DATASHEET

FortiAnalyzer

Centralized Logging, Analysis, and Reporting

Enhanced Visibility With FortiAnalyzer Platforms

FortiAnalyzer platforms integrate network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout your network. They provide organizations of any size with centralized security event analysis, forensic research, reporting, content archiving, data mining, malicious file quarantining and vulnerability management. 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 to help you fine tune your policies. In addition, FortiAnalyzer platforms provide detailed data capture for forensic purposes to comply with 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 further reduce the amount of time you need to spend managing the range of security activity in your enterprise or organization.

Vulnerability Management

Fortinet offers an enhanced scanning capability that utilizes a dynamic signature dataset to detect devices on your network, catalog vulnerabilities, and recommend remediation. Additional capabilities include device discovery, mapping, asset definition and prioritization, and customized reporting. An optional Vulnerability Management subscription provides frequent updates developed by the FortiGuard Labs with up-to-date vulnerability scan data to keep abreast of current threats.

The FortiAnalyzer Difference

A FortiAnalyzer platform delivers complete security oversight with granular graphical reporting. Its breadth of data collection functions eliminate blind spots in 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. The FortiAnalyzer system's forensic analysis tool enables detailed user activity reports, while the vulnerability management tool automatically discovers, inventories and assesses the security posture of servers and hosts within the network infrastructure.

FortiAnalyzer systems come with a one-year limited hardware warranty and 90-day limited software warranty.

Features	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.
Seamless Integration with the Fortinet Product Portfolio	Tight integration maximizes performance and allows FortiAnalyzer resources to be managed from FortiGate or FortiManager™ user interfaces.
Choice of Collector or Analyze mode	Can be optimized for either Store & Forward or Analytic operations.

FortiAnalyzerOS 4.1 provides the following features

General System Functions

Profile-Based Administration
Secure Web Based User Interface for 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 Statistics
View Operational History
View Session Information
Backup / Restore
Restore Factory Default System Settings
Format Log Disks
Migrate data from FortiAnalyzer to another
Per-ADOM Dashboard

DLP Archive / Data Mining

All Functions of Log Analysis & Reporting with additional tools to detect and analyze data losses
View by Traffic Type
View Content Including: HTTP (Web URLs), FTP (Filenames), Email (Text), and Instant Messaging (Text)
View Security Event Summaries
View Traffic Summaries
View Top Traffic Producers

Network Analyzer

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

Log Analysis & Reporting

View/Search/Manage Logs
Automatic Log Watch
Profile-Based Reporting
Over 300 Predefined Reports plus customization
Example Reports Include:

- 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
- Wan-Opt log information

Log Aggregation to Centralized FortiAnalyzer
FortiClient Specific Reports
SQL Database Integration
SQL support for all features – including alerts, dashboard widgets, log viewer, FortClient, and FortiMail
SQL Query / Schema tools

Central Quarantine

Configure Quarantine Settings
View Quarantined Files List
Quantine Release API
Quantine Summary by type of file, reason it was detected, first and last detected times, total unique quarantine files, and total number of detections for each type and reason

Forensic Analysis

E-Discovery
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 and Output
Customized Report Output
Reports on Demand
Report Browsing

Log Browser And Real-Time Log Viewer

Web 2.0 Style, Real-Time Log Viewer
Historical & Custom Log Views
Log Filtering, Search, and Rolling
View Web, Email and/or 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 and Compliance Management Scanning

Basic set of vulnerability signatures included with 4.3 OS, updates available as optional subscription
Detect vulnerabilities / recommend remediation
Group/report by asset class
CVE compatibility with search by CVE names
PCI DSS scans and reports
Compatibility with SQL log database and report engine
Unified reporting for FortiGate scan and FortiAnalyzer scan results
XML API to retrieve IPS Packet Log
Log Forwarding in CEF Format
ConnectWise Support
TACACS+ and SNMPv3 Support

Graphic 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.

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.

Real-Time Log Viewer

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

Supported Devices

- FortiGate Multi-Threat Security Systems
- FortiMail Messaging Security Systems
- FortiClient Endpoint Security Suite
- FortiManager Centralized Management
- Any Syslog-Compatible Device

FortiAnalyzer	100C	400B	1000C	2000B	4000B
Hardware Specification					
Security Hardened Platform	Yes	Yes	Yes	Yes	Yes
10/100/1000 Ethernet	2	4	4	6	2
10/100 Ethernet	1	0	0	0	0
1GbE SPF	0	0	0	0	2
Number of Hard Drives	1	1 (One Drive Optional)	1 (Three Drives Optional)	2 (Four Drives Optional)	6 (Eighteen Drives Optional)
Total Hard Drive Capacity	1 TB	500 GB (1 TB Optional)	1.0 TB (4 TB Optional)	2.0 TB (6 TB Optional)	6 TB (P24 TB Optional, 16 TB File System)
RAID Storage Management	No	No (Yes with Optional Drive 0, 1)	No (Yes with Optional Drives 0, 1, 10)	Yes (0, 1, 5, 10, 50)	Yes (0, 1, 5, 6, 10, 50, 60: default is 50)
Number of Logs	912,680,550	912,680,550 (RAID 0)	3,865,470,566 (RAID 0)	5,798,205,850 (RAID 0)	16,384, 000,000 (RAID 0)
Redundant Hot Swap Power Supplies	No	No	No	Yes	Yes
System Performance					
Log Performance (Logs / Sec)	Up to 200	Up to 500	Up to 1,000	Up to 3,000	Up to 6,000
Data Receive Rate	800 Kbps	2 Mbps	4 Mbps	12 Mbps	24 Mbps
Number of Licensed Network Devices[1]	100	200	2,000	2,000	2,000
Number of FortiClient Agents	100	2,000	No Restriction	No Restriction	No Restriction
FortiGate Models Supported	All Models	All Models	All Models	All Models	All Modules
Dimensions					
Height	1.75 in (4.4 cm)	1.7 in (4.3 cm)	1.7 in (4.3 cm)	3.4 in (8.6 cm)	6.89 in (17.5cm)
Width	15 in (38 cm)	17.5 in (43.8 cm)	17.1 in (43.4 cm)	17.4 in (44.3 cm)	19.09 in (48.5 cm)
Length	6.3 in (16 cm)	14.5 in (36.8 cm)	24.7 in (62.7 cm)	26.8 in (68.1 cm)	27.17 in (69.0 cm)
Weight	4 lbs (1.8 kg)	10 lbs (4.5 kg)	35.0 lbs (15.9 kg)	57.5 lbs (26.1 kg)	94.5 lbs (43kg)
Rack Mountable	Yes	Yes	Yes	Yes	Yes
Environment					
AC Power Required	100 – 240 VAC, 50 – 60 Hz, 1.5 Amp (Max)	100 – 240 VAC, 50 – 60 Hz, 4 Amp (Max)	100 – 240 VAC, 50 – 60 Hz, 7 Amp (Max)	100 – 240 VAC, 50 – 60 Hz, 8 Amp (Max)	100-240 VAC, 50 - 60 Hz, 5.5 - 11.5 Amps (Max)
Power Consumption (AVG)	56W	83W	189W	152W	420W for 6 HDD
Heat Dissipation	190.4 BTU	283 BTU	643.6 BTU	519 BTU	1433.7 BTU (6 drives) 2034.6 BTU (12 drives)
Operating Temperature	32 – 104 deg F (0 – 40 deg C)		32 – 95 deg F (0 – 35 deg C)	32 – 104 deg F (0 – 40 deg C)	
Storage Temperature	-13 – 158 deg F (-25 – 70 deg C)				
Humidity	5 to 95% non-condensing				
Compliance					
	FCC Class A Part 15, UL/CUL, C Tick, CE, VCCI				

[1]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

FortiGuard® Security Subscription Services deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispam, vulnerability and compliance management, application control, and database security services.

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with "return and replace" hardware replacement or 24x7 Comprehensive Support with advanced replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and 90-day limited software warranty.

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

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 – SINGAPORE
Fortinet Incorporated
300 Beach Road 20-01, The Concourse
Singapore 199555
Tel: +65-6513-3730
Fax: +65-6223-6784

Copyright© 2011 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance 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 the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. 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. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.

FAZ-000-DAT-R8-201107