EnCase® Cybersecurity In Action

EnCase Cybersecurity has transformed the way enterprises expose, analyze, and respond to advanced endpoint threats and errant sensitive data

Guidance® SOFTWARE

While every other solution defends against known threats, EnCase® Cybersecurity is the only solution to expose, triage, and remediate the unknown elements within your network. This proven solution automates incident response and data auditing processes and guides you to undiscovered data that may represent a threat to the enterprise, supporting global scale, remote access, system integrity assessments, and similar file analysis for the most accurate, prompt investigations.

The case studies that follow are groundbreaking, real-world examples of how our customers are using EnCase Cybersecurity to expose and mitigate evolving threats as well as audit and control sensitive data.

Incident Response and Remediation

INDUSTRY: Hospitality

EnCase® Cybersecurity exposed malware that PCI fraud heuristics and signature-based scans had missed

It seemed like a one-off hack. A hotel booking system in Texas had been compromised, and the hacker had locked out some administrators when he gained root access while stealing credit card data. After a reimaging, the company thought systems were clean again. However, a few months later, a call from VISA showed the hacker had just moved on. A PCI Qualified Incident Responder was sent on the trail of new fraudulent transactions coming from a common point of purchase (CPP) hotel booking system in Europe. The investigator could trace some of the transactions, but could not figure out exactly which systems had been used, so they could not get to the root of the problem.

After this, the CISO engaged with Guidance Software to deploy EnCase Enterprise. Guidance Software experts were onsite when the next call came from VISA's fraud team. VISA was able to pinpoint the system originating the fraudulent transactions in Europe. From Houston, the Guidance experts remotely scanned that machine and looked at the traffic it was sending.

They compared the system to a trusted baseline of the software that was expected to be on the system, capturing live running memory, and correlated outbound traffic with log files from an intrusion detection system, looking for unusual activity. EnCase Cybersecurity exposed anomalous behavior that proved to be specialized malware that searched for and validated credit card data, then shipped files using SSL encryption to an Internet drop box. The criminal could anonymously stop by and pick up fresh, valid card data.

The remediation recipe might have seemed simple: create a signature of the code and look for it on every other system. However, a signature-based scan of other CPP systems came up empty. So, EnCase Cybersecurity was used to look for variations on the known malware, "like" code that was similar but not identical. Powerful similar file analysis capabilities scanned 3000 systems and found six compromised sites in South Africa and Europe. The criminal had used a compiler on each host to recompile his malware, ensuring the signature would be different on each compromised system, eluding standard signature-based scans.

Once the compromised systems had been identified, the next step was scoping the extent of the breach. Letters would need to be sent to credit card holders living in regions with breach notification requirements, such as the majority of U.S. states, the UK and the European Union. EnCase Cybersecurity helped the hospitality company's IT team determine exactly which data had been stolen, minimizing the quantity and cost of the notifications required. Total elapsed time? Just 8 days.

During the process, the company realized that lax controls over these systems had allowed local users to install a medley of login software and development tools on each system, including source code. This playground enabled the hacker to cover his tracks. Now, the company uses EnCase Cybersecurity to automate a standardized data audit process, validating remote systems against a trusted baseline to ensure configurations do not drift from the approved standard.

INDUSTRY: Energy

In under 4 days, uncovered 16 compromised computers on 3 continents

When a major oil company discovered that one of their servers in Asia had been taken over by a hacker, they called in Guidance Software Professional Services consultants. The oil company wanted to know what was happening, how much damage had been done and how to get their critical systems well again—as quickly as possible.

First, the consultants used EnCase Cybersecurity to thoroughly scan the known compromised system over the network, looking at registry files to create a timeline of what had happened on the system. Because EnCase Cybersecurity can circumvent operating-system level login restrictions, the consultants could get past the hacker's control of the host and see the data. Artifacts and metadata revealed each action with timestamps, so the Guidance Software consultants could reconstruct the attack and understand what evidence to look for on other systems.

Like many enterprises, oil companies have sensitive information that is unregulated, but has an enormous street value if stolen. The assumed goal of this attack was to exfiltrate sensitive oil production data in order to let the attacker profit from fluctuating prices. The hacker had used a phishing email to lure an employee to a website that contained hidden malware. The malware dropped onto its target, then beaconed back to the criminal's command and control center and downloaded additional malware to give the criminal remote control of the machine. From this compromised system, the criminal obtained VPN credentials and was able to reconnoiter the network to locate systems that monitored oil reserves. On systems he obtained access to, he dropped malware that would copy the data from memory, save it to a file, and ship it back to him.

The Guidance team used the recovered artifacts and metadata to create a "fingerprint" of the criminal's malware. It then launched parallel hands-free EnCase Cybersecurity scans of similar machines over the network in sites from a U.S. campus to field facilities in Asia and Africa that had to be reached over satellite. Scanning non-stop for almost four days, the software investigated 465 systems and determined that 16 machines had been compromised. The Guidance team then trained the oil company's administrators to remediate these systems using EnCase Cybersecurity.

INDUSTRY: Government

Deep inspections revealed dirty systems in the DoD

Defense department organizations surround themselves with layers of security, yet sometimes malware still sneaks through. This federal organization was frustrated by alerts that indicated compromised endpoints, yet traditional scans revealed nothing. Consultants had analyzed the systems, but for every system that was cleaned up, another emerged from hiding, like the proverbial "whack a mole." However, this was not a game. Classified data was at risk.

EnCase Cybersecurity was used for an automated, comprehensive inspection of networked endpoints, looking deep inside the file system for rootkits, evasive threats and the existence of potentially risky processes. By operating over the network, users were not disrupted while systems were thoroughly inspected. After a week, the team identified several "dirty" systems, characterizing the malware with a specific fingerprint so that the organization's environment could be cleaned up once and for all. EnCase Cybersecurity was used to remediate malicious data during the investigation in order to prevent further spread of the malware until the scope of infection could be determined and a comprehensive remediation plan formulated.

INDUSTRY: Retail

Digging up worms at a retail company

A recent well-publicized worm had tunneled deeply into the home offices of a large retail company. While IT security worked with its AV vendor to figure out a plan of attack for this polymorphic—constantly evolving—worm, the company's incident response team called in Guidance Software for expertise.

The AV vendor suggested monitoring traffic with intrusion detection, identifying suspicious systems, sending an administrator to each machine, diagnosing the ports and processes used and creating a custom signature for each instance of the malware. This expensive and slow option would leave the company chasing an ever-elusive worm. With dozens of subnets, each with hundreds of hosts, scattered at sites across the country, there was little hope of a complete clean up.

Instead, the Guidance team used EnCase Cybersecurity to run a complete scan of the first subnet in 30 minutes. The scan identified the suspicious process running on the box, as well as four related processes. The team collected logical evidence from the running files and processes to fully characterize the actions of the worm, and then took the system offline to be rebuilt. Using the newly found malware as a source for EnCase Cybersecurity similar file analysis, the Incident Response team was able to scan all 45 subnets. They exposed an additional 10-15 infected systems among the hundreds on each network in scans that took under an hour per subnet. The local administrators could then take the systems offline for full remediation.

INDUSTRY: Financial Services

Dethroning Zeus in banking network

An EnCase Enterprise banking customer was concerned about the possibility that the Zeus Trojan had infected its systems, jeopardizing its billion plus dollars in daily transactions. It knew that anti-virus signatures were ineffective, since they took days to be distributed and were limited to detecting known malware, not the morphing and obfuscated variants distributed by the Zeus botnets. Network Data Loss Prevention (DLP) could not be relied on to catch outbound transfers of sensitive data if the attacker had control over the system and could disguise or encrypt the data. For peace of mind, the executives demanded a complete network-wide scan to expose any instance of Zeus hiding in the environment.

The bank felt that the remote investigation features of EnCase Enterprise were a good approach and upgraded to EnCase Cybersecurity to support threat investigation on a large scale. Using EnCase Cybersecurity, they looked for unknown running processes across critical systems. An automated assessment revealed several machines with unknown processes which upon investigation were found to be exhibiting unusual behavior. Further inspection confirmed an instance of the Zeus Trojan. Using this as a source for an enterprise-wide similar file analysis, they utilized EnCase Cybersecurity technology to inspect all systems for other iterations of the Trojan.

Similarly, a large payment-processing firm is using EnCase Cybersecurity to look for iterations of the Zeus Trojan, as well as other threats designed specifically for the banking sector. Using Cybersecurity, investigations that used to take weeks now take a few hours, delivering results that are more accurate with much higher productivity and no additional resources.

A large insurance company is using EnCase Cybersecurity data audit and remediation capabilities to enforce records retention policies.

Data Audits

INDUSTRY: Entertainment Software

Searching for Intellectual Property (IP) leaks in 91 countries, without a single plane trip

Video gaming features cutthroat competition, both on and off the screen. Leaked story lines can take the sizzle out of a product launch, and pirated software has a devastating effect on profits. When a Global 100 entertainment software company found source code of one of its unreleased games on a public site, it suspected insider theft. The internal incident response team needed to investigate the leak, searching a global network of 91 countries without alerting employees.

EnCase Cybersecurity was chosen to audit the systems to find every specific instance of the leaked source code, identify the trail connecting the user's system to external sites, and preserve the evidence. The Cybersecurity software was installed at a central site, and then sent off to explore the global network looking for the source code. Overnight, it investigated over 50 devices to construct an incident evidence trail reflecting laptops, desktops, servers (including a 4 terabyte server), email accounts, USB storage, and Internet histories, finding the matching file in several locations. Once these systems had been identified, the investigation was narrowed to a specific suspect that had access to the identified workstations and servers. Upon further investigation of those machines by trained individuals, the organization was able to prove the suspect had used a file-sharing program on his own workstation to leak the source code. By capturing information while the systems were running, the process was both deeply revealing and invisible to the user.

From start to finish, the investigation took two weeks. Today, EnCase Cybersecurity is part of a formal, company-wide intellectual property and human resources audit process designed to keep sensitive and proprietary information confidential.

> "The non-disruptive element of EnCase minimized the financial, commercial, and operational impact of the leaked IP and accelerated the successful resolution of this incident."
>
> *CEO & President - European Operations, Global Entertainment Software Co.*

INDUSTRY: Hospitality

System integrity assessment and data audits shrink the chance of data loss

Point of sale device vulnerabilities and fraud at storefront and retail sites have made merchants of every size nervous about controls over data. PCI regulations insist on strong controls, but minimum-wage workers and non-stop operations at remote sites hinder processes.

A major restaurant chain wanted to limit its risk of data loss by limiting the storage of PCI regulated data across the transaction process, from the point-of-service device through to the back office server at each site. EnCase Cybersecurity software was used to reliably ensure no system was storing sensitive data in its local hard drive or in memory, ensuring minimal losses in the event those devices became compromised.

EnCase Cybersecurity runs a sensitive data assessment of each of these devices every day, looking for any PCI regulated data, so that devices that have errant sensitive data can be easily identified and restored to a compliant state. These processes are administered from the central office, allowing a reliable change control process without dependence on on-site IT expertise. As well, if a problem is suspected, the centralized system can run an on-demand assessment of a specific site to investigate, capture and document forensics-quality evidence as needed.

A South African bank is using EnCase Cybersecurity to proactively find and remove account data from unauthorized machines across 45k nodes.

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 1140-13009