SIEM Solutions from McAfee

Continuously monitor, identify, investigate, and resolve threats.

Security information and event management (SIEM), originally driven by compliance mandates, has been around for more than a decade and focused on collecting and storing logs from the network and security infrastructure. Today, in addition to compliance, SIEM solutions are being used to defend against malware and attacks that emerge from today's fast-changing threat landscape. With stealthy actors hiding behind normal enterprise activity, security organizations are using SIEM to enable actionable insights, smart decisions, and quick actions by finding threats under mountains of data. SIEM solutions from McAfee provide the performance, intelligence, and visibility to protect business assets from these ever-increasing, evasive threats.

Award-winning[1] McAfee® Enterprise Security Manager, the core product of our SIEM solution portfolio, provides key elements for optimizing threat and compliance management, including a highly tuned database, advanced risk and threat detection via contextual enrichment, policy-aware compliance reporting and centralized management. McAfee Enterprise Security Manager is a next-generation SIEM that enables your business with real-time situational awareness at the speed and scale required to identify critical threats, respond intelligently, and provide continuous compliance monitoring. SIEM appliances are available in physical or virtual appliances (stand-alone or all in one) as well as in managed service provider (MSP) offerings.

SIEM Foundation

McAfee Enterprise Security Manager for threat management and compliance

McAfee Enterprise Security Manager advances SIEM by integrating security intelligence with information management for enterprise situational awareness. By combining and associating events across network, endpoint, and security management solutions, McAfee Enterprise Security Manager delivers understanding of the world outside—threat data, reputation feeds, and vulnerability status—as well as a real-time view of the systems, data, risks and activities inside your enterprise. Additionally, by storing billions of events and flows, combined with rapid security data access, security teams gain valuable insights in minutes, not hours. This is critical for investigating low-and-slow attacks, searching for indicators of compromise, or remediating compliance controls. To optimize security operations, McAfee Enterprise Security Manager also provides integrated tools for configuration and change management, case management, and centralized management of policy—the essentials you need to improve workflow and efficiencies of your security operations team.

When it comes to compliance, McAfee Enterprise Security Manager makes it easy to achieve, maintain, and document compliance with

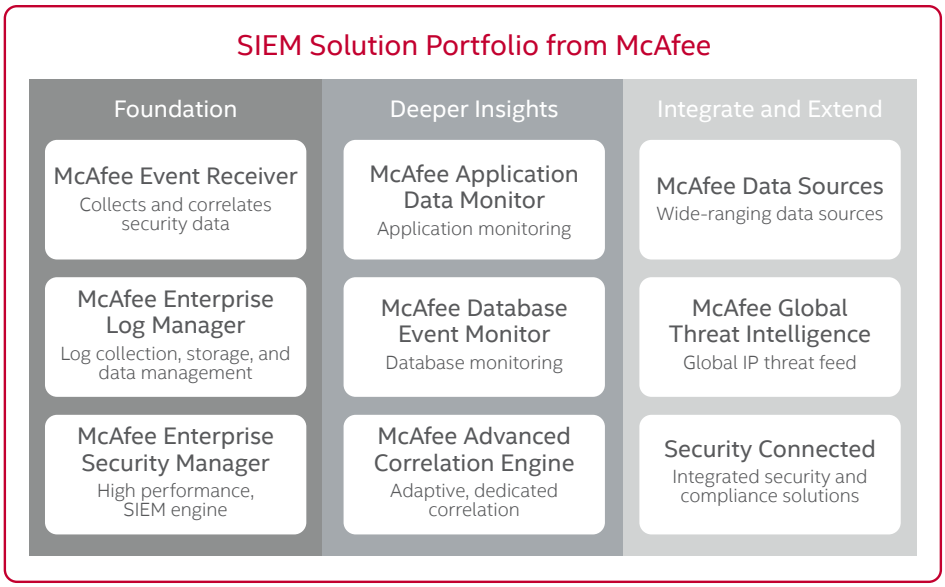

Figure 1. Integrated, extensible, high-performance SIEM solutions from McAfee.

hundreds of out-of-the box dashboards, audit trails, and reports for more than 240 global regulations. Additionally, pre-defined advanced correlation rules can automate workflows for achieving and maintaining compliance.

McAfee Enterprise Log Manager for log storage and management
McAfee Enterprise Log Manager efficiently collects, compresses, signs, and stores all original events with a clear audit trail of activity that can't be repudiated. Security events are collected and linked directly to the original record stored on McAfee Enterprise Log Manager, enabling one-click access for event management, forensic investigations, and compliance monitoring. McAfee Enterprise Log Manager accommodates different log management needs via flexible storage pools spanning local or remote storage devices and configurable retention periods.

McAfee Event Receiver for scalable log collection
McAfee Event Receiver appliances are responsible for the collection of event and flow information from hundreds of third-party devices, including firewalls, intrusion prevention system (IPS) devices, unified threat management (UTM) solutions, switches, routers, applications, servers and workstations, identity and authentication systems, vulnerability assessment scanners, and more. McAfee Event Receiver uses a variety of collection methods, including passive log collection, authenticated log collection, CEF, OPSEC, SDEE, XML, ODBC, and encrypted collection validated to FIPS 140-2 Level 2. The McAfee Event Receiver is offered as part of an all-in-one SIEM event collection and management solution or as part of a fully distributed event collection deployment using dedicated McAfee Event Receiver appliances, which are rated for several thousand to tens of thousands of events per second. Deployment models support redundancy for continuity of data collection.

Optional Solutions for Deeper Insights

McAfee Advanced Correlation Engine for additional, dedicated correlation
McAfee Advanced Correlation Engine provides SIEM solutions from McAfee with a dedicated engine to analyze large volumes of event data. The purpose-built, high-performance engine houses four correlation types, including rule-based, risk-based, standard deviation, and historical, for a real-time look at a broad spectrum of threats against high-value assets, sensitive data, or by privileged users. Preloaded with hundreds of correlation rules and dashboards, the McAfee Advanced Correlation Engine appliance allows for easy customization of existing rules and provides an easy-to-use drag-and-drop interface to create new rules.

McAfee Application Data Monitor for application layer inspection

As threat activity moves up the stack, the McAfee Application Data Monitor appliance takes security and compliance beyond security event management by monitoring all the way to the application layer. This fully integrated McAfee appliance decodes the application sessions and provides analysis from the underlying protocols and sessions into the content of the application itself (such as the text of an email or its attachments). This level of detail allows in-depth analysis of application usage, while also enabling validation of application use policies and detecting malicious or covert traffic.

McAfee Database Event Monitor for database transaction visibility

McAfee Database Event Monitor for SIEM delivers non-intrusive visibility into database transactions via detailed logging of databases and applications, monitoring access to sensitive data and with an understanding of who is accessing your data and how. McAfee Database Event Monitor is fully integrated with McAfee Enterprise Security Manager to enable database transactions for event correlation usage and includes predefined rules, reports, and privacy-friendly logging features to make compliance regulations management easy while helping you strengthen your organization's overall security posture.

Integrate and Extend

McAfee Global Threat Intelligence for enhanced threat feeds

McAfee Global Threat Intelligence for McAfee Enterprise Security Manager connects the power of McAfee Labs directly into the SIEM solution by bringing in reputation data for hundreds of millions of IP addresses. This continually updated security feed enhances situational awareness by enabling rapid discovery of events involving communications with suspicious or malicious IPs and allows security administrators to identify conditions where a known or suspicious bad actor was the source of threat activity.

Security Connected across the IT infrastructure

Integration across security and compliance solutions delivers more than the individual solutions alone and enables an unprecedented level of real-time visibility into your security posture. While SIEM solutions from McAfee collect valuable data from hundreds of types of security vendor's devices, McAfee Enterprise Security Manager also offers active integration with McAfee products and third-party solutions via a rich set of interfaces. Examples of McAfee product family connections include McAfee® ePolicy Orchestrator® (McAfee ePO™) software for policy-based management, McAfee Network Security Manager for intrusion prevention, and McAfee Vulnerability Manager for vulnerability scanning and remediation. SIEM solutions from McAfee leverage these integrations for making policy changes at the endpoint, quarantining suspicious systems at the network, and gathering critical intelligence through vulnerability scanning—all from the McAfee Enterprise Security Manager console.

The Security Connected platform from McAfee provides a unified framework for hundreds of products, services, and partners to work with each other. With Security Connected solutions, such as SIEM, security teams can view context-specific data in real time, offering immediate visibility into your organization's infrastructure-wide security posture and enabling optimized response times, from discovery to remediation.

Scalable Deployment Options

SIEM solutions from McAfee can be deployed all in one or distributed over multiple appliances, providing flexibility and scalability for your current or future needs. Hybrid delivery choices include physical and virtual appliances with high-availability options. McAfee Professional Services is available to help meet your organization's deployment objectives, accelerate time to protection, and enhance your security technology investment.

Learn More

For more information on SIEM solutions from McAfee, visit **www.mcafee.com/siem**.

1. Winner of 2014 *SC Magazine* Reader Trust Award for Best SIEM Solution.

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

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee, the McAfee logo, ePolicy Orchestrator, and McAfee ePO are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US 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 © 2014 McAfee, Inc. 61244ds_siem-family_0914_fnl_ETMG