DATA SHEET

FortiAnalyzer

Security-Driven Analytics and Log Management

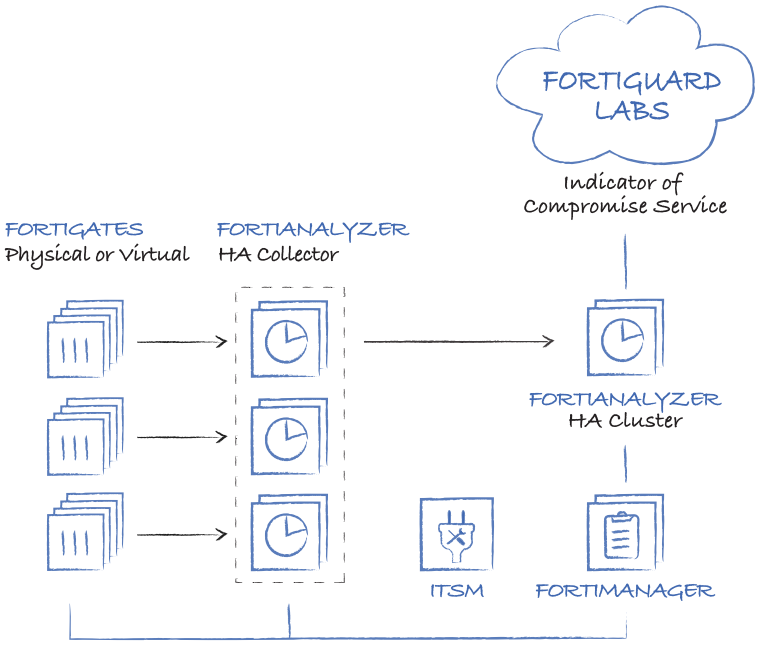
FortiAnalyzer provides deep insights into advanced threats through **Single-Pane Orchestration, Automation, and Response** for your entire attack surface to reduce risks and improve your organization's overall security.

Integrated with **Fortinet's Security Fabric**, FortiAnalyzer simplifies the complexity of analyzing and monitoring new and emerging technologies that have expanded the attack surface, and delivers **end-to-end visibility**, helping you identify and eliminate threats.

Advanced Threat Detection and Correlation allows security and network teams to immediately identify and respond to network security threats across the infrastructure.

Automated Workflows and Compliance Reporting provides customizable dashboards, reports, and advanced workflow handlers for both security and network teams to accelerate workflows and assist with regulation and compliance audits.

Scalable Log Management collects logs from FortiGate, FortiClient, FortiManager, FortiSandbox, FortiMail, FortiWeb, FortiAuthenticator, Generic syslog, and others. Deploy as an individual unit or optimize for a specific operation, and scale storage based on retention requirements.



Key Features

Security Fabric Analytics

- Event correlation across all logs and real-time anomaly detection, with Indicator of Compromise (IOC) service and threat detection, reducing time-to-detect

Fortinet Security Fabric integration

- Correlates with logs from FortiClient, FortiSandbox, FortiWeb, and FortiMail for deeper visibility and critical network insights

Enterprise-grade High Availability

- Automatically back-up FortiAnalyzer databases (up to four node cluster) that can be geographically dispersed for disaster recovery

Security Automation

- Reduce complexity and leverage automation via REST API, scripts, connectors, and automation stitches to expedite security response

Multi-Tenancy and Administrative Domains (ADOMs)

- Separate customer data and manage domains leveraging ADOMs to be compliant and operationally effective

Flexible Deployment Options and Archival Storage

- Supports deployment of appliance, VM, hosted, or cloud. Use AWS, Azure, or Google to archive logs as a secondary storage

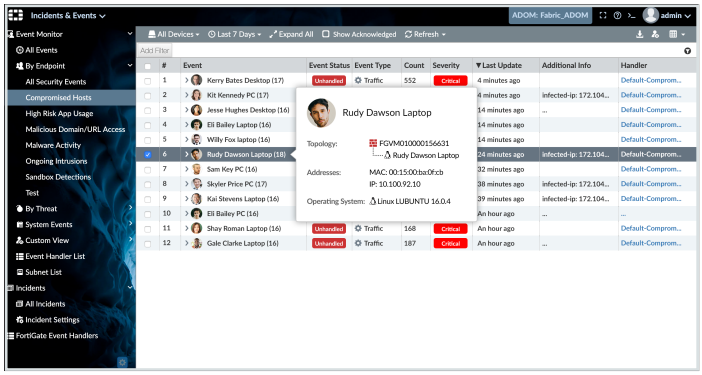
Feature Highlights

Security Operations Center

FortiAnalyzer's Security Operations Center (SOC) helps security teams protect networks with real-time log and threat data in the form of actionable views, notifications, and reports. Analysts can protect network, web sites, applications, databases, data centers, and other technologies through centralized monitoring, awareness of threats, events, and network activity. The predefined and custom dashboards provide a single-pane-of-glass for easy integration into your Security Fabric. The new FortiSOC service subscription provides built-in incident management workflows with playbooks and connectors to simplify the security analysts' role with enhanced security automation and orchestration.

Incident Detection and Response

FortiAnalyzer's automated incident response capability enables security teams to manage incident life cycle from a single view. Analysts can focus on event management and identification of compromised endpoints through default and customized event handlers with quick detection, automated correlation, and connected remediation of Fortinet devices and syslog servers with incident management and playbooks for quick assignment of incidents for analysis. Track timelines and artifacts with audit history and incident reports, as well as streamline integration with ITSM platforms that help bridge gaps in your Security Operations Center and reinforces your security posture.

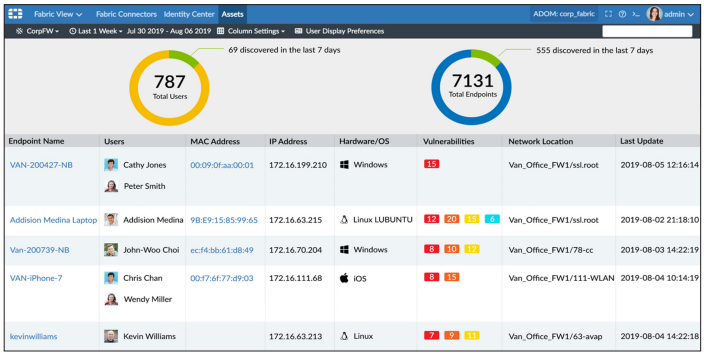


FortiAnalyzer Playbooks

FortiAnalyzer Playbooks boost security team abilities to simplify efforts and focus on critical tasks. Out-of-the-box playbook templates enable SOC analysts to quickly customize and automate their investigation use cases to respond to compromised hosts, critical intrusions, blocking C&C IPs, and more. Flexible playbook editor for hosts under investigation. FortiAnalyzer also allows analysts to drill down to a playbook and review task execution details and edit playbooks to define custom processes and tasks. FortiAnalyzer includes built-in connectors for playbooks to interact with other Security Fabric devices like FortiOS and EMS.

Indicators of Compromise

The Indicators of Compromise (IOC) service identifies suspicious usage and artifacts observed on a network or in an operations system that are determined with high confidence to be a computer intrusion. FortiGuard's IOC subscription provides intelligence information to help security analysts identify risky devices and users based on these artifacts. The IOC package consists of around 500K IOCs daily and delivers it via our Fortinet Developers Network (FNDN) to our FortiSIEM, FortiAnalyzer, and FortiCloud products. Analysts can also re-scan historical logs for threat hunting and identify threats based on new intelligence, as well as review users' aggregated threat scores by IP addresses, hostname, group, OS, overall threat rating, a location Map View, and a number of threats.



Asset and Identity

Security Fabric assets and identity monitoring and vulnerability tracking provides full SOC visibility and analytics of the attack surface. Assets and identity visibility and assets classification based on telemetry from NAC. Built-in SIEM module for automated log collection, normalization, and correlation. Integrated with FortiSOAR for further incident investigation and threat eradication. Support export of incident data to FortiSOAR through the FortiAnalyzer Connector and API Admin.

Reports

FortiAnalyzer provides 39+ built-in templates that are ready to use with sample reports to help identify the right report for you. You can generate custom data reports from logs by using the Reports feature. Run reports on-demand or on a schedule with automated email notifications, uploads, and an easy to manage calendar view. Create custom reports with the 700+ built-in charts and datasets that are ready with flexible formats including PDF, HTML, CSV, and XML.

Feature Highlights

SD-WAN Monitoring

SD-WAN dashboards enable customers to instantly see the benefit of applying SD-WAN across multiple WAN interfaces with event handlers to detect SD-WAN alerts for real-time notification and action. History graphs for WAN link health monitoring: Jitter, Latency, Packet Loss, Critical- and High- severity SD-WAN alerts. New Secure SD-WAN report provides an executive summary of important SD-WAN metrics, detailed charts and history graphs for SD-WAN link utilization by applications, latency, Packet Loss, Jitter changes, and SD-WAN performance statistics.

Log Forwarding for Third-Party Integration

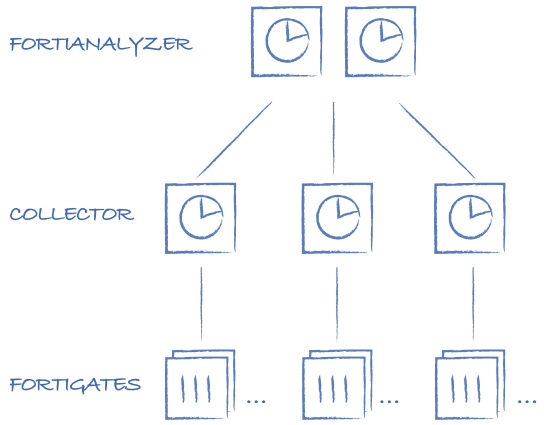
You can forward logs from a FortiAnalyzer unit to another FortiAnalyzer unit, a syslog server, or (CEF) server. The client FortiAnalyzer forwards logs to the server FortiAnalyzer unit, syslog server, or CEF server. In addition to forwarding logs to another unit or server, the client retains a local copy of the logs that are subject to the data policy settings for archived logs. Logs are forwarded in real-time or near real-time as they are received.

Multi-Tenancy with Flexible Quota Management

Time-based archive / analytic log data policy per Administrative Domain (ADOM), automated quota management based on the defined policy, and trending graphs to guide policy configuration and usage monitoring.

Analyzer Collector Mode

You can deploy in Analyzer mode and Collector mode on different FortiAnalyzer units and make the units work together to improve the overall performance of log receiving, analyses, and reporting. When FortiAnalyzer is in Collector mode, its primary task is forwarding logs of the connected devices to an Analyzer and archiving the logs. The Analyzer off-loads the log-receiving task to the Collector so that the Analyzer can focus on data analysis and report generation. This feature maximizes the Collector's log receiving performance.



Virtual Machines

FortiAnalyzer-VM-S

The new FortiAnalyzer subscription license model consolidates the VM product SKU and the FortiCare Support SKU, as well as IOC and FortiAnalyzer SOC (SOAR/SIEM) services into one single SKU to simplify the product purchase, upgrade, and renewal.

The FortiAnalyzer S-Series SKUs come in stackable 5, 50, and 500 GB/day logs licenses so that multiple units of this SKU can be purchased at a time to increase the number of GB/day logs. This SKU can also be purchased together with other FAZ VM-S SKUs to expand the total number of GB/day logs.

FortiAnalyzer-VM

FortiAnalyzer-VM integrates network logging, analyses, and reporting into a single system, delivering increased knowledge of security events throughout a network. Using virtualization technology, FortiAnalyzer-VM is a software-based version of the FortiAnalyzer hardware appliance and is designed to run on many virtualization platforms. It offers all the features of the FortiAnalyzer hardware appliance.

FortiAnalyzer-VM provides organizations with centralized security event analyses, forensic research, reporting, content archiving, data mining, malicious file quarantining, and vulnerability assessment. Centralized collection, correlation, and analyses of geographically and chronologically diverse security data from Fortinet and third party devices deliver a simplified, consolidated view of your security posture.

FortiAnalyzer Cloud

Fortinet also offers cloud-based analytics and reporting service to enable customers who want to leverage Fortinet managed FortiAnalyzer infrastructure. Customers and partners can easily access their FortiAnalyzer Cloud from their FortiCloud Single-Sign-On Portal.

Specifications

FORTIANALYZER VIRTUAL APPLIANCES	FAZ-VM-BASE	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100	FAZ-VM-GB500	FAZ-VM-GB2000
Capacity and Performance							
GB/Day of Logs	1 incl.*	+1	+5	+25	+100	+500	+2,000
Storage Capacity	500 GB	+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	10,000
Options							
FortiGuard Indicator of Compromise (IOC)				✓			
SOC Subscription				✓			
Hypervisor Requirements							
Hypervisor Support	VMware ESX/ESXi 5.5/6.0/6.5/6.7/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+ and Open Source Xen 4.1+, KVM on Redhat 6.5+ and Ubuntu 17.04, Nutanix AHV (AOS 5.10.5), Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI), Alibaba Cloud (AliCloud)						
Network Interface Support (Minimum / Maximum)	1 / 4						
vCPUs (Minimum / Maximum)	4 / Unlimited						
Memory Support (Minimum / Maximum)	8 GB / Unlimited						

* Unlimited GB/Day when deployed in collector mode

FORTIANALYZER APPLIANCES	FORTIANALYZER 150G	FORTIANALYZER 300G	FORTIANALYZER 800F
Capacity and Performance			
GB/Day of Logs	25	100	300
Analytic Sustained Rate (logs/sec)*	500	2,000	8,250
Collector Sustained Rate (logs/sec)*	750	3,000	12,000
Devices/VDOMs (Maximum)	50	180	800
Max Number of Days Analytics**	38	28	30
Options			
FortiGuard Indicator of Compromise (IOC)	✓	✓	✓
SOC Subscription	–	✓	✓
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 GE, 2 x SFP
Storage Capacity	4TB (2x 2TB)	8 TB (2 x 4 TB)	16 TB (4 x 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	No	Optional
Dimensions			
Height x Width x Length (inches)	9.5 x 3.5 x 8	1.73 x 17.24 x 16.38	1.75 x 17.44 x 22.16
Height x Width x Length (cm)	24.1 x 8.9 x 20.55	4.4 x 43.8 x 41.6	4.4 x 44.3 x 56.3
Weight	9.35 lbs (4.24 kg)	22.5 lbs (10.2 kg)	28.6 lbs (13.0 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	108W / 186 W
Heat Dissipation	147.4 BTU/h	337.8 BTU/h	634 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)	-31–158° F (-35–70° C)
Humidity	5 to 95% non-condensing	20 to 90% non-condensing	20 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)
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.
**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.

Specifications




FORTIANALYZER APPLIANCES	FORTIANALYZER 1000F	FORTIANALYZER 3000G	FORTIANALYZER 3500G	FORTIANALYZER 3700F
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	✓	✓	✓	✓
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 x 10GbE RJ45, 2 x 10GbE SFP+	2 x GE RJ45, 2x 25GE SFP28	2 x GbE RJ45, 2 x SFP28	2 x SFP+, 2 x 1GE
Storage Capacity	32 TB (8 x 4 TB)	64 TB (16 x 4TB)	96 TB (24 x 4 TB)	240 TB (60 x 4 TB SAS HDDs)
Usable Storage (After RAID)	24	56 TB	80	216 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	✓	✓	✓	✓***
Dimensions				
Height x Width x Length (inches)	3.5 x 17.2 x 25.6	5.2 x 17.2 x 25.5	7.0 x 17.2 x 26.0	7 x 17.2 x 30.2
Height x Width x Length (cm)	8.9 x 43.7 x 65.0	13.0 x 44.0 x 65.0	17.8 x 43.7 x 66.0	17.8 x 43.7 x 76.7
Weight	34 lbs (15.42 kg)	66.5 lbs (30.15 kg)	90.75 lbs (41.2 kg)	118 lbs (53.5Kg)
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	850W / 1423.4 W
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 7,000 ft (2133 m)
Compliance				
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, 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.
***3700F must connect to a 200V - 240V power source.

Order Information

Product	SKU	Description
FortiAnalyzer 150G	FAZ-150G	Centralized log and analysis appliance — 2 x RJ45 GE, 4 TB storage, up to 25 GB/day of logs.
FortiAnalyzer 300G	FAZ-300G	Centralized log and analysis appliance — 4 x RJ45 GE, 8 TB storage, up to 100 GB/day of logs.
FortiAnalyzer 800F	FAZ-800F	Centralized log and analysis appliance — 4 x GE, 2 x SFP, 16 TB storage, up to 300 GB/day of logs.
FortiAnalyzer 1000F	FAZ-1000F	Centralized log and analysis appliance — 2 x 10GE RJ45, 2 x 10GbE SFP+, 32 TB storage, dual power supplies, up to 660 GB/day of logs.
FortiAnalyzer 3000G	FAZ-3000G	Centralized log and analysis appliance — 2 x GE RJ45, 2x 25GE SFP28, 64 TB storage, dual power supplies, up to 3,000 GB/day of logs.
FortiAnalyzer 3500G	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.
FortiAnalyzer 3700F	FAZ-3700F	Centralized log and analysis appliance — 2 x SFP+, 2 x 1GE slots, 240 TB storage, up to 8,300 GB/day of logs.
FortiAnalyzer-VM Subscription License with Support	FC1-10-AZVMS-431-01-DD	Central Logging and Analytics subscription for 5 GB/day logs. Include 24x7 FortiCare support, IOC, SOC Subscription.
	FC2-10-AZVMS-431-01-DD	Central Logging and Analytics subscription for 50 GB/day logs. Include 24x7 FortiCare support, IOC, SOC Subscription.
	FC3-10-AZVMS-431-01-DD	Central Logging and Analytics subscription for 500 GB/day logs. Include 24x7 FortiCare support, IOC, SOC Subscription.
FortiAnalyzer-VM	FAZ-VM-BASE	Base license for stackable FortiAnalyzer-VM; 1 GB/day of logs and 500 GB storage capacity. Unlimited GB/day when used in collector mode only. Designed for all supported platforms.
	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	FC-10-[FortiGate Model Code]-188-02-DD	FortiAnalyzer Cloud: Cloud-based Events and Security Log Monitoring including IOC Service [1].
	FC-10-[FortiGate Model Code]-816-02-DD	360 Protection (SD-WAN Cloud Monitoring, FMG/FAZ Cloud, IPS, AMP, App Ctrl, Web Filtering, AS, Security Rating, Industrial Security, FortiConverter Svc, and ASE FortiCare)[1].
	FC-10-[FortiGate VM Model Code]-819-02-DD	360 Protection (SD-WAN Cloud Monitoring, FMG/FAZ Cloud, IPS, AMP, App Ctrl, Web Filtering, AS, Security Rating, Industrial Security, FortiConverter Svc, and ASE FortiCare)[1].
	FC-10- [FortiGate Model Code]-208-02-DD	Premium subscription for Cloud-based Central Logging and Analytics. Supports all FortiGate log types with IOC service, SOC subscription and 24x7 FortiCare support included [2].
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.
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.
Enterprise Protection Bundle	FC-10-[Model Code]-432-02-DD	Enterprise Protection (24x7 FortiCare plus Indicators of Compromise Service and SOC Subscription license).
Hardware Bundle	FAZ-[Hardware Model]-BDL-432-DD	Hardware plus 24x7 FortiCare and FortiAnalyzer Enterprise Protection.

[1] Requires FortiCloud Premium Account license.
[2] Requires FortiCloud Premium Account license. This is not included as part of 360 Protection Bundle.