DATA SHEET

FortiAnalyzer

Available in:

Appliance Virtual Machine Cloud

Fortinet Security Fabric Visibility, Analytics and Automation for the Modern Enterprise

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, advanced threat detection capabilities, centralized security analytics, end-to-end security posture awareness and control, helps security teams identify and mitigating threats before a breach can occur.

Orchestrate security tools, people, and process for streamlined execution of tasks and workflows, incident analysis and response, and rapidly expedite threat detection, case creation and investigation, and mitigation and response.

Automate workflows and trigger actions with connectors, playbooks, and event handlers to accelerate your network security team's ability to respond to critical alerts, events, and service level agreement (SLA) for regulation and compliance.

Respond in real-time to network security attacks, vulnerabilities, and warnings of potential compromises, with threat intelligence, event correlation, monitoring, alerts and reporting for immediate tactical response and remediation.

Key Features

- Security Fabric Analytics with event correlation and real-time detection across all logs, with Indicators of Compromise (IOC) service and detection of advanced threats
- Fortinet Security Fabric integration with FortiGate NGFWs, FortiClient, FortiSandbox, FortiWeb, FortiMail, and others for deeper visibility and critical network insights
- Enterprise-grade high availability to automatically back-up FortiAnalyzer databases (up to four node cluster), which can be geographically dispersed for disaster recovery
- Security Automation reduces complexity, leveraging REST API, scripts, connectors, and automation stitches to expedite security response and reduce time-to-detect
- Multi-Tenancy solution with quota management, leveraging (ADOMs) to separate customer data and manage domains for operational effectiveness and compliance
- Flexible deployment options as appliance, VM, hosted, or public cloud. Use AWS, Azure, or Google for cloud secondary archival storage

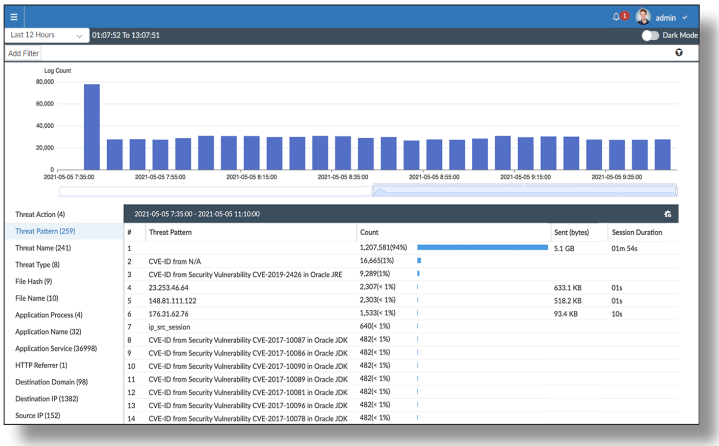
FEATURE HIGHLIGHTS

Across Fortinet's Security Fabric

Incident Detection and Response

Centralized NOC/SOC Visibility for the Attack Surface

The FortiSOC view helps security and network operations teams protect network assets with correlated log and threat data and insights through actionable views with deep drill-down capabilities. Real-time notifications, reports, predefined or customized dashboards delivery single-pane visibility and actionable results. Utilize FortiAnalyzer workflow automation for simplified orchestration of security operations, management of threats, vulnerabilities, and incident response. Proactively investigate anomalies and threats through analysis of SIEM normalized logs in Threat Hunting view.

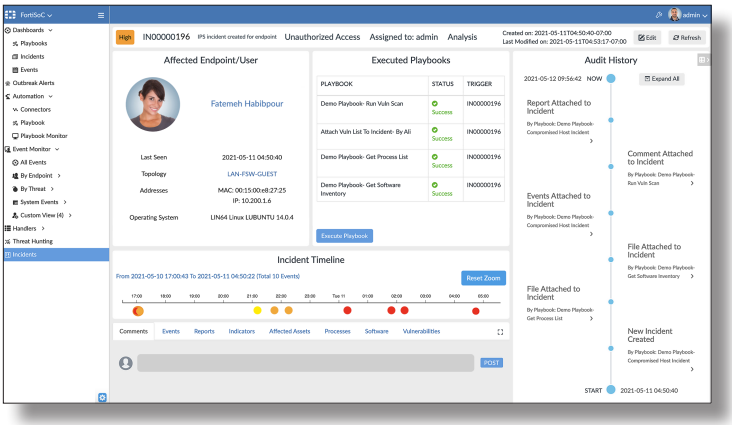


Event Management

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.

Incident Management

The Incidents component in FortiSOC enables security operations teams to manage incident handling and life cycle with incidents created from events to show affected assets, endpoints, and users. Analysts can assign incidents, view and drill down on event details, incident timelines, add analysis comments, attach reports and artifacts, and review playbook execution details for complete audit history.



Integrate with FortiSOAR for further incident investigation and threat eradication including support to export incident data to FortiSOAR through the FortiAnalyzer fabric connector.

Playbook Automation

FortiAnalyzer Playbooks boost the security team's abilities of an organization to simplify investigation efforts through automated incident response, freeing up resources and allowing analysts to focus on tasks that are more critical.

Out-of-the-box playbook templates enable SOC analysts to quickly customize their use cases, including playbooks for investigation of compromised hosts, infections and critical incidents, data enrichment for Fabric View Assets & Identity views, blocking of malware, C&C IPs, and more. Security teams can define custom processes, edit playbooks and tasks in the visual playbook editor, utilize the Playbook monitor to review task execution details, import or export playbooks, and use built-in connectors with **OAuth2** authentication, allowing playbooks to interact with other Security Fabric devices like FortiOS and EMS. The new connector health check provides an indicator for verifying that connectors are always up and working.

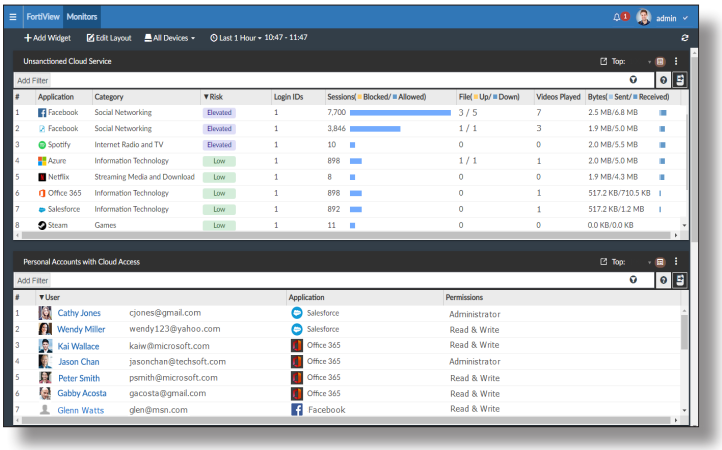
Subscription Licenses and FortiGuard Security Services

The 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.

The FortiGuard Indicators of Compromise subscription 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.

FEATURE HIGHLIGHTS

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

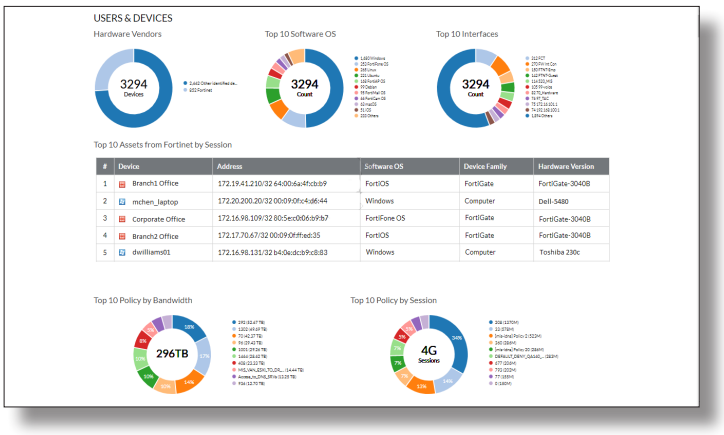


Include the FortiSOC subscription to enable further automation for incident response with enhanced alert monitoring and escalation, built-in incident management workflows, connectors, and many more FortiSOC playbooks.

Security Fabric Analytics

Analytics and Reporting

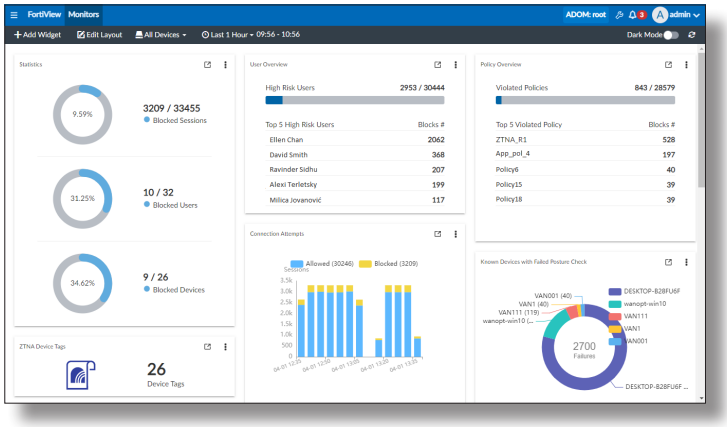
FortiAnalyzer automation driven analytics empowers security teams by providing full visibility of network devices, systems, and users, with correlated log data for threat intelligence and analysis of real-time and historical events. Analysts have access to correlated monitoring views and reports to provide deep insights with context and meaning of network activity, risks, vulnerabilities, attack attempts and investigation of operational anomalies, with monitoring of sanctioned and unsanctioned user activity for SaaS applications.



FortiAnalyzer provides over 70 report templates, 950+ datasets, 900+ charts, and 160+ macros that are ready-to-use including reports for Secure SD-WAN, VPN, threat assessments, 360 Security Reviews, situational awareness, self-harm and risk indicators to deliver specific business metrics to target stakeholders in flexible viewing formats including PDF, HTML, CSV, XML, and JSON.

FortiView is a comprehensive monitoring solution that provides multilevel views and summaries of real-time critical alerts and information such as top threats and IOCs to your network including Botnet and C&C, top sources/destinations of network traffic, top applications, websites and SaaS, VPN and System information, and other Fabric device intelligence.

Monitors view provides operations teams with customizable NOC and SOC dashboards and widgets designed for display across multiple screens in the Operations Center. Monitor events in real-time through the pre-defined dashboard views for SD-WAN, VPN, Wi-Fi, Incoming/Outgoing Traffic, Applications and Websites, FortiSandbox Detections, Endpoint Vulnerabilities, Software Inventory, Top Threats, Shadow IT (monitoring service), ZTNA and many more.



Assets and Identity

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

Log View enables analysts to expand their investigation and utilize search filters on managed device logs, with log drill down, formatted or raw logs, log import/export, custom views and log groups, including a SIEM database with normalized logs for devices in Fabric ADOMs.

FEATURE HIGHLIGHTS

Deployments

Deploying FortiAnalyzer

FortiAnalyzer plays a pivotal role in the Fortinet Security Fabric and can be deployed in a variety of configurations to best support the needs of any organization for analytics, back-ups, disaster recovery, storage, availability, and redundancy plus log collection and log forwarding for high-volume networks with sizable generation of event logs.

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 Mode

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.

Trusted Platform Module (TPM) Encryption

FortiAnalyzer G Series features a dedicated micro-controller module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys in TPM, with hardware-based security mechanisms that protect against malicious software and phishing attacks.

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. With the FortiCloud Premium subscription, customers can easily enable the FortiAnalyzer Cloud service by purchasing a FortiAnalyzer Cloud SOCaaS subscription.

Customers can easily access their FortiAnalyzer Cloud from their FortiCloud single sign-on portal.

VIRTUAL OFFERINGS

FortiAnalyzer Virtual Machines

FortiAnalyzer Virtual Machines are a virtual version of the hardware appliance and are designed to run on many virtualization platforms, offering all the latest features of the FortiAnalyzer appliance. They allow organizations to simplify their centralized log management and analytics solution, automate workflows, and help NOC and SOC teams identify and respond to threats. FortiAnalyzer-VMs are available in both a subscription and perpetual offering.

FortiAnalyzer-VM S

The new FortiAnalyzer Subscription license model consolidates the VM product SKU and the FortiCare Support SKU, plus IOC and FortiAnalyzer SOC (SOAR/SIEM) services into one single SKU, 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 services available for 24×7 FortiCare support and subscription license for the FortiGuard Indicator of Compromise (IOC).

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.

SPECIFICATIONS

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
Storage Capacity	+500 GB	+3 TB	+10 TB	+24 TB	+48 TB	+100 TB
Devices/VDOMs Maximum	10,000	10,000	10,000	10,000	10,000	10,000
Chassis Management	✓	✓	✓	✓	✓	✓
Virtual Machine						
FortiGuard Indicator of Compromise (IOC)			✓			
SOC Subscription			✓			
Virtual Machine						
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) [5]	1 / 4					
Memory Support (Minimum / Maximum)	8 GB / Unlimited for 64-bit					

* Unlimited GB/ day when deployed in collector mode

SPECIFICATIONS



FORTIANALYZER APPLIANCES	FAZ-150G	FAZ-300G	FAZ-800G
Capacity and Performance			
GB/ day of Logs	25	100	200
Analytic Sustained Rate (logs/sec)*	500	2,000	4,000
Collector Sustained Rate (logs/sec)*	750	3,000	6,000
Devices/VDOMs (Maximum)	50	180	800
Max Number of Days Analytics**	90	50	50
Options			
FortiGuard Indicator of Compromise (IOC)	✓	✓	✓
SOC Subscription	✓	✓	✓
FortiGuard Outbreak Detection Service	✓	✓	✓
Enterprise Bundle	✓	✓	✓
Hardware Bundle	✓	✓	✓
Hardware Specifications			
Form Factor (supports EIA/non-EIA standards)	Desktop	1 RU Rackmount	1 RU Rackmount
Total Interfaces	2 x RJ45 GE	4 x RJ45 GE	4 x RJ45 GE, 2 x SFP
Storage Capacity	4TB (2× 2TB)	8 TB (2 × 4 TB)	16 TB (4 × 4 TB)
Usable Storage (After RAID)	2 TB	4 TB	8 TB
Removable Hard Drives	No	No	✓
RAID Levels Supported	0/1	RAID 0/1	RAID 0/1,1s/5,5s/10
RAID Type	Software	Software	Hardware / Hot Swappable
Default RAID Level	1	1	10
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
Height x Width x Length (cm)	24.1 × 8.9 × 20.55	4.4 × 43.8 × 41.6	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)
Environment			
AC Power Supply	100–240V AC, 50–60 Hz	100–240V AC, 60–50 Hz	100–240V AC, 50–60 Hz
Power Consumption (Average / Maximum)	36W / 43W	90.1W / 99 W	134W / 174.2 W
Heat Dissipation	147.4 BTU/h	337.8 BTU/h	594.4 BTU/h
Operating Temperature	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)
Humidity	5 to 95% non-condensing	20 to 90% non-condensing	5 to 95% non-condensing
Operating Altitude	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 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

* 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-3500G	FAZ-3700G
Capacity and Performance				
GB/ day of Logs	660	3,000	5,000	8,300
Analytic Sustained Rate (logs/sec)*	20,000	42,000	60,000	100,000
Collector Sustained Rate (logs/sec)*	30,000	60,000	90,000	150,000
Devices/VDOMs (Maximum)	2,000	4,000	10,000	10.000
Max Number of Days Analytics**	34	30	38	60
Options				
FortiGuard Indicator of Compromise (IOC)	✓	✓	✓	✓
SOC Subscription	✓	✓	✓	✓
FortiGuard Outbreak Detection Service	✓	✓	✓	✓
Enterprise Bundle	✓	✓	✓	✓
Hardware Bundle	✓	✓	✓	✓
Hardware Specifications				
Form Factor (supports EIA/non-EIA standards)	2 RU Rackmount	3 RU Rackmount	4 RU Rackmount	4 RU Rackmount
Total Interfaces	2 × 10GbE RJ45, 2 × 10GbE SFP+	2 x GE RJ45, 2× 25GE SFP28	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)	96 TB (24 × 4 TB)	240TB (60 × 4TB) 3.5" HDD + 19.2TB (6× 3.2TB) NVMe SSD
Usable Storage (After RAID)	24 TB	56 TB	80 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 0/1,1s/5,5s/6,6s/10/50/60
RAID Type	Hardware / Hot Swappable	Hardware / Hot Swappable	Hardware / Hot Swappable	Hardware / Hot Swappable
Default RAID Level	50	50	50	50
Redundant Hot Swap Power Supplies	✓	✓	✓	✓
Trusted Platform Module (TPM) ***	No	No	Gen 2	✓
Dimensions				
Height x Width x Length (inches)	3.5 × 17.2 × 25.6	5.2 × 17.2 × 25.5	7.0 × 17.2 × 26.0	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 × 66.0	17.8 × 43.7 × 76.7
Weight	34 lbs (15.42 kg)	66.5 lbs (30.15 kg)	90.75 lbs (41.2 kg)	118 lbs (53.5 kg)
Environment				
AC Power Supply	100–240V AC, 50–60 Hz	100-127V~/10A, 200-240V~/5A	100-240 VAC, 50-60 Hz	2000W AC****
Power Consumption (Average / Maximum)	192.5W / 275 W	385 W / 500 W	629.5 W / 677.3W	850 W / 1423.4W
Heat Dissipation	920 BTU/h	1350 BTU/h	2345.07 BTU/h	4858 BTU/h
Operating Temperature	50–95°F (10 – 35°C)	32 - 104°F (0 - 40°C)	41–95°F (5–35°C)	50–95°F (10 – 35°C)
Storage Temperature	-40–140°F (-40–60°C)	-4 - 167°F (-20 - 75°C)	-40–140°F (-40–60°C)	-40–158°F (-40–70°C)
Humidity	8 to 90% non-condensing	5% to 95% (non-condensing)	8% to 90% (non-condensing)	8% to 90% (non-condensing)
Operating Altitude	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 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	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.

ORDER 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-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 3,000 GB/ day of logs.
	FAZ-3500G	Centralized log and analysis appliance — 2 x GbE RJ45, 2 x SFP28, 96 TB storage, dual power supplies, up to 5,000 GB/ day of logs.
	FAZ-3700G	Centralized log & 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	Central Logging and Analytics subscription for 5 GB/ day logs. Include 24×7 FortiCare support, IOC, SOC Subscription , and FortiGuard Outbreak Detection service.
	FC2-10-AZVMS-465-01-DD	Central Logging and Analytics subscription for 50 GB/ day logs. Include 24×7 FortiCare support, IOC, SOC Subscription , and FortiGuard Outbreak Detection service.
	FC3-10-AZVMS-465-01-DD	Central Logging and Analytics subscription for 500 GB/ day logs. Include 24×7 FortiCare support, IOC, SOC Subscription , and FortiGuard Outbreak Detection service.
FortiAnalyzer-VM	FAZ-VM-GB1	Upgrade license for adding 1 GB/ day of logs and 500 GB storage capacity.
	FAZ-VM-GB5	Upgrade license for adding 5 GB/ day of logs and 3 TB storage capacity.
	FAZ-VM-GB25	Upgrade license for adding 25 GB/ day of logs and 10 TB storage capacity.
	FAZ-VM-GB100	Upgrade license for adding 100 GB/ day of logs and 24 TB storage capacity.
	FAZ-VM-GB500	Upgrade license for adding 500 GB/ day of logs and 48 TB storage capacity.
	FAZ-VM-GB2000	Upgrade license for adding 2 TB/Day of Logs and 100 TB storage capacity.
FortiAnalyzer Cloud Storage Subscription	FC1-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 5 GB/ day for Central Logging & Analytics and FortiCloud SOCaaS. Include 24×7 FortiCare support, IOC and SOC subscription.
	FC2-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 50 GB/ day for Central Logging & Analytics and FortiCloud SOCaaS. Include 24×7 FortiCare support, IOC and SOC subscription.
	FC3-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 500 GB/ day for Central Logging & Analytics and FortiCloud SOCaaS. Include 24×7 FortiCare support, IOC and SOC subscription.
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*	FC-10-[FortiGate Model Code]-464-02-DD	FortiAnalyzer Cloud SOCaaS: Cloud-based Log Monitoring (PaaS), including IOC Service and FortiCloud SOCaaS.
	FC-10-[FortiGate VM Model Code]-464-02-DD	FortiAnalyzer Cloud with SOCaaS: Cloud-based Log Monitoring (PaaS), including IOC Service and FortiCloud SOCaaS.
FortiGuard Indicator of Compromise (IOC) Subscription	FC-10-[Model Code]-149-02-DD	One year subscription license for the FortiGuard Indicator of Compromise (IOC).
FortiAnalyzer SOC Subscription	FC-10-[Model Code]-335-02-DD	Subscription license for the FortiAnalyzer SOC component.
FortiAnalyzer-VM SOC Subscription Service	FC[GB Day Code]-10-LV0VM-335-02-DD	Subscription license for FortiAnalyzer-VM SOC service.
FortiGuard Outbreak Detection Service	FC-10-[Model Code]-462-02-DD	Subscription license for FortiGuard Outbreak Detection Service.
FortiAnalyzer-VM Perpetual Outbreak Detection Service	FC[GB Day Code]-10-LV0VM-462-02-DD	Subscription license for FortiAnalyzer VM Perpetual FortiGuard Outbreak Detection Service.
Enterprise Protection Bundle	FC-10-[Model Code]-466-02-DD	Enterprise Protection (24×7 FortiCare plus Indicators of Compromise Service and SOC Subscription license).
Hardware Bundle	FAZ-[Hardware Model]-BDL-466-DD	Hardware plus 24×7 FortiCare and FortiAnalyzer Enterprise Protection.

* Requires FortiCloud Premium Account license. See FortiGate services for SOCaaS and other Cloud bundles.

www.fortinet.com