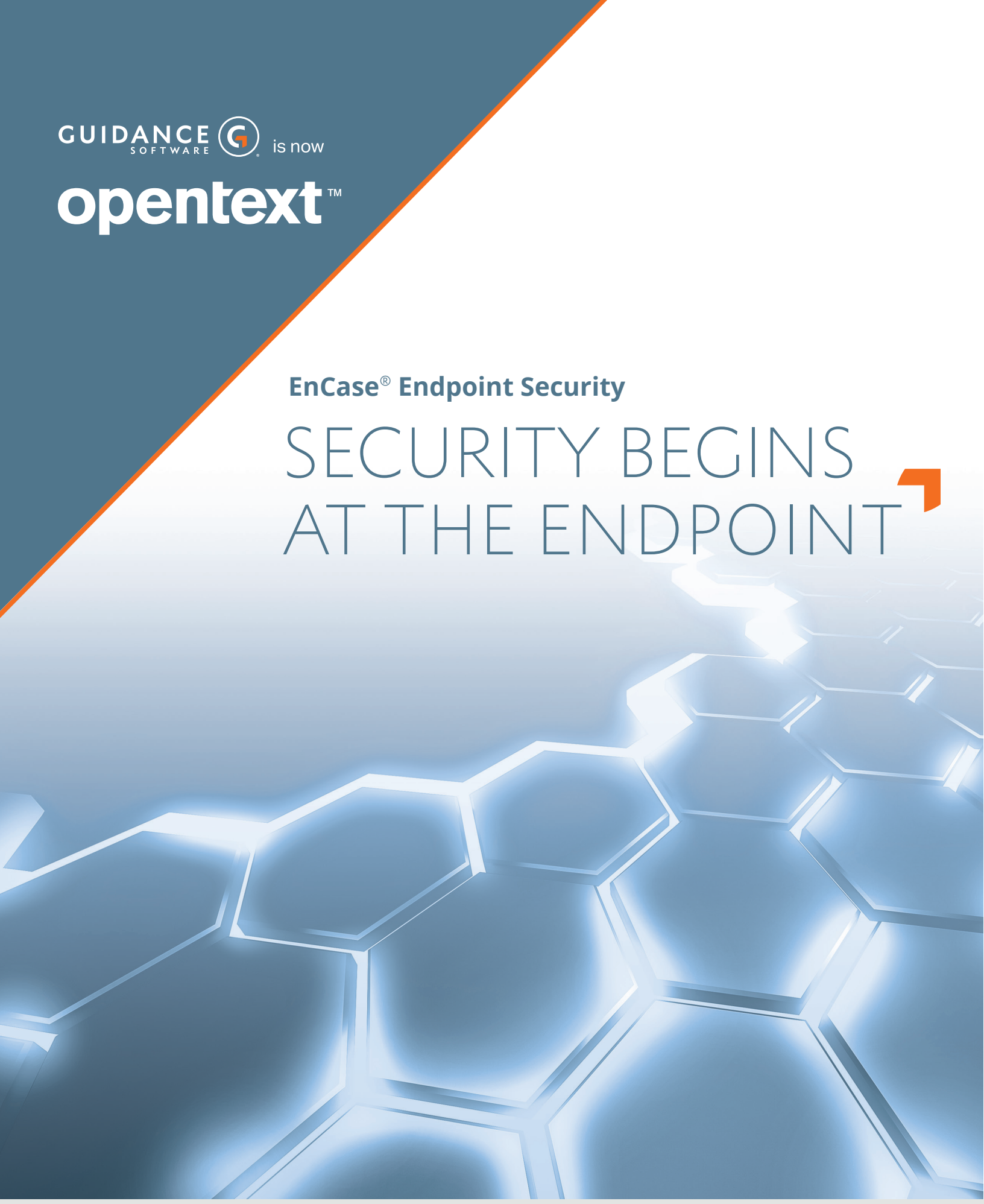
GUIDANCE SOFTWARE is now

opentext™

EnCase® Endpoint Security

SECURITY BEGINS AT THE ENDPOINT



experts@guid.com

guidancesoftware.com

EnCase Endpoint Security

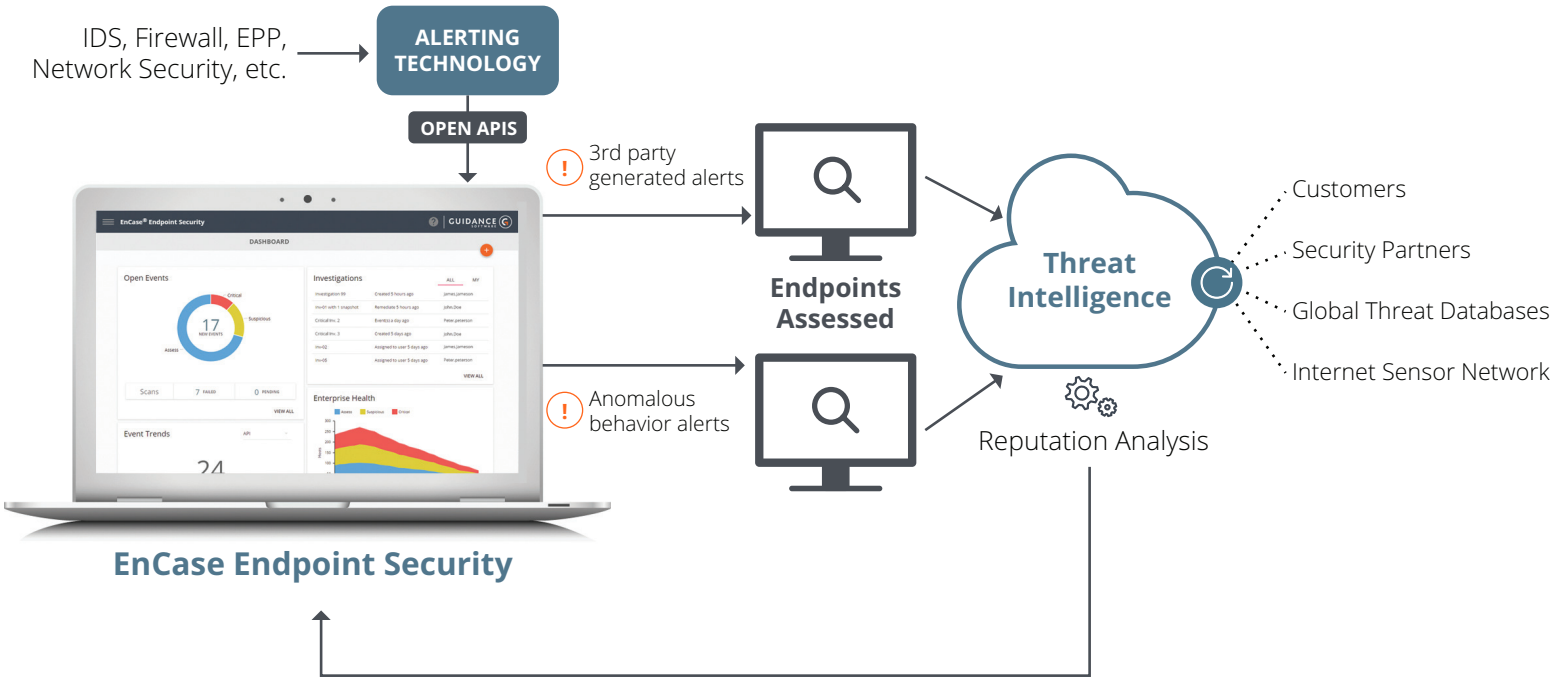
SECURITY BEGINS AT THE ENDPOINT

Cybercriminals are approaching an unprecedented level of sophistication and only a best-of-breed Endpoint Detection and Response (EDR) solution can provide meaningful value in a world of continuous compromise. Guidance Software has deep forensic heritage and 360-degree endpoint visibility that has become synonymous with the most proven, widely deployed, and most effective EDR solution available today.

The effectiveness of EnCase Endpoint Security lies in its ability to quickly validate every alert from various security technologies, accelerate detection of unknown intrusions, and surgically remediate threats before irreparable damage or loss of sensitive data.

Gartner named Guidance Software as the market share leader in their 2017 Competitive Landscape report for Endpoint Detection and Response with more than 13.4 million agents deployed worldwide

Threat Detection Process



Complete Endpoint Visibility with Advanced Detection

Modern attacks are designed to bypass both traditional and Next-Gen AV/EPP technologies. EnCase Endpoint Security, however, includes advanced anomalous behavior scans and embedded threat intelligence to identify and validate suspicious endpoint activities.

Detection features include:

- Integrated and streamlined alert notifications
- Real-time continuous monitoring and timeline analysis
- Cloud-based threat intelligence with automated reputation lookup
  - 13.5 billion file records updated every five minutes
  - Millions of real-time reputation input

Benefits:

- Save critical time by detecting threats at the point of attack
- Quickly prioritize events with actionable threat scores
- Reduce the time to triage security events by up to 90%
- Proactively hunt for threats

Actionable Insight for Fast Incident Response

Security teams often lose valuable time responding to false alarms, re-imaging infected devices, or manually coordinating between various security tools. EnCase Endpoint Security is purpose-built with security-first workflows designed for professionals working in Security Operations Centers (SOCs), Incident Response (IR) teams, and IT Operations to quickly triage security incidents and escalate only the most critical events for incident response.

Incident Response features include:

- Forensic-grade remediation of files, registry keys, and system processes
- Timeline and differential analysis for root cause analysis
- Ability to flag processes, IPs, or connections of interest
- Process tree visualization and navigation
- IOC scans that support YARA and STIX

Benefits

- Reduce the time to remediate a threat by approximately 77%
- Malicious artifacts, processes, and files cannot be reconstituted once removed
- Uptime and productivity maintained with remote surgical remediation
- Retrospective visibility into all endpoint activity

As next generation infrastructure continues to evolve, the lines between storage, networking, and compute silos will blur. What remains constant, however, is the 'endpoint' where the struggle to manage agent bloat wears on. Guidance Software's single lightweight and unified agent works across all Guidance products, with optional passive and active modes.

In addition to an enhanced agent, open RESTful APIs provide the option to integrate Endpoint Security with third-party security tools in order to leverage existing investments.

Whether you choose to utilize the Endpoint Security user interface or opt for a single-pane-of-glass experience via another tool, the choice is yours.

EnCase Endpoint Security is truly an integrated best-of-breed EDR solution that will best position your organization against the most advanced forms of attack at the endpoint, whether from external actors or internal threats. Contact us today to learn more about Endpoint Security and to schedule a demonstration.

- **Kernel-level visibility into the widest variety of relevant artifacts**
- **1MB in size and <1% CPU**
- **Use cases include:**
  - Desktops & laptops
  - Servers
  - Point-of-sale terminals
  - ATM machines
  - Printers
  - Industrial control systems
  - Medical devices

GUIDANCE SOFTWARE

From beginning to endpoint.

ABOUT GUIDANCE

Guidance exists 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. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 35 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.

REQUEST A DEMO

experts@guid.com | 888.999.9712 | guidancesoftware.com