Data Sheet

McAfee Enterprise Security Manager

Discover. Prioritize. Respond. Adapt.

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 Intel Security, delivers real-time situational awareness and actionable intelligence at the speed and scale required for security organizations. It allows you to quickly identify, prioritize, and respond to stealthy threats and evolving risk, including the risk of audit findings.

Key Advantages

- Real-time and historical visibility shorten time to detect, contain, and remediate attacks.
- Prioritized, actionable information in minutes for fast threat triage.
- Advanced analytics and data enrichment turn a sea of raw data into a crisp and active dashboard.
- Faster decision making and action cycles increase efficiency, automation, and labor-hour output.
- Integrate security and risk management, operationalize compliance, and reduce deployment, management, and reporting complexity of the entire security ecosystem.
- Open and modular design drops quickly into existing infrastructure and adapts readily to new requirements.

McAfee Enterprise Security Manager delivers a real-time understanding of the world outside—threat data and reputation feeds—as well as a view of the systems, data, risks, and activities inside your enterprise. It offers security teams complete and correlated access to the content and context needed for fast, risk-based decisions, so you can invest resources to best effect in a dynamic threat and operational landscape. This is critical for investigating low-and-slow attacks, searching for indicators of compromise (IoCs), or remediating audit findings. To make threat and compliance management an integral part of security operations, McAfee Enterprise Security Manager also provides integrated tools for configuration and change management, case management, and centralized policy management—everything you need to improve workflow and security operations team efficiency. Additionally, the McAfee Enterprise Security Manager content packs offer fast and automated configuration of advanced security use cases as well as simplifying ongoing management.

Built for Big Data

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 uses a data management system (recognized by industry analysts and customers as a core strength of Intel® Security SIEM solutions) that was built specifically for high-volume data processing.

McAfee Enterprise Security Manager is designed to store massive amounts of contextual data and enrich events in real time. 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. McAfee Enterprise Security Manager leverages these large volumes of security data and goes far beyond pattern matching to provide long-term IoCs and actionable threat intelligence.

Critical Facts in Minutes, Not Hours

Rapid access to long-term storage of event data is critical for investigating incidents, searching for evidence of advanced attacks, 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.

intel Security

Scalable Deployment Options

- Hybrid delivery choices give you the flexibility to choose physical and virtual appliances with high-availability options, as well as MSSP options.
- Solutions that grow with you—from single-appliance deployments for smaller enterprises to distributed solutions for large enterprises.
- Highly scalable appliances enable massive data collection across a wide range of security and infrastructure assets and turn it into prioritized, actionable intelligence.

Our highly tuned appliances can collect, process, and correlate log events from multiple years with other data streams, including STIX-based threat intelligence feeds, 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.

Context and Content Awareness

When contextual information is available—threat data and reputation feeds, identity and access management systems, privacy solutions, or other supported systems—each event is enriched with that context. This enrichment delivers better understanding and accurate triage based on how network and security events correlate to asset attributes and real business processes and policies.

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

Advanced Threat Interpretation

Whether it is 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 and enriches each event with that context for a better understanding of how security events can impact real business processes.

McAfee Enterprise Security Manager's Cyber Threat Management dashboards offer enhanced real-time monitoring and understanding of emerging threats. Suspicious or confirmed threat information reported via STIX/TAXII, McAfee Advanced Threat Defense, and/or third-party web URLs can be aggregated and correlated in real time or historically (using the BackTrace feature) against event data, providing security teams with a deeper understanding of the threat propagation within an environment.

This intelligence enables organizations to align the right data with the right people to take action in real time and make smarter decisions.

Optimize Security Operations

McAfee Enterprise Security Manager streamlines security operations, providing a centralized view of an organization's security posture, compliance status, and prioritized incidents 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 baselining 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.

In addition, McAfee Enterprise Security Manager offers Content Packs to simplify security operations with 'ready-to-go' security use cases, preconfigured, offering fast access to advanced threat or compliance-management capabilities. Content Packs are prebuilt configurations for common security use cases that provide sets of rules, alarms, views, reports, variables, and watchlists. Many Content Packs provide prepackaged triggers for behaviors that may warrant additional scrutiny or automatic remediation.

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 prebuilt 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 individual solution alone can, and delivers an unprecedented level of real-time visibility into an organization's security posture. While McAfee Enterprise Security Manager can collect valuable data from hundreds of types of security vendor devices across an infrastructure as well as third-party threat intelligence, the solution also offers active integrations with the McAfee ePolicy Orchestrator® (McAfee ePO™) platform for policy-based endpoint management and remediation and McAfee Network Security Manager for intrusion prevention.

McAfee Enterprise Security Manager is also integrated with McAfee Threat Intelligence Exchange, McAfee Advanced Threat Defense, and McAfee Active Response. Unlike standard security approaches, this combination provides organizations with detailed, closed-loop workflow from discovery to containment and remediation. 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 other integrated products, such as McAfee Advanced Threat Defense, to further analyze and convict files. Incident response teams and administrators can use McAfee Active Response to look for malicious zero-day files that lay dormant on systems, as well as active processes in memory and many other IoCs. In addition, McAfee Active Response uses persistent collectors to continuously monitor your endpoints for specific IoCs, automatically alerting you if an IoC transpires somewhere in your environment. This approach gives organizations context-aware visibility of how security events impact real business processes and policies, to more effectively focus security efforts.

These deep integrations with Intel 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 and quarantining suspicious systems at the network, 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.

Intel Security delivers an integrated security system that empowers you to prevent and respond to emerging threats. We help you resolve more threats faster and with fewer resources. Our connected architecture and centralized management reduce complexity and improve operational efficiency across your entire security infrastructure. Intel Security is committed to being your number-one security partner—providing a complete set of integrated security capabilities.

Learn More

For more information on McAfee Enterprise Security Manager, visit **www.mcafee.com/us/products/siem/index.aspx** .

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