EnCase® Endpoint Security
by Guidance Software

SECURITY BEGINS AT THE ENDPOINT

GUIDANCE SOFTWARE™

GUIDANCE SOFTWARE

ENCASE® ENDPOINT SECURITY

In 2008, Guidance Software released its first endpoint security solution, EnCase® Cybersecurity, leveraging the enterprise-proven EnCase® platform to gain full access to the endpoint and help security teams like yours automatically or manually collect, validate, triage, investigate, and remediate all instances of a threat. EnCase® Analytics followed in 2013, taking the knowledge gathered from years of automated incident response to provide the ability to detect unknown threats and anomalous behavior from one of the most under-utilized intelligence sources available, your organizational endpoints.

Encase® Endpoint Security is the evolution of the two market leading solutions, EnCase Analytics and EnCase Cybersecurity, to help security teams proactively address the gaps in their security framework, detect unknown risks or threats, respond to any events for validation, and recover endpoints to a trusted state through remediation – all without the administrative and process overhead of managing two disparate solutions.

Gartner named Guidance Software the estimated 2013 market share leader for Endpoint Detection and Response (EDR) tools in their recent Competitive Landscape Report.

EnCase® Analytics
+
EnCase® Cybersecurity

= EnCase® Endpoint Security
by Guidance Software

COMPLETE YOUR SECURITY STRATEGY WITH ENCASE ENDPOINT SECURITY

Organizations have traditionally invested a large percentage of security budget in perimeter technology designed to identify and prevent the infiltration of the "known bad."

Despite the revenue allocated, the number of successful breaches has continually risen. The time to discovery and resolution of enterprise threats is still in the region of months while the attackers can gain access to your business systems in mere hours.

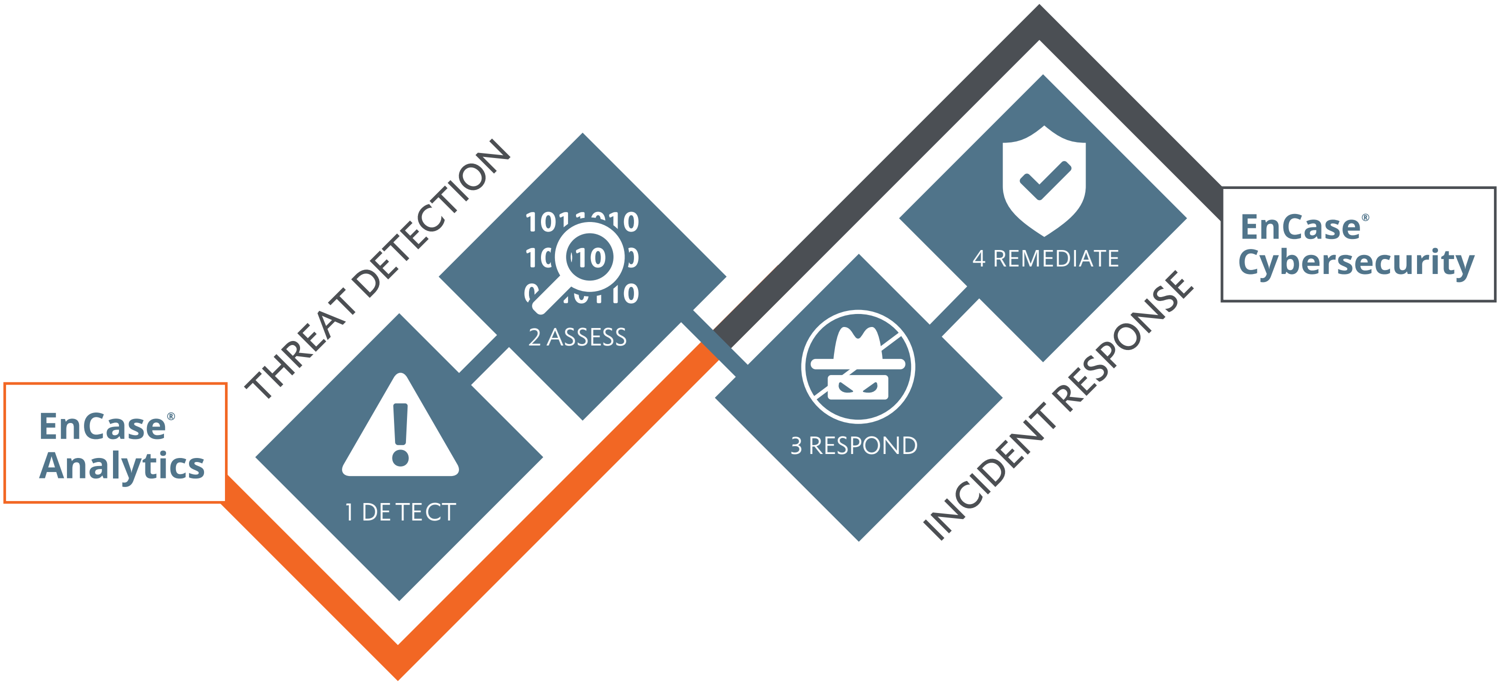
Within your enterprise you have literally billions of data points, artifacts that can be used to understand your current security posture, your potential gaps, and the hidden threats lurking unseen due to the lack of visibility. EnCase Endpoint Security enables that visibility, collecting snapshots of data (smaller than a web page in size) to provide your security team with the ability to see into the fray and extract meaningful security intelligence from the endpoints where data ultimately resides, and is the target or vehicle of every attack.

KEY BENEFITS

- Baseline all endpoint activity and maintain a historical record
- Identify gaps in security policies and frameworks
- Detect previously unseen process threats
- Identify anomalous user activity
- Search for known potential threats
- Reduce risk by limiting sensitive data
- Prioritize and triage legitimate alerts
- Validate and remove false positive alerts
- Forensically investigate high priority events
- Perform incident response at global scale
- Incorporate custom scripts and programs into one central platform
- Securely remediate bad actors or errant sensitive data

Not only does EnCase Endpoint Security let you proactively hunt unknown threats unique to your organization—it also lets you respond if a genuine breach is identified, empowering your security team to identify, investigate, validate, and eradicate those bad actors.

Employing EnCase Endpoint Security while planning, implementing or optimizing a security strategy will provide your organization with the ability to understand your security posture, target security gaps, detect unknown threats and respond to any alert regardless of your current approach.



DETECT

To gain insights into unknown threats, most security intelligence tools in the market focus on structured data such as log files or network packets. However, simply analyzing these data points from select systems or egress points is not sufficient to identify gaps within your security posture or detect the anomalous behavior of the emerging breed of threats. You need visibility into endpoints to get to the heart of the threats.

EnCase Endpoint Security changes the security workflow from waiting for an alert to "threat hunting," or proactively correlating endpoint data for anomalies indicative of a breach. In addition, EnCase Analytics can also identify gaps in your current security strategy, giving you a means of validating whether your security policies are being enforced and exposing areas not covered by existing controls or technology.

EnCase Endpoint Security leverages the proven EnCase endpoint collection capability, adding security intelligence which exposes risk and threats that evade traditional detection technology. It provides a bird's-eye view of your endpoint risk through an interactive visual interface, so you can look for anomalous behavior in the system and quickly expose signs of intrusion.

KEY FEATURES

- Ongoing and on-demand data collection from enterprise-wide endpoints
- Instant visualization of endpoint data and activities, no data scientists required
- Extensible architecture that allows for self-built applications and customization
- Integration with third-party data sources such as whitelists or threat intelligence
- Report-sharing & exporting as images, PDFs, or spreadsheet files

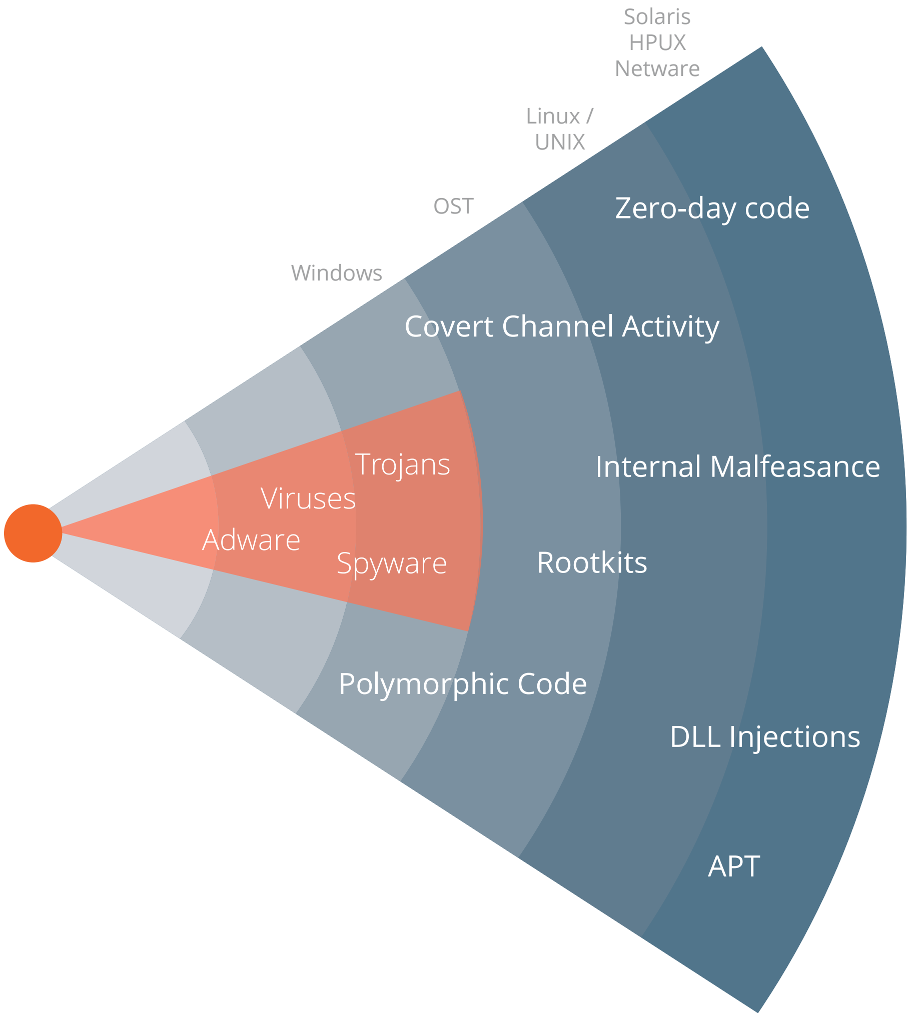
RESPOND

Sensitive data is what drives your business, making loss of that data one of the largest risks your organization faces today. Adding to this vulnerability are the rising frequency of attacks, growing costs of remediation, and lengthening time-to-response.

Limited visibility into both the targets of attacks as well as where and how sensitive data is stored only compounds the problem.

The warranted and needed investment in perimeter technology to solve the infiltration of the "known bad" has also created a resounding number of security alerts coming from those technologies. The proliferation of these tools—along with the alerts they generate—and the fact that actionable data related to the incident can decay in minutes or even seconds, further complicates the incident response challenge.

EnCase Endpoint Security helps you implement both a rapid-response process and a sensitive data discovery plan that complement and extend your current security technologies. Leveraging the resources you already have and requiring no additional staff.



KEY FEATURES

- Increase overall efficiency of security tools that create alerts through integration and automated response scenarios
- Identify false positive and validate alerts detected by other security technologies
- Shorten response times by getting context to triage threats at the point of the alert and expand searches to identify the total impact to the organization
- Prioritize response based on incident scope as well as data and systems at risk
- Proactively and reactively run scans to find sensitive intellectual property (IP), personally identifiable information (PII), and classified or sensitive data, exposing systems that present a risk
- Web-based reporting offers a convenient way to swiftly review, act on, and present findings for small and large security teams
- Documented chain of custody lets you supply evidence of illicit activity on endpoints during prosecution
- Forensic detail of every endpoint for deep investigations and incident response

KEY FEATURES

- Kill running malware, morphed instances and related processes
- Forensically wipe malicious files and hard-disk artifacts to halt the spread of the threat
- Remotely delete sensitive data files from unauthorized locations
- Ensure deleted artifacts cannot be reconstituted
- Maintain uptime and productivity of infected systems during remediation

WHAT IS AN ENDPOINT?

Any machine on a network with the following operating systems:

- Microsoft Windows
- Apple Mac
- Linux
- IBM AIX
- SUN Solaris
- HP UX
- Novel Netware

Any physical or virtual computer on a network:

- Servers
- Desktops or Workstations
- Laptops

Any supported computer-based technology:

- Printers
- Automated Teller Machines (ATMs)
- Point of Sales Terminals
- Ticketing Machines
- Industrial Control Systems (ICS)
- Computer Integrated Manufacturing (CIM)

RECOVER

Once malware or a risk of sensitive data is exposed and identified, EnCase® Endpoint Security lets you take definitive action and remove any reliance on traditional remediation processes like wiping and reimaging, which mean system downtime, loss of productivity and may incur potential data and revenue loss.

AUTOMATION & INTEGRATION PARTNERS

- HP ArcSight ESM
- HP ArcSight Express
- FireEye NX
- Cisco Sourcefire NGIPS
- Cisco ThreatGrid
- IBM QRadar
- Blue Coat Security Analytics
- Palo Alto Networks WildFire
- ...and more

MORE INFORMATION

Further information, whitepapers and webinars on Threat Detection and Incident Response available at guidancesoftware.com/endpointsecurity

About Guidance Software (NASDAQ: GUID)
At Guidance, we exist to turn chaos and the unknown into order and the known—so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. Makers of EnCase®, the gold standard in digital investigations and endpoint data security, Guidance provides a mission-critical foundation of applications that have been deployed on an estimated 25 million endpoints and work in concert with other leading enterprise technologies from companies such as Cisco, Intel, Box, Dropbox, Blue Coat Systems, and LogRhythm. Our field-tested and court-proven solutions are used with confidence by more than 70 of the Fortune 100 and hundreds of agencies worldwide.