McAfee Enterprise Security Manager


The most effective security starts with real-time visibility into all activity on all systems, networks, databases, and applications. McAfee® Enterprise Security Manager, the foundation of the security information and event management (SIEM) solution family from McAfee, delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

McAfee Enterprise Security Manager delivers a real-time understanding of the world outside—threat data, reputation feeds, and vulnerability status—as well as a view of the systems, data, risks, and activities inside your enterprise. IT can finally have complete and correlated access to the content and context needed for fast, risk-based decisions, investing resources to best effect in a dynamic threat landscape. 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—everything you need to improve workflow and the efficiency of your security operations team.

Advanced Threat Intelligence
Whether it’s network traffic, user activity, or application use, any variation from normal activity could indicate that a threat is imminent and that your data or infrastructure is at risk. McAfee Enterprise Security Manager calculates baseline activity for all collected information, in real time, and provides prioritized alerts with the goal of discovering 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 and 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 action in real time and make smarter decisions.

Critical Facts in Minutes, Not Hours
Our highly tuned database appliance can collect, process, and correlate billions of log events from multiple years with other data streams at the speed enterprises require. McAfee Enterprise Security Manager is able to store billions of events and flows, keeping all information available for immediate ad hoc queries, forensics, rules validation, and compliance.

Key Advantages
- Real-time and historical visibility for comprehensive threat detection and response.
- Prioritized, actionable information in minutes for fast threat response.
- Advanced analytics and data enrichment turn data into security intelligence.
- Compliance framework for more than 240 global regulations.

McAfee Enterprise Security Manager

[Image of McAfee logo]
Rapid access to long-term storage of event data is critical for investigating low-and-slow attacks, searching for indications of advanced persistent threats (APTs), or attempting to remediate a failed compliance audit—all of which require visibility into historical data and full access to the complete details of each specific event.

Built for Big Data
Big Data Security can be extremely valuable and these ever-growing volumes of events, as well as asset, threat, user, and other relevant data, have created a massive challenge for security teams. To overcome this challenge, McAfee Enterprise Security Manager started with a data management system (recognized by Gartner as a core strength of SIEM solutions from McAfee) that was built specifically for the type of operations that SIEM requires.

McAfee Enterprise Security Manager was designed to store massive amounts of contextual data (hundreds of millions of data points) and enrich events in real time. All that information is heavily indexed, normalized, and correlated to detect a wider range of risks and threats. Delivering fast response to both simple and complex queries, McAfee Enterprise Security Manager has 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. McAfee Enterprise Security Manager leverages these large volumes of security data and goes far beyond pattern matching to provide long-term indicators of compromise and actionable threat intelligence.

Context and Content Awareness
When contextual information is available—from vulnerability scanners, identity and authentication management systems, privacy solutions, or other supported systems—each event is enriched with that context, allowing for a better understanding of how network and security events correlate to real business processes and policies.

McAfee Enterprise Security Manager's scalability and performance enables collection of more information from more sources, including application content such as documents, transactions, and communications, providing deep forensics value. All that information is heavily indexed, normalized, and correlated to detect a wider range of risks and threats.

Optimize Security Operations
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.

The usability of McAfee Enterprise Security Manager starts right out of the box, with hundreds of reports, views, rules, and alerts to use immediately—and all are easily customizable. Whether setting up base-lining for understanding typical network usage or simply customizing alerts, McAfee Enterprise Security Manager’s dashboard enables 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.

Simplify Compliance
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. Support for the UCF brings efficiencies to compliance by normalizing the specifics of each regulation which enables the single set of collected events to be easily mapped to the individual regulations.

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. Beyond the extensive out-of-the-box support, all McAfee Enterprise Security Manager compliance reports, rules, and dashboards are fully customizable.
Connecting Your IT Infrastructure
Integration across security and compliance solutions delivers more together than any one individual solution alone can, and delivers 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 security vendor’s devices across an infrastructure, McAfee Enterprise Security Manager also offers active integrations with the McAfee® 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.

McAfee Enterprise Security Manager is integrated with McAfee Threat Intelligence Exchange. Unlike standard security approaches, this combination provides organizations with detailed, closed loop workflow from discovery to containment. Based on endpoint monitoring, McAfee Threat Intelligence Exchange aggregates low-prevalence attacks, leveraging global, third-party, and local threat intelligence. Additionally McAfee Threat Intelligence Exchange can utilize any integrated Security Connected product, such as McAfee Advanced Threat Detection, to further analyze and convict files. This approach gives organizations context-aware situational awareness of how security events impact real business processes and policies, for understanding how best to focus security efforts.

These deep integrations with McAfee security solutions bring security intelligence to the next level—taking intelligent actions from the McAfee Enterprise Security Manager console. McAfee Enterprise Security Manager 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 includes data from McAfee Labs more than 100 million global threat sensors, offering a constantly updated feed of known malicious IP addresses. With such integrations, McAfee Enterprise Security Manager 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.

Learn More
For more information on McAfee Enterprise Security Manager, visit www.mcafee.com/siem.