

ENCASE ENTERPRISE

FOR CORPORATIONS

**The Complete, Cutting-Edge Investigative
Infrastructure for Corporations**



“ EnCase Enterprise 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 with any other software or services options in the market today.”

– Ted Barlow, CSO & VP, Risk Management, McAfee, Inc.

Bring real-time incident response, efficient and accurate eDiscovery and the world's leading forensic investigation capabilities in house with the only enterprise-wide investigative platform on the market. . .

NETWORK-ENABLED

SCALABLE

AUTOMATED, TARGETED eDISCOVERY

REAL-TIME INCIDENT RESPONSE

THE DEEPEST LEVEL OF FORENSIC ANALYSIS AVAILABLE

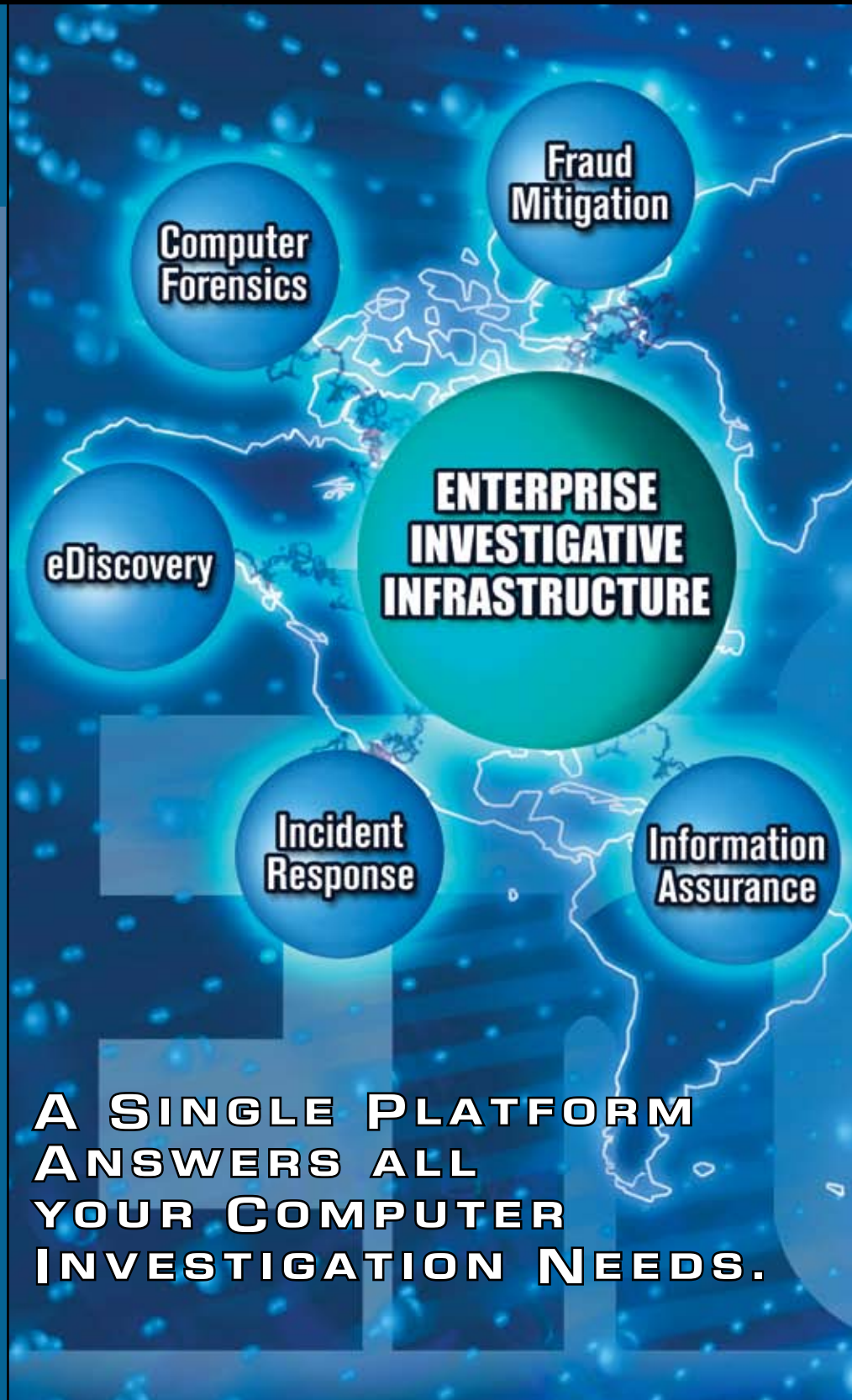
ABILITY TO SCAN THOUSANDS OF MACHINES IN MINUTES

DETAILED REPORTING AND ANALYSIS

UNPARALLELED REMEDIATION CAPABILITIES

The egregious costs, regulatory risks and business disruption associated with the traditional methods of forensic-level investigations, eDiscovery and incident response can handicap corporations of any size.

The answer is EnCase Enterprise, an enterprise-scale platform that integrates with your existing security infrastructure to deliver comprehensive analysis, forensic-level investigation, eDiscovery and remediation. You can scan 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. With EnCase Enterprise, you will experience unbelievable cost savings and ensure your compliance with critical regulations such as Sarbanes-Oxley, GLBA, NIST and others.



**A SINGLE PLATFORM
ANSWERS ALL
YOUR COMPUTER
INVESTIGATION NEEDS.**

AUTOMATED eDISCOVERY

"The highly flexible search and analysis capabilities of EnCase® Enterprise software enabled investigators to reduce the amount of data pulled by a least an order of magnitude. Processing fees associated with this investigation would've been on the order of about \$300,000 had Halliburton used traditional data-gathering methods. Net savings in that case were on the order of \$250,000."

— Ronald Perkowski, Senior Counsel, Halliburton

The traditional process of electronic discovery is fragmented. Manual collection results in delays, the inadvertent destruction of data and over-collection of irrelevant data. This drives up costs, exposes you to the risk of severe court penalties and could ultimately force you to compromise your litigation strategy.

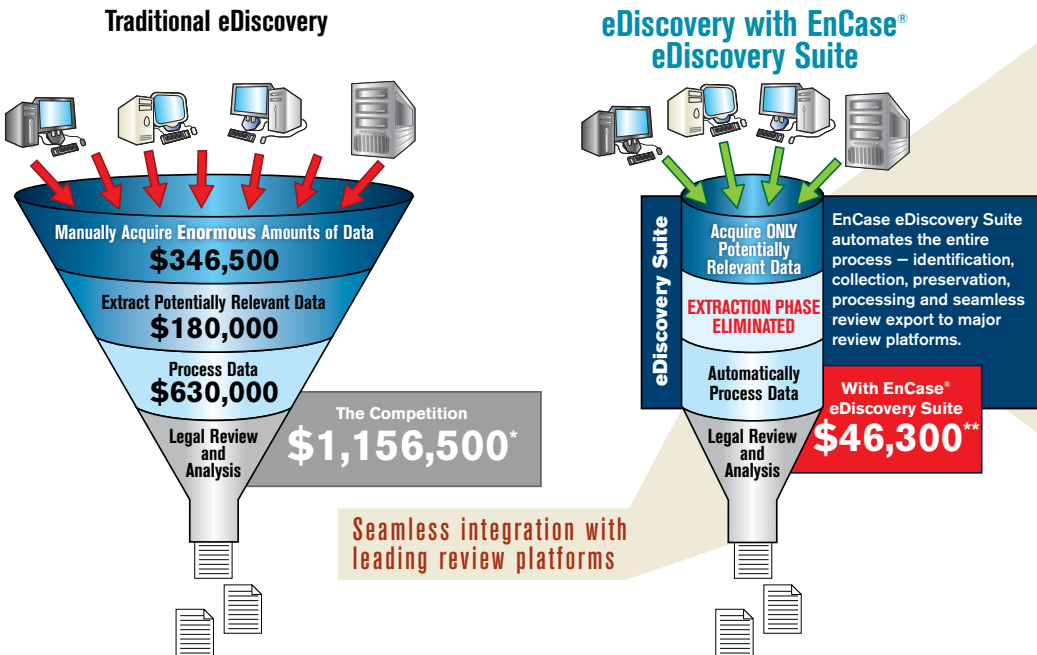
EnCase Enterprise can perform collections on thousands of machines across the enterprise, from a central location, with little manpower and no travel required in most cases. It enables you to conduct targeted keyword searches, culling at the point of collection, so you capture only potentially relevant data. Furthermore, because the forensic technology

of EnCase Enterprise has the backing of court precedent around the world, you can be confident that your collection process and the resulting data are defensible in court.

The eDiscovery solution also allows you to do a proactive eRecords management audit to ensure all data is compliant with your policies. It identifies all noncompliant records with unparalleled speed and accuracy. You can automatically search by any combination of select criteria and generate a detailed report of all records that violate your records management policy. In addition, you have the ability to preserve and erase noncompliant records.

ONLY ENCASE SOLUTIONS CAN DO THIS. . .

- Automate and streamline the collection process for around-the-clock productivity.
- Collect only potentially relevant data by culling at the point of collection.
- Preserve key metadata on an individual-file basis.
- Integrate seamlessly with leading review platforms.
- Scale to cases from a few megabytes to terabytes of data.
- Automate the reporting and auditing of all collection and processing activities.
- Work transparently; you never have to take the servers offline.

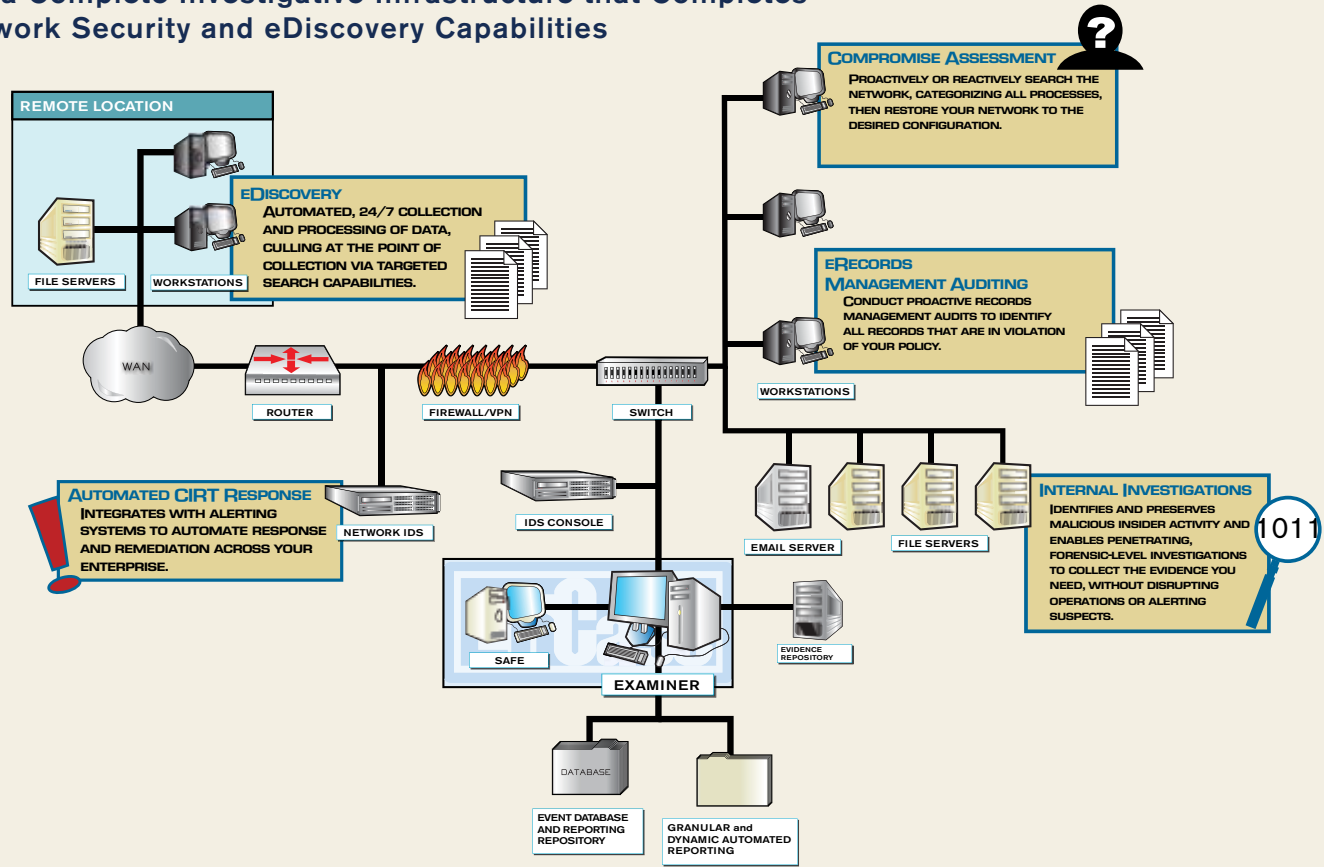


* Assuming leading competitor extends a 10% discount from published rates due to size of the engagement

** See cost calculations set forth in the brochure, *EnCase Enterprise Substantially Reduces eDiscovery Costs: An ROI Analysis*.

ENCASE[®] ENTERPRISE

Provides a Complete Investigative Infrastructure that Completes Your Network Security and eDiscovery Capabilities



INTERNAL, FORENSIC-LEVEL INVESTIGATION

"It's a sad fact that many a network manager will skip this review. This in spite of Sarbanes-Oxley, HIPAA, and Gramm-Leach-Bliley. This in spite of identity theft, corporate espionage, and a bucket full of other white-collar crimes. Network managers will avoid this review because these are worst-case scenarios, and it's easier not to think about them than it is to rationally consider their potential costs. Mitigating these costs, both soft and hard dollar, is precisely what Guidance Software's EnCase Enterprise is designed to handle."

— InfoWorld

EnCase Enterprise enables investigators to reach across the network from a central location to securely investigate multiple machines simultaneously, at the disk and memory levels. This allows companies to identify and respond to any type of organizational issue, such as fraud, intellectual property theft, employee malfeasance, wrongful terminations and other types of employee-integrity issues, before

it causes financial loss or damage to reputation. With EnCase Enterprise you have the power to conduct a penetrating, forensic-level investigation to locate and preserve the evidence you need to make critical decisions and protect your assets – without disrupting business or alerting suspects. It drastically reduces your exposure to risk and maintains your compliance with critical regulations, such as Sarbanes-Oxley.

ONLY ENCASE SOLUTIONS CAN DO THIS. . .

- Audit individual or multiple machines running on Windows, Linux, Solaris or Mac OS X for sensitive information, unauthorized processes and network connections.
- Investigate multiple machines with different operating systems simultaneously in a secure, consistent and forensically sound fashion.
- Automate any task, drastically reducing investigation time.
- Provide pre-built machine profiles that focus on only the relevant information.
- Preview computers to determine whether relevant evidence exists.
- Provide cutting-edge acquisition capabilities, including metadata preservation on individual files.
- Create logical evidence files to preserve only relevant data – no need to capture the entire hard drive.

REAL-TIME INCIDENT RESPONSE

"Coupled with the right training, EnCase® Enterprise has the potential to bring accurate closure to every intrusion alarm. As regulatory pressure increases to protect consumer data, due diligence can come in the form of EnCase Enterprise."

— InfoWorld

EnCase Enterprise integrates with your network content monitoring, SIM and IDS tools to automate the incident response and investigation process. Information security professionals, auditors and incident response teams can now reach any computer on the network within seconds to analyze, search and preserve volatile and static data without disrupting operations.

EnCase Enterprise is the only tool that enables deep, real-time response and investigation across multiple operating systems, simultaneously. If malicious or unauthorized activity, such as intellectual property theft, unauthorized communications, virus outbreak or

hacking incident is identified, you can automatically or manually preserve critical information and remediate the issue quickly and easily, regardless of the size or type of the event.

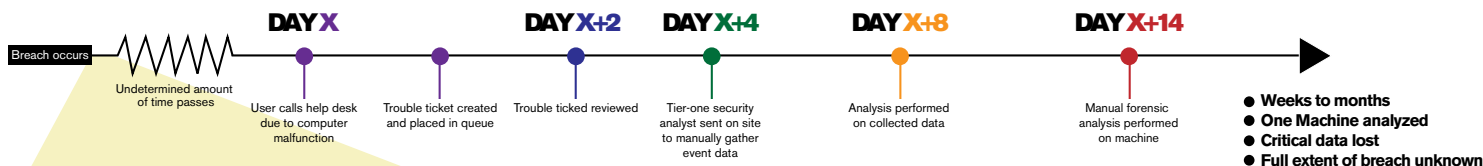
In addition to having cutting-edge response capabilities, it is critical that companies take a proactive approach to reducing risks. EnCase Enterprise provides you and your organization with the means to truly achieve visibility into the state of your network. The solution's compromise assessment capabilities allow you to audit your network proactively to understand what is running and how that picture deviates from your existing policies.

ONLY ENCASE SOLUTIONS CAN DO THIS...

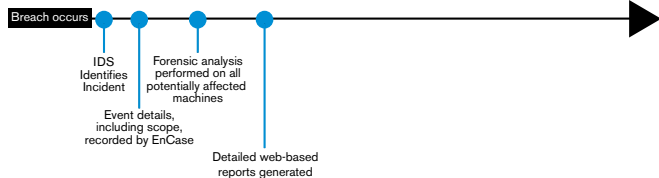
- Fields alerts generated by IDS, SIM and content monitoring tools to identify meaningful events and begin analysis.
- Scan more than 30,000 machines per hour for malicious and unauthorized activity.
- Analyze system Snapshots across time to obtain a detailed analysis of the impact of a computer attack and the point of entry.
- Find and remediate zero-day events and other malicious code.
- Application descriptors and machine profiles allow you to focus on only the relevant data during incident response or an audit.
- Allows full compliance with the NIST *Computer Security Incident Handling Guide*.

THE ENCASE ENTERPRISE DIFFERENCE

Traditional Incident Response Timeline



Seconds...



Incident Response with EnCase® Automated Incident Response Suite

- >Entire process takes seconds.
- >All potentially affected machines analyzed.
- >Critical data preserved.
- >Full extent of breach realized.

DEPTH OF ANALYSIS

	EnCase IR/ Compromise Assessment	Typical Auditing Tools
Detect Running Processes	✓	✓
Detect Hidden Processes	✓	⊘
Detect Renamed Processes or Drivers	✓	⊘
Detect Running Services	✓	✓
Detect Injected DLLs	✓	⊘
Detect Rootkits	✓	⊘
Identify Current Logged-on User	✓	✓
Enumerate Autostart Registry Keys	✓	⊘
Detect Hidden Ports	✓	⊘
Identify Hidden Registry Keys	✓	⊘
Provide Detailed Reporting	✓	⊘
Machine Profiling	✓	⊘

ABOUT GUIDANCE SOFTWARE

Founded in 1997, Guidance Software is recognized worldwide as the industry leader in computer investigation solutions. 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 computer investigations of all types, respond promptly to eDiscovery requests, and conduct rapid and thorough internal investigations involving digital evidence, all while maintaining the forensic integrity of the data. More than 20,000 investigators depend on EnCase software, and more than 4,000 investigators attend Guidance Software's forensic methodology training annually. Validated by numerous courts worldwide, EnCase software is also frequently honored with top security awards from *eWEEK*, *SC Magazine*, *Network Computing* and others.