McAfee Global Threat Intelligence for Enterprise Security Manager

Bring the power of McAfee® Labs™ to situational awareness

Key Advantages

- Bring the power of McAfee Labs to SIEM
- Accurately understand the risk associated with events
- Leverage the massive threat feed of McAfee GTI without impacting performance
- Automatically receive and process new source reputations in McAfee Enterprise Security Manager
- Increase threat detection accuracy while reducing time to respond
- Quickly identify attack paths and past interactions with known bad actors associated with botnet/ distributed denial-of-service (DDoS), mail/spam-sending malware that hosts network probing, malware presence, DNS hosting, and activity generated by intrusion attacks

McAfee Global Threat Intelligence™ for Enterprise Security Manager brings the power of McAfee Labs to enterprise security monitoring. For the first time, IP reputations—gathered by McAfee Labs from more than 100 million global threat sensors—are available to a security information and event management (SIEM) solution. This constantly updated, rich feed for McAfee Enterprise Security Manager enhances situational awareness by enabling rapid discovery of events involving communications with suspicious or malicious IPs. This allows security administrators to determine what hosts have communicated or are currently communicating with bad actors and to quickly identify conditions where a known bad actor was the source of threat activity.

The Need for External Context

Security events provide information about security-related activity based on a moment in time. While SIEM has the ability to correlate these events, a number of questions are still left up to the operator to address: Is this activity acceptable? How do I know what is most urgent? How do I detect sophisticated attacks that don't make a lot of noise? Multiply these questions by a typical enterprise's daily events—more than a quarter of a billion—and it is clear that the detection of known patterns that legacy SIEM focuses on is just the tip of the security monitoring iceberg. One of the most important contextual elements behind this unknown is understanding the reputation of external systems. Until now, having this clear understanding of security events has been impossible.

The power of McAfee Labs direct to SIEM

McAfee Global Threat Intelligence for Enterprise Security Manager puts the power of McAfee Labs directly into the security monitoring flow through high-speed, highly intelligent McAfee SIEM, which is built for Big Security Data. This optional subscription service continually delivers and adjusts source reputations for more than 140 million IP addresses, bringing the context of external system reputations directly into the security event stream and quickly identifying current and past interactions with known bad actors. McAfee Global Threat Intelligence (McAfee GTI™) IP reputation is derived from the correlation of threat intelligence from all major threat vectors, leveraging more than 100 million global sensors and more than 350 researchers.

Benefits of McAfee Global Threat Intelligence for Enterprise Security Manager

- *Enhanced protection for the entire network*—McAfee Global Threat Intelligence for Enterprise Security Manager immediately detects when any node on your network is communicating with a suspicious or known bad actor and quickly understands the threat's path
- *Risk-based prioritization*—IP reputation is automatically incorporated into the McAfee Enterprise Security Manager rule-less risk scoring algorithm, automatically pinpointing the need to respond
- *24/7 threat monitoring*—McAfee Labs is constantly scouring threat information to detect newly infected and malicious systems—and when those systems have been cleaned—providing organizations with an accurate, up-to-date understanding of the global threat landscape

Specifications

Supported versions

McAfee Enterprise Security Manager 9.1 and McAfee Event Reporter Appliance 9.1

- McAfee Labs threat intelligence network: more than 100 million nodes in more than 120 counties
- Average IP reputations: varies based on threat landscape

Pinpoint malicious activity in real time

With McAfee Global Threat Intelligence for and Enterprise Security Manager, organizations now have the power to understand the IP reputation for any event, including heterogeneous firewalls, intrusion prevention systems, routers, and endpoints. Leveraging McAfee Enterprise Security Manager's dynamic watch list capability, events are automatically associated with the source reputation score, and risk is adjusted. As global threats change, McAfee GTI keeps McAfee Enterprise Security Manager updated, ensuring that servers and systems continually have an accurate reputation score. This not only helps organizations understand risk, but also pinpoints urgent issues in real time, shrinking the incident response time window and providing accurate risk analysis.

Find what you didn't know about

A core strength of McAfee Enterprise Security Managers is the ability to store, retrieve, and perform historical correlation over years' worth of data. Now, with McAfee GTI, security analysts can go back in time, over years' worth of data, to understand interactions with bad actors in the past. This is critical to detecting low and slow attacks, repeated activity from botnets, cross-site scripting, and SQL injection attempts.

Reduce time to respond

McAfee GTI integrates seamlessly with McAfee Enterprise Security Manager alarm and alerting mechanisms, ensuring that interactions with known malicious systems gain the attention they deserve.

Backed by the McAfee Database, Built for Big Security Data

There's been a lot of talk about data getting bigger, and that includes bringing the wealth of security-related knowledge of McAfee Labs to SIEM. McAfee Enterprise Security Manager is unique in its ability to store, correlate, and update the massive McAfee GTI IP reputation data store without unacceptable performance impacts. McAfee Enterprise Security Manager features a proprietary database that not only eliminates time-consuming database administration for SIEM, it also was specifically built for massive intake and processing of event and relational data at extremely high speeds. With McAfee Global Threat Intelligence for Enterprise Security Manager, customers can have confidence that McAfee GTI knowledge will be delivered in real time.

McAfee
An Intel Company

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

46502ds_gti-esm_0612_ETMG