EnCase® Cybersecurity

Network-enabled Incident Response and Endpoint Data Control through Cyberforensics

Guidance® SOFTWARE

EnCase® Cybersecurity

Key Benefits

- Expose, analyze and remove threats designed to evade traditional layered, defense-in-depth security approaches
- From a central location, quickly and effectively respond to and recover from computer security incidents, with no disruption to operations
- Find and remove sensitive data, such as credit card data or intellectual property, from unauthorized locations
- Remotely triage incidents across worldwide networks and combat insider threats
- Audit data to prove compliance with records retention and data management policies

Key Features

- Patent-pending Entropy Near-match Analyzer identifies similar files and binaries to expose advanced threats such as polymorphic malware
- Compares endpoints against a trusted baseline and performs live memory analysis
- Wipes files and kills running processes with forensically sound remediation capabilities
- Operates at the disk and memory levels, providing complete visibility and control over endpoint data
- Lets you combine and fine tune various search criteria – keyword, hash value, regular expressions, date ranges and more.

It only takes one. One successful attack from the average 500,000 attacks barraging government agencies and *Fortune* 500 companies daily. One costly theft of intellectual property by an insider. One infected USB stick carelessly attached to a laptop. It only takes one, and your confidential data and assets start speeding off to greedy criminals or competitors.

Once an attack or incident is discovered, the clock begins to tick as you scope, triage, and remediate the damage. Every delay and false positive costs you time and money and increases the chances of significant loss or permanent damage. The problem is compounded by lack of visibility into the troves of sensitive data being stored in violation of policy.

When your organization has been hacked, you suspect advanced threats are evading your layered security technologies, or need to expose and remove sensitive data from unauthorized locations get guidance from the forensics experts. Guidance Software's EnCase® Cybersecurity brings data-centric cyberforensics to the enterprise. We help you expose advanced malware and errant PII or IP on your endpoints, diagnose malware, locate similar malware such as morphed iterations, assist in attack attribution, and bring systems back to health. Once you have remediated anomalies and errant sensitive data, ongoing system integrity and data risk assessments maintain the trust level of your endpoints. Rigorous, remote scanning helps ensure your endpoints remain free of stealth malware and inappropriately stored sensitive data.

You've been compromised—Now What?

- **Is the threat internal or external?**
- **Inadvertent or malicious?**
- **Was there malware involved?**
  - Where was it?
  - What's it look like?
  - Where is it now?

Find it, where it went, what it morphed to, and remediate it

99% Effective is not Enough

EnCase Cybersecurity combats data theft where it happens most easily: the endpoint. Threats are getting through to these endpoints because traditional security software is waging a losing war against malware, and defense-in-depth protections still leave holes. For instance, designed for simple, static code that it can track with signatures, conventional anti-virus sees no evil in new, unknown code. Until malware is reported to anti-virus vendors, it is free to circulate throughout the Internet — and your network. In order to remain unrecognized as long as possible, today's malware changes often, sometimes after each execution. Each time it changes, anti-virus scanners see it as new and safe, and the criminals see another window of opportunity.

Anti-virus is used with other security products in layers, each with benefits, but none with complete, guaranteed effectiveness. Security leaders responding to the *2010 CyberSecurity Watch Survey* rated firewalls at the most effective, at just 86 percent, with data loss prevention rated one of the least effective, at 39 percent. With these gaps, network security has to layer and layer, striving for 99 percent effectiveness.It only takes one successful attack to leave your data and systems at risk, and there are thousands of attacks and new threats each day.

Unlike traditional security tools that leave you waiting, vulnerable, EnCase Cybersecurity lets you take charge, moving quickly and effectively to reduce risk in your environment.

Data-centric Cyberforensics

EnCase Cybersecurity is built on forensics processes and technologies. Where traditional security products look for component problems, such as viruses, network probes, or vulnerabilities, EnCase Cybersecurity looks at the complete picture, without constraints or assumptions that limit understanding or investigation. Instead of one limited piece of the puzzle, forensic grade disk-level visibility gives you a complete unobstructed view of the endpoint. A tiny, passive service on each system will perform all needed activities, and it can be disguised to prevent deletion by malware or notice by malicious insiders. The entire operation is transparent to users, avoiding disruption and suspicion. It works on a wide variety of operating systems for laptops, desktops, file servers, email servers and print servers.

System Integrity Assessments

After diligently restoring affected systems, most organizations want to avoid a repeat performance. Because end-users routinely install unknown code or store sensitive data on local systems, EnCase Cybersecurity offers you a way to use ongoing scans to expose and reduce endpoint risk.

First, you create "profiles" approved and trusted configurations for various builds on your network. Against these profiles, you can schedule periodic scans of network endpoints to detect any deviation from the approved baseline. Any anomalous code is treated as an incident following your EnCase-enabled incident response process and either eliminated or added to the trusted profile. This flexibility lets you define your preferred configuration of software and data.

Network-enabled Incident Response

When you realize you have a problem, the first challenge is to characterize the attack and scope the damage. Is the threat internal or external? Malicious or inadvertent? How big is the incident? Which systems are affected? How long has it been active? How can I recover?

EnCase Cybersecurity gets you moving immediately with high-level threat analysis of live systems performed over the network, allowing you to zero in on endpoints that have been affected. Multiple deep inspection and analysis techniques, including patent-pending Entropy Near-match Analyzer technology for similar file analysis quickly and automatically expose suspicious activity and software running on any system.

Triage

Forensics enter the equation with RAM and binary analysis, allowing a thorough investigation of an affected machines behavior, including how the machine is communicating with the network, what kind of privilages the machine is operating under and more. This insight gives you a complete understanding of the threat and can indicate other systems or areas that may be affected or at risk.

As you identify malware, EnCase Cybersecurity can look for that file or process on systems throughout your network, keeping you in control from a central console. Since so much malicious code is disguised or mutating today, Entropy Near-match Analyzer technology will expose similar files as well.

Unlike slow, easy-to-fool signature-based, packet inspection, and hashing techniques, Entropy Near-match Analyzer provides accurate analysis that can scale to the size and pace of enterprise incident response. The secret to our scalability is innovative analysis that computes thousands of values in minutes, comparing bytes rather than hash files. This approach makes our technology versatile as well as fast. This technology can detect small changes to code, work with foreign languages, and catch small adjustments to images, not merely text.

"Compared to manual auditing and remediation, our workflows and deep inspection return big dividends. In about 48 hours, one US federal agency runs full hard drive scans on 1,200 workstations dispersed around the world, automation that saves over $280,000 a year."

- Deputy Director, IRM office and ISO, U.S. Federal Agency

Entropy Near-Match Analyzer

In minutes, not days, track down specific and similar risky code or perform attack attribution based on a suspicious sample, without needing source code or physical access to each computer.

Infected systems can be addressed remotely, collecting all or part of the hard drive — including the malware and its artifacts — including the system's memory. You can collect as much or as little evidence as you require. By giving you visibility into every layer of software from registry and drivers up through applications, you can see what has happened and make informed decisions about the appropriate next steps — from remediation to legal action.

Remediate

Once malware is exposed and identified, EnCase Cybersecurity can take definitive action. It can kill related processes and wipe hard disk artifacts for complete remediation. The system can be completely restored to health — using operations performed transparently over the network.

Data Risk and Compliance Assessment

Scans can also search out sensitive intellectual property (IP), personally identifiable information (PII), and classified data, exposing systems that pose a risk. With the ability to search memory and hard drives at the disk level, EnCase Cybersecurity can target and locate sensitive data no matter where, or in what manner, it is stored, and even if it has been deleted or resides in unallocated space.

You can target the data you care about based on pre-defined criteria. EnCase Cybersecurity comes with pre-configured templates for the most common types of PII, such as credit card numbers and social security numbers. To hunt down business-specific IP, such as blueprints, source code or classified data you scan based on a combination of specific keywords with other criteria such as date range, general expressions or hash value.

When sensitive data is found to be in unauthorized locations and collected, forensic-grade remediation capabilities completely wipe the offending data from the endpoint, ensuring policy is enforced and that the errant data no longer poses a risk to the organization.

Standardize and Save

We are committed to your increased success, your improved security, and your efficiency. From initial gap analysis to repeatable workflows to quarterly audits, our experts can help modernize your approach to cybersecurity, digital investigations and eDiscovery. While ensuring your company is following best practices, the Guidance Advisory Program can eliminate wasted resources and manual processes to establish the most cost-effective methods for handling incident response, investigations and electronically stored information.

The professional services team will diagnose your current processes and provide a roadmap to greater efficiency and industry standard practices. They help you deploy and successfully adopt EnCase products within your business processes and operations. Detailed quarterly audits can document your company's progress with tangible statistics, such as compliance with best practices, the type and number of incidents you have responded to, and the increased speed at which these incidents are resolved. Best of all, the Program's design goal is positive return on investment within the first year.

Enforce Policy

In your audit, any anomalies or errant sensitive data detected can be your first hint of a new problem, allowing you to move into action before a major loss or incident:

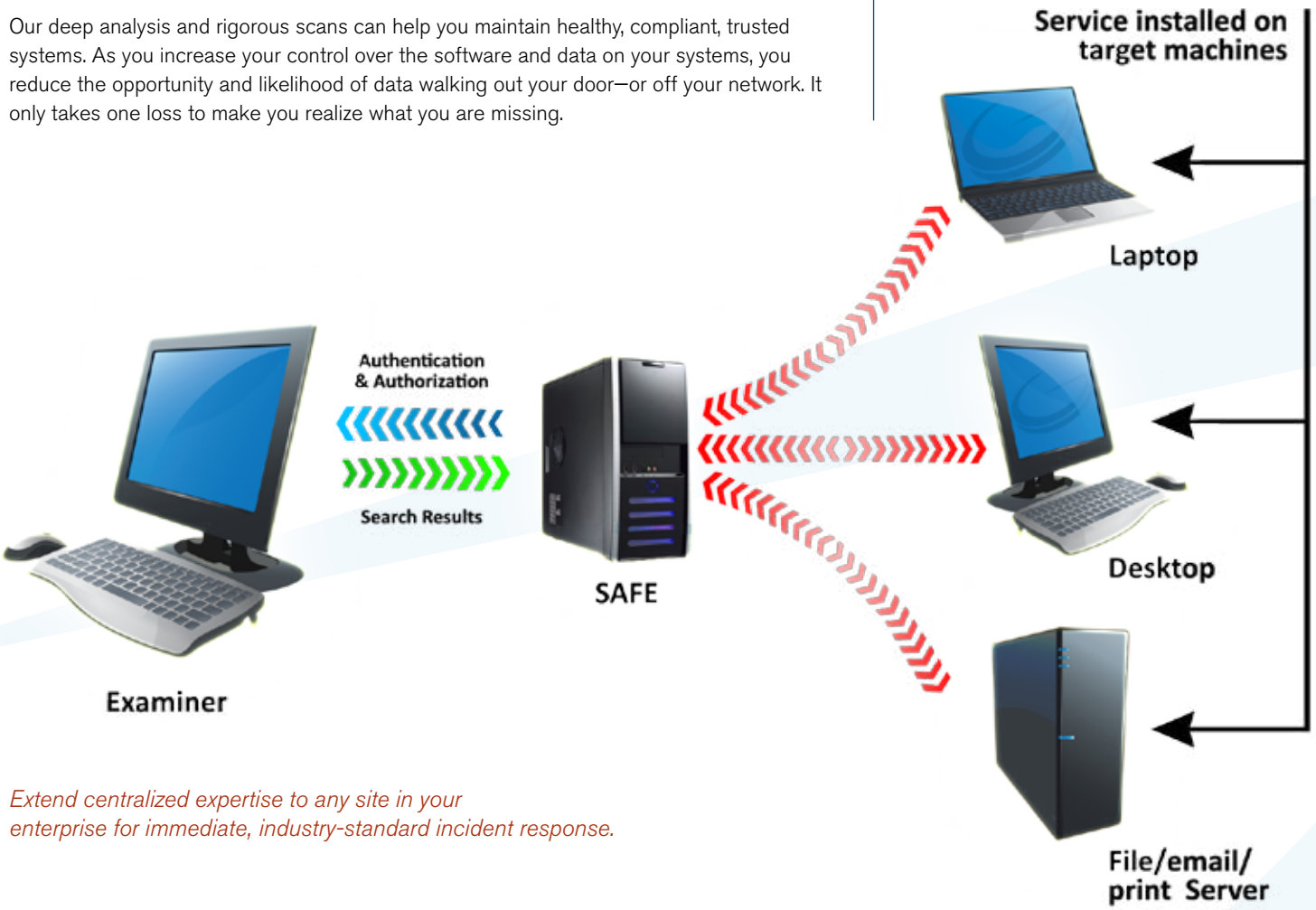
- If a customer database or classified data is on an unauthorized laptop, it may be a simple oversight or accident. It's probably enough to refresh that person's knowledge of data handling policy–after you instruct the EnCase Cybersecurity service to delete the file.
- A risky peer-to-peer filesharing application can simply be deleted remotely.
- Cracker tools on an engineer's system may be a precursor to data theft or illicit activity.
- Unknown code may be a nascent zero-day attack, spurring you to move immediately into incident response.

All of our enterprise products utilize the exact same lightweight, passive 800K endpoint driver. This means other Guidance Software solutions can be added later without additional change management processes and burdensome endpoint deployments.

Conclusion

It only takes one successful attack or theft for a company to realize its data defenses are down. EnCase Cybersecurity applies cyber forensic processes and technologies to reduce the risk and cost associated with responding to incidents and losses. We help you methodically purge systems of surreptitious, malicious code designed to siphon information and disrupt operations. Then, we help preserve a trusted state with scheduled threat or risk assessments that reduce the risk of sensitive data loss and stealth malware.

Our deep analysis and rigorous scans can help you maintain healthy, compliant, trusted systems. As you increase your control over the software and data on your systems, you reduce the opportunity and likelihood of data walking out your door—or off your network. It only takes one loss to make you realize what you are missing.



Extend centralized expertise to any site in your enterprise for immediate, industry-standard incident response.

Get Guidance

Guidance Software leads the world in digital investigation technologies and innovations. Thousands of forensic investigators have trained with us to earn the coveted EnCE® certification, proof of expertise in the art and science of forensics. Once EnCase software is in place, you have a strong foundation for the lifecycle of data protection. The same infrastructure you use for Cybersecurity also supports EnCase® eDiscovery and other digital investigations. Our Advisory Consultants can help upgrade your data handling processes to industry best practices that preserve your resources and protect your business reputation. Learn more at www.guidancesoftware.com/cybersecurity and view an animated overview of the EnCase Cybersecurity solution.

Guidance® SOFTWARE

www.guidancesoftware.com

Our Customers

Guidance Software's customers are corporations and government agencies in a wide variety of industries, such as financial and insurance services, technology, defense contracting, pharmaceutical, manufacturing and retail. Representative customers include Allstate, Chevron, FBI, Ford, General Electric, Honeywell, NATO, Northrop Grumman, Pfizer, SEC, UnitedHealth Group and Viacom.

About Guidance Software (NASDAQ: GUID)

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® platform provides the foundation for government, corporate and law enforcement organizations to conduct thorough, network-enabled, and court-validated computer investigations of any kind, such as responding to e-discovery requests, conducting internal investigations, responding to regulatory inquiries or performing data and compliance auditing - all while maintaining the integrity of the data. There are more than 30,000 licensed users of the EnCase technology worldwide, the EnCase® Enterprise platform is used by more than half of the Fortune 100, and thousands attend Guidance Software's renowned training programs annually. Validated by numerous courts, corporate legal departments, government agencies and law enforcement organizations worldwide, EnCase has been honored with industry awards and recognition from *Law Technology News*, *KMWorld*, *Government Security News*, and *Law Enforcement Technology*.

ECS BR 0160-13005