Microsoft Azure

OpenText™ EnCase™ Endpoint Investigator in the Microsoft Azure Cloud

Bringing the power of the cloud to forensic investigations

- Connect to the cloud
- Reliable acquisition of evidence
- Deep forensic analysis
- Mobile collection for 27,000-plus profiles
- Image analysis
- Broad OS/ decryption support

SC 2020 awards Winner

About OpenText™ EnCase™ Endpoint Investigator:

OpenText EnCase™ Endpoint Investigator is the gold standard identifying, collecting, and analyzing digital data necessary for investigations that involve physical access to a target device. Comprehensively acquire from the widest range of devices and cloud sources to support IT and law enforcement investigations. Accurately and defensibly investigate target information in Microsoft Azure and boost investigation power with cloud processing.

For digital investigations, examiners need to be able to prioritize, collect and decrypt evidence from a wide variety of devices while maintaining their integrity. The process needs to be quick, efficient, repeatable and defensible, with the ability to create intuitive reports.

OpenText™ EnCase™ is recognized globally as the gold standard for digital forensics and is a court-proven solution built for deep-level digital forensic investigation, powerful processing and integrated investigation workflows with flexible reporting options.

With EnCase in the Microsoft Azure Cloud, internal investigators and law enforcement can quickly grant external access to reviewers and collaborators on case findings.

Use case No. 1: Collaborative investigations via Azure

Quickly grant external access to review and collaborate on case findings via the cloud

As investigations evolve, it may become necessary to share case data with an outside source for collaboration and input into the investigation. For example, a forensic investigator with a municipal law enforcement team might need to share evidence with federal law enforcement personnel if the case includes federal violations.

Third-parties can access EnCase Endpoint Investigator on Azure via EnReview for OpenText EnCase – an application that enables secure access to case data for outside consulting. The outside reviewer then contributes to the investigation and delivers changes back to the original investigator to incorporate the results and accept any changes.

Use case No. 2: Scale evidence processing with EnCase on Azure

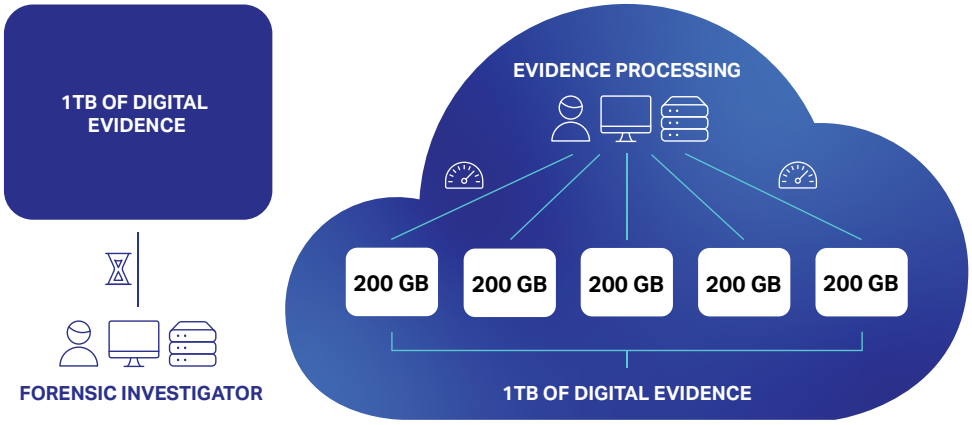
Leverage the cloud to process large amounts of case data

As operations have modernized, the proliferation of data means that the scope of digital investigations has changed dramatically. Volumes of data must be analyzed for relevant evidence to create a clear picture of what did or did not take place – with some processes requiring analysis of terabytes of data. Traditional endpoints have hardware limitations, and processing evidence in extremely high volumes could lead to case delays and headaches for investigators.

opentext™

Leveraging Microsoft Azure to process high volumes of case data allows organizations to.

1. Push evidence to the cloud for processing to preserve capacity and bandwidth on hardware
2. Assign the cloud processor node in Azure to accept evidence
3. Process evidence with horizontal scaling



HORIZONTALLY SCALE PROCESSING POWER WITH THE CLOUD

Use Case No. 3: Investigate evidence in the cloud

Preview, collect and analyze digital evidence stored in the cloud

As organizations shift operations to the cloud, investigative teams must also keep pace and increase visibility and control in cloud environments to maintain continuity of investigations. User and application interactions in cloud environments are next-to-impossible to view and analyze without brokered access between the cloud vendor and investigative technology.

With EnCase on Azure, organizations can comprehensively investigate digital evidence, both off-cloud and in the cloud, for complete and accurate findings.

1. Preview

Not all data needs to be collected. Understand quickly what is relevant to your investigation by previewing data, and only collect what is essential from Azure.

2. Collect

Forensically acquire digital data for investigations. Gather and collect necessary evidence in a defensible and accurate way.

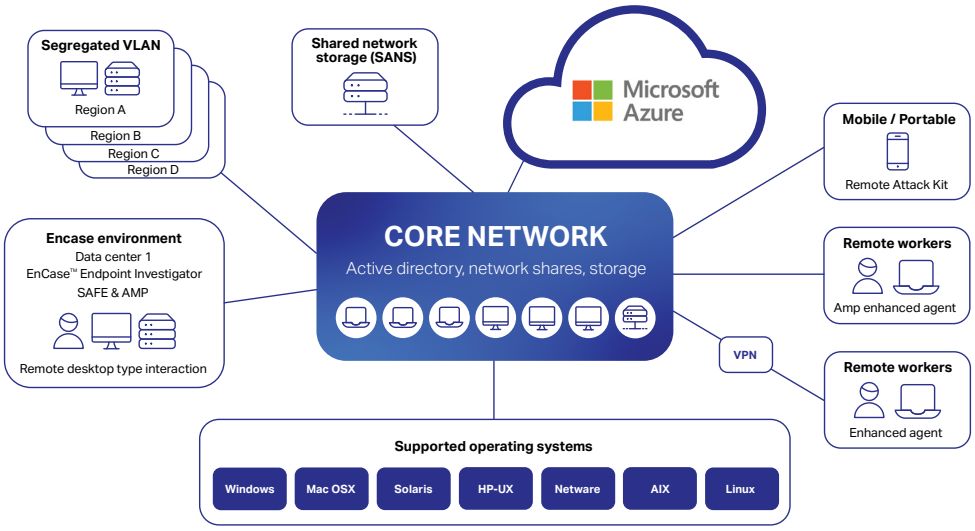
3. Analyze

The most important part of any investigation is the ability to analyze collected evidence. EnCase is built with the investigator in mind, providing a wide range of capabilities that enables deep forensic analysis and fast triage analysis from the same solution.

4. Report

EnCase Forensic provides a flexible reporting framework that empowers investigators to tailor case reports to meet specific needs. Comprehensive and triage reporting options are built in to create reports for a wide range of audiences and easily share them across the organization.

opentext™



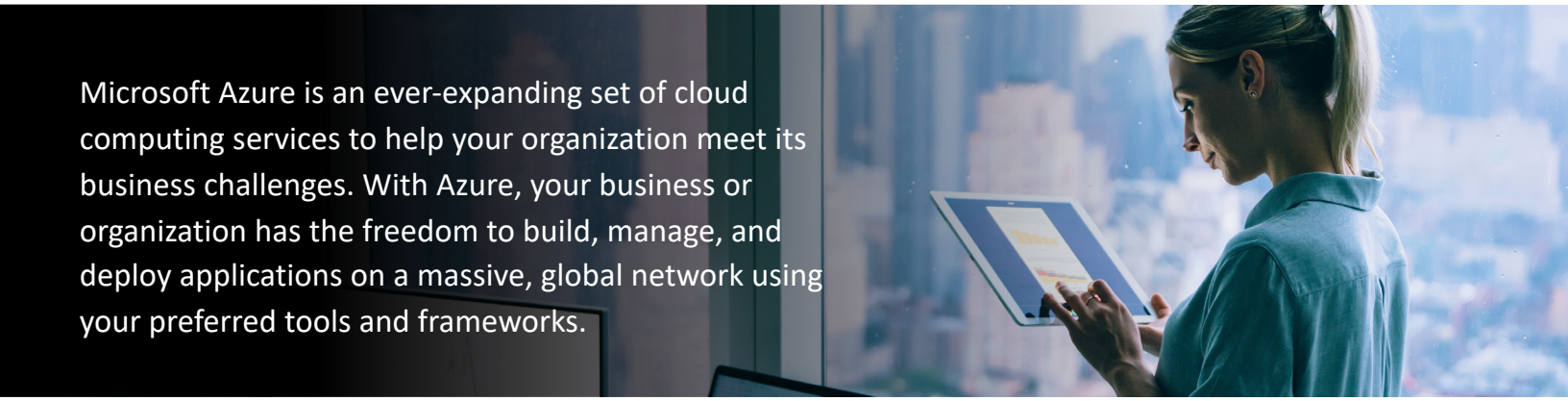
Benefits

Same trust as EnCase, now in the cloud	EnCase is the original digital investigation solution and continues to be the gold-standard. No other solution delivers the same level of access to digital data, alongside maximum trust and accuracy in collection and analysis.
Comprehensive access to all evidence	EnCase supports the widest array of devices, operating systems, digital artifacts, and encryption technologies – enabling teams to *investigate everywhere*.
Defensible investigation findings	EnCase has a lengthy history of court acceptance, meaning when an investigation is performed, teams can rely on accurate and defensible results.
Guided workflows for junior personnel	Templates and guided workflows assist junior investigators in knowing what's relevant and how to proceed in an investigation.
Simplified reporting	Templatized reporting helps to create compelling and easy-to-read reports that can be shared for any case. Display investigation findings in a compelling and easy-to-understand way.

Copyright © 2020 Open Text. All Rights Reserved. Trademarks owned by Open Text.
For more information, visit: https://www.opentext.com/about/copyright-information (09/2020)16507-Endpoint-EN

opentext™

Microsoft Azure



Microsoft Azure is an ever-expanding set of cloud computing services to help your organization meet its business challenges. With Azure, your business or organization has the freedom to build, manage, and deploy applications on a massive, global network using your preferred tools and frameworks.

WHY AZURE

Be future-ready

Continuous innovation from Microsoft supports your development today and your product visions for tomorrow. With 1,000+ new capabilities in the past year, you can build on the latest advancements in AI, blockchain, Kubernetes, containers, and databases to keep you ahead of the curve.

Our enterprise-grade analytics solution outperforms the competition, costs less, and is fully compatible with your existing development, BI, and data science tools.

Build on your terms

You have choices. With our commitment to open source and support for all languages and frameworks, you can build and deploy how you want to. Take advantage of the full-featured, integrated development environments with built-in support for Visual Studio and Visual Studio Code, the most popular IDEs trusted by 15M+ developers.

We embrace open source, drive innovation through collaboration, and contribute back to the community.

Operate hybrid seamlessly

On-premises, in the cloud, and at the edge—we'll meet you where you are. Integrate and manage your environments with tools and services designed for hybrid cloud.

Enhance security, simplify access, and set smart policies across your different environments with a single identity platform trusted by 90 percent of enterprises globally.

Trust your cloud

Get security from the ground up, backed by a team of experts, and proactive compliance trusted by enterprises, governments, and startups.

With its $1B+ investment in security R&D and 3,500 cybersecurity experts, security is foundational for Azure.

Learn more: www.microsoftazure.com

Microsoft Partner
Microsoft
Gold Application Development
Gold Cloud Platform
Silver Datacenter