

Log Data Management

Integrate Log Data Reporting for Security and Compliance with McAfee ePolicy Orchestrator



McAfee Compatible Solution
• SenSage 4.0 and McAfee ePO 4.0

SenSage's log data management solution enables reporting on log data from virtually any McAfee® product and publishes summary reports directly to dashboards in McAfee ePolicy Orchestrator® (McAfee ePO™) software, McAfee's centralized security and compliance management platform. Through this integration, customers gain a 360-degree view of activity across the network to meet their compliance, security, and root-cause investigation requirements.

Business Problem

Log data management and analysis has become one of the biggest challenges for IT and security and compliance departments. To maintain regulatory compliance and address security risks, organizations now are required to collect, store and analyze this data on a daily basis, including log and event data from security and compliance solutions from vendors like McAfee.

The problem is that this data comes from many sources, in many different formats, and in such massive volumes that it can completely overwhelm IT staff. Combine this with the need to store and retain one to five years of this data, and suddenly organizations find that they have to manage tens or hundreds of terabytes of log data. In response to incidents, administrators also need to quickly perform fast, accurate investigations over months or years of data. SenSage offers a comprehensive, enterprise-class solution for managing the avalanche of data while minimizing the cost and impact to the organization.

McAfee and SenSage Joint Solution and Benefits Business

SenSage's powerful log management solution is now optimized for McAfee customers. SenSage analyzes and reports on log data from McAfee products and hundreds of other sources. The integrated solution allows McAfee customers to view and access compliance and security reporting directly within the McAfee ePO console. For further analysis, customers can seamlessly drill down from the McAfee ePO console into the full-featured SenSage Analyzer.

Integrated Reporting with ePolicy Orchestrator

SenSage reports are now integrated directly into McAfee ePO dashboards. For detailed analysis and investigations, McAfee ePO administrators can simply click on a URL to drill deeper into related data in the SenSage console. SenSage offers out-of-the-box support and reporting for a host of McAfee products, including:

- McAfee Network Security Platform
- McAfee Email and Web Security Appliance
- McAfee Vulnerability Manager
- McAfee ePolicy Orchestrator

SenSage offers 18 reports from the above McAfee sources and will continue to add support for additional McAfee products. The flexibility of the SenSage solution ensures that log data from a new or future product can be collected, stored, and analyzed in the SenSage system.

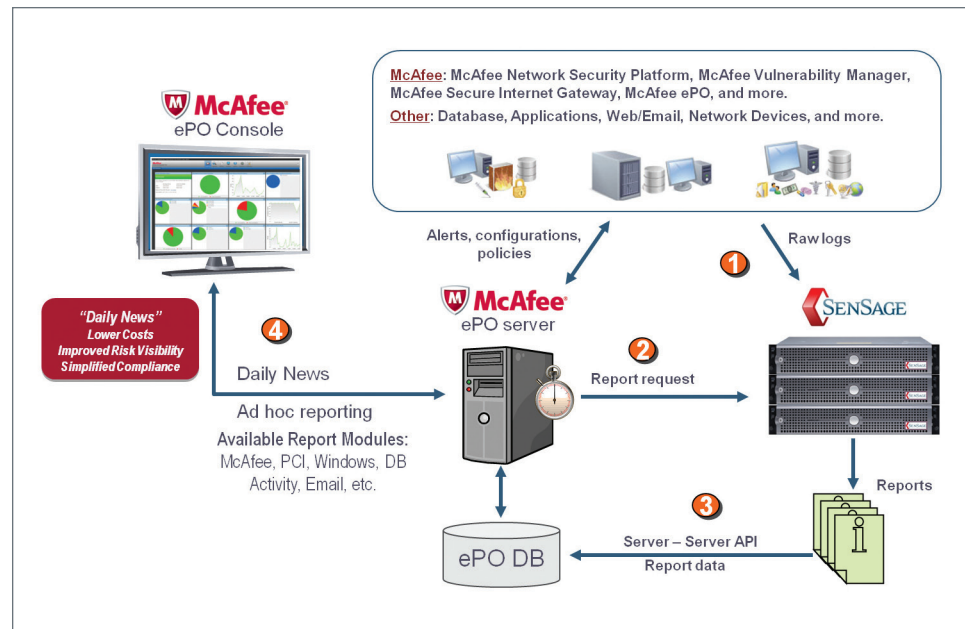


Figure 1. SenSage and McAfee integration overview.

About SenSage

SenSage provides actionable information and business intelligence on massive amounts of log and event data. Customers deploy SenSage solutions to reduce the risks associated with insider threats, system downtime and failed audits by providing faster, more granular analysis of privileged user behavior and analyzing anomalies across network, system and application activity.

About McAfee ePolicy Orchestrator (ePO) software

McAfee ePO software is the industry-leading security and compliance management platform. With its single agent and single-console architecture, ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.

