



FortiAnalyzer™

Centralized logging, analytics and reporting



# FortiAnalyzer

FortiAnalyzer 200D, 300D, 1000D, 2000B, 3000E, 3500E, 3900E and FAZ-VM

## Centralized logging, analytics and reporting

### Comprehensive Visualization of Your Network

FortiAnalyzer platforms integrate network logging, analytics, and reporting into a single system, delivering increased knowledge of security events throughout your network. The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns to help you fine tune your policies. Organizations of any size will benefit from centralized security event logging, forensic research, reporting, content archiving, data mining and malicious file quarantining.

You can deploy FortiAnalyzer physical or virtual appliances to collect, correlate, and analyze geographically and chronologically diverse security data. Aggregate alerts and log information from Fortinet appliances and third-party devices in a single location, providing a simplified, consolidated view of your security posture. In addition, FortiAnalyzer platforms provide detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of information security breaches.

### Key Features & Benefits

|   |   |
|---|---|
| <b>Graphical Summary Reports</b>                                | Provides network-wide reporting of events, activities and trends occurring on FortiGate® and third-party devices.   |
| <b>Network Event Correlation</b>                                | Allows IT administrators to quickly identify and react to network security threats across the network.  |
| <b>Scalable Performance and Capacity</b>                        | FortiAnalyzer family models support thousands of FortiGate and FortiClient™ agents, and can dynamically scale storage based on retention/compliance requirements. |
| <b>Choice of Standalone, Collector or Analyzer mode</b>         | Can be deployed as an individual unit or optimized for a specific operation (such as store & forward or analytics).   |
| <b>Seamless Integration with the Fortinet Product Portfolio</b> | Tight integration allows FortiAnalyzer resources to be managed from FortiGate or FortiManager™ user interfaces.   |

## Fortinet's Versatile Management Solution

Networks are constantly evolving due to threats, organizational growth or new regulatory/business requirements. Traditional analysis products focus on recording and identifying company-wide threats through logging, analysis and reporting over time.

FortiAnalyzer offers enterprise class features to identify these threats, but also provides flexibility to evolve along with your ever-changing network. FortiAnalyzer can generate highly customized reports for your business requirements while aggregating logs in a hierarchical, tiered logging topology.

Key tenets of Fortinet's management versatility:

- Diversity of form factors
- Architectural flexibility
- Highly customizable
- Simple licensing



## HIGHLIGHTS

### Reporting and Visualization Tools

- **FortiView Summary**

Views Generation ad-hoc graphical, filterable views of top users, applications, destinations, websites, threats, VPN usage and more.

- **Built-in Report Templates**

Utilize or modify the PDF templates to display colorful, comprehensive, graphical network security and usage reports.

- **UTM & Traffic Summary Reports**

Regularly analyze the security profile and traffic/bandwidth patterns with a new consolidated UTM/Traffic report.

- **Event Management**

Raise and monitor important events to present the IT administrator with unprecedented insight into potentially anomalous behavior.

- **Import/Export Templates**

After building a report, export and modify the configuration on another FortiAnalyzer or different ADOM.

### JSON and XML (Web Services) APIs

- APIs are available on all FortiAnalyzer hardware models and virtual machines
- JSON API — Allows MSSPs/large enterprises to manipulate FortiAnalyzer reports, charts/datasets and objects
- XML API — Enables IT administrators to quickly provision/configure FortiAnalyzer and generate reports
- Access tools, sample code, documentation and interact with the Fortinet developer community by subscribing to the Fortinet Developer Network (FNDN)

### Log Viewer

- View logs in real-time or historical
- Select from traffic, event and full security logs
- Browse by device, ADOM or in aggregate
- Log filtering and search capabilities
- Granular inspection with the log details pane
- Intuitive icons for countries, applications, etc.

### Event Management

- Comprehensive alert builder
- Trigger off of severity levels, specific events, actions and destinations
- Set varying thresholds by number of events within a certain timeframe
- View or search through historical alerts
- Notify via email/SNMP or raise a syslog event

### Better with FortiManager

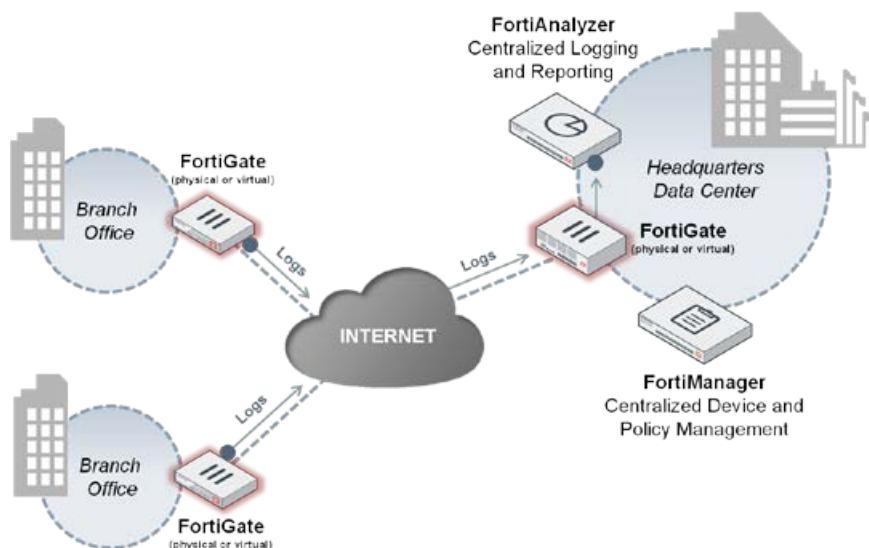
- Enterprise-class device management
- Familiar GUI for full network control
- Available as integrated solution with FortiAnalyzer

### DLP Archiving

- Investigate DLP content archives
- Supported archive types include: email, HTTP, FTP, IM
- View archive text or download files

### FortiAnalyzer Supported Devices

- FortiGate Multi-Threat Security Systems
- FortiMail Messaging Security Systems
- FortiClient Endpoint Security Suite
- FortiWeb Web Application Security
- FortiManager Centralized Management
- FortiSandbox Threat Protection
- FortiCache Web Caching
- Any Syslog-Compatible Device



## SPECIFICATIONS

|  | FORTIANALYZER 200D  | FORTIANALYZER 300D                                | FORTIANALYZER 1000D                                     | FORTIANALYZER 2000B   |
|--|---|---|---|---|
| <b>Capacity and Performance</b>              |   |   |   |   |
| GB/Day of Logs                               | 5   | 15  | 75  | 200   |
| Sustained Log Rate (Standalone Mode)         | 120   | 200   | 350   | 1,500   |
| Peak Log Rate (Standalone Mode)*             | 350   | 625   | 1,000   | 5,000   |
| Devices/VDOMs/ADOMs (Maximum)                | 150   | 175   | 2,000   | 2,000   |
| <b>Hardware Specifications</b>               |   |   |   |   |
| Form Factor                                  | 1 RU Rackmount  | 1 RU Rackmount                                    | 2 RU Rackmount  | 2 RU Rackmount  |
| Total Interfaces                             | 4x GE   | 4x GE   | 6x GE, 2x GE SFP  | 6x GE   |
| Storage Capacity                             | 1 TB (1x 1 TB)  | 4 TB (2x 2 TB)                                    | 8 TB (4x 2 TB)  | 4 TB (2x 2 TB – 12 TB maximum)                                    |
| Removable Hard Drives                        | No  | No  | Yes   | Yes   |
| RAID Levels Supported                        | None  | RAID 0/1  | RAID 0/1/5/10   | RAID 0/1/5/10/50  |
| Default RAID Level                           | –   | 1   | 10  | 10  |
| Redundant Hot Swap Power Supplies            | No  | No  | Yes   | Yes   |
| <b>Dimensions</b>                            |   |   |   |   |
| Height x Width x Length (inches)             | 1.8 x 17.1 x 13.9   | 1.7 x 17.1 x 14.3                                 | 3.5 x 17.2 x 14.5                                       | 3.4 x 17.4 x 26.8   |
| Height x Width x Length (cm)                 | 4.5 x 43.3 x 35.2   | 4.4 x 43.5 x 36.4                                 | 9 x 43.8 x 36.8   | 8.6 x 44.3 x 68.1   |
| Weight                                       | 13.4 lbs (6.1 kg)   | 15.9 lbs (7.2 kg)                                 | 30.6 lbs (13.9 kg)                                      | 63 lbs (28.6 kg)  |
| <b>Environment</b>                           |   |   |   |   |
| AC Power Supply                              | 100–240V AC, 50–60 Hz, 6 Amp Max.                                 | 100–240V AC, 50–60 Hz, 4 Amp Max.                 | 100–240V AC, 50–60 Hz, 5 Amp Max.                       | 100–240V AC, 50–60 Hz, 9 Amp Max.                                 |
| Power Consumption (Average)                  | 60 W  | 162 W   | 133 W   | 200 W   |
| Heat Dissipation                             | 205 BTU/h   | 666 BTU/h   | 546 BTU/h   | 519 BTU/h   |
| Operating Temperature                        | 32–104°F (0–40°C)   | 50–95°F (10–35°C)                                 | 32–104°F (0–40°C)                                       | 50–95°F (10–35°C)   |
| Storage Temperature                          | -13–158°F (-35–70°C)  | -40–158°F (-40–70°C)                              | -13–158°F (-25–70°C)                                    | -40–149°F (-40–65°C)  |
| Humidity                                     | 5–95% non-condensing  | 8–90% non-condensing                              | 5–95% non-condensing                                    | 5–95% 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 7,400 ft (2,250 m)  |
| <b>Compliance</b>                            |   |   |   |   |
| 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, BSMI, UL/cUL, CB | FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST |
| <b>FortiAnalyzer 3000E, 3500E, and 3900E</b> |   |   |   |   |
| <b>Capacity and Performance</b>              |   |   |   |   |
| GB/Day of Logs                               | 800   | 3,000   | 4,000   |   |
| Sustained Log Rate (Standalone Mode)         | 15,000  | 36,000  | 48,000  |   |
| Peak Log Rate (Standalone Mode)*             | 50,000  | 60,000  | 75,000  |   |
| Devices/VDOMs/ADOMs (Maximum)                | 4,000   | 4,000   | 4,000   |   |
| <b>Hardware Specifications</b>               |   |   |   |   |
| Form Factor                                  | 2 RU Rackmount  | 4 RU Rackmount                                    | 2 RU Rackmount  |   |
| Total Interfaces                             | 4x GE, 2x GE SFP  | 2x GE, 2x GE SFP                                  | 2x GE, 2x GE SFP+                                       |   |
| Storage Capacity                             | 16 TB (8x 2 TB)   | 24 TB (12x 2 TB – 48 TB maximum)                  | 15 TB SSD (15x 1 TB SSD)                                |   |
| Removable Hard Drives                        | Yes   | Yes   | Yes   |   |
| RAID Storage Management                      | RAID 0/1/5/6/10/50/60   | RAID 0/1/5/6/10/50/60                             | RAID 0/1/5/6/10/50/60                                   |   |
| Default RAID Level                           | 10  | 10  | 10  |   |
| Redundant Hot Swap Power Supplies            | Yes   | Yes   | Yes   |   |
| <b>Dimensions</b>                            |   |   |   |   |
| Height x Width x Length (inches)             | 3.4 x 19 x 29.7   | 6.9 x 19.1 x 27.2                                 | 3.5 x 17.2 x 26.9                                       |   |
| Height x Width x Length (cm)                 | 8.7 x 48.2 x 75.5   | 17.5 x 48.5 x 69.0                                | 8.9 x 43.7 x 68.4                                       |   |
| Weight                                       | 71.5 lbs (32.5 kg)  | 77 lbs (34.9 kg)                                  | 52 lbs (23.6 kg)  |   |
| <b>Environment</b>                           |   |   |   |   |
| AC Power Supply                              | 100–240V AC, 50–60 Hz, 10 Amp Maximum                             | 100–240V AC, 50–60 Hz, 11.5 Amp Maximum           | 100–240V AC, 50–60 Hz, 11.5 Amp Maximum                 |   |
| Power Consumption (Average)                  | 375.8 W   | 465 W for 12 HDD                                  | 470 W for 15 HDD  |   |
| Heat Dissipation                             | 1947 BTU/h  | 1904 BTU/h  | 1637 BTU/h  |   |
| Operating Temperature                        | 50–95°F (10–35°C)   | 32–104°F (0–40°C)                                 | 50–95°F (10–35°C)                                       |   |
| Storage Temperature                          | -40–149°F (-40–65°C)  | -13–158°F (-25–70°C)                              | -40–60°C (-40–140°F)                                    |   |
| Humidity                                     | 20–90% non-condensing   | 10–90% non-condensing                             | 5–95% (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)                                |   |
| <b>Compliance</b>                            |   |   |   |   |
| Safety Certifications                        | FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB       |   |

\* Peak log rate can hold for up to 2 hours

## SPECIFICATIONS

|   | FAZ-VM-BASE  | FAZ-VM-GB1 | FAZ-VM-GB5 | FAZ-VM-GB25 | FAZ-VM-GB100 |
|---|--|------------|------------|-------------|--------------|
| <b>Capacity and Performance</b>               |  |            |            |             |              |
| GB/Day of Logs                                | 1 incl.**  | +1         | +5         | +25         | +100         |
| Storage Capacity                              | 200 GB   | +200 GB    | +1 TB      | +8 TB       | +16 TB       |
| Devices/ADOMs/VDOMs Supported (Maximum)       | 10,000   | 10,000     | 10,000     | 10,000      | 10,000       |
| Hypervisor Support                            | VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5, Microsoft Hyper-V 2008 R2 / 2012, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS) |            |            |             |              |
| Network Interface Support (Minimum / Maximum) | 1 / 4  |            |            |             |              |
| vCPUs (Minimum / Maximum)                     | 1 / Unlimited  |            |            |             |              |
| Memory Support (Minimum / Maximum)            | 1 GB / Unlimited   |            |            |             |              |

\*\* Unlimited GB/Day when deployed in collector mode

## ORDER INFORMATION

| Product                | SKU            | Description   |
|------------------------|----------------|---|
| FortiAnalyzer 200D     | FAZ-200D       | Centralized log and analysis appliance — 4x GE RJ45, 1 TB storage, up to 5 GB/Day of logs.  |
| FortiAnalyzer 300D     | FAZ-300D       | Centralized log and analysis appliance — 4x GE RJ45, 4 TB storage, up to 15 GB/Day of logs.   |
| FortiAnalyzer 1000D    | FAZ-1000D      | Centralized log and analysis appliance — 6x GE RJ45, 2x SFP slots, 8 TB storage, up to 75 GB/Day of Logs.   |
| FortiAnalyzer 2000B    | FAZ-2000B-E03S | Centralized log and analysis appliance — 6x GE RJ45, 12 TB storage, dual power supplies, up to 200 GB/Day of Logs.  |
| FortiAnalyzer 3000E    | FAZ-3000E      | Centralized log and analysis appliance — 4x GE RJ45, 2x GE SFP slots, 16 TB storage, dual power supplies, up to 800 GB/Day of Logs.   |
| FortiAnalyzer 3500E    | FAZ-3500E-E02S | Centralized log and analysis appliance — 2x GE RJ45, 2x GE SFP slots, 48 TB storage, dual power supplies, up to 3,000 GB/Day of Logs.   |
| FortiAnalyzer 3900E    | FAZ-3900E      | Centralized log and analysis appliance — 2x GE RJ45, 2x 10 GE SFP+ slots, flash-based 15 TB SSD storage, dual power supplies, up to 4,000 GB/Day of Logs.   |
| FortiAnalyzer VM Base  | FAZ-VM-Base    | Base license for stackable FortiAnalyzer-VM; 1 GB/Day of Logs and 200 GB storage capacity. Unlimited GB/Day when used in collector mode only. Designed for AWS, VMware vSphere, Xen, KVM and Hyper-V platforms. |
| FortiAnalyzer VM GB1   | FAZ-VM-GB1     | Upgrade license for adding 1 GB/Day of Logs and 200 GB storage capacity.  |
| FortiAnalyzer VM GB5   | FAZ-VM-GB5     | Upgrade license for adding 5 GB/Day of Logs and 1 TB storage capacity.  |
| FortiAnalyzer VM GB25  | FAZ-VM-GB25    | Upgrade license for adding 25 GB/Day of Logs and 8 TB storage capacity.   |
| FortiAnalyzer VM GB100 | FAZ-VM-GB100   | Upgrade license for adding 100 GB/Day of Logs and 16 TB storage capacity.   |



GLOBAL HEADQUARTERS  
Fortinet Inc.  
899 Kifer Road  
Sunnyvale, CA 94086  
United States  
Tel: +1.408.235.7700  
www.fortinet.com/sales

EMEA SALES OFFICE  
120 rue Albert Caquot  
06560, Sophia Antipolis,  
France  
Tel: +33.4.8987.0510

APAC SALES OFFICE  
300 Beach Road 20-01  
The Concourse  
Singapore 199555  
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE  
Prol. Paseo de la Reforma 115 Int. 702  
Col. Lomas de Santa Fe,  
C.P. 01219  
Del. Álvaro Obregón  
México D.F.  
Tel: 011-52-(55) 5524-8480