



# 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.

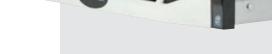
The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns to help you fine tune your policies. In addition, FortiAnalyzer platforms provide detailed data capture for forensic purposes to comply with policies regarding privacy 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 Standalone, Collector or Analyzer mode	Can be deployed as an individual unit or optimized for a specific operation (such as Store & Forward or Analytics)

# FortiAnalyzerOS 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, FortiClient, and FortiMail

SQL Query / Schema tools

#### **Central Quarantine**

Configure Quarantine Settings View Quarantined Files List Quarantine Release API

Quarantine 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

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 and 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**

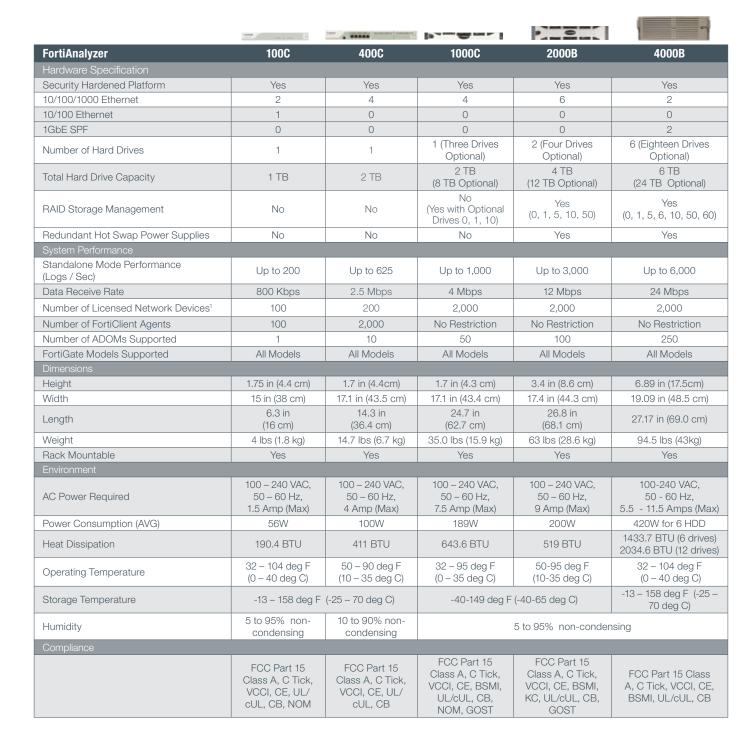
The FortiAnalyzer User Interface (UI) enables administrators to drill deep within security log data to provide the granular level of reporting necessary to understand what is happening on your network. Historical or real-time views allow administrators to analyze log and content information, as well 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
- FortiWeb Web Application Security
- FortiManager Centralized Management
- Any Syslog-Compatible Device



A licensed network device is defined as:

letwork device is defined as One (1) FortiGate device without Virtual Domain (VDOM) mode enabled, One (1) VDOM if FortiGate device is running in multiple VDOM mode One (1) Third-party SYSLOG compatible device

#### **GLOBAL HEADQUARTERS**

www.fortinet.com/sales

Fortinet Incorporated 1090 Kifer Road, Sunnyvale, CA 94086 USA Tel +1.408.235.7700 Fax +1.408.235.7737

**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: +65-6513-3734 Fax: +65-6295-0015



Copyright© 2012 Fortinet, Inc. All rights reserved. Fortinet@, FortiGate@, and FortiGate@, 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 Fortinet. 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.

FST-PROD-DS-AZ FAZ-DAT-R9-201204