GUIDANCE SOFTWARE is now

opentext™

EnCase Endpoint Security

Detect Threats & Secure Your Data

Often the **custodians of sensitive and regulated data,** the domain of **content and data owners** is increasingly falling under the purview of regulations mandating **security and incident response** such as GDPR; **digital investigations** such as data breach notification laws; and **electronic discovery for legal matters**.

Agenda

Anthony Di Bello

- Who is Guidance Software
  - Business Overview
  - Solution Overview
  - Acquisition Rationale
- Today’s Data Security and Privacy Challenges
- EnCase Endpoint Investigator and EnCase Endpoint Security
- The Future of Information Security @ OpenText

GUIDANCE SOFTWARE is now

opentext™

About OpenText EnCase

Proven in the courtroom and trusted in the boardroom, we solve highly sensitive data risk management problems for the largest organizations in the world

About OpenText EnCase

Trusted by the largest global enterprises

Exelon. verizon✓ DEPARTMENT OF STATE · UNITED STATES OF AMERICA SOUTHERN CALIFORNIA EDISON An EDISON INTERNATIONAL® Company

intel Fidelity INVESTMENTS ORACLE DEPARTMENT OF ENERGY · UNITED STATES OF AMERICA

McDonald's Allstate. Deutsch USAA®

DELL™ Chevron COX. Walmart

Genentech Aetna® THE HOME DEPOT® Roche

CENTRAL INTELLIGENCE AGENCY · UNITED STATES OF AMERICA NOVARTIS MOTOROLA CSC

78 of the Fortune 100

#1 solution for Government agencies

48% of the Fortune 500

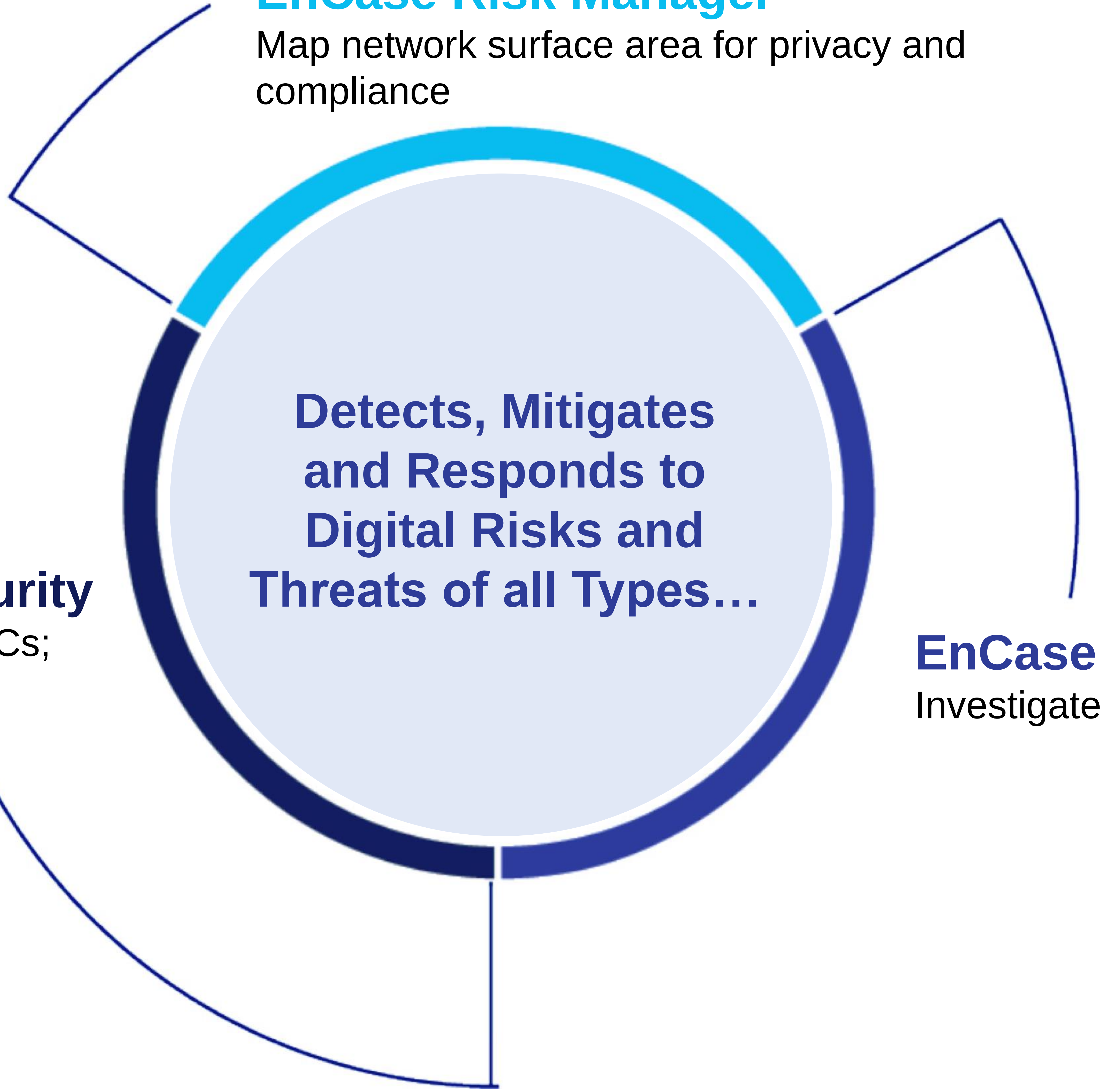
#1 tool for the incident response service providers; FireEye, KPMG, PWC, Deloitte, CSC, AT&T

More than 5,000 EnCE Certified Investigators

38M Agents Deployed

…and counting

Forensic security



EnCase Risk Manager

Map network surface area for privacy and compliance

Detects, Mitigates and Responds to Digital Risks and Threats of all Types…

EnCase Endpoint Security

Detect anomalies, malware, IoCs; validate, triage and remediate

EnCase Endpoint Investigator

Investigate analyze and produce evidence

Why Do Customers Choose EnCase?

Scalability to manage widest range of OS/File systems, networks, and devices

Deep visibility and powerful below the Operating Systems

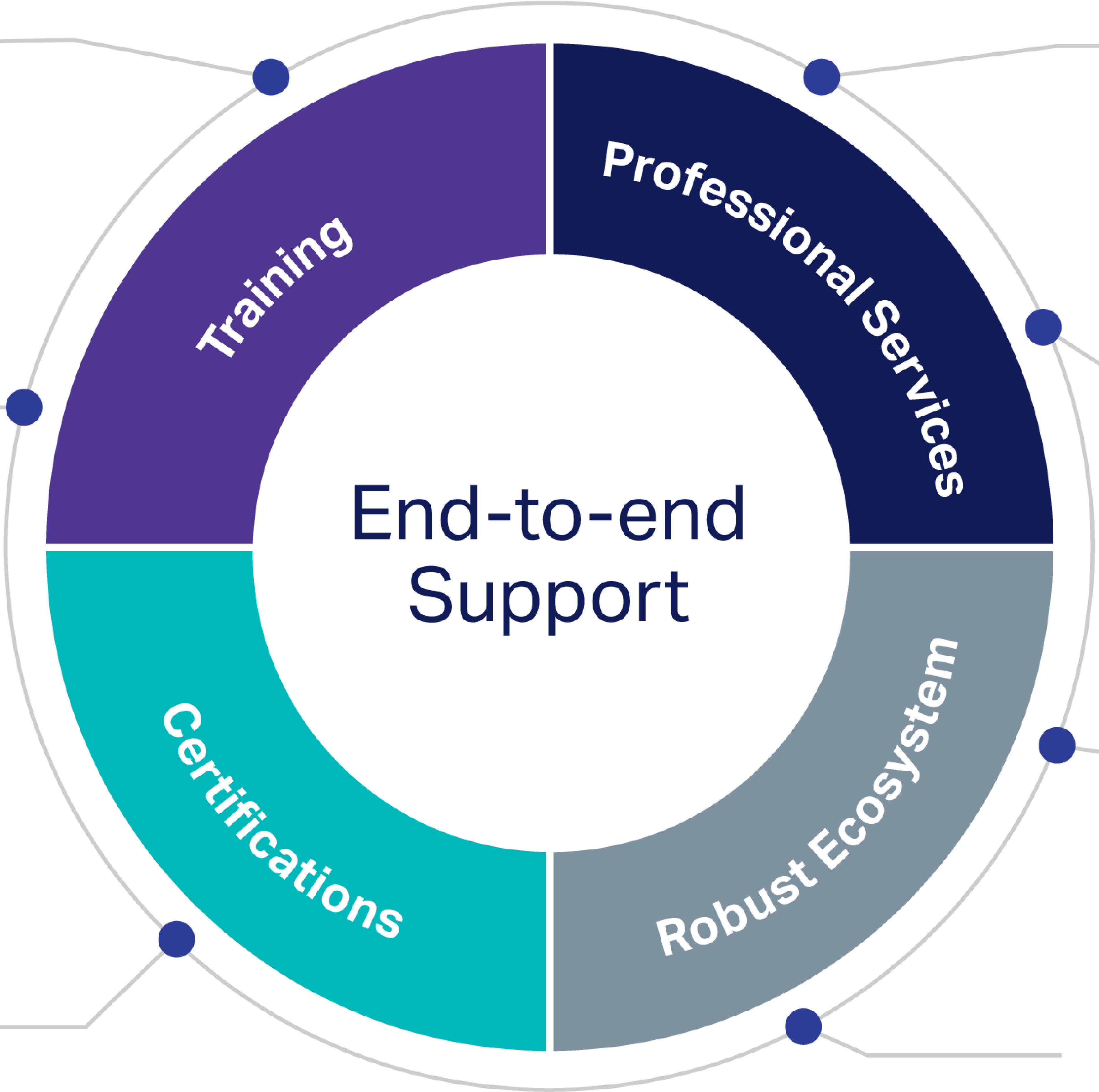
Effective solution for highly sensitive demands of risk management frameworks

Single agent architecture with low impact to end user devices

Trusted brand proven to support global requirements

Non-intrusive and comprehensive remediation

Intelligent services ensures success



Incident response, Investigation and ediscovery processes, methodologies and best practices

Over 60,000 seats to date

Industry recognized certifications

Consulting, implementations, integrations and staff augmentation

Investigations, implementations, customization and staff augmentation

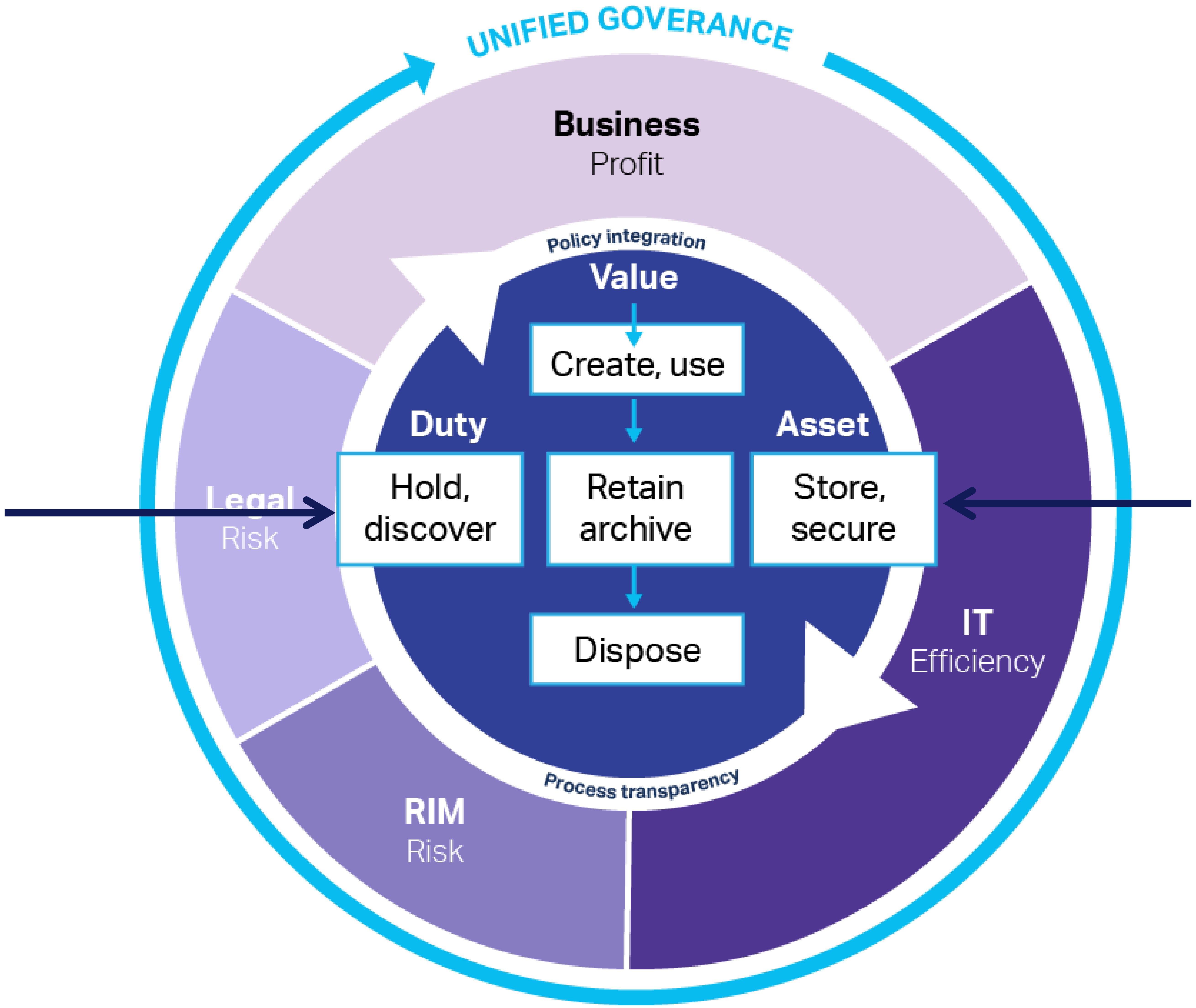
Open platform, supporting open standards

Integrate with industry-leading security technologies

opentext™

Best-of-breed Enterprise Information Management

EnCase eDiscovery and **EnCase Risk Manager** fill key in-house data discovery requirements



EnCase Endpoint Investigator and **EnCase Endpoint Security** enable investigative requirements and data-centric security for the needs of the EIM customer base

opentext™

OpenText is Enterprise Information Management

Guidance Software Joins a Strategic and Innovative Business Unit

Address Business Risk Converging Forces

opentext™ | Security

Provides a comprehensive digital forensic security solution to proactively audit your sensitive data, mitigate threats, and conduct digital investigations of security incidents

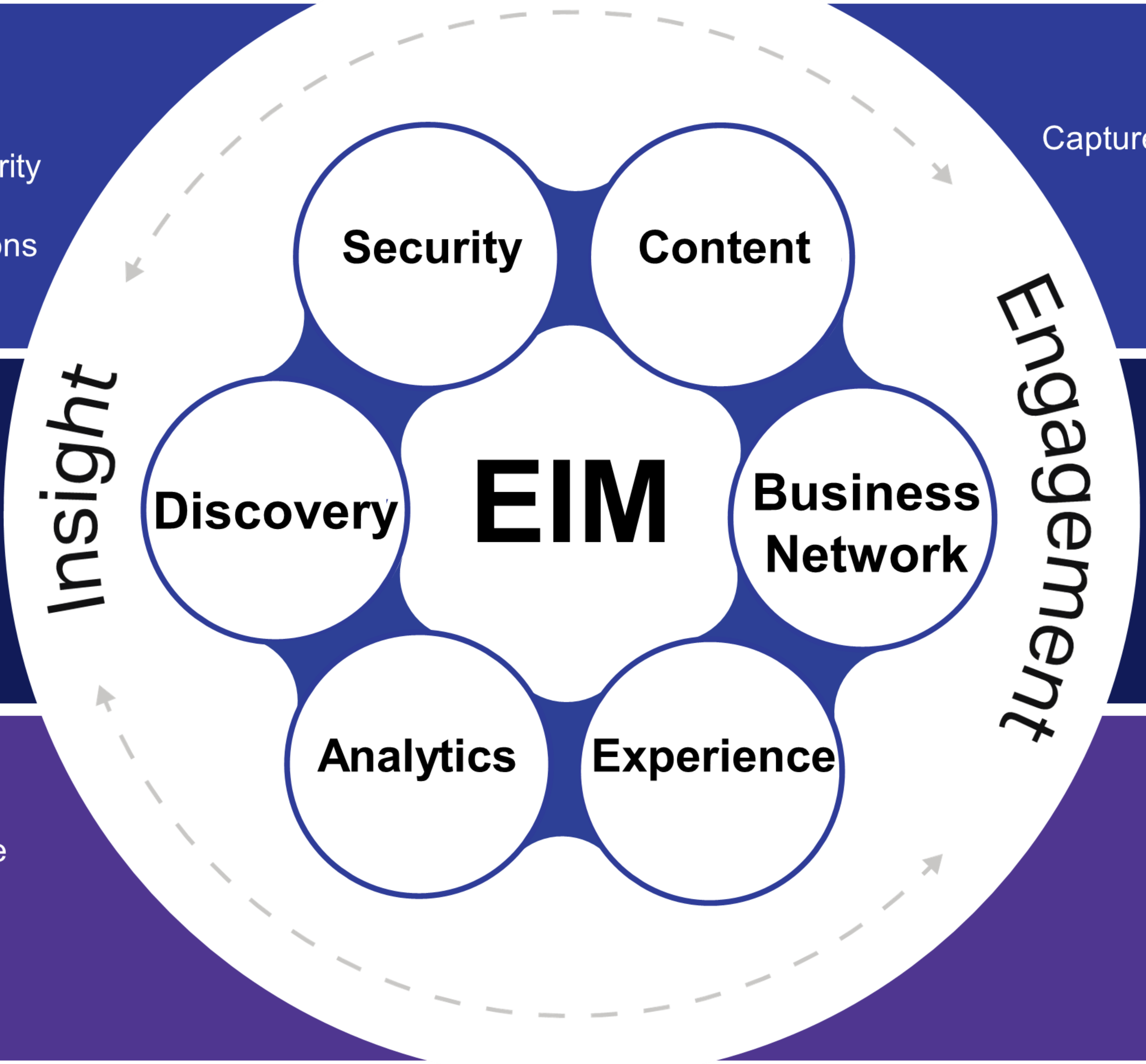
Acquisition closed in September 2017

opentext™ | Discovery

Enables discreet, forensically-sound access to key documents, contract terms, and critical early insights to manage risk and efficiently meet legal obligations

opentext™ | Analytics

Provides enterprise-grade Business Intelligence to improve decision-making and operational efficiency; OpenText Magellan adds AI, machine learning, text analytics, and big data ingestion and processing capabilities



opentext™ | Content

Capture and manage information from different sources in an integrated, enterprise-wide information grid to transform personal productivity, process productivity, and control

opentext™ | Business Network

Enables the seamless, secure flow of information across an extended business ecosystem of partners, systems, and devices; simplify inherent complexities and gain insights to drive efficiencies and speed time to revenue

opentext™ | Experience

Delivers exceptional continuous, connected customer experiences to increase engagement, drive revenue and promote customer lifetime value

GUIDANCE SOFTWARE is now

opentext™

Security & Privacy Challenges

Digital risk is a global problem

90% Attacks
on organizations
use unique malware
(signatures/hashes)

30 Billion
devices by 2020

$.5 Trillion
cyber crime related
expenses

$3 Trillion
lost revenue opportunity

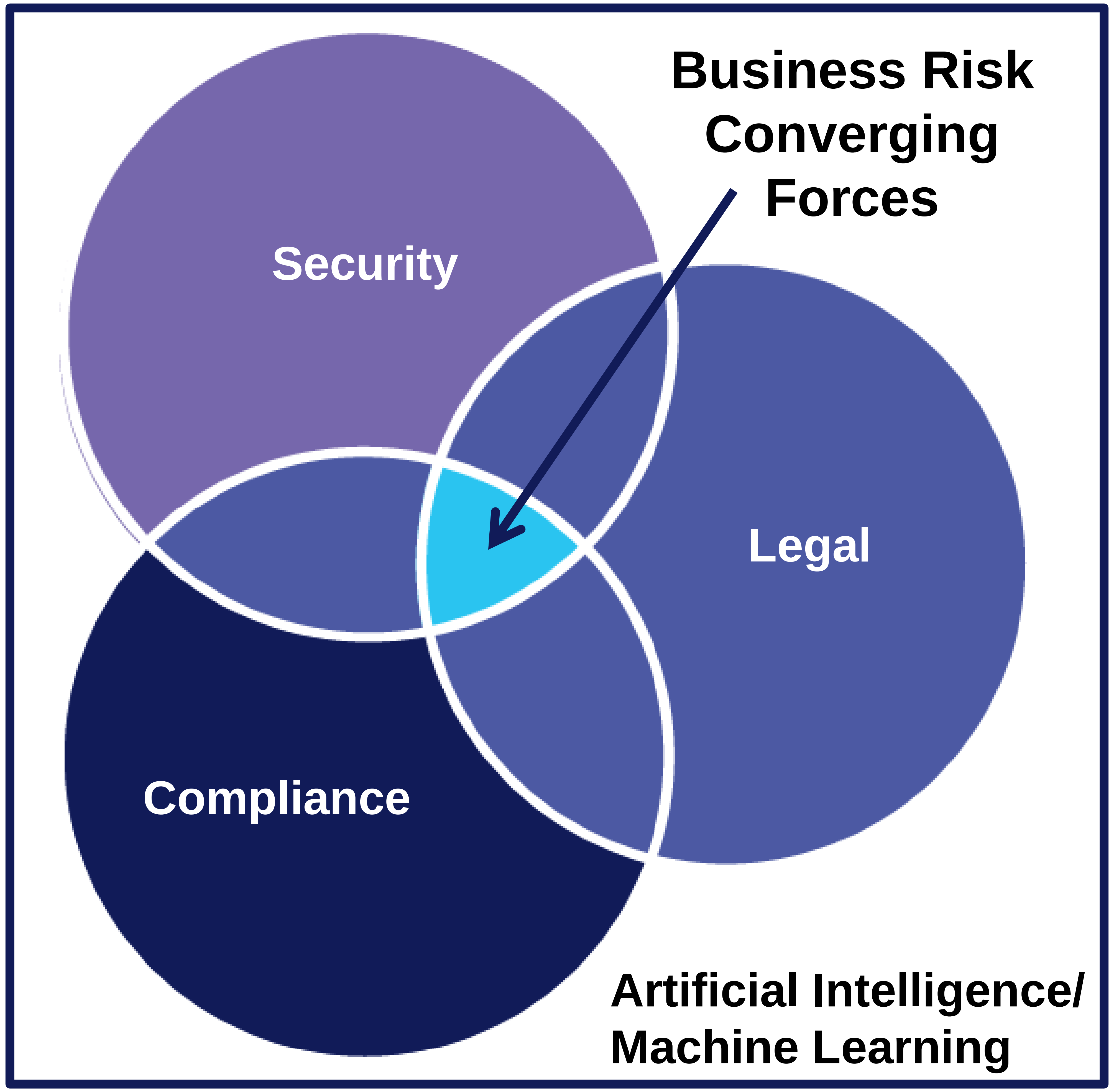
>90 Million
breaches and attacks
every year

opentext™

Converging Market Forces Drive OpenText Strategy

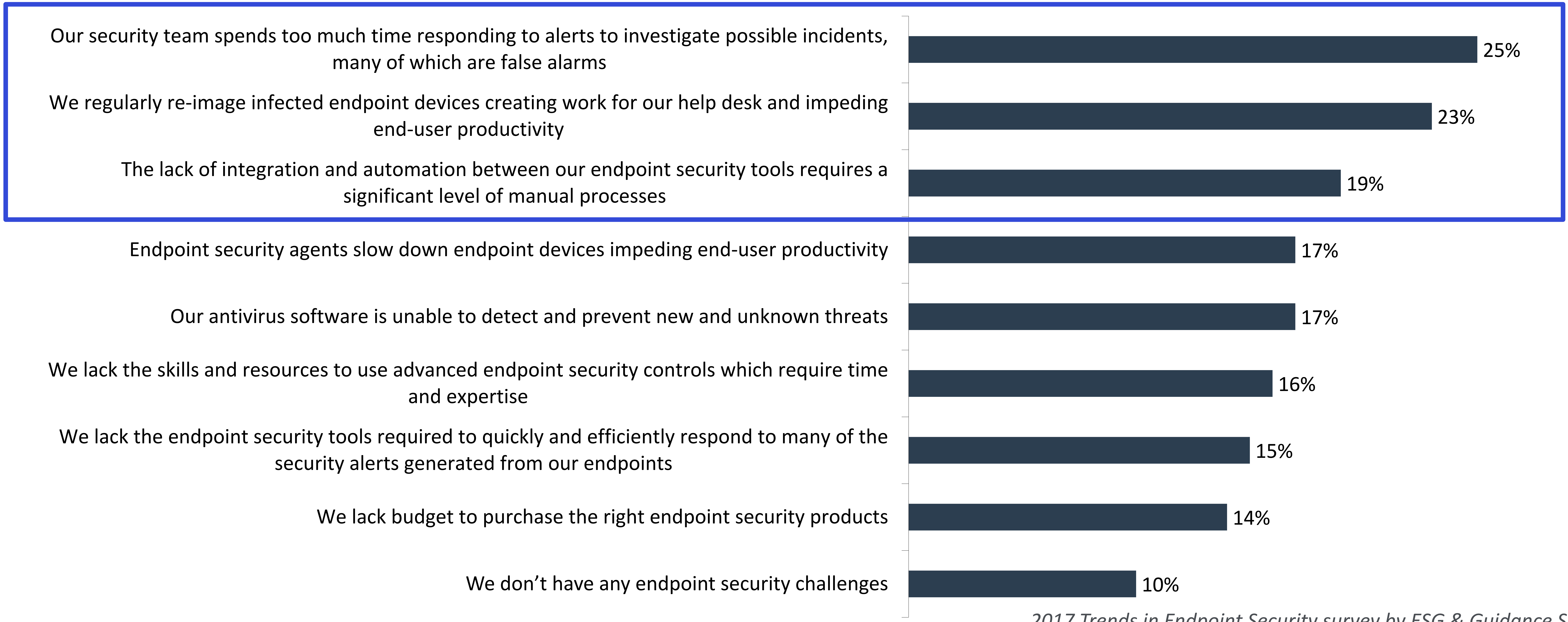
Organizations Facing A Perfect Storm

- Security Breaches and Data Protection
  - Prevent threats and minimize breach impact
  - Manage security risks in business terms
- Data Privacy, Regulations, and Policies
  - Growing industry regulations (GDPR, PCI DSS, HIPAA)
  - Internal policies (records retention, computer use, etc.)
- Investigations and eDiscovery
  - Internal HR, IP, and policy investigations
  - Case collection, assessment and litigation
- Artificial Intelligence/Machine Learning
  - Organizations seek solution for better insights and greater automation to efficiently manage business risks


Business Risk Converging Forces
Security
Legal
Compliance
Artificial Intelligence/ Machine Learning

Guidance Research Highlights Security Gaps

In your opinion, which of the following presents the most significant endpoint security challenges to your organization? (Percent of respondents, N=385, two responses accepted)



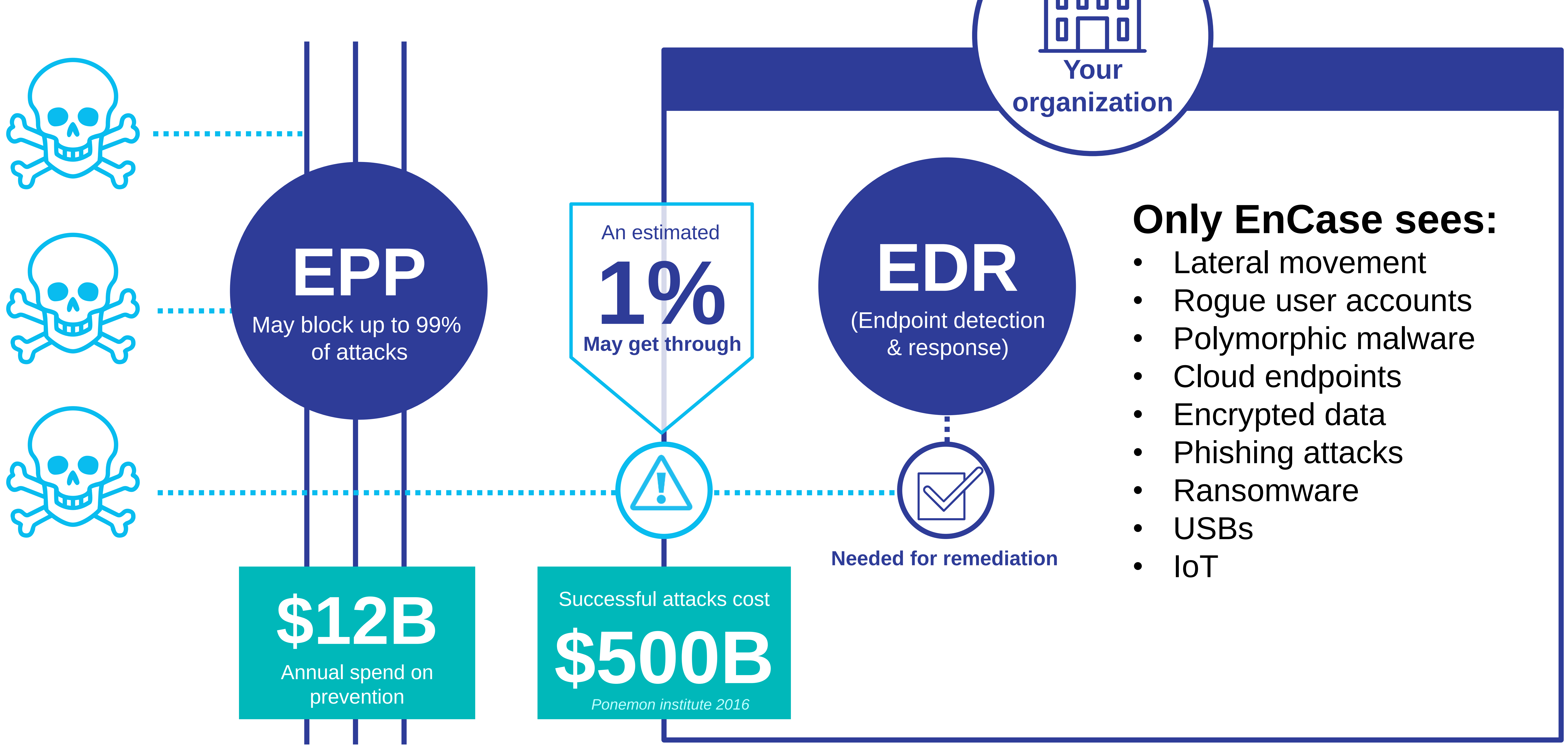
2017 Trends in Endpoint Security survey by ESG & Guidance Software

Prevention is important, but not sufficient

EDR is essential for complete cybersecurity

Attacks on your organization

Tens of thousands daily



$12B
Annual spend on prevention

Successful attacks cost
$500B
Ponemon institute 2016

Only EnCase sees:

- Lateral movement
- Rogue user accounts
- Polymorphic malware
- Cloud endpoints
- Encrypted data
- Phishing attacks
- Ransomware
- USBs
- IoT

Visibility is a critical gap

Organizations report little to no visibility in:

87%	Kernel level visibility
86%	Cloud repositories
81%	Anomalous behavior
78%	IOCs

Sans Survey, 2016

GDPR Incident Response Requirements

Article 33

- In the case of a personal data breach, the controller shall without undue delay and, where feasible, **not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority** competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
- The notification referred to in paragraph 1 shall at least:
  - describe the nature of the personal data breach including where possible, the **categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;**
  - **describe the likely consequences of the personal data breach;**

GUIDANCE SOFTWARE is now

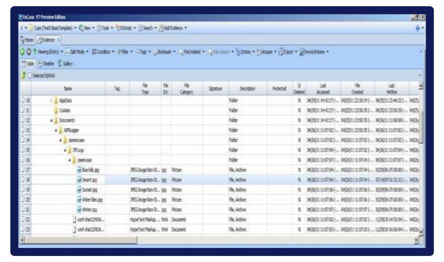
opentext™

EnCase Endpoint Security

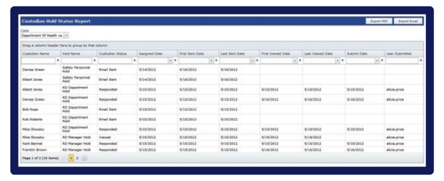
EnCase Forensic Security

Endpoint Agent is the Platform for an Expanding Suite of Applications

opentext™ | EnCase®

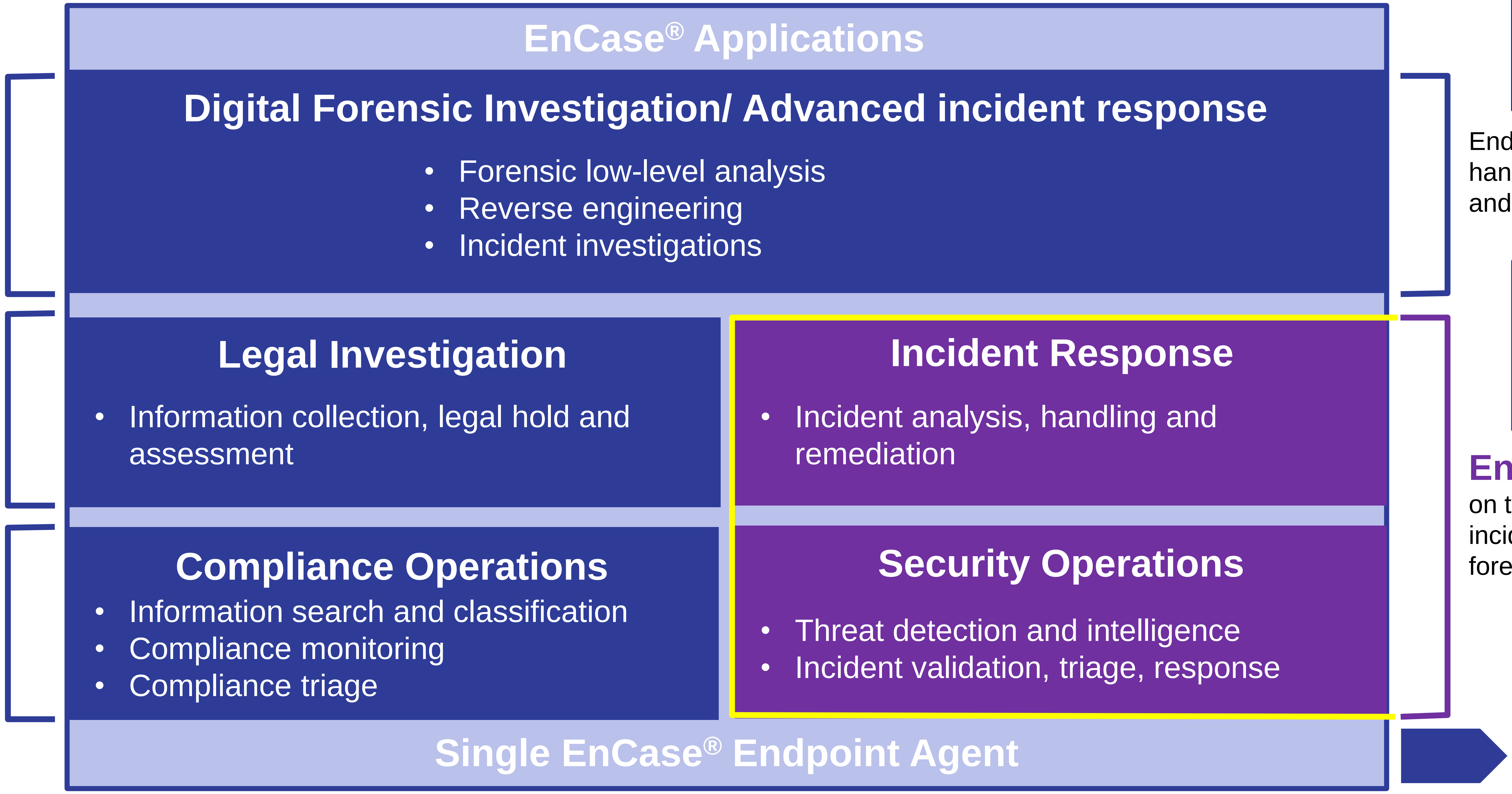


Endpoint Investigator is designed to handle HR, fraud and policy violation investigations and forensic analysis



eDiscovery supports legal hold through load-file generation in support of in-house corporate legal matters

Endpoint Risk Manager is focused on identification of proprietary and sensitive information to support compliance needs



EnCase® Applications

Digital Forensic Investigation/ Advanced incident response

- Forensic low-level analysis
- Reverse engineering
- Incident investigations

Legal Investigation

- Information collection, legal hold and assessment

Incident Response

- Incident analysis, handling and remediation

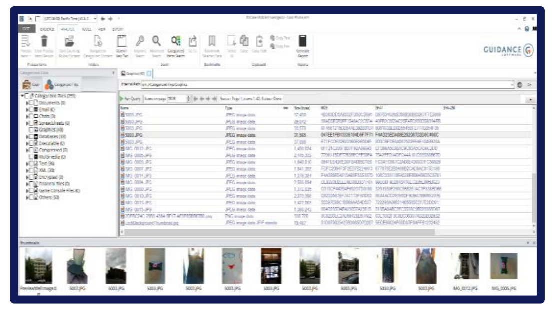
Compliance Operations

- Information search and classification
- Compliance monitoring
- Compliance triage

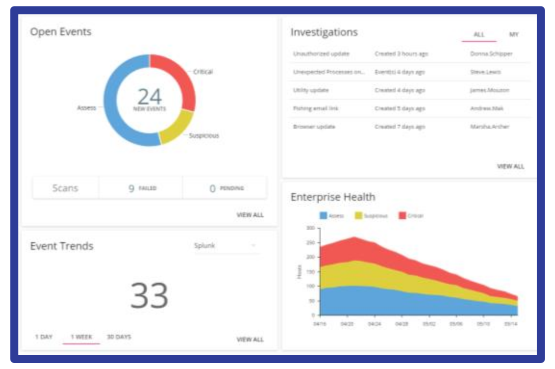
Security Operations

- Threat detection and intelligence
- Incident validation, triage, response

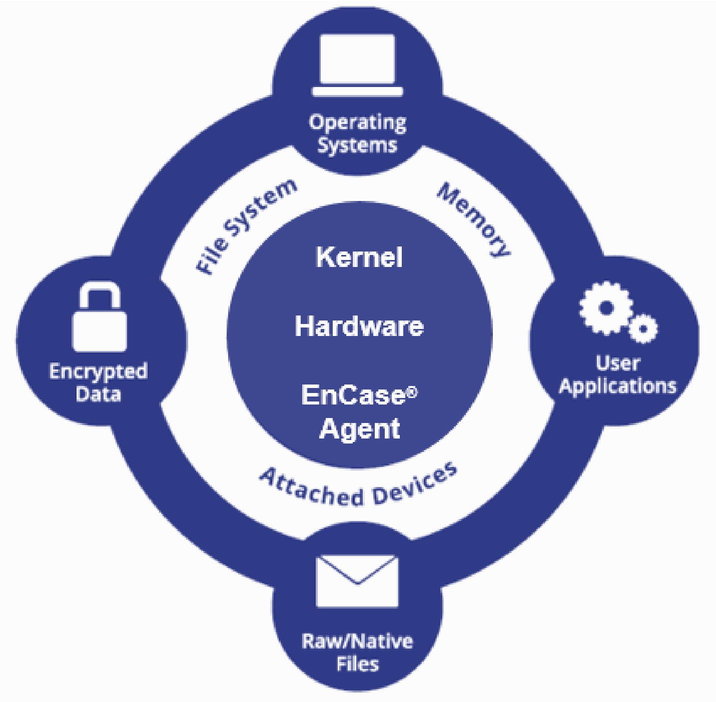
Single EnCase® Endpoint Agent



Endpoint Investigator is designed to handle advanced incident response and forensic analysis



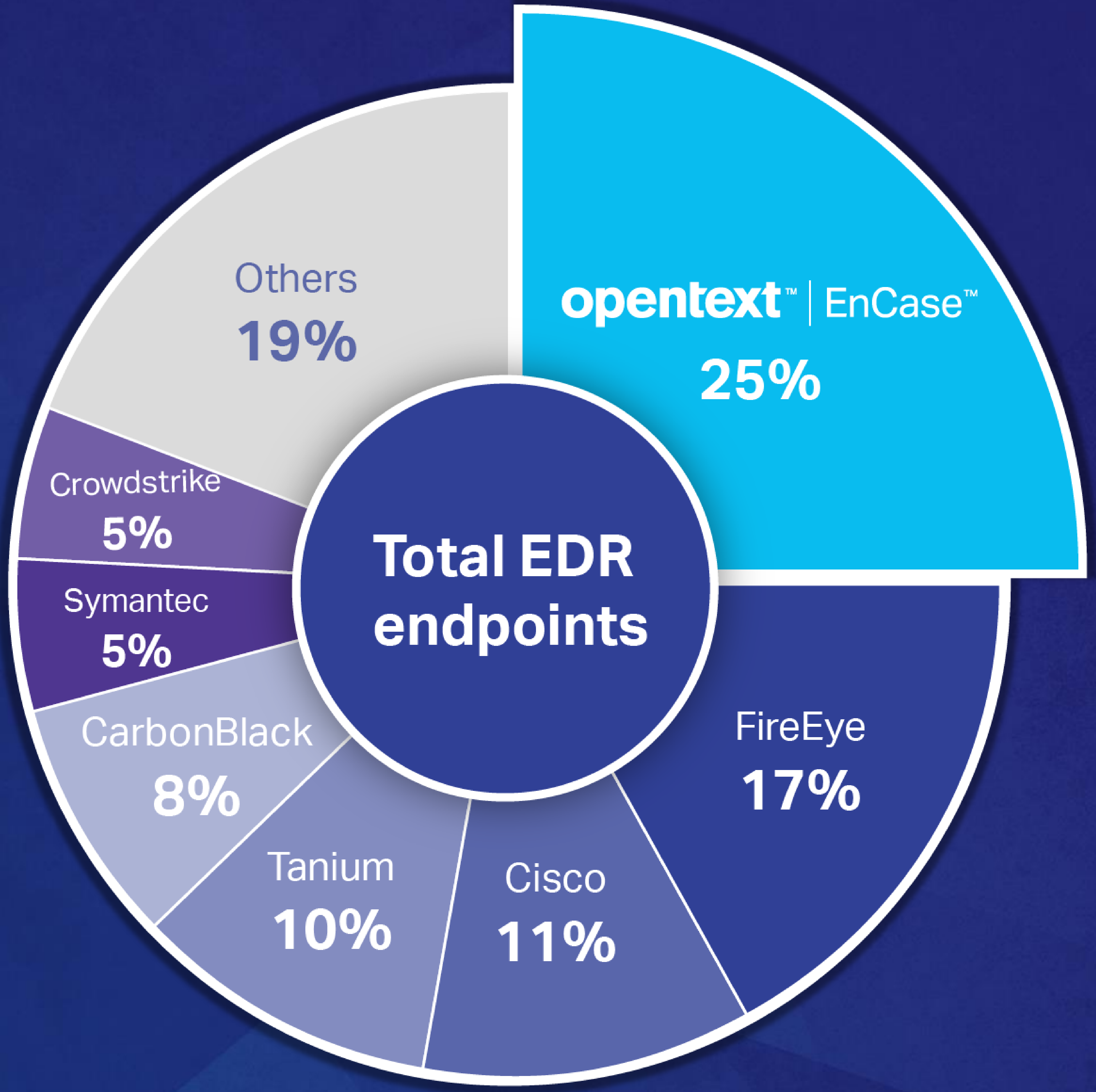
Endpoint Security is focused on threat detection, alert triage and incident handling and NOT deep forensic analysis



Note: **Forensic and Tableau** innovation will be a continuing priority that will benefit from the EnCase Endpoint Investigator roadmap

#1 in endpoints deployed

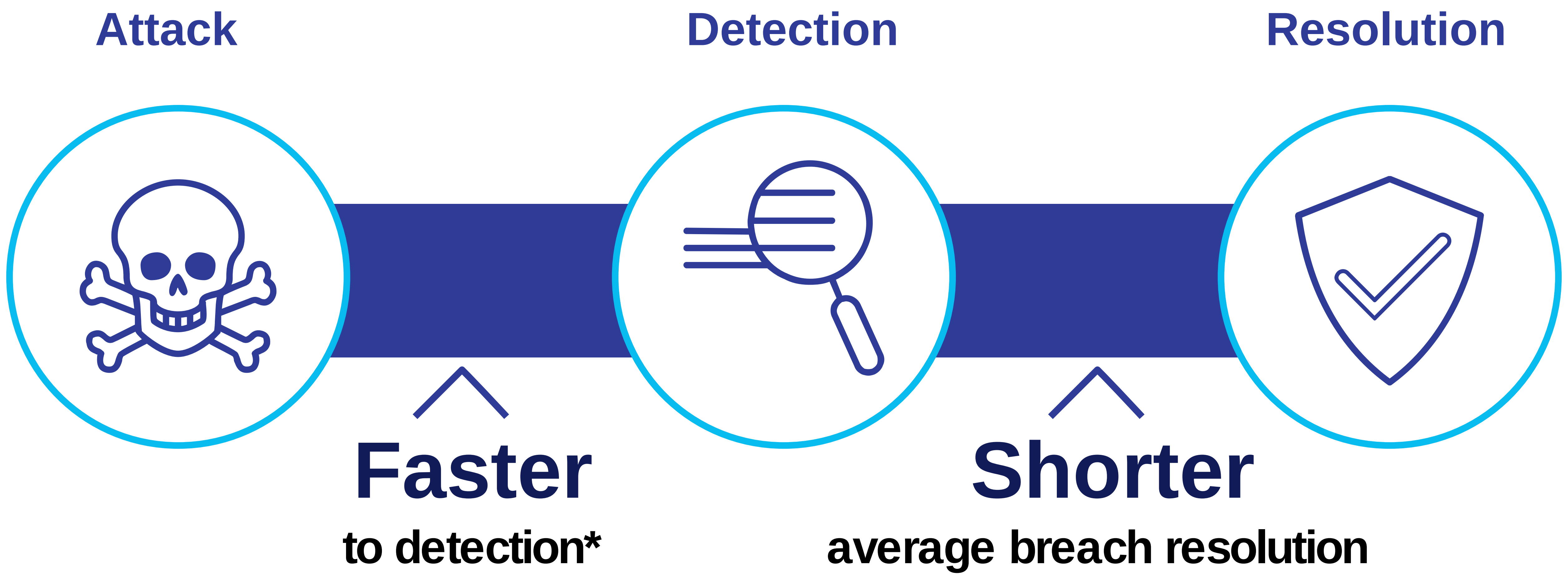
Gartner EDR Competitive Landscape Report



Accelerate Time to Detect and Response to Threats

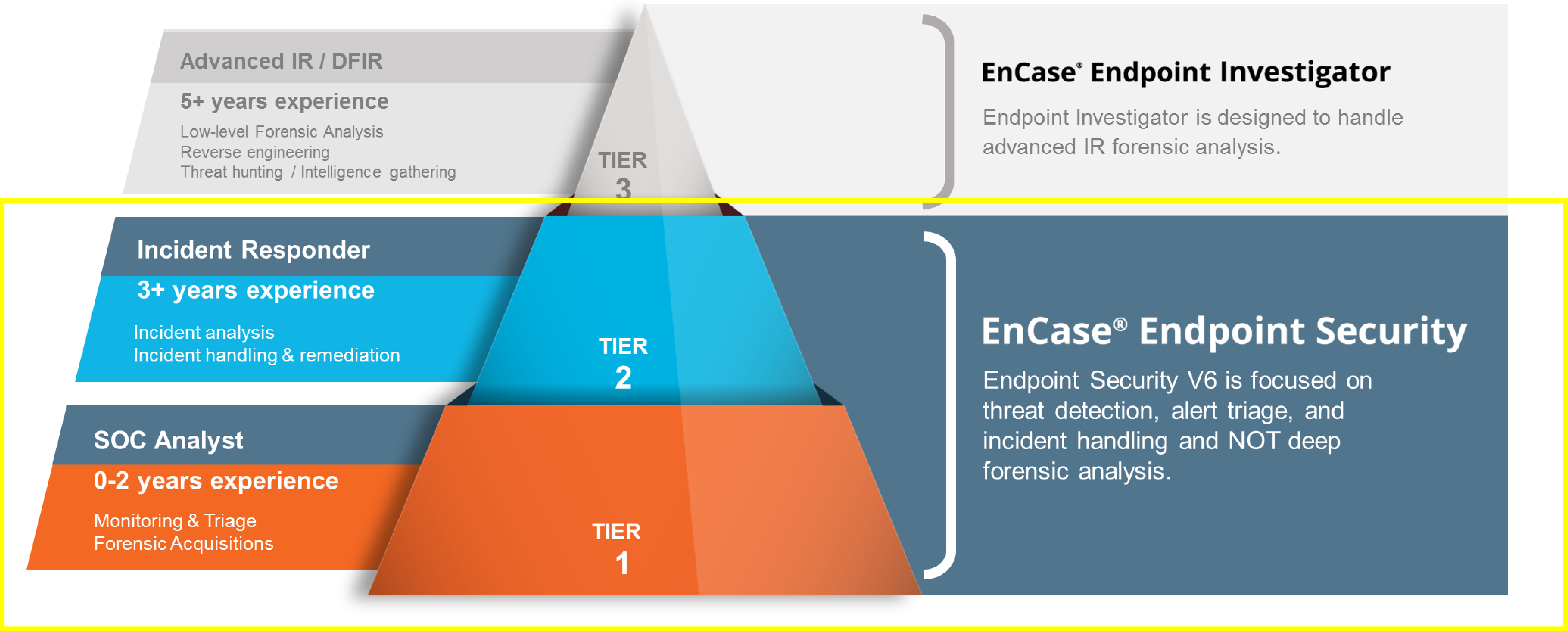
EnCase Endpoint Security aligns with the threat detection and response requirements of numerous regulations and mandates such as:

- PCI-DSS
- HIPAA-HITECH
- GDPR



Fewer resources, less exposure and reduced level of risk at a lower cost

Who Uses EnCase Endpoint Security?



Advanced IR / DFIR

5+ years experience

Low-level Forensic Analysis
Reverse engineering
Threat hunting / Intelligence gathering

Incident Responder

3+ years experience

Incident analysis
Incident handling & remediation

SOC Analyst

0-2 years experience

Monitoring & Triage
Forensic Acquisitions

EnCase® Endpoint Investigator

Endpoint Investigator is designed to handle advanced IR forensic analysis.

EnCase® Endpoint Security

Endpoint Security V6 is focused on threat detection, alert triage, and incident handling and NOT deep forensic analysis.

EnCase Endpoint Security…

Proactive threat detection, alert triage, and incident response

Detect sooner

- Expose internal or external risks or threats with anomaly-based detection
- Reduce the time to discover a compromise

Respond faster

- Increase efficiency and ROI with on-demand and automated response
- Reduce the total time and costs of response

Recover effectively

- Remediate a threat completely; eliminate wipe and reimage process
- Accurately asses impact to sensitive data and clean up data spillage

Differentiated Features

- **Scan for Indicators of Compromise (IoCs), and detect bad actors**
- **Validate the presence of any threat**
- **Deliver automated response via integration with alerting tools**
- **Forensic-grade targeted remediation – remotely delete files, kill processes, and reset registry keys**

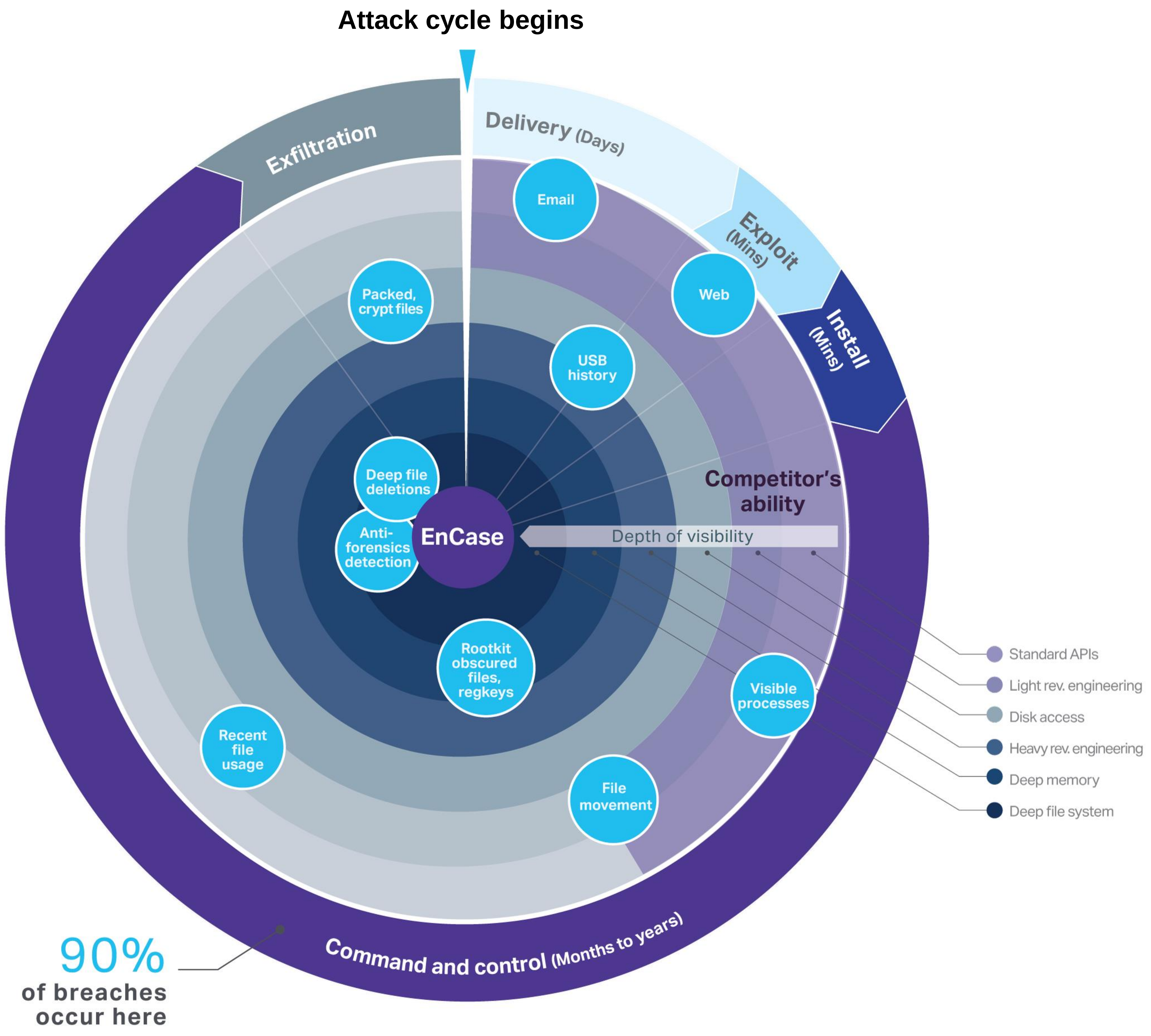
…with 360-degree visibility

- **Uncover forensic residue across every stage of the attack cycle**

- **Reveal data security risk, no matter how well hidden**

- **Approach addresses both external and insider threats**

- **Visibility unmatched by surface level competitors**



opentext™

EnCase® Endpoint Security

GUIDANCE SOFTWARE

DASHBOARD

Open Events

17 NEW EVENTS

Critical
Suspicious
Assess

Scans | 7 FAILED | 0 PENDING

VIEW ALL

Investigations

ALL MY

Investigation 99	Created 5 hours ago	James.Jameson
Inv-01 with 1 snapshot	Remediate 5 hours ago	John.Doe
Critical Inv. 2	Event(s) a day ago	Peter.peterson
Critical Inv. 3	Created 5 days ago	John.Doe
Inv-02	Assigned to user 5 days ago	James.Jameson
Inv-05	Assigned to user 5 days ago	Peter.peterson

VIEW ALL

Event Trends

API

24

1 DAY 1 WEEK 30 DAYS

VIEW ALL

Enterprise Health

EnCase® Endpoint Security
GUIDANCE SOFTWARE

EVENTS

□	Event ID	⚠	Date	Time	Target	State	Alert Score
□	SPLUNK-2-10	⚠	2017/05/05	0956	RD-1234567.rd.iridium	Critical	20
□	SPLUNK-2-26	⚠	2017/05/05	0956	DEV-1234567.rd.iridium	Critical	20
☑	SPLUNK-2-32		2017/05/05	0956	QA--1234567.rd.iridium	Suspicious	20
□	ARCSIGHT-2-13		2017/05/05	0956	DEV-1234567.rd.iridium	Suspicious	20
□	FIREEYE-2-18		2017/05/05	0956	RD-1234567.rd.iridium	Suspicious	20
□	FIREEYE-2-21		2017/05/05	0956	DEV-1234567.rd.iridium	Assess	20
□	ARCSIGHT-2-3		2017/05/05	0956	RD-1234567.rd.iridium	Assess	20
□	SPLUNK-2-7		2017/05/05	0956	SA-1234567.rd.iridium	Assess	20
□	SPLUNK-2-6		2017/05/05	0956	QA-1234567.rd.iridium	Assess	20
□	ARCSIGHT-2-4		2017/05/05	0956	QA-1234567.rd.iridium	Assess	20
□	FIREEYE-2-11		2017/05/05	0956	SC-1234567.rd.iridium	Assess	20
□	ARCSIGHT-2-5		2017/05/05	0956	DEV -1234567.rd.iridium	Assess	20
□	ARCSIGHT-2-36		2017/05/05	0956	SA-1234567.rd.iridium	Assess	20
□	SPLUNK-2-12		2017/05/05	0956	RD-1234567.rd.iridium	Assess	20

1 selected

24 of 24 events

EVENT ID	SPLUNK-2-32
BROWSER TIME	2017/05/05, 0956:07 (UTC-07:00)
IP/HOST	QA-TG1.rd.gsi
SOURCE	API
THREAT SCORE	45
ALERT SCORE	20
SPLUNK ID	SPLUNK-001
COMMENT	Policy violations detected

Malicious Hashes	Malicious Connections	Malicious DNS
49	-	-
Suspicious Hashes	*Suspicious Connections*	*Suspicious DNS*
13.6k	116	86

Top Malicious

Malicious Hashes

CompositeBus.sys
drmkaud.sys
srvcli.dll
tsusbhub.sys

Malicious Connections

none

Malicious DNS

none

EnCase® Endpoint Security
GUIDANCE SOFTWARE
INVESTIGATION
PROCESSES (554)
File Name
Inst
chrome
Suspicious
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
explorer.exe
CodeMeterCC.exe
TSVNCache.exe
tabsystray.exe
cmd.exe
notepad.exe
Q-Dir.exe
B.exe
devenv.exe
Tree.exe
chrome.exe
firefox.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
SUMMARY
DLLs
CONNECTIONS
CLOSE

Process 'chrome.exe'

NAME	chrome.exe
PID	9432
PATH	C:\Program Files (x86)\Google\...
HASH	EC820250BBF2AC99B27DD3A...
THREAT SCORE	-3
PARAMETERS	"C:\Program Files (x86)\Googl...
HIDDEN	No
CHILD PROCESSES	0
DLLS	48
CONNECTIONS	0

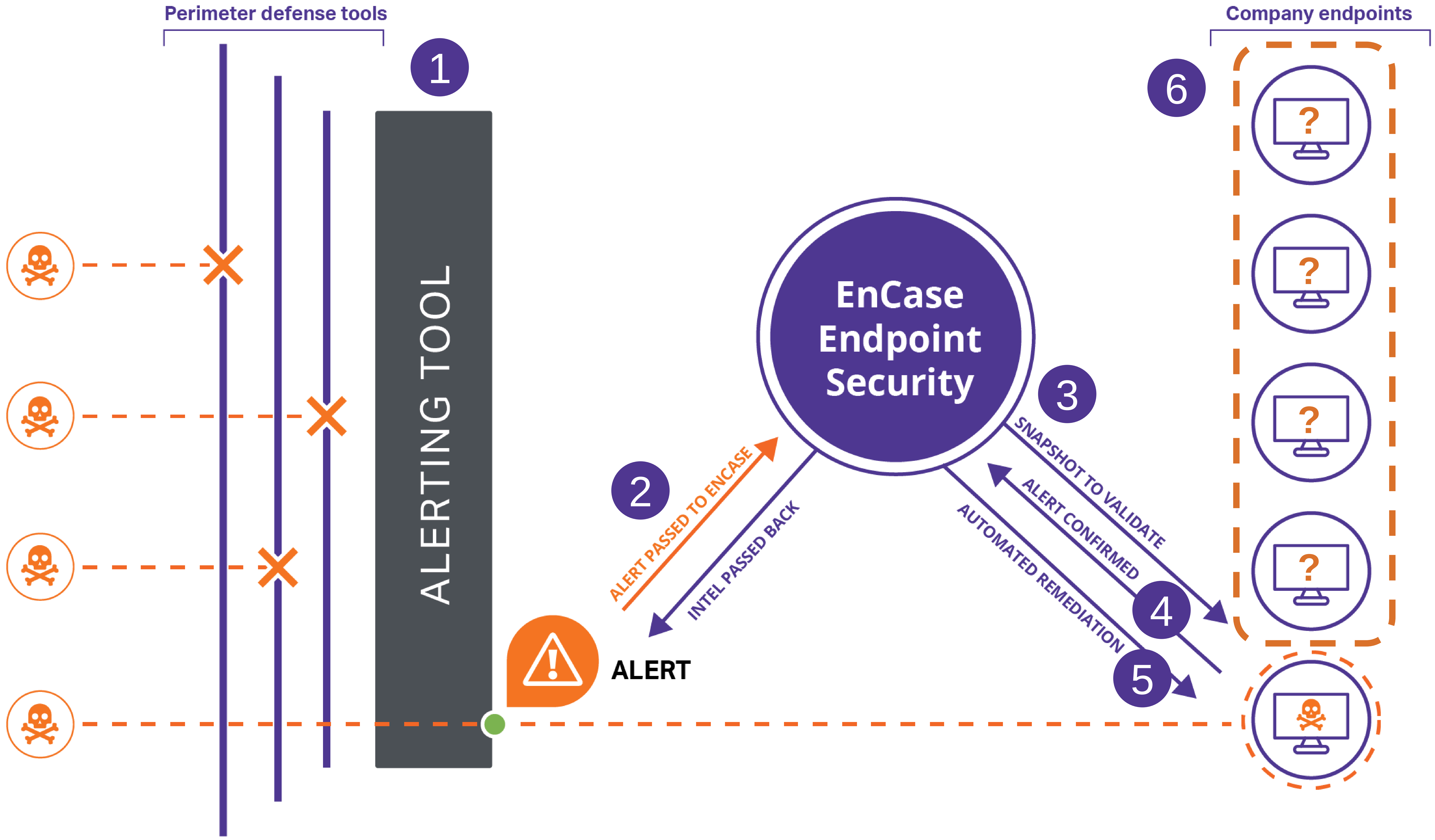
Inv-01 with 1 snapshot

STATE	Opened 5 days ago
ASSIGNED TO	RD\john.doe
HASH DETECTIONS	6
IP DETECTIONS	3
DOMAIN NAME DETECTIONS	1

History

Remediate RD\james.jameson	5 hours ago
Event(s) RD\john.doe	2 days ago
Event(s) RD\john.doe	2 days ago
Snapshot RD\john.doe	2 days ago
Remediate RD\james.jameson	2 days ago
Remediate RD\james.jameson	2 days ago
Event(s) RD\john.doe	5 days ago
Event(s) RD\john.doe	5 days ago
Snapshot RD\john.doe	5 days ago
Created RD\john.doe	5 days ago

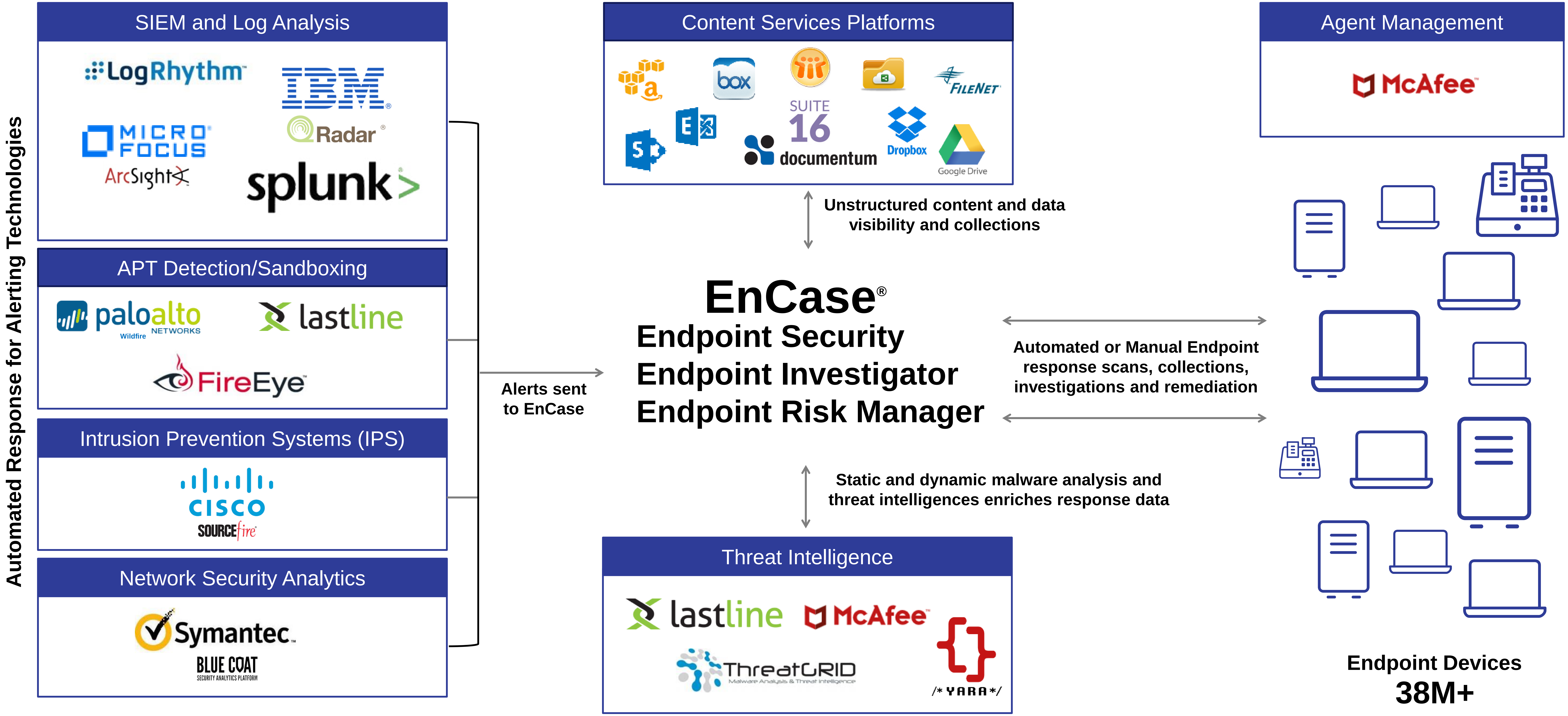
EnCase Endpoint Security



1. Alerts generated indicating a potential threat got through defenses.
2. 3rd Party tool configured to send EnCase Endpoint Security (ES) relevant data to query endpoints.
3. ES takes alert data, and queries endpoints for evidence of threats.
4. ES generates a critical event based on confirmation of threat.
5. Analyst confirms results and, using ES eliminates the threat from the device.
6. At this point, analyst queries enterprise against newly found threat intel, ensuring the threat did not spread.

EnCase Ecosystem

Delivers Intelligence, Automation and Reach to Defend Against Threats



Automated Response for Alerting Technologies

SIEM and Log Analysis

LogRhythm
IBM Qradar
MICRO FOCUS ArcSight
splunk>

APT Detection/Sandboxing

paloalto NETWORKS Wildfire
lastline
FireEye

Intrusion Prevention Systems (IPS)

CISCO SOURCEfire

Network Security Analytics

Symantec. BLUE COAT SECURITY ANALYTICS PLATFORM

Alerts sent to EnCase

Content Services Platforms

box
SUITE 16
documentum
Dropbox
FileNet
Google Drive

Unstructured content and data visibility and collections

EnCase®
Endpoint Security
Endpoint Investigator
Endpoint Risk Manager

Automated or Manual Endpoint response scans, collections, investigations and remediation

Static and dynamic malware analysis and threat intelligences enriches response data

Threat Intelligence

lastline
McAfee
ThreatGRID Malware Analysis & Threat Intelligence
/*YARA*/

Agent Management

McAfee

Endpoint Devices
38M+

Roadmap key themes and examples

Expand interoperability

- RESTful API development
- Collection manager
- Repository connectors
- Response automation

Workflow automation

- Detection and response
- Role-based access controls
- Seamless eDiscovery
- Orchestration

Customer-driven features

- Timeline analysis
- Enhanced agent
- Collaboration features

Innovation

- Continuous monitoring
- Enhanced threat intelligence
- IoT agents (Raspian, Windows IoT)

RoI Analysis:

Global Automobile Manufacturer

Situation: Prior to deployment, customer suffered lengthy server downtime, alert fatigue and lengthy response times.

Solution: With EnCase Endpoint Security customer dramatically reduced response time, and experienced a rapid ROI by increasing the update of loan processing servers in particular.

388% ROI >

- Savings of over **$2.4 millions** in incident-related costs
- Reduced time to validate and triage threats by **89%**
- Reduced time to remediate breaches by **90%**
- Reduced impact on server downtime by **98%**

Key Benefits

Business Stakeholders

- Add immediate value to existing operational teams
- Reduce costs related to training and remediation
- Mitigate business risks and ensure compliance

Operational Users

- Quickly validate security incidents
- Less user frustration and human error
- Open RESTful APIs for an integrated best-of-breed solution
- Installs and up and running in hours

GUIDANCE SOFTWARE is now

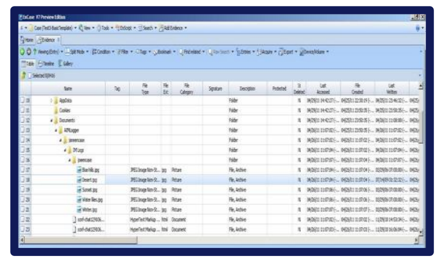
opentext™

EnCase Endpoint Investigator

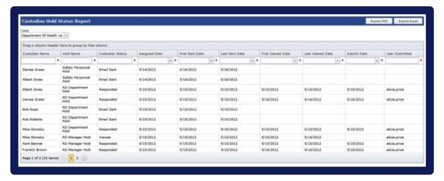
EnCase Forensic Security

Endpoint Agent is the Platform for an Expanding Suite of Applications

opentext™ | EnCase®



Endpoint Investigator is designed to handle HR, fraud and policy violation investigations and forensic analysis



eDiscovery supports legal hold through load-file generation in support of in-house corporate legal matters

Endpoint Risk Manager is focused on identification of proprietary and sensitive information to support compliance needs

EnCase® Applications

Digital Forensic Investigation/ Advanced incident response

- Forensic low-level analysis
- OS Reverse engineering
- Incident investigations (post-mortem)

Legal Investigation

- Information collection, legal hold and assessment

Incident Response

- Incident analysis, handling and remediation

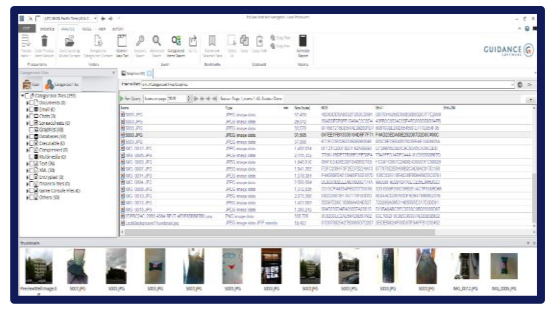
Compliance Operations

- Information search and classification
- Compliance monitoring
- Compliance triage

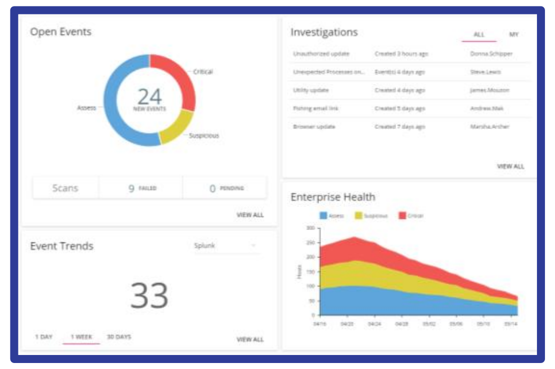
Security Operations

- Threat detection and intelligence
- Incident validation, triage, response

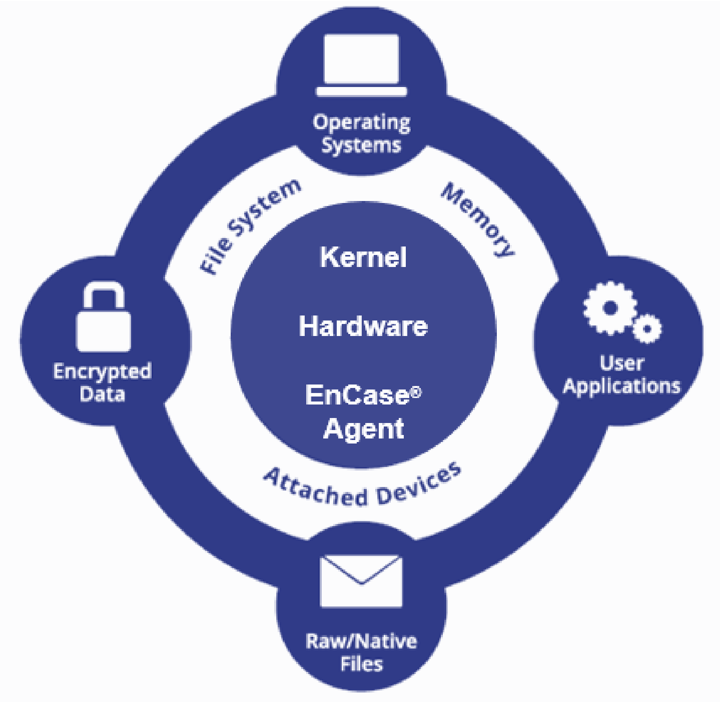
Single EnCase® Endpoint Agent



Endpoint Investigator is designed to handle advanced incident response and forensic analysis

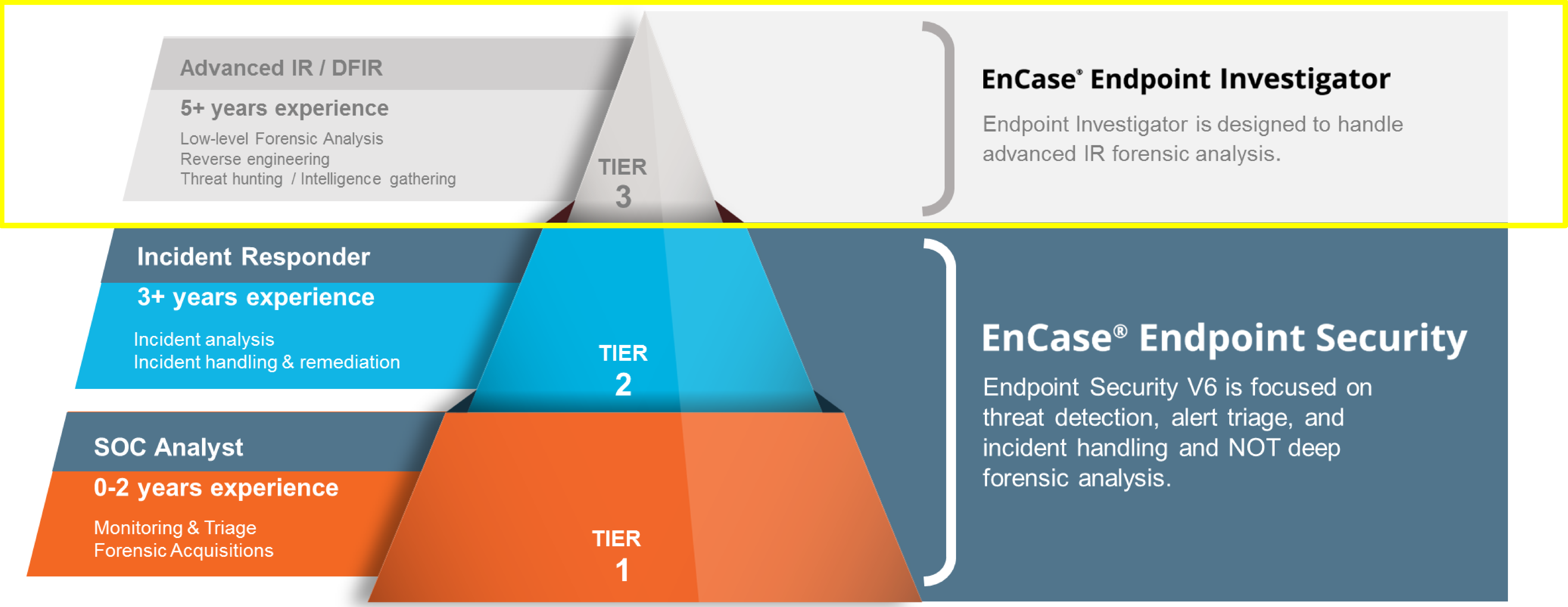


Endpoint Security is focused on threat detection, alert triage and incident handling and NOT deep forensic analysis



Note: **Forensic and Tableau** innovation will be a continuing priority that will benefit from the EnCase Endpoint Investigator roadmap

Who Uses EnCase Endpoint Investigator?



Advanced IR / DFIR

5+ years experience

Low-level Forensic Analysis
Reverse engineering
Threat hunting / Intelligence gathering

TIER 3

EnCase® Endpoint Investigator

Endpoint Investigator is designed to handle advanced IR forensic analysis.

Incident Responder

3+ years experience

Incident analysis
Incident handling & remediation

TIER 2

SOC Analyst

0-2 years experience

Monitoring & Triage
Forensic Acquisitions

TIER 1

EnCase® Endpoint Security

Endpoint Security V6 is focused on threat detection, alert triage, and incident handling and NOT deep forensic analysis.

EnCase Endpoint Investigator

Industry-standard digital investigations solution

Reduce cost and complexity
Remote investigations are more effective than alternative processes

Ensure confidence in findings
Disk-level visibility enables complete search and collection of relevant data

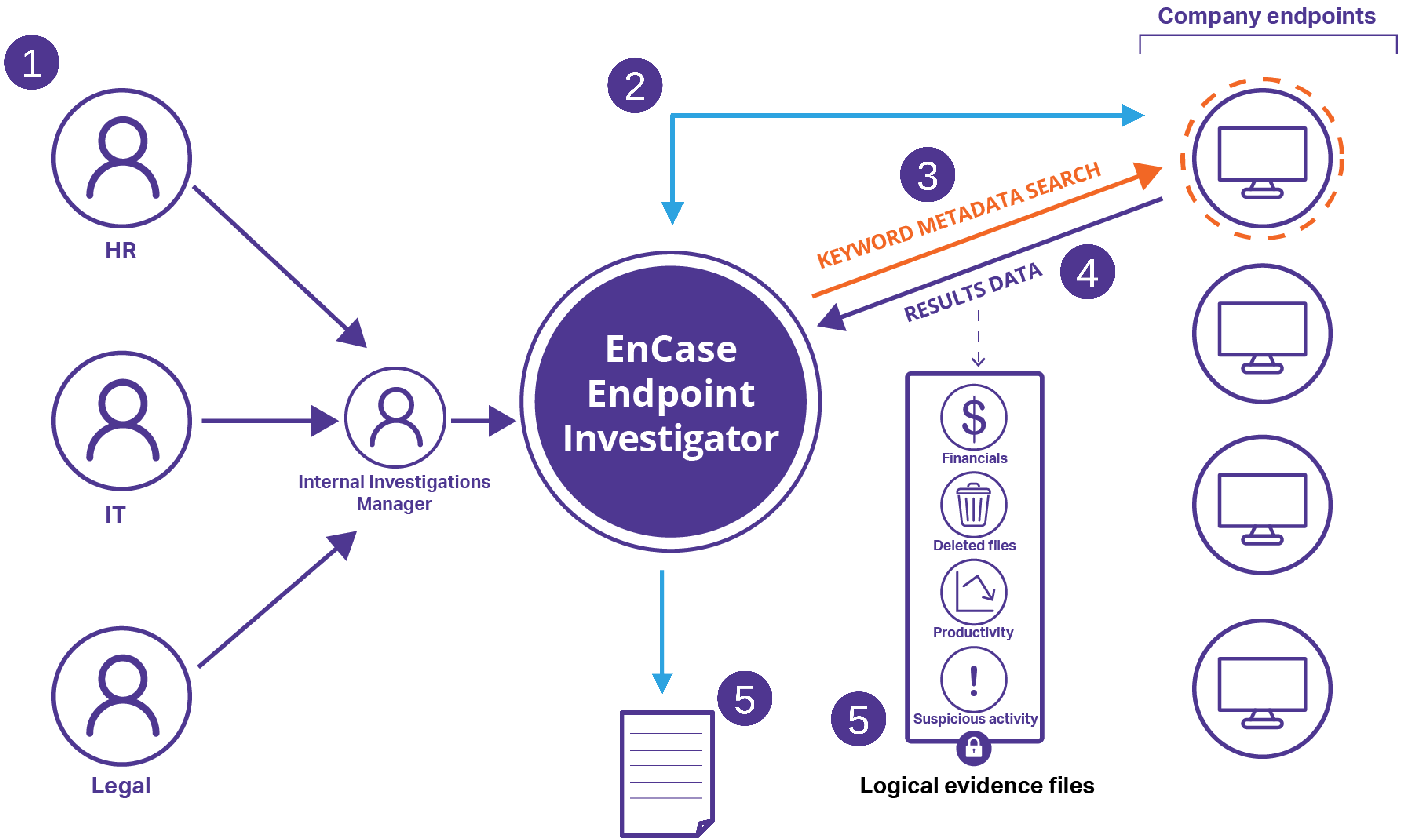
Investigate discreetly
Discreet investigations across the network without business disruption

Manage from a central location
Eliminate travel, employee downtime, and case duration with centrally managed investigations

Differentiated Features

- **Kernel-level agent-based access across the widest range of files and OS**
- **Templates and workflows for most common investigative tasks**
- **Roles and permissions to ensure authorized access to endpoints**
- **Complete access to disk, memory, and email**

EnCase Endpoint Investigator



1. Internal Investigation Team Receives Request
2. Examiner (person) connects to subjects device via installed agent.
3. Keyword and date range searches are performed.
4. Examiner reviews results and collects responsive data.
5. Examiner generates final report for requesting party, and preserves findings in a logical evidence file.

Case Study: Global Insurance Company

- **Decision Maker:** Global Head Cyber Response & Office of Digital Investigations
- Required a means to address company-owned device digital forensic cases
- Global deployment across 108,000 nodes
- **Why EnCase:** other products did not scale well, and took too long to collect data across the global WAN; intuitive UI. Influencer (Global Corporate Forensics Manager) used EnCase at another company, and during his time at a federal agency.

> “ *Endpoint Investigator is the gold standard in hard disk forensics. I appreciate the fact that EI could preview remote machines, have a tree-view of a machine, and conduct analysis from that preview without needing to conduct a complete acquisition.”*

GUIDANCE SOFTWARE is now

opentext™

EnCase Innovation

Strategy and Roadmap Briefing

Portfolio Powering a New Wave of Innovation and Automation

EnCase eDiscovery + Axcelerate = Seamless eDiscovery

EnCase Endpoint Security + Magellan = Machine learning-powered security

EnCase Endpoint Investigator + iHub = Big Data investigations

Magellan Advances OpenText Security Strategy

Provides AI/Machine Learning Driven Insights and Automation

opentext™ | Magellan

Content and Data

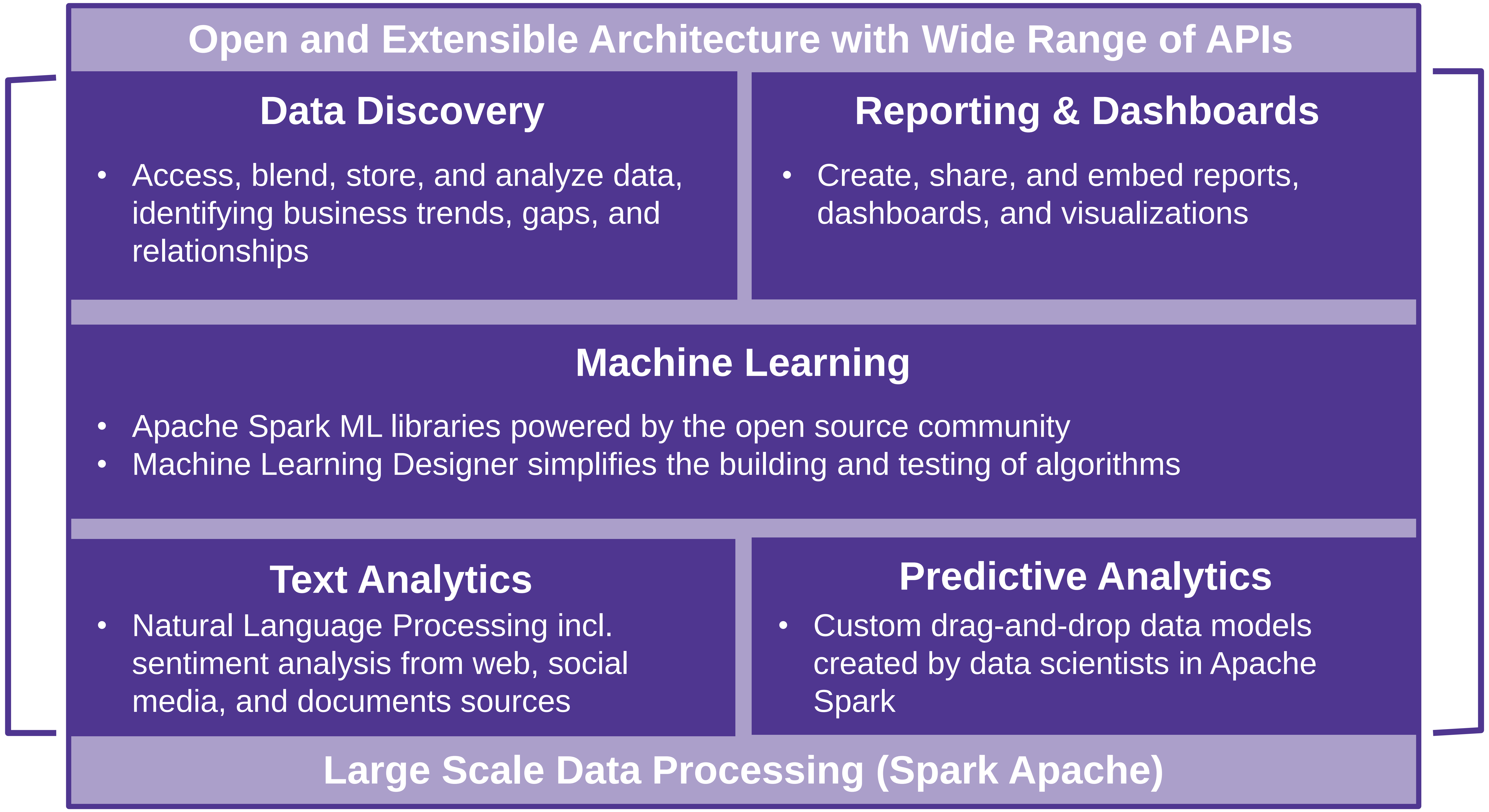
Enterprise Data

IoT Data

Enterprise Content

Social Content

Desktop Data



Open and Extensible Architecture with Wide Range of APIs

Data Discovery

- Access, blend, store, and analyze data, identifying business trends, gaps, and relationships

Reporting & Dashboards

- Create, share, and embed reports, dashboards, and visualizations

Machine Learning

- Apache Spark ML libraries powered by the open source community
- Machine Learning Designer simplifies the building and testing of algorithms

Text Analytics

- Natural Language Processing incl. sentiment analysis from web, social media, and documents sources

Predictive Analytics

- Custom drag-and-drop data models created by data scientists in Apache Spark

Large Scale Data Processing (Spark Apache)

AI Based Insights

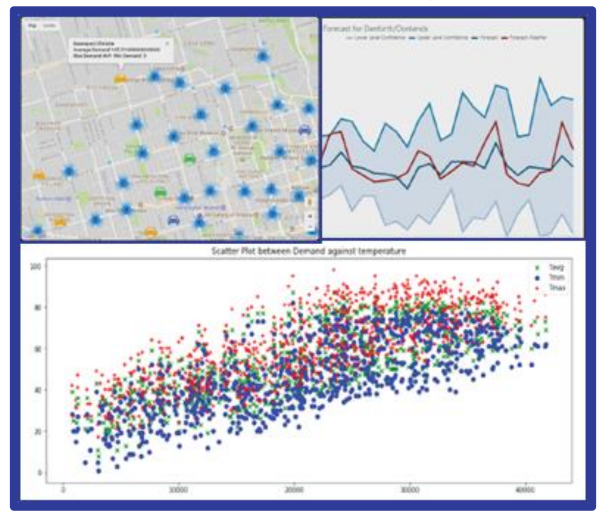
eDiscovery

Information Governance

Risk Management

Data Privacy

Information Security



EnCase Directions

Leverage OpenText Portfolio and Partnerships to Drive Innovation

- Embedded AI/Machine Learning
  - Endpoint Security integration with Magellan to hunt, detect, and remediate unknown threats
  - Discover sensitive data in context of compliance mandates and find new relationships for investigations
- Ubiquitous Connectivity to Endpoints
  - On and off network agent connectivity and access
  - Agentless connectivity for endpoint analysis and threat detection
- Deeper Investigation and Remediation of Threats including Insiders
  - EnCase, Discovery, and Analytics integration brings new investigation capabilities
  - Anonymization, pseudonymization, and encryption of sensitive data on endpoints
- EnCase Ecosystem Expansion
  - Security orchestration advances workflow automation to shorten the time to detect and remediate threats
  - Host intrusion prevention adds patient zero intelligence for threat hunting
  - Data centric security intelligence including file analytics, DLP, and DRM for advanced remediation actions
  - Full scanning and analytics for cloud repositories, mobile devices, and IoT devices

Key Takeaways

- Information security is a fundamental requirement for best-of-breed information management
- EnCase provides a foundation for data-centric security
- OpenText reach has extended to nearly 40 million installed endpoint agents around the globe
- Managed services expanded to include world-class threat hunting, incident response, and investigations
- OpenText will leverage EnCase to innovate across other technologies solving new problems for our customer base

opentext™

Thank you

twitter.com/opentext

facebook.com/opentext

linkedin.com/company/opentext

opentext.com