opentext™

PRODUCT OVERVIEW

OpenText™ EnCase™ Endpoint Security

Deep endpoint visibility for earlier detection of advanced external and insider threats and alert triage and fearless response, including comprehensive remediation

Realtime alerts of compromise

High-fidelity response and recovery

Scalability Cover *all* enterprise 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 responders find and triage security incidents faster to reduce the risk of loss or damage.

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 time significantly reduces the risk of data loss and system damage

Early detection of enterprise security threats with 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.

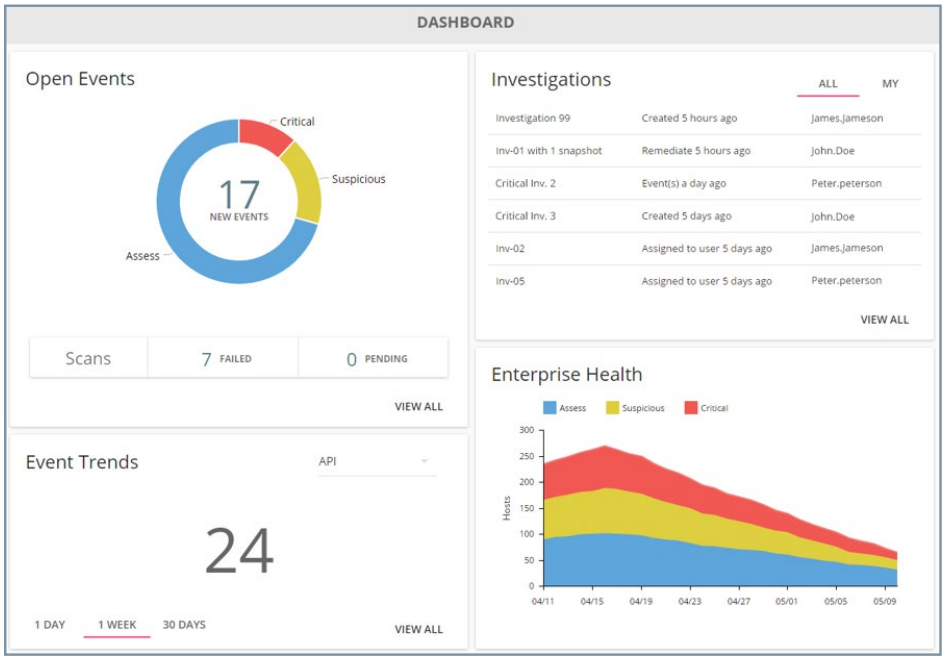
Response to malicious activity with EnCase Endpoint Security accelerates overall response time, significantly reducing the risk of data loss and system damage. It reduces triage time by up to 90 percent, helping incident response teams validate and assess the impact of malicious activity—even polymorphic or memory-resident malware. Organizations can also integrate EnCase Endpoint Security with third-party alerting technologies via RESTful APIs.

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 percent.

Greater visibility via continuous monitoring of endpoints

Today's security teams require the ability to continuously capture endpoint data 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.



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

opentext™

OpenText™ EnCase™ Endpoint Security features	
Continuous endpoint monitoring	Unearth cyber threats in real time across the enterprise with behavior-based detections, inspired by industry-leading frameworks including Mitre ATT&CK®. Included custom anomaly rule builder for focused detection of environment-specific issues.
Embedded threat intelligence	Automatically prioritize alerts by severity with complete file reputation and IP reputation analysis, displayed in a single view.
Dynamic analysis (sandboxing)	Fully assess potential zero-day threats with dynamic analysis of unknown files and processes for additional threat intelligence and alert contextualization.
Comprehensive remediation	Fully respond to and recover from cyber threats by isolating infected endpoints to reduce lateral spread. eliminating malicious processes, deleting corrupted files and resetting affected registry keys on compromised endpoints. Leverage a simplified and streamlined response for Tier I security analysts and a complete DFIR toolkit for Tier II/III to identify patient zero, create new IOCs, discover unknown threat vectors and forensically investigate challenging security issues.
Orchestration with automated response	Create on-demand actions with automated response for event post-processing. Add as many custom actions as needed to drive desired outcomes.
Off-VPN anomaly detection	Collect anomaly and telemetry data from off-VPN endpoints for quick detection of anomalies and immediate reporting. Ability to install multiple telemetry listener components for scalable solutions.
Open, RESTful API and Software Development Kit (SDK)	Leverage integration and automation with adjacent security solutions in the environment for efficient security operations.
Content Security and Exfiltration Defense	Monitor cloud repositories for behaviors indicative of a data security breach or insider threat.
Full endpoint access with a low resource agent	Maximize collection capabilities and minimize business disruption and end user CPU bandwidth usage with the lightest agent available.
Efficient operations for Tier I analysts	Bring the power of EnCase to junior analysts and incident response staff with a simplified UI and user workflows.

Training

OpenText offers a variety of professional training programs and industry-recognized certifications to help users develop expertise in EnCase software and enterprise security.

Managed Security Services

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 implement the necessary technology middleware and workflow automation to ensure that organizations are prepared when the incident strikes.

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 forensic investigation.

opentext™

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**
- **Twitter** | **LinkedIn**

opentext.com/contact