



ENCASE[®] ENTERPRISE

for Corporations

The challenge of securing, monitoring and maintaining today's networks is monumental. They house corporate or even national assets, face continual assault by attackers, more insidious attacks by insiders, and must operate under strict operational and regulatory mandates.

“CEOs and CFOs must personally certify the accuracy of their company’s financial statements and the adequacy of internal controls; as a practical matter, they will need to investigate all suggestions of fraud before providing the required certifications . . . Sarbanes-Oxley virtually mandates internal investigations.”

— Morrison & Forrester

Security professionals, network administrators and investigators are desperate for access to meaningful information about the activities of users and computers so they can take decisive action.

IT: Where all investigations converge

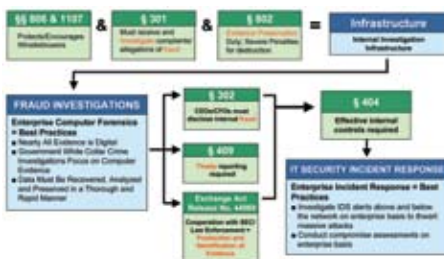
This cross-industry requirement is driving the need for an enterprise-scale platform capable of delivering comprehensive analysis, handling investigations and eDiscovery, and performing remediation. At Guidance Software we call this platform the “enterprise investigative infrastructure” and it is exactly what EnCase® Enterprise was designed to deliver. Anytime an issue comes down to finding information or conducting an investigation and then taking action based on that information, EnCase Enterprise is an optimal solution – from eDiscovery to real-time network incident response.

Using EnCase Enterprise, you can scan hundreds or thousands of nodes at unprecedented speeds, understand at the deepest level what is stored or occurring on your machines, and if necessary, remediate improper activity without disrupting operations.

Mitigating the monetary and business impact of fraud

Intellectual property theft, organizational policy violations and other types of fraud rarely occur in a vacuum. There are almost always warning signs of malicious activity long before it negatively impacts the business. By understanding these warning signs and proactively monitoring and investigating the activity associated with them, Guidance Software enables companies to drastically reduce their exposure to risk and maintain compliance with critical statutes such as Sarbanes-Oxley.

The key to this proactive approach is the investigative infrastructure provided by EnCase Enterprise. It enables investigators to reach across the network in a forensically sound manner with minimal effort, and analyze and capture the information necessary to understand what users are or have been doing. This capability makes it possible for companies to catch and respond to issues before they cause financial loss or loss of reputation.



Fraud prevention is not just good business, it's necessary for Sarbanes-Oxley compliance



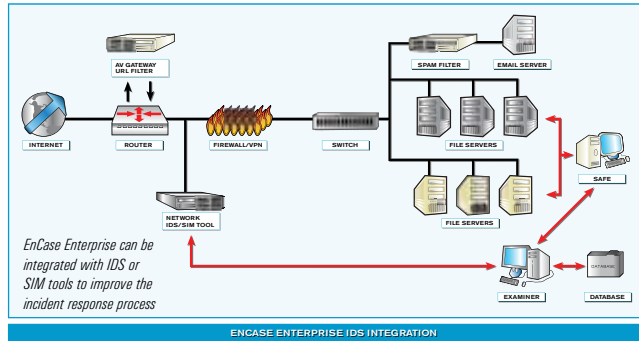
EnCase Enterprise enables a proactive approach to fraud detection and mitigation that allows companies to reduce exposure to the unique risks of their industry.

Maintain business continuity through improved incident response

In addition to the deep forensic analysis provided by EnCase Enterprise, its investigative infrastructure is a platform for advanced incident response. With EnCase Enterprise, a security specialist can quickly dive into the state of a machine to identify all running processes, including hidden ones, differentiate between

malicious and unauthorized applications, identify all open ports and files, determine user activity, and more. If malicious or unauthorized activity such as a virus outbreak or hacking incident is identified, you can automatically or manually remediate the issue quickly and easily regardless of the size or type of the event.

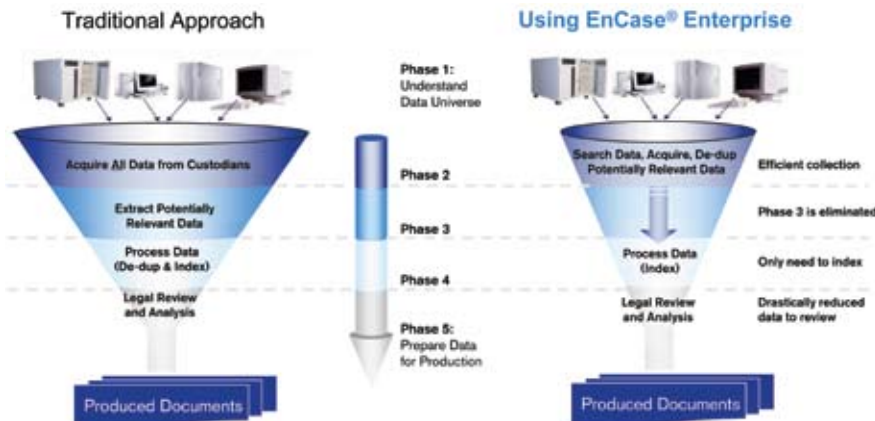
By combining these core incident response capabilities and an ability to integrate with leading monitoring technologies such as IDS and SIM systems, you can automate the incident response and analysis process – and respond to the most advanced and dangerous security threats.



Drastically reduce the cost and burden of eDiscovery

Responding to legal discovery requests stemming from lawsuits, merger and acquisition activity, or even more generic audits, is an inefficient process at best. The manual approach of investigating machine-by-machine is far too costly, disruptive, inconsistent and inherently inaccurate.

The investigative infrastructure provided by EnCase Enterprise is superior to traditional approaches. It can conduct parallel searches of large numbers of machines in a consistent, automated manner and collect only the information that is relevant, drastically reducing the cost and burden of eDiscovery. This is accomplished through our unique data collection process. You define criteria up front and capture only information that is relevant, significantly reducing the amount of data collected and the cost of hosting, processing and reviewing that data. And because the product is based on the forensic technology of EnCase, everything collected is admissible in a court of law and has the backing of extensive case law from around the world.



EnCase Enterprise significantly reduces the volume of data and the costs associated with eDiscovery by improving the data collection process. It eliminates several steps of the production process (phase 3 and much of phase 4), as shown above.

Fraud Prevention at Work

The heart of technology companies is closely tied to intellectual property. So when five key developers recently resigned from a large technology firm, it raised a warning flag. Fearing a violation of their key IP, the security team used EnCase Enterprise to investigate the activity of these developers during the weeks prior to their departure.

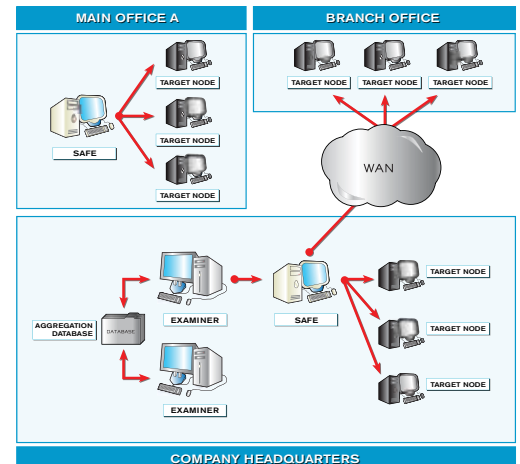
Through forensic analysis of their computers, investigators determined that these developers had downloaded millions of lines of critical code onto thumbnail drives. In addition, e-mail and Instant Messenger correspondence between them revealed their intention to use the stolen IP to set up a competing company. Using this conclusive evidence, the company obtained legal injunctions barring these individuals from competing or using the stolen code.

How EnCase Enterprise works

EnCase Enterprise is a powerful, network-enabled, multiplatform enterprise investigation solution. It brings law-enforcement grade computer investigative technology to the large and mid-market enterprise, giving you unprecedented incident response and analysis capability. Information security professionals, auditors and incident response teams can now reach any computer on the network within seconds and analyze, search and preserve volatile and static data without disrupting operations.

EnCase Enterprise is built on four core capabilities that enable its broad range of functionality:

- **Deep system analysis:** EnCase Enterprise offers the same thorough forensic analysis as EnCase Forensic and much more. It has the power to uncover hidden and deleted files, detect rootkits, search for documents, identify rogue processes, reconstruct Web and e-mail activity – even decrypt certain types of encryption and identify unauthorized network communications. And if necessary, the data gathered will stand up in courts worldwide.



- **Parallel analysis:** EnCase Enterprise quickly analyzes large numbers of machines at the same time, harvesting critical information about the state and contents of the machines. Parallel analysis is the core capability that enables EnCase Enterprise to produce enterprise search and incident response speeds that dwarf those of competing technologies.
- **Remediation:** Once you identify a malicious event, EnCase Enterprise helps contain and control it. In nearly all instances when responding to incidents, you can see the issue. But doing something about it requires shutting down at least a portion of the network, not doing anything, or using third-party tools to remediate. With EnCase Enterprise, you can document the incident in detail, then reach out to compromised machines and remediate the problem.
- **Integration:** EnCase Enterprise can be integrated with a company's existing security infrastructure to provide real-time automated incident response. Alerts generated by monitoring technologies like IDS and SIM trigger automated responses by EnCase, enabling security professionals to respond to hundreds and potentially thousands of security alerts a day – within moments of an event taking place.



Count on Guidance Software expertise

Founded in 1997, Guidance Software is recognized worldwide as the industry leader in investigative technologies. Its EnCase® solutions provide the foundation for both law enforcement and corporate enterprise investigations that enable corporate, government and law enforcement agencies to conduct effective investigations of all types, respond promptly to eDiscovery requests, and take decisive action in response to external attacks, all while maintaining the forensic integrity of the data. More than 20,000 investigators depend on EnCase software, and more than 5,000 investigators attend Guidance Software's forensic methodology training annually. Validated by numerous courts worldwide, EnCase is also frequently honored with top security awards from eWEEK, SC Magazine, Network Computing and others.

215 North Marengo Avenue, Pasadena, CA 91101 | Ph: 626.229.9191 | Fax: 626.229.9199 | www.guidancesoftware.com