McAfee
Together is power.

Compliance Made Easy

Centralize and automate monitoring and reporting

McAfee® Enterprise Security Manager is a high-performance security information and event management (SIEM) solution that correlates, stores, analyzes, and reports on events and logs to meet compliance requirements. By centralizing and automating compliance monitoring and reporting, McAfee Enterprise Security Manager eliminates time-consuming manual processes. Additionally, integration with the Unified Compliance Framework (UCF) enables a "collect once, comply with many" methodology for meeting compliance requirements and keeping audit efforts and expense to a minimum.

Compliance Challenge

Global organizations are facing the challenge of keeping pace with the volume and complexity of regulatory compliance, often answering to multiple government and industry mandates originating in different countries around the world. This can be an overwhelming task for IT organizations. Demonstrating compliance with disconnected regulations and industry mandates can be arduous, and, if there are gaps, organizations put themselves at risk of failing audits and incurring financial penalties. Beyond penalties, many organizations are simply spending far more on resources and operational costs than is necessary.

McAfee Simplifies Compliance

McAfee Enterprise Security Manager addresses today's complex compliance challenges by combining an established unified compliance framework with superior abilities to collect, retrieve, and protect the data required to assess and demonstrate compliance in real time. Its tightly integrated log collection, management, analysis, and reporting improves an organization's ability to meet compliance requirements through frameworks, streamlined workflow, and automation.

Out-of-the-Box Framework

McAfee Enterprise Security Manager makes compliance management easy and fast with hundreds of pre-built dashboards, comprehensive audit trails, and reports for more than 240 global regulations and control frameworks, including PCI-DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX, and SOX. Support for the UCF brings efficiencies to compliance by normalizing the specifics of each regulation, enabling the single set of collected events to be easily mapped to the individual regulations. Beyond the extensive out-of-the-box support, all McAfee Enterprise Security Manager compliance reports, rules, and dashboards are fully customizable.

Figure 1. Out-of-the-box compliance dashboards available in McAfee Enterprise Security Manager can be customized to meet user requirements.

Continuous Compliance Monitoring

As regulations change, the UCF is automatically updated and pushed to McAfee Enterprise Security Manager, enabling organizations to easily assess status and consistently report on the latest compliance requirements. This continuous compliance monitoring and reporting, as opposed to one-time audit driven compliance, is achieved via McAfee Enterprise Security Manager's real-time collection and analysis of logs, events, and flows. Real-time compliance monitoring dashboards complement static reports and provide analysts with an instant view of the company's most up-to-date compliance posture.

Compliance Intelligence

McAfee Enterprise Security Manager's out-of-the-box advanced correlation rules can automate key workflows for achieving and maintaining compliance. For example, rules can be set to automatically detect changes in the compliance status of the infrastructure, such as configuration changes and anomaly detection. This actionable compliance intelligence immediately triggers alerts to the appropriate teams for remediation of compliance violations in real time.

Log Collection, Storage, and Management

Collection, retention, and management of events and logs are required to meet compliance mandates. McAfee Enterprise Security Manager delivers the speed and scale to automatically store days, months, and years of events and flows for all log types, including Microsoft Windows event logs, database logs, application logs, and syslogs. In addition, it ensures that all information is available for immediate reporting and management of compliance regulations. Logs are signed and validated, ensuring authenticity and integrity required for regulatory compliance and forensics, while leveraging customizable storage pools enables logs to be stored accurately and for the required amount of time. By not altering the original log files, McAfee Enterprise Security Manager supports chain of custody and non-repudiation efforts for meeting legal requirements.

Reports in Minutes

As events and logs are continuously collected, McAfee Enterprise Security Manager offers the critical ability to rapidly sift through massive amounts of compliance data to produce the meaningful and timely reports required to answer auditors' questions. This enables the demonstration of compliance in minutes instead of hours or even days by leveraging McAfee Enterprise Security Manager's high-performance data management engine and real-time user interface to respond to queries and analytics in seconds—even on historical data over multiple years.

Dedicated Database Compliance

The McAfee Database Event Monitor is an add-on SIEM solution that expands support for compliance requirements to one of the most critical assets of IT infrastructures—databases. This non-intrusive appliance enables dedicated compliance auditing and reporting requirements for database operations. While it monitors all database transactions, McAfee Database Event Monitor provides a complete audit trail of all database activities, including queries, results, authentication activity, and privilege escalations to ensure an organization's most valuable IT assets are secure.

Compliance Beyond a Check Box

McAfee Enterprise Security Manager enables IT to go beyond simply meeting compliance mandates to integrating mandatory regulatory compliance requirements within daily operations, optimizing the overall compliance posture and workflow. This centralized solution allows security and compliance teams to collect, store, analyze, and act upon compliance requirements, risks and threats—all from a single location. As a result of using McAfee Enterprise Security Manager as the central point for ongoing monitoring, organizations can fully align security and compliance to improve operational efficiencies of both teams.

Ultimately, McAfee Enterprise Security Manager reduces the compliance burden by decreasing the time and effort needed to understand applicable mandates, continuously monitor status, produce easily customizable audit reports, and leverage compliance intelligence to make informed decisions and take action.

To learn more about SIEM solutions from McAfee, please visit: **www.mcafee.com/SIEM**.

McAfee
Together is power.

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

 61168brf_siem-compliance_0714B
JULY 2014