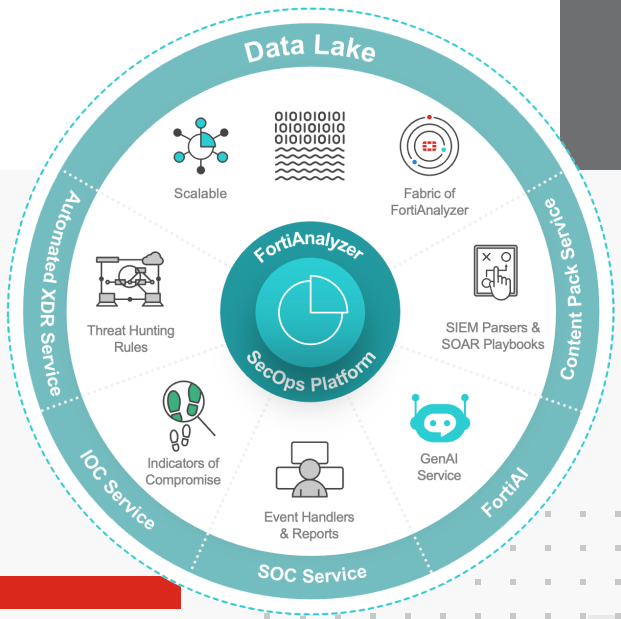
FortiAnalyzer™

Unified Data Lake, Visibility, and Automation

Available in:

Appliance | Virtual Machine | Cloud | Hosted



Highlights

- Centralized log collection. Unified visibility across network and security assets
- Real-time system and network monitoring
- Prebuilt reports and dashboards
- Built-in SIEM and SOAR
- Advanced threat detection
- Regularly updated SOC Automation Content packs
- Generative AI assistant
- Built-in threat intelligence. Enriches events with real-time context from FortiGuard
- Scalable data lake and XDR-ready. Unified data lake connects events across endpoints, network and cloud
- Designed to complement and work alongside any SIEM or logging solution customers use

FortiAnalyzer: The Turnkey Security Operations Platform

As the Data Lake of the Fortinet Security Fabric, FortiAnalyzer consolidates telemetry across networks, endpoints, and cloud environments, integrating Fortinet and third-party tools. It normalizes and enriches data with AI/ML-powered analytics, providing structured dashboards for IoT, SOC, email, and endpoint vulnerabilities. It streamlines operations with built-in threat intelligence, SIEM, and SOAR capabilities, along with prebuilt SOC automation content packs that are updated monthly. Enhanced with AI assistance and augmented operations delivered by FortiAI. Offering flexible deployment options across appliances, VMs, and the cloud, FortiAnalyzer enables network and security teams to detect faster, respond smarter, and improve efficiency—all from a single platform.

Security teams are increasingly challenged to defend against complex and targeted threats — often with limited staff and resources.

FortiAnalyzer addresses this challenge by consolidating core SecOps capabilities into a single, turnkey platform that delivers a plug-and-play experience.

Designed for both on-premises and cloud environments, it eliminates the need for multiple security tools. This AI-driven solution empowers lean security teams to strengthen threat detection, automate incident response, and streamline critical security operations from one centralized platform.

Key Capabilities

Unified Security Data Lake

Centralized Visibility Across the Security Fabric

FortiAnalyzer aggregates logs and telemetry from Fortinet products and third-party systems into a unified data lake. This centralized view enables better threat detection across networks, endpoints, applications, and cloud infrastructure and faster incident response.

Supports ingestion through various methods such as syslog, APIs, alert ingestion service, and agent-based forwarding using FortiClient. Offers scalable log storage with role-based access control and data retention policies to meet compliance requirements.

Advanced Analytics and Correlation

Detect Threats Earlier with Context-Rich Intelligence

With built-in analytics and correlation across Security Fabric components, FortiAnalyzer helps identify sophisticated attacks by connecting seemingly unrelated events. Automated playbooks and event handlers improve response time and reduce manual workload.

Real-Time Threat Intelligence

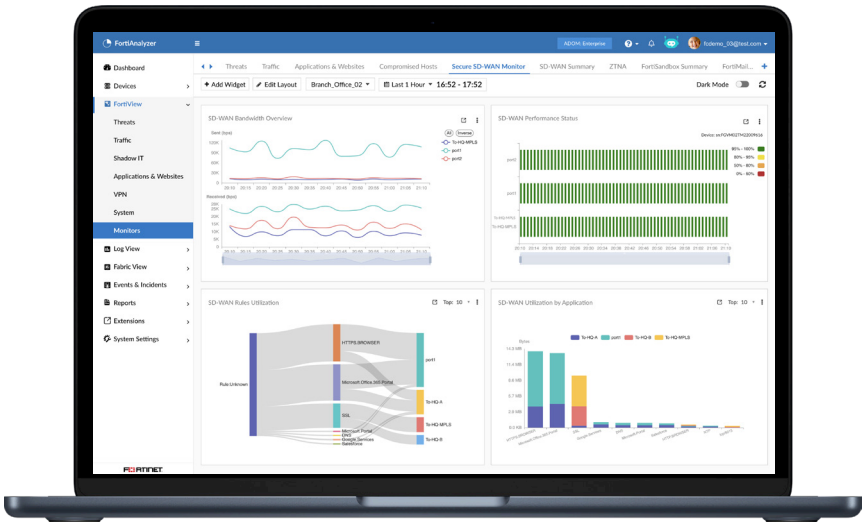
Strengthen Detection with FortiGuard Feeds

Integrates seamlessly with FortiGuard Labs' threat intelligence to enhance detection with the latest indicators of compromise, outbreak alerts service, enabling proactive defense and rapid investigation.

Automation and Custom Reporting

Operational Efficiency Through Automation

Supports automated workflows for alert handling, ticketing, and notification. Built-in and Custom dashboards and compliance reports (e.g., PCI-DSS, HIPAA) provide actionable insights for both technical and executive audiences.



Pre-Built Content Packs for SOC Automation

Continuously Updated Intelligence to Accelerate SOC Operations

FortiAnalyzer provides monthly content packs from FortiGuard Labs, delivering pre-built use cases that include log parsers, reports, correlation rules, event handlers, and automated playbooks. These content packs help organizations quickly onboard new log sources, detect emerging threats, and meet compliance requirements without extensive manual setup.

Streamlined SOC Operations

From Alert Monitoring to Automated Response

FortiAnalyzer helps security operations centers manage the full incident lifecycle — from alert monitoring and triage to deep investigation and response. Analysts can efficiently prioritize alerts using built-in correlation, indicator enrichment, and user assets and identity tracking. Integrated connectors simplify data ingestion from Fortinet and third-party sources, while built-in playbooks and automation tools enable faster, consistent responses to common threats.

Generative AI Assistant for Faster Insights

Simplifying Investigations and Enhancing Analyst Efficiency

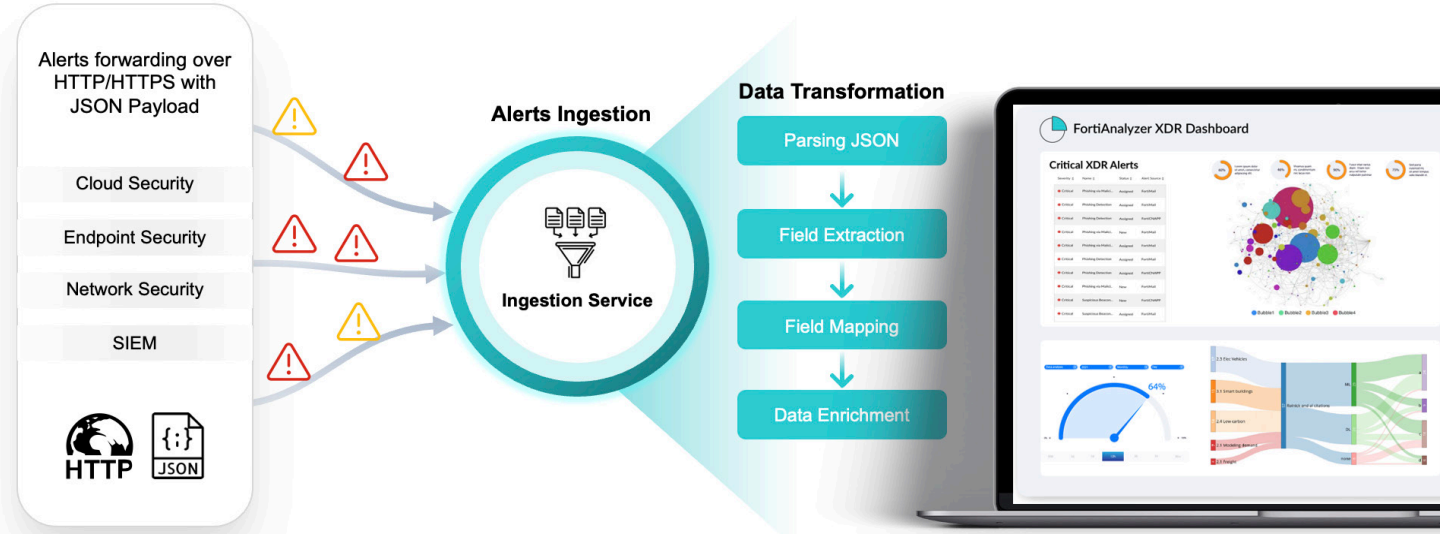
FortiAnalyzer includes a built-in Generative AI assistant that helps security teams quickly analyze and understand complex data. Analysts can use natural language queries to explore logs, summarize incidents, or ask questions about alerts—without needing deep query language expertise. The AI assistant provides context-aware insights, speeds up investigations, and reduces time spent on manual data correlation. Integrated with the Security Fabric, it helps SOC teams make faster, more informed decisions across a broad range of security events.

Extended Detection and Response Across the Security Fabric

Coordinated Detection and Response Across Multiple Security Layers

FortiAnalyzer enables extended detection and response (XDR) by integrating with key Fabric SecOps platforms such as FortiEDR, FortiNDR, FortiDeceptor, FortiCNAPP, and FortiDLP. It correlates data across these layers to deliver unified visibility, advanced threat detection, and enriched context for faster investigations.

Automated responses can be triggered through integrated enforcement points such as FortiGate, FortiManager, FortiMail, FortiEDR, FortiAuthenticator and FortiCNAPP — enabling quick containment, policy enforcement, or remediation actions. This tightly integrated approach helps SOC teams detect threats earlier, respond faster, and reduce risk across endpoints, networks, applications, and the cloud.



High Availability and Scalable Fabric Architecture

Resilient and Distributed for Enterprise and Hyperscale Environments

- **Flexible Deployment Options**

FortiAnalyzer supports a wide range of deployment models to fit diverse infrastructure needs, offering adaptability across on-premises, cloud, and hybrid environments. It is available as a physical appliance for on-premises deployments, a virtual appliance for private or public cloud environments, and also as a hosted solution. This flexibility enables easy scalability across branch offices, hybrid cloud setups, and centralized Security Operations Centers (SOCs).

- **FortiAnalyzer High Availability (HA)**

FortiAnalyzer HA provides real-time redundancy to protect organizations by ensuring continuous operational availability. In the event that the primary (active) FortiAnalyzer fails, a secondary (passive) FortiAnalyzer (up to four-node cluster) will immediately take over, providing log and data reliability and eliminating the risk of having a single point of failure.

- **FortiAnalyzer Fabric**

FortiAnalyzer Fabric allows SOC Administrators to configure two operation modes - Supervisor and Member. This allows viewing of member devices, ADOMs and authorized logging devices, as well as incidents and events created on members. Admins get access to Reports and FortiView across all member FortiAnalyzers, and can perform global search in Log View of logs collected across FortiAnalyzer Fabric members with pre-defined device filters and log drill down for each Member and Member ADOMs.

- **Analyzer Collector Modes**

FortiAnalyzer provides two operation modes: Analyzer and Collector. In Collector mode, the primary task is forwarding logs of the connected devices to an Analyzer and archiving the logs. This configuration greatly benefits organizations with increasing log rates, as the resource intensive log-receiving task is off-loaded to the Collector so that the Analyzer can focus on generating analytics and reports.

Network operations teams can deploy multiple FortiAnalyzers in Collector and Analyzer modes to work together to improve the overall performance of log receiving and processing increased log volumes, providing log storage and redundancy, and rapid delivery of critical network and threat information.

- **Log Forwarding for Third-Party Integration**

Forward logs from one FortiAnalyzer to another FortiAnalyzer unit, a syslog server, or (CEF) server. In addition to forwarding logs to another unit or server, the client FortiAnalyzer retains a local copy of the logs, which are subject to the data policy settings for archived logs. Logs are forwarded in real-time or near real-time as they are received from network devices.

Subscriptions and Extensions

Subscription Licenses and FortiGuard Security Services

- **FortiGuard Outbreak Detection Service**

Deliver automated content package download for detecting the latest malware, including a summary of outbreaks and kill chain mapping for how the malware works. The package includes a FortiGuard Report for the outbreak, Event Handler, and a Report Template to detect outbreaks.

- **FortiGuard Indicators of Compromise Service**

Empower security teams with forensic data from 500 000 IOCs daily, used in combination with FortiAnalyzer analytics to identify suspicious usage and artifacts observed on the network or in an operations system, that have been determined with high confidence to be malicious infections or intrusions, and historical rescan of logs for threat hunting.

- **OT Security Service**

Provide security teams with advanced OT analytics, risk and compliance reports, OT event handlers, and use-case correlation rules.

- **FortiAnalyzer Attack Surface Security Rating and Compliance Service**

Helps security teams design, implement, and maintain their security posture, and provides actionable configuration recommendations as well as key performance and risk indicators

.

- **SOC Automation Subscription Service**

Subscription enables further automation for incident response with enhanced monitoring and escalation, built-in incident management workflows, connectors, playbooks and more.

- **FortiAI Subscription Service**

Provide a generative AI security assistant integrated into FortiAnalyzer for incident investigation, response, and threat hunting. It interprets security events, generates summaries, identifies potential impacts, and offers remediation recommendations. By using natural language prompts, FortiAI can create complex database queries, generate reports, and efficiently perform various other FortiAnalyzer functions.

Cloud Services

FortiAnalyzer Cloud

FortiAnalyzer Cloud offers customers a PaaS-based delivery option for automation-driven, single pane analytics, providing log management, analytics, and reporting for Fortinet NGFW and SD-WAN with an easily accessible cloud-based solution. FortiAnalyzer Cloud delivers reliable real-time insights into network activity with extensive reporting and monitoring for clear, consistent visibility of an organization's security posture. Customers can easily access their FortiAnalyzer Cloud from their FortiCloud single sign-on portal.

Virtual Offerings

FortiAnalyzer VM Subscription

The FortiAnalyzer VM Subscription license model consolidates into one single SKU: VM product SKU, FortiCare Support SKU, FortiGuard IOC and Outbreak Detection Service, SOC Automation services, to simplify the product purchase, upgrade, and renewal. FortiAnalyzer-VM S provides organizations with centralized security event analysis, forensic research, reporting, content archiving, data mining, malicious file quarantining, and vulnerability assessment. Centralized collection, correlation, and analysis of geographically and chronologically diverse security data from Fortinet and third party devices deliver a simplified, consolidated view of your security posture.

The FortiAnalyzer-VM S series SKUs come in stackable 5, 50, and 500 GB/ day logs licenses, so that multiple units of this SKU can be purchased together providing organizations with the ability and cost-efficiencies to scale and meet their logging needs.

FortiAnalyzer VM

Fortinet offers FortiAnalyzer-VM licensing in a perpetual license model with a-la-carte technical support and subscription services. This software-based version of the FortiAnalyzer hardware appliance is designed to run on many virtualization platforms, allowing you to expand your virtual solution as your environment expands.

FORTIANALYZER VIRTUAL APPLIANCES	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100	FAZ-VM-GB500	FAZ-VM-GB2000
Capacity						
GB/ day of Logs *	+1	+5	+25	+100	+500	+2000
Devices/VDOMs Maximum	10 000	10 000	10 000	10 000	10 000	10 000
FortiGuard IOC Service			✓			
Security Automation Service			✓			
Hypervisor Support	Up-to-date hypervisor support can be found in the release note for each FortiAnalyzer version. Visit https://docs.fortinet.com/product/fortianalyzer/ and find the Release Information at the bottom section. Go to "Product Integration and Support" → "FortiAnalyzer [version] support" → "Virtualization"					
vCPU Support (Minimum / Maximum)	4 / Unlimited					
Network Interface Support (Min / Max) **	1 / 12					
Memory Support (Minimum / Maximum)	16 GB / Unlimited for 64-bit					

* Unlimited GB/ day when deployed in collector mode.

** VM supports up to 12 vNIC interfaces/ports. Applicable to 6.4.3+. Actual consumable numbers vary depending on cloud platforms.

Specifications




FORTIANALYZER APPLIANCES	FAZ-150G	FAZ-300G	FAZ-810G	FAZ-1000G
Capacity and Performance				
GB/ day of Logs	25	100	200	660
Analytic Sustained Rate (logs/sec)*	500	2000	4000	20 000
Collector Sustained Rate (logs/sec)*	750	3000	6000	30 000
Devices/VDOMs (Maximum)	50	180	800	2000
Max Number of Days Analytics**	90	50	50	60
Options				
FortiGuard IOC and Outbreak Detection Service	✓	✓	✓	✓
SOC Automation Service	✓	✓	✓	✓
Enterprise Bundle	✓	✓	✓	✓
Hardware Bundle	✓	✓	✓	✓
OT Security Service	✓	✓	✓	✓
Security Rating and Compliance Service	✓	✓	✓	✓
Hardware Specifications				
Form Factor (supports EIA/non-EIA standards)	Desktop	1 RU Rackmount	1 RU Rackmount	2 RU Rackmount
Total Interfaces	2x RJ45 GE	4x RJ45 GE	4x RJ-45 2x GE SFP	2× 2.5GbE RJ45 + 2× 25GbE SFP28
Storage Capacity	4TB (2× 2TB)	8 TB (2× 4 TB)	16TB (4× 4TB) 3.5 in SAS HDDs	32 TB (8 × 4TB) 3.5 in SAS SED HDD
Usable Storage (After RAID)	2 TB	4 TB	8 TB	24 TB
Removable Hard Drives	No	No	✓	✓
RAID Levels Supported	0/1	RAID 0/1	RAID 0/1,1s/5,5s/10	RAID 0/1/5/6/10/50/60
RAID Type	Software	Software	Hardware / Hot Swappable	Hardware / Hot Swappable
Default RAID Level	1	1	10	50
Redundant Hot Swap Power Supplies	No	Optional	Optional	✓
Trusted Platform Module (TPM) ***	Gen 2	Gen 2	✓	✓
Dimensions				
Height x Width x Length (inches)	9.5 × 3.5 × 8	1.73 × 17.24 × 16.38	1.73 × 17.32 × 21.65	3.46 × 17.24 × 24.41
Height x Width x Length (cm)	24.1 × 8.9 × 20.55	4.4 × 43.8 × 41.6	4.4 × 44.0 × 55.0	8.8 × 43.8 × 62.0
Weight	9.35 lbs (4.24 kg)	22.5 lbs (10.2 kg)	25.75 lbs (11.68 kg)	49.6 lbs (22.5 kg)
Environment				
AC Power Supply	100–240V AC, 50–60 Hz	100–240V AC, 60–50 Hz	100-240Vac, 50~60Hz, 4A max	100-240Vac, 50~60Hz, 4A max
Power Consumption (Average / Maximum)	36 W / 43 W	90.1 W / 99 W	115W / 150W	251.36W / 302W
Heat Dissipation	147.4 BTU/h	337.8 BTU/h	433 BTU/h	857.73 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)	32°F to 104° F (0°C to 40° C)
Storage Temperature	-4°F to 167° F (-20°C to 75° C)	-13°F to 167° F (-25°C to 75° C)	-4°F to 167° F (-20°C to 75° C)	-40°F to 158° F (-40°C to 70° C)
Humidity	5% to 95% non-condensing	20% to 90% non-condensing	5% to 95% non-condensing	5% to 95% non-condensing
Forced Airflow	Front to Back	Front to Back	Front to Back	Front to Back
Operating Altitude	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m)	Up to 16 404 ft (5000 m)
Compliance				
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

* Sustained Rate - maximum constant log message rate that the FAZ platform can maintain for minimum 48 hours without SQL database and system performance degradation.

** The maximum number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.

*** Gen2 refers to hardware that has been upgraded since initial release.

Specifications



FORTIANALYZER APPLIANCES	FAZ-3100G	FAZ-3510G	FAZ-3700G
Capacity and Performance			
GB/ day of Logs	3000	5000	8300
Analytic Sustained Rate (logs/sec)*	42 000	60 000	100 000
Collector Sustained Rate (logs/sec)*	60 000	90 000	150 000
Devices/VDOMs (Maximum)	4000	10 000	10 000
Max Number of Days Analytics**	30	35	60
Options			
FortiGuard IOC and Outbreak Detection Service	✓	✓	✓
Security Automation Service	✓	✓	✓
Enterprise Bundle	✓	✓	✓
Hardware Bundle	✓	✓	✓
OT Security Service	✓	✓	✓
Security Rating and Compliance Service	✓	✓	✓
Hardware Specifications			
Form Factor (supports EIA/non-EIA standards)	3 RU Rackmount	4 RU Rackmount	4 RU Rackmount
Total Interfaces	2x GE RJ45, 2× 25GE SFP28	2× 10GbE RJ45, 2× 25GbE SFP28	2× 10GE RJ-45 + 2× 25GE SFP28
Storage Capacity	64 TB (16 × 4TB) 3.5" SAS SED HDD + 3.84 (2× 1.92TB) 2.5" NVMe SSD	24× 4TB (96TB) + 2× 3.84TB (7.68TB)	240TB (60× 4TB) 3.5 in HDD + 19.2TB (6× 3.2TB) NVMe SSD
Usable Storage (After RAID)	56 TB	84 TB	224 TB
Removable Hard Drives	✓	✓	✓
RAID Levels Supported	RAID 0/1,1s/5,5s/6,6s/10/50/60	RAID 0/1,1s/5,5s/6,6s/10/50/60	RAID 0/1,1s/5,5s/6,6s/10/50/60
RAID Type	Hardware / Hot Swappable	Hardware / Hot Swappable	Hardware / Hot Swappable
Default RAID Level	50	50	50
Redundant Hot Swap Power Supplies	✓	✓	✓
Trusted Platform Module (TPM) ***	✓	✓	✓
Dimensions			
Height x Width x Length (inches)	5.2 × 17.2 × 25.5	7 × 17.2 × 27.5	7.0 × 17.2 × 30.2
Height x Width x Length (cm)	13.0 × 44.0 × 65.0	17.8 × 43.7 × 69.9	17.8 × 43.7 × 76.7
Weight	69.6 lbs (31.57 kg)	65 lbs (29.5 kg)	118 lbs (53.5 kg)
Environment			
AC Power Supply	100-127V~/10A, 200-240V~/5A	100-127V~/10A, 200-240V~/5A	2000W AC****
Power Consumption (Average/Max)	395 W / 510 W	983 W / 1278 W	850 W / 1423.4 W
Heat Dissipation	1740.19 BTU/h	3424 BTU/h	4858 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	50°F to 95°F (10°C to 35°C)
Storage Temperature	-4°F to 158°F (-20°C to 70°C)	-4°F to 167°F (-20°C to 75°C)	-40°F to 158°F (-40°C to 70°C)
Humidity	5% to 95% (non-condensing)	5% to 95% (non-condensing)	8% to 90% (non-condensing)
Forced Airflow	Front to Back	Front to Back	Front to Back
Operating Altitude	Up to 13 123 ft (4000 m)	Up to 10 000 ft (3048 m)	Up to 7400 ft (2250 m)
Compliance			
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

* Sustained Rate - maximum constant log message rate that the FAZ platform can maintain for minimum 48 hours without SQL database and system performance degradation.

** is the max number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.

*** Gen2 refers to hardware that has been upgraded since initial release.

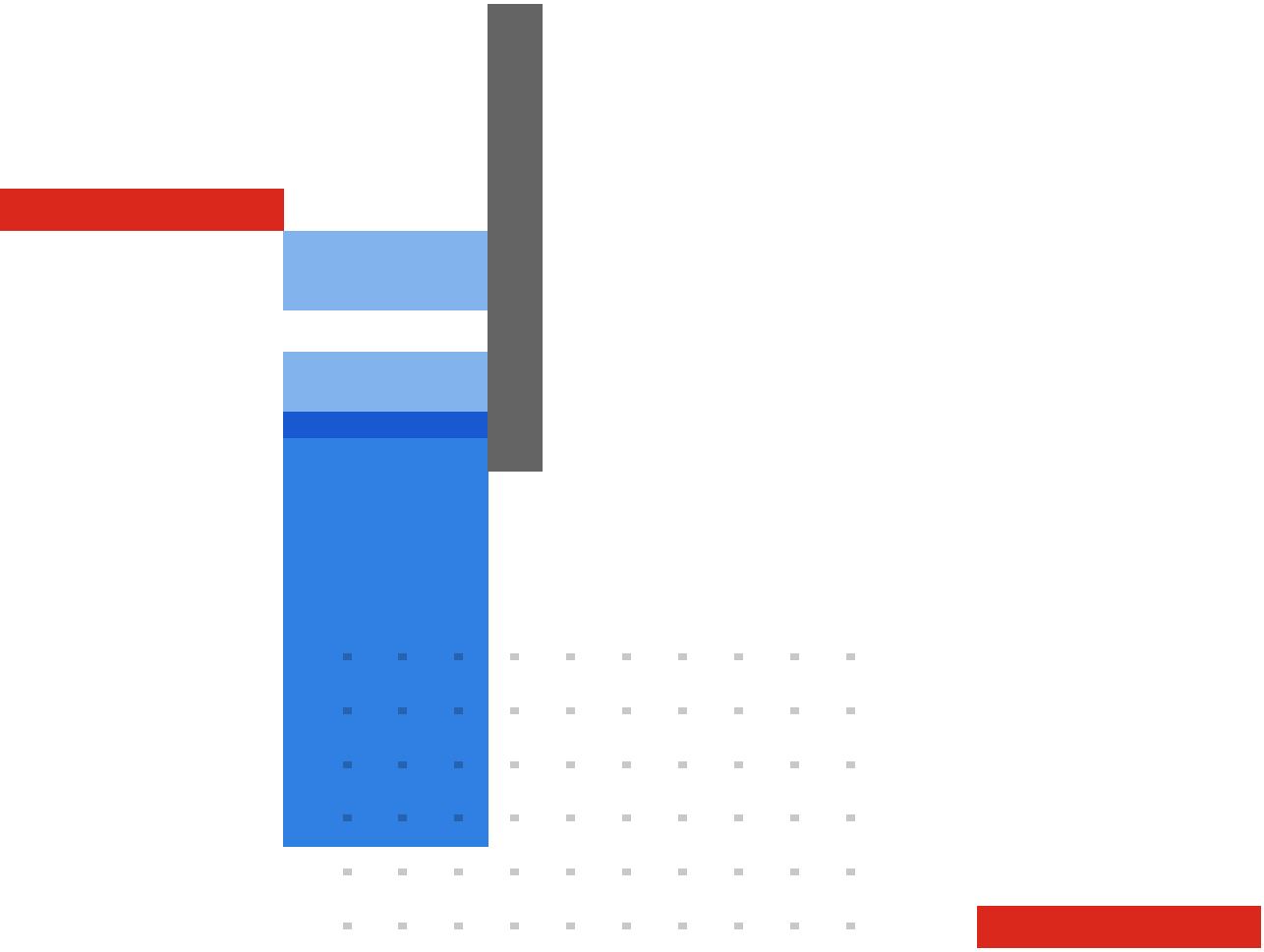
****3700G must connect to a 200V - 240V power source.

Ordering Information

Product	SKU	Description
FortiAnalyzer	FAZ-150G	Centralized log and analysis appliance — 2x RJ45 GE, 4 TB storage, up to 25 GB/ day of logs.
	FAZ-300G	Centralized log and analysis appliance — 4x RJ45 GE, 8 TB storage, up to 100 GB/ day of logs.
	FAZ-810G	Centralized log and analysis appliance — 4x GE, 2x SFP, 16 TB self-encrypting storage, up to 200 GB/ day of logs.
	FAZ-1000G	Centralized logging and analysis appliance - 2× 2.5GbE RJ45 + 2× 25GbE SFP28, 32TB storage, up to 660 GB/Day of Logs.
	FAZ-3100G	Centralized log and analysis appliance — 2x GE RJ45, 2× 25GE SFP28, 64 TB storage, dual power supplies, up to 3000 GB/ day of logs.
	FAZ-3510G	Centralized log and analysis appliance — 2× 10GbE RJ45, 2× 25GbE SFP28, 96 TB storage, up to 5000 GB/ day of logs.
	FAZ-3700G	Centralized log and analysis appliance - 2× 10GE RJ-45 + 2× 25GE SFP28 slots, 240TB HDD + 19.2TB NVMe SSD storage, up to 8300 GB/ day of Logs.
FortiAI Subscription	FC-10-[Model Code]-1118-02-DD	Generative AI powered security service utilizing large language models (LLMs) for real-time assistance in SOC analysis, incident investigation, triage and response.
FortiAnalyzer-VM Subscription License with Support	FC1-10-AZVMS-465-01-DD	Subscription license for 5 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service.
	FC2-10-AZVMS-465-01-DD	Subscription license for 50 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service.
	FC3-10-AZVMS-465-01-DD	Subscription license for 500 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service.
FortiAnalyzer-VM	FAZ-VM-GB1	Upgrade license for adding 1 GB/Day of Logs.
	FAZ-VM-GB5	Upgrade license for adding 5 GB/Day of Logs.
	FAZ-VM-GB25	Upgrade license for adding 25 GB/Day of Logs.
	FAZ-VM-GB100	Upgrade license for adding 100 GB/Day of Logs.
	FAZ-VM-GB500	Upgrade license for adding 500 GB/Day of Logs.
	FAZ-VM-GB2000	Upgrade license for adding 2 TB/Day of Logs.
FortiAnalyzer Cloud Storage Subscription	FC1-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 5 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.
	FC2-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.
	FC3-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 500 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.
FortiAnalyzer - Backup to Cloud Service	FC-10-FAZ00-286-02-DD	One year subscription to FortiAnalyzer storage connector service for 10TB data transfer to public cloud.
SOCaaS	FC-10-[Model Code]-464-02-DD	SOCaaS: 24×7 cloud-based managed log monitoring, incident triage and SOC escalation service.
FortiAnalyzer Cloud	FC-10-[Model Code]-585-02-DD	FortiAnalyzerCloud: cloud-based central logging and analytics. Include all FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Detection Service.
Security Automation Service	FC-10-[Model Code]-335-02-DD	Subscription license for Security Automation Service - Appliance.
	FC[GB Day Code]-10-LV0VM-335-02-DD	Subscription license for Security Automation Service - Virtual Machine.
FortiGuard IOC and Outbreak Detection Service	FC-10-[Model Code]-661-02-DD	Subscription license for FortiGuard IOC and Outbreak Detection Service - Appliance.
	FC[GB Day Code]-10-LV0VM-661-02-DD	Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine.
OT Security Service	FC-10-[Model Code]-159-02-DD	OT Security Service including advanced OT analytics, risk and compliance reports, event handlers, and use-case correlation rules.
FortiAnalyzer Security Rating and Compliance Service	FC-10-[Model Code]-175-02-DD	Subscription license for FortiAnalyzer Security Rating and Compliance Service.
Enterprise Protection Bundle	FC-10-[Model Code]-466-02-DD	Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Detection service).
Hardware Bundle	FAZ-[Hardware Model]-BDL-466-DD	Hardware plus FortiCare Premium and FortiAnalyzer Enterprise Protection.

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

April 4, 2025

FAZ-DAT-R86-20250404