replaces the 1000F and 2000E.

Detailed 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

Detailed 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 dynamic analysis VM 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 Executable, Microsoft Office, Document/Email, Android files, Linux files, MacOS, Web files
- File Compression Support
- User-defined extensions

Detailed 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

Deployment and Detection Specifications

FEATURE	CLOUD				ON PREMISE	
	FSA SaaS	FSA IL MPS	FSA PaaS	FSA Public Cloud	FSA VMs	FSA Hardware
Deployment and Integration						
Type						
Deployment	Fortinet Hosted	Fortinet Hosted	Fortinet Hosted	Azure, AWS, GCP, OCI	On Premise	On Premise
Hosting	Shared	Shared	Dedicated	Dedicated	Dedicated	Dedicated
Integration						
Security Fabric	Centralized	Centralized	Centralized	Centralized	Centralized	Centralized
Fabric Partner	—	—	✓	✓	✓	✓
API, BCC, ICAP, MTA, NetShare, and Sniffer Mode	—	—	only API	✓	✓	✓
FortiGate Capabilities						
Detection (Visibility and Log Enrichment)	✓	✓	✓	✓	✓	✓
Prevention (Inline Blocking)	—	✓	✓	✓	✓	✓
Detection						
Static Analysis						
Advanced AI[1]	✓	✓	Coming Q4 2025	✓[1]	✓[1]	✓[1]
Static AI Engine[3]	✓	✓	✓	✓	✓	✓
Accelerated AI Pre-filter[2]		✓	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
Universal VM[4]				✓	✓	✓
Real-Time Anti-Phishing			Add-on	✓[1]	✓[1]	✓[1]
Anti-Evasion Detection	✓	✓	✓	✓	✓	✓
IPS and C&C Detection	✓	✓	✓	✓	✓	✓
Supported OS						
Windows	✓	✓	✓	✓	✓	✓
MacOS, Linux, Android	—	✓[5]	✓[5]	✓	✓	✓
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.
4. Supported on firmware version 5.0.
5. Dynamic Scan on Android is scheduled for 2025/Q3.

Supported File Type Specifications

FEATURE	CLOUD				ON PREMISE	
	FSA SaaS	FSA IL MPS	FSA PaaS	FSA Public Cloud	FSA VMs	FSA Hardware
Supported File Type						
Windows Executables						
Portable executable (exe, dll, scr)	✓	✓	✓	✓	✓	✓
Installer and script files (bat, cmd, jse, msi, ps1, vbe, vbs, wsf)	✓	✓	✓	✓	✓	✓
Productivity Files						
Microsoft Office (Word, Excel, Powerpoint, Publisher, OneNote)	✓	✓	✓	✓	✓	✓
Portable document format files (pdf)	✓	✓	✓	✓	✓	✓
Other related files (csv, ics, rtf)	✓	✓	✓	✓	✓	✓
Email						
Email files (eml, msg)	✓	✓	✓	✓	✓	✓
Links contained in emails (lnk)	✓	✓	✓	✓	✓	✓
Web files						
Common files (html, js, lnk, url)	—	—	✓	✓	✓	✓
Adobe Flash files (swf)	—	—	✓	✓	✓	✓
Images						
Images with QR Code and Ransomware	—	—	✓	✓	✓	✓
Additional OS						
Android application package files (apk)	—	✓[1]	✓[1]	✓	✓	✓
Linux and Shell scripts files (elf, sh)	—	✓	✓	✓	✓	✓
MacOS files (dmg)	—	✓	✓	✓	✓	✓
Archive Common files						
Common files (7z, arj, cab, bzip, gzip, jar, lzw, rar, tar, lzh, zip, xz)	✓	✓	✓	✓	✓	✓
Additional Archive files (ace, iso, kgb, pst, tgz, udf, upx, vhd, z)	—	—	✓	✓	✓	✓

1. Dynamic Scan on Android is scheduled for 2025/Q3.

Capacity and Performance Specifications

FEATURE								
	FSA-PaaS	FSA-VMS1	FSA-VMS2	FSA-VMS3	FSA-VMS4[9]	FSA-500G	FSA-1500G	FSA-3000G
Capacity								
Local VM Capacity		0-8	0-16	0-32	0-64	2-14	2-28	8-150
Cloud VM Expansion[1]	1-200	1-200	1-200	1-200	1-200	1-80	1-120	1-200
Performance and Capacity								
Effective Sandboxing Throughput[2] (Files/Hr)	5000[3]	8000[4]	24 000	48 000	96 000	10 000	32 000	160 000
Static Analysis Throughput[5] (Files/Hr)	10 000[3]	20 000[4]	60 000	120 000	240 000	20 000	80 000	320 000
Dynamic Analysis Throughput[6] (Files/Hr)	160[3]	200[4]	400	800	—	500	1000	5700
FortiMail Throughput[7] (Emails/Hr)	50 000	80 000	240 000	480 000	960 000	100 000	320 000	1 600 000
MTA Adapter Throughput (Emails/Hr)	—	20 000	60 000	120 000	240 000	25 000	80 000	320 000
Sniffer Mode Throughput (Gbps)	—	1	TBD	TBD	TBD	0.5	4	9.6
Number of Users[8]	650	1000	3000	6000	12 000	1250	4000	20 000

Notes:

The FSA VMS is tested on premise Hyper-V server with corresponding CPUs, memory, and VMs.

The FSA Public Cloud BYOL could achieve similar performance based on chosen resources.

The performance of FSA SaaS, FSA IL MPS and FSA Public Cloud PAYG are not included, as they cannot be accurately measured.

1. The ranges reflect Universal VM support through firmware version 5.0.
2. 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.
3. 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.
4. Tested on a Hyper-V (with 16 CPUs and 32GB RAM) and 8 VMs.
5. Includes receiving, job handling, AV engine, Yara engine, Cloud Query; measured based on v5.0.
6. Tested with Static Analysis and all files are forwarded to Dynamic Analysis.
7. Based on a ratio of one email with attachment to 10 emails.
8. Based on a ratio of one user per 80 emails on 10 hour period with 10% on Dynamic Scan.
9. Throughput is constrained by the 96 vCPU limit in version 5.0.

Hardware Specifications

FEATURE	FSA 500G	FSA 1500G	FSA 3000G
System Information			
Form Factor	1RU Appliance	1RU Appliance	2RU Appliance
Network Interfaces	4x GE RJ45 ports	4x GE RJ45 ports, 2× 10 GE SFP+ slots	8× 10 GE SFP+ slots
Storage	1× 960 GB	2× 960 GB RAID1	4× 2 TB RAID-10
Hot Swappable	—	✓	✓
Trusted Platform Module (TPM)	✓	✓	✓
Dimensions			
Height x Width x Length (inches)	1.73×17.24×14.96	1.73×17.24×24.02	3.5×17.2×25.6
Height x Width x Length (mm)	44×438×380	44×438×610	88×438×650
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	471.9 W / 542.4 W
Redundancy	—	✓	✓
Hot Swappable	—	✓	✓
Environment			
Forced Airflow	Front to Back	Front to Back	Front to Back
Heat Dissipation	333.63 BTU/h	1027.22 BTU/h	1850.67 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)	-40°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	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST		
Additional Services			
24 × 7 Support	✓	✓	✓

FortiSandbox 500G

FortiSandbox 1500G

FortiSandbox 3000G

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 V7.0+		FortiClient for Windows OS V7.0+	FortiClient for Windows OS V7.0+	
FORTIMAIL	FortiMail OS V6.2+		FortiMail V7.0+	FortiMail OS V7.0+	
FORTIWEB	FortiWeb OS V7.0+			FortiWeb OS V7.0+	
FORTIADC	FortiADC OS v6.0+			FortiADC OS V7.0+	
FORTIPROXY	FortiProxy OS v7.0+ FortiProxy OS v7.4+			FortiProxy OS V7.0+	

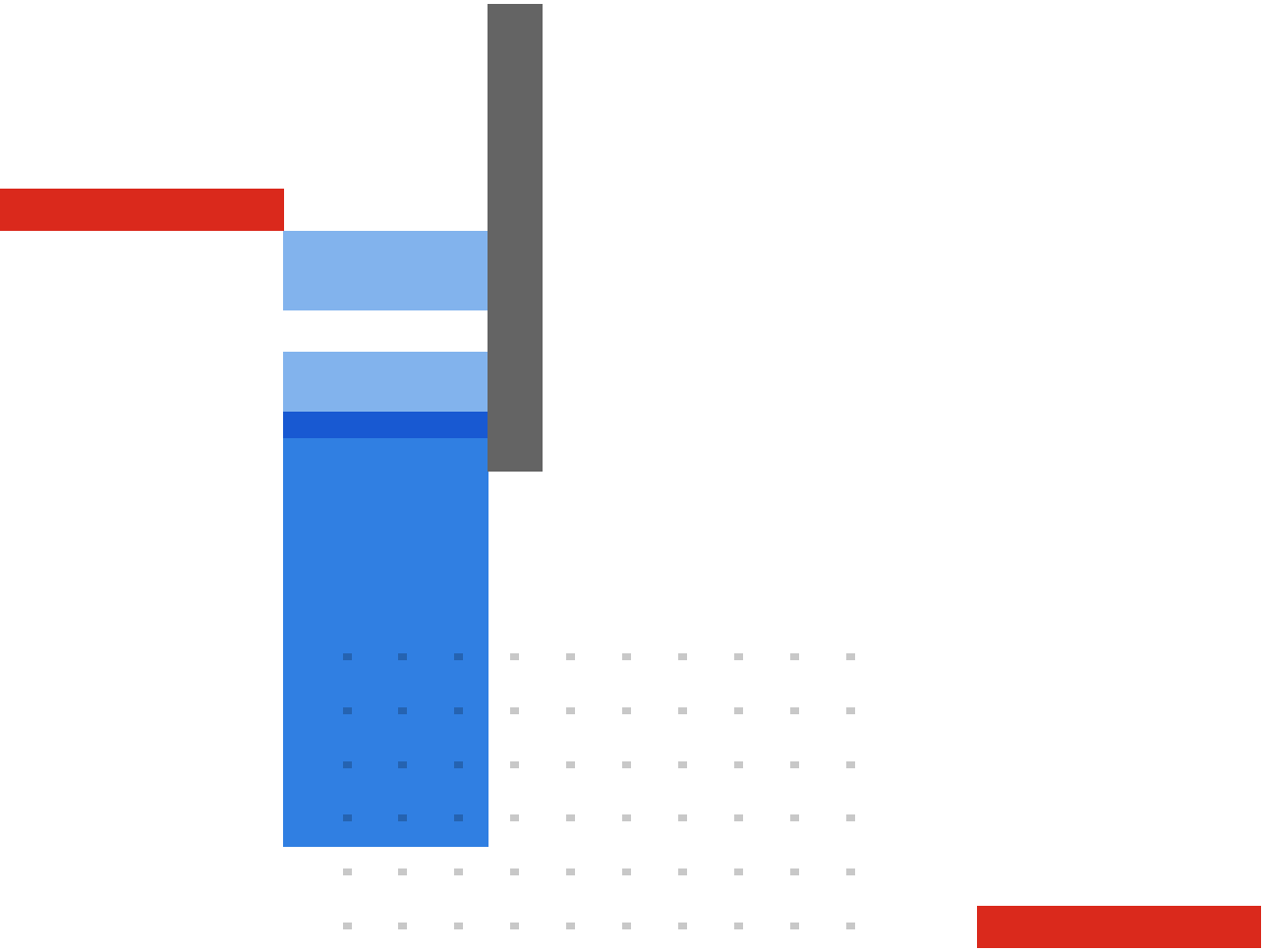
Ordering Information

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.
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.
FortiSandbox Pub Cloud / FortiSandbox VM Appliance		
FortiSandbox-VMS	FSA-VMS	Subscription license for FortiSandbox-VM with Advanced AI bundle, supporting 16 vCPUs and expandable up to 8 Universal VMs.
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 3000G	FSA-3000G	Sandboxing Hardware Appliance for Enterprise. Includes eight Universal VM count. Available VM count expansion up to max 150 Local and 200 Cloud. Includes 4xWin10, 4xWin11, 1xOffice21 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

August 27, 2025

FSA-DAT-R66-20250827