

Incident Response and Forensics

Use McAfee ePO for deploying Guidance Software's EnCase across your network

Guidance Software's EnCase[®] Enterprise product is now integrated with McAfee[®] ePolicy Orchestrator[®] (ePO[™]), allowing an organization to streamline internal digital investigations on any ePO-managed asset.

Business Problem

Organizations increasingly need the capability to perform digital investigations across the network to defend their digital assets against misuse. While some federal and state laws require rapid response when data may have been compromised, taking proper steps when an incident occurs can also reduce the risk of public embarrassment and damaging lawsuits.

McAfee ePO + EnCase Enterprise—Solution and Benefits

EnCase Enterprise provides an investigative infrastructure that allows you to investigate HR matters, suspected fraud, and external threats in a forensically sound manner from a central console with no disruption to business and network operations. By combining EnCase Enterprise with McAfee ePO, an organization can protect its data, deploy the EnCase Servlet quickly and efficiently, and monitor EnCase Servlets across all network assets managed by ePO.

EnCase Enterprise gives you the power to search, collect, preserve, and analyze vast amounts of data, and to generate detailed reports on your findings from a central location—all with minimal disruption, no matter how large and complex your network environment might be.

With McAfee ePO + EnCase Enterprise, you can:

- Reduce time to deploy EnCase and perform the analysis
- Ensure defensibility using “court validated” evidence handling technology
- Investigate multiple machines in a secure, forensically sound manner
- Preserve metadata on individual files during acquisitions
- Create logical evidence files preserving only relevant data

Leverage Your Security Management Framework

By giving administrators the ability to deploy and monitor the EnCase Servlet via McAfee's security and compliance management framework, organizations can reduce costs and increase the return on investment of their IT infrastructure. In addition, you can ensure full compliance with your internal IT processes by deploying the EnCase Servlet using ePO by leveraging the systems hierarchy already defined in ePO.

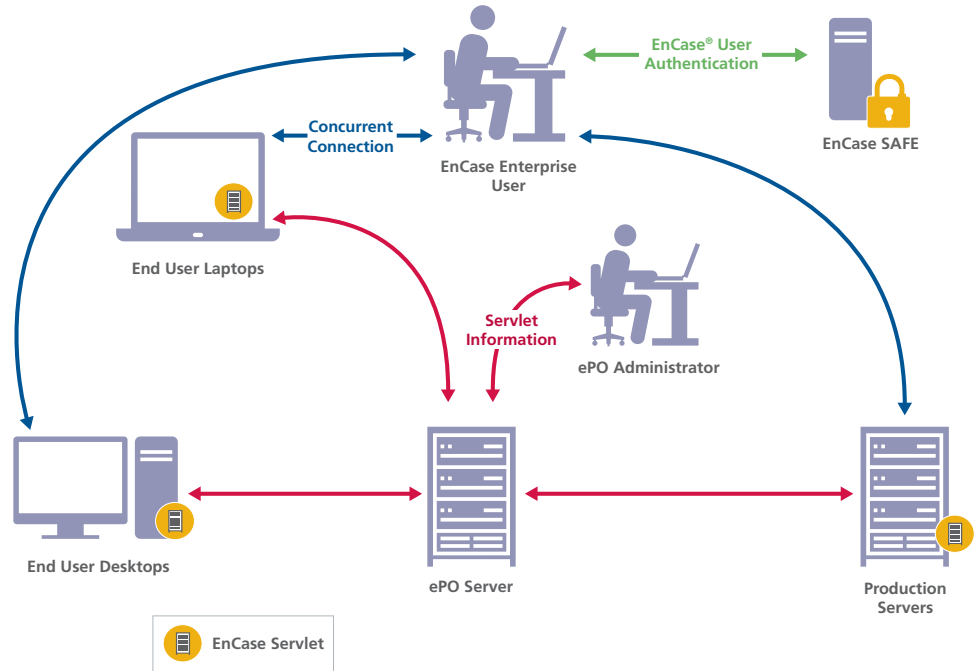
McAfee Compatible Solution

Guidance Software EnCase Enterprise 6.14 and higher and McAfee ePO 4.0

How It Works

The EnCase Servlet communicates the following information to the ePO agent:

- Installation status
- Language of the machine
- Version of servlet ePO plug-in
- Servlet status
- Directory where the servlet is installed
- Version of the installed servlet



When an incident occurs, the ePO administrator can automatically deploy an EnCase Servlet to the node under investigation via ePO. Once the servlet is installed, a user can quickly search and collect information associated with the incident using EnCase Enterprise. After the incident has been resolved, the ePO administrator can then automatically uninstall the servlet, if desired.

This rapid response leveraging ePO helps minimize the impact of incidents and reduce downtime on the end nodes, thus delivering a highly scalable solution for finding, preserving, and analyzing digital evidence.

About Guidance Software

Guidance Software EnCase® platform provides the foundation for organizations to conduct thorough and effective computer investigations of any kind, such as intellectual property theft, incident response, compliance auditing, and responding to eDiscovery requests—all while maintaining the forensic integrity of the data. There are more than 30,000 licensed users of the technology.

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.

