

ENCASE ENTERPRISE

FOR EDUCATION

Achieve law-enforcement-grade investigative capabilities and cutting-edge incident response, regardless of budget constraints.



IDENTIFY AND RESPOND TO ANY TYPE OF ORGANIZATIONAL ISSUE BEFORE IT CAUSES DAMAGE. . .

Network visibility and the ability to respond to incidents has become critical to educational institutions from elementary schools to universities. Furthermore, with new regulations requiring public disclosure of incidents when personal records are compromised, you need to be prepared to deal with any type of computer incident – before it happens.

Hacking, blackmail, abusive emails, adult web content, theft of personal information, emails containing threats to the school or its students – these are the challenges educational institutions face. These are the challenges EnCase® Enterprise is engineered to overcome.

Harness the power of your network to protect your students, your faculty and your institution.

Court-approved and widely used by law enforcement officials, EnCase® software has long been utilized to investigate cyber crimes, track down child predators, and investigate other malicious activity by way of computer forensics. EnCase Enterprise extends this solution to networked environments to create an infrastructure

that allows investigators to securely investigate multiple machines simultaneously, at the disk and memory levels, without taking computers offline. This allows you to identify and respond to any type of issue before it becomes a serious problem.

With EnCase Enterprise you have the power to conduct a penetrating, forensic-level investigation to locate and preserve the evidence you need to protect your students, the faculty and the institution – without disrupting daily operations or alerting suspects. It drastically reduces your exposure to risk and maintains your compliance with state and federal regulations.

Because EnCase Enterprise closely maps to generally accepted best practices put forth by the National Institute of Standards and Technology, a school is insulated from claims of negligence that often result from certain types of incidents. This investigative infrastructure with its capability to perform incident response on private networks is currently implemented at many *Fortune* 500 companies, government agencies and various universities nationwide.

Transitioning from social security numbers to student ID numbers?

Use the power of EnCase Enterprise to conduct network sweeps during your transition from social security numbers to identification numbers. Simply conduct SSN and other keyword searches to identify computers that host the confidential data you want to locate; collect the target documents; and then remediate – all from a central location.

Specially Priced Bundles for K–12 and Universities

In consideration of your strict budget constraints, we are now offering the EnCase Enterprise solution in specially priced bundles tailored to K–12 school districts and universities. This solution allows schools to enforce their policies and protect their students, their confidential information and their organizational integrity. With EnCase Enterprise you will be able to respond to network security breaches and inappropriate conduct in a manner that reduces liability and mitigates overall impact from both a legal and technical perspective.

EnCase Enterprise delivers several key capabilities that can scale to the largest organization or enterprise network:

NETWORK-ENABLED: Securely investigate machines over the LAN/WAN from a central location, without disturbing operations.

BROADEST OPERATING SYSTEM SUPPORT: Investigate computers running on Windows, Linux, Solaris, Mac OS X and AIX.

AUTOMATED, TARGETED SEARCH CAPABILITIES: conduct automated SSN and other targeted searches to identify computers that host confidential data and collect documents in question – all from a central location.

IDS/SIM/CMS INTEGRATION CAPABILITIES PROVIDES REAL-TIME RESPONSE: Use the EnCase Automated Incident Response Suite to integrate the EnCase Enterprise platform with your IDS, SIM and content monitoring tools to field alerts, provide real-time intrusion analysis and investigation into events.

SCAN THOUSANDS OF MACHINES IN MINUTES: up to 30,000 per hour for volatile data to detect and kill unapproved processes and other malicious activity.

SMART EVIDENCE COLLECTION: No other forensic tool gives organizations the ability to forensically preserve only the relevant evidence, without capturing the entire hard drive.

FORENSIC ANALYSIS: EnCase Enterprise provides the same thorough forensic analysis as EnCase Forensic. It allows the investigator to understand exactly what a perpetrator did on a given machine and, if necessary, use that information in a court of law.

UNPARALLELED REMEDIATION CAPABILITIES: the only tool that can quickly pinpoint relevant data, both volatile and static, across multiple file systems, and surgically extract, kill or wipe remotely and without disruption.

With EnCase® Enterprise fully integrated into your school, you will be able to perform various live, network-enabled functions from a centralized location:

- Investigate inappropriate web surfing.
- Search the contents of files for inappropriate images, photos and movies.
- Identify traces of abusive behavior in emails and stored documents.
- Protect highly sensitive information such as tests, grades and confidential student/teacher data (social security numbers, addresses, etc.).
- Enforce computer use policies.
- Respond to network breaches and identify compromised systems.
- Identify rootkit and rogue process propagation.
- Universities can ensure their compliance with HIPAA.

EnCase Enterprise Depth of Analysis	Typical Auditing Tools
✓ Detect running processes	✓
✓ Detect hidden processes	✗
✓ Detect renamed processes or Drivers	✗
✓ Detect running services	✓
✓ Detect injected DLLs	✗
✓ Identify currently logged-on user	✓
✓ Autostart registry keys	✗
✓ Detect hidden ports	✗
✓ Create machine profiles	✗
✓ Port-to-process mapping	✗
✓ Provide detailed reporting	✓
✓ Remediate	✗

Associated Press reports on a university's drop in donations due to data thefts:

“While the university received 4,882 donations in May and June last year, it received 3,693 in those months this year... The computer breaches exposed about 367,000 files containing Social Security numbers, names, medical records and home addresses.”

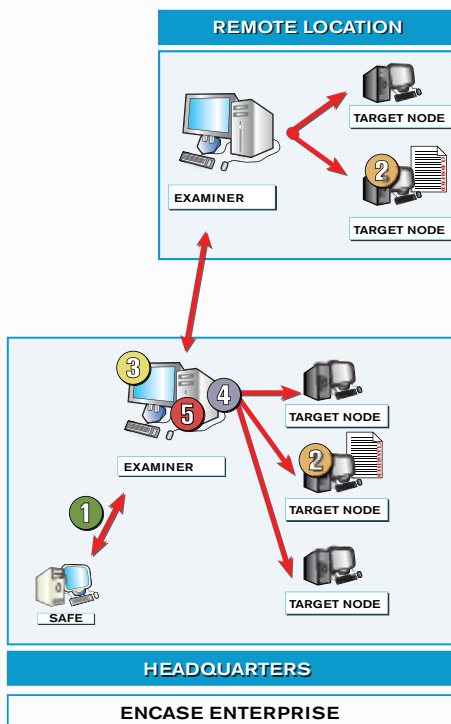
Deep System Analysis: Built upon the same forensic technology used by law enforcement and government agencies around the world, EnCase Enterprise uncovers hidden/deleted files; detects injected dlls, hidden/rogue processes and rootkits; searches for documents; reconstructs Web and email activity – even decrypts certain types of encryption and identifies unauthorized network communications. Furthermore the data gathered will stand up in courts worldwide

Parallel Analysis: EnCase Enterprise quickly analyzes large numbers of machines at the same time. Parallel analysis is the core capability that enables EnCase Enterprise to achieve enterprise search and incident response speeds that dwarf those of competing technologies.

Remediation: Once you identify a malicious event, you can document the incident in detail, zeroing in on all compromised machines, then reach out to those machines and remediate the problem – all from a central location without taking machines offline.

Integration: EnCase Enterprise can be integrated with a company's existing system to create an enterprise investigative infrastructure that provides complete network visibility and total control over your information assets.

How EnCase Enterprise Works



- 1 Examiner logs into SAFE for authentication and authorization
- 2 Examiner sends request to target node to snapshot volatile data or to preview drive
- 3 Examiner analyzes/reviews forensic or volatile data from target node
- 4 Analyze further or acquire image
- 5 Generate reports

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 5,000 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.