EnCase® Cybersecurity

Defend your network, respond to incidents, conduct counterintelligence and recover from classified spillage—using one solution

Guidance® SOFTWARE
The World Leader in Digital Investigations™

EnCase® Cybersecurity

Key Benefits

- Determine threat level of endpoints, analyze process code, and then remediate registry entries, files and processes to proactively identify and recover from covert threats
- Perform code and behavioral analysis of malware and recover systems from a central location with no disruption to operations
- Identify binaries similar to a source file to help attribute malicious code and identify and remediate iterations of polymorphic malware
- Proactively audit for sensitive data and recover from classified spillage
- Triage incidents across worldwide networks and combat insider threats
- Investigate network breaches, personnel matters and allegations of fraud while preserving the chain of custody

For cybersecurity personnel and response teams, the mission is to achieve situational awareness, defend sensitive information and proactively identify and respond to network threats—around the clock and across global networks. Fulfilling that mission requires nothing less than the ability to identify, analyze, triage, respond to and recover from classified spills or threats to the network, all while ensuring endpoints remain in a trusted, operational state.

EnCase Cybersecurity is an all-in-one solution that provides cybersecurity personnel and others in government agencies with the ability to dynamically detect covert malicious code and proactively identify network threats in any cyber environment. With EnCase Cybersecurity, agencies can shift from a reactive to a proactive approach by zeroing in on potential threats, completely recovering computers from malicious code infiltration and drastically reducing recovery cost and time.

Keep Pace with Evolving and Covert Threats

Hackers have realized that static malicious code is easily thwarted. New methods are being employed to allow malicious code—such as polymorphic code—that can morph frequently to avoid detection from conventional scanners.

EnCase Cybersecurity includes unique capabilities that put agencies one step ahead of those who wish to do harm to government controlled networks.

With the ability to triage for covert threats, perform detailed code analysis to determine if a particular piece of malware has the ability to morph, and leverage advanced algorithms to determine code similarity, EnCase Cybersecurity allows agencies to zero in on and recover from the most evasive threats.

Identify Unknown Threats and Mitigate Risk Across the Enterprise

EnCase Cybersecurity provides robust endpoint threat detection and mitigation across the enterprise.

Once a computer is identified to contain a potential threat, EnCase Cybersecurity can determine exactly where malicious data resides on an endpoint. It also can thoroughly analyze unknown or suspicious processes. For example, with code analysis capabilities powered by HBGary Responder Pro, users can reverse engineer running RAM or a single process to determine the capabilities of a given process such as the ability to morph. This provides agencies with a full understanding of the threat, as well as an indication of other systems or areas that have either been affected, or could potentially be affected, by the threat.

Networks can be scanned from a central console and threats can be remediated without operational disruption.

Stop Polymorphic Malware in its Tracks

EnCase Cybersecurity enables agencies to fight polymorphic and metamorphic malicious code by determining if new binaries share similarities with previously attributed code. This is achieved by comparing the entropy, or randomness, of binaries.

Unlike fuzzy hashing approaches, EnCase Cybersecurity technology provides rapid on-the-fly assessment of malware across the enterprise with a proven degree of accuracy, without requiring an organization to possess the source files of known malware beyond the initial point of infection.

Ensure Endpoints Remain in a Trusted State

EnCase Cybersecurity provides agencies with the ability to utilize and augment EnCase Bit9 Analyzer with their own set of trusted and un-trusted hashes. With this capability, agencies can periodically scan network endpoints against millions of records to ensure there is no deviation from the baseline. If unknown files or processes are encountered, EnCase Cybersecurity can provide a high-level threat analysis, allowing security teams to zero in on endpoints with the highest threat levels.

Secure Sensitive and Classified Data

With the ability to search a hard drive at the disk level, EnCase Cybersecurity can target and locate sensitive and classified data no matter where, or in what manner, it is stored on the network, and even if it has been deleted. Once identified, agencies can collect and remove the responsive data from unauthorized locations to ensure data remains safe, secure and available only to individuals authorized to access it.

Thorough Remediation and Recovery

EnCase Cybersecurity provides the capability to remediate files, processes and registry settings—allowing not only for full recovery from a network threat, but also the means to recover from a classified spillage incident. Other technologies may provide ways to search for data, but none have the breadth of remediation capabilities found in EnCase Cybersecurity.

Enhance Cybersecurity with Advanced Algorithms Designed to Adapt to New Attack Vectors

EnCase Cybersecurity Entropy Near Match Analyzer

Using technology designed and patented by Guidance Software, EnCase Cybersecurity provides the ability to compare files for similarities over the network. The unique nature of our approach—measuring the entropy, or randomness, of a file—enables more accurate and faster comparisons than the traditional method of fuzzy hashing to determine file similarities. This capability allows analysts to locate iterations of polymorphic malware, identify older/newer versions of documents, and it assists in determining file attribution.

Our groundbreaking method to determine file similarities allows agencies to dynamically adapt to polymorphic and metamorphic code used by cyber attackers.

EnCase Cybersecurity Code Analysis

Once EnCase Cybersecurity identifies an unknown process, deeper memory analysis provides intelligence on any given process and how that process executes, as well as determining whether malicious code is polymorphic and where residual malware artifacts might reside.

With new memory analysis capabilities, identification of unknown threats is now possible.

EnCase Cybersecurity Bit9 Analyzer

The Bit9 Global Software Registry contains information on the metadata of over 400 million files, hash values on over 9 million applications from over 20 thousand vendors and hash values for nearly all known malware. With EnCase Cybersecurity's Bit9 Analyzer, users can easily leverage this data to save time when scanning their own systems.

This solution greatly reduces the time to identify unknown threats, known malware and unauthorized software.

Key Features

- Operates at the disk and memory levels, providing complete visibility into endpoint data
- Allows for the capture and in-depth analysis of unknown files and processes via integration with HBGary Responder Professional
- Provides the ability to compare endpoints against a trusted baseline or the Bit9 Global Software registry to identify any deviation from a trusted state
- Preserves the chain of custody with forensic technology, ensuring no harm is done from the perspective of a federal prosecutor
- Enables collection and preservation of only relevant data; no need to capture entire hard drives
- Integrates with the DISA STIGS XML database to ensure IAVA compliance
- Ensures compliance with key government mandates, such as FISMA and DCID 6/3

"Protected U.S. government networks have fallen prey to an alarming array of attacks in recent months. For contractors like Guidance Software, this is a critical time to support government agencies at a tactical level to meet threats headfirst as they try to gain control of the cyber-crisis."

-INPUT, the leading authority on government business

Certified Safe for Use in Secure Environments

Guidance Software is the only vendor in the enterprise investigation space holding DIACAP, Common Criteria EAL-2 and FIPS 140-2 certifications, validating that security protocols are safe to use in a secure environment.

Guidance® SOFTWARE
The World Leader in Digital Investigations™

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. Our EnCase® customer base includes more than 100 of the Fortune 500 and over half of the 50, including: Allstate, Chevron, Ford, General Electric, Honeywell, Mattel, Northrop Grumman, Pfizer, UnitedHealth Group, Viacom and Wachovia.

About Guidance Software (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 eDiscovery 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, 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 eWEEK, SC Magazine, Network Computing, and the Socha-Gelbmann survey. For more information about Guidance Software, visit www.guidancesoftware.com.

ECS BR 9070-13002