OpenText™ EnCase™ Endpoint Security

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

Real-time 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™ EnCase™ Endpoint Security provides security teams with 360-degree endpoint visibility to validate, analyze, scope and respond to incidents quickly and completely.

EnCase™ 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 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 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.

EnCase Endpoint Security Dashboards help security teams quickly prioritize alerts and make evidence-based decisions to investigate or remediate threats.
The key features are as follows:

<table>
<thead>
<tr>
<th>OpenText™ EnCase™ Endpoint Security features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous endpoint monitoring</td>
</tr>
<tr>
<td>Embedded threat intelligence</td>
</tr>
<tr>
<td>Dynamic analysis (sandboxing)</td>
</tr>
<tr>
<td>Comprehensive remediation</td>
</tr>
<tr>
<td>Open, RESTful API and Software Development Kit (SDK)</td>
</tr>
<tr>
<td>Content Security and Exfiltration Defense</td>
</tr>
<tr>
<td>Full endpoint access with a low resource agent</td>
</tr>
<tr>
<td>Efficient Operations for Tier I Analysts</td>
</tr>
</tbody>
</table>

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 will implement the necessary technology, middleware and workflow automation across tools to ensure that organizations are prepared when the inevitable 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.

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
- encase@opentext.com

opentext.com/contact  Twitter  LinkedIn