



ENCASE[®] ENTERPRISE

The Next Generation of Incident Response

Your company **is** its information,
and it's your job to **protect** it.
Yet **attacks** can come from a
variety of sources that you can't begin
to **pinpoint** using manual processes.

FEATURES

Protecting vital corporate assets — and your IT infrastructure — requires successfully fending off attacks by disgruntled employees, hackers and corporate spies and combating increasingly sophisticated worms, trojans and other hidden threats.

It puts every piece of your security infrastructure to the test. Unfortunately, even the most intelligent and finely tuned systems that detect and manage threats — IDS, IPS, SIMS and antivirus agents — still fall short.

EnCase® Enterprise puts teeth in your existing security components to help you respond effectively to security events and network attacks, and maximize the power of your existing investments. The solution automatically responds to security alerts and validates whether an attack actually happened. If the attack is successful, EnCase can automatically take steps to remediate the event before it causes further damage. Following best practices, EnCase completes the incident response process by letting you quickly analyze thousands of computers across your enterprise to reveal other compromised machines, saving your staff countless hours of manual labor.

EnCase Enterprise is the industry's only complete, automated incident response solution that delivers a standard, repeatable process in line with SANS and the National Institute of Standards and Technology (NIST) for best practices on handling computer incidents.

EnCase Enterprise works by providing an investigative infrastructure that gives you deep insight into the state of computers running on your network. It shows what they're doing and whether they're running rogue processes or are engaged in unauthorized communications. The solution hones in on rootkits, trojans, worms and other malicious entities, to help ensure your network is truly clean.

EnCase Enterprise is a highly secure and trusted platform that works across multiple operating systems and scales to meet the needs of the largest organizations.

Make the most of your existing security investments — Your Intrusion Detection Systems (IDS) and Security Information Management Systems (SIMS) kick out hundreds or thousands of alerts each day. But it's nearly impossible to learn which of those pose a true danger — and no organization has the resources to track and analyze every alert. By the time you determine which alert is most critical using manual procedures and tools that are not integrated, it's too late. During that time — between when an event occurs and the time you are able to respond — the information you need is stale, no longer relevant, or simply gone.

EnCase Enterprise solves the problem by integrating smoothly with your IDS and other security monitoring systems to trigger a real-time automated incident response process known as a "Snapshot" when an alert is received. Immediate analysis from the source and target reveals details of known,

unknown and hidden processes, TCP network socket information, open files, device drivers, services and more, to show whether machines have been compromised. Subsequent automated Snapshots are triggered shortly after the event to show attack results in time slices, revealing whether the event actually occurred, and if so, its impact and origin.

The ability to automatically investigate alerts means you can address all meaningful events from a number of sources.

Automate tedious, time-consuming tasks — After discovering an attack, EnCase Enterprise can, with a high level of certainty, automatically analyze computers across your entire enterprise to find other machines compromised by the same, worm, zero-day exploit or trojan. The solution takes information gleaned from the initial Snapshot — a signature or "fingerprint" that reveals characteristics of the attack — then looks for those same identifiers on all your machines. Detailed reports for each computer save valuable and measurable blocks of time by providing specific information about what actually happened and the source of the compromise. EnCase Enterprise can also regularly scan your environment to proactively identify and report similar compromises. IT staff and security investigators save the time-consuming task of manually inspecting each machine to assess and remediate the damage from new or prior incidents.

Protect against other growing threats — These days, savvy hackers increasingly rely on rootkits to compromise corporate networks. These

tools lets intruders operate – and return anytime they like – completely unseen, and essentially “own” your network. Rootkits have grown more robust and widespread over time, becoming a tool of choice among attackers who plunder private customer data, then often extort money from the companies they hack. Windows-based rootkits were completely undetectable until recently. EnCase Enterprise offers the only available commercial-grade solution to find and remediate those threats. It peers deeply into your operating systems to identify and destroy hidden processes and hooks used by rootkits – even when hackers go to great lengths to remain invisible.

Respond fast and effectively to any attack — Timely response is key to understand a computer attack, stop its spread and remediate the damage. In addition to capturing static data from computer hard drives, the EnCase Enterprise Snapshot capability snares “volatile” or live data stored in RAM. That critical information is necessary to identify hackers, worms and rootkits spreading through the network and to respond before the damage spreads. EnCase Enterprise automates incident response and compromise assessment by harnessing the power of more than 20 software tools in one secure enterprise product to assess more than 10,000 machines per hour. This approach to incident response and remediation gives you a standard, repeatable process that meets standards

and best practices set by the System Administration, Networking and Security Institute (SANS) and the National Institute of Standards and Technology (NIST) for handling computer incidents.

Tap deep analysis to strengthen your defenses — EnCase lets your security analysts do deep analysis on compromised computers required as part of a strong incident response effort. The ability to see the big picture – files manipulated or deleted, tools used to compromise the host, how long intruders operated within your environment – helps you find weak points to protect against future attacks.

Profit from an all-encompassing solution

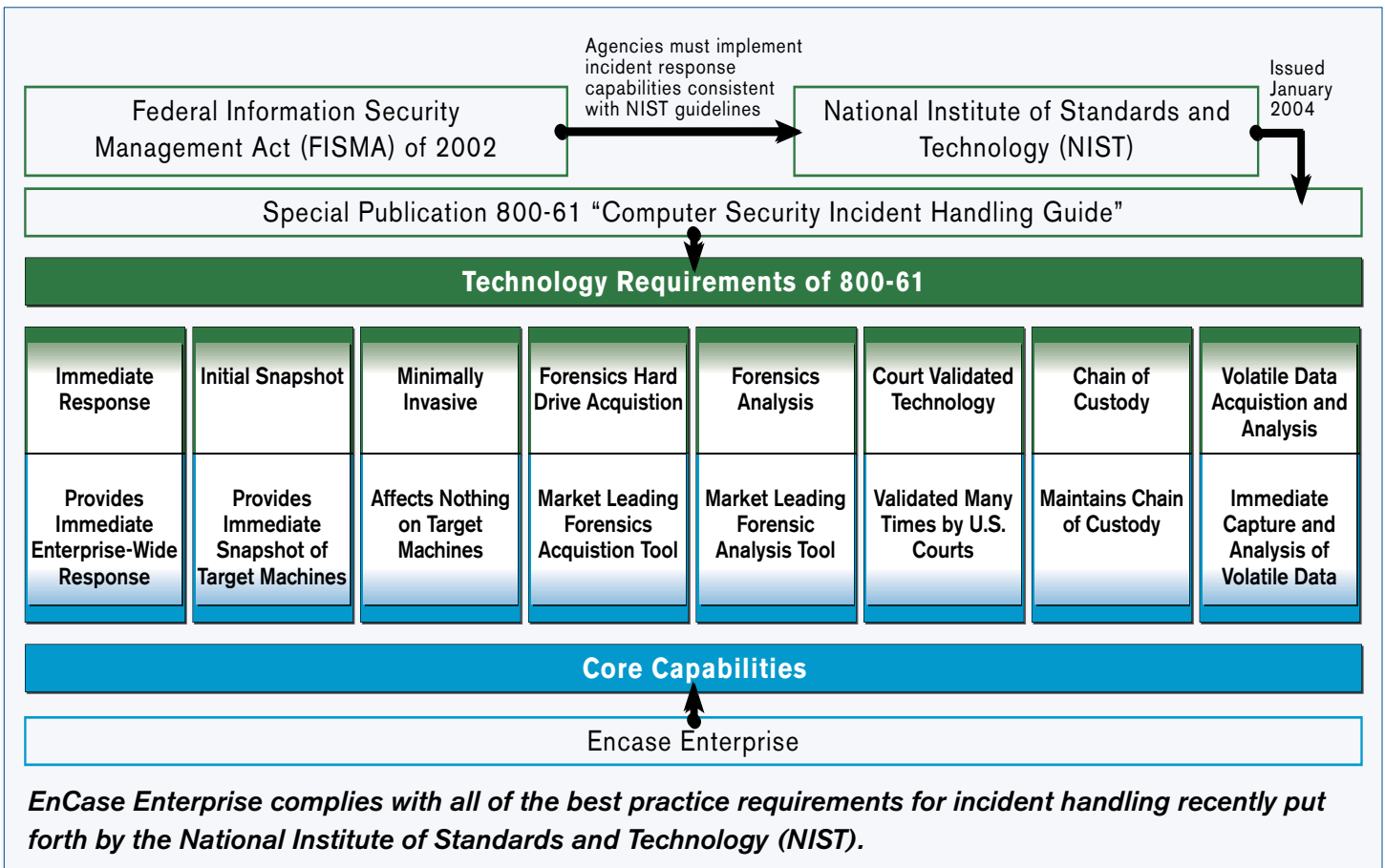
Guidance Software’s total solution can include professional services to help you quickly build a sophisticated incident response program – or integrate with your existing program.

The solution is designed to evolve as your company grows, and save your staff time immediately. Our expert consultants help you identify major threats to your environment, develop scripts to automate tasks and refine your responses to an incident, and incorporate these into a detailed incident response methodology. They’ll also fully integrate your IDS or SIM tools with EnCase Enterprise. Finally, as part

of our knowledge transfer approach, we’ll provide informal mentoring to your staff and brief executives on your new capabilities.

Learn from our world-class experts

Highly skilled IT professionals are at a premium, and we can keep your investigators thoroughly trained in the latest incident response technology and investigative processes. Thousands of corporations and forensic labs rely on Guidance Software’s expansive educational offerings and methodology. Our training program features industry-leading instructors, and offers basic and advanced incident response classes to help you conduct corporate investigations more effectively. Individual and career-track coursework is geared specifically to corporate investigators and counsel.



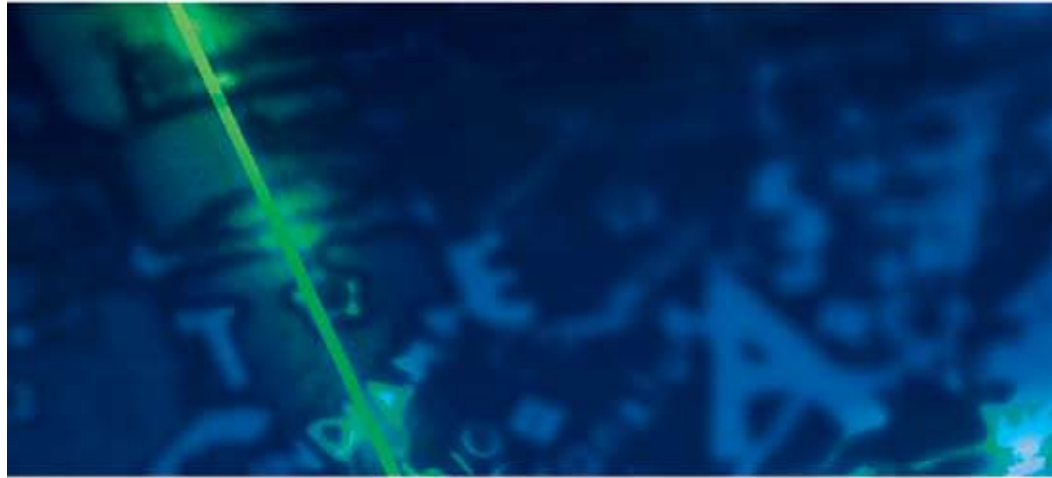
Basic Components

EnCase Enterprise lets investigators examine computer and network-related events in a highly secure environment, without compromising evidence. It relies on 128-bit AES encryption to protect data transmission, and all authentication and rights delegation is overseen by PKI-like scheme. Basic components include:

Examiner software — Installs on a system used to perform investigations and related audits.

SAFE (Secure Authentication For EnCase) — A server that authenticates users, administers access rights, retains EnCase transactions logs and provides secure data transmission. The SAFE communicates with the Examiner and target computers using encrypted data streams.

Servlet — Agent software installed on workstations and servers to enable analysis and investigation of target nodes.



About Guidance Software

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