Lack of visibility continues to extend breach and compromise events to an average of more than 100 days. For each day an organization is exposed it’s another opportunity for attackers to get to sensitive customer and confidential information. FortiAnalyzer delivers critical insight into threats across the entire attack surface and provides instant visibility, situation awareness, real-time threat intelligence and actionable analytics. With action oriented views and deep drill down capabilities, FortiAnalyzer offers centralized logging and reporting for Fortinet’s Security Fabric.

Centralized Logging and Reporting

Event Correlation & Advanced Threat Detection - Allows IT administrators to quickly identify and respond to network security threats across the network.

Powerful NOC/SOC Dashboard - Customizable NOC/SOC dashboards provide management, monitoring and control over your network.

Scalable Performance & Flexible Deployments - Supports thousands of FortiGate and FortiClient™ agents, and dynamically scale storage based on retention requirements. Deploys as an individual unit or optimized for a specific operation.

Fortinet Security Fabric can provide unified, end-to-end protection by deploying Fortinet Enterprise Firewalls to battle the advanced persistent threats, and adding FortiAnalyzer to expand the Security Fabric for increased visibility and robust security alert information that is both actionable and automated.

FortiAnalyzer enables you to collect, analyze and correlate log data from your distributed network of Fortinet Enterprise Firewalls from one central location, and to view all your firewall traffic and generate reports from a single console. With a subscription to FortiGuard Indicator of Compromise (IOC) service, it can provide a prioritized list for compromised hosts, so you can quickly take action.

Features

- Centralized Search and Reports - Simple and intuitive Google-like search experience and reports on network traffic, threats, network activities and trends across the network.
- Automated Indicators of Compromise (IOC) - Scans security logs using FortiGuard IOC Intelligence for APT detection.
- Real-time and Historical Views into Network Activity - View a summary of applications, sources, destinations, websites, security threats, administrative modifications and system events.
- Light-weight Event Management - Predefined security event definitions are easily customizable with automated alerts.
- Seamless Integration with the Fortinet Security Fabric - Correlates with logs from FortiClient, FortiSandbox, FortiWeb and FortiMail for deeper visibility.
Feature Highlights

FortiView — Powerful Network Visibility
FortiAnalyzer’s customizable interactive dashboard helps you rapidly pinpoint problems, with intuitive summary views (Fig. 1) of network traffic, threats, applications and more. FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more. FortiView allows you to use multiple filters in the consoles, enabling you to narrow your view to a specific time, by user ID or local IP address, by application, and others. You can use it to investigate traffic activity such as user uploads/downloads or videos watched on YouTube on a network-wide user group or on an individual-user level. It presents information in both text and visual format.

Reports
You can generate custom data reports from logs by using the Reports feature. FortiAnalyzer provides 30+ built-in templates that are ready to use, with sample reports to help identify the right report for you. Run reports on-demand or on a schedule with automated email notifications, uploads and a 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.

Monitor and Alert
Event handlers define what messages to extract from logs and display in Event Management. You must enable an event handler to start generating events. You can configure event handlers to generate events for a specific device, for all devices, or for the local FortiAnalyzer unit. You can create event handlers for FortiGate, FortiCarrier, FortiCache, FortiMail, FortiManager, FortiWeb, FortiSandbox devices, and syslog servers. You can configure the system to send you alerts for event handlers via email address, SNMP community, or syslog server.

Network Operation Center (NOC) and Security Operation Center (SOC)
FortiAnalyzer’s NOC/SOC in a management center that helps you secure your overall network by providing actionable log and threat data. The SOC helps you protect your network, web sites, applications, databases, servers and data centers, and other technologies, with centralized monitoring and awareness of the threats, events and network activity, using the predefined FAZ dashboards and widgets, or customize your own, delivered through a single-pane-of-glass interface for easy integration into your Security Fabric. (fig 2.)

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. You can drill down to view threat details. To generate the Indicators of Compromise, FortiAnalyzer checks the web filter 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 the UTM web filter of FortiGate devices and FortiAnalyzer subscription to FortiGuard to keep its local threat database synced with the FortiGuard threat database.

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.

Log Fetch for Forensic Analysis
Log fetching is used to retrieve archived logs from one FortiAnalyzer device to another. This allows administrators to run queries and reports against historic data, which can be useful for forensic analysis. A FortiAnalyzer device can be either the fetch server or the fetching client, and it can perform both roles to retrieve the log data for a specified device and time period, based on specified filters. The retrieved data are then indexed, and can be used for data analysis and reports.
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 3)

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 VMware™ 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.

The FortiAnalyzer virtual appliance family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns that can be used to fine tune the security policy, thwarting future attackers. In addition, FortiAnalyzer-VM provides detailed data capture that can be used for forensic purposes to comply with regulations and policies regarding privacy and disclosure of information security breaches

Specifications

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<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>
<td>+2,000</td>
</tr>
<tr>
<td>Storage Capacity (GB/Day)</td>
<td>500 GB</td>
<td>+500 GB</td>
<td>+10 GB</td>
<td>+25 GB</td>
<td>+100 GB</td>
<td>+500 GB</td>
<td>+2,000 GB</td>
</tr>
<tr>
<td>Devices/ADOMs/VDOMs (Max)</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>
<td>10,000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HYPERVISOR REQUIREMENTS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor Support</td>
<td>VMware ESXi/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure</td>
</tr>
<tr>
<td>Network Interface Support (Min./Max.)</td>
<td>1/4</td>
</tr>
<tr>
<td>vCPUs (Min./Max.)</td>
<td>2/Unlimited</td>
</tr>
<tr>
<td>Memory Support (Min./Max.)</td>
<td>4 GB/Unlimited</td>
</tr>
</tbody>
</table>

* Unlimited GB/Day when deployed in collector mode
## Specifications

**FORTIANALYZER 200F**

<table>
<thead>
<tr>
<th>GB/Day of Logs</th>
<th>Analytic Sustained Rate (logs/sec)</th>
<th>Collector Sustained Rate (logs/sec)</th>
<th>Devices/VDOMs/ADOMs (Maximum)</th>
<th>Max Number of Days Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>3,000</td>
<td>4,500</td>
<td>150</td>
<td>30</td>
</tr>
<tr>
<td>200</td>
<td>6,000</td>
<td>9,000</td>
<td>200</td>
<td>30</td>
</tr>
<tr>
<td>600</td>
<td>18,000</td>
<td>27,000</td>
<td>2,000</td>
<td>30</td>
</tr>
<tr>
<td>1,000</td>
<td>30,000</td>
<td>45,000</td>
<td>2,000</td>
<td>30</td>
</tr>
</tbody>
</table>

**Options Supported**

- FortiGuard Indicator of Compromise (IOC): Yes
- FortiManager Capabilities (up to 20 devices): No

**Hardware Specifications**

- Form Factor: 1 RU Rackmount
- Total Interfaces: 2xRJ45 GE, 4x GE
- Storage Capacity: 4 TB (1 x 4 TB)
- Usable Storage (After RAID): 4 TB
- Removable Hard Drives: N/A
- RAID Levels Supported: RAID 0, 1, 5, 10
- Default RAID Level: N/A
- Redundant Hot Swap Power Supplies: No

**Dimensions**

- Height x Width x Length (inches): 1.75 x 17.0 x 15.0
- Weight: 17.1 lbs (7.8 kg)

**Environment**

- AC Power Supply: 100–240V AC, 60–50 Hz
- Power Consumption (Average): 49 W
- Heat Dissipation: 390 BTU/h
- Operating Temperature: 32 - 104°F (0 - 40°C)
- Storage Temperature: 95% to 90% non-condensing
- Operating Altitude: Up to 7,400 ft (2,250 m)
- Safety Certifications: FCC Part 15 Class A, C-Tick, VCCI, CE, UL/ULc, CB

**FORTIANALYZER 400E**

<table>
<thead>
<tr>
<th>GB/Day of Logs</th>
<th>Analytic Sustained Rate (logs/sec)</th>
<th>Collector Sustained Rate (logs/sec)</th>
<th>Devices/VDOMs/ADOMs (Maximum)</th>
<th>Max Number of Days Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>3,000</td>
<td>4,500</td>
<td>150</td>
<td>30</td>
</tr>
<tr>
<td>200</td>
<td>6,000</td>
<td>9,000</td>
<td>200</td>
<td>30</td>
</tr>
<tr>
<td>600</td>
<td>18,000</td>
<td>27,000</td>
<td>2,000</td>
<td>30</td>
</tr>
<tr>
<td>1,000</td>
<td>30,000</td>
<td>45,000</td>
<td>2,000</td>
<td>30</td>
</tr>
</tbody>
</table>

**Options Supported**

- FortiGuard Indicator of Compromise (IOC): Yes
- FortiManager Capabilities (up to 20 devices): No

**Hardware Specifications**

- Form Factor: 1 RU Rackmount
- Total Interfaces: 4x GE
- Storage Capacity: 12 TB (4x 3 TB)
- Usable Storage (After RAID): 6 TB
- Removable Hard Drives: N/A
- RAID Levels Supported: RAID 0/1/5/10
- Default RAID Level: 10
- Redundant Hot Swap Power Supplies: No

**Dimensions**

- Height x Width x Length (inches): 1.7 x 17.2 x 19.8
- Weight: 31 lbs (14.1 kg)

**Environment**

- AC Power Supply: 100–240V AC, 60–50 Hz
- Power Consumption (Average): 93 W
- Heat Dissipation: 468 BTU/h
- Operating Temperature: 41–95°F (5–35°C)
- Storage Temperature: 95% to 90% non-condensing
- Operating Altitude: Up to 9,842 ft (3,000 m)
- Safety Certifications: FCC Part 15 Class A, C-Tick, VCCI, CE, UL/ULc, CB

**FORTIANALYZER 1000E**

<table>
<thead>
<tr>
<th>GB/Day of Logs</th>
<th>Analytic Sustained Rate (logs/sec)</th>
<th>Collector Sustained Rate (logs/sec)</th>
<th>Devices/VDOMs/ADOMs (Maximum)</th>
<th>Max Number of Days Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>3,000</td>
<td>4,500</td>
<td>150</td>
<td>30</td>
</tr>
<tr>
<td>200</td>
<td>6,000</td>
<td>9,000</td>
<td>200</td>
<td>30</td>
</tr>
<tr>
<td>600</td>
<td>18,000</td>
<td>27,000</td>
<td>2,000</td>
<td>30</td>
</tr>
<tr>
<td>1,000</td>
<td>30,000</td>
<td>45,000</td>
<td>2,000</td>
<td>30</td>
</tr>
</tbody>
</table>

**Options Supported**

- FortiGuard Indicator of Compromise (IOC): Yes
- FortiManager Capabilities (up to 20 devices): No

**Hardware Specifications**

- Form Factor: 2 RU Rackmount
- Total Interfaces: 2x GE, 4x GE
- Storage Capacity: 24 TB (8x 3 TB)
- Usable Storage (After RAID): 18 TB
- Removable Hard Drives: N/A
- RAID Levels Supported: RAID 0/1/5/6/10/50/60
- Default RAID Level: 50
- Redundant Hot Swap Power Supplies: No

**Dimensions**

- Height x Width x Length (inches): 3.5 x 17.2 x 25.2
- Weight: 52 lbs (23.6 kg)

**Environment**

- AC Power Supply: 100–240V AC, 60–50 Hz
- Power Consumption (Average): 192.5 W
- Heat Dissipation: 920 BTU/h
- Operating Temperature: 41–95°F (5–35°C)
- Storage Temperature: 95% to 90% non-condensing
- Operating Altitude: Up to 7,400 ft (2,250 m)
- Safety Certifications: FCC Part 15 Class A, C-Tick, VCCI, CE, UL/ULc, CB

**FORTIANALYZER 2000E**

<table>
<thead>
<tr>
<th>GB/Day of Logs</th>
<th>Analytic Sustained Rate (logs/sec)</th>
<th>Collector Sustained Rate (logs/sec)</th>
<th>Devices/VDOMs/ADOMs (Maximum)</th>
<th>Max Number of Days Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>3,000</td>
<td>4,500</td>
<td>150</td>
<td>30</td>
</tr>
<tr>
<td>200</td>
<td>6,000</td>
<td>9,000</td>
<td>200</td>
<td>30</td>
</tr>
<tr>
<td>600</td>
<td>18,000</td>
<td>27,000</td>
<td>2,000</td>
<td>30</td>
</tr>
<tr>
<td>1,000</td>
<td>30,000</td>
<td>45,000</td>
<td>2,000</td>
<td>30</td>
</tr>
</tbody>
</table>

**Options Supported**

- FortiGuard Indicator of Compromise (IOC): Yes
- FortiManager Capabilities (up to 20 devices): No

**Hardware Specifications**

- Form Factor: 2 RU Rackmount
- Total Interfaces: 4x GE, 2 x SFP+
- Storage Capacity: 36 TB (12x 3 TB)
- Usable Storage (After RAID): 30 TB
- Removable Hard Drives: N/A
- RAID Levels Supported: RAID 0/1/5/6/10/50/60
- Default RAID Level: 50
- Redundant Hot Swap Power Supplies: No

**Dimensions**

- Height x Width x Length (inches): 3.5 x 17.2 x 25.6
- Weight: 58 lbs (26.3 kg)

**Environment**

- AC Power Supply: 100–240V AC, 60–50 Hz
- Power Consumption (Average): 293.8 W
- Heat Dissipation: 1,840 BTU/h
- Operating Temperature: 50–95°F (10 – 35°C)
- Storage Temperature: 95% to 90% non-condensing
- Operating Altitude: Up to 7,400 ft (2,250 m)
- Safety Certifications: FCC Part 15 Class A, C-Tick, VCCI, CE, UL/ULc, CB
## Specifications

### CAPACITY AND PERFORMANCE

<table>
<thead>
<tr>
<th></th>
<th>FORTIANALYZER 3000F</th>
<th>FORTIANALYZER 3500F</th>
<th>FORTIANALYZER 3700F</th>
<th>FORTIANALYZER 3900E</th>
</tr>
</thead>
<tbody>
<tr>
<td>GB/Day of Logs</td>
<td>3,000</td>
<td>5,000</td>
<td>8,300</td>
<td>4,000</td>
</tr>
<tr>
<td>Analytic Sustained Rate (logs/sec)</td>
<td>42,000</td>
<td>63,000</td>
<td>100,000</td>
<td>72,000</td>
</tr>
<tr>
<td>Collector Sustained Rate (logs/sec)</td>
<td>60,000</td>
<td>90,000</td>
<td>150,000</td>
<td>98,000</td>
</tr>
<tr>
<td>Devices/VDOMs/ADOMs (Maximum)</td>
<td>4,000</td>
<td>10,000</td>
<td>10,000</td>
<td>10,000</td>
</tr>
<tr>
<td>Max Number of Days Analytics</td>
<td>21</td>
<td>30</td>
<td>60</td>
<td>5</td>
</tr>
</tbody>
</table>

### OPTIONS SUPPORTED

- FortiGuard Indicator of Compromise (IOC)
- FortiManager Capabilities (up to 20 devices)

### HARDWARE SPECIFICATIONS

<table>
<thead>
<tr>
<th></th>
<th>FORTIANALYZER 3000F</th>
<th>FORTIANALYZER 3500F</th>
<th>FORTIANALYZER 3700F</th>
<th>FORTIANALYZER 3900E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Factor</td>
<td>3 RU Rackmount</td>
<td>4 RU Rackmount</td>
<td>4 RU Rackmount</td>
<td>2 RU Rackmount</td>
</tr>
<tr>
<td>Total Interfaces</td>
<td>4x GE, 2 x SFP+</td>
<td>2x GE, 2 x SFP ports</td>
<td>2xGE+, 2x1GE</td>
<td>2x GE, 2x 10GE SFP+</td>
</tr>
<tr>
<td>Storage Capacity</td>
<td>48 TB (16x 3 TB – 48 TB max)</td>
<td>72 TB (24x 3TB)</td>
<td>240 TB (60x4TB SAS HDDs)</td>
<td>15 TB SSD (15x 1 TB SSD)</td>
</tr>
<tr>
<td>Removable Hard Drives</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>RAID Levels Supported</td>
<td>RAID 0/1/5/6/10/50/60</td>
<td>RAID 0/1/5/6/10/50/60</td>
<td>RAID 0/1/5/6/10/50/60</td>
<td>RAID 0/1/5/6/10/50/60</td>
</tr>
<tr>
<td>Default RAID Level</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Redundant Hot Swap Power Supplies</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

### DIMENSIONS

<table>
<thead>
<tr>
<th></th>
<th>FORTIANALYZER 3000F</th>
<th>FORTIANALYZER 3500F</th>
<th>FORTIANALYZER 3700F</th>
<th>FORTIANALYZER 3900E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height x Width x Length (inches)</td>
<td>5.2 x 17.2 x 25.5</td>
<td>6.9 x 19.0 x 27.2</td>
<td>7 x 17.2 x 30.2</td>
<td>3.5 x 17.2 x 26.9</td>
</tr>
<tr>
<td>Height x Width x Length (cm)</td>
<td>13.2 x 43.7 x 64.8</td>
<td>17.6 x 48.2 x 69.0</td>
<td>17.8 x 43.7 x 76.7</td>
<td>8.9 x 43.7 x 68.4</td>
</tr>
<tr>
<td>Weight</td>
<td>76 lbs (34.5 kg)</td>
<td>93.74 lbs (42.59kg)</td>
<td>118 lbs (53.5kg)</td>
<td>52 lbs (23.6 kg)</td>
</tr>
</tbody>
</table>

### ENVIRONMENT

<table>
<thead>
<tr>
<th></th>
<th>FORTIANALYZER 3000F</th>
<th>FORTIANALYZER 3500F</th>
<th>FORTIANALYZER 3700F</th>
<th>FORTIANALYZER 3900E</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC Power Supply</td>
<td>100–240V AC, 50–60 Hz, 11.5 Amp Maximum</td>
<td>100–240V AC, 60–50 Hz</td>
<td>100-240V AC, 60-50 Hz</td>
<td>100–240V AC, 50–60 Hz, 11.5 Amp Maximum</td>
</tr>
<tr>
<td>Power Consumption (Average)</td>
<td>449 W for 12 HDD</td>
<td>465 W</td>
<td>850 W</td>
<td>470 W for 15 HDD</td>
</tr>
<tr>
<td>Heat Dissipation</td>
<td>1846.5 BTU/h</td>
<td>1904 BTU</td>
<td>4858 BTU</td>
<td>1351 BTU</td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>50–95°F (-10–35°C)</td>
<td>32–104°F (0–40°C)</td>
<td>50–95°F (10–35°C)</td>
<td>50–95°F (10–35°C)</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>-40–158°F (-40–70°C)</td>
<td>-13–158°F (-25–70°C)</td>
<td>-40–158°F (-40–70°C)</td>
<td>-40–140°F (-40–60°C)</td>
</tr>
<tr>
<td>Humidity</td>
<td>8–90% non-condensing</td>
<td>10–90% non-condensing</td>
<td>8% to 90% (non-condensing)</td>
<td>5–95% non-condensing</td>
</tr>
<tr>
<td>Operating Altitude</td>
<td>Up to 7,400 ft (2,250 m)</td>
<td>Up to 7,400 ft (2,250 m)</td>
<td>Up to 7,000 ft (35°C ambient)</td>
<td>Up to 7,400 ft (2,250 m)</td>
</tr>
</tbody>
</table>

### COMPLIANCE

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

* 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 200F</td>
<td>FAZ-200F</td>
<td>Centralized log and analysis appliance — 2x RJ45 GE, 4 TB storage, up to 100 GB/day of logs.</td>
</tr>
<tr>
<td>FortiAnalyzer 1000E</td>
<td>FAZ-1000E</td>
<td>Centralized log and analysis appliance — 2x GE RJ45, 24 TB storage, dual power supplies, up to 650 GB/day of logs.</td>
</tr>
<tr>
<td>FortiAnalyzer 2000E</td>
<td>FAZ-2000E</td>
<td>Centralized log and analysis appliance — 4x GE RJ45, 2 x SFP+, 36 TB storage, dual power supplies, up to 1,000 GB/day of logs.</td>
</tr>
<tr>
<td>FortiAnalyzer 3000F</td>
<td>FAZ-3000F</td>
<td>Centralized log and analysis appliance — 4x GE RJ45, 2 x SFP+, 48 TB storage, dual power supplies, up to 3,000 GB/day of logs.</td>
</tr>
<tr>
<td>FortiAnalyzer 3500F</td>
<td>FAZ-3500F</td>
<td>Centralized log and analysis appliance — 2x GE RJ45, 2x SFP ports, 72 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 — 2x RJ45 GE, 2x SFP+, 15 TB SSD storage, dual power supplies, up to 4,000 GB/day of logs.</td>
</tr>
<tr>
<td>FortiAnalyzer VM</td>
<td>FAZ-VM-BASE</td>
<td>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 VMware (vSphere, Xen), KVM and Hyper-V platforms.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB</td>
<td>Upgrade license for adding 1 GB/day of logs and 500 GB storage capacity.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB5</td>
<td>Upgrade license for adding 5 GB/day of logs and 3 TB storage capacity.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB25</td>
<td>Upgrade license for adding 25 GB/day of logs and 10 TB storage capacity.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB100</td>
<td>Upgrade license for adding 100 GB/day of logs and 24 TB storage capacity.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB500</td>
<td>Upgrade license for adding 500 GB/day of logs and 48 TB storage capacity.</td>
</tr>
<tr>
<td>FortiAnalyzer for AWS</td>
<td>FAZ-VM-BASE-AWS</td>
<td>Base license for stackable FortiAnalyzer VM— 2x RJ45 GE, 12 TB storage, up to 200 GB/day of logs.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB</td>
<td>Upgrade license for adding 1 GB/day of logs and 500 GB storage capacity.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB5</td>
<td>Upgrade license for adding 5 GB/day of logs and 3 TB storage capacity.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB25</td>
<td>Upgrade license for adding 25 GB/day of logs and 10 TB storage capacity.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB100</td>
<td>Upgrade license for adding 100 GB/day of logs and 24 TB storage capacity.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB500</td>
<td>Upgrade license for adding 500 GB/day of logs and 48 TB storage capacity.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB2000-AWS</td>
<td>Upgrade license for adding 2 TB/day of logs and 100 TB storage capacity.</td>
</tr>
<tr>
<td>FortiAnalyzer on-Demand</td>
<td>FAZ-VM-BASE-AZ</td>
<td>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 Azure platform.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB</td>
<td>Upgrade license for adding 1 GB/day of logs and 500 GB storage capacity.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB5</td>
<td>Upgrade license for adding 5 GB/day of logs and 3 TB storage capacity.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB25</td>
<td>Upgrade license for adding 25 GB/day of logs and 10 TB storage capacity.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB100</td>
<td>Upgrade license for adding 100 GB/day of logs and 24 TB storage capacity.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB500</td>
<td>Upgrade license for adding 500 GB/day of logs and 48 TB storage capacity.</td>
</tr>
<tr>
<td></td>
<td>FAZ-VM-GB2000-AZ</td>
<td>Upgrade license for adding 2 TB/day of logs and 100 TB storage capacity.</td>
</tr>
<tr>
<td>FortiAnalyzer Add-on Management Capabilities</td>
<td>FAZ-MGMT20</td>
<td>License to add FortiManager capabilities for up to 20 devices (1000 series and above — hardware only).</td>
</tr>
</tbody>
</table>

---

FORTINET | www.fortinet.com/sales
GLOBAL HEADQUARTERS | EMEA SALES OFFICE | APAC SALES OFFICE | LATIN AMERICA SALES OFFICE
Fortinet Inc. | 905 rue Albert Einstein | 300 Beach Road 20-01 | Sawgrass Lakes Center
899 Kifer Rd | Valbonne 06560 | The Concourse | 13450 W. Sunrise Blvd., Suite 430
Sunnyvale, CA 94086 | Alpes-Maritimes, France | Singapore 198955 | Sunrise, FL 33323
+1.408.235.7700 | Tel: +33.4.8987.0500 | Tel: +65.6395.2788 | Tel: +1.954.368.9990
United States | www.fortinet.com/sales | FST-PROD-DS-FAZ

Copyright © 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.