Solution Brief

# A Case for the Value of SIEM: The Security Evolution

**SIEM is your security intelligence partner.**

What worked in the previous decade with legacy security information and event management (SIEMs) simply doesn't address today's more dynamic security needs. Next-generation SIEM requirements around Big Data, security intelligence, operational efficiencies, and security infrastructure integrations leave many legacy SIEM customers more challenged than ever with underperforming SIEM solutions that lack both the intelligence and scalability to meet these expanded security needs. In addition, organizations face new threats, such as targeted and persistent attacks; new trends like mobile, cloud, and virtualization; shifting business priorities to meet market needs; and increased pressure around operational efficiencies.

In the past, organizations have had to make an unacceptable choice—they could either deploy an SIEM that was smart and slow or basic and fast—yet neither provided the combination of performance and intelligence required to combat today's threats. As a result, organizations now require more advanced capabilities and are expecting more from their SIEM solution. As SIEM solutions continue to evolve beyond logging and compliance reporting to become security intelligence platforms, legacy SIEM solutions often fall short in the areas of performance and intelligence.

McAfee® Enterprise Security Manager, the core of the SIEM offering from McAfee, is a unique SIEM solution that is both smart and fast because it addresses the information management challenge first. McAfee Enterprise Security Manager's proprietary information management back end, purpose-built for managing Big Data, offers the critical combination of intelligence and speed.

### How Critical Is Big Data Security Analytics?

- The amount of data analyzed by enterprise information security organizations will double every year through 2016.
- By 2016, 40% of enterprises will actively analyze at least 10 terabytes of data for information security intelligence, up from less than 3 percent in 2011.

(Source: Gartner report, "*Information Security Is Becoming a Big Data Analytics Problem, 23 March, 2013*")

## Built for the Big Data Security Challenge

Big Data Security can be extremely valuable—if you're able to use it. Legacy SIEM solutions weren't designed to integrate with such a broad number of endpoint, network, and data sources, nor intended to process such high event rates or maintain such long retention policies. These ever-growing volumes of events, as well as asset, threat, user, and other relevant data, have created a Big Data challenge for security teams. To overcome this challenge, enterprises need to move from legacy SIEM data management architectures to SIEMs that are purpose-built to handle security data management. Instead of taking a data management system and forcing SIEM functionality to work within it, SIEM solutions from McAfee start with a data management system (recognized by Gartner as a core McAfee strength in the realm of SIEM) that was built specifically for the type of operations that SIEM requires.

McAfee Enterprise Security Manager, the foundation of the McAfee SIEM solution, was designed to store massive amounts of contextual data (hundreds of millions of data points) and enrich events in real time. Delivering rapid response to both simple and complex queries, McAfee solutions have an efficient indexing system that also enables simultaneous real-time and historical operations for optimizing threat investigations and forensics. Mining Big Data to find critical security information is a key SIEM requirement. The McAfee SIEM solution leverages these large volumes of security data and goes far beyond pattern matching to provide long-term trending and weighted risk analysis.

## The Power of Security Intelligence

Historically, SIEM was simply a security tool to correlate raw events across firewalls and intrusion detection systems, and then perhaps apply some vulnerability assessment data. Even today, there are some SIEMs that rely primarily on network flow data. While all of these sources are important, they need to be enriched with application, data, and identity context to understand and prioritize events with enough intelligence to be actionable and timely.

McAfee SIEM solutions deliver the intelligence needed for quickly identifying, investigating, and resolving threats to an infrastructure. The SIEM solution calculates baseline activity for all collected information, in real time, and enable alerts of potential threats before they occur, while at the same time analyzing that data for patterns that may indicate a larger threat. In addition, McAfee Enterprise Security Manager leverages contextual information (such as vulnerability scans, identity, and authentication management systems) and enriches each event with that context for a better understanding of how security events can impact real business processes. This intelligence enables organizations to align the right data with the right people to take real-time action and make smarter decisions.

### Advantages of Security Intelligence

- Automatic establishment of security baselines in real time to easily see “normal” versus “abnormal” behavior.
- Proactive risk and threat detection based on an organization’s priorities.
- Automated or controlled launching of mitigations, such as configuration, policy, or software updates.
- Tracking and logging of all incident investigations and response activities.

## Usability

Organizations using McAfee Enterprise Security Manager can investigate everything they view on their dashboard and drill into both current and historical data for ad hoc and larger forensics investigations.

A McAfee government customer describes the power of McAfee Enterprise Security Manager’s security dashboard best when he states that “From my position, I want to know the current state of my systems and who is attacking them. What I needed was a way to roll up that collected information into one pane of glass. The only product I found that met all of my criteria and allowed that data to seamlessly integrate into one dashboard was McAfee Enterprise Security Manager.”

McAfee Enterprise Security Manager streamlines security operations, providing a centralized view of an organization’s security posture, compliance status, and prioritized security issues that require investigation. By combining and associating events across network, endpoint, and security management solutions, organizations gain a real-time understanding of the world outside (such as threat data, reputation feeds, and vulnerability status) with the systems, data, risks and activities inside their enterprise.

The usability of McAfee Enterprise Security Manager starts right out of the box, with hundreds of reports, views, rules, and alerts to immediately utilize—and all are easily customizable. Whether setting up base-lining for understanding typical network usage or simply customizing alerts, McAfee Enterprise Security Manager dashboards enable easy visualization, investigation, and reporting on the most relevant security information. Now, organizations can have comprehensive and correlated access to the data and context needed for making fast and smart decisions.

## Compliance Monitoring

When it comes to compliance, McAfee Enterprise Security Manager makes it easy to achieve, maintain, and document compliance with out of the box support for more than 240 global regulations within a Unified Compliance Framework (UCF). This integration with the UCF enables a "collect once, comply with many" methodology for meeting compliance requirements and keeping audit efforts and expense to a minimum.

Additionally, the advanced correlation rules in McAfee Enterprise Security Manager can automate key workflows for achieving and maintaining compliance. For example, rules can be set to automatically detect changes in the compliance status of an 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.

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. As a result of using McAfee Enterprise Security Manager as the central point for ongoing monitoring, organizations can more fully align security and compliance teams to improve operational efficiencies of both.

## Integrated Security

Integration across security and compliance solutions delivers more together than just the individual solutions alone and offers an unprecedented level of real-time visibility into an organization's security posture. While SIEM solutions from McAfee collect valuable data from hundreds of types of devices from various vendors across an infrastructure, McAfee Enterprise Security Manager also offers active integrations with the ePolicy Orchestrator® (McAfee ePO™) platform for policy-based endpoint management, McAfee Network Security Manager for intrusion prevention, and McAfee Vulnerability Manager for vulnerability scanning and remediation. These direct integrations with McAfee security solutions bring security intelligence to the next level—taking intelligent actions from the SIEM console. The SIEM solution leverages these integrations for changing policies at the endpoint, quarantining suspicious systems at the network, and gathering critical intelligence through vulnerability scanning, again all from the McAfee Enterprise Security Manager console. McAfee Global Threat Intelligence (McAfee GTI) integration with McAfee Enterprise Security Manager offers a constantly updated feed of known malicious IP addresses, leveraging more than 100 million global threat sensors supplied by McAfee Labs. With such integrations, the McAfee solution can automate many "first response" actions, helping organizations respond to attacks more quickly and efficiently.

The Security Connected platform from McAfee provides a unified framework for hundreds of products, services, and partners to collaborate with each other. With Security Connected solutions, such as McAfee Enterprise Security Manager, security teams can view context-specific data in real time, offering immediate visibility into an organization's security posture across their infrastructure to enable organizations to optimize response time from discovery to remediation.

**McAfee. Part of Intel Security.**
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com