McAfee
An Intel Company

# McAfee Enterprise Security Manager

Discover. Respond. Comply.

Effective security starts with real-time visibility into all activity on all systems, networks, databases, and applications. McAfee® Enterprise Security Manager enables your business with true, real-time situational awareness and the speed and scale required to identify critical threats, respond intelligently, and continuous compliance monitoring. McAfee Global Threat Intelligence™ (McAfee GTI™) and McAfee® ePolicy Orchestrator® (McAfee ePO™) software integration help you detect, correlate, and remediate threats in minutes across your entire IT infrastructure.

### Key Advantages

- Actionable information in minutes instead of hours
- Massive data collection across a wide range of information sources
- Real-time threat and risk data integration and event correlation
- Immediate access to years of event and flow data
- Supports monitoring and reporting against more than 240 regulations
- Integrated tools for improved security workflow
- Flexible, hybrid delivery options include physical and virtual appliances
- High-availability options

McAfee Enterprise Security Manager revolutionizes security information and event management (SIEM) by integrating security intelligence with information management for enterprise situational awareness. We connect a real-time understanding of the world outside—threat data, reputation data, and vulnerability news—with a real-time understanding of the systems, data, 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.

Since the compliance burden continues to evolve, we consolidate audit and compliance activities within a single pane of glass to keep audit effort and expense to a minimum. We make it easier to achieve, maintain, and document compliance with unified support for the more than 240 regulations in the Unified Compliance Framework.

### 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.

Rapid access to long-term storage of event data is critical for investigating low-and-slow attacks, searching for indications of advanced persistent threats, 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.

### Massive Data Collection

A single McAfee Receiver can collect up to 18,000 events per second. The McAfee Enterprise Security Manager itself can support multiple distributed receivers, and is able to handle hundreds of thousands of events per second without compression or aggregation. With aggregation, a single appliance can support tens of millions of events per second—enough to address the demands of the largest enterprise networks.

### Advanced Risk and Threat Detection

Whether it's network traffic, user activity, or application use, any variation from normal activity could indicate that a threat is imminent, and your network is at risk. McAfee Enterprise Security Manager calculates baseline activity for all collected information across the enterprise—in real time—and alerts you of potential threats before they occur, while at the same time analyzing that data for patterns that could indicate a larger threat.

### 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.

## Connecting Your IT Infrastructure

Two-way integration with McAfee ePO software extends visibility and control across your entire security and compliance management environment. McAfee Enterprise Security Manager can automatically detect and collect data from McAfee ePO-managed data sources.

McAfee Enterprise Security Manager can also feed events (including correlated events) back into the McAfee ePO system, which can then be transferred to other SIEMs, IT governance, risk, and compliance solutions, and McAfee Security Innovation Alliance partner products.

## 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 ESM can use the GTI IP Reputation data to quickly identify conditions where an internal host has communicated with a known bad actor.

## Decisions Based on Risk and Asset Value

Integration with McAfee Risk Advisor enables real-time risk management. Complementing the McAfee GTI assessment of external risk factors, McAfee Risk Advisor (MRA) scores internal assets based on assigned value, providing you an environmental risk assessment. MRA provides accurate risk scores of end points based on asset configuration, vulnerability, and deployed controls along with available countermeasure options.

The McAfee ESM correlation engine associates the external GTI threat feeds with the internal MRA risk scores to surface the events that matter to your organization, saving you time and alerting you faster to potential problems. Visual indicators show trend activity across all dashboards for at-a-glance analysis.

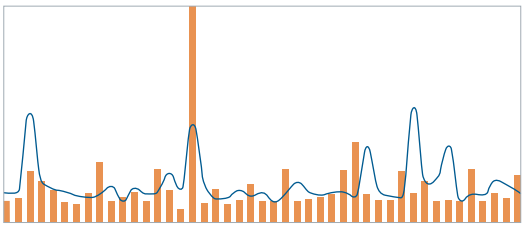

Figure 1. Dynamic baselines indicate anomalies at a glance.

## Improved Event Management and Workflows

Automated actions let you use prioritization to manage security as risks change. For example, a watch list can be set to flag dangerous activities, such as contact with a known bad IP address. Or, you might use McAfee ePO to take a range of corrective actions: issue new configurations, implement new policies, or deploy a software update.

To enhance security operations, McAfee Enterprise Security Manager also provides integrated tools for configuration and change management, case management, and centralized management of policy—everything needed to improve workflow and facilitate daily information security operations.

## Policy-Aware Compliance Management

McAfee Enterprise Security Manager makes compliance management easy with hundreds of pre-built dashboards, complete audit trails, and reports for PCI-DSS, HIPAA, NERC-CIP, FISMA, GLBA, SOX, and others. Our support for the Unified Control Framework also allows you to report your policies against more than 240 global regulations and control frameworks.

## System Specifications

| Hardware Specifications | ETM-X6 | ETM-X4 | ETM-6000 | ETM-5600 |
|---|---|---|---|---|
| Collection Rates | 300,000 events per second[1] | 150,000 events per second[1] | 70,000 events per second[1] | 50,000 events per second[1] |
| Analytical Performance | Less than 10 seconds[2] | Less than 30 seconds[2] | Less than 1 minute[2] | Less than 3 minutes[2] |
| Local Storage | 14 TB[3] + 3.2 TB Flash | 14 TB[3] + 800 GB SSD | 14 TB[3] | 8 TB[3] |

[1] Based on typical network environments using average event and flow aggregation.
[2] Indicates the average response time to generate a monthly report consisting of all events that occurred over a period of 30 days.
[3] Represents usable event and flow storage, after RAID configuration.

For more information, visit mcafee.com/ESM.

McAfee
An Intel Company

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


47101ds_esm_0612_fnl_ETMG