Solution Brief

Accelerate Incident Response and Forensics

McAfee + EnCase from Guidance Software help speed-up incident response and investigations

McAfee Compatible Solution

Guidance Software EnCase Enterprise 7.5 and McAfee ePO software 4.6

Guidance Software EnCase® products integrate with McAfee® ePolicy Orchestrator® (McAfee ePO™) software and McAfee Endpoint Encryption software, allowing an organization to streamline internal digital investigations and incident response on any McAfee ePO-managed asset or McAfee Endpoint Encryption for PC encrypted data.

Business Problem

Organizations increasingly need the capability to perform digital investigations or respond to suspected compromise across the network to defend their data 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 + EnCase—Solution and Benefits

Guidance Software's EnCase products provide investigative and incident response capabilities that allow you to rapidly investigate human resource matters, suspected fraud, and potential data breaches in a forensically sound manner with no disruption to business and network operations. By combining EnCase products with McAfee ePO and McAfee Endpoint Encryption software, an organization can protect its data, deploy the EnCase Servlet quickly and efficiently, monitor EnCase Servlets across all network assets managed by McAfee ePO software, and ensure rapid access to any and all relevant data.

EnCase gives you the power to investigate, preserve, and analyze vast amounts of endpoint data, and to generate detailed reports on your findings with minimal disruption, no matter how large and complex your network environment might be.

With McAfee + EnCase Enterprise, You Can:

- Reduce time-to-deploy EnCase and perform analysis.
- Ensure data encryption does not impede investigations.
- Implement a defensible process that ensures a strict chain of custody.
- Streamline your incident-management process, dramatically reducing time-to-respond.
- Preserve metadata on individual files during acquisitions.
- Create logical evidence files preserving only relevant data.

McAfee COMPATIBLE

Leverage Your Security Management Framework

By giving administrators the ability to deploy and monitor the EnCase Servlet via the McAfee security and compliance management framework, and authorized users the ability to easily investigate encrypted data, 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 McAfee ePO software by leveraging the systems hierarchy already defined in the McAfee ePO platform.

This rapid response leveraging McAfee ePO software 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 ePO Software

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

How It Works

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

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

McAfee
An Intel Company

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

McAfee, the McAfee logo, ePolicy Orchestrator, and McAfee ePO are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications, and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2014 McAfee, Inc.