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**

### 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 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)
FortiAnalyzer’s SOC (Security Operations Center) helps security teams protect networks with real-time log and threat data in the form of actionable views, notifications and reports. Analysts can protect networks, 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 & 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 streamlined integration with ITSM platforms helps bridge gaps in your Security Operations Center and reinforces your Security Posture.

Indicators of Compromise
The Indicators of Compromise (IOC) service identifies suspicious usage and artifacts observed on a network or in an operations system, 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 consisting 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 & Identity
Security Fabric assets and identity monitoring and vulnerability tracking provides full SOC visibility and analytics of the attack surface. Assets & Identity visibility and assets classification based on telemetry from NAC. Built-in SIEM module for automated log collection, normalization & 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 ready for creating your custom reports, with flexible report formats include 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 & action. History graphs for WAN link health monitoring: Jitter, Latency and Packet Loss Critical & 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, 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.

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 off-loads 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.

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.

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, 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 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.

FortiAnalyzer Cloud
Fortinet also offers cloud-based analytics and reporting service to enable customers that 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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity and Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GB/Day of Logs</td>
<td>1 incl.*</td>
<td>+1</td>
<td>+5</td>
<td>+25</td>
<td>+100</td>
<td>+500</td>
</tr>
<tr>
<td>Storage Capacity</td>
<td>500 GB</td>
<td>+500 GB</td>
<td>+3 TB</td>
<td>+10 TB</td>
<td>+24 TB</td>
<td>+48 TB</td>
</tr>
<tr>
<td>Devices/VDOMs (Maximum)</td>
<td>10,000</td>
<td>10,000</td>
<td>10,000</td>
<td>10,000</td>
<td>10,000</td>
<td>10,000</td>
</tr>
</tbody>
</table>

### Options

- FortGuard Indicator of Compromise (IOC)
- SOC Subscription
- Hypervisor Requirements
  - Hypervisor Support: VMware ESXi 5.5/6.0/6.5/7.0, 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 5.10.9), Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI), Alibaba Cloud (NCloud)

### Hardware Specifications

- Form Factor (supports EA/non-EA standards): Desktop
- Total Interfaces: 2 x RJ45 GE, 2 x SFP
- Storage Capacity: 4TB (2x 2TB)
- Removable Hard Drives: No
- RAID Levels Supported: 0,1
- RAID Type: Software
- Redundant Hot Swap Power Supplies: No
- Dimensions: Height x Width x Length (inches) 9.5 x 3.5 x 8
- Weight: 9.35 lbs (4.24 kg)

### Environment

- AC Power Supply: 100–240V AC, 50–60 Hz
- Power Consumption (Average / Maximum): 36W / 43W
- Heat Dissipation: 147.4 BTU/h
- Operating Temperature: 32–104° F (0–40° C)
- Storage Temperature: 95–168° F (35–70° C)
- Humidity: 5 to 95% non-condensing

### Compliance

- Safety Certifications: FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB
- UL/cUL, CB

* Unlimited GB/Day when deployed in collector mode

---

### FORTIANALYZER APPLIANCES

<table>
<thead>
<tr>
<th>FORTIANALYZER 150G</th>
<th>FORTIANALYZER 200F</th>
<th>FORTIANALYZER 300F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity and Performance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GB/Day of Logs</td>
<td>50</td>
<td>100</td>
</tr>
<tr>
<td>Analytic Sustained Rate (logs/sec)*</td>
<td>1500</td>
<td>3000</td>
</tr>
<tr>
<td>Collector Sustained Rate (logs/sec)*</td>
<td>3000</td>
<td>4500</td>
</tr>
<tr>
<td>Devices/VDOMs (Maximum)</td>
<td>50</td>
<td>150</td>
</tr>
<tr>
<td>Max Number of Days Analytics**</td>
<td>38</td>
<td>40</td>
</tr>
</tbody>
</table>

### Options

- FortGuard Indicator of Compromise (IOC)
- SOC Subscription
- Enterprise Bundle
- Hardware Bundle

### Hardware Specifications

- Form Factor (supports EA/non-EA standards): Desktop
- Total Interfaces: 2 x RJ45 GE
- Storage Capacity: 4 TB (1 x 4 TB)
- Removable Hard Drives: No
- RAID Levels Supported: 0,1
- RAID Type: Software
- Redundant Hot Swap Power Supplies: No
- Dimensions: Height x Width x Length (inches) 9.5 x 3.5 x 8
- Weight: 9.35 lbs (4.24 kg)

### Environment

- AC Power Supply: 100–240V AC, 50–60 Hz
- Power Consumption (Average / Maximum): 36W / 43W
- Heat Dissipation: 147.4 BTU/h
- Operating Temperature: 32–104° F (0–40° C)
- Storage Temperature: 95–168° F (35–70° C)
- Humidity: 5 to 95% non-condensing

### Compliance

- Safety Certifications: FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB
- 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

<table>
<thead>
<tr>
<th>FORTIANALYZER APPLIANCES</th>
<th>FORTIANALYZER 800F</th>
<th>FORTIANALYZER 1000F</th>
<th>FORTIANALYZER 2000E</th>
</tr>
</thead>
<tbody>
<tr>
<td>GB/Day of Logs</td>
<td>300</td>
<td>600</td>
<td>1,000</td>
</tr>
<tr>
<td>Analytic Sustained Rate (logs/sec)*</td>
<td>8,250</td>
<td>20,000</td>
<td>30,000</td>
</tr>
<tr>
<td>Collector Sustained Rate (logs/sec)*</td>
<td>12,000</td>
<td>40,000</td>
<td>45,000</td>
</tr>
<tr>
<td>Devices/VDOMs (Maximum)</td>
<td>800</td>
<td>2000</td>
<td>2000</td>
</tr>
<tr>
<td>Max Number of Days Analytics**</td>
<td>30</td>
<td>34</td>
<td>30</td>
</tr>
</tbody>
</table>

### Options
- FortiGuard Indicator of Compromise (IOC)
- SOC Subscription
- Enterprise Bundle

### Hardware Specifications
- Form Factor (supports EIA/non-EIA standards)
  - 1 RU Rackmount
  - 2 RU Rackmount
  - 2 RU Rackmount
- Total Interfaces
  - 4 x GE, 2 x SFP
  - 2 x 10GbE RJ45, 2 x 10GbE SFP+
  - 4 x GE, 2 x SFP+
- Storage Capacity
  - 16 TB (4 x 4 TB)
  - 32 TB (8 x 4 TB)
  - 36 TB (12 x 3 TB)
- Usable Storage (After RAID)
  - 8 TB
  - 24 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
- Redundant Hot Swap Power Supplies
  - Optional

### Dimensions
- Height x Width x Length (inches)
  - 1.75 x 17.44 x 22.16
  - 3.5 x 17.2 x 25.6
  - 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 65.0
  - 8.9 x 43.7 x 64.8
- Weight
  - 28.6 lbs (13.0 kg)
  - 34 lbs (15.42 kg)
  - 58 lbs (26.3 kg)

### Environment
- AC Power Supply
  - 100–240V AC, 50–60 Hz
  - 100–240V AC, 50–60 Hz
  - 100–240V AC, 50–60 Hz
- Power Consumption (Average / Maximum)
  - 106W / 195W
  - 192.5W / 275 W
  - 293.8W / 354 W
- Heat Dissipation
  - 634 BTU/h
  - 920 BTU/h
  - 1840 BTU/h
- Operating Temperature
  - 32–104°F (0–40°C)
  - 50–95°F (10–35°C)
  - 50–95°F (10–35°C)
- Storage Temperature
  - 95–158°F (–35–70°C)
  - 40–158°F (–40–70°C)
  - 40–158°F (–40–70°C)
- Humidity
  - 20 to 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 7,400 ft (2,250 m)

### Compliance
- Safety Certifications
  - FCC Part 15 Class A, ROM, VCCI, CE, UL/cUL, CB
  - FCC Part 15 Class A, ROM, VCCI, CE, UL/cUL, CB
  - FCC Part 15 Class A, ROM, 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

<table>
<thead>
<tr>
<th>FORTIANALYZER APPLIANCES</th>
<th>FORTIANALYZER 3000G</th>
<th>FORTIANALYZER 3500G</th>
<th>FORTIANALYZER 3700F</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Capacity and Performance</strong></td>
<td>3,000</td>
<td>5,000</td>
<td>8,300</td>
</tr>
<tr>
<td>GB/Day of Logs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analytic Sustained Rate (logs/sec)*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collector Sustained Rate (logs/sec)*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Devices/VDOMs (Maximum)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Max Number of Days Analytics</strong>**</td>
<td>30</td>
<td>50</td>
<td>60</td>
</tr>
</tbody>
</table>

## Options
- FortiGuard Indicator of Compromise (IOC)
- SOC Subscription
- Enterprise Bundle
- Hardware Bundle

## Hardware Specifications
- **Form Factor (supports EIA/non-EIA standards)**
  - 3 RU Rackmount
  - 4 RU Rackmount
  - 4 RU Rackmount
- **Total Interfaces**
  - 2 x GE RJ45, 2x 25GE SFP28
  - 2 x GE RJ45, 2 x SFP28
  - 2 x SFP+, 2 x 1GE
- **Storage Capacity**
  - 64 TB (16 x 4TB)
  - 96 TB (24 x 4 TB)
  - 240 TB (60 x 4 TB SAS HDDs)
- **Usable Storage (After RAID)**
  - 56 TB
  - 80
  - 160
- **Removable Hard Drives**
- **RAID Levels Supported**
  - 0/1/5/6/10/50/60
  - 0/1/5/6/10/50/60
  - 0/1/5/6/10/50/60
- **Default RAID Level**
  - 50
  - 50
  - 50
- **RAID Type**
  - Hardware / Hot Swappable
  - Hardware / Hot Swappable
  - Hardware / Hot Swappable
- **Redundant Hot Swap Power Supplies**
- **Dimensions**
  - **Height x Width x Length (inches)**
    - 5.2 x 12.7 x 25.5
    - 7.0 x 12.7 x 26.0
    - 7 x 12.7 x 30.2
  - **Height x Width x Length (cm)**
    - 13.0 x 44.0 x 65.0
    - 17.8 x 44.0 x 66.0
    - 17.8 x 43.7 x 76.7
- **Weight**
  - 66.5 lbs (30.15 kg)
  - 90.75 lbs (41.2 kg)
  - 118 lbs (53.5Kg)
- **Environment**
  - **AC Power Supply**
    - 100-127V~/10A, 200-240V~/5A
    - 100-240 VAC, 50-60 Hz
    - 2000W AC
  - **Power Consumption (Average / Maximum)**
    - 365 W / 600 W
    - 629.5 W / 877.3W
    - 850W / 1425.4 W
  - **Heat Dissipation**
    - 1020 BTU/h
    - 2345 BTU/h
    - 4858 BTU/h
  - **Operating Temperature**
    - 32 - 104°F (0 - 40°C)
    - 41°F - 55°C
    - 50 - 95°F (10 - 35°C)
  - **Storage Temperature**
    - -40°F - 140°F (-40 - 60°C)
    - 40 - 149°F (-40 - 60°C)
    - -40°F - 158°F (-40 - 70°C)
  - **Humidity**
    - 5% to 95% (non-condensing)
    - 7% 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, RCM, VCCI, CE, UL 61000-4, CB
  - FCC Part 15 Class A, RCM, VCCI, CE, UL 61000-4, CB
  - FCC Part 15 Class A, RCM, VCCI, CE, UL 61000-4, 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

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiAnalyzer 1500F</td>
<td>FAZ-1500F</td>
<td>Centralized log and analysis appliance — 2 x RJ45 GE, 4 TB storage, up to 50 GB/day of logs.</td>
</tr>
<tr>
<td>FortiAnalyzer 2000F</td>
<td>FAZ-2000F</td>
<td>Centralized log and analysis appliance — 2 x RJ45 GE, 4 TB storage, up to 100 GB/day of logs.</td>
</tr>
<tr>
<td>FortiAnalyzer 3000F</td>
<td>FAZ-3000F</td>
<td>Centralized log and analysis appliance — 4 x RJ45, 2 x 10GbE SFP+, 32 TB storage, dual power supplies, up to 600 GB/day of logs.</td>
</tr>
<tr>
<td>FortiAnalyzer 4000F</td>
<td>FAZ-4000F</td>
<td>Centralized log and analysis appliance — 2 x 10GbE SFP+, 2 x 10GbE SFP+, 64 TB storage, dual power supplies, up to 3,000 GB/day of logs.</td>
</tr>
<tr>
<td>FortiAnalyzer 5000G</td>
<td>FAZ-5000G</td>
<td>Centralized log and analysis appliance — 2 x 10GbE SFP+, 2 x SFP28, 86 TB storage, dual power supplies, up to 5,000 GB/day of logs.</td>
</tr>
<tr>
<td>FortiAnalyzer 3700F</td>
<td>FAZ-3700F</td>
<td>Centralized log and analysis appliance — 2 x SFP+, 2 x 1GE slots, 240 TB storage, up to 8,300 GB/day of logs.</td>
</tr>
<tr>
<td>FortiAnalyzer-VM Subscription</td>
<td>FC1-10-AZVMS-431-01-DD</td>
<td>Central Logging &amp; Analytics subscription for 5 GB/day logs, include 24x7 Forticare support, IOC, SOC Subscription.</td>
</tr>
<tr>
<td>FortiAnalyzer-VM Subscription</td>
<td>FC2-10-AZVMS-431-01-DD</td>
<td>Central Logging &amp; Analytics subscription for 50 GB/day logs, include 24x7 Forticare support, IOC, SOC Subscription.</td>
</tr>
<tr>
<td>FortiAnalyzer-VM Subscription</td>
<td>FC3-10-AZVMS-431-01-DD</td>
<td>Central Logging &amp; Analytics subscription for 500 GB/day logs, include 24x7 Forticare support, IOC, SOC Subscription.</td>
</tr>
<tr>
<td>FortiAnalyzer-VM</td>
<td>FAZ-VM-GB1</td>
<td>Upgrade license for adding 1 GB/day of logs and 500 GB storage capacity.</td>
</tr>
<tr>
<td>FortiAnalyzer-VM</td>
<td>FAZ-VM-GBS</td>
<td>Upgrade license for adding 5 GB/day of logs and 3 TB storage capacity.</td>
</tr>
<tr>
<td>FortiAnalyzer-VM</td>
<td>FAZ-VM-GBS5</td>
<td>Upgrade license for adding 25 GB/day of logs and 10 TB storage capacity.</td>
</tr>
<tr>
<td>FortiAnalyzer-Cloud</td>
<td>FC10-01-AZVMS-431-01-DD</td>
<td>Central Logging &amp; Analytics subscription for 5 GB/day logs, include 24x7 Forticare support, IOC, SOC Subscription.</td>
</tr>
<tr>
<td>FortiAnalyzer - Backup to Cloud Service</td>
<td>FC10-FAZ0U-208-02-DD</td>
<td>Year subscription to Forticare storage connector service for 10TB data transfer to public cloud.</td>
</tr>
<tr>
<td>FortiGuard Indicator of Compromise (IOC) Subscription</td>
<td>FC10-01-AZVMS-431-01-DD</td>
<td>Premium subscription for Cloud-based Central Logging &amp; Analytics. Supports all FortiGate log types with IOC service, SOC subscription and 24x7 Forticare support included.</td>
</tr>
<tr>
<td>FortiAnalyzer SOC Subscription</td>
<td>FC-10-(FortiGate Model Code) - 149-02-DD</td>
<td>Year Subscription license for the FortiGuard Indicator of Compromise (IOC).</td>
</tr>
<tr>
<td>Enterprise Protection Bundle</td>
<td>FC10-(FortiGate Model Code) - 135-02-DD</td>
<td>Subscription license for the FortiAnalyzer SOC component.</td>
</tr>
<tr>
<td>Hardware Bundle</td>
<td>FAZ-[Hardware Model]-BDL-432-DD</td>
<td>Hardware plus 24x7 Forticare and FortiAnalyzer Enterprise Protection.</td>
</tr>
</tbody>
</table>

* Requires FortiCloud Premium Account license.

+ Requires FortiCloud Premium Account license. This is not included as part of 360 Protection Bundle.