GUIDANCE SOFTWARE™

From beginning to endpoint.

ETAT DE L’ART SOC

FRANCIS IA-SOLUTION CONSULTANT
FORTUNATO GUARINO-SOLUTION CONSULTANT

GUIDANCE SOFTWARE™

From beginning to endpoint.

Proven in the courtroom and trusted in the boardroom, Guidance provides smart and dependable solutions to problems that often go **undetected or unsolved on the endpoint**.

We know how to get a business back on track fast so you can restore order and feel confident.

Founded in 1997
EnCase = Gold Standard Forensic investigation solutions

72 of the Fortune 100, 47% of the Fortune 500 - **25M** endpoints deployed

#1 software for the **incident response** service providers;
ATOS, Airbus Defense & Space, KPMG, PWC

Fortunato Guarino – Cyber Crime & Data Protection Advisor
Francis Ia – Endpoint Detection & Response, Forensic Security

TRUSTED BY THE LARGEST GLOBAL ENTERPRISES

eni BNP PARIBAS Caisse desDépôts NATIXIS

NOVARTIS ENGIE HSBC adidas

EXPANDING WINDOW OF EXPOSURE

TODAY’S REALITY

ATTACK

DETECTION

RESOLUTION

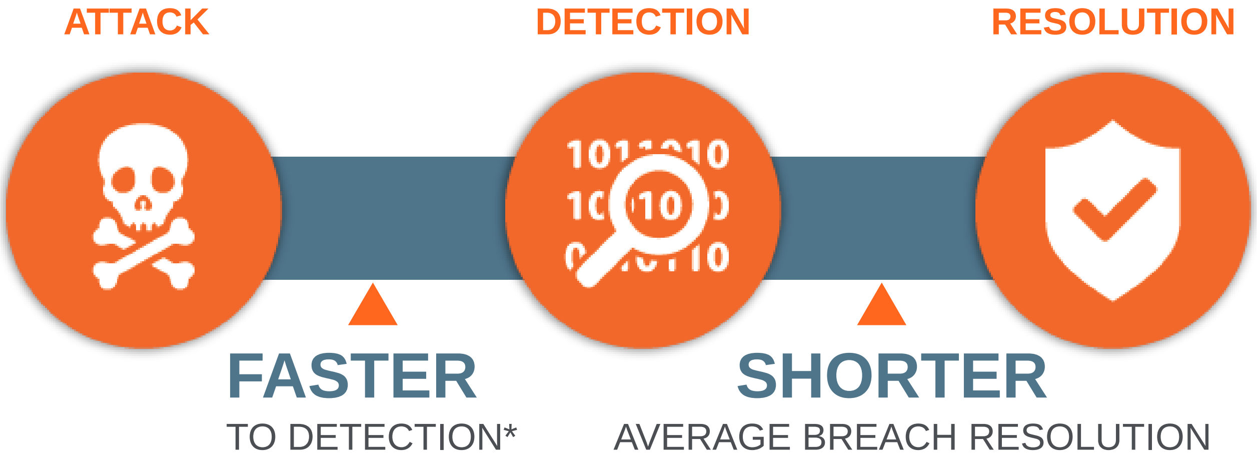
206 DAYS
TO DETECTION*

21-35 DAYS
AVERAGE BREACH RESOLUTION

* Verizon 2014 Data Breach Investigations Report

QUICKLY CLOSING THE WINDOW

OUR MISSION



ATTACK

DETECTION

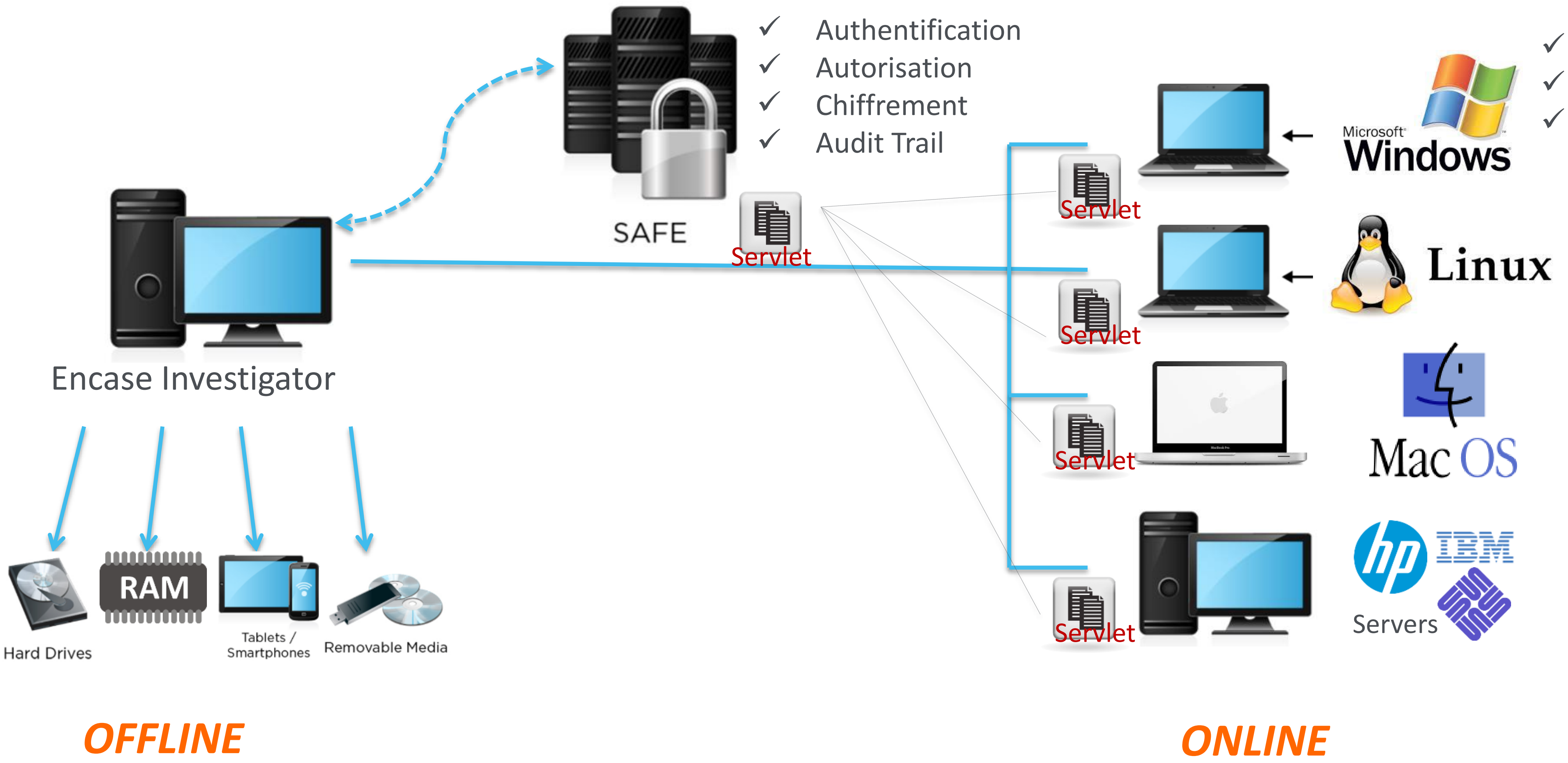
RESOLUTION

FASTER
TO DETECTION*

SHORTER
AVERAGE BREACH RESOLUTION

NET RESULT = LOWER COST
manpower, time, exposure to business and mitigated risk

ENCASE® ENDPOINT SECURITY



- ✓ Authentification
- ✓ Autorisation
- ✓ Chiffrement
- ✓ Audit Trail

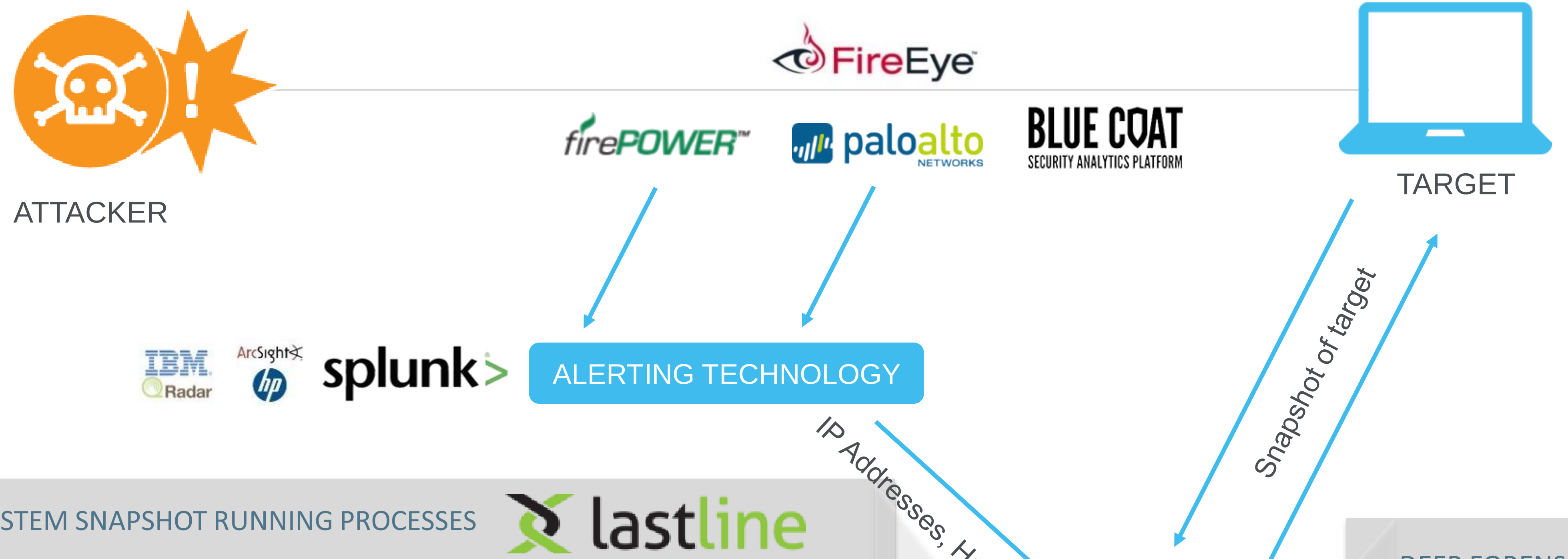
- ✓ Multi-OS
- ✓ Multi-plateformes
- ✓ Niveau noyau

ENCASE ENDPOINT SECURITY
“STATE OF ART” EDR (ENDPOINT DETECTION & RESPONSE) PLATFORM

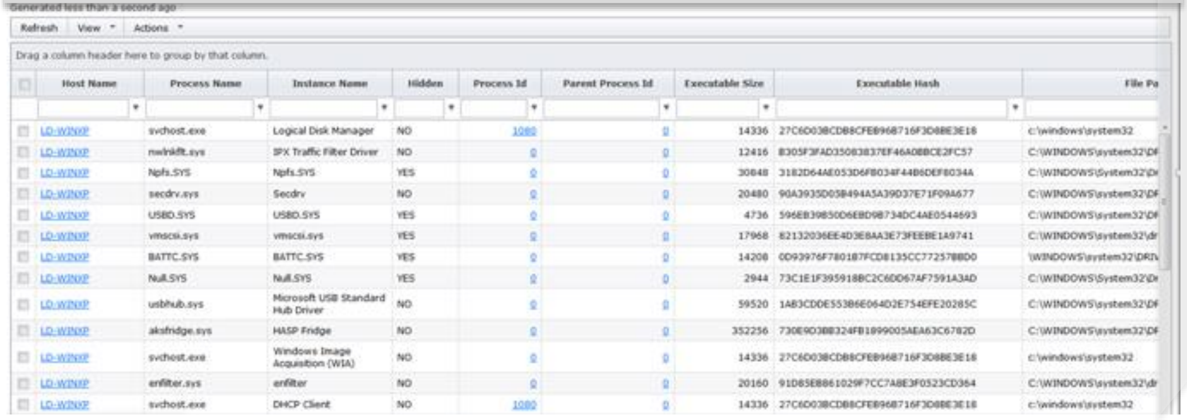
MATCHING THE TEAM TIER TO THE FEATURES

Security Team Tier	Primary Use Case	Endpoint Security Features	Benefit
Tier 1 (SOC)	Alert Triage	• Snapshot • SIEM (or other alerting tool) Integration • **Cyber Threat Intel (CTI)** Integration	Endpoint context from the time of the alert enables quicker triage and prioritization.
Tier 2+ (CIRT)	IR Support	• **IOC** & **multi-pattern Search** • **Forensic Remote Collection** • Memory acquisition • Registry Search • **Polymorphic** Entropy Near Match Scan • **Remediation**	Broad (enterprise-wide) and deep dive investigation to determine scope and root cause. Bring compromised systems back to a trusted state via remediation.
Trending & Intel (Threat Hunting/Intelligence)	Threat Detection and Threat Hunting	• **Analytics** • Scalable Enterprise-wide Snapshot • Historical Snapshot Database • **Long term Retrospective Analysis**	Improved situational awareness from knowledge of endpoint activity. Rich endpoint dataset that enables proactive threat hunting and detection of threats without known indicators via anomaly detection.

How Response Automation Works



SYSTEM SNAPSHOT RUNNING PROCESSES

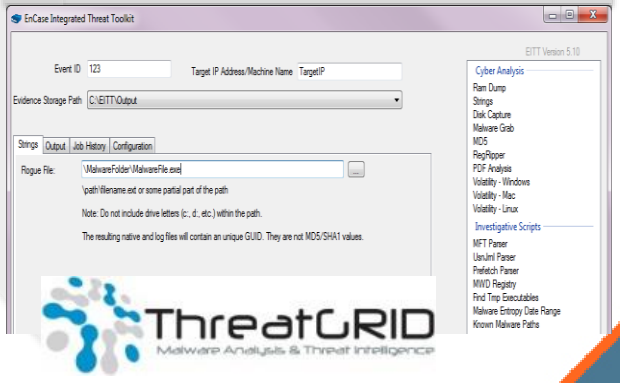


Generated less than a second ago

Drag a column header here to group by that column.

☐	Host Name	Process Name	Instance Name	Hidden	Process Id	Parent Process Id	Executable Size	Executable Hash	File Pa
☐	LD-WINXP	svchost.exe	Logical Disk Manager	NO	1080	0	14336	27C6D03BCDB8CFEB968716F3D8BE3E18	c:\windows\system32
☐	LD-WINXP	nwlnkflt.sys	IPX Traffic Filter Driver	NO	0	0	12416	8305F3FAD35083837EF46A0BBCE2FC57	C:\WINDOWS\system32\DF
☐	LD-WINXP	Npfs.SYS	Npfs.SYS	YES	0	0	30848	3182D64AE053D6FB034F44B6DEF8034A	C:\WINDOWS\System32\Dr
☐	LD-WINXP	secdrv.sys	Secdrv	NO	0	0	20480	90A3935D05B494A5A39D37E71F09A677	C:\WINDOWS\system32\DF
☐	LD-WINXP	USBD.SYS	USBD.SYS	YES	0	0	4736	596EB39B50D6EBD9B734DC4AE0544693	C:\WINDOWS\system32\DF
☐	LD-WINXP	vmscsi.sys	vmscsi.sys	YES	0	0	17968	82132036EE4D3E8AA3E73FEEBE1A9741	C:\WINDOWS\system32\dr
☐	LD-WINXP	BATTC.SYS	BATTC.SYS	YES	0	0	14208	0D93976F780187FCD8135CC77257BBD0	\WINDOWS\system32\DRIV
☐	LD-WINXP	Null.SYS	Null.SYS	YES	0	0	2944	73C1E1F395918BC2C6DD67AF7591A3AD	C:\WINDOWS\System32\Dr
☐	LD-WINXP	usbhub.sys	Microsoft USB Standard Hub Driver	NO	0	0	59520	1AB3CDDE553B6E064D2E754EFE20285C	C:\WINDOWS\system32\DF
☐	LD-WINXP	aksfridge.sys	HASP Fridge	NO	0	0	352256	730E9D3BB324FB1899005AEA63C6782D	C:\WINDOWS\system32\DF
☐	LD-WINXP	svchost.exe	Windows Image Acquisition (WIA)	NO	0	0	14336	27C6D03BCDB8CFEB968716F3D8BE3E18	c:\windows\system32
☐	LD-WINXP	enfilter.sys	enfilter	NO	0	0	20160	91D85EB861029F7CC7A8E3F0523CD364	C:\WINDOWS\system32\dr
☐	LD-WINXP	svchost.exe	DHCP Client	NO	1080	0	14336	27C6D03BCDB8CFEB968716F3D8BE3E18	c:\windows\system32

DEEP FORENSIC ANALYSIS & EITT



EnCase Integrated Threat Toolkit

EITT Version 5.10

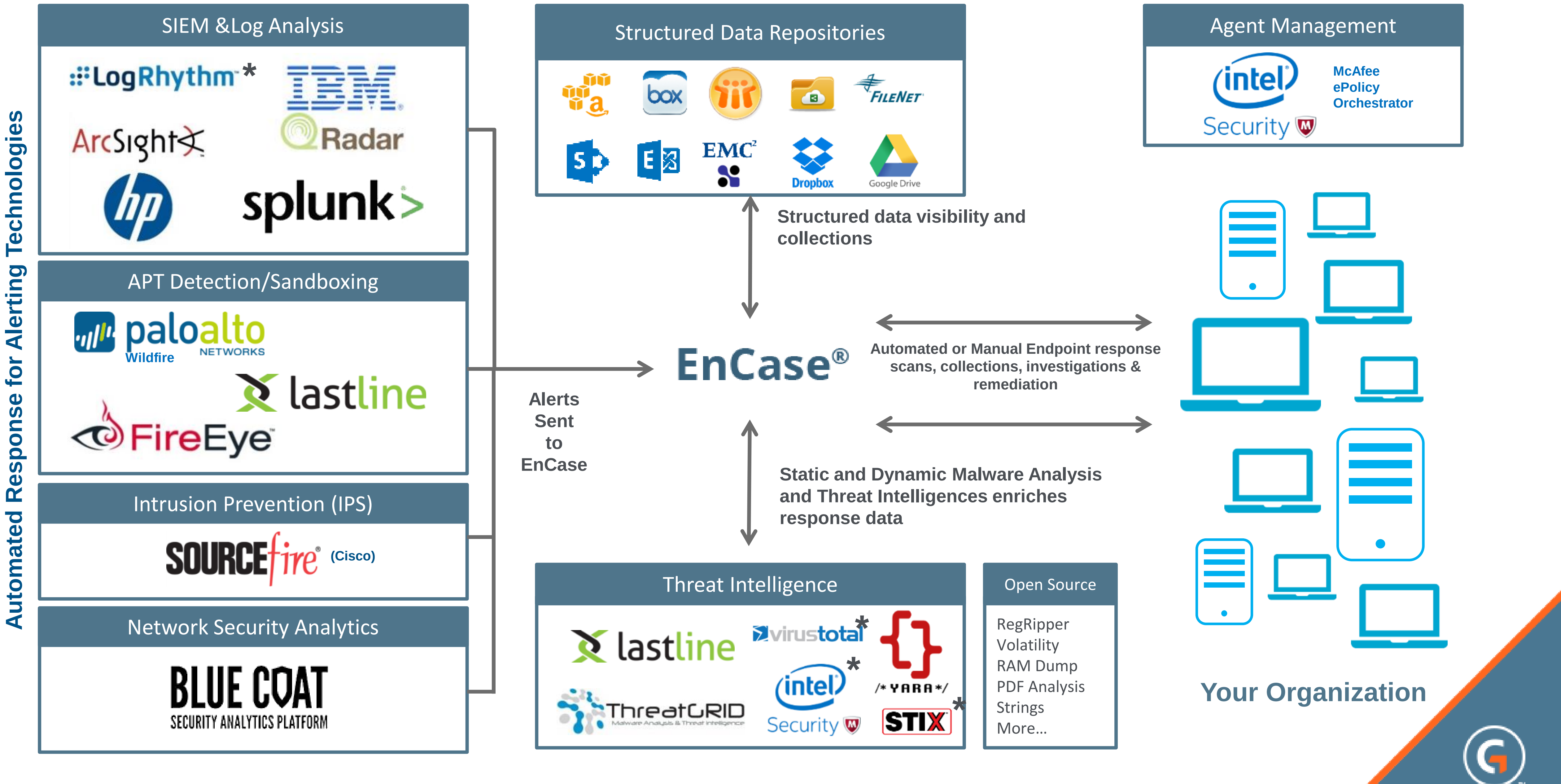
Event ID: 123
Target IP Address/Machine Name: TargetIP
Evidence Storage Path: C:\EITT\Output

Rogue File: \MalwareFolder\MalwareFile.exe

\path\filename.ext or some partial part of the path

Note: Do not include drive letters (c:, d:, etc.) within the path.

The resulting native and log files will contain an unique GUID. They are not MD5/SHA1 values.



Automated Response for Alerting Technologies

SIEM &Log Analysis

APT Detection/Sandboxing

Intrusion Prevention (IPS)

(Cisco)

Network Security Analytics

Alerts Sent to EnCase

Structured Data Repositories

Structured data visibility and collections

EnCase®

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

Static and Dynamic Malware Analysis and Threat Intelligences enriches response data

Threat Intelligence

Open Source

RegRipper
Volatility
RAM Dump
PDF Analysis
Strings
More…

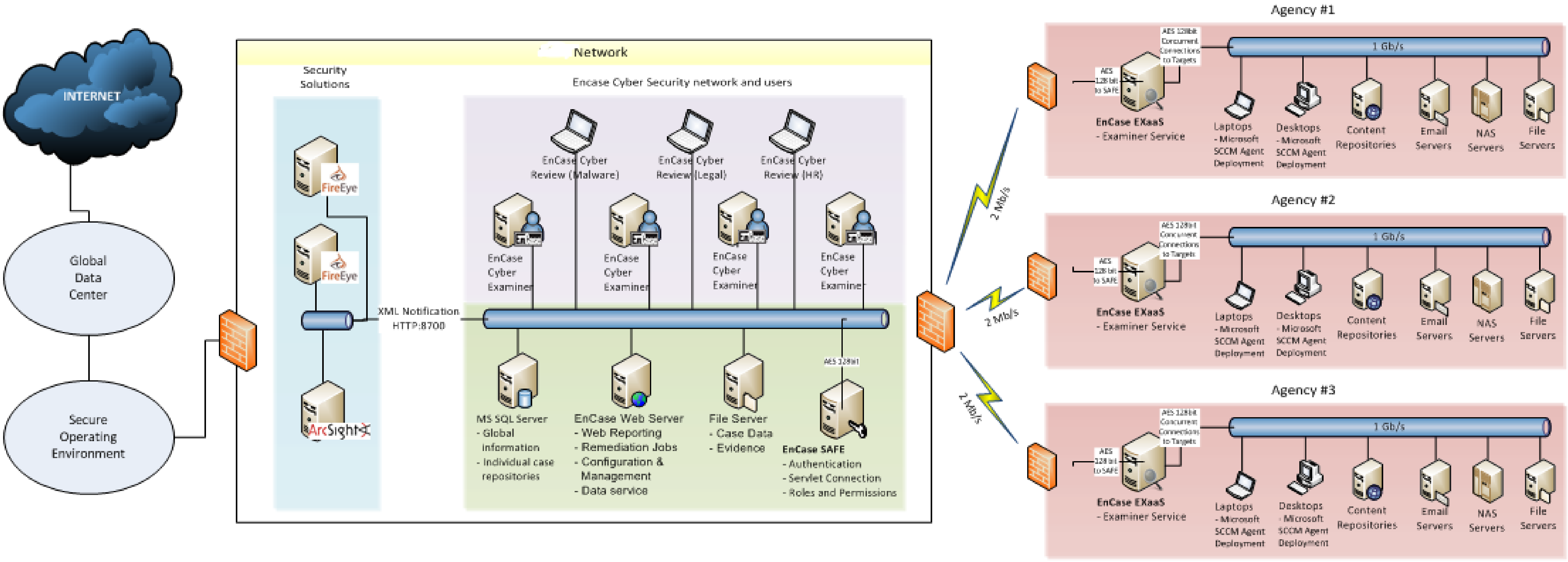
Agent Management

McAfee ePolicy Orchestrator

Your Organization

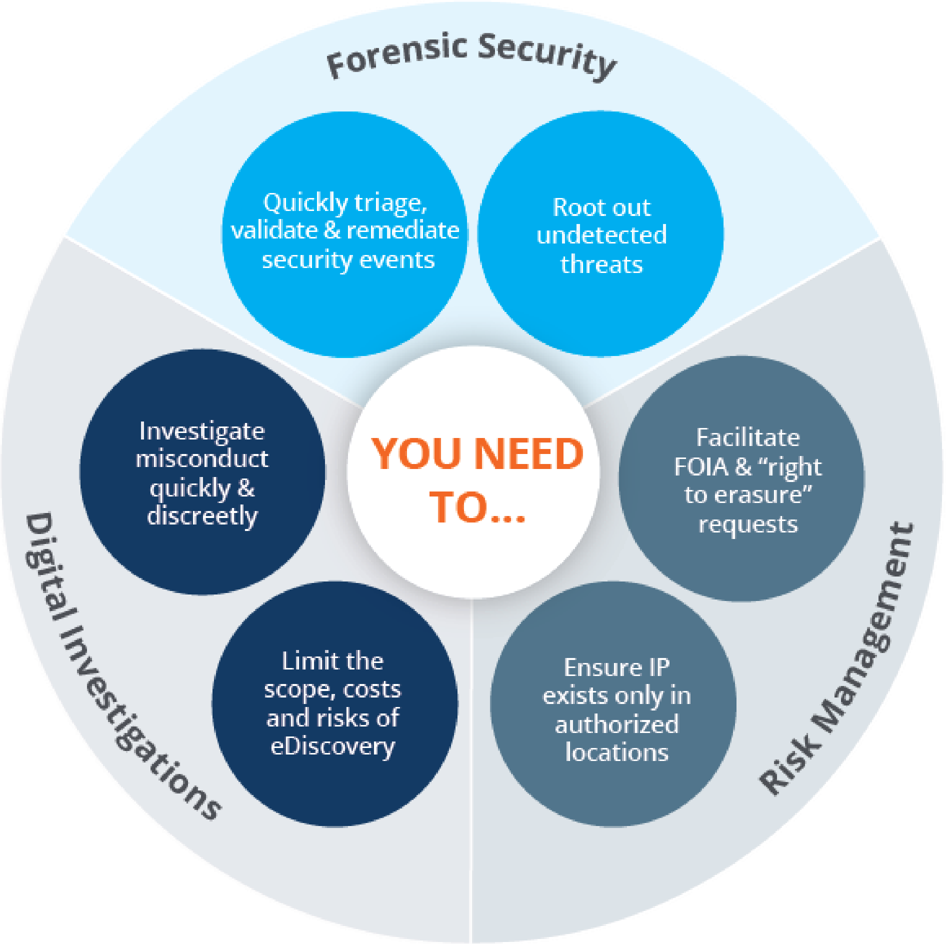
* Pending

ARCHITECTURE – SOC+IR



YOU REQUIRE MANAGEMENT OF & CONTROL OVER

DIGITAL RISK


Forensic Security
Quickly triage, validate & remediate security events
Root out undetected threats
YOU NEED TO...
Investigate misconduct quickly & discreetly
Limit the scope, costs and risks of eDiscovery
Digital Investigations
Facilitate FOIA & "right to erasure" requests
Ensure IP exists only in authorized locations
Risk Management

Guidance gives you complete visibility to address real business problems

- Regulatory Compliance
- Breach Detection & Response
- Employee Investigation
- Law Enforcement Investigation
- Litigation Support
- Sensitive Data Control

ADDRESS REAL BUSINESS PROBLEMS WITH

360° VISIBILITY

DIGITAL INVESTIGATIONS

Industry standard Digital Forensic solution

- Remote, Defensible Collections
- Search & Analysis
- Customizable Reporting and Secure Collaboration
- Extensible Platform

E-DISCOVERY

4 Year Gartner Magic Quadrant Leader

- Early Case Assessment
- Legal Hold
- Search & Identification
- Collection & Preservation
- Review & Production

ENDPOINT DETECTION & RESPONSE

#1 Market share leader as ranked by Gartner

- Anomaly Detection
- Threat Assessment
- Automated and On-demand Incident Response
- Incident Triage
- Validation & Remediation

UNIFIED ENDPOINT AGENT ARCHITECTURE

Deployed to more than 25 Million Endpoints globally

[1] Gartner, Inc., "Competitive Landscape: Endpoint Detection and Response Tools, 2014"

MERCI

Fortunato Guarino
Solution Consultant
Guidance Software
fortunato.guarino@guid.com

Francis Ia
Solution Consultant
Guidance Software
francis.ia@guid.com

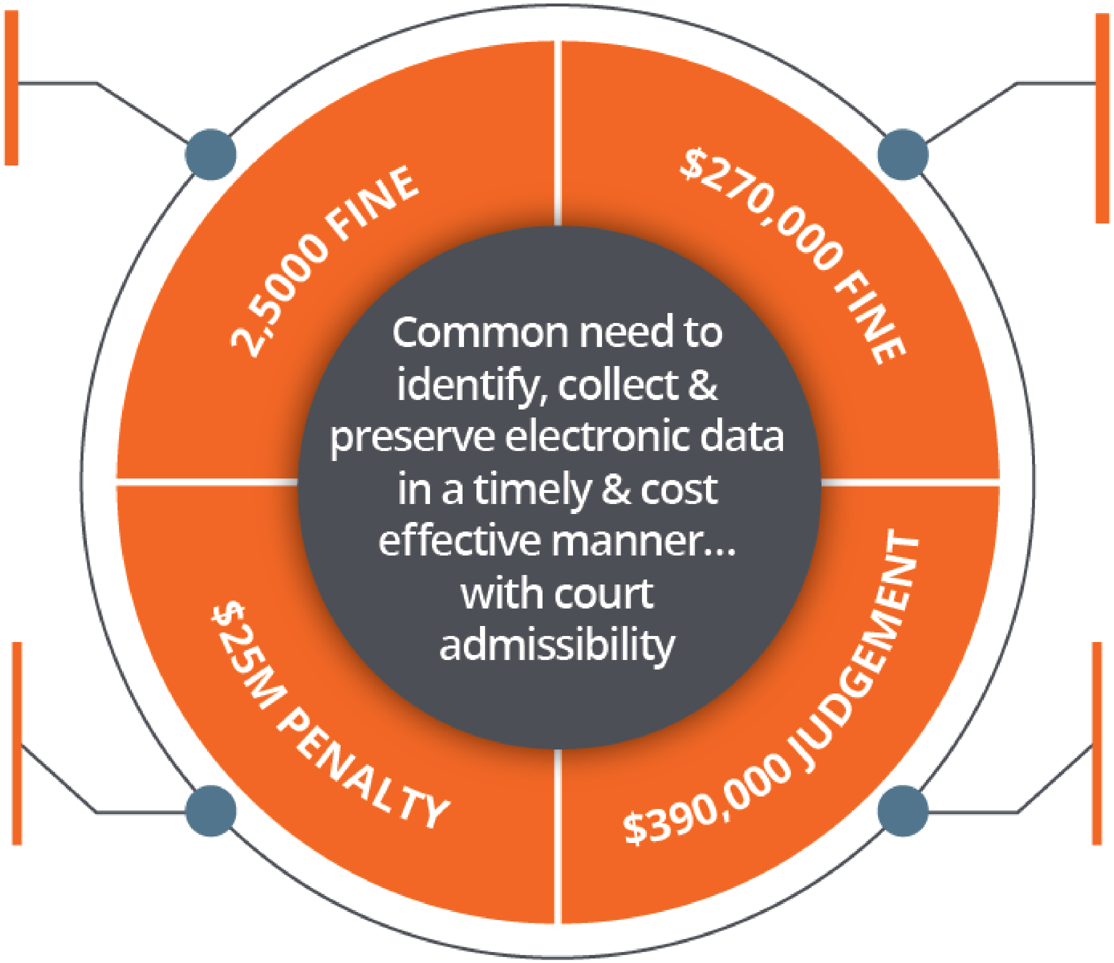
EnCase® Endpoint Investigator

by Guidance Software

THE COST OF NON-COMPLIANCE

FCC INVESTIGATIONS
Internet search giant fails to produce evidence validating responses to a request

REGULATORY REQUESTS
Global financial services firm fails to respond to FINRA requests in a timely manner



Common need to identify, collect & preserve electronic data in a timely & cost effective manner… with court admissibility

SEC FRAUD INVESTIGATION
Communications technology company fails to properly conduct internal investigation

HR INVESTIGATIONS
EEOC* sues large internet search provider for failure to investigate discrimination claim

Actual Penalties Based on Publicly Available Information, Such as Media Reports or Court Filings.

DIGITAL INVESTIGATION CHALLENGES

ORGANIZATIONS ARE ASKING:

HOW DO I...

INVESTIGATE SUSPECTED HR/PERSONNEL VIOLATIONS?

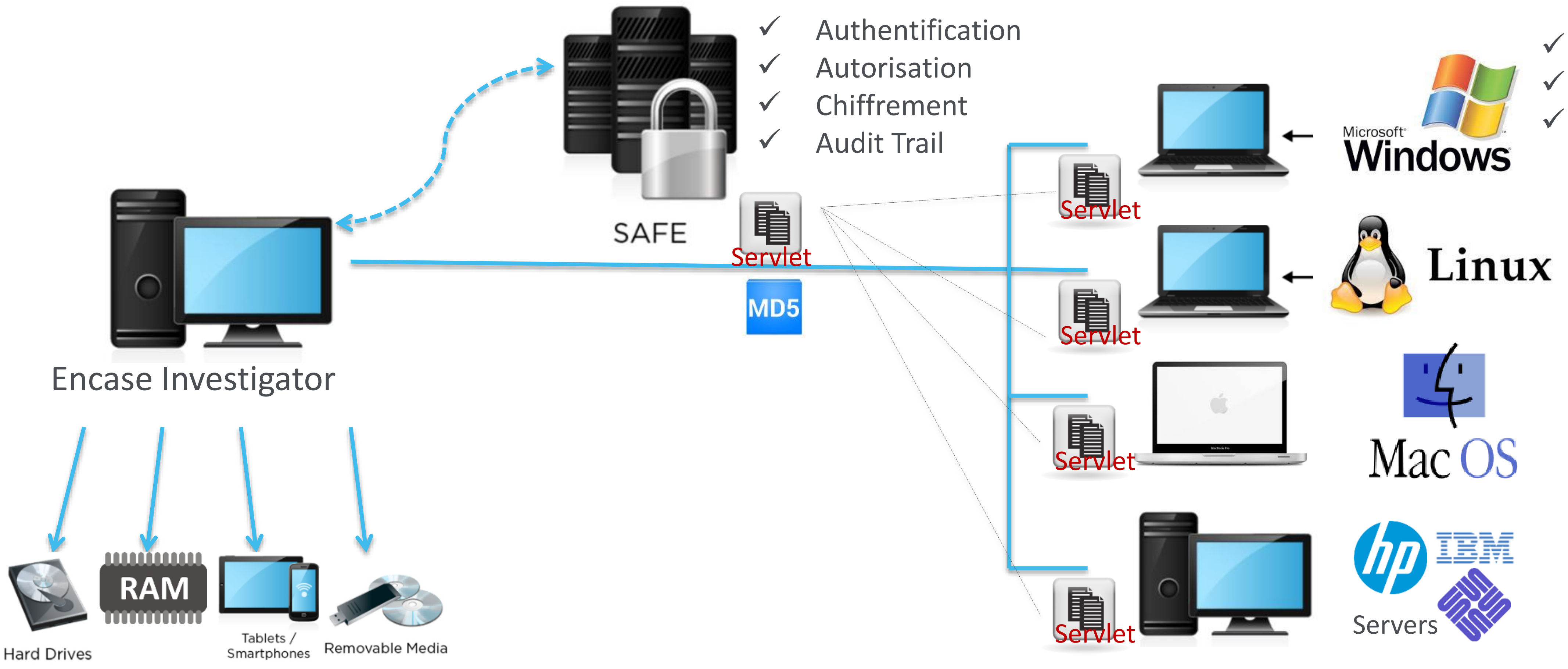
CONFIRM OR DENY ALLEGATIONS OF FRAUD OR FINANCIAL MISMANAGEMENT?

ENSURE ACCURACY & COMPLETENESS OF INVESTIGATION?

SCALE OUR ABILITY TO INVESTIGATE?

ENSURE DIGITAL INVESTIGATIONS ARE DONE COVERTLY DURING BUSINESS HOURS?

ENCASE® ENDPOINT SECURITY



- ✓ Authentification
- ✓ Autorisation
- ✓ Chiffrement
- ✓ Audit Trail

- ✓ Multi-OS
- ✓ Multi-plateformes
- ✓ Niveau noyau

OFFLINE

ONLINE

WHY ENCASE ENDPOINT INVESTIGATOR

Industry-standard digital investigation solution for organizations of all sizes and industries

Reduce the cost and complexity

- Enterprise investigations are more effective

Ensure confidence in findings

- Uncover more evidence faster than with any other solution

Investigate discreetly

- Achieve full, secure and discreet visibility to all endpoints

Manage from a central location

- Eliminate examiner travel, employee downtime, and analysis times with centrally managed investigations

THE VALUE OF REMOTE FORENSIC

Faster response

- Immediate access to networked devices, quicker investigations
- Centralized control and instant results
- On-site internal staff enabled to investigate from an central location

THE VALUE OF REMOTE FORENSIC

Improved visibility

- Find and understand data on any endpoints
- Access to “live” data found in RAM for key insights
- EnCase agent sees “below” the operating system
- Endpoints include e-mail servers and file shares
- Broadest OS, file system, and encryption support

THE VALUE OF REMOTE FORENSIC

Efficient and effective

- Rapid, concurrent investigation of devices
- Template-driven workflow
- Patented Distributed Optimized Search includes; file type, keywords, metadata, hash values, patterns and more
- Judicially accepted collection and preservation
- Ability to conduct covert investigations

CASE STUDY:

CORPORATE FRAUD INVESTIGATION

Recovery of previously deleted documents in an investigation leads to terminations and criminal charges

A large multinational corporation was **accused of questionable financial reporting** by the Securities and Exchange Commission, resulting in an investigation by a major independent consulting company. The goal of the investigation was to determine if the CFO had ordered his staff to alter or destroy transactions to help the company's financial position appear more favorable. **EnCase Endpoint Investigator was used to perform an exhaustive search of all computer records** within the company's large finance division.

It was soon discovered that management had ordered staff to destroy key documents. However, some employees did not fully comply with the order, making the files easy to recover. The entire **process occurred covertly, without impacting business operations** or productivity. Eventually, **enough information was recovered to reconstruct the actual events** and prove that numerous high-level managers had schemed to alter the records of the company. The suspected staff members were terminated and criminal charges were brought against them.

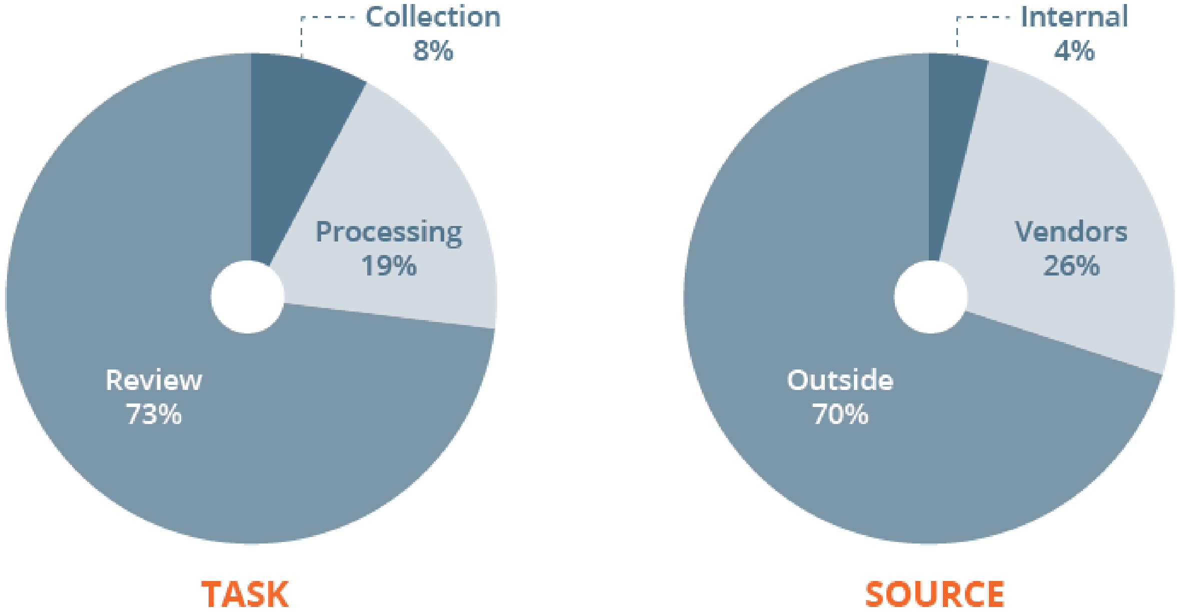
EnCase® eDiscovery

by Guidance Software

THE HIGH COST OF E-DISCOVERY

- Average cost of e-discovery expenditures: **$1.8 Million**
- Cost per GB Produced: **Average $83K**
- Average GBs Produced per Matter: **30**

Figure S.1
Relative Costs of Producing Electronic Documents



NOTE: Values reflect median percentages for cases with complete data, adjusted to 100 percent.
RAND *MG1208-S.1*

Institute for Civil Justice, A RAND LAW, BUSINESS, AND REGULATION INSTITUTE, 2012

DISCOVERY CHALLENGES

ORGANIZATIONS **ARE ASKING...**

DO I HAVE A JUDICIALLY DEFENSIBLE AND REPEATABLE PROCESS?

AM I PREPARED TO RESPOND TO AN E-DISCOVERY REQUEST OR INVESTIGATION?

CAN I EFFICIENTLY ISSUE AND ENFORCE LEGAL HOLDS?

HOW CAN I REDUCE THE COSTS AND RISKS ASSOCIATED WITH E-DISCOVERY?

CAN I QUICKLY IDENTIFY AND PRESERVE POTENTIALLY RELEVANT ESI?
(ELECTRONICALLY STORED INFORMATION)

WHERE IS THE “SMOKING GUN”?

WHY ENCASE EDISCOVERY

Reduce Costs and Risk while Streamlining Your E-Discovery Process

Reduce costs

- A projected 67% savings with in-house e-discovery

Accelerate Review

- Eliminate time spent reviewing duplicate documents

Increase productivity

- Reduce risk of spoliation with an automated & defensible legal hold process

Control costs and scope

- Early and ongoing case assessment

CAPABILITIES:

EARLY CASE ASSESSMENT

Legal Hold and Pre-collection Analytics

- Automated legal hold
  - Manager Escalations
  - Approval workflows
- Keyword testing
- Custodian overview dashboards
- Non-disruptive collections

CAPABILITIES:

EFFICIENT DATA MANAGEMENT

Manage Multiple Matters & Reuse Data

- Eliminate unnecessary costs
- Reduce data volumes
- Save money and time
- Improve consistency
- Leverage existing work product
- Reduce time to resolution

CAPABILITIES:

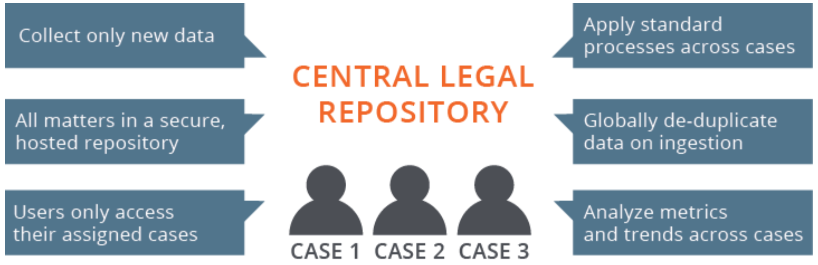
DEFENSIBLE COLLECTIONS

Collections and Preservation

- Patented optimized distributed search
- Non-disruptive, highly scalable, & automated collections
- Target keywords, hash values, or metadata properties
- Collect and preserve only those files that fit your criteria
- Supports widest variety of document repositories
- No pre-indexing required
- Judicially accepted targeted collections

CAPABILITIES:

INTEGRATED REVIEW


Collect only new data
All matters in a secure, hosted repository
Users only access their assigned cases
CENTRAL LEGAL REPOSITORY
CASE 1
CASE 2
CASE 3
Apply standard processes across cases
Globally de-duplicate data on ingestion
Analyze metrics and trends across cases

Review and Production

- Centralized repository for cross-case efficiency
- Reduction in human error while improving knowledge base
- Powerful analysis for early data assessment
- Consistency across all cases – coding, privilege decisions, tagging, etc.
- Cloud-hosted web application allows for collaboration
- Technology assisted review (TAR) functionality

CUSTOMERS WIN WITH GUIDANCE

FORTUNE 50

PROCTOR & GAMBLE

“Fortunately for P&G, we found this capability in a few vendors, like Guidance Software, and depend on their products and services to achieve an efficient, repeatable, and defensible e-discovery process.”

Scott Van Nice
E-discovery Manager
Proctor & Gamble

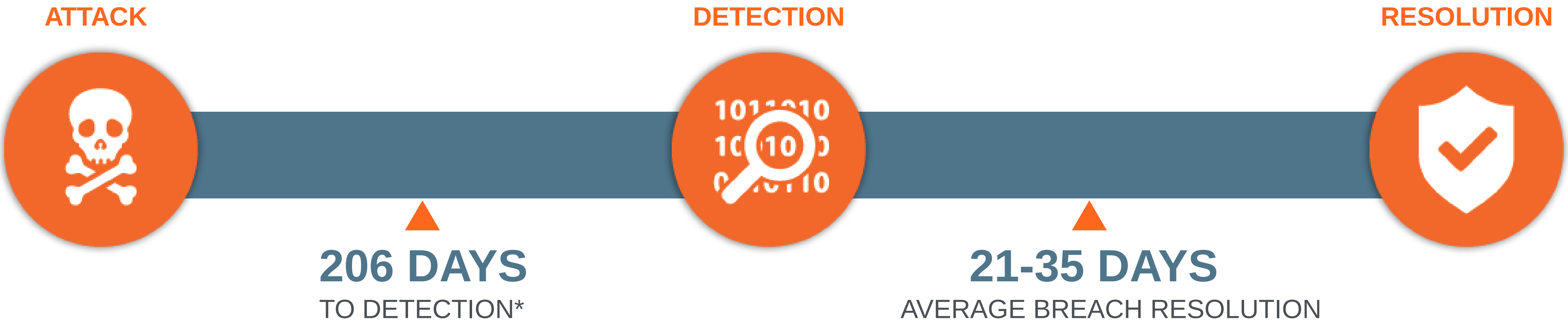
Situation	Solution	Results
Before brining e-discovery in-house, P&G had to rely on multiple outside vendors. There was no consistency, policy, or standard cost structure, and start-up time varied.	P&G identified thresholds of what to handle in-house and where to lean on trusted partners (decided on left side of EDRM using GSI)	eDiscovery matters from small to large are now handled in-house by a team of two
#Became apparent 8 years ago that with the right tools, training, and procedures, they could do more with less and save money at the same time.	Used EnCase for key custodians and scaled up for larger number of custodians	Reduced e-discovery spend by 50% in the first eight weeks
	Created an E-Discovery Governance Board, cross-functionally, that provides governance, insight, focus, and support	Reduced a four to six week case start-up to just two days
		Instituted a repeatable and defensible process

EnCase® Endpoint Security

by Guidance Software

EXPANDING WINDOW OF EXPOSURE

TODAY’S REALITY



ATTACK

DETECTION

RESOLUTION

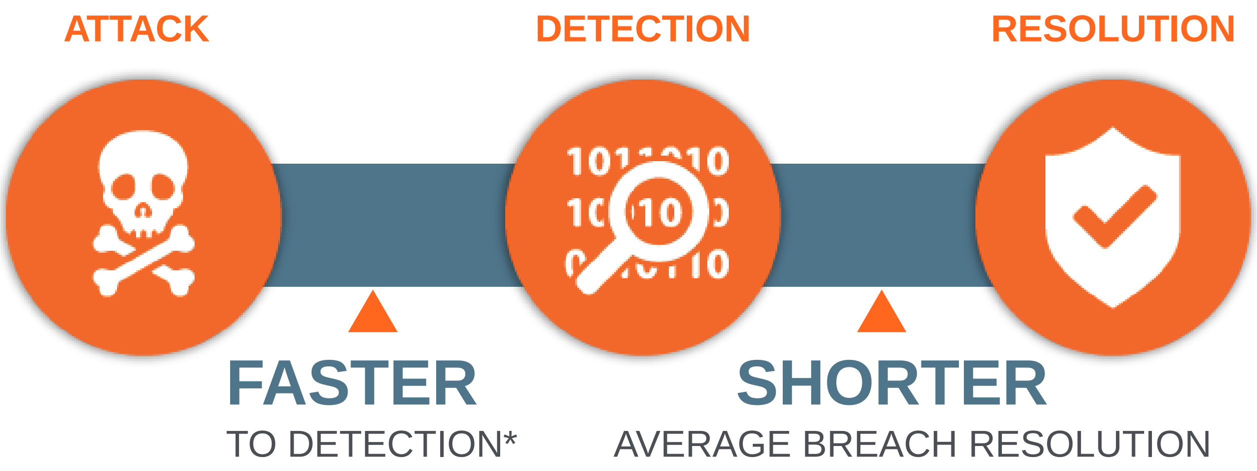
206 DAYS
TO DETECTION*

21-35 DAYS
AVERAGE BREACH RESOLUTION

* Verizon 2014 Data Breach Investigations Report

QUICKLY CLOSING THE WINDOW

OUR MISSION



ATTACK

DETECTION

RESOLUTION

FASTER
TO DETECTION*

SHORTER
AVERAGE BREACH RESOLUTION

NET RESULT = LOWER COST
manpower, time, exposure to business and mitigated risk

ENDPOINT SECURITY CHALLENGES

ORGANIZATIONS ARE **WORRIED ABOUT…**

RISK OF UNDISCOVERED THREATS (PREVENTION ISN'T WORKING BUT THERE IS NO NEXT STEP)

LACK OF 360° VISIBILITY INTO ENDPOINTS — THE TARGET OF ATTACKS

VALUABLE TIME WASTED MANUALLY COLLECTING AND CORRELATING ENDPOINT DATA

NO WAY TO IDENTIFY SECURITY GAPS AND VERIFY POLICIES ARE WORKING

HUGE RATE OF ALERTS, LACK OF EFFECTIVE VALIDATION & PRIORITIZATION CAPABILITY

WHY ENCASE ENDPOINT SECURITY

Close the security gap with proactive threat detection, alert triage and incident response

Detect sooner

- Expose unknown 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

CAPABILITIES:

DETECTION

Eliminate your reliance on signatures, heuristics, policies or IOCs

The only way to detect what you haven’t already!

- Every tiny action leaves an artifact of either system or user activity
- Artifact correlation defines a baseline and tells a story of use, no limitations
- Proactively detect the aberrations – known, unknown, insider, and zero day threats
  - Anomalies indicate unseen threats
  - Review of security policies redefine direction

ON-DEMAND:

INCIDENT RESPONSE

Reduce compromise to discovery and time to resolution from months to hours

Response shouldn’t take forever

- Quickly identify suspect processes using localized white/black lists
- Root out all potential indicators
- Determine if suspect files are Threats with ThreatGrid and other intelligence sources
- Determine scope and impact across the organization of any threat instance
- Integrate with existing workflow management, home grown and third party point solutions

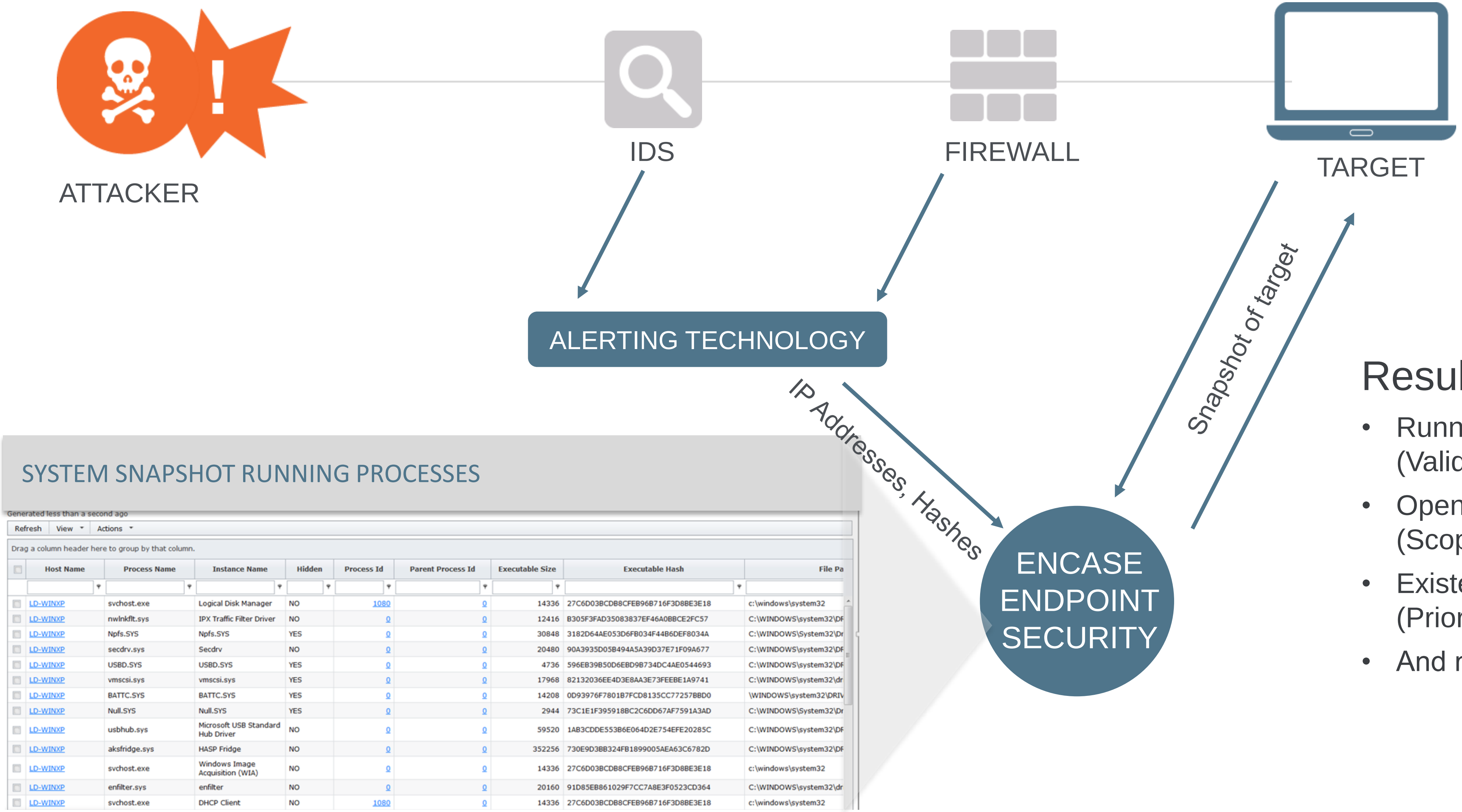
AUTOMATED INCIDENT RESPONSE

Ensure valid perimeter, network and log events are being seen!

Reduce compromise to discovery from months to days or hours

- Automated forensic collection integrates with existing security technologies
    - No information decay; works 24/7
- Reduce false-positive events quickly and gain down-stream benefits
- Identify unknown binaries triggering behavioral or heuristic alerts

HOW RESPONSE AUTOMATION WORKS



SYSTEM SNAPSHOT RUNNING PROCESSES

Generated less than a second ago

Drag a column header here to group by that column.

☐	Host Name	Process Name	Instance Name	Hidden	Process Id	Parent Process Id	Executable Size	Executable Hash	File Pa
☐	LD-WINXP	svchost.exe	Logical Disk Manager	NO	1080	0	14336	27C6D03BCDB8CFEB96B716F3D8BE3E18	c:\windows\system32
☐	LD-WINXP	nwlnkflt.sys	IPX Traffic Filter Driver	NO	0	0	12416	B305F3FAD35083837EF46A0BBCE2FC57	C:\WINDOWS\system32\DF
☐	LD-WINXP	Npfs.SYS	Npfs.SYS	YES	0	0	30848	3182D64AE053D6FB034F44B6DEF8034A	C:\WINDOWS\System32\Dr
☐	LD-WINXP	secdrv.sys	Secdrv	NO	0	0	20480	90A3935D05B494A5A39D37E71F09A677	C:\WINDOWS\system32\DF
☐	LD-WINXP	USBD.SYS	USBD.SYS	YES	0	0	4736	596EB39B50D6EBD9B734DC4AE0544693	C:\WINDOWS\system32\DF
☐	LD-WINXP	vmscsi.sys	vmscsi.sys	YES	0	0	17968	82132036EE4D3E8AA3E73FEEBE1A9741	C:\WINDOWS\system32\dr
☐	LD-WINXP	BATTC.SYS	BATTC.SYS	YES	0	0	14208	0D93976F7801B7FCD8135CC77257BBD0	\WINDOWS\system32\DRIV
☐	LD-WINXP	Null.SYS	Null.SYS	YES	0	0	2944	73C1E1F395918BC2C6DD67AF7591A3AD	C:\WINDOWS\System32\Dr
☐	LD-WINXP	usbhub.sys	Microsoft USB Standard Hub Driver	NO	0	0	59520	1AB3CDDE553B6E064D2E754EFE20285C	C:\WINDOWS\system32\DF
☐	LD-WINXP	aksfridge.sys	HASP Fridge	NO	0	0	352256	730E9D3BB324FB1899005AEA63C6782D	C:\WINDOWS\system32\DF
☐	LD-WINXP	svchost.exe	Windows Image Acquisition (WIA)	NO	0	0	14336	27C6D03BCDB8CFEB96B716F3D8BE3E18	c:\windows\system32
☐	LD-WINXP	enfilter.sys	enfilter	NO	0	0	20160	91D85EB861029F7CC7A8E3F0523CD364	C:\WINDOWS\system32\dr
☐	LD-WINXP	svchost.exe	DHCP Client	NO	1080	0	14336	27C6D03BCDB8CFEB96B716F3D8BE3E18	c:\windows\system32

Results

- Running processes (Validation)
- Open ports & N/w connections (Scope Assessment)
- Existence of sensitive data (Prioritization)
- And more…

RECOVERY & REMEDIATION

Wipe and reimage costs weeks!

Reduce time to resolution from weeks to hours

- Kill running processes
- Surgically remove all iterations of malware and related artifacts
- Wipe sensitive data from unauthorized locations
- Produce reports demonstrating success/compliance

CASE STUDY:

PROVEN RESULTS

Global Automotive Manufacturer

- Deliver 388% ROI
- Savings of over $2.4 millions in incident-related costs
- Reduce time to validate and triage threats by 89%
- Reduce time to remediate breaches by 90%
- Reduce impact onserver downtime by 98%