

# FORTIREPORTER™ SECURITY ANALYZER

## Comprehensive Security Reporting and Analysis

An award winning, easy-to-use, and cost effective Security Information/Event Management (SIEM) and Compliance Audit Lifecycle Management (CALM) solution that provides essential real-time security intelligence to help decipher hacker/virus behavior, combat security threats, and meet compliance requirements.

Fortinet's Fortigate FortiReporter Security Analyzer ("FortiReporter") provides security professionals with the essential real-time security intelligence to help identify and understand hacker, virus, and SPAM/spyware behavior to combat security threats and meet compliance auditing requirements. FortiReporter provides essential real-time security intelligence across 1000s of network devices that have an impact on a company's security framework. Fortireporter automatically collects and correlates event data from variety of heterogeneous multi-vendor network devices and systems including routers, switches, firewalls, VPNs, IDS/IPS systems, proxy servers, antivirus, SPAM, and spyware systems, content filtering and web security appliances. FortiReporter helps to eliminate false positives, improve security operations and delivers all necessary tools to meet Sarbanes-Oxley, GLBA, HIPAA, and FISMA compliance. FortiReportersupports a variety of devices from leading security vendors.

FortiReporter helps minimize incident response time and maximize the ability to take proactive and preventative actions to improve security information management, reduce hacker and virus attacks, and meet regulatory compliance requirements. Using the real-time monitoring and correlation analysis, security professionals can quickly and easily gain insight into hacker and virus activity to improve the overall security posture.

### Key Benefits

Heterogeneous security management
Real-time monitoring and correlated alerting
Forensics analysis for security-related investigations
Supports routers, switches, firewalls, VPNs, IDS/IPS, antivirus, SPAM/spyware
Reporting and monitoring portals and MSSP support
Compliance Audit Lifecycle Management

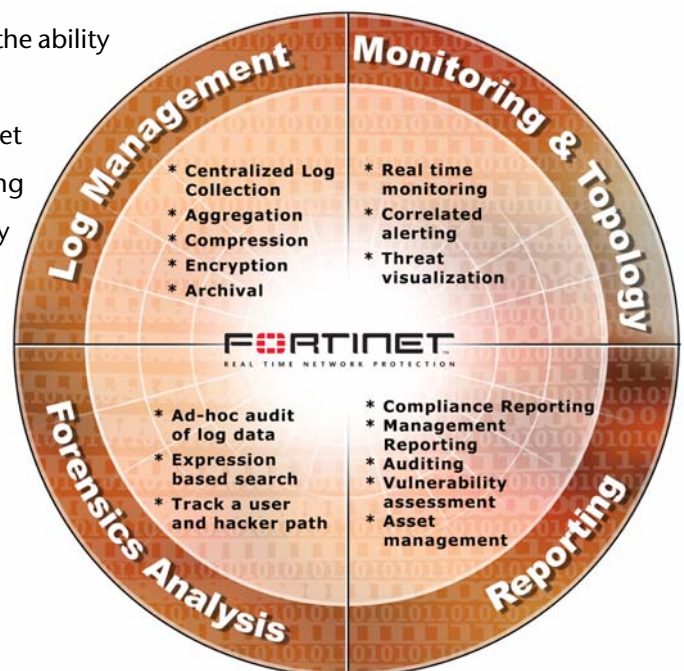


Figure 1: Comprehensive SIEM and Compliance Audit Management solution required to meet government regulations including HIPAA, GLBA, Sarbanes-Oxley, and FISMA

# FORTIREPORTER™ SECURITY ANALYZER

## Architectural Overview

In today's environment, a key feature required for a security management solution is the ability to scale to large networked environments. FortiReporter provides a distributed enterprise-class architecture that scales to 1000s of network devices. The architecture supports both a stand-alone deployment for smaller networks and a distributed deployment for large enterprise installations. The flexibility of the FortiReporter architecture allows for the creation of a security information and event management system that can adapt to any environment. The architecture allows MSSPs to easily integrate into existing security portals. FortiReporter delivers all necessary tools—such as centralized log management, monitoring/alerting, reporting, and forensics analysis, to help meet compliance requirements.

## Architectural Benefits

**Distributed Enterprise Class Architecture** – The hub and spoke architecture can scale to 15,000 network devices.

**Cost Effective and Powerful** - FortiReporter offers the industry's best ROI and TCO with powerful and scalable implementation. It is easy-to-use and requires little or no help with installation.

**Managed Services Offering Providers (MSSPs) Support** - MSSPs can use FortiReporter to provide on-demand security monitoring and reporting services to managed services customers.

**Heterogeneous Device and Vendor Support** - Supports data from all leading switches, routers, firewalls, VPNs, IDS/IPS, antivirus systems, SPAM, content filtering, proxy servers, and web security appliances.

**Role-based Access and Active Directory/LDAP User Management**– Integrates with Active Directory for single user sign-on and role-based access to the reporting and monitoring portals.

**Anytime, Anywhere Access and Management** - Browser-based access allows report generation from any computer on the local network or remotely.

**Embedded Database and ODBC Support** - Stores syslog data using either an embedded database or the enterprise-level database of choice. Relieves security administrators from writing SQL queries and scripts.

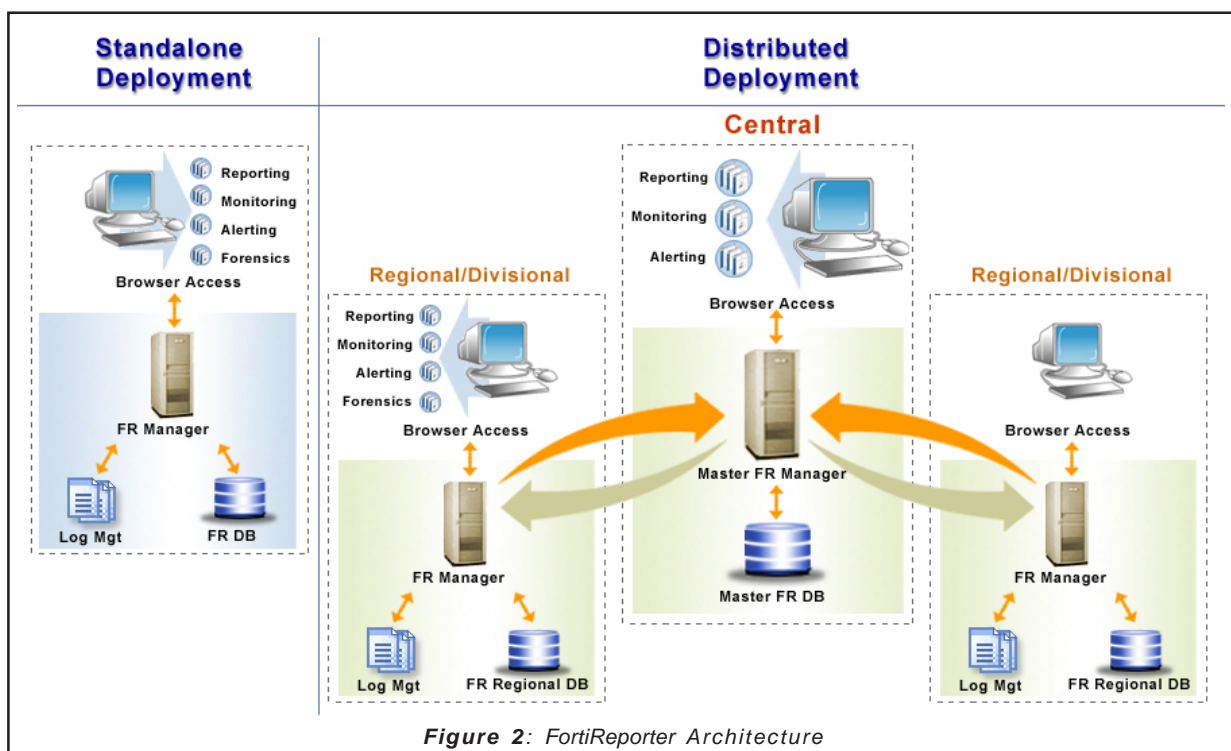


Figure 2: FortiReporter Architecture



## Log Management Key Benefits

- **Scalable**—Automatically detect, collect and aggregate log data from all licensed devices. Process 100s of GBs of log files from 1000s of devices at user defined intervals for reporting and monitoring.
- **Automated Log Archiving for Compliance** – Automatically compresses, encrypts, and archives log files for investigative analysis and regulatory compliance.

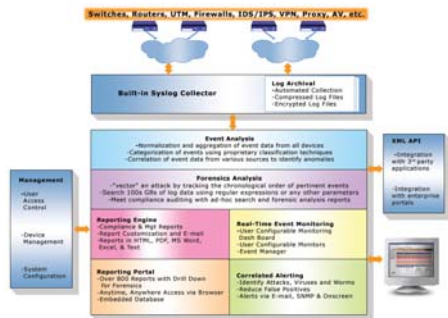


Figure 3: FortiReporter Schematic Diagram

## Monitoring and Correlated Alerting Key Benefits

- **Heterogeneous Monitoring**—Monitors security event data across the entire network of security devices in real-time.
- **Real-time Correlated Alerting**—Template-driven Alert Manager allows creation and definition of any number of alerts to reduce false positives and identify blended attacks.
- **Real-time Event Manager**—View security events data from 1000s of heterogeneous and multi-vendor network devices and prioritize actions based on business impact of each event, allowing for corrective actions before an incident occurs.
- **Dashboard**—Monitoring dashboard provides a quick, consolidated view of the environment.

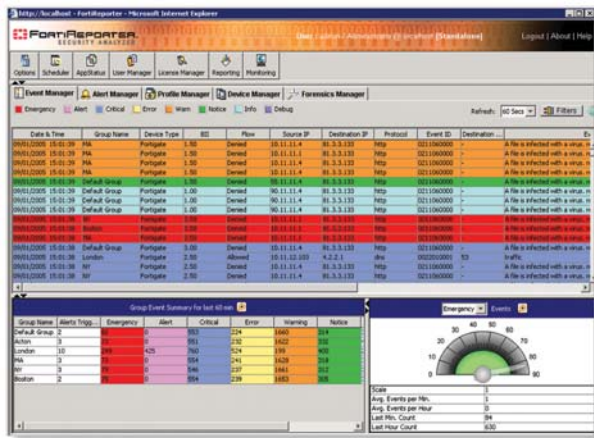


Figure 4: FortiReporter Monitoring Dashboard

## Reporting Key Benefits

- **Correlation Analysis** - Get a holistic view and understanding of hacker and virus activity by correlating data across all network devices instead of looking at each device data separately.
- **Anti-Virus Analysis** - Generates over 100 anti-virus activity-related reports that identify the presence of viruses across enterprise networks.
- **SPAM and Spyware Analysis** - Generates over 30 SPAM and spyware activity related reports.
- **Content Categorization Analysis** - Generates content categorization-related reports to help understand employee web usage patterns.
- **Reporting Portal with Powerful Drill Down** - Reporting portal gives access to over 800 reports. Powerful drill-down feature displays 2nd and 3rd level details with a single click.
- **Automated Report Generation and Distribution** - Generates over 800 easy-to-understand reports. Provides a mechanism to e-mail reports automatically to multiple recipients in HTML, MHTML, PDF, Word, Excel, and Text formats.
- **Dashboard** - Reporting dashboard provides a quick bird's eye view of the environment.

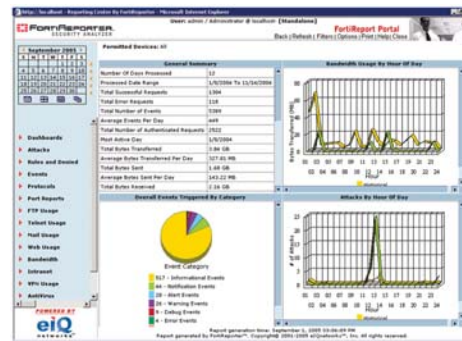


Figure 5: FortiReporter Portal Dashboard

## Forensics Analysis Key Benefits

- **Scalable Search**—An easy-to-use mechanism to search 100s of GB of log data across multiple devices based on user-configurable search criteria to aid in investigative/forensics analysis.
- **Activity Investigation**—Identify anomalies and employee corporate policy violations.

## System Requirements

- Processor - Pentium 4 – 2.4 GHz or higher
- Disk Space – 20 GB or higher
- RAM - 2 GB or higher
- Operating System - Windows Server 2000 / 2003
- Fast IO
- Internet Explorer 6.0 with Java
- IIS (for increased security)

**Australia**

Level 17, 201 Miller Street  
North Sydney 2060  
Australia

Tel: +61-2-8923-2555  
Fax: +61-2-8923-2525

**China**

Cyber Tower, Suite B-903  
2 Zhongguancun South Ave.  
Beijing 100086  
China

Tel: +8610-8251-2622  
Fax: +8610-8251-2630

**France**

4 Place de la Defense  
92974 Paris La Défense Cedex  
France

Tel: +33-1-4610-5000  
Tech Support: +33-4-9300-8810  
Fax: +33-1-5858-0025

**Germany**

Feringapark  
Feringastrasse 6  
85774 München-Unterföhring  
Germany

Tel: +49-(0)-89-99216-300  
Fax: +49-(0)-89-99216-200

**Hong Kong**

Room 2429-2431, 24/F  
Sun Hung Kai Centre  
No.30 Harbour Road, WainChai  
Hong Kong

Tel: +852-3171-3000  
Fax: +852-3171-3008

**Japan**

Kokusai Tameike Building 6F  
2-12-10 Akasaka, Minato-ku  
Tokyo 107-0052  
Japan

Tel: +81-3-5549-1640  
Fax: +81-3-5549-1641

**Korea**

27th Floor  
Korea World Trade Center  
159 Samsung-Dong  
Kangnam-Ku  
Seoul 135-729  
Korea

Tel: +82-2-6007-2007  
Fax: +82-2-6007-2703

**Taiwan**

6 F-1, 122 Xin-Hu 3 Road  
Nei-Hu District, Taipei City,  
Taiwan, R.O.C.

Tel: +886-2-27961666  
Fax: +886-2-27960999

**United Kingdom**

Quatro House  
Frimley Road  
Camberley, Surrey GU16 7ER  
United Kingdom

Tel: +44-(0)-8707-353666  
Fax: +44-(0)-8707-353667

**United States**

1090 Kifer Road  
Sunnyvale, CA 94086  
USA

Tel: +1-408-235-7700  
Fax: +1-408-235-7737  
Email: sales@fortinet.com