

## FortiAnalyzer™ Appliances

Centralized Logging,  
Analysis, and Reporting

Datasheet

### Centralized Management Solutions for Fortinet Systems

#### Enhanced Visibility With FortiAnalyzer Platforms

FortiAnalyzer platforms integrate network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout a network. It 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 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 platforms provide detailed data capture that can be used for forensic purposes to comply with regulations and policies regarding privacy and disclosure of information security breaches.

#### Security Event Information Management

You can put time back in your day by deploying a FortiAnalyzer platform into your security infrastructure, creating a single view of your security events, archived content, and vulnerability assessments. FortiAnalyzer platforms accept a full range of data from Fortinet solutions, including traffic, event, virus, attack, content filtering, and email filtering data. It eliminates the need to manually search multiple log files or manually analyze multiple consoles when performing forensic analysis or network auditing. A FortiAnalyzer platform's central data archiving, file quarantine and vulnerability assessment functionality further reduce the amount of time you need to spend managing the range of security activity in your enterprise or organization.

#### Key Features and Benefits

- Network Event Correlation** Allows IT administrators to more quickly identify and react to network security threats across the network.
- Streamlined Graphical Reports** Provides network-wide reporting of events, activities and trends occurring on FortiGate® and third party devices.
- Scalable Performance and Capacity** FortiAnalyzer family models support thousands of FortiGate and FortiClient™ agents.
- Centralized Logging of Multiple Record Types** Including traffic activity, system events, viruses, attacks, Web filtering events, and messaging activity/data.
- Centralized Content Archiving with Centralized Quarantine** Provides reliable archiving of content data, such as email content, IM chat and file transfers, as well as a centralized quarantine repository for infected files.
- Centralized Log Aggregation** Supports flexible deployment scenarios, such as deploying lower cost models in regional offices, and aggregating logs to centralized office.
- Seamless Integration with the Fortinet Product Portfolio** Tight integration maximizes performance and allows FortiAnalyzer resources to be managed from FortiGate or FortiManager™ user interfaces.



FortiAnalyzer-100B



FortiAnalyzer-400B



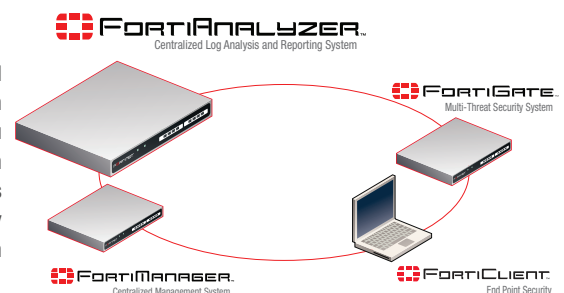
FortiAnalyzer-1000B



FortiAnalyzer-4000A

#### The FortiAnalyzer Difference

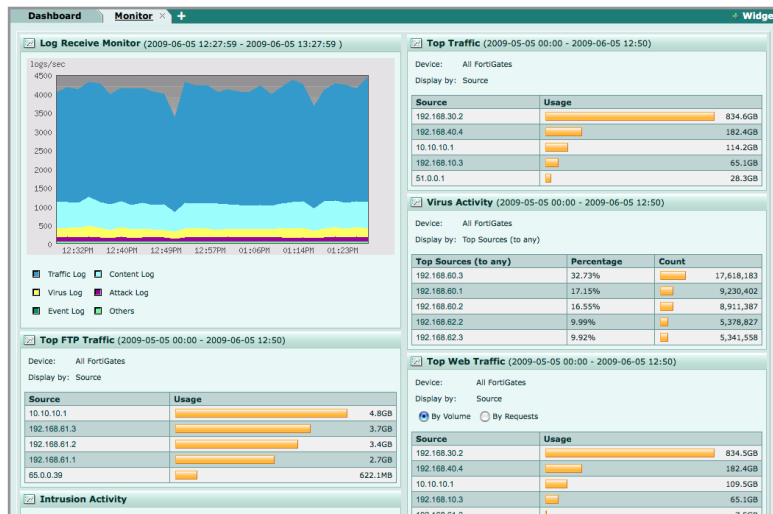
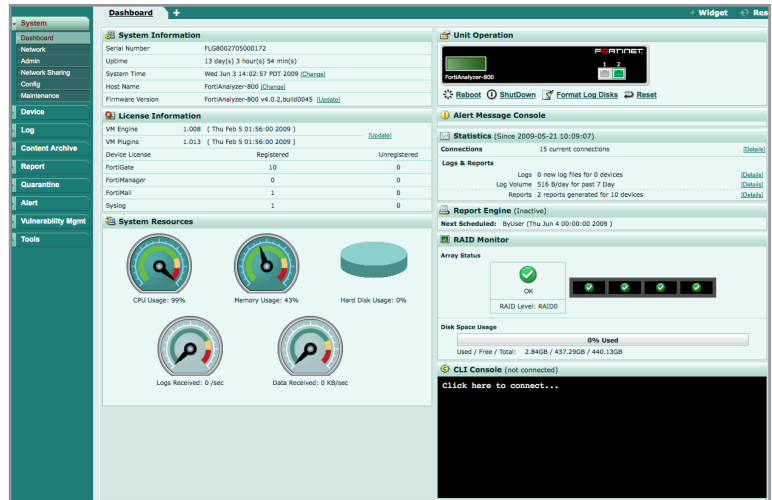
A FortiAnalyzer platform delivers complete security oversight with granular graphical reporting. Its breadth of data collection functions eliminate the blind spots in understanding your security posture. Its unique forensic analysis tools provide you with the ability to discover, analyze, and mitigate threats before perimeter breach or data loss/theft occurs. The FortiAnalyzer system's forensic analysis tool enables detailed user activity reports, while the vulnerability assessment tool automatically discovers, inventories and assesses the security posture of servers and hosts within the network infrastructure.



# Centralized Logging and Reporting with FortiAnalyzer Solutions— Complete Knowledge and Control

## Security Reporting—Security Management

A FortiAnalyzer platform is a centralized solution designed to ease the burden of network activity, logging and reporting challenges in today's complex, heterogeneous security environments. Its advanced reporting functions enable you to understand the entire range of security threat information, not just the Firewall or intrusion prevention elements. It delivers essential information you need through graphical reporting that are easy to configure, understand and use. The FortiAnalyzer dashboard enables administrators to assess the key health metrics of the network quickly, and immediately address critical issues.



## Understanding the Dynamic Security Environment

New regulatory requirements, industry policies, and legal mandates continue to evolve rapidly to attempt to stay abreast of security threats. Organizations are under tremendous pressure to comply with these regulations and policies, and often lack the ability to measure their compliance. FortiAnalyzer can deliver the necessary data to demonstrate policy compliance, in exactly the right format, eliminating the need to create reports manually. FortiAnalyzer platforms provide hundreds of customizable, pre-defined graphical reports that you can modify to fit your unique business requirements.

## Content Logging & Data Mining

Organizations of any size need network-wide log aggregation and archiving to identify security threats and manage network usage. FortiAnalyzer platforms provide detailed content logging of user activities and network traffic, in addition to in-depth, real-time event logging and reporting. You can monitor network activity in real-time or archive data for analysis at a later time. You can also track activity using a wide range of criteria including user, protocol, source, and destination, as well as capture the actual content exchanged in a particular session. Content logging is an essential element to complying with regulatory requirements such as HIPAA and SOX. It is also required to enforce acceptable use policies, protect valuable corporate assets and intellectual property, and protect brand equity.

The screenshot shows the 'Web Archive' interface with a table of activity logs. The table includes columns for #, Last Activity, Subtype, Source, URL, Method, Size, and Status.

#	Last Activity	Subtype	Source	URL	Method	Size	Status
1	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.208/iecar.com	GET	433 B	virus
2	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.208/iecar.com	GET	433 B	virus
3	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.208/iecar.com	GET	433 B	virus
4	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.208/iecar.com	GET	433 B	virus
5	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.208/iecar.com	GET	433 B	virus
6	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.208/iecar.com	GET	433 B	virus
7	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.208/iecar.com	GET	433 B	virus
8	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.208/iecar.com	GET	433 B	virus
9	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.208/iecar.com	GET	433 B	virus
10	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.208/iecar.com	GET	433 B	virus
11	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.208/iecar.com	GET	433 B	virus
12	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.217/iecar.com	GET	433 B	virus
13	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.217/iecar.com	GET	433 B	virus
14	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.217/iecar.com	GET	433 B	virus
15	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.217/iecar.com	GET	433 B	virus
16	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.217/iecar.com	GET	433 B	virus
17	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.217/iecar.com	GET	433 B	virus
18	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.217/iecar.com	GET	433 B	virus
19	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.217/test.com	GET	862 B	clean
20	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.217/iecar.com	GET	433 B	virus
21	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.217/iecar.com	GET	433 B	virus
22	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.217/test.com	GET	862 B	clean
23	2009-05-21 16:52:10	HTTP	192.168.61.2	10.10.10.205/iecar.com	GET	433 B	virus
24	2009-05-21 16:52:10	HTTP	192.168.61.2	10.10.10.205/iecar.com	GET	433 B	virus
25	2009-05-21 16:52:10	HTTP	192.168.61.2	10.10.10.205/iecar.com	GET	433 B	virus
26	2009-05-21 16:52:10	HTTP	192.168.61.2	10.10.10.205/iecar.com	GET	433 B	virus
27	2009-05-21 16:52:10	HTTP	192.168.61.2	10.10.10.205/iecar.com	GET	433 B	virus
28	2009-05-21 16:52:10	HTTP	192.168.61.2	10.10.10.205/iecar.com	GET	433 B	virus
29	2009-05-21 16:52:10	HTTP	192.168.61.2	10.10.10.205/iecar.com	GET	433 B	virus
30	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.217/iecar.com	GET	433 B	virus
31	2009-05-21 16:52:10	HTTP	192.168.61.3	10.10.10.217/iecar.com	GET	433 B	virus
32	2009-05-21 16:52:10	HTTP	192.168.61.2	10.10.10.205/iecar.com	GET	433 B	virus
33	2009-05-21 16:52:10	HTTP	192.168.61.2	10.10.10.205/iecar.com	GET	433 B	virus
34	2009-05-21 16:52:10	HTTP	192.168.61.2	10.10.10.205/iecar.com	GET	433 B	virus

## FortiAnalyzer Models



Feature	FortiAnalyzer-100B	FortiAnalyzer-400B	FortiAnalyzer-1000B	FortiAnalyzer-4000A
Security Hardened Platform	Yes	Yes	Yes	Yes
Log Performance (Logs / Sec)	Up to 200	Up to 500	Up to 1,000	Up to 5,000
Data Receive Rate	800 Kbps	2 Mbps	4 Mbps	20 Mbps
Number of Licensed Network Devices <sup>(1)</sup>	100	200	2,000	2,000
Number of FortiClient Devices	100	2,000	No Restriction	No Restriction
10/100 Ethernet	4	0	0	0
10/100/1000 Ethernet	0	4	4	2
Number of Hard Drives	1	1 (Second Drive Optional)	1 (Second Drive Optional)	12
Total Hard Drive Capacity	250.0 GB	500 GB (1.0 TB Optional)	1.0 TB (2.0 TB Optional)	6.0 TB
RAID Storage Management	No	No (Yes w/ Optional Drive-0, 1)	No (Yes w/ Optional Drive-0, 1)	Yes (0, 1, 5, 10, 50)
Redundant Hot Swap Power Supplies	No	No	No	Yes
Dimensions (H, W, L)	2.0 x 13.3 x 6.8 in. (5 x 33.7 x 17.5 cm)	1.7 x 17.25 x 14.5 in. (4.5 x 43.8 x 36.8 cm)	1.7 x 16.7 x 30.4 in. (4.3 x 42.6 x 77.2 cm)	3.5 x 19.0 x 27.0 in. (8.9 x 48.3 x 68.6 cm)
Weight	4.4 lbs (2.0 kg)	10.0 lbs (4.5 kg)	36.0 lbs (16.3 kg)	68.0 lbs (30.8 kg)
Rack Mountable	No	Yes	Yes	Yes
Input Voltage	100-240VAC	100-240VAC	100-240VAC	100-240VAC
Input Current (Max)	0.8A	4A	10A	9A
Average Power Consumption	24W	121W	260W	432W
Operating Temperature			32 to 104 deg F (0 to 40 deg C)	
Storage Temperature			-13 to 158 deg F (-25 to 70 deg C)	
Humidity			5 to 95% non-condensing	
Regulatory			FCC Class A (Part 15), UL/CUL, C Tick, CE, VCCI	
Recommended FortiGate Models	FortiGate-30-224B	All Models	All Models	All Models

<sup>(1)</sup> A licensed network device is defined as:  
 One (1) FortiGate device without Virtual Domain (VDOM) mode enabled  
 or One (1) VDOM if FortiGate device is running in multiple VDOM mode  
 or One (1) Third-party SYSLOG compatible device

### FortiAnalyzer Logging and Reporting Features

FortiAnalyzer supports the following logging, reporting and analysis features:

- Log Aggregation & Archiving**  
 Analyze logs from multiple devices, by user, or by group of users, and generate a variety of reports that enable you to proactively secure networks as threats arise, avoid network abuses, manage bandwidth, monitor Web site visits, and ensure appropriate usage policies.
- Data Mining, Trend and Forensic Analysis**  
 Archived content is data mined to report on types of traffic on your networks as well as actual content of data transferred in Web, FTP, email and IM traffic. Security event summaries identify unwanted traffic in the network and the top traffic producers, while traffic summaries identify the type of traffic on your network. Reports identify high volume users, information leakage events and acceptable use policy violations.  
 The forensic analysis tools available within the FortiAnalyzer interface enable administrators to analyze archived content to track user activities by username, email address, or IM name. The FortiAnalyzer system supports FortiGuard<sup>®</sup> Web filtering reports to analyze Web site access and blocked Web sites on a per user basis.
- Central Quarantine**  
 For FortiGate systems that do not have a hard disk, the FortiAnalyzer offers the ability to quarantine infected or suspicious files entering your network environment. A quarantine browser allows you to view the files to determine whether they are dangerous or not.
- Log Browser**  
 Log Browser enables you to view any log file or messages from registered devices. All log files and messages are searchable and can be filtered to drill down and locate specific information.
- Real-Time Log Viewer**  
 Real-time display of information allows you to follow real-time trends in network usage such as the source IP address and the destination URL for HTTP traffic or IM message traffic.
- Network Analyzer**  
 The integrated network analysis tool allows any available interface on the FortiAnalyzer to be used to monitor traffic on a segment of network. The FortiAnalyzer network analyzer functions much like a packet capture device to capture traffic data, save it to the FortiAnalyzer hard disk and display the data for analysis.
- Vulnerability Scanner**  
 The integrated vulnerability scanner identifies vulnerabilities on a host or server, such as a mail server, FTP server or other UNIX or Windows host and generates vulnerability reports showing potential weaknesses to attacks that may exist for a selected device.  
 FortiGuard Services deliver dynamic updates to vulnerability management functionality through intelligence gathered by Fortinet's dedicated global threat research team.

### GRAPHICAL REPORTING

FortiAnalyzer systems empower the network or security administrator with the knowledge needed to secure their networks through a comprehensive suite of standard graphical reports and the total flexibility to customize custom reports. Network knowledge can be archived, filtered and mined for compliance or historical analysis purposes.

### REAL-TIME LOG VIEWER

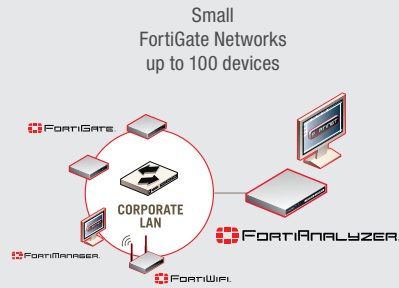
The ability to monitor network, traffic and user events in real-time or browse historical for specific events provides powerful insight into network security threats, performance and user behavior.

### GRANULAR INFORMATION

The FortiAnalyzer User Interface (UI) enables administrators to drill deep within security log data to provide the granular level of reporting necessary to understand what is happening on your network. Historical or real-time views allow administrators to analyze log and content information, as well as network traffic. The advanced forensic analysis tools allow the administrator to track user activities to the content level.

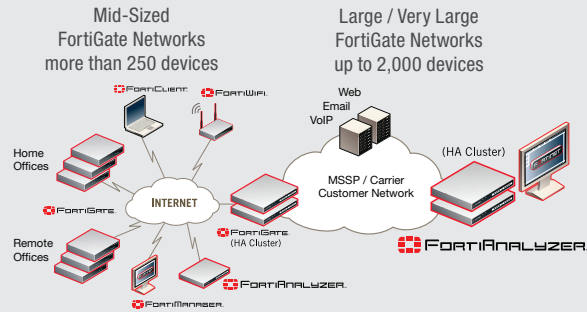
## TYPICAL APPLICATIONS

### FortiAnalyzer-100B



Small-Medium Enterprise Network with Central Logging / Reporting

### FortiAnalyzer-400B



Enterprise / MSSP / Carrier Networks Multiple Layered Log Aggregation and Customer Access

### FortiAnalyzer-1000B

Large / Very Large FortiGate Networks up to 2,000 devices

## All FortiAnalyzer models provide the following features

### GENERAL SYSTEM FUNCTIONS

- Profile-Based Administration
- Secure Web Based User Interface Encrypted Communication & Authentication Between FortiAnalyzer Server and FortiGate Devices
- Mail Server Alert Output
- Connect / Sync FortiAnalyzer
- SNMP Traps
- Syslog Server Support
- RAID Configurations
- Change / View RAID Level
- Support For Network Attached Storage (NAS)
- Launch Management Modules
- Launch Administration Console
- Configure Basic System Settings
- Online Help
- Add/Change/Delete a FortiGate Device
- View Device Groups
- View Blocked Devices
- View Alerts / Alert Events
- Alert Message Console
- View FortiManager Connection Status
- View System Information / Resources
- View License Information
- View Statistics
- View Operational History
- View Session Information
- Backup / Restore
- Restore Factory Default System Settings
- Format Log Disks
- Change the Firmware
- Change the Host Name

### NETWORK ANALYZER

- Real-Time Traffic Viewer
- Historical Traffic Viewer
- Customizable Traffic Analyzer Log
- Search Network Traffic Logs

### CENTRAL QUARANTINE

- Configure Quarantine Settings
- View Quarantined Files List

### LOG ANALYSIS & REPORTING

- View/Search/Manage Logs
- Automatic Log Watch
- Profile-Based Reporting
- Over 300 Predefined Reports
- Example Reports Include:
  - Attacks: By FortiGate Unit, by Hour Of The Day, by Category, and by Top Sources
  - Viruses: Top Viruses Detected, Viruses Detected by Protocol
  - Events: By Firewall, Overall Events Triggered, Security Events Triggered, & Events Triggered by Day of Week
  - Mail Usage: Top Mail Users by Inbound and Outbound Web Usage Reports
  - Web Usage: Top Web Users, Top Blocked Sites, and Top Client Attempts to Blocked Sites
  - Bandwidth Usage: Top Bandwidth Users, Bandwidth by Day and by Hour, and Bandwidth Usage by Protocol Family
  - Protocols: Top Protocols Used, Top FTP Users, & Top Telnet Users
- Log Aggregation to Centralized FortiAnalyzer
- FortiClient Specific Reports

### FORENSIC ANALYSIS

- Track User Activities by Username, Email Address, or IM Name
- Supports FortiGuard Web Filtering Reports to Show Web Site Access And Blocked Web Sites Per User
- Configurable Report Parameters including:
  - Profiles
  - Devices
  - Scope
  - Types
  - Format
  - Schedule
  - Output
- Customized Report Output
- Reports on Demand
- Report Browsing

### CONTENT ARCHIVING / DATA MINING

- All Functions of Log Analysis & Reporting
- View by Traffic Type
- View Content Including:
  - HTTP (Web URLs)
  - FTP (Filenames)
  - Email (Text)
  - Instant Messaging (Text)
- View Security Event Summaries
- View Traffic Summaries
- View Top Traffic Producers

### LOG BROWSER AND REAL-TIME LOG VIEWER

- Real-Time Log Viewer
- Historical Log Viewer
- Customized Log Views
- Log Filtering
- Log Search
- Log Rolling
- Top Users
- View Web Traffic
- View Email Traffic
- View FTP Traffic
- View Instant Messaging and P2P Traffic
- Filter Traffic Summaries
- Device Summary
- Traffic Reports Including:
  - Event (Admin Auditing)
  - Viruses Detected
  - Attack (IPS Attacks)
  - Web Content Filtering
  - Email Filtering
  - Content (Web, Email, IM)

### VULNERABILITY SCANNER

- Configure Vulnerability Scan Jobs
- Run Vulnerability Scan Jobs
- View Summary Reports
- View Detailed Reports

### Supported Devices

- FortiGate Multi-Threat Security Systems
- FortiMail Messaging Security Systems
- FortiClient Mobile End-Point Security
- FortiClient PC End-Point Security
- FortiManager Centralized Management
- Any Syslog-Compatible Device

### FortiCare™ Technical Support Services

- 24 x 7 x 365 Comprehensive Support
- 8 x 5 Enhanced Support
- 1-Year Limited Hardware Warranty
- 90-Day Limited Software Warranty

# FORTINET®

### GLOBAL HEADQUARTERS

Fortinet Incorporated  
1090 Kifer Road, Sunnyvale, CA 94086 USA  
Tel +1-408-235-7700  
Fax +1-408-235-7737  
[www.fortinet.com/sales](http://www.fortinet.com/sales)

### EMEA SALES OFFICE-FRANCE

Fortinet Incorporated  
120 Rue Albert Caquot  
06560 Sophia Antipolis, France  
Tel +33-4-8987-0510  
Fax +33-4-8987-0501

### APAC SALES OFFICE-HONG KONG

Fortinet Incorporated  
61 Robinson Road  
#09-04 Robinson Centre  
Singapore 068893  
Tel: +65-6513-3730  
Fax: +65-6223-6784