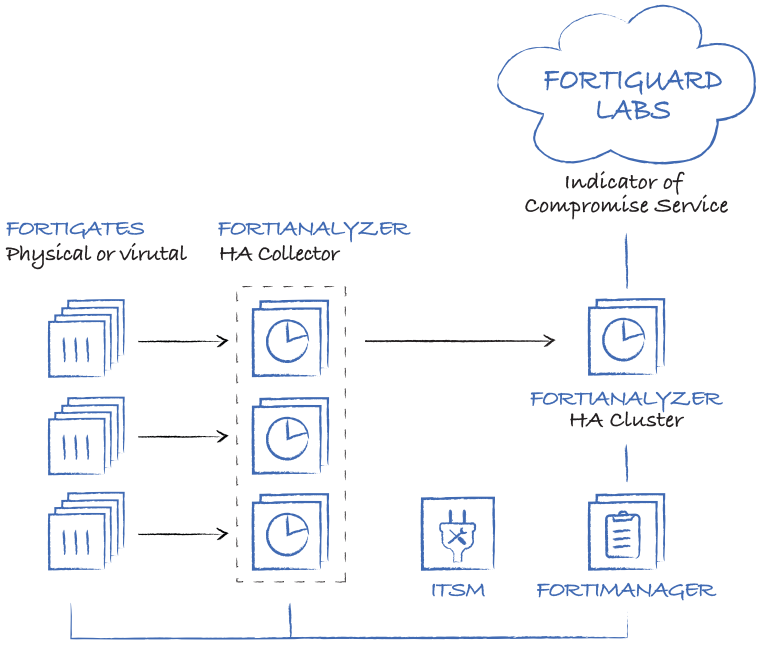
DATA SHEET

# FortiAnalyzer

Security-Driven Analytics & Log Management

FortiAnalyzer provides deep insights into advanced threats through **Single-Pane Orchestration, Automation & 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 & Correlation** allows Security & Network teams to immediately identify and respond to network security threats across the infrastructure.

**Automated Workflows & Compliance Reporting** provides customizable dashboards, reports and advanced workflow handlers for both Security & Network teams to accelerate workflows & 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 optimized for a specific operation and scale storage based on retention requirements.

## Key Features

**End-to-end visibility**

- Event correlation, threat detection and Indicator of Compromise (IOC) service reduce time-to-detect and identity threats

**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 DB's (up to 4 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 & archival storage**

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

# Feature Highlights

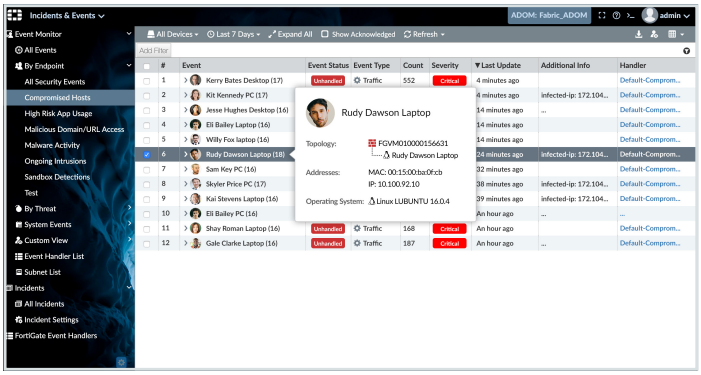
## Security Operations Center (SOC)

FortiAnalyzers SOC management center helps secure your overall network by providing actionable views of log and threat data. Protect your network, web sites, applications, databases, servers and data centers, and other technologies, with centralized monitoring, awareness of the threats, events and network activity, using predefined and customized dashboards delivered through a single-pane-of-glass interface for easy integration into your Security Fabric.

## Incident Detection & Response

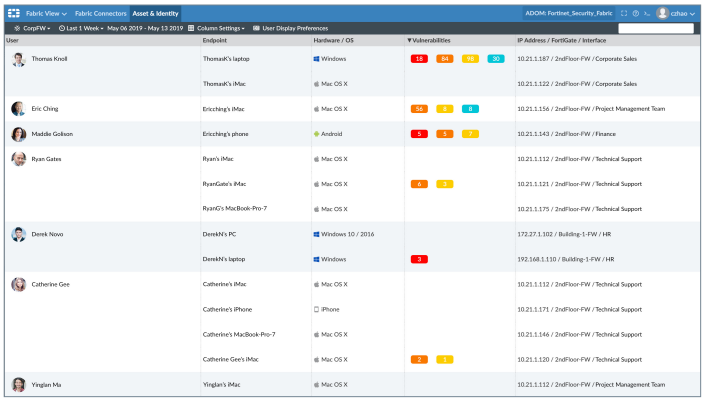
FortiAnalyzer's Automated Incident Response capability improves Management & Analytics with focus on event management and identification of compromised endpoints. Improved default and custom event handlers can be used to detect malicious and suspicious activities on the spot. Integration of events with the FOS automation framework for automated actions such as endpoint quarantine or blacklist IPs. Incident detection and tracking, as well as evidence collection and analysis are streamlined through integration with ITSM platforms, helping to bridge gaps in your Security Operations Center and reinforce your Security Posture.

Event handlers enable quick detection, automated correlation and connected remediation with incident management to simplify log analysis and threat identification across your Fortinet Security Fabric. Create event handlers for FortiGate, FortiCarrier, FortiCache, FortiMail, FortiManager, FortiWeb, FortiSandbox devices, and syslog servers. Define what messages to extract from logs and display in events and send alerts for event handlers via email address, webhook, SNMP community, or syslog server.




## Indicators of Compromise

The Indicators of Compromise (IOC) summary shows end users with suspicious web usage compromises. It provides information such as end users' IP addresses, host name, group, OS, overall threat rating, a Map View, and number of threats and you can drill down to view threat details. Analysts can re-scan historical logs for threat hunting, and identify threats based on new intelligence. To generate the Indicators of Compromise, FortiAnalyzer checks web filter, DNS and traffic logs of each end user against its threat database. When a threat match is found, a threat score is given to the end user. FortiAnalyzer aggregates the threat scores of an end user and gives its verdict of the end user's overall Indicators of Compromise. The Indicators of Compromise summary is produced through logs from the FortiGate devices and FortiAnalyzer subscription to FortiGuard to keep its local threat database synced with the FortiGuard threat database.




## 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 300+ built-in charts and datasets ready for creating your own custom reports, with flexible report formats include PDF, HTML, CSV and XML.

# Feature Highlights

### Log Forwarding for Third-Party Integration

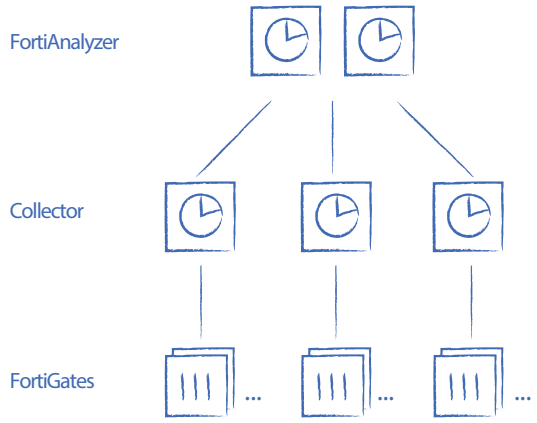
You can forward logs from a FortiAnalyzer unit to another FortiAnalyzer unit, a syslog server, or a Common Event Format (CEF) server. The client is the FortiAnalyzer unit that forwards logs to another device. The server is the FortiAnalyzer unit, syslog server, or CEF server that receives the logs. In addition to forwarding logs to another unit or server, the client retains a local copy of the logs. The local copy of the logs is subject to the data policy settings for archived logs. Logs are forwarded in real-time or near real-time as they are received. Forwarded content files include: DLP files, antivirus quarantine files, and IPS packet captures.

### 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, analysis, 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 offloads the log receiving task to the Collector so that the Analyzer can focus on data analysis and report generation. This maximizes the Collector's log receiving performance. (Figure 4)

### 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.




## FortiAnalyzer-VM

FortiAnalyzer-VM integrates network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout a network. Utilizing 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 of any size 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 appliances and third-party devices deliver a simplified, consolidated view of your security posture.

# 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 |
| FortiGuard Indicator of Compromise (IOC) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Hypervisor Requirements** | | | | | | | |
| Hypervisor Support | VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/6.7, 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) | 2 / Unlimited | | | | | | |
| Memory Support (Minimum / Maximum) | 4 GB / Unlimited | | | | | | |

* Unlimited GB/Day when deployed in collector mode

# Specifications



| | FORTIANALYZER 200F | FORTIANALYZER 300F | FORTIANALYZER 400E |
|---|---|---|---|
| **Capacity and Performance** | | | |
| GB/Day of Logs | 100 | 150 | 200 |
| Analytic Sustained Rate (logs/sec)* | 3000 | 4500 | 6,000 |
| Collector Sustained Rate (logs/sec)* | 4500 | 6,750 | 9,000 |
| Devices/VDOMs (Maximum) | 150 | 180 | 200 |
| Max Number of Days Analytics** | 40 | 28 | 30 |
| **Options Supported** | | | |
| FortiGuard Indicator of Compromise (IOC) | ✓ | ✓ | ✓ |
| **Hardware Specifications** | | | |
| Form Factor | 1 RU Rackmount | 1 RU Rackmount | 1 RU Rackmount |
| Total Interfaces | 2 x RJ45 GE | 2 x RJ45 GE, 2 x SFP | 4 x GE |
| Storage Capacity | 4 TB (1 x 4 TB) | 8 TB (2 x 4 TB) | 12 TB (4 x 3 TB) |
| Usable Storage (After RAID) | 4 TB | 4 TB | 6 TB |
| Removable Hard Drives | No | No | ✓ |
| RAID Levels Supported | N/A | RAID 0/1 | RAID 0/1/5/10 |
| RAID Type | N/A | Software | Software |
| Default RAID Level | N/A | 1 | 10 |
| Redundant Hot Swap Power Supplies | No | No | No |
| **Dimensions** | | | |
| Height x Width x Length (inches) | 1.75 x 17.0 x 15.0 | 1.75 x 17.0 x 15.0 | 1.7 x 17.2 x 19.8 |
| Height x Width x Length (cm) | 4.4 x 43.2 x 38.1 | 4.4 x 43.2 x 38.0 | 4.3 x 43.7 x 50.3 |
| Weight | 17.1 lbs (7.8 kg) | 18.9 lbs (8.6 kg) | 31 lbs (14.1 kg) |
| **Environment** | | | |
| AC Power Supply | 100–240V AC, 60–50 Hz | 100–240V AC, 60–50 Hz | 100–240V AC, 60–50 Hz |
| Power Consumption (Average / Maximum) | 49W / 114W | 65W / 130W | 93W / 133W |
| Heat Dissipation | 390 BTU/h | 445 BTU/h | 456 BTU/h |
| Operating Temperature | 32–104° F (0–40° C) | 32–104° F (0–40° C) | 41–95°F (5–35°C) |
| Storage Temperature | 95–158° F (-35–70° C) | 95–158° F (-35–70° C) | -40–140°F (-40–60°C) |
| Humidity | 20 to 90% non-condensing | 20 to 90% non-condensing | 8– 90% non-condensing |
| Operating Altitude | Up to 7,400 ft (2,250 m) | Up to 7,400 ft (2,250 m) | Up to 9,842 ft (3,000 m) |
| **Compliance** | | | |
| Safety Certifications | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB | FCC Part 15 Class A, C-Tick, 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.

# Specifications



| | FORTIANALYZER 800F | FORTIANALYZER 1000E | FORTIANALYZER 2000E |
|---|---|---|---|
| **Capacity and Performance** | | | |
| GB/Day of Logs | 300 | 600 | 1,000 |
| Analytic Sustained Rate (logs/sec)* | 8,250 | 18,000 | 30,000 |
| Collector Sustained Rate (logs/sec)* | 12,000 | 27,000 | 45,000 |
| Devices/VDOMs (Maximum) | 800 | 2,000 | 2,000 |
| Max Number of Days Analytics** | 30 | 30 | 30 |
| **Options Supported** | | | |
| FortiGuard Indicator of Compromise (IOC) | ✓ | ✓ | ✓ |
| **Hardware Specifications** | | | |
| Form Factor | 1 RU Rackmount | 2 RU Rackmount | 2 RU Rackmount |
| Total Interfaces | 4 x GE, 2 x SFP | 2 x GE | 4 x GE, 2 x SFP+ |
| Storage Capacity | 16 TB (4 x 4 TB) | 24 TB (8 x 3 TB) | 36 TB (12 x 3 TB) |
| Usable Storage (After RAID) | 8 TB | 18 TB | 30 TB |
| Removable Hard Drives | ✓ | ✓ | ✓ |
| RAID Levels Supported | RAID 0/1/5/10 | RAID 0/1/5/6/10/50/60 | RAID 0/1/5/6/10/50/60 |
| RAID Type | Hardware / Hot Swappable | Hardware / Hot Swappable | Hardware / Hot Swappable |
| Default RAID Level | 10 | 50 | 50 |
| Redundant Hot Swap Power Supplies | No | ✓ | ✓ |
| **Dimensions** | | | |
| Height x Width x Length (inches) | 1.75 x 17.44 x 22.16 | 3.5 x 17.2 x 25.2 | 3.5 x 17.2 x 25.6 |
| Height x Width x Length (cm) | 4.4 x 44.3 x 56.3 | 8.9 x 43.7 x 68.4 | 8.9 x 43.7 x 64.8 |
| Weight | 28.6 lbs (13.0 kg) | 52 lbs (23.6 kg) | 58 lbs (26.3 kg) |
| **Environment** | | | |
| AC Power Supply | 100–240V AC, 60–50 Hz | 100–240V AC, 60–50 Hz | 100–240V AC, 60–50 Hz |
| Power Consumption (Average / Maximum) | 108W / 186W | 192.5W / 275W | 293.8W / 354W |
| Heat Dissipation | 634 BTU/h | 920 BTU/h | 1840 BTU/h |
| Operating Temperature | 32–104° F (0–40° C) | 41–95°F (5–35°C) | 50–95°F (10–35°C) |
| Storage Temperature | 95–158° F (-35–70° C) | -40–140°F (-40–60°C) | -40–158°F (-40–70°C) |
| Humidity | 20 to 90% non-condensing | 8–90% non-condensing | 8–90% 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, C-Tick, VCCI, CE, UL/cUL, CB | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB | FCC Part 15 Class A, C-Tick, 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.

# Specifications



| | FORTIANALYZER 3000F | FORTIANALYZER 3500G | FORTIANALYZER 3700F |
|---|---|---|---|
| **Capacity and Performance** | | | |
| GB/Day of Logs | 3,000 | 5,000 | 8,300 |
| 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) | 4,000 | 10,000 | 10,000 |
| Max Number of Days Analytics** | 30 | 38 | 60 |
| **Options Supported** | | | |
| FortiGuard Indicator of Compromise (IOC) | ✓ | ✓ | ✓ |
| **Hardware Specifications** | | | |
| Form Factor | 3 RU Rackmount | 4 RU Rackmount | 4 RU Rackmount |
| Total Interfaces | 4 x GE, 2 x SFP+ | 2 x GbE RJ45, 2x SFP28 | 2 x SFP+, 2 x 1GE |
| Storage Capacity | 48 TB (16 x 3 TB – 48 TB max) | 96 TB (24x 4 TB) | 240 TB (60 x 4 TB SAS HDDs) |
| Usable Storage (After RAID) | 42 TB | 80 | 216 TB |
| Removable Hard Drives | ✓ | ✓ | ✓ |
| RAID Levels Supported | RAID 0/1/5/6/10/50/60 | RAID 0/1/5/6/10/50/60 | RAID 0/1/5/6/10/50/60 |
| RAID Type | Hardware / Hot Swappable | Hardware / Hot Swappable | Hardware / Hot Swappable |
| Default RAID Level | 50 | 50 | 50 |
| Redundant Hot Swap Power Supplies | ✓ | ✓ | ✓*** |
| **Dimensions** | | | |
| Height x Width x Length (inches) | 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) | 13.2 x 43.7 x 64.8 | 17.8 x 43.7 x 66.0 | 17.8 x 43.7 x 76.7 |
| Weight | 76 lbs (34.5 kg) | 90.75 lbs (41.2 kg) | 118 lbs (53.5Kg) |
| **Environment** | | | |
| AC Power Supply | 100–240V AC, 50–60 Hz, 11.5 Amp Maximum | 100-240 VAC, 60-50 Hz | 100–240V AC, 60–50 Hz |
| Power Consumption (Average / Maximum) | 449 W / 541W for 12 HDD | 629.5W / 677.3W | 850 W / 1423.4W |
| Heat Dissipation | 1846.5 BTU/h | 2345.07 BTU/h | 4858 BTU/h |
| Operating Temperature | 50–95°F (10–35°C) | 41–95°F (5–35°C) | 50–95°F (10–35°C) |
| Storage Temperature | -40–158°F (-40–70°C) | -40–140°F (-40–60°C) | -40–158°F (-40–70°C) |
| Humidity | 8–90% 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 7,000 ft (2133 m) |
| **Compliance** | | | |
| Safety Certifications | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB | FCC Part 15 Class A, C-Tick, 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.
*** 3700F must connect to a 200V - 240V power source.

# Order Information

| Product | SKU | Description |
|---|---|---|
| FortiAnalyzer 200F | FAZ-200F | Centralized log and analysis appliance — 2 x RJ45 GE, 4 TB storage, up to 100 GB/day of logs. |
| FortiAnalyzer 300F | FAZ-300F | Centralized log and analysis appliance — 2 x RJ45 GE, 8 TB storage, up to 150 GB/day of logs. |
| FortiAnalyzer 400E | FAZ-400E | Centralized log and analysis appliance — 4 x GE RJ45, 12 TB storage, up to 200 GB/day of logs. |
| FortiAnalyzer 800F | FAZ-800F | Centralized log and analysis appliance — 4 x GE, 2x SFP, 16 TB storage, up to 300 GB/day of logs. |
| FortiAnalyzer 1000E | FAZ-1000E | Centralized log and analysis appliance — 2 x GE RJ45, 24 TB storage, dual power supplies, up to 650 GB/day of logs. |
| FortiAnalyzer 2000E | FAZ-2000E | Centralized log and analysis appliance — 4 x GE RJ45, 2 x SFP+, 36 TB storage, dual power supplies, up to 1,000 GB/day of logs. |
| FortiAnalyzer 3000F | FAZ-3000F | Centralized log and analysis appliance — 4 x GE RJ45, 2 x SFP+, 48 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, 2x 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 | 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 - 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 | 1 Year Subscription license for the FortiGuard Indicator of Compromise (IOC). |