opentext™

Product overview

OpenText EnCase Endpoint Security

Deep endpoint visibility for earlier detection of insider and external threats, alerts validation and forensic-grade incident response including complete remediation

Earlier detection of endpoint security threats

Faster response to malicious activity of up to 90%

More efficient recovery from security incidents of up to 77%

Greater visibility via continuous monitoring of endpoints

The rapidly evolving cyber threat landscape is reducing the effectiveness of traditional perimeter and signature-based security systems. Additionally, Security Information Event Management (SIEM) and other alerting technologies are bombarding security teams with alerts, overtaxing their ability to analyze, prioritize and respond to threats before irreparable damage or data loss occurs. Organizations need to establish better visibility into endpoints to face these challenges.

OpenText™ EnCase™ Endpoint Security provides security teams with 360-degree endpoint visibility to validate, analyze, scope and respond to incidents quickly and completely. As a best-of-breed Endpoint Detection and Response (EDR) solution, it empowers organizations to tackle the most advanced forms of attack at the endpoint, whether from external actors or internal threats. EnCase Endpoint Security is designed with automation and operational efficiencies that help incident responders find and triage security incidents faster to reduce the risk of loss or damage.

Earlier detection of endpoint security threats

EnCase Endpoint Security enables security teams to redefine their workflow from passive 'alerting' mode to proactive 'threat hunting', actively scanning for anomalies indicative of a security breach. It creates a baseline of endpoint activity used to detect anomalous behavior or recreate how a data breach occurred using historical intelligence.

opentext™

"It helps us mitigate any kind of cyber issue, any kind of malware...and remove those threats from our network before there is any kind of a breach."

Fortune 500 Luxury Resort Group

Faster response to malicious activity

EnCase Endpoint Security accelerates response time, significantly reducing the risk of data loss and damage to systems. It reduces triage time by up to 90%, helping incident response (IR) teams validate and assess the impact of malicious activity – even polymorphic or memory-resident malware. Organizations can realize even greater efficiencies by integrating EnCase Endpoint Security with third-party alerting technologies via RESTful APIs.

More efficient recovery from security incidents

Once a threat is identified, EnCase Endpoint Security surgically contains and remediates malicious files, processes and registry keys without the need to conduct a full wipe-and-reimage. This approach avoids the costly system downtime, loss in productivity and lost revenue associated with traditional forms of remediation, reducing the time to remediate a threat by approximately 77%.

Greater visibility via continuous monitoring of endpoints

Today's security teams require the ability to capture endpoint data on an ongoing basis to quickly identify changes and create a historical timeline of activity for root-cause analysis. Configurable realtime, continuous monitoring capabilities provide the necessary level of visibility and insight required to monitor all network endpoints at any scale.

OpenText EnCase Endpoint Security features

Complete endpoint visibility with advanced detection	Integrated and streamlined alert notifications with realtime, continuous monitoring and timeline analysis; cloud-based threat intelligence and automated reputation lookup are also available.
Tools for actionable insight	• 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. • Forensic-grade remediation of files, registry keys and system processes.
Automated response workflows	Purpose-built automation tools and integrations with open RESTful APIs to mitigate security risks and reduce costs associated with incident response.
Bi-directional Splunk integration	Ensures all event data generated within EnCase Endpoint Security can be automatically exported into Splunk, including all processes, DLLs, connections and DNS. Bi-directional integration enables incident responders to triage their security events directly within Splunk for a "single-pane-of-glass" experience.
Differential analysis	Enables security analysts to quickly conduct efficient root cause analysis. With any given security event, incident responders can rapidly compare snapshots from the target endpoint to any other baseline snapshot—whether on the same machine or a different one.
Metadata scans	Allows users to create data collection scans that take daily snapshots of metadata, like DLLs and processes, from one or more host machines for efficient review, comparison and analysis.
Secure Authentication for EnCase (SAFE) architecture	Authenticates users, retains transaction logs and brokers secure data transmission to ensure no information can be intercepted and interpreted.
Intuitive UI and workflows	A modern and streamlined user interface, intuitive for Security Operations Center (SOC) analysts or early Incident Response (IR) responders, to reduce human error and save time and frustration.

opentext™

"No other product in the world could do this. It's our secret weapon."

Fortune 500 Global
Automobile Manufacturer

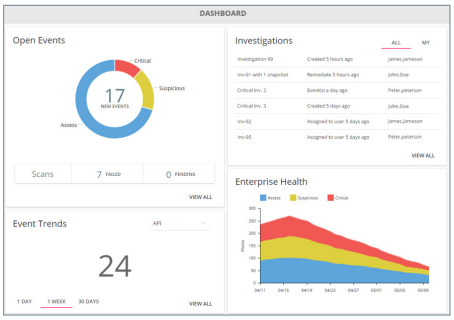
Learn more

See the demo

Keep up to date

OpenText LinkedIn

- **Training—**OpenText offers a wide variety of professional training programs and industry recognized certifications to help you develop expertise in EnCase software and forensic security.
- **Process and operation development—**The OpenText Professional Services team leverages extensive experience to craft response playbooks and custom workflows to drive the success of corporate security teams. OpenText consultants will implement the necessary technology, middleware and workflow automation across tools to ensure that organizations are prepared when the inevitable incident strikes.
- **360° endpoint threat assessment—**The OpenText Professional Services team will perform a comprehensive scan of the enterprise's environment to expose any hidden threats by leveraging cloud-based, agentless technology. Because there is no agent to deploy, the assessment can be set up within minutes of arrival, ensuring minimal impact to corporate operations and systems.
- **Threat triage and Incident Response—**In case of a breach or detection of a potential threat during threat assessment, OpenText provides highly skilled digital forensic incident response (DFIR) professionals with decades of forensic investigation and incident response experience to help triage and remediate the issue through a complete forensics investigation.
- **EnCase Advanced Detection—**A unique combination of detection techniques, machine learning, orchestration and automation adds active breach detection to OpenText EnCase Endpoint Security.



EnCase Endpoint Security Dashboards help security teams quickly prioritize alerts and make evidence-based decisions to investigate or remediate threats.

Unlike other tools in the market, EnCase Endpoint Security is the most complete threat detection and response solution. It eliminates the time it takes to detect, validate, triage, investigate and remediate known and unknown threats lurking across the enterprise, unseen by perimeter and network solutions. An organization's security is simply not complete without the endpoint visibility provided by EnCase.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- opentext.com/security

opentext.com/contact Twitter | LinkedIn