McAfee Firewall Reporter

Security Event Analysis and Reporting

McAfee® Firewall Reporter is an award-winning, enterprise-class security event management (SEM) reporting solution that combats hackers and threats, and quickly documents regulatory compliance.

The Challenge

Today's multi-layer IT security systems generate enormous volumes of audit and log data. Mining those volumes for actionable intelligence is an overwhelming challenge; there's too much data noise and too little information.

The Solution

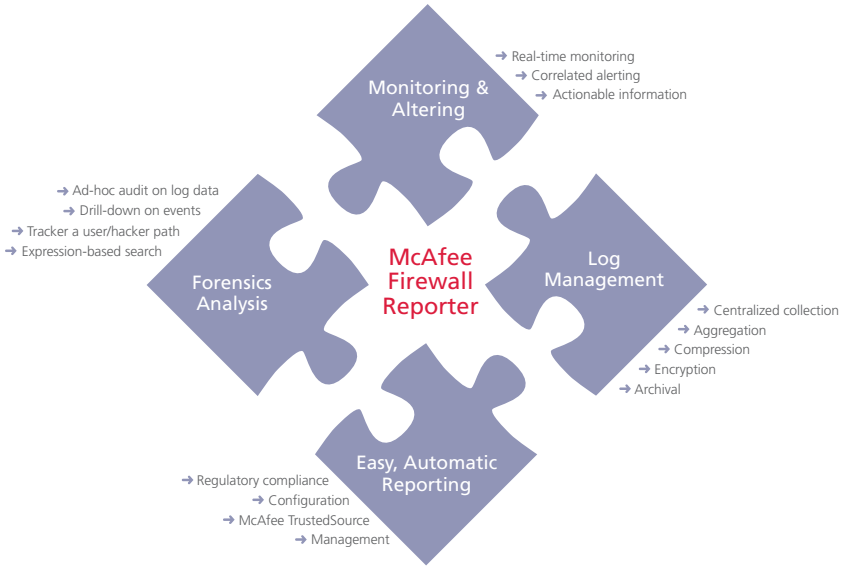
McAfee Firewall Reporter software delivers central monitoring, correlated alerting, and reporting on McAfee Firewall Enterprise (Sidewinder) and McAfee UTM Firewall audit streams. It separates real security threats from meaningless noise and provides real-time action points to keep the enterprise safer. This graphically rich tool strengthens your overall security posture, quickly documents regulatory compliance, and highlights the ROI on your McAfee Firewall investment for management.

A Central One-Stop Solution

McAfee Firewall Reporter provides a global aggregation point for log and audit data from McAfee network gateway security appliances across the enterprise. Because it's scalable to the largest environments, you receive a complete picture of enterprise security events with no hours wasted in manual analysis of individual device logs.

Actionable Information in Real Time

Collecting, monitoring, correlating, and threat alerting happen in real time to enable decisive, intelligent action. Actionable information is prioritized by business impact to minimize response time and expedite corrective action before a threat can spread or compromise sensitive information.



McAfee Firewall Reporter automatically identifies and reports security threats. Its extensive reporting capabilities and templates take the pain out of regulatory compliance

Documenting IT Security ROI

With McAfee security products at the gateway you have much less unwanted and infected traffic entering your network. McAfee® TrustedSource™ reputation-based global intelligence, for example, drops more than 70 percent of all spam instantly at the network edge. McAfee Firewall Reporter's TrustedSource global reputation report makes this incredibly positive security impact visible and tangible.

McAfee Firewall Reporter Turns Audit and Log Data "Noise" into Actionable Information:

For Everyone:

- Enjoy a personalized reporting experience – see the data you want to see, as and when you want to see it

For security administrators:

- Quickly see the organization's overall security posture
- Prove the value of your McAfee investment

For auditors:

- Receive customizable alerts to security threats
- Forensic quality data shows attack type, source, destination, port, protocol, severity, rule, etc., in real time
- Understand protocol usage by device, user, and department
- Analyze security issues and trends over time

The Personalized Dashboard Experience—Monitoring, Alerting, and Event Management

Real-time dashboard monitoring

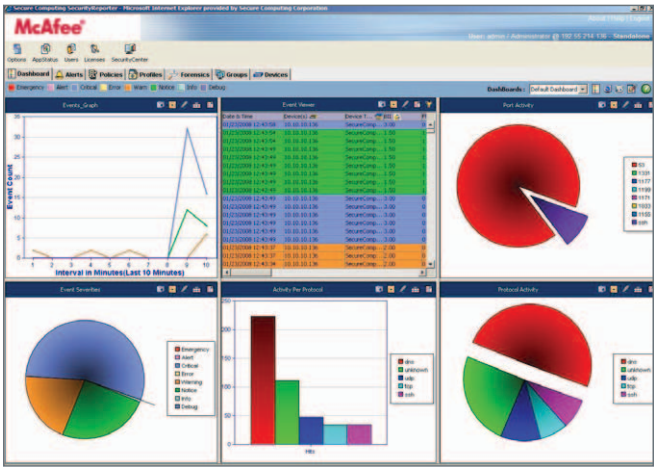
Get a quick and easy-to-understand bird's-eye view of the environment with the graphical dashboard.

- The customizable dashboard shows six security measures at a glance. Choose the security measures that are useful to you on your portal.

Alerting and event management

Create and define any number of alerts to trigger automated response strategies. Separate real threats from data noise, reduce false positives, and identify blended attacks.

- Event Manager prioritizes events based on business impact for decisive, strategic action before an incident occurs.



The dashboard – A real-time, personalized snapshot of the security information you want, as and when you want it.

Event classification	Classify events based on each policy and define which queries will be affected by the classification.
Threat level classification	Change the threat level of events based on policies.
More alerting choices	Users can set alert correlation intervals, severity, and precedence; and can negate per alert rule. Includes pattern analysis based on filter expressions.

Table 1: Advanced alerting provides personalization

Broad, exhaustive reporting—300 reports allow you to proactively secure the network, manage bandwidth requirements, and ensure appropriate usage. Historical attack reports can be generated for events categorized by hour, day, week, month, quarter, or current comparisons by each device, as well as across all devices.	
Spam, spyware, and anti-virus	Over 100 reports identify spam, spyware and viruses across enterprise networks. They provide information on virus type, source, destination, frequency, file name, extension, and protocol.
TrustedSource global reputation report	Graphically see the Spam that has been dropped at the network edge using the industry-first, reputation-based filtering of TrustedSource. Quickly document the large value of your McAfee investment.
Protocol and web usage	Provides a clear picture of protocol and web usage by user, department, and/or device. Identifies inappropriate usage including user activity associated with security appliance URL filtering.
Bandwidth usage	See bandwidth utilization by department, client, and protocol.
Regulatory compliance	Report templates take the pain out of regulatory compliance for Sarbanes-Oxley (SOX), PCI, HIPAA, GLBA, and FISMA.
Configuration management	Show configuration change detail to prove that corporate networks are configured to government requirements.

Easy, automated report generation and distribution
• Email reports ad-hoc or automatically to multiple recipients on a regular distribution list.
• Formats include: HTML, MHTML, PDF, Word, Excel, and Text

Table 2: Reporting Benefits—Advanced Security Intelligence

McAfee Firewall Enterprise (Sidewinder)

Device compatibility:

• McAfee Firewall Enterprise (Sidewinder) 7.0 or higher and Sidewinder 6.1.2 or higher

McAfee UTM Firewall

Device compatibility:

• McAfee UTM Firewall firmware version 3.1.5u3 or higher

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

5698brf_nts_firewall-reporter_1209_ETMG