SOLUTION BRIEF

McAfee Enterprise Security Manager and McAfee Threat Intelligence Exchange

Deliver Context-Aware, Prioritized Threat Intelligence Across Your Enterprise.

There's no doubt that organizations face significant challenges protecting their intellectual property and critical assets. Emerging threats are targeting their environments. The sheer volume of data and the complex, dynamic nature of the IT landscape make it difficult to identify and respond quickly to stealthy threats—particularly when they're hidden in an immense amount of log and event data. In order to get effective protection, you need solutions that deliver comprehensive visibility with prioritized, actionable intelligence to make better decisions and respond automatically with instantaneous speed.

Key Advantages

Instant, adaptive protection
Neutralize emerging threats in milliseconds through a self-updating security infrastructure that shares insights and takes actions instantly for faster, more effective protection.

Prioritized knowledge
Optimize risk prioritization through advanced analytics coupled with deep contextual insights on endpoint file reputation and execution.

Visibility and control
Quickly identify where threats are attempting to gain a foothold, investigate point of origin, and isolate exposure with precision and speed.

Dramatically reduced TCO
Speed and automation significantly reduce manual analysis to drive lower operating costs, streamline protection and response, and shift valuable security team resources towards strategic priorities.

As a part of the McAfee® product offering, McAfee Enterprise Security Manager and McAfee Threat Intelligence Exchange work together to provide organizations with exactly what they need to fight advanced threats. You get the situational awareness, actionable intelligence, and instantaneous speed to immediately identify, respond to, and proactively neutralize threats in just milliseconds. The combined solution brings unprecedented synthesis across endpoint events, reputation analysis, and advanced security information and event management (SIEM) correlation to quickly distill down the wealth of relevant threat information and focus efforts where they matter most.

McAfee Threat Intelligence Exchange provides an ecosystem of connected security components that work collaboratively to share insights, provide context, and act upon emerging threats. On the endpoint, the solution separates stealthy, low-prevalence attack payloads from the ongoing background noise of legitimate new files. It uses a groundbreaking reputation-based conviction model that leverages global, third-party, and local threat intelligence. Additionally, McAfee Threat Intelligence Exchange utilizes any connected security product, such as McAfee Advanced Threat Defense, to further analyze and convict files. Combined with an architecture that adapts and learns from individual encounters, McAfee Threat Intelligence Exchange enables systems to share insights and learn from each other to collectively get stronger.

McAfee Enterprise Security Manager consumes and correlates insights from McAfee Threat Intelligence Exchange and provides advanced alerting and historic views for enhanced security intelligence, risk prioritization, and real-time situational awareness. Detailed file reputation and execution events from McAfee Threat Intelligence Exchange drive analysis in the McAfee Enterprise Security Manager solution to quickly detect, understand, prioritize, and respond to threats. It provides a historic view and monitors endpoint event baselines to dynamically act on significant deviations and established thresholds while adjusting user and asset risk. McAfee Enterprise Security Manager provides a clear understanding of risk so you can make immediate corrective actions, such as issuing new configurations, implementing new policies, and deploying software updates that can proactively mitigate risk.

Enabling a Security Connected Framework with the Data Exchange Layer

McAfee® Threat Intelligence Exchange and McAfee Enterprise Security Manager leverage our proprietary data exchange layer (DXL), an ultra-fast, bidirectional communications fabric that enables information and context sharing between any connected security technologies. The dxl fabric is highly scalable and provides low-latency transactions via persistent network connectivity, allowing instantaneous communication and action across any enabled device. Products connected on the data exchange layer simply subscribe and publish to the fabric without the need for complex application programming interface (API)-based integration efforts or burdensome configurations. It marks a new era in security where all components come together to work as a single cohesive system, regardless of vendor or underlying architecture.

Actionable, Prioritized Intelligence

Unlike standard security approaches, McAfee Enterprise Security Manager working with McAfee Threat Intelligence Exchange provides organizations with detailed file-level insights coupled into a complete and automated closed-loop workflow from discovery to containment. This approach gives organizations context-aware situational awareness that clearly maps detailed security events to real business processes and policies so you can prioritize where to focus efforts.

Dynamic Mitigation

McAfee Enterprise Security Manager provides a historic view and monitors baseline activity of McAfee Threat Intelligence Exchange endpoint events. Now you can deploy an array of interactive and automated mitigations and alerts when significant deviations or established thresholds are observed. With new information of an attack or compromise in hand, McAfee Enterprise Security Manager gives incident responders tools to take real-time corrective action to lock down relevant user access or assets and then initiate the appropriate policies and countermeasures.

Detailed Incident Response

McAfee Threat Intelligence Exchange stores details on file reputation and execution to investigate and respond to low-prevalence attacks, suspicious files, and general threats. With it, you'll quickly identify where a threat exists in your environment and how it has spread. You'll also identify the first or only instance of a payload "patient zero."

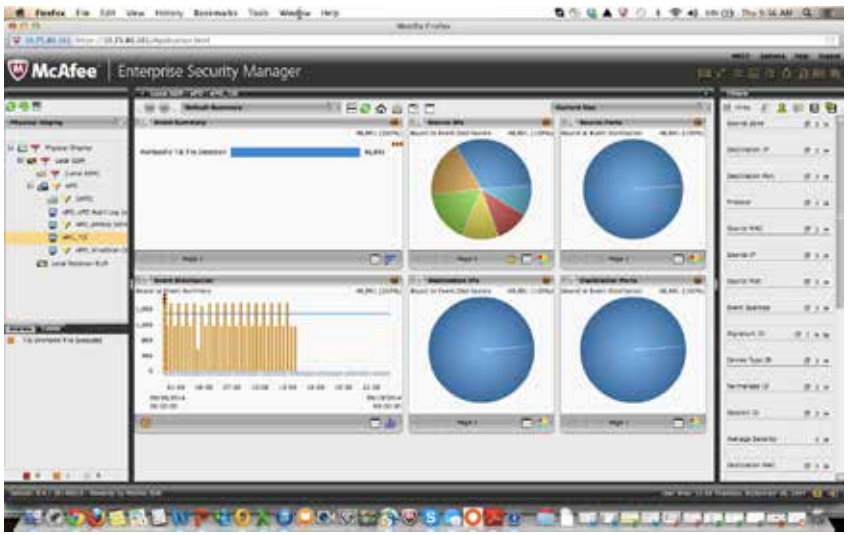

Figure 1. Actionable views with correlated McAfee Threat Intelligence Exchange events.

Advanced Protection

McAfee Threat Intelligence Exchange delivers a new kind of endpoint protection that identifies potential risks from the background noise of known good and bad files. Performing an in-depth analysis of suspect files using local, global, and enterprise-level intelligence, smart execution-time decisions are made to identify and convict both low-prevalence attacks and stealthy malware. Conviction precision is further refined through advanced logic that analyzes an array of execution and file characteristics, such as the location from which a file is executing, suspicious metadata, or if the file has been packed in an attempt to obfuscate it.

Comprehensive Threat Intelligence

McAfee Threat Intelligence Exchange integrates multiple threat data sources, including McAfee Global Threat Intelligence (McAfee GTI), third-party vendor results from VirusTotal, and local knowledge specific to your environment. Together, this information is used to accurately determine a file's reputation risk score.

Instantaneous Architecture

Instantly adapt to threats as the insights from a single encounter are propagated to all endpoints through the dxl, without the need to submit a sample or wait for an antivirus signature update. Completely automate the adaptive response for a closed-loop process or use it interactively to protect against malware, high-risk files, or simply unwanted applications. The end result drastically reduces the time it takes to contain and remediate emerging threats.

Simplified Deployment and Management

Integration between McAfee Threat Intelligence Exchange and McAfee Enterprise Security Manager is seamless across the data exchange layer. Designed as an open framework, the data exchange layer enables security components to dynamically join the McAfee Threat Intelligence Exchange without the need for extensive APIs or complex product configurations, thereby reducing errors and eliminating extensive manual effort.

Information shared from McAfee Threat Intelligence Exchange to the McAfee Enterprise Security Manager is correlated and integrated in the Enterprise Security Manager dashboard, providing administrators with a single pane of glass to review and act on threat information.

Learn More

McAfee Enterprise Security Manager provides access to historical security information and the ability to create automated watch lists while increasing the security efficiency for organizations.

http://www.mcafee.com/TIE

http://www.mcafee.com/ESM

McAfee
Together is power.

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