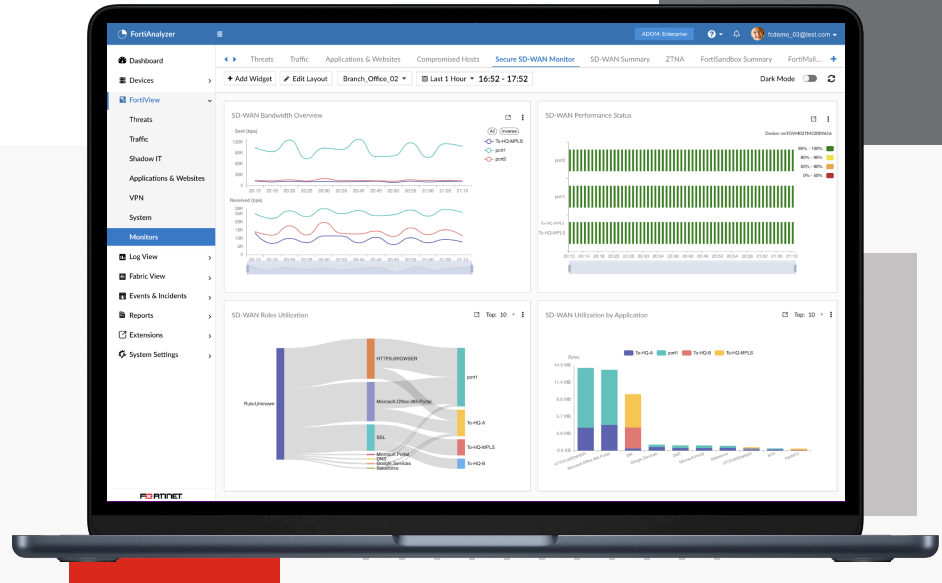# FortiAnalyzer™

Security Fabric Network Analytics

Highlights

- Centralized network monitoring and visibility

- Advanced threat and vulnerability detection with event and log data correlation

- Augmented NOC/SOC operations for real-time response, analytics, and reporting

- Automation to save time, reduce errors, and improve efficiency

- Multi-tenancy solution with quota management

- Administrative domains for operational effectiveness and compliance

- 70+ reports and 2000+ ready-to-use datasets, charts, and macros

Analytics, Reports, and Compliance Across the Security Fabric

FortiAnalyzer is a powerful log management, analytics, and reporting platform that provides organizations with a single console to manage, automate, orchestrate, and respond, enabling simplified security operations, proactive identification and remediation of risks, and complete visibility of the entire attack landscape.

Integrated with the Fortinet Security Fabric, FortiAnalyzer enables Network and Security Operations Teams with real-time detection capabilities, centralized security analytics and end-to-end security posture awareness to help analysts identify advanced persistent threats (APTs) and mitigate risks before a breach can occur.

Capabilities

Incident Detection and Response

Centralized NOC/SOC Visibility for the Attack Surface

FortiAnalyzer provides Security Fabric Analytics across all device logs with event correlation and real-time detection of Advanced Persistent Threats (APTs), vulnerabilities and Indicators of Compromise (IOC) for FortiGate NGFWs, FortiClient, FortiSandbox, FortiWeb, FortiMail and other Fortinet products, for deep visibility and critical network insights. Simplified orchestration and automated workflows provide Network Security Operations teams with real-time notifications, reports, and dashboards for single-pane visibility and actionable results.

Incidents and Events Management

Security teams can monitor and manage alerts and event logs from Fortinet devices, with events processed and correlated in a format that analysts can easily understand. Investigate suspicious traffic patterns and search using filters in predefined or custom event handlers to generate real-time notifications and monitoring for NOC and SOC operations, SD-WAN, SSL VPN, wireless, Shadow IT, IPS, network recon, FortiClient, and more.

The Incidents component enables analysts to manage incident handling and life cycle, with incidents generated by events that show affected assets, endpoints, users and timelines.

Fabric Automation

FortiAnalyzer Playbooks boost an organization's security team abilities to simplify investigation efforts through automated incident response, freeing up resources and allowing analysts to focus on critical tasks. Out-of-the-box playbook templates enable SOC analysts to quickly customize their use cases, define custom processes, interact with other Security Fabric devices like FortiOS and EMS, edit playbooks and tasks in the visual playbook editor and use the Playbook Monitor for investigation of compromised hosts, infections and critical incidents, data enrichment for Assets and Identity views, blocking malware, C&C IPs, and more.

Security Fabric Analytics

Analytics and Reporting

FortiAnalyzer automation driven analytics empowers network security operations teams to complete a fast assessment of network devices, systems, and users, with correlated log data and FortiGuard threat intelligence for analysis of real-time and historical events.
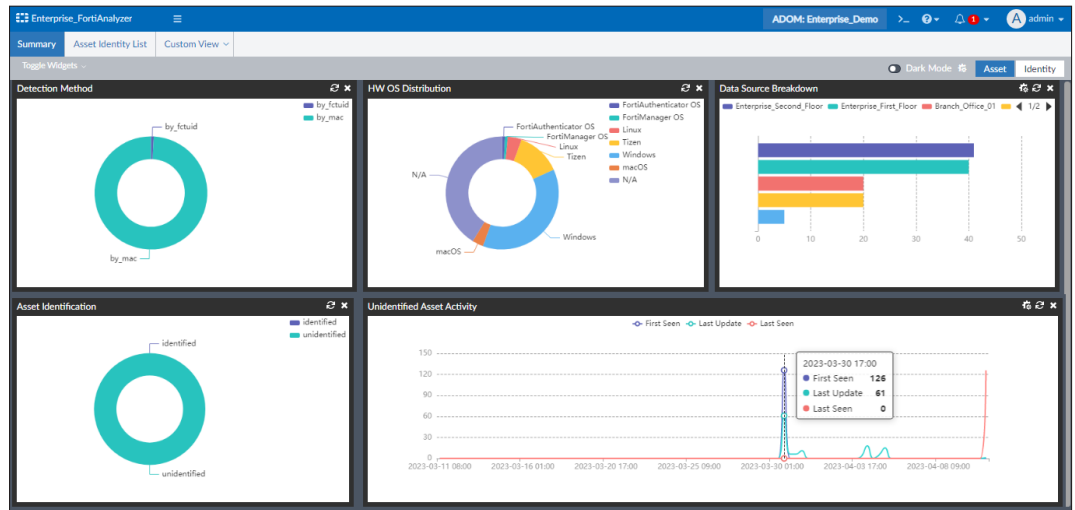
- **FortiView** Monitors and Views provide deep insights with context and meaning of network activity, risks, vulnerabilities, attack attempts, indicators of compromise and anomalies, sanctioned and unsanctioned user activity.

- **Log View** enables analysts to expand their investigation and utilize search filters on managed device logs, drill down on logs, with custom views and log groups, including a SIEM database with normalized logs for Fortinet devices in Fabric ADOMs.

- **Reports** provide comprehensive analysis of your Security Posture, including reports for Operational Technology (OT), security rating, security rating for PCI, Secure SD-WAN, VPN, FortiNDR network anomaly detection, cyber threat assessments, 360 Security Reviews, situational awareness, compliance, auditing, and more.

Capabilities

Assets and Identity

FortiAnalyzer Fabric View with Assets and Identity monitoring provides SOC teams with elevated awareness and visibility into an organization's endpoints and users with dashboards and correlated device and UEBA information, vulnerability detections, EMS tagging, and asset classifications through telemetry with EMS, NAC, Fortinet Fabric Agent, and an OT Dashboard View.

Subscriptions and Extensions

### Subscription Licenses and FortiGuard Security Services

- **FortiGuard Outbreak Detection Service** delivers 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** empowers 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.

- **Shadow IT Monitoring Service** provides continuous monitoring of unapproved devices, resources, unsanctioned accounts and unauthorized use of SaaS and IaaS, API integration, and third party apps. The service identifies rogue users using personal accounts for managing company assets, using correlated FortiOS and FortiCASB data with a FortiCASB account subscribed for SaaS features.

- **OT Security Service** provides security teams with advanced OT analytics, risk and compliance reports, OT event handlers, and use-case correlation rules.

- **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.

- **Security Automation Service** subscription enables further automation for incident response with enhanced monitoring and escalation, built-in incident management workflows, connectors, playbooks and more.

Management Extension Applications (MEAs)

The Management Extensions pane allows you to enable licensed applications that are released and signed by Fortinet, which can be installed and run on FortiAnalyzer, including the FortiSIEM and FortiSOAR.

Capabilities
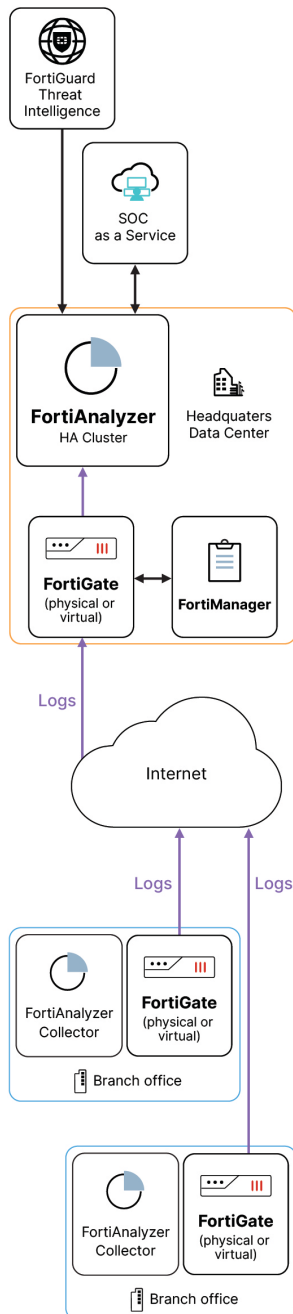
Deployments

Deploying FortiAnalyzer

FortiAnalyzer can be deployed as a physical hardware appliance, virtual machine (VM) and virtual machine subscription (VM-S), as well as private or public cloud instance, with scalability, redundancy and backup, and high availability capabilities.

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.

Multi-Tenancy with Flexible Quota Management

FortiAnalyzer provides the ability to manage multiple sub-accounts with each account having its own administrators and users. The time-based archive/analytic log data policy, per Administrative Domain (ADOM), allows automated quota management based on the defined policy, with trending graphs to guide policy configuration and usage monitoring.

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.

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 and support for .

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.

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, Security 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 the FortiAnalyzer-VM licensing in a stackable 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, which allows 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	+2,000
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-800G	FAZ-810G
Capacity and Performance				
GB/ day of Logs	25	100	200	200
Analytic Sustained Rate (logs/sec)*	500	2000	4000	4000
Collector Sustained Rate (logs/sec)*	750	3000	6000	6000
Devices/VDOMs (Maximum)	50	180	800	800
Max Number of Days Analytics**	90	50	50	50
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)	Desktop	1 RU Rackmount	1 RU Rackmount	1 RU Rackmount
Total Interfaces	2 x RJ45 GE	4 x RJ45 GE	4 x RJ45 GE, 2 x SFP	4x RJ-45 2x GE SFP
Storage Capacity	4TB (2× 2TB)	8 TB (2 × 4 TB)	16 TB (4 × 4 TB)	16TB (4× 4TB) 3.5 in SAS HDDs
Usable Storage (After RAID)	2 TB	4 TB	8 TB	8 TB
Removable Hard Drives	No	No	✓	✓
RAID Levels Supported	0/1	RAID 0/1	RAID 0/1,1s/5,5s/10	RAID 0/1,1s/5,5s/10
RAID Type	Software	Software	Hardware / Hot Swappable	Hardware / Hot Swappable
Default RAID Level	1	1	10	10
Redundant Hot Swap Power Supplies	No	Optional	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	1.73 × 17.32 × 21.65
Height x Width x Length (cm)	24.1 × 8.9 × 20.55	4.4 × 43.8 × 41.6	4.4 × 44.0 × 55.0	4.4 × 44.0 × 55.0
Weight	9.35 lbs (4.24 kg)	22.5 lbs (10.2 kg)	25.75 lbs (11.68 kg)	25.75 lbs (11.68 kg)
Environment				
AC Power Supply	100–240V AC, 50–60 Hz	100–240V AC, 60–50 Hz	100–240V AC, 50–60 Hz	100-240Vac, 50~60Hz, 4A max
Power Consumption (Average / Maximum)	36 W / 43 W	90.1 W / 99 W	134 W / 174.2 W	115W / 150W
Heat Dissipation	147.4 BTU/h	337.8 BTU/h	594.4 BTU/h	433 BTU/h
Operating Temperature	32°–104° F (0°–40° C)	32°–104° F (0°–40° C)	32°–104° F (0°–40° C)	32°–104° F (0°–40° C)
Storage Temperature	-4°–167° F (-20°–75° C)	-13°–167° F (-25°–75° C)	-4°–167° F (-20°–75° C)	-4°–167° F (-20°–75° 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 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, 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-1000F	FAZ-3000G	FAZ-3700G
Capacity and Performance			
GB/ day of Logs	660	3000	8300
Analytic Sustained Rate (logs/sec)*	20 000	42 000	100 000
Collector Sustained Rate (logs/sec)*	30 000	60 000	150 000
Devices/VDOMs (Maximum)	2000	4000	10 000
Max Number of Days Analytics**	34	30	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)	2 RU Rackmount	3 RU Rackmount	4 RU Rackmount
Total Interfaces	2 × 10GbE RJ45, 2 × 10GbE SFP+	2 x GE RJ45, 2× 25GE SFP28	2× 10GE RJ-45 + 2× 25GE SFP28
Storage Capacity	32 TB (8 × 4 TB)	64 TB (16 × 4TB)	240TB (60 × 4TB) 3.5" HDD + 19.2TB (6x 3.2TB) NVMe SSD
Usable Storage (After RAID)	24 TB	56 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) *	No	No	✓
Dimensions			
Height x Width x Length (inches)	3.5 × 17.2 × 25.6	5.2 × 17.2 × 25.5	7.0 × 17.2 × 30.2
Height x Width x Length (cm)	8.9 × 43.7 × 65.0	13.0 × 44.0 × 65.0	17.8 × 43.7 × 76.7
Weight	34 lbs (15.42 kg)	66.5 lbs (30.15 kg)	118 lbs (53.5 kg)
Environment			
AC Power Supply	100–240V AC, 50–60 Hz	100-127V~/10A, 200-240V~/5A	2000W AC****
Power Consumption (Average / Maximum)	192.5 W / 275 W	385 W / 500 W	850 W / 1423.4 W
Heat Dissipation	920 BTU/h	1350 BTU/h	4858 BTU/h
Operating Temperature	50°–95°F (10°–35°C)	32°-104°F (0°-40°C)	50°–95°F (10°–35°C)
Storage Temperature	-40°–140°F (-40°–60°C)	-4°-167°F (-20°-75°C)	-40°–158°F (-40°–70°C)
Humidity	8% to 90% 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 7400 ft (2250 m)	Up to 7400 ft (2250 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.
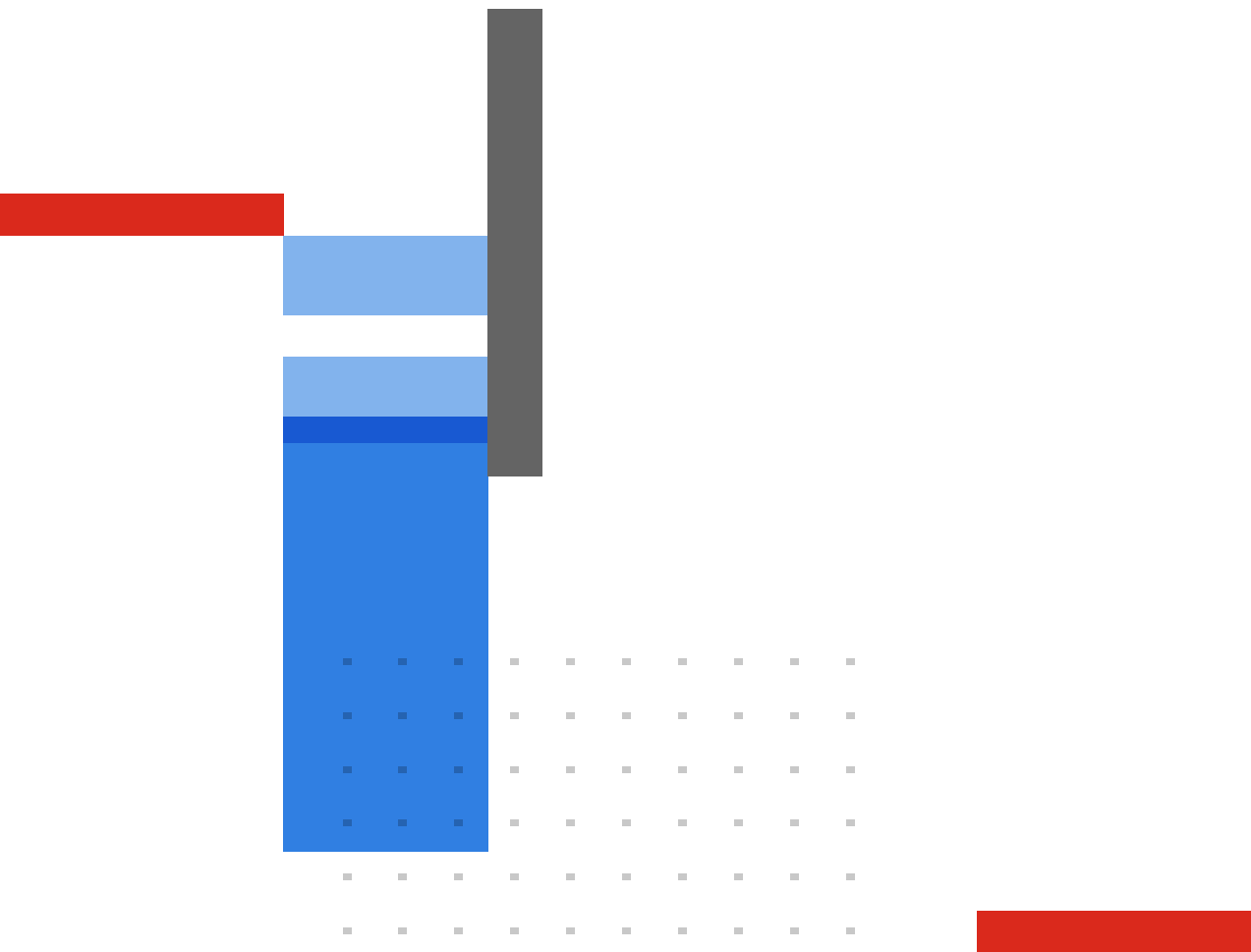
****3700G must connect to a 200V - 240V power source.

Ordering Information

Product	SKU	Description
FortiAnalyzer	FAZ-150G	Centralized log and analysis appliance — 2 x RJ45 GE, 4 TB storage, up to 25 GB/ day of logs.
	FAZ-300G	Centralized log and analysis appliance — 4 x RJ45 GE, 8 TB storage, up to 100 GB/ day of logs.
	FAZ-800G	Centralized log and analysis appliance — 4 x GE, 2 x SFP, 16 TB storage, up to 200 GB/ day of logs.
	FAZ-810G	Centralized log and analysis appliance — 4 x GE, 2 x SFP, 16 TB self-encrypting storage, up to 200 GB/ day of logs.
	FAZ-1000F	Centralized log and analysis appliance — 2 × 10GE RJ45, 2 × 10GbE SFP+, 32 TB storage, dual power supplies, up to 660 GB/ day of logs.
	FAZ-3000G	Centralized log and analysis appliance — 2 x GE RJ45, 2× 25GE SFP28, 64 TB storage, dual power supplies, up to 3000 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.
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.
FortiAnalyzer Cloud with SOCaaS	FC-10-[Model Code]-464-02-DD	FortiAnalyzer Cloud with SOCaaS: cloud-based central logging and analytics. Include All FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Service and SOCaaS.
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.

FURTINET®

www.fortinet.com