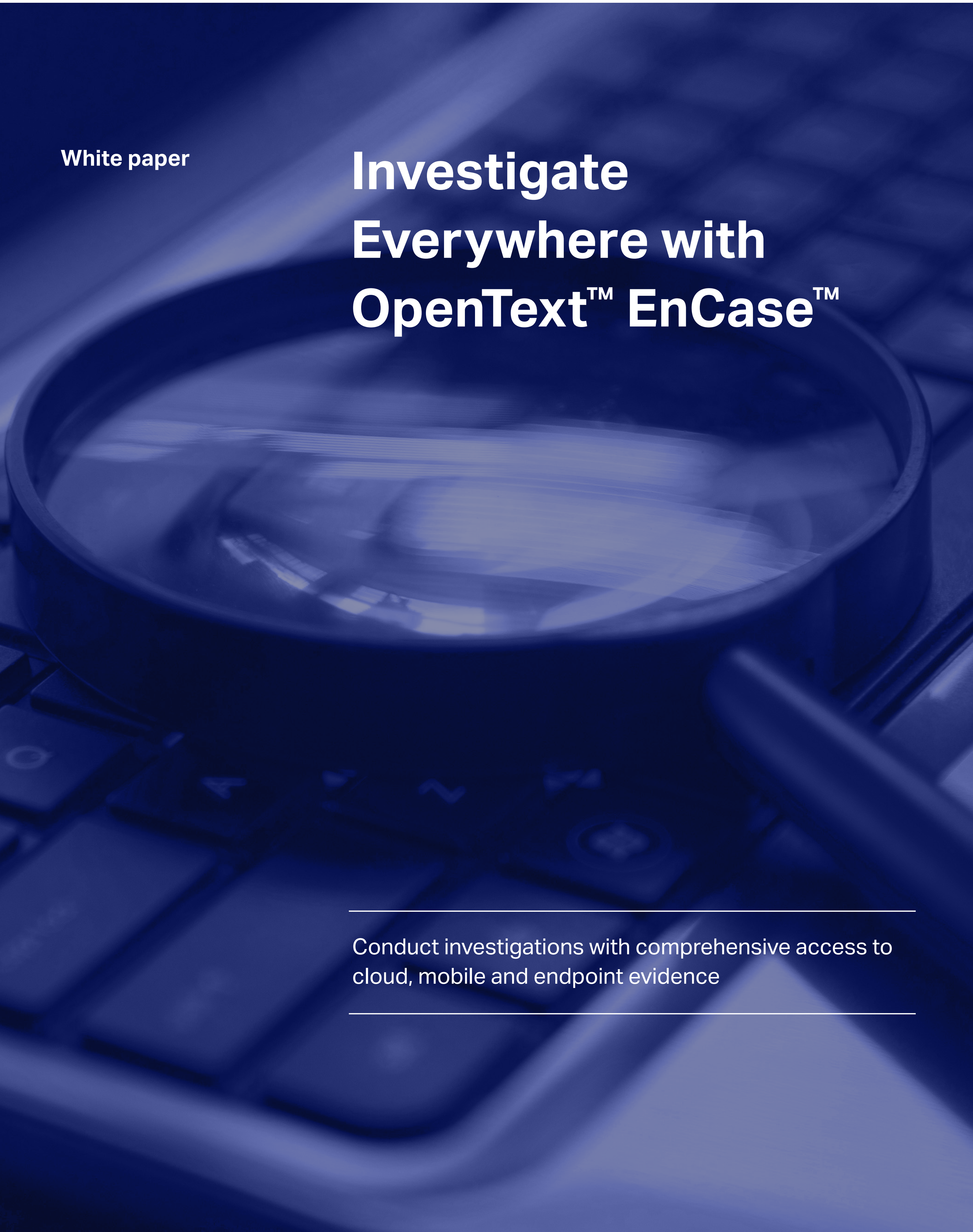
opentext™



White paper

Investigate Everywhere with OpenText™ EnCase™

Conduct investigations with comprehensive access to cloud, mobile and endpoint evidence

Contents

Introduction 3

Challenges with modern digital investigations 4

Investigate Everywhere with OpenText™ EnCase™ 5

- The Enhanced EnCase agent 5
  - Devices 5
  - Operating Systems 5
- Cloud shares and content repositories 6
- Encryption technologies 6
  - Apple T2 Security chip 7

EnCase™ Endpoint Investigator 7

EnCase™ Mobile Investigator 8

OpenText™ Media Analyzer 8

Training and Professional Services 8

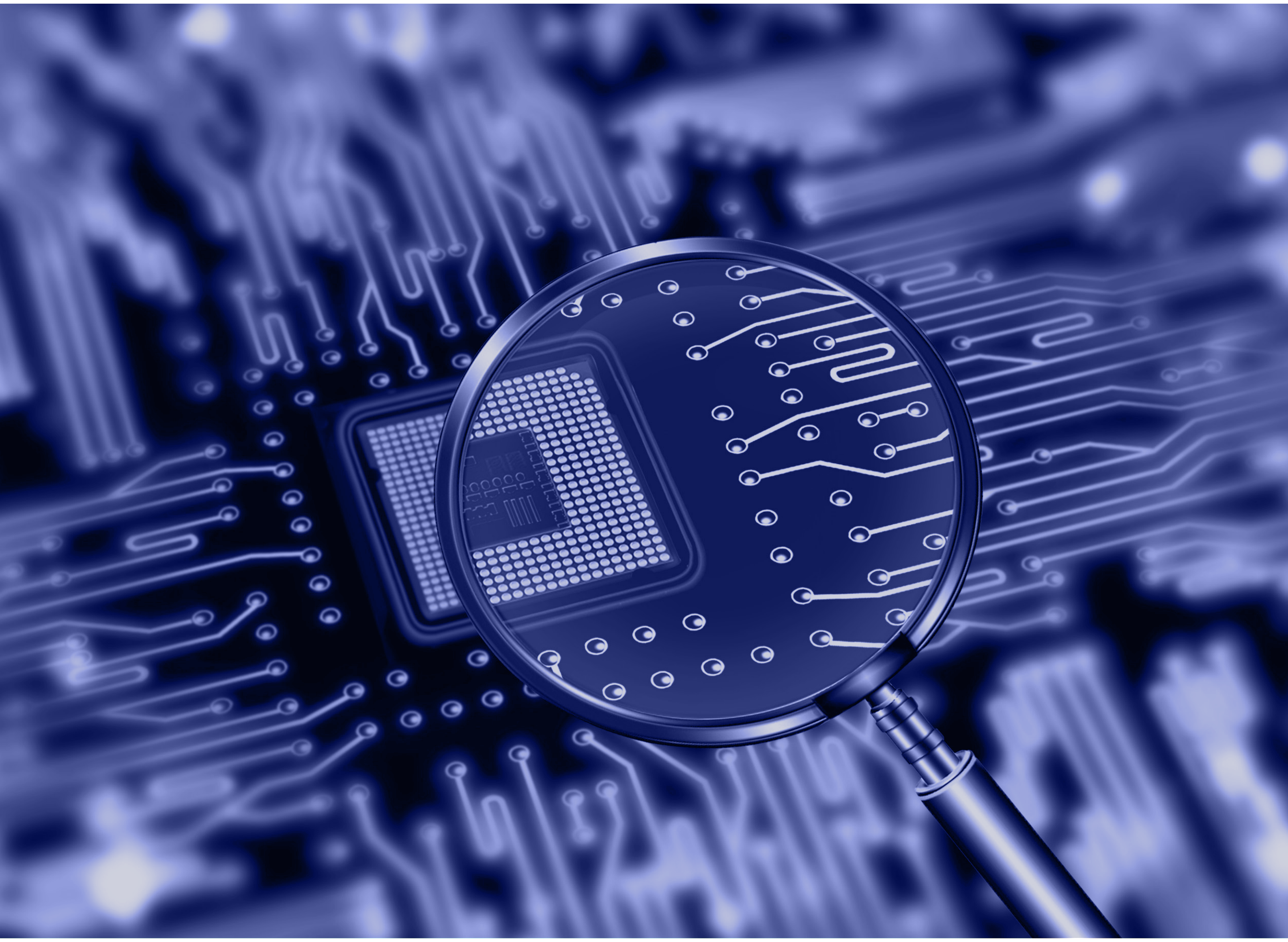
Introduction

Modern digital investigations can involve many systems and devices across locations and geographies, and can even involve local and national law enforcement or regulatory bodies. Without a digital solution with remote access, investigation teams must retrieve the physical device and transport it to a lab for processing, which can disrupt productivity and a timely resolution to the investigation.

Sensitive investigations must be conducted without the acquisition target's foreknowledge to prevent any potential tampering with or deletion of evidence.

Digital investigations become even more complex when the employee under investigation operates in a remote or work-from-home environment, leading to challenges around investigation fidelity and inability to access 100% of the required evidence.

OpenText allows for security and investigation teams to have full access to digital evidence, no matter the device or location, and to investigate everywhere.



Challenges with modern digital investigations

Digital evidence is everywhere and is frequently required for investigations into fraud, employee misconduct or separation, IP theft and DFIR. These investigations can involve legal / law enforcement, creating the need for accurate and defensible findings.

For example, a routine employee investigation could surface material that would require law enforcement involvement because the offense is criminal. Improper evidence handling can lead to more risk for the organization, including legal action or criminal charges.

Inability to access relevant digital evidence on devices where it is stored leads to investigative roadblocks. Incomplete information leads to incomplete investigations - meaning that investigators that are not able to access 100% of relevant digital evidence to a given case might miss a metaphorical "smoking gun" that could lead to an incorrect case outcome. Digital investigations must also be discreet, due to the possibility of evidence deletion or corruption by an insider or target of an investigation.

Modern digital investigations are further complicated by dramatic shifts to work-from-home environments and off-network endpoints. Accessing endpoint data for investigations in traditional ways can be challenging under normal circumstances, but the proliferation of off-network endpoints compounds that challenge dramatically.

Investigate everywhere with OpenText EnCase™

Investigate everywhere with the most powerful and efficient solution available for remote, discreet and secure internal investigations.

To meet the stringent requirements of modern investigations, complete visibility and access to enterprise endpoints is a necessity, no matter the location, device or file type that requires investigation.

Increase confidence in investigation findings using EnCase™ technology that is trusted by corporations and governments with a proven record of court acceptance. No other solution offers the same level of forensic access, capabilities and flexibility.

The Enhanced EnCase™ Agent collects from the broadest array of systems and endpoints while also delivering the highest degree of forensic accuracy in all findings.

Devices

Most investigations take place on traditional endpoints, meaning the bulk of evidence is contained on workstations and servers. At times, investigations can involve auxiliary devices and evidence locations, meaning investigative teams should be prepared to collect from any device or condition seen in the field.

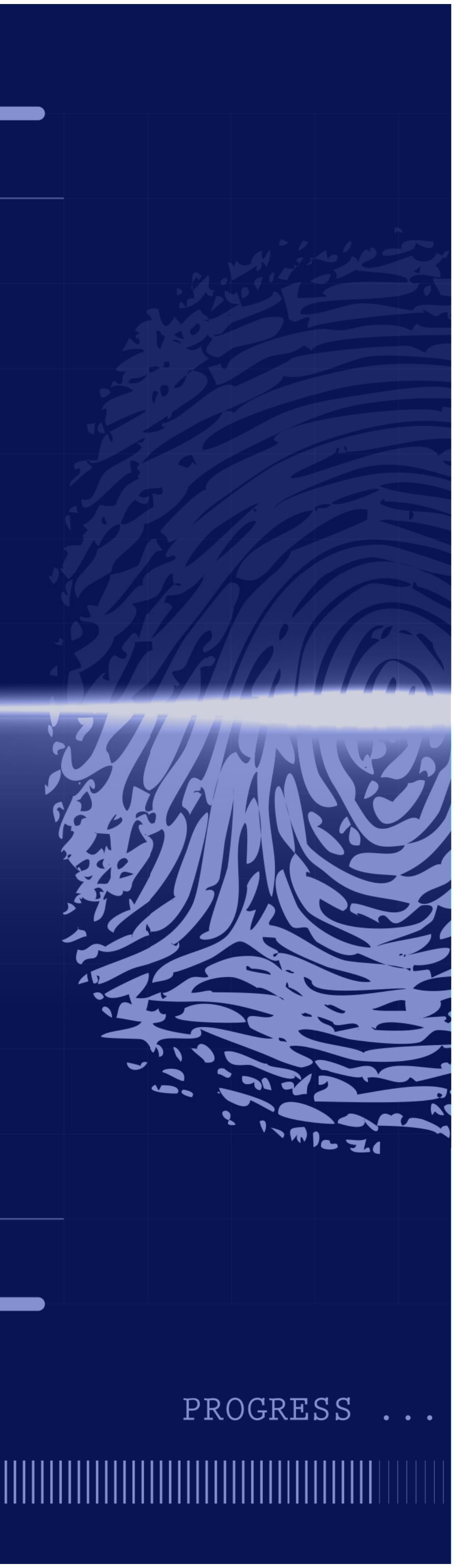
EnCase™ Endpoint Investigator can collect from:

- Traditional endpoints, including Windows, Mac Linux based devices
- Server architectures
- Mobile devices
- IoT / ARM devices

Operating System support				
Target OS	Versions	x86	x64	ARM
AIX	5.1, 5.2, 5.3, 6.1, 7.1	✓	✓	
HPUX	11.0, 11.1x, 11.2x	✓	✓	
Linux Kernels	2.6.4 or higher with procfs	✓	2.6.9 or higher with procfs	Linux ARM and Raspberry Pi
macOS	10.6 - 10.15		✓	
Red Hat Enterprise Linux	7, 8	✓	✓	
Solaris	9, 10, 11.3, SPARC only	9 and 10, SPARC only	✓	
Windows	Vista, 7, 8, 8.1	✓	✓	
Windows 10	1507 - 1809, IoT Core	✓	✓	IoT Core
Windows Server	2008, 2008 R2, 2012, 2012 R2, 2016, 2019	2008 and 2012 only	✓	

Enhanced EnCase Agent—collect and investigate offline endpoints

- **Lightweight**—8MB at rest
- **Low impact**—brief spike to 200MB during moment of collection
- **Discreet**—will not tip off acquisition target



Cloud shares and content repositories

If the investigation involves an insider threat, IP theft, or movement of sensitive data stored in a cloud data share, reverse compatibility is a requirement in order to ensure collection of all relevant investigation data. Cloud environments and content repositories support the monitoring of data as it ingresses and egresses the repository, but visibility into what takes place inside of the cloud environment is a separate and difficult challenge for investigative teams.

OpenText™ monitors cloud repositories for issues located in the following repositories:

- OpenText Documentum
- OpenText Content Suite
- OpenText InfoArchive
- OpenText Capture Center
- Microsoft SharePoint
- Microsoft SharePoint Online
- Microsoft OneDrive
- IBM FileNet
- Box
- G-Suite

As issues surface, investigators can dive deep into the details for full forensic analysis and response.

Encryption technologies

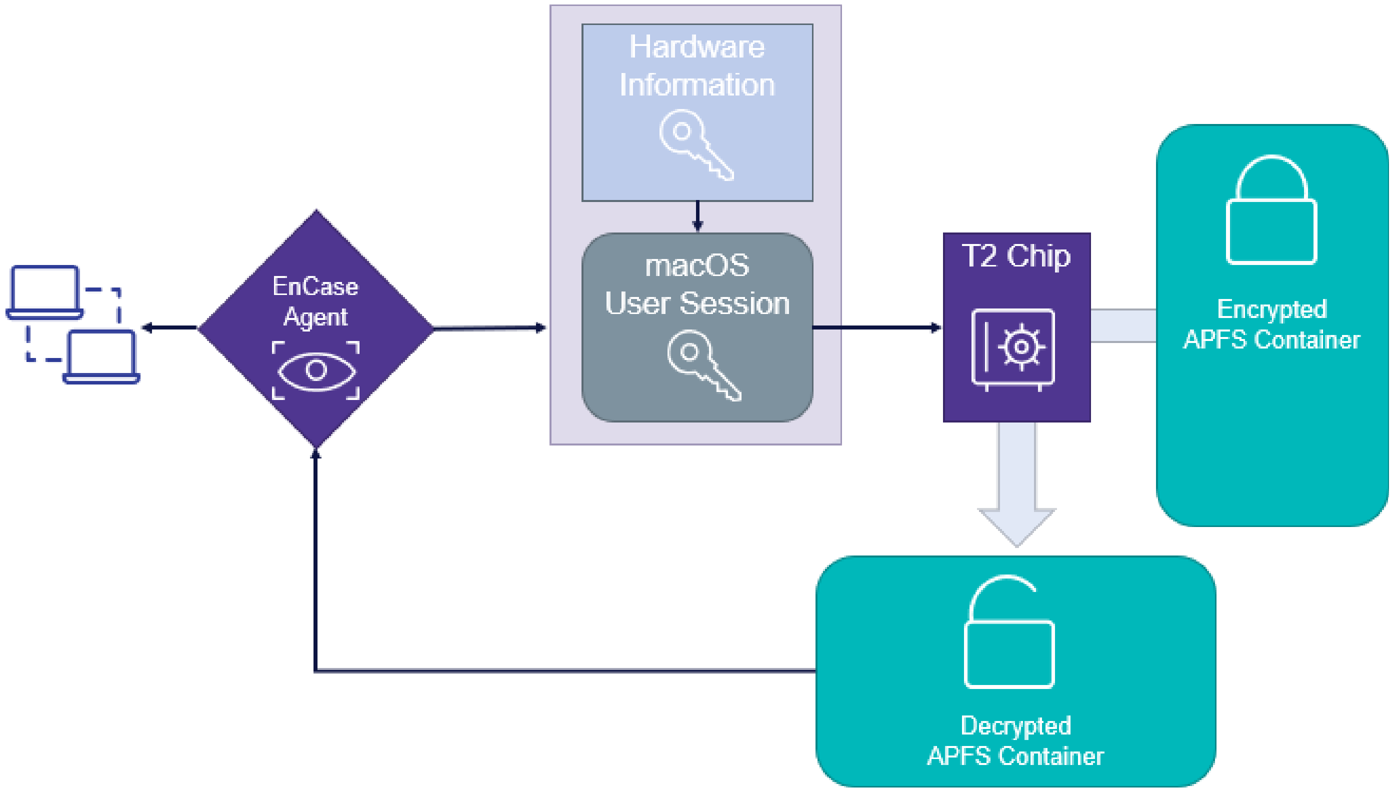
Encryption of the disk is a useful strategy to protect on-network endpoints. Full disk encryption scrambles and disguises native endpoint data so that it is inaccessible to off-network outsiders.

Investigators should rely on collection and analysis solutions to guarantee compatibility and the full access required for a complete investigation.

Encryption support with EnCase Endpoint Investigator now includes out-of-the-box abilities to investigate Apple devices secured with the T2 chip. Any modern Apple device with a T2 enabled security chip physically generates encryption to protect files in the Apple File System (APFS) from outside view and access. EnCase™ Endpoint Investigator allows investigative teams full access to encrypted drives and Apple devices secured with the T2 chip.

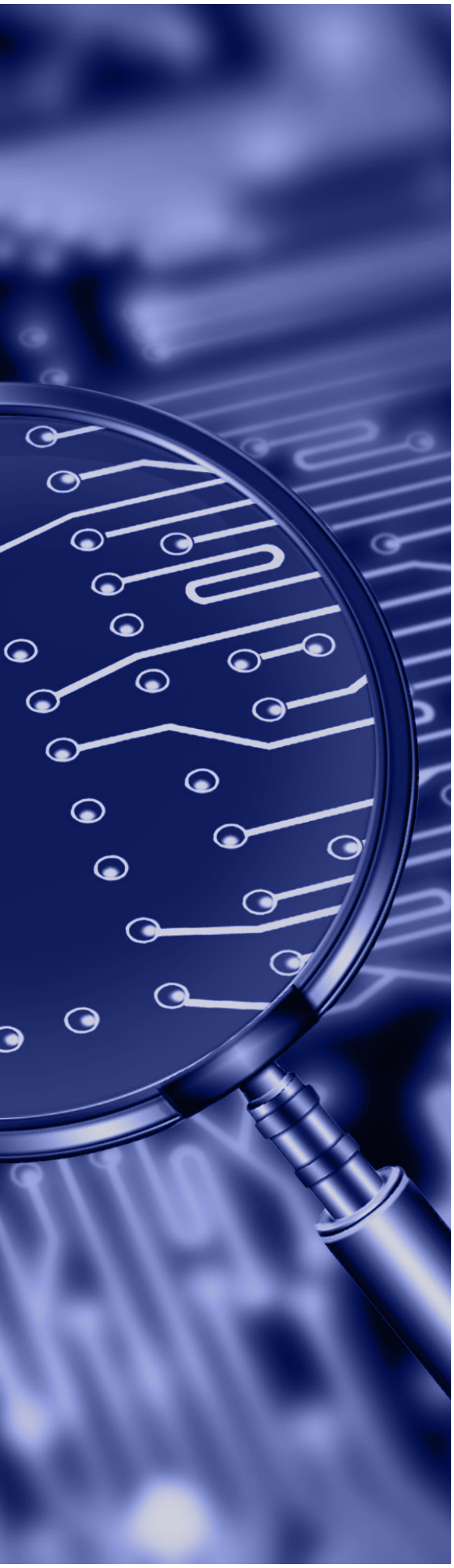
Apple devices with the T2 security chip:

- iMac Pro
- Mac Pro introduced in 2019
- Mac mini introduced in 2018
- MacBook Air introduced in 2018 or later
- MacBook Pro introduced in 2018 or later



Other supported encryption technologies

- Apple File System (APFS) Encryption
- Check Point® Full Disk Encryption (formerly Pointsec PC)
- Mobile Guardian (subsumed by Dell)
- Data Protection Enterprise Edition
- Full Disk Encryption
- Encryption Plus/Anywhere
- Hard Disk Encryption
- Endpoint Encryption (formerly SafeBoot)
- BitLocker® and BitLocker To Go
- SafeGuard® Easy and Enterprise (formerly Utimaco)
- PGP Whole Disk Encryption
- Endpoint Encryption
- Vera™ for Files
- SecureDoc Full Disk Encryption and Self-Encrypting Drives



Benefits of OpenText EnCase Endpoint Investigator

Comprehensive collection and access to all relevant endpoint data

Fully investigate any endpoint regardless of the OS, cloud source, encryption technology, or artifact type involved in the collection.

Reduce investigation time with rapid evidence processing

Investigators are no longer required to wait for the acquisition target to reconnect to the corporate network to continue investigations. Fully investigate off-network endpoints and remote users without interruption.

Maintain business continuity & discretion

Asynchronous connections ensure investigations aren’t interrupted if the endpoint goes offline or disconnects from the corporate network or VPN.

Reduce legal and regulatory risks

At times, investigations can involve collected evidence that requires involvement of law enforcement personnel or regulators. If the investigation leads to the domain of regulators, investigators can rely on defensible findings and forensic accuracy in collection results. EnCase™ supports high-fidelity investigations to ensure confident actions and resolutions.

Access all the evidence needed for an investigation and preserve that evidence forensically to avoid a negative case outcome.

Governing bodies and regulators are increasingly adding protections and mandates that involve digital investigation capabilities. GDPR, PCI-DSS, and Sarbanes-Oxley (among others) all include requirements that necessitate the collection and analysis of digital data to maintain compliance. Access all evidence needed for a compliance investigation, analyze for violations and preserve that evidence forensically.

Efficient collection and triage

Whole disk data investigations to examine all data content stored on the target machine hard drive, including encrypted data. Extensive triage capabilities to determine if any relevant information exists on the machine before performing a collection.

Multiple system search capability

Perform search and collection across multiple machines at a time, decreasing the time to investigation closure.

Deep-dive DFIR investigations

Create new IOC’s, forensically analyze “patient zero”, and assess complicated security detections with tier-3 incident investigations.

Learn more

Support digital investigations with an ecosystem of solutions and services from OpenText

EnCase Mobile Investigator

Add on component to EnCase™ Endpoint Investigator to collect and review from the widest variety of mobile devices. Find evidence within text messages, emails, call records, associated cloud repositories, internet history, photos, application data, and deleted data.

OpenText Media Analyzer

Add on component to EnCase Endpoint Investigator to identify images and video containing visual threats. Reduce manual review and identify adult content, violence, extremism, drugs, child abuse material, weapons, or other categories.

World class support via services and training

Create internal experts to meet the demands of modern investigations with proven training programs. Over 6,600 EnCE (EnCase Certified Examiner) certifications have been awarded.

Support installation, knowledge transfer, staff augmentation, guided assistance and more with OpenText Professional Services for security and investigations.

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