McAfee Event Reporter

Centralized, fast, and scalable security event analysis and reporting

Key Advantages

- Consolidates and enhances visibility across McAfee solutions
- High-performance reporting and investigation platform—with both real-time and historical information
- Expert-built views for individual McAfee solutions and multiple McAfee solutions
- Supports integration of third-party event sources
- Optional support for McAfee Labs Global Threat Intelligence™ (McAfee GTI™) IP Reputation service
- Powered by McAfee Enterprise Security Manager and our Big Security Data database

McAfee® Event Reporter delivers consolidated, rapid, and relevant reporting for McAfee endpoint, network, and security management solutions. Expert-built content provides McAfee customers with rich real-time and historical insights into McAfee event streams in a responsive, intuitive investigation platform. McAfee Event Reporter offers both single-solution and consolidated views across multiple technologies in a variety of formats, including real-time dashboards and long-term historical reports.

Why Visibility Is Critical

The success of regulatory compliance initiatives, risk management, and security operations are directly tied to the information that security teams are able to collect, access, store, and report on. Security monitoring can no longer operate in silos. An intelligent central information repository is critical for effectively managing operational complexity, reducing time-to-respond, and meeting continuously increasing regulatory compliance requirements.

Streamline Operations

McAfee Event Reporter provides a consolidated, information-rich means of gaining a rapid visual understanding of organizational security posture, compliance with regulatory requirements, and urgent security issues that require investigation. By combining and associating events across McAfee network, endpoint, and security management solutions, enterprises now have access to a single reporting solution that supports even the largest of deployments. Benefits of McAfee Event Reporter include:

- Centralized repository for security information
- Contextual enrichment of events for effective risk management
- High-performance correlation, views, and reporting across McAfee and third-party solutions
- Extensive expert-developed content

Centralized, Extensible Event Repository

McAfee Event Reporter offers a centralized repository for years' worth of event data—in the most demanding enterprise environments. McAfee Event Reporter offers extensive local storage and seamless integration with storage area network (SAN), network-attached storage (NAS), and direct-attached storage (DAS) environments. Rapid retrieval for even the most complex queries can be performed in seconds. Query results are presented in a wide variety of real-time graphical views and reporting formats.

Contextual Data Enrichment Drives Strong Insight

Events alone are not enough to understand the state of security. To be truly helpful, event data requires additional information to help you fully understand the nature of the source, destination, and context of the communication. McAfee Event Reporter offers extensive enrichment of event data—including geo-location mapping, vulnerability and countermeasure context, and user context. You also have the option to integrate McAfee Event Reporter with McAfee Global Threat Intelligence IP Reputation service to automatically identify the reputation of external IPs. All this data is easily leveraged in McAfee Event Reporter standard and customized content.

High-Performance Correlation, Views, and Reporting Across Systems

McAfee Event Reporter consolidates security visibility across solutions through statistical and logic-based correlation, enterprise views, and centralized reporting. Organizations can move away from fragmented reporting processes to a centralized, high-speed system that not only provides insight into individual events, but also a rich understanding of security operations, risk, and requirements throughout the enterprise.

System Requirements

McAfee Event Reporter 5600

- The McAfee Event Reporter appliance provides compliant log management and collects data for correlation and analysis
- Eight TB of local storage is included, rated for 2,500 events per second
- Please refer to the McAfee SIEM device support document, located at http://www.mcafee.com/us/resources/data-sheets/ds-siem-device-support-matrix.pdf, for the complete list of supported devices

McAfee Event Reporter VM 25

- Licensed per ESX Server, McAfee Event Reporter VM is a software download for installation in a VMware environment (VMware license not included)
- It provides SIEM, enterprise log management, and event receiver functions with support for up to 25 McAfee-only devices. It is rated for 1,000 events per second.
- The VMware ESX/ESXi Server v.5.x+ with four processor cores, and 4 GB of memory is recommended. (Hardware is not included.)
- Please refer to the McAfee SIEM device support document, located at http://www.mcafee.com/us/resources/data-sheets/ds-siem-device-support-matrix.pdf, for the complete list of McAfee supported devices

Extensive Content Developed by Experts

McAfee Event Reporter offers expert-built views, reports, and correlation rules for individual McAfee solutions, multiple McAfee solutions, important security objectives (including threat detection), regulatory compliance requirements such as PCI DSS, HIPAA/HITECH, Sarbanes-Oxley, and more. You can easily customize the content to provide views unique to enterprise security risk, operations, and objectives.

Backed by Our for Big Security Data Database

As part of the McAfee Enterprise Security Manager family of products, McAfee Event Reporter is unique in its ability to store, correlate, and update massive amounts of event and enrichment data, including the McAfee GTI IP Reputation service. McAfee Enterprise Security Manager products feature a proprietary database that not only eliminates time-consuming database administration for security information management, but also is specifically built for massive intake and processing of event and relational data at extremely high speeds.

McAfee Global Threat Intelligence

An optional live feed of McAfee GTI IP Reputation data provides valuable, real-time information on external bad actors gathered from hundreds of millions of sensors around the globe, allowing you to pinpoint malicious activity on your network. McAfee Event Reporter can use McAfee GTI IP Reputation data to quickly identify conditions where an internal host has communicated with a known bad actor.

Connecting Your IT Infrastructure

Two-way integration with McAfee ePolicy Orchestrator® (McAfee ePO™) software extends visibility and control across your entire security and compliance management environment. McAfee Event Reporter can automatically collect data from McAfee ePO-managed data sources.

Supported McAfee Enterprise Security Manager solutions:

- *Virtual machine (VM)*—McAfee security devices only, up to 25 devices.
- *Appliance*—McAfee GTI and others
- For the complete list of McAfee-supported devices please refer to the McAfee SIEM device support document at http://www.mcafee.com/us/resources/data-sheets/ds-siem-device-support-matrix.pdf.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee, the McAfee logo, McAfee Global Threat Intelligence, McAfee GTI, ePolicy Orchestrator, and McAfee ePO are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2012 McAfee, Inc.
49000ds_event-reporter_0812_fnl_ETMG