EnCase® Endpoint Investigator

by Guidance Software

MASTER EVERY DIGITAL INVESTIGATION

GUIDANCE SOFTWARE

ENCASE® ENDPOINT INVESTIGATOR

From cyber-crime and insider fraud to class-action lawsuits and harassment allegations, IT teams are increasingly being asked to manage investigations of many kinds, often involving multiple people and computers in multiple locations. With budget pressure rising along with outsource costs and caseloads, the time is right to bring digital investigations in-house. Deployed on more than 20 million endpoints, EnCase Endpoint Investigator is helping 65 percent of the Fortune 100 and more than 45 percent of the Fortune 500 tackle all of these types of cases in-house every day.

Easily installed in about an hour, EnCase Endpoint Investigator gives your team everything you need to immediately and thoroughly search, collect, preserve, and analyze data from servers and workstations anywhere on a network—without taking systems offline or alerting users.

Laptops — Concurrent Connection — EXAMINER — Concurrent Connection — Servers

Desktops — Concurrent Connection — EXAMINER — User Authentication — SAFE

KEY FEATURES

- Easy, scalable deployment of servlets to as many target machines as needed
- Can search unallocated space for deleted data
- SAFE operates on standard laptop or desktop system
- Passive, lightweight servlets can be deployed tactically, as needed
- Requires no expensive back-end database
- Fully scalable with options to add additional examiners and concurrent connects as needed

KEY BENEFITS

- Gain remote access to multiple machines without staff travel
- Swiftly install and begin investigating in about an hour
- Get the most complete results faster with the most powerful, defensible search and collection capabilities in the market
- Discreetly investigate across the network without having to seize employee systems
- Minimize capital investment by using an inexpensive laptop as a SAFE and with no back-end database required
- Document investigations and processes with an audit trail created by the SAFE
- Ensure security of all investigations and prevent misuse with SAFE-centered authentication
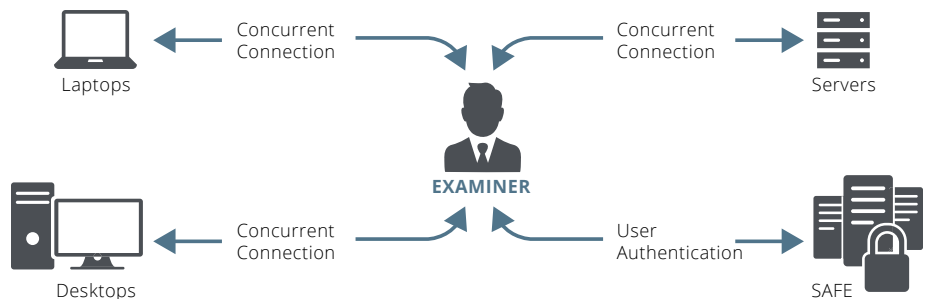
HANDLE EVERY INTERNAL INVESTIGATION

With EnCase Endpoint Investigator, you will readily find every shred of data and evidence related to:

HR Investigations:

- Sexual harassment
- Employee misconduct
- Insider threat
- Wrongful termination
- Computer misuse

Regulatory audit and compliance support:

- Sarbanes-Oxley (SOX)
- HIPAA
- Safe Harbor
- Dodd-Frank
- SEC Investigations

E-discovery collections

Security incident response

Preview and Collect Remotely: Collect and analyze electronic information on multiple remote machines simultaneously, including volatile memory and data on-disk.

Supports Multiple Platforms: Perform investigations on a comprehensive list of operating systems, including Windows, Linux, Mac, and other UNIX Operating Systems, as well as mobile devices including Android, iPhone, and Blackberry.

Discreet and Secure: Execute discreet digital investigations across multiple machines without disrupting business activity. Additionally, manage secure centralized access to target machines with examiner machine authentication and audit trail reports.

EFFICIENTLY CAPTURE POTENTIAL EVIDENCE FROM VOLATILE DATA
The Snapshot feature in EnCase Endpoint Investigator gives you the ability to quickly capture and analyze RAM from target machines—even from numerous target computers concurrently. This simplifies the process of determining commonalities or exposing anomalies, which can be critical when investigating computer security incidents. Snapshot quickly captures volatile data to reveal details about open ports, running processes, and other crucial information.

SEARCH MULTIPLE SYSTEMS SIMULTANEOUSLY
Sweep Enterprise allows investigators to scope their investigation immediately through the selection of target systems and search for data using keywords, dates, and other criteria. The Sweep Enterprise module enables investigators to:

1. Simultaneously search multiple target systems
2. Use keyword or date-specific search criteria provided by HR or counsel
3. Manage search changes and leverage past searches with new interface and functionality

SIMPLIFY MANAGEMENT OF MULTIPLE CASES
EnCase Endpoint Investigator is geared to scale from the small business to the large corporation, offering investigators the most powerful case-management features on the market.

Concurrent case management views enable greater speed and efficiency.

With EnCase Endpoint Investigator, you can:

Share Findings: Make case information viewable by more than one investigator at a time.

Manage Cases Concurrently: Review data from more than one case at a time, simplifying case-comparison analysis functions like keyword searches, search hits review, etc.

Automate Processing and Indexing: Spend more time analyzing and less time on processing and indexing.

> "EnCase Endpoint Investigator saved us more than $1 million in the first six months of its use. It also allowed us to complete a critical M&A discovery issue that would have been impossible wit h any other software or services options in the market today."
>
> - Ted Barlow, CSO and VP, Risk Management McAfee, Inc.

> "I have about 100 different duties to perform on an annual basis. With EnCase Endpoint Investigator, I'm able to take care of 80% of my workload in 48 hours."
>
> - Deputy Director, IRM Office and ISSO U.S. Federal Agency

GUIDANCE G
SOFTWARE ™

About Guidance Software (NASDAQ: GUID)
We exist to turn chaos and the unknown into order and the known—so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. Makers of EnCase®, the gold standard in digital investigations and endpoint data security, Guidance provides field-tested and court-proven applications that have been deployed on an estimated 25 million endpoints and work in concert with several other leading enterprise technologies.