In today’s dynamic and fast changing security landscape, 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, along with NOC-SOC security analysis and operations perspective for Fortinet’s Security Fabric.

**Centralized Analysis**

**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

Incident Response
FortiAnalyzer’s Incident Response capability improves Management & Analytics with focus on event management and identification of compromised endpoints. Use improved default and custom event handlers to detect malicious and suspicious activities on the spot. Integration of events with the FOS automation framework for automated endpoint quarantine. 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.

FortiView — Powerful Network Visibility
Provides a customizable interactive dashboard that 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.

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.

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)
FortiAnalyzers NOC-SOC is 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.)

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 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

<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</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>
<td>+100 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>
<td>10,000</td>
</tr>
<tr>
<td>FortiGuard Indicator of Compromise (IOC)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

Hypervisor Requirements

Hypervisor Support
VMware ESXi 5.0/5.5/6.0/6.5, Microsoft Hyper-V 2008 R2/2012 R2/2016, Citrix XenServer 6.0+ and Open Source Xen 4.1+, KVM on Redhat 6.5+ and Ubuntu 17.04, Amazon Web Services (AWS), Microsoft Azure

Network Interface Support (Minimum / Maximum)
2 / Unlimited

vCPUs (Minimum / Maximum)
2 / Unlimited

Memory Support (Minimum / Maximum)
4 GB / Unlimited

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

### CAPACITY AND PERFORMANCE

<table>
<thead>
<tr>
<th></th>
<th>FORTIANALYZER 200F</th>
<th>FORTIANALYZER 300F</th>
<th>FORTIANALYZER 400E</th>
<th>FORTIANALYZER 1000E</th>
</tr>
</thead>
<tbody>
<tr>
<td>GB/Day of Logs</td>
<td>100</td>
<td>150</td>
<td>200</td>
<td>600</td>
</tr>
<tr>
<td>Analytic Sustained Rate (logs/sec)</td>
<td>3000</td>
<td>4500</td>
<td>6,000</td>
<td>18,000</td>
</tr>
<tr>
<td>Collector Sustained Rate (logs/sec)</td>
<td>4500</td>
<td>6,750</td>
<td>9,000</td>
<td>27,000</td>
</tr>
<tr>
<td>Devices/VDOMs (Maximum)</td>
<td>150</td>
<td>180</td>
<td>200</td>
<td>2,000</td>
</tr>
<tr>
<td>Max Number of Days Analytics</td>
<td>40</td>
<td>28</td>
<td>30</td>
<td>30</td>
</tr>
</tbody>
</table>

### OPTIONS SUPPORTED

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

### HARDWARE SPECIFICATIONS

- **Form Factor**: 1 RU Rackmount
- **Total Interfaces**: 2x RJ45 GE
- **Storage Capacity**: 4 TB (1 x 4 TB)
- **Usable Storage (After RAID)**: 4 TB
- **Removable Hard Drives**: No
- **RAID Levels Supported**: N/A
- **RAID Type**: N/A
- **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
- **Height x Width x Length (cm)**: 44.4 x 43.2 x 38.1
- **Weight**: 17.1 lbs (7.8 kg)

### ENVIRONMENT

- **AC Power Supply**: 100–240V AC, 60–50 Hz
- **Power Consumption (Max / Average)**: 49 W / 114W
- **Heat Dissipation**: 390 BTU/h
- **Operating Temperature**: 32 - 104° F (0 - 40° C)
- **Storage Temperature**: 95 - 158° F (35 - 70° C)
- **Humidity**: 20 to 90% non-condensing
- **Operating Altitude**: Up to 7,400 ft (2,250 m)

### COMPLIANCE

- **Safety Certifications**: FCC, CE, UL/cUL, CB

---

**FortiAnalyzer: Instant Visibility**
## Specifications

### CAPACITY AND PERFORMANCE

<table>
<thead>
<tr>
<th></th>
<th>FortiAnalyzer 2000E</th>
<th>FortiAnalyzer 3000F</th>
<th>FortiAnalyzer 3500F</th>
<th>FortiAnalyzer 3700F</th>
</tr>
</thead>
<tbody>
<tr>
<td>GB/Day of Logs</td>
<td>1,000</td>
<td>3,000</td>
<td>5,000</td>
<td>8,300</td>
</tr>
<tr>
<td>Analytic Sustained Rate (logs/sec)</td>
<td>30,000</td>
<td>42,000</td>
<td>63,000</td>
<td>100,000</td>
</tr>
<tr>
<td>Collector Sustained Rate (logs/sec)</td>
<td>45,000</td>
<td>60,000</td>
<td>90,000</td>
<td>150,000</td>
</tr>
<tr>
<td>Devices/VDOMs (Maximum)</td>
<td>2,000</td>
<td>4,000</td>
<td>10,000</td>
<td>15,000</td>
</tr>
<tr>
<td>Max Number of Days Analytics</td>
<td>30</td>
<td>30</td>
<td>30</td>
<td>60</td>
</tr>
</tbody>
</table>

### OPTIONS SUPPORTED

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

### HARDWARE SPECIFICATIONS

- **Form Factor**
  - 2 RU Rackmount
  - 3 RU Rackmount
  - 4 RU Rackmount
- **Total Interfaces**
  - 4x GE, 2 x SFP+
  - 4x GE, 2 x SFP+
  - 2x GE, 2x SFP ports
- **Storage Capacity**
  - 36 TB (12x 3TB)
  - 48 TB (16x 3TB – 48 TB max)
  - 72 TB (24x 3TB)
  - 240 TB (60x4TB SAS HDDs)
- **Usable Storage (After RAID)**
  - 30 TB
  - 42 TB
  - 63 TB
  - 210 TB
- **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 0/1/5/6/10/50/60
- **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

<table>
<thead>
<tr>
<th></th>
<th>2 RU Rackmount</th>
<th>3 RU Rackmount</th>
<th>4 RU Rackmount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height x Width x Length (inches)</td>
<td>3.5 x 17.2 x 25.6</td>
<td>5.2 x 17.2 x 25.6</td>
<td>6.9 x 19.0 x 27.2</td>
</tr>
<tr>
<td>Height x Width x Length (cm)</td>
<td>8.9 x 43.7 x 64.8</td>
<td>13.2 x 43.7 x 64.8</td>
<td>17.6 x 49.2 x 69.0</td>
</tr>
<tr>
<td>Weight</td>
<td>58 lbs (26.3 kg)</td>
<td>76 lbs (34.5 kg)</td>
<td>93.74 lbs (42.52 kg)</td>
</tr>
</tbody>
</table>

### ENVIRONMENT

<table>
<thead>
<tr>
<th></th>
<th>2 RU Rackmount</th>
<th>3 RU Rackmount</th>
<th>4 RU Rackmount</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC Power Supply</td>
<td>100–240V AC, 60–50 Hz</td>
<td>100–240V AC, 50–60 Hz, 11.5 Amp Maximum</td>
<td>100–240V AC, 60–50 Hz</td>
</tr>
<tr>
<td>Heat Dissipation</td>
<td>1840 BTU/h</td>
<td>1846.5 BTU/h</td>
<td>1904 BTU/h</td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>50–95°F (10 – 35°C)</td>
<td>50–95°F (10–35°C)</td>
<td>32–104°F (0–40°C)</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>-40–158°F (-40–70°C)</td>
<td>-40–158°F (-40–70°C)</td>
<td>-13–158°F (-25–70°C)</td>
</tr>
<tr>
<td>Humidity</td>
<td>8–90% non-condensing</td>
<td>8–90% non-condensing</td>
<td>10–90% 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 7,400 ft (2,250 m)</td>
</tr>
</tbody>
</table>

### 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
  - 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 — 2xRJ45 GE, 4 TB storage, up to 100 GB/day of logs.</td>
</tr>
<tr>
<td>FortiAnalyzer 300F</td>
<td>FAZ-300F</td>
<td>Centralized log and analysis appliance — 2xRJ45 GE, 8 TB storage, up to 150 GB/day of logs.</td>
</tr>
<tr>
<td>FortiAnalyzer 400E</td>
<td>FAZ-400E</td>
<td>Centralized log and analysis appliance — 4x GE RJ45, 12 TB storage, up to 200 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 SFP+, 2x1GE slots, 240 TB storage, up to 8,300 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 all supported platforms.</td>
</tr>
<tr>
<td></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></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>FortiAnalyzer AWS</td>
<td>On-Demand</td>
<td><a href="https://aws.amazon.com/marketplace/pp/B01N5K7210/ref=portal_asin_url">https://aws.amazon.com/marketplace/pp/B01N5K7210/ref=portal_asin_url</a></td>
</tr>
<tr>
<td>FortiAnalyzer Add-on</td>
<td>FOM-MGMT20</td>
<td>License to add FortiManager capabilities for up to 20 devices (1000 series and above — hardware only).</td>
</tr>
<tr>
<td>Management Capabilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Indicator</td>
<td>FC-10-[Model code]</td>
<td>1 Year Subscription license for the FortiGuard Indicator of Compromise (IOC).</td>
</tr>
<tr>
<td>of Compromise (IOC)</td>
<td>-149-02-DD</td>
<td></td>
</tr>
</tbody>
</table>