Trellix

EMEA & LTAM Tech Summit

3-6 November 2025

Madrid, Spain

Trellix

Welcome to the Endpoint journey

Speaker Intro

Robert Lourenco

EMEA Solution Architect

Steen Pedersen

Global Technical product manager

Marco Kappert

Director of Solution engineering EMEA

Trellix

Before We Begin

Use the following WIFI:
SID: **???????**
Password: **??????**

Please pay attention to the following items...

Silence Your Devices

Please mute or turn off your smartphones and other electronic devices to minimize distractions during the presentation.

Restrooms

Restrooms are located ?????.

Emergency Exits

The main exit is located at ?????.

Q&A

We will have a Q&A throughout the session

Session Schedule

The session is expected to last approximately 3 hours with one 30 min. break.

Trellix

Our Agenda Today

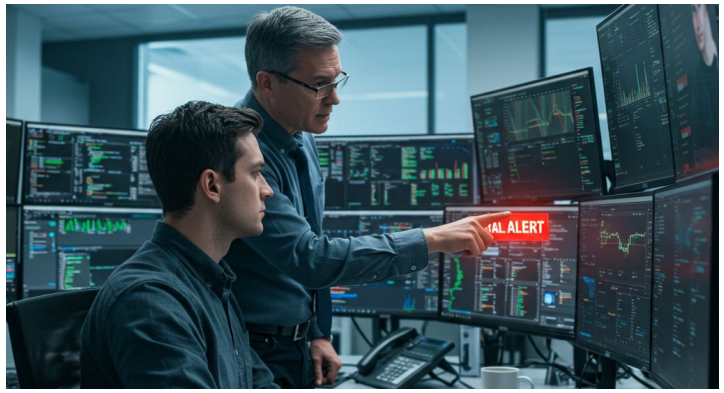
Trellix Endpoint Security

1) Introduction to Endpoint Suite
2) Overview of Key Components
3) EDRF overview/architecture & roadmap
4) ENS, ePO and TACC Roadmap
5) System information reporter
6) Key Use cases
7) Demo
8) Licensing

Trellix

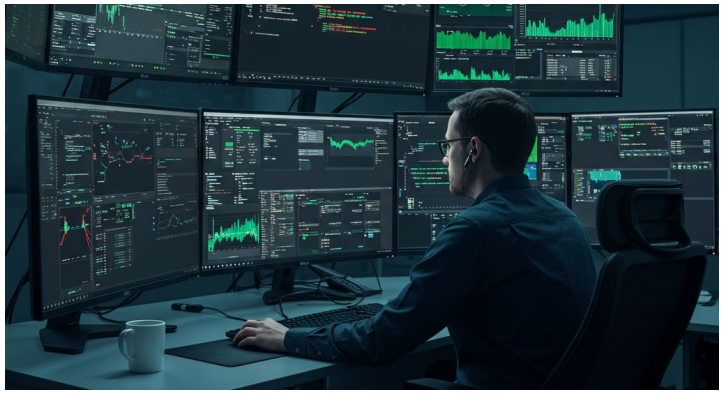
Challenges

Organization’s evolving challenges



Security Analyst

"I'm drowning in alerts, lacking **critical context**, and wasting time on manual data collection, leading to **alert fatigue** and slow investigations.”



SOC Manager

"My team's efficiency is hampered by **limited resources** and a need to elevate skills, making it hard to keep pace with threats and **optimize our security operations.**"

CISO

“I'm under immense pressure to **prove our security program's maturity** and resilience, worried about our ability to withstand **advanced attacks** and demonstrate **due diligence post-breach.**"

Trellix

Required Capabilities

Organization's evolving challenges

Achieve Endpoint Resilience

w/ **Battle-tested** protection **optimized** on all endpoints **proactively**

Uncover Evasive Threats

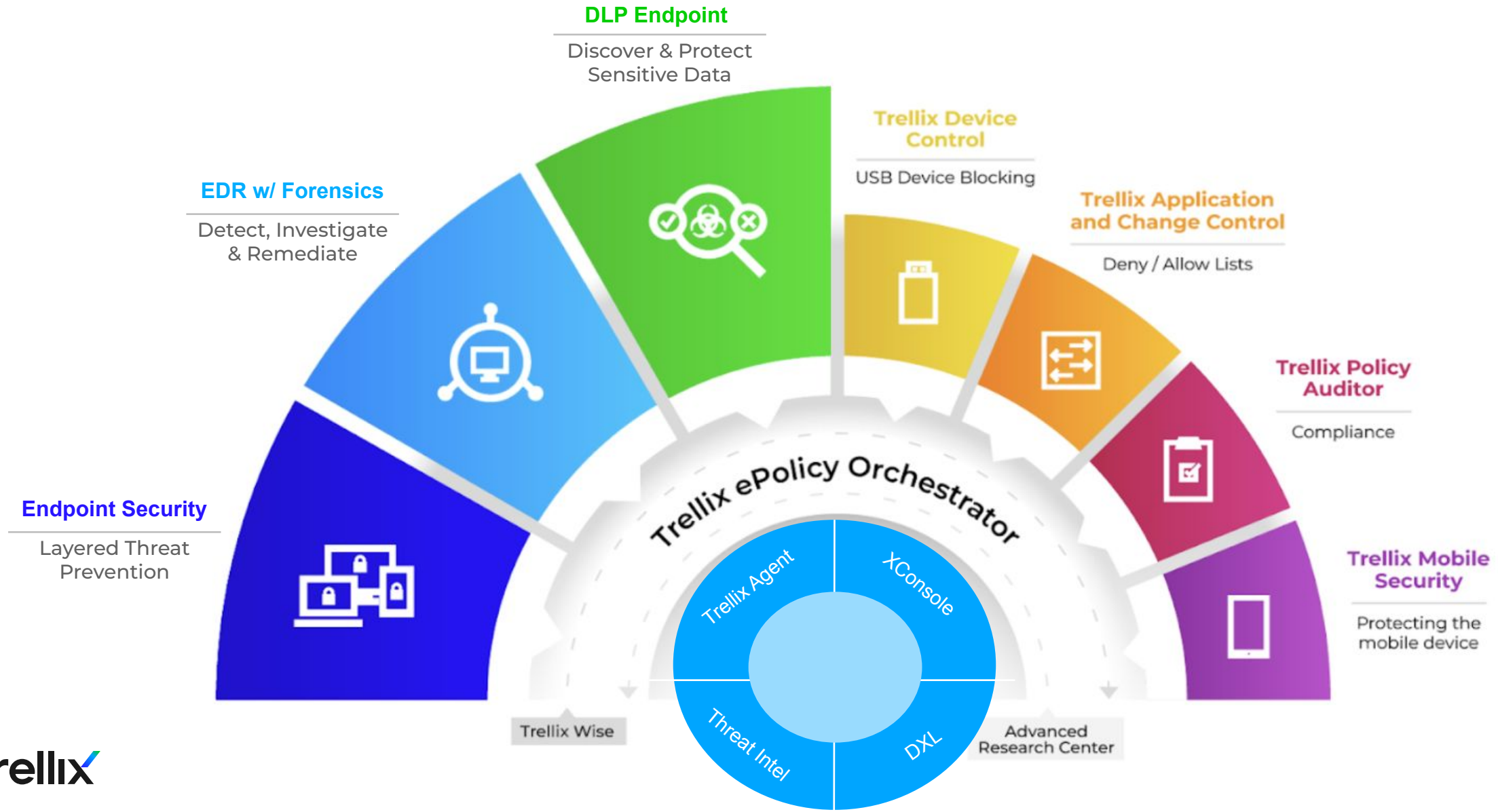
w/ Effective and **accurate alerts**, incident **triage,** and **prioritization**

Neutralize Security Incidents

w/ Immediate **response, root cause** awareness, and **remediation**

Trellix

Integrated & Performant Layered Security



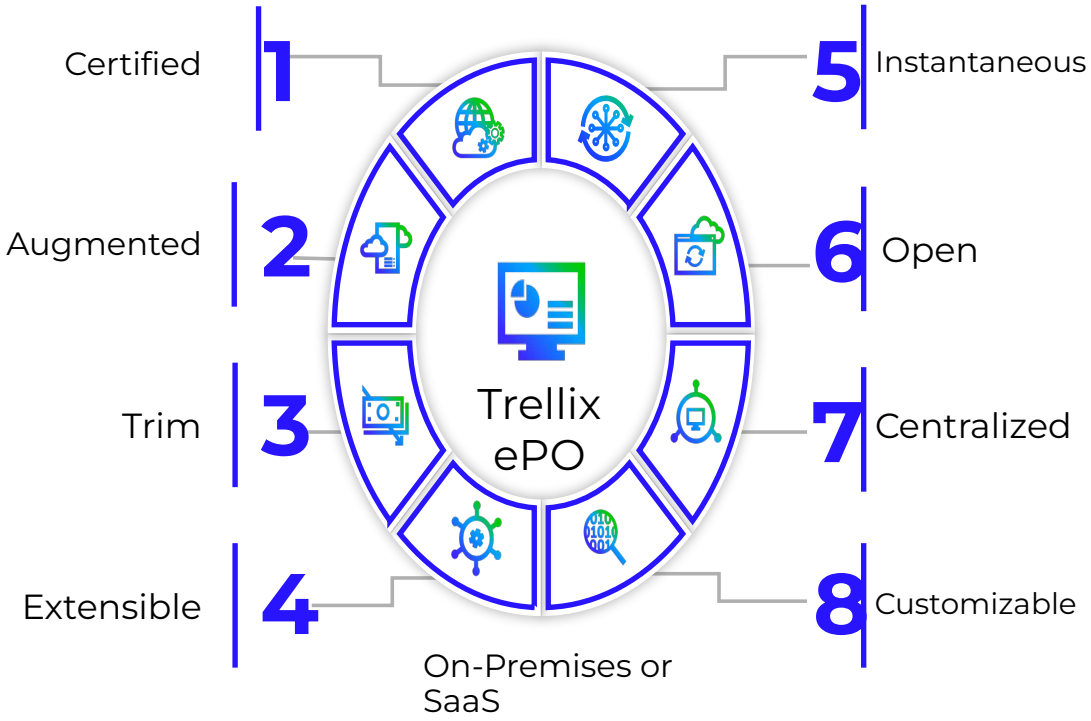
Trellix

Trellix ePolicy Orchestrator

ePolicy Orchestrator
Endpoint Security Platform (ENS)
Adaptive Threat Protection
Device Control
Insights
Threat Intelligence Exchange
IVX
Application Control
EDRF

Streamlined deployment and policy management for all endpoints

- Dashboards and reports for security posture, monitoring and compliance
- Managed risk with Role-based access and controlled updates
- SaaS, on-premises, and hybrid deployment for flexibility and resiliency



Trellix

Trellix ePolicy Orchestrator

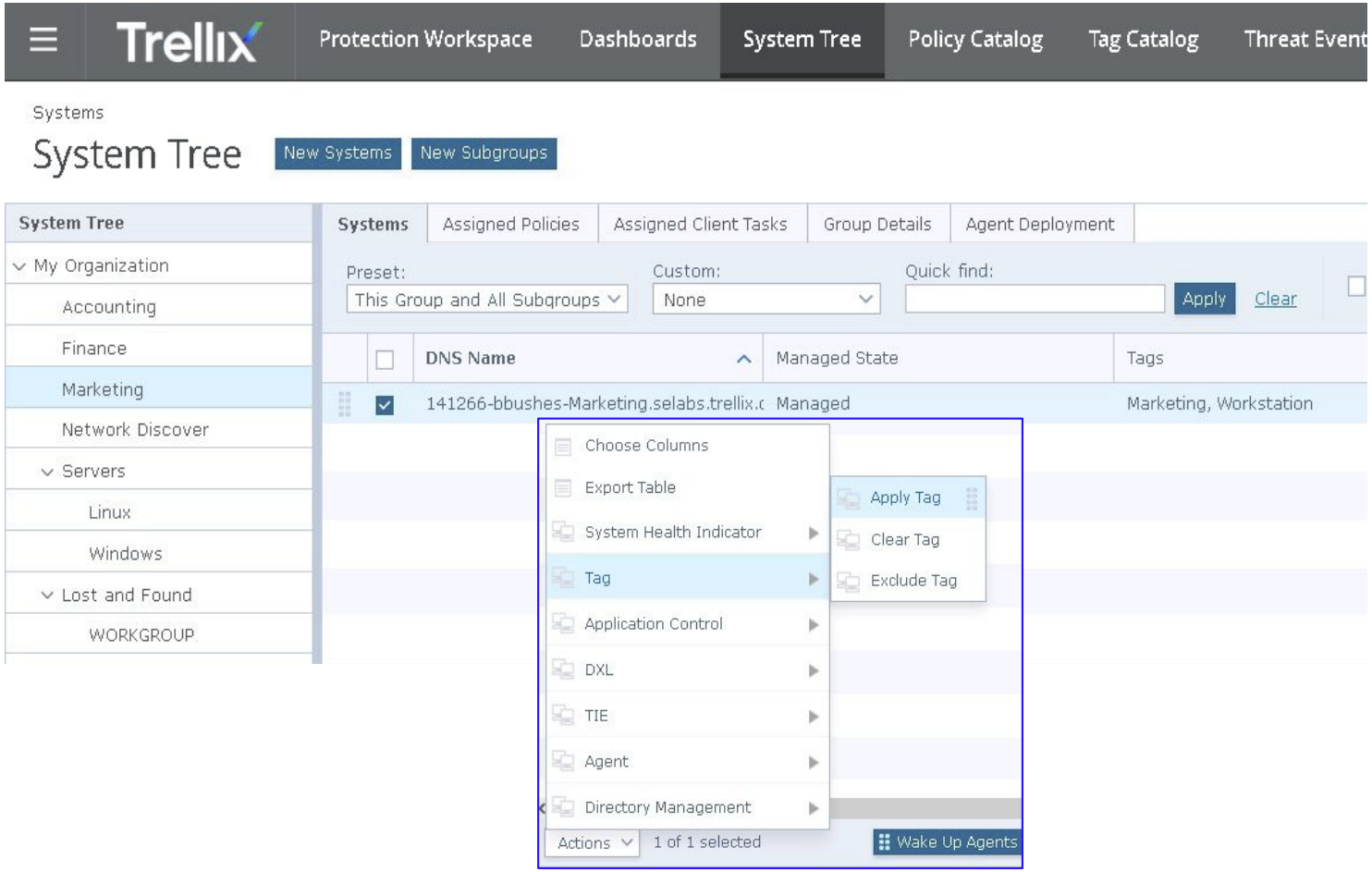
ePolicy Orchestrator
Endpoint Security Platform (ENS)
Adaptive Threat Protection
Device Control
Insights
Threat Intelligence Exchange
IVX
Application Control
EDRF

Flexible Policy Management

- Manage all endpoints, anywhere
- Automatically adapt policies to risk

Outcome

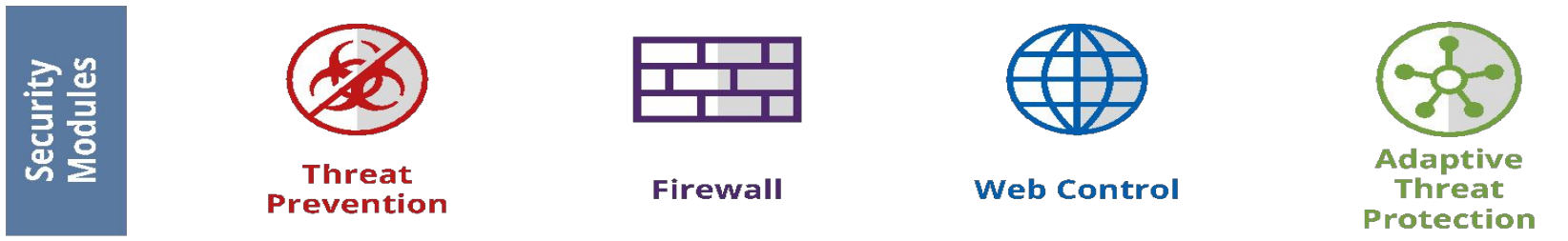
- Simplify endpoint security architecture
- Contain users and systems exposed to threats



Trellix

Trellix Endpoint security platform

- ePolicy Orchestrator
- **Endpoint Security Platform (ENS)**
- Adaptive Threat Protection
- Device Control
- Insights
- Threat Intelligence Exchange
- IVX
- Application Control
- EDRF



- ENS is a common service platform that is managed by ePO through the Trellix Agent
- ENS includes protection for:
  - Known Threats (Signatures)
  - Host Network Security (Firewall)
  - Safe browsing (Web Control)
  - Advanced and Zero Day Threats (Adaptive Threat Protection)

Trellix

Trellix Adaptive threat protection

- ePolicy Orchestrator
- Endpoint Security Platform (ENS)
- **Adaptive Threat Protection**
- Device Control
- Insights
- Threat Intelligence Exchange
- IVX
- Application Control
- EDRF

ML Protect

Block zero-day malware before it executes with static analysis machine learning and dynamic behavioral cloud-based machine learning

ML Protect Static (Pre-Execution)

Detect malware based on pre-execution static binary analysis using machine learning and comparison to known malware attributes

ML Protect Dynamic (Post-Execution)

Detect dynamic behavior of Greyware on the endpoint, compare to known malware behaviors for a match via behavioral cloud-based machine learning

Dynamic Application Containment

Containment = Limit or eliminate the ability of grayware to make changes on the endpoint while running endpoint detection analysis

Trellix

Trellix Device control

ePolicy Orchestrator
Endpoint Security Platform (ENS)
Adaptive Threat Protection
Device Control
Insights
Threat Intelligence Exchange
IVX
Application Control
EDRF

Centrally managed device blocking for unauthorized peripherals.

- **Ensure control of all external devices**
- **Prevent malware from entering the environment through unauthorized devices**
- **Granular controls to specify authorized devices by Vendor / Product ID or Serial**

Trellix

Trellix Insights

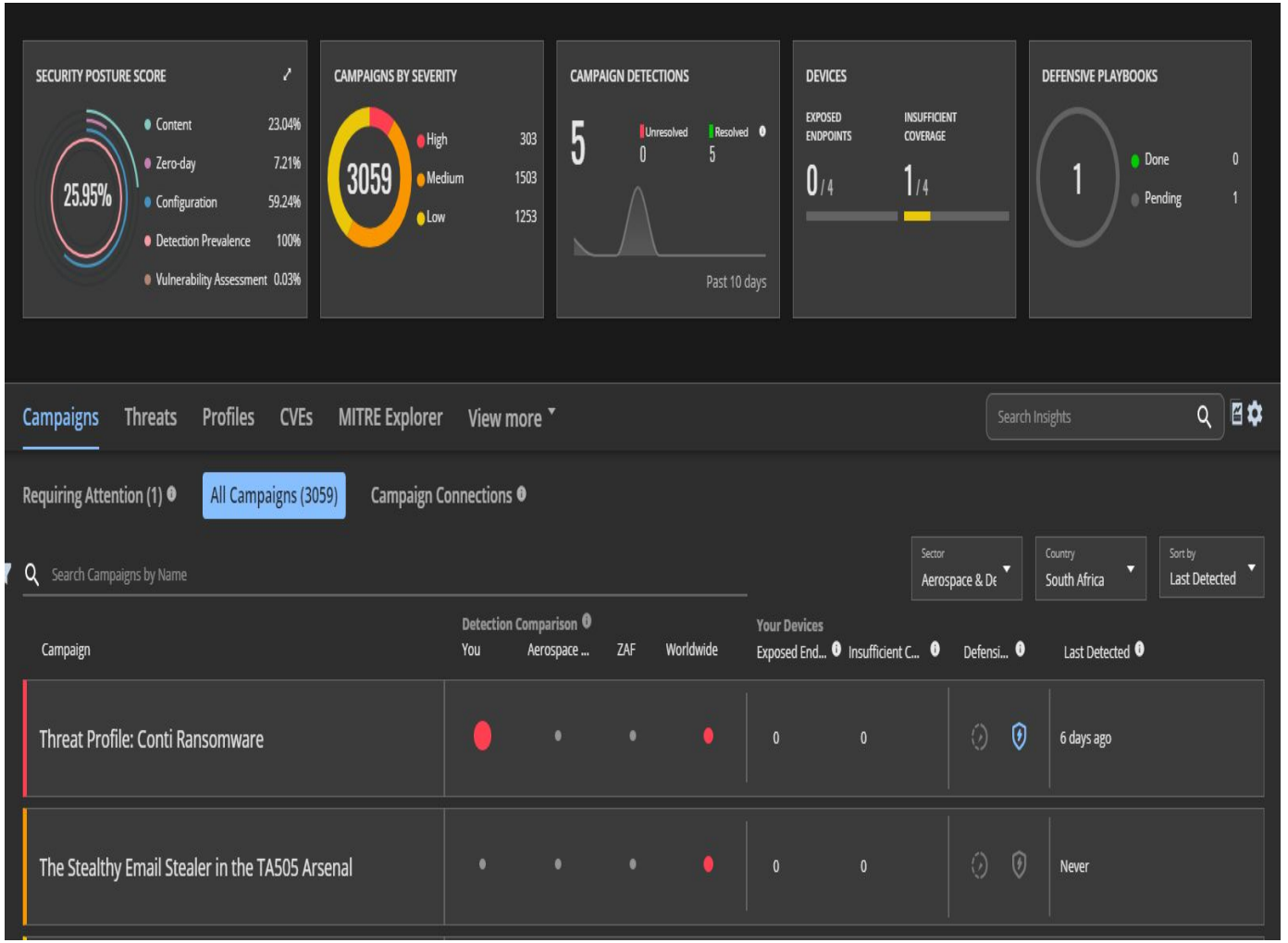
ePolicy Orchestrator
Endpoint Security Platform (ENS)
Adaptive Threat Protection
Device Control
Insights
Threat Intelligence Exchange
IVX
Application Control
EDRF

Threat Intelligence

- Detailed Threat Library
- Mapped to Industry and Geo

Outcome

- Threat attribution for detected attacks
- Reduced attack surface with tailored counter-measures
- Security Posture Assessments



Trellix Threat Intelligence Exchange

ePolicy Orchestrator
Endpoint Security Platform (ENS)
Adaptive Threat Protection
Device Control
Insights
Threat Intelligence Exchange
IVX
Application Control
EDRF

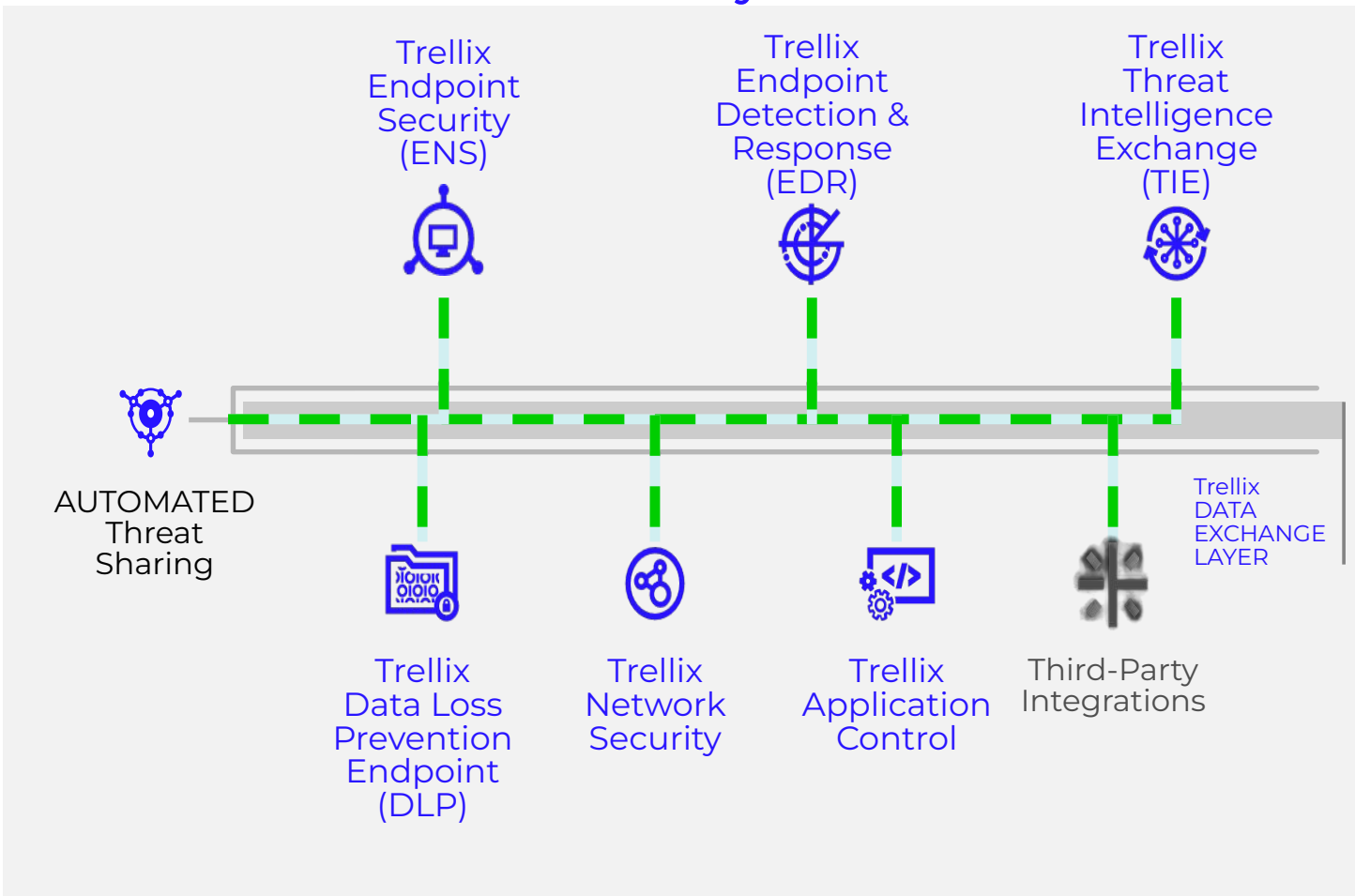
Reputation Sharing

- Security products work together
- Unknown Threats Discovered

Outcome

- Prevent unknown threats
- Adapt to global threats before they arrive
- Improve performance with rapid reputation checks

Share reputation intelligence instantly across the entire ecosystem

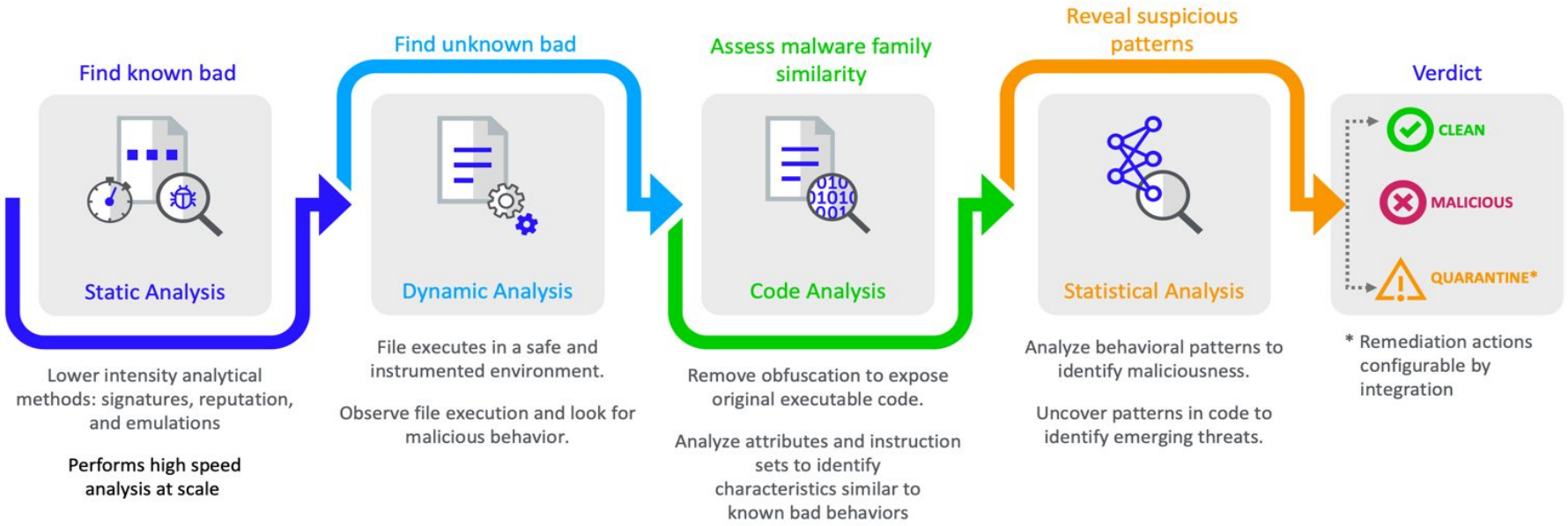


Trellix

Trellix Intelligence Virtual Execution

ePolicy Orchestrator
Endpoint Security Platform (ENS)
Adaptive Threat Protection
Device Control
Insights
Threat Intelligence Exchange
IVX
Application Control
EDRF

Multi-stage inspection process



Trellix

Trellix Application control

ePolicy Orchestrator
Endpoint Security Platform (ENS)
Adaptive Threat Protection
Device Control
Insights
Threat Intelligence Exchange
IVX
Application Control
EDRF

Whitelist created during install-time by scanning system for applications, libraries, drivers, and scripts

- Application attempting to launch can be an executable or an OS component
- Trellix Application Control verifies binary code from whitelist
- If not found in the whitelist, the program is not launched

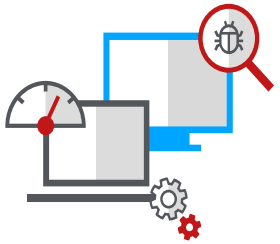
Dynamic Whitelisting  Dynamic Allow Listing	Prevents all unauthorized code from running
Memory Protection 	Prevents whitelisted apps from being exploited via buffer overflow attacks
File Reputation 	Integrates with GTI and TIE to classify binaries as Good, Bad and Unknown

Trellix

Trellix EDR with Forensics

- ePolicy Orchestrator
- Endpoint Security Platform (ENS)
- Adaptive Threat Protection
- Device Control
- Insights
- Threat Intelligence Exchange
- IVX
- Application Control
- **EDRF**

Collect Data



Always-on data collection

Broad visibility

Flexible retention

Surface Threats

Suspicious behavior detection

File-based and fileless threats

MITRE ATT&CK™ framework driven identification, and mapping

Guide Investigation

Investigate the Alert

Enable junior analysts

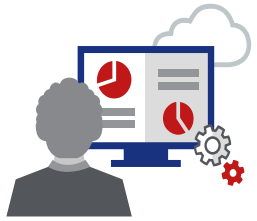
Automate alert triage

Correlate

Forensic Data Capture

Trellix WISE for EDR

Respond



Historical search

Real-time search

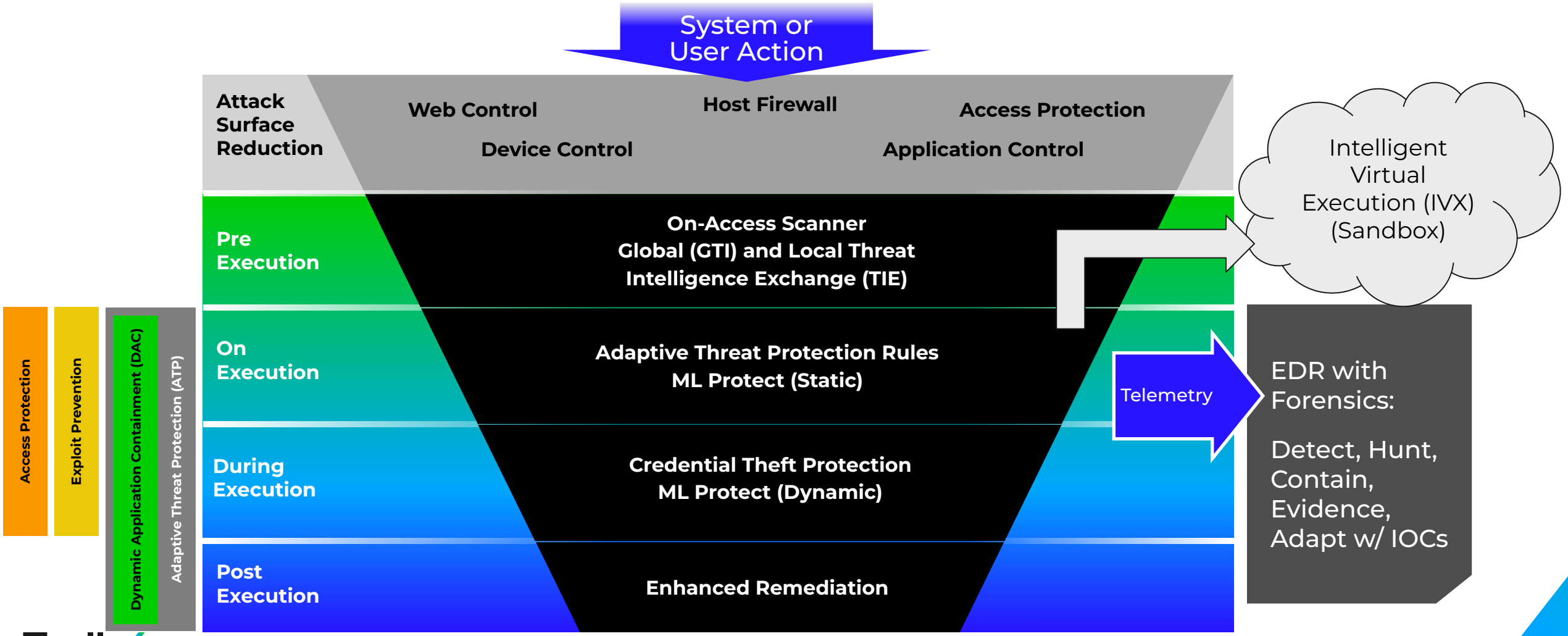
Data visualization

Robust response actions

Trellix

Achieve Endpoint Resilience

Multi-Layered Endpoint Protection

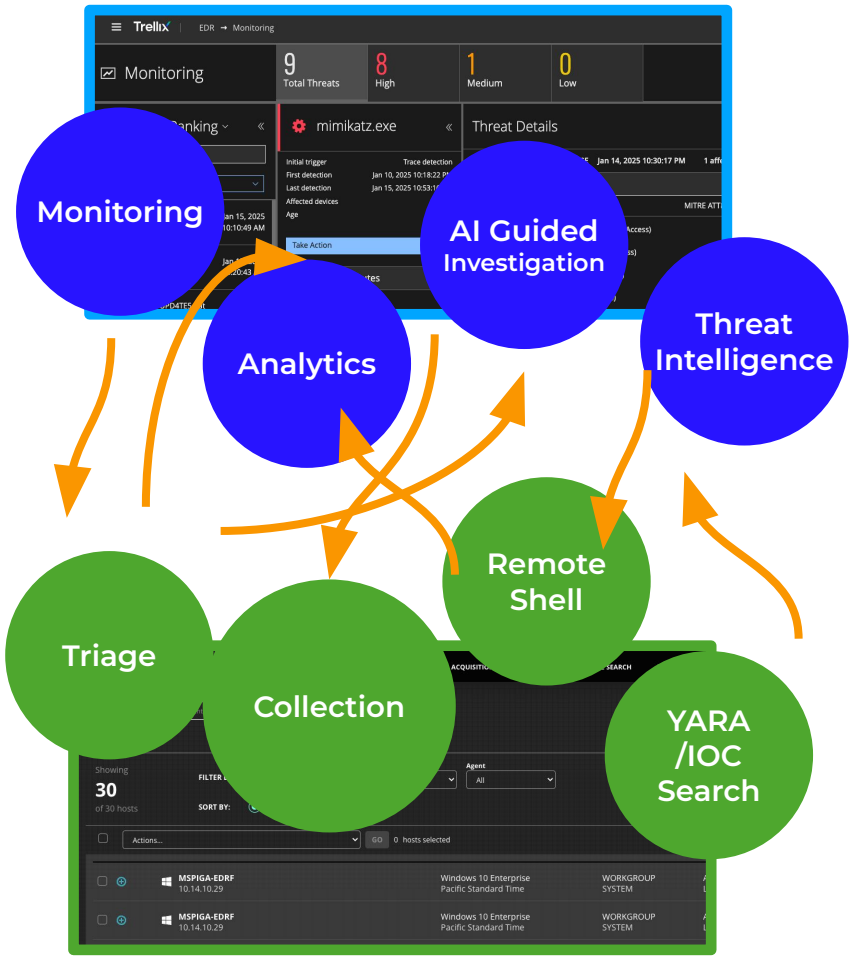


Trellix

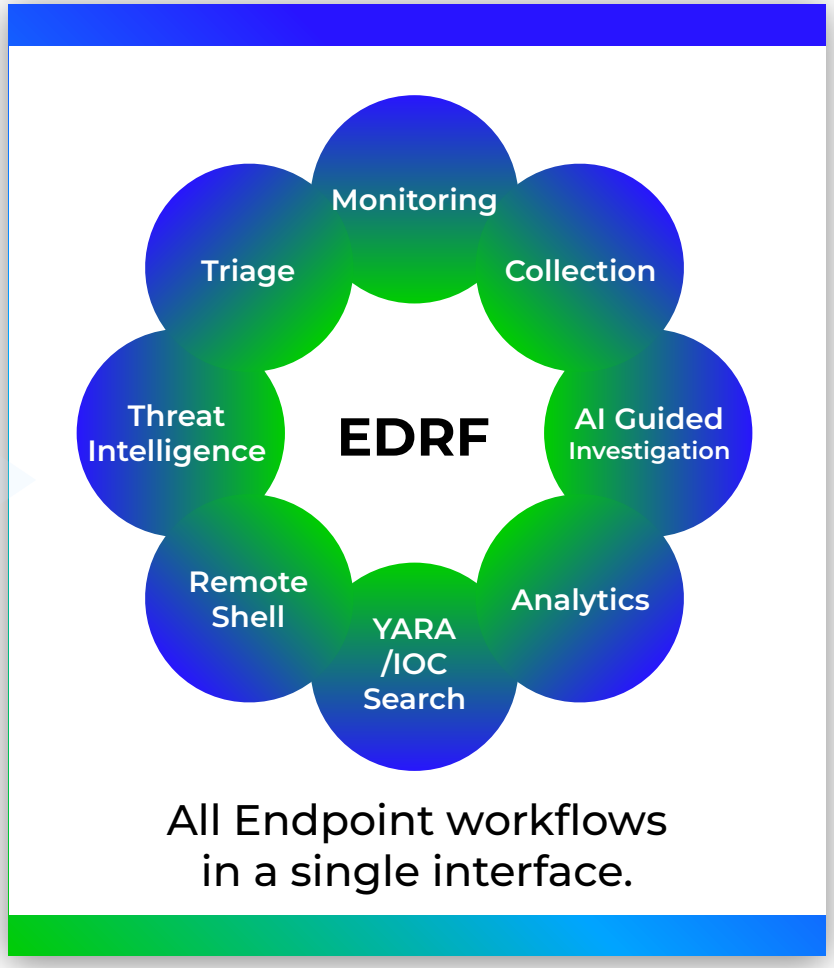
Trellix

Endpoint Detection and Response w/ Forensics

Unified Analyst Experience



The best capabilities brought together to reduce MTTD / MTTR for analysts



All Endpoint workflows in a single interface.

Trellix

Recent Progress: EDR with Forensics Cloud

Unifying EDR and Forensics

	Q2 2025	Q3 2025	Q4 2025 (Soon)
Unified Client	• Combined EDR + Forensics agent (Q4 2024)	• Remote Shell • Logon Tracker • Process Tracker • IPv6 support	• EDRF Client FIPS support
Unified Experience	•Streamlined analyst workflows •Custom IoCs creation •“One Click” EDR migration	• Expanded acquisition actions	• “One Click” HX migration (limited availability)
Unified Efficacy		• Improved detections w ETW-TI	

Vision for 2026

Trellix Analyst Workbench for all Trellix products

- Increases velocity for innovation, improvement and features
- Consistent user experience regardless of deployment type

Recent Progress: EDR with Forensics On-Prem

Leading on premise solution

Phase 1 (Dec '24)

Unified Client

- New EDRF Client launched 2024
- Improved responsiveness during bulk acquisitions
- More reliable backup and restore

Phase 2 (Sept'25)

Historical Search

- EDRF gains key Forensics functions:
  - Remote Shell
  - Logon Tracker
  - Process Tracker
- IPv6 Support
- ETW-TI
- Deployment improvements

Phase 3 (Nov '25)

Unified Experience

- Increased real-time endpoint behavior Visibility
- Historical Search for endpoints on or offline
- In-depth threat hunting of undetected malicious activity

Vision for 2026

Trellix Analyst Workbench for all Trellix products

- Increases velocity for innovation, improvement and features
- Consistent user experience regardless of deployment type

Management Benefits

ePolicy Orchestrator adds value not available with HX

Feature	Value
Advanced Policy Management	Flexible policy assignment, orchestration and management in ePO - policy history, approval, compare, revert, export, import, and clear policy assignments. Policy assignment rules. Clear view of what policies are assigned to any systems and usage of policies.
Custom Dashboard, Reporting and Queries	Generate custom dashboards, queries, and reports in ePO (alert, management data, and compliance reporting). Schedule and email reports and queries results automatically.
Improved scalability and availability	One ePO can handle multiple HX servers and move endpoints between different HX servers for migration and consolidation and for the forensics storage. Multiple Agent Handlers improve availability and scalability.
Automatic Responses	Automated reactions based on events, send email, tag system, run client tasks, assign different policy etc.

Feature	Value
Scheduled reactions and package deployment	Initiate and deploy any script or package on any endpoints or group of endpoints now, next time connected or scheduled interval (Win, Linux and macOS) using ePO Endpoint Deployment Kit (EEDK)
Detect unmanaged endpoints	Identify unmanaged endpoints on the network - Rogue System Detection (RSD)
Detect unmanaged virtual servers	Identify unmanaged virtual servers using Hypervisor connection (Cloud Workload Security add-on)
Identify software installed	Report on software installed on Windows endpoints - System Information Reporter (SIR)
Real time reputation lookup	Trellix Agent provide Data Exchange Layer (DXL) - Fast reputation lookup,Link to OpenDXL

Trellix

Protection Benefits

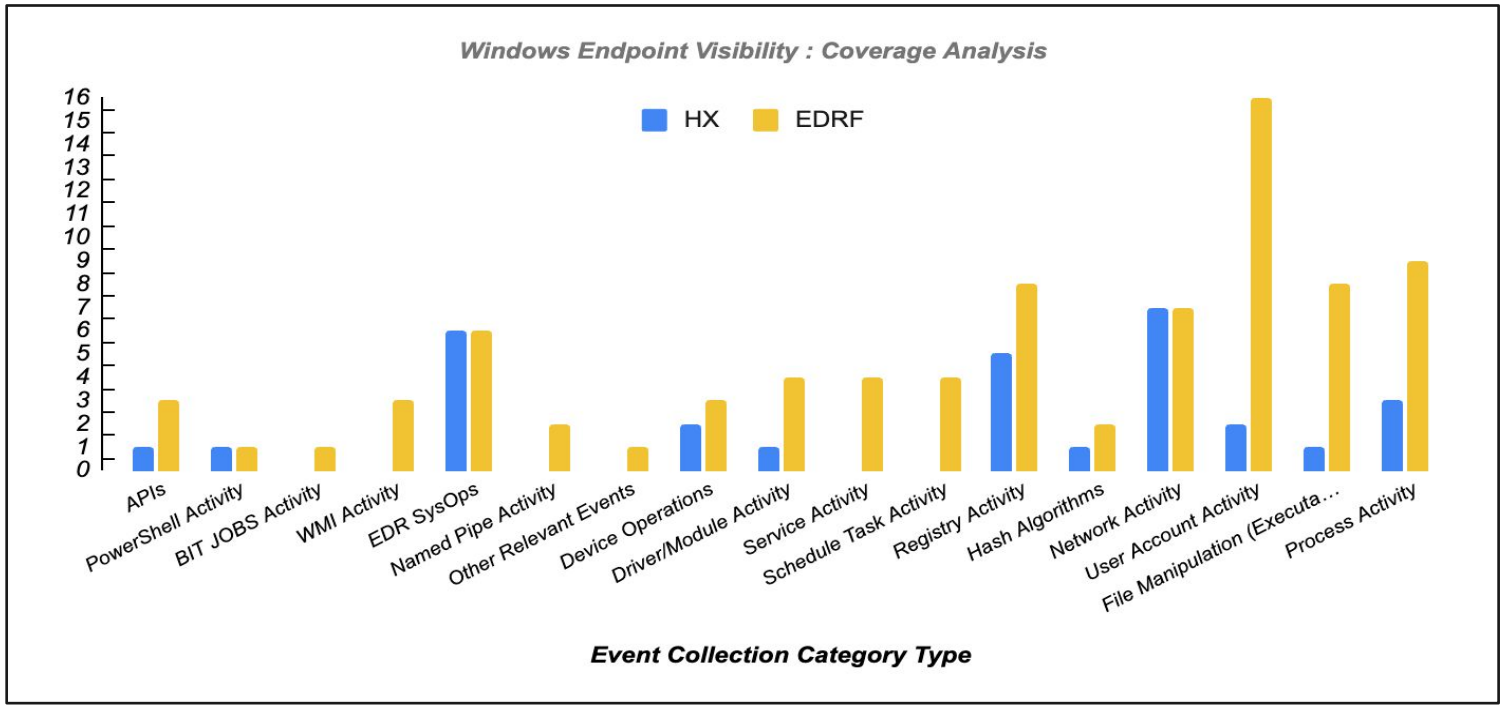
Offers increased prevention capabilities

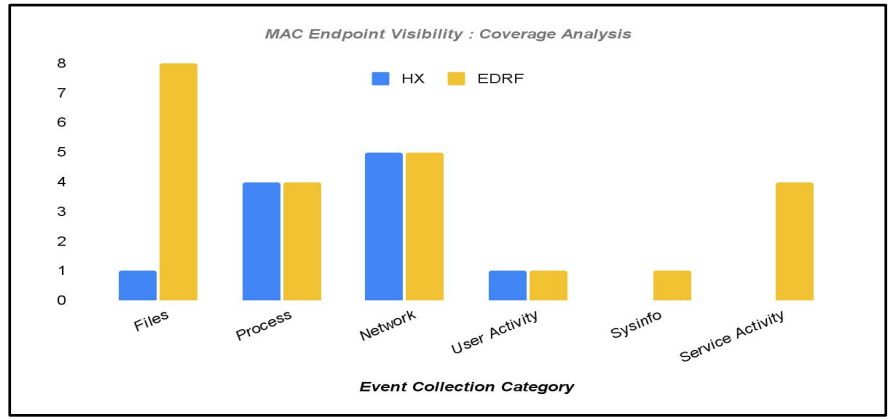
Feature	HX Feature	Value
Threat Prevention	**Malware Protection**	Prevents threats from accessing systems, scans files automatically when they are accessed, and runs targeted scans for malware on client systems.
Endpoint Firewall	**Unsupported**	Monitors communication between the computer and resources on the network and the Internet. Intercepts suspicious communications.
Web Control	**Unsupported**	Monitors web searching and browsing activity on client systems and blocks websites and downloads based on safety rating and content.
Adaptive Threat Protection	**Exploit Guard and Malware Guard**	Detect unknown threats through malicious behavior on and during execution by applying reputation, rules, and machine learning to process behaviors. Proactively protects and restores system through application containment.
Device Control	**Device Guard**	Provides protection for USB drives, smartphones, Bluetooth devices, and other removable media. Control removable device data transfer and execution.
Application Control	**Unsupported***	Application Control protects your organization against malware attacks before they occur by proactively controlling the applications that run on your devices
Exploit Prevention	**Exploit Guard**	Threat Prevention protects against exploits such as Buffer Overflow Protection and Illegal API Use. Customize detections and preventions with Expert Rules.
Network Intrusion Prevention	**Unsupported**	Protect against network denial-of-service attacks and bandwidth-oriented attacks that deny or degrade network traffic.
Access Protection	**Unsupported***	Protect against unwanted changes to client systems by restricting access to specified files, shares, registry keys, registry values, and preventing or restricting processes and services from executing threat behavior.

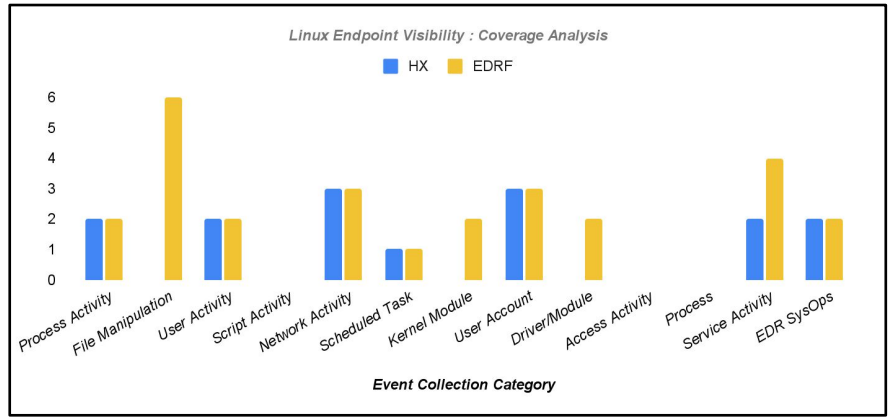
Trellix

Endpoint Event Visibility

EDRF vs HX event collection







Trellix

Event Visibility with EDRF - Windows

Telemetry Feature Category	Event
Process Activity	Process Creation
	Process Refreshed
	Process Forked
	Process Reputation changed
	Process Termination/Deleted
	Process Access
	Image/Library Loaded
	Remote Thread Creation/Injection
	Process Tampering Activity
File Manipulation (Executable & Non-Executable)	**File Created**
	File Attribute Changed
	File Modified
	File Deleted
	File Moved
	File Executed
	File Read/Write
	File Reputation Changed
User Account Activity	User Login
	User Logout
	Account Changed
	Password Changed
	Password Reset
	Account Disabled
	Account Deleted
	Account Enabled
	Account Locked
	Account Unlocked
	ACL on Admin Group
	Username Changed
	Admin Pass Restored
	Successful RDP Logon
	Credential Backup
	Credential Restored

Telemetry Feature Category	Event
Network Activity	TCP Connection Open /Close
	UDP Connection Open
	Port Open /Close
	HTTP/S/URL
	DNS Lookup
	File Downloaded
	IP Address Change Notification
Hash Algorithms	MD5
	SHA
Registry Activity	Key/Value Creation
	Key/Value Replaced
	Key/Value Restored
	Key/Value Queried
	Key/Value Enumerated
	Key/Value Modification
	Key/Value Read
	Key/Value Deletion
Schedule Task Activity	Scheduled Task Creation
	Scheduled Task Execution
	Scheduled Task Modification
	Scheduled Task Deletion
Service Activity	Service Creation
	Service Started
	Service Modification
	Service Deletion

Telemetry Feature Category	Event
Driver/Module Activity	**Driver Loaded**
	Loaded DLLs/Images
	Driver Modification
	Driver Unloaded
Device Operations	**Virtual Disk Mount**
	USB Device Unmount
	USB Device Mount
Other Relevant Events	Group Policy Modification
Named Pipe Activity	**Pipe Creation**
	Pipe Connection
EDR SysOps	Agent Start
	Agent Stop
	Agent Install
	Agent Uninstall
	Agent Keep-Alive
	Agent Errors
WMI Activity	**WmiEventConsumerToFilter**
	WmiEventConsumer
	WmiEventFilter
BIT JOBS Activity	**BIT JOBS Activity**
PowerShell Activity	Script-Block Activity
APIs	**COM API**
	Write to Memory
	Code Injection

BOLD is not available in

Event Visibility with EDRF - Linux

Telemetry Feature Category	Event
Process Activity	Process Creation
	Process Termination
File Manipulation	**File Creation**
	File Modification
	File Moved
	File Symbolic Link
	File Deletion
	File Read
User Activity	Logon Success
	Logon Failed
Network Activity	Network Connection Outbound
	Network Connection Inbound
	Additional L7 Information
Scheduled Task Activity	Scheduled Task
Kernel Module Events	Loaded
	Unloaded
User Account Activity	User Account Created
	User Account Modified
	User Account Deleted
	SSH Logon (Success/Failure)
Driver/Module Activity	Kernel Module Load
	Kernel Module Unload
Service Activity	Service Start
	Service Modification
	Service Restart
	Service Stop
EDR SysOps	Agent Start
	Agent Stop

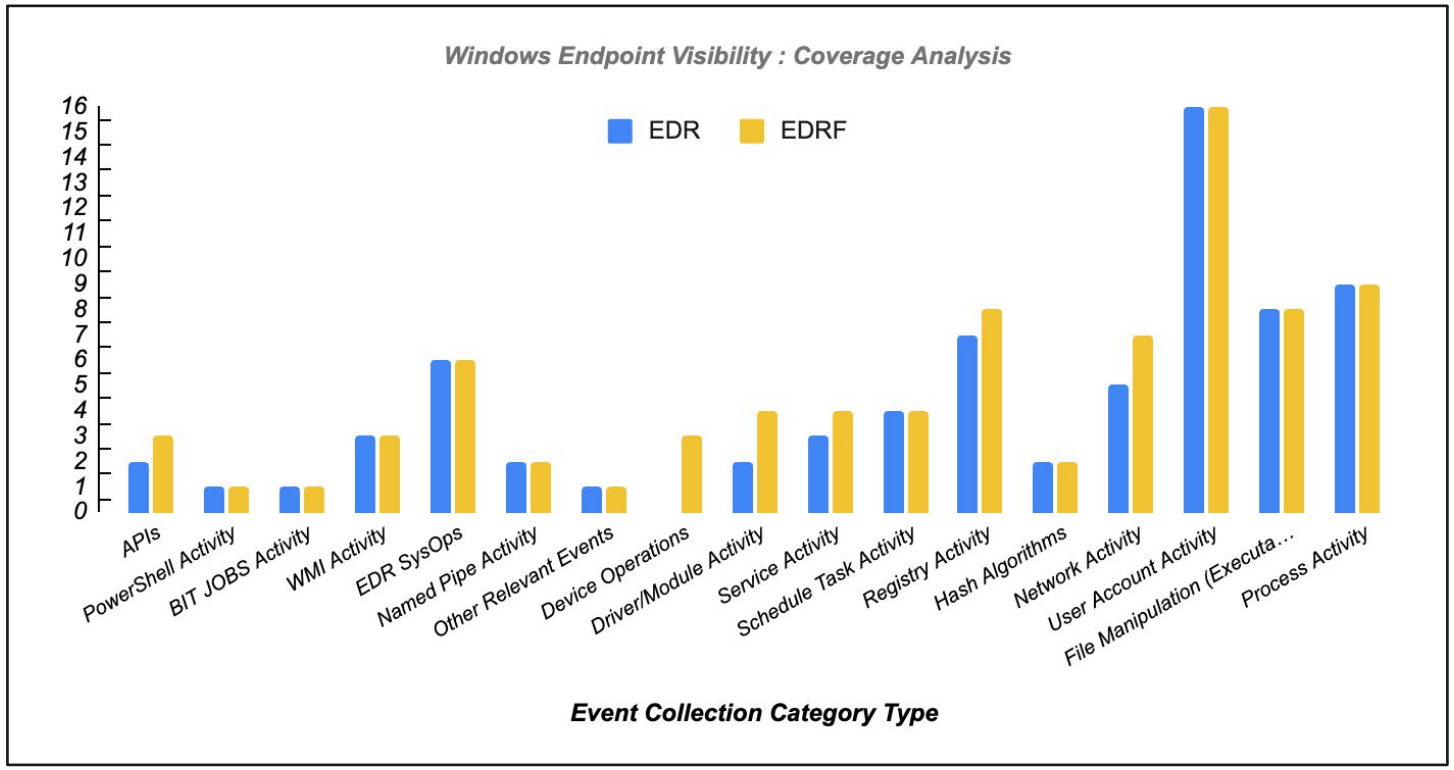
Event Visibility with EDRF - Mac

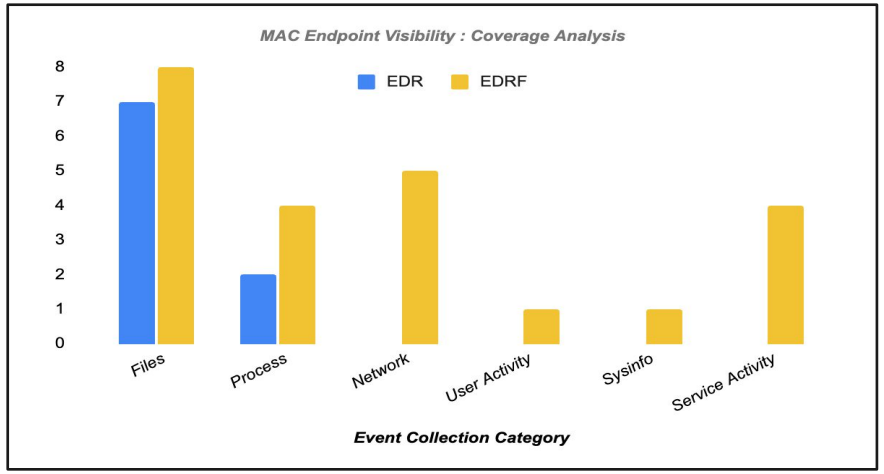
Telemetry Feature Category	Event
Files	**Create**
	Read
	Write
	Hardlinked
	Delete
	Rename
	Move
	Modified
Process	Created
	Image / Library loaded
	Fork/Exec
	Stop
Network	Accept
	Connect
	DNS Lookup
	IP Address Change Notification
	Network access
User Activity	SSH & Apple Remote Desktop
Sysinfo	
Service Activity	**Service Start**
	Service Modification
	Service Restart
	Service Stop

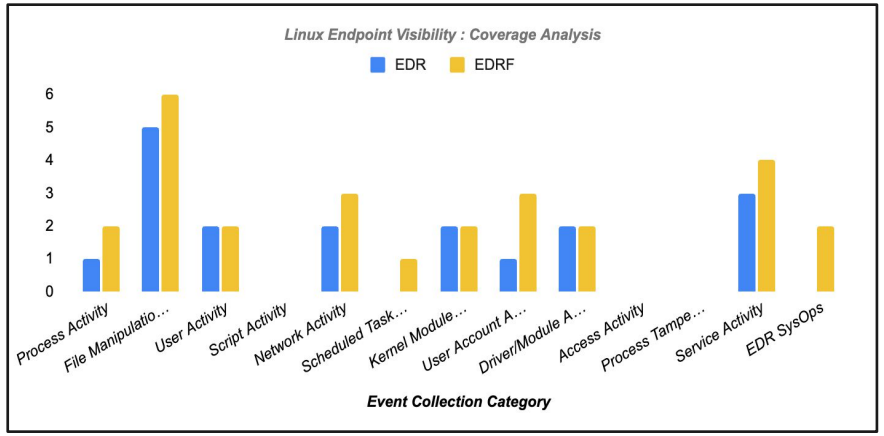
BOLD is not available in

Endpoint Event Visibility

EDRF vs EDR event collection





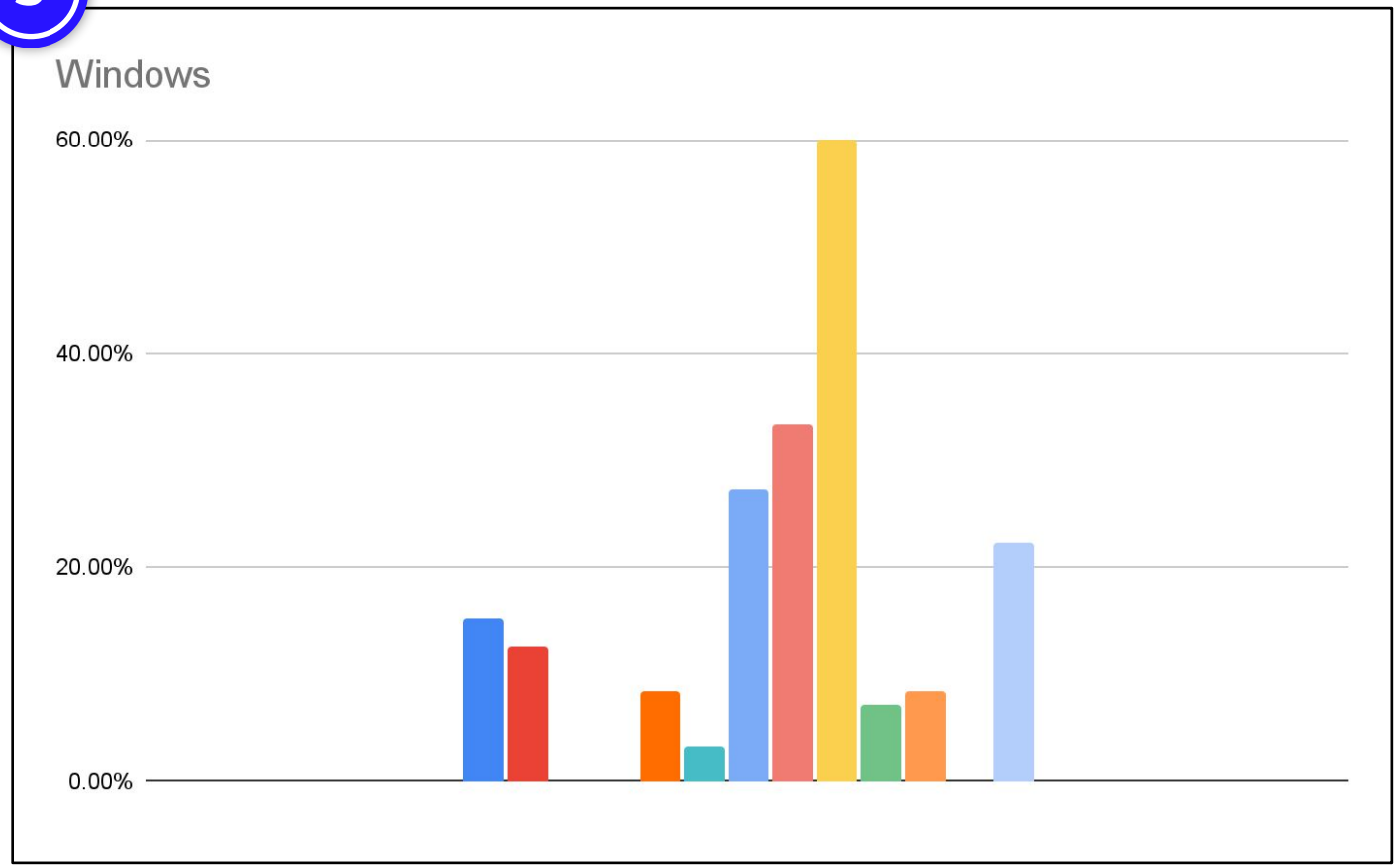


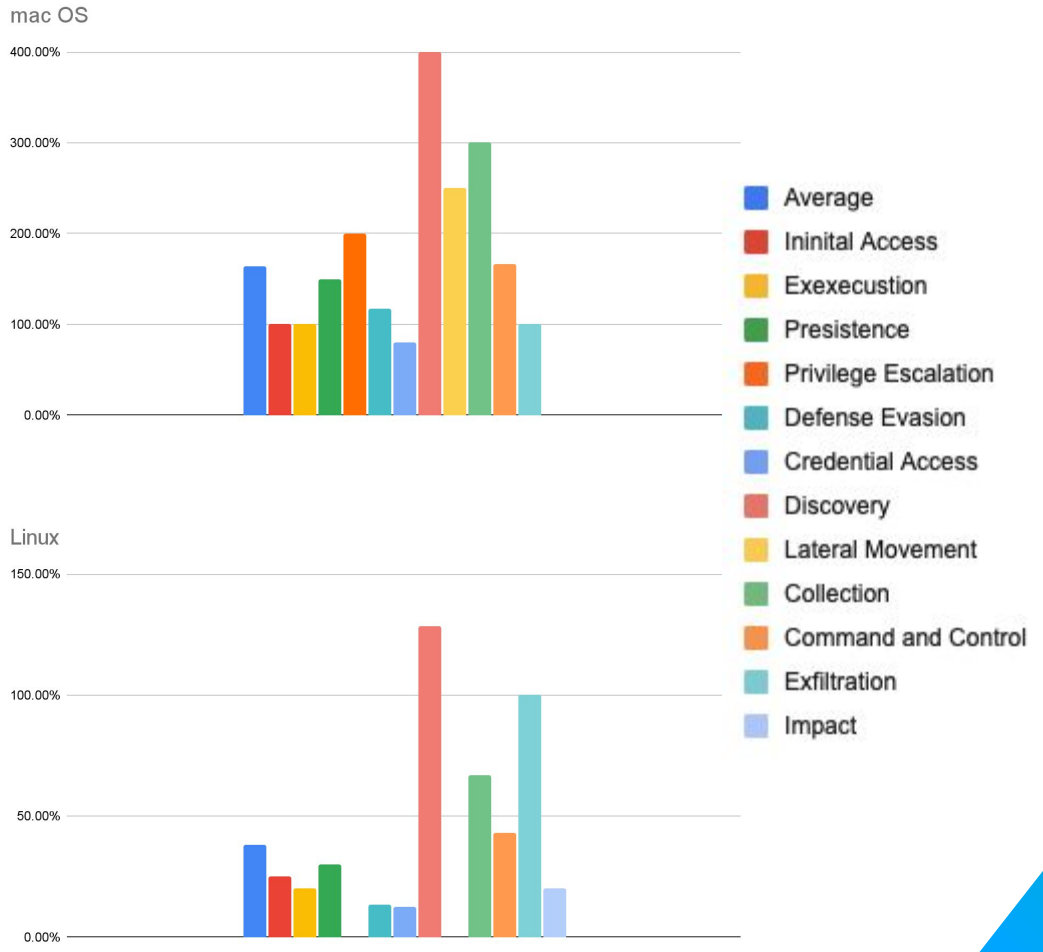
Trellix

Detection Coverage

EDRF vs HX MITRE ATTACK Framework detections

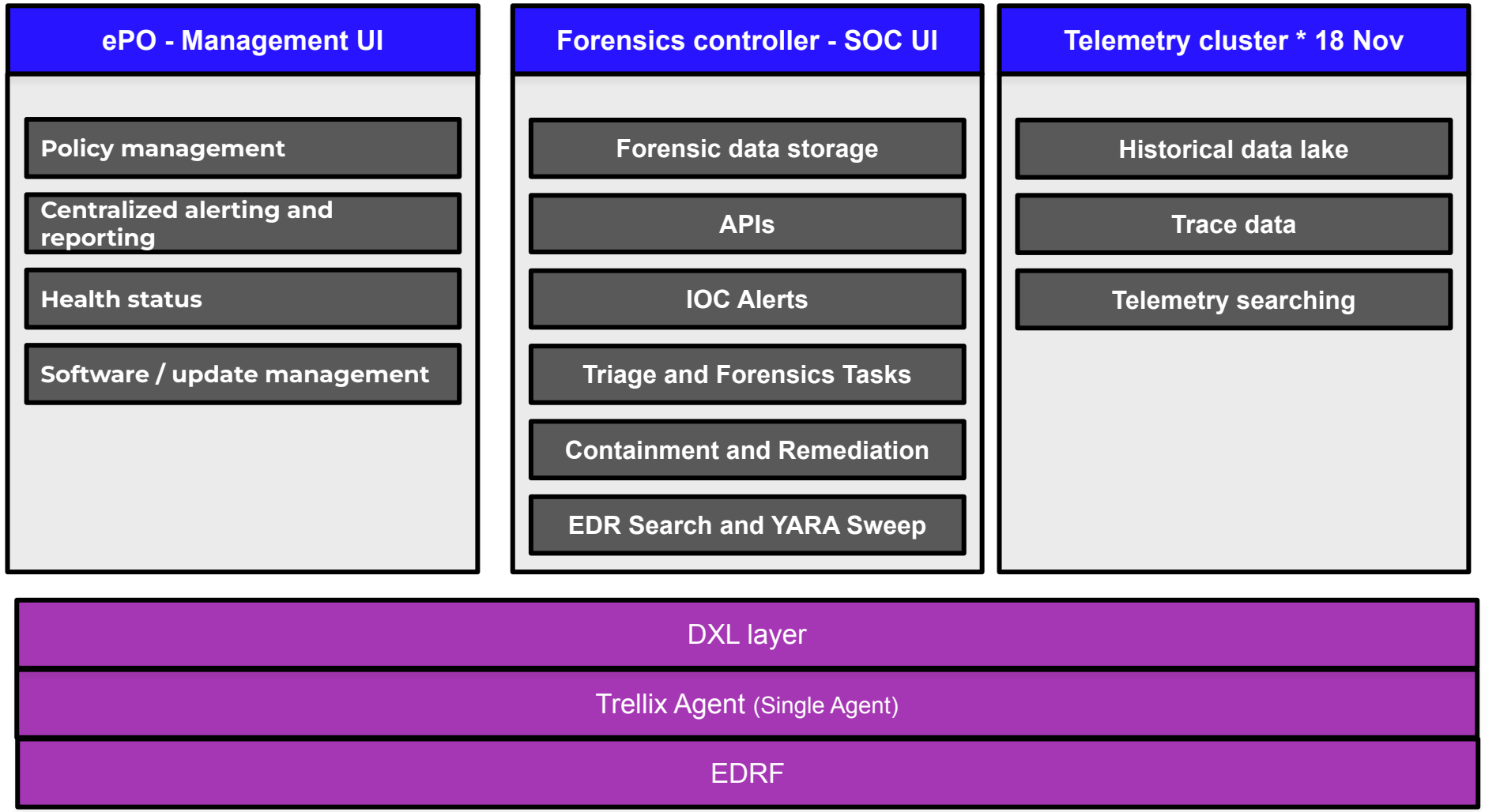
3





Trellix

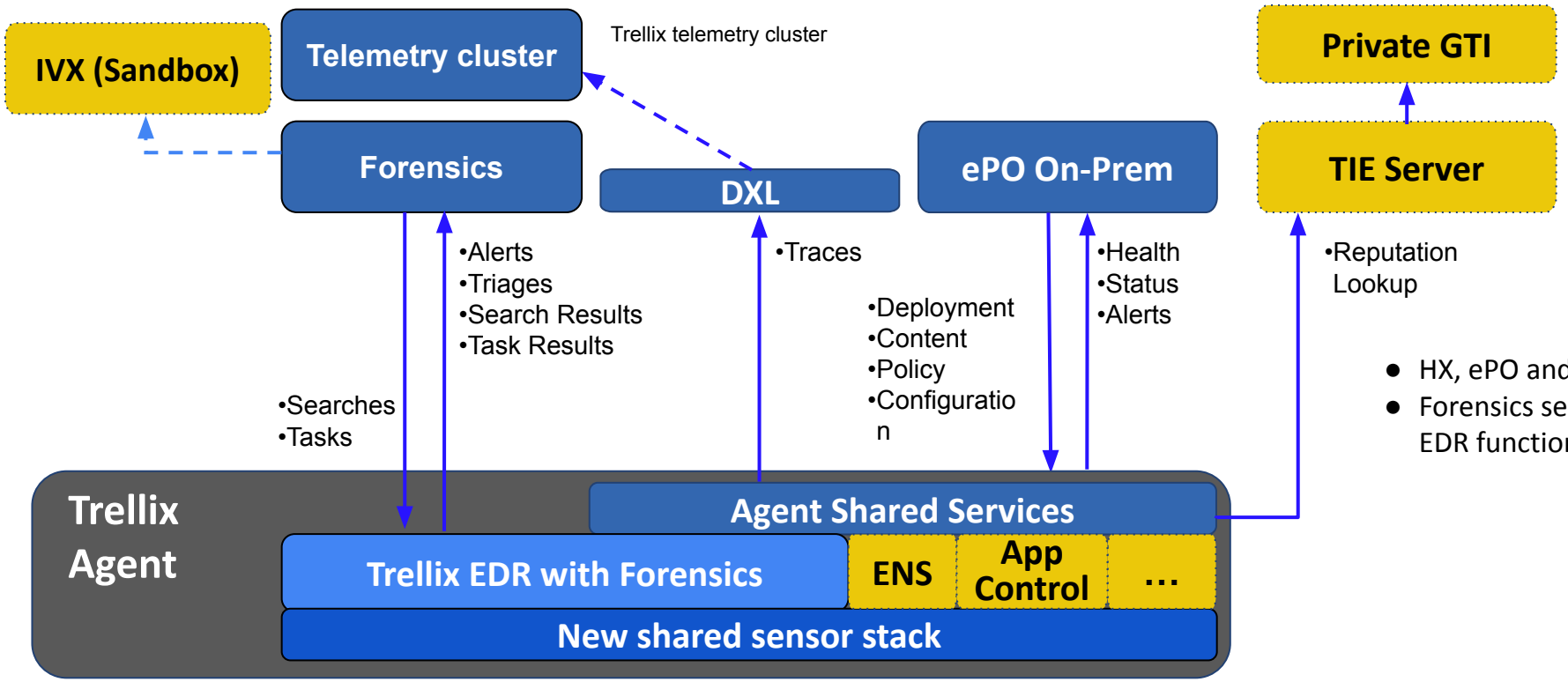
Trellix EDRF as of today * 18 Nov



Trellix

Hybrid and On-Prem Deployments

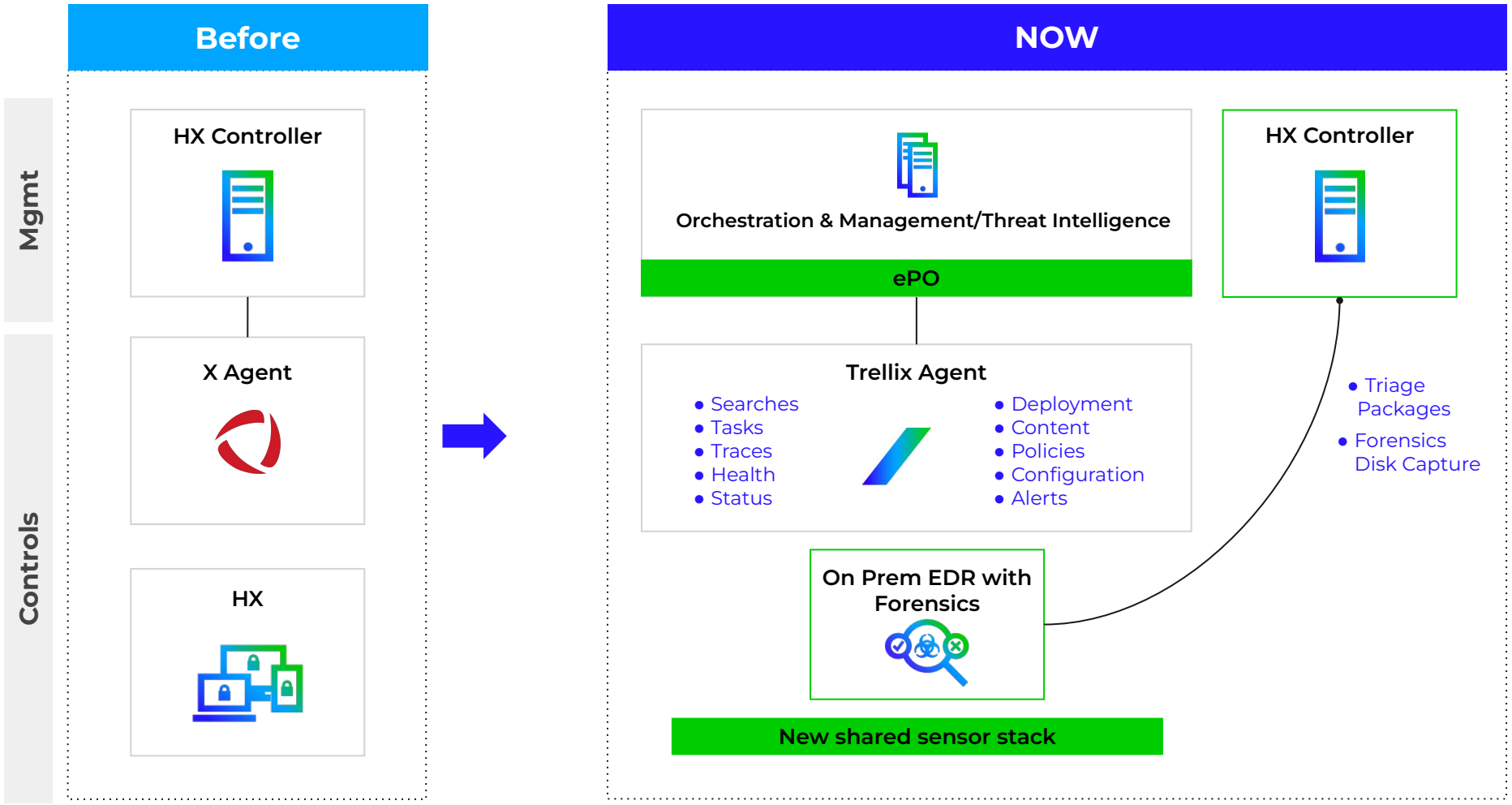
Trellix ENS and EDR w/ Forensics with On-Premise ePO and “HX”



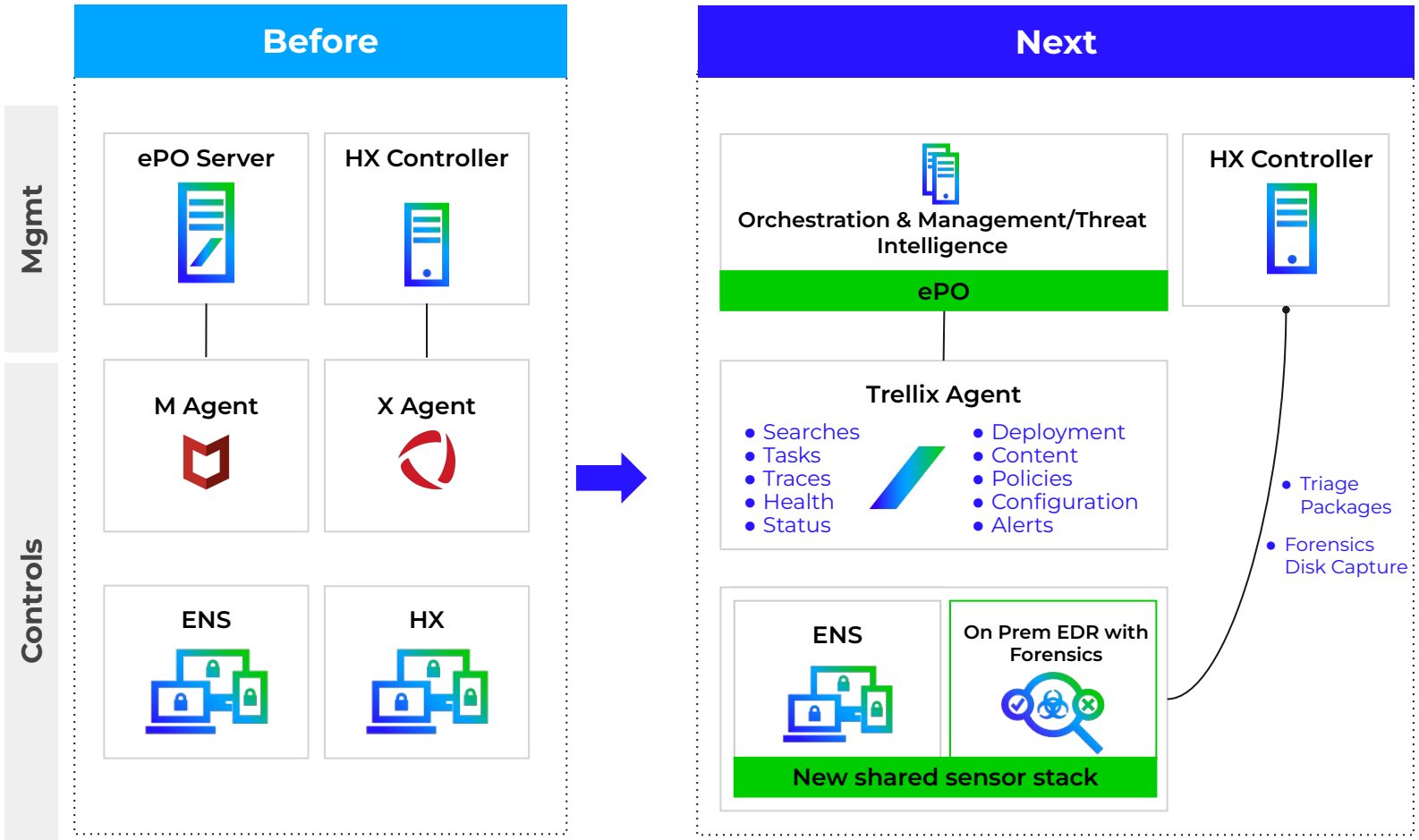
- HX, ePO and TIE are onprem or IaaS
- Forensics server delivers on-premise EDR functionality

Trellix

HX - On Prem Managed

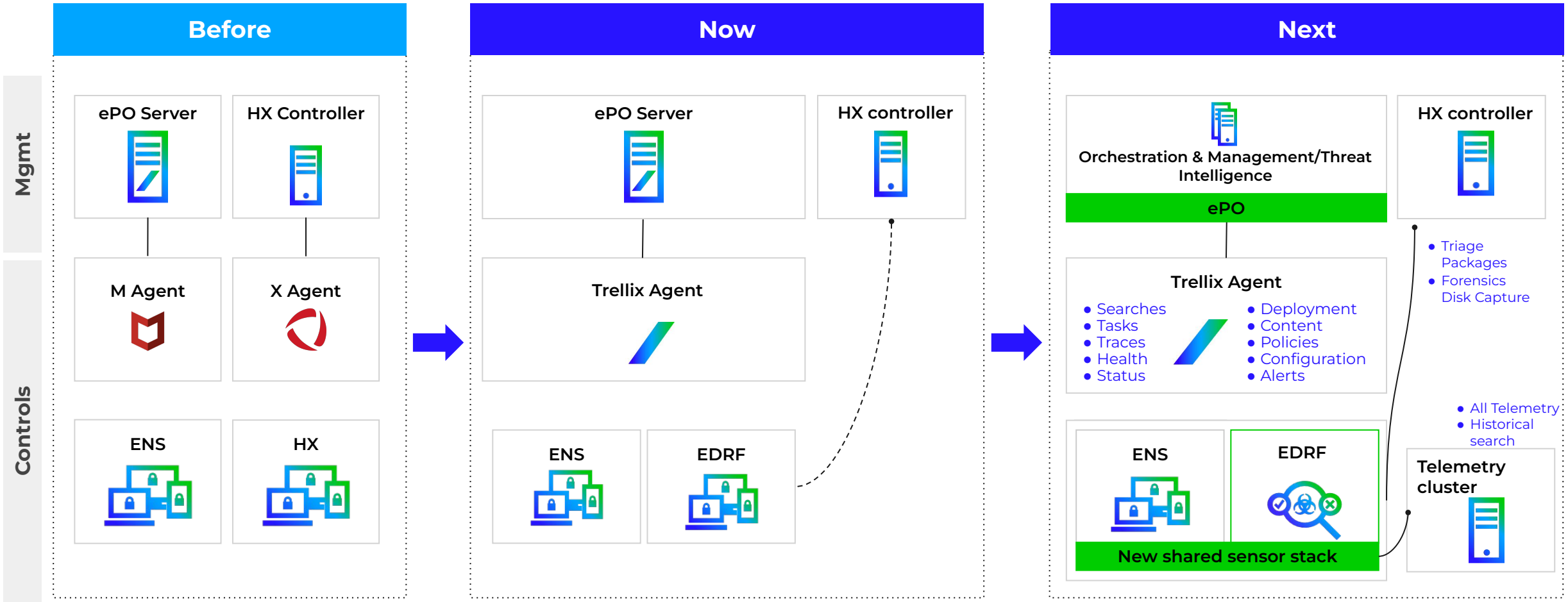


ENS and HX - On Prem Managed



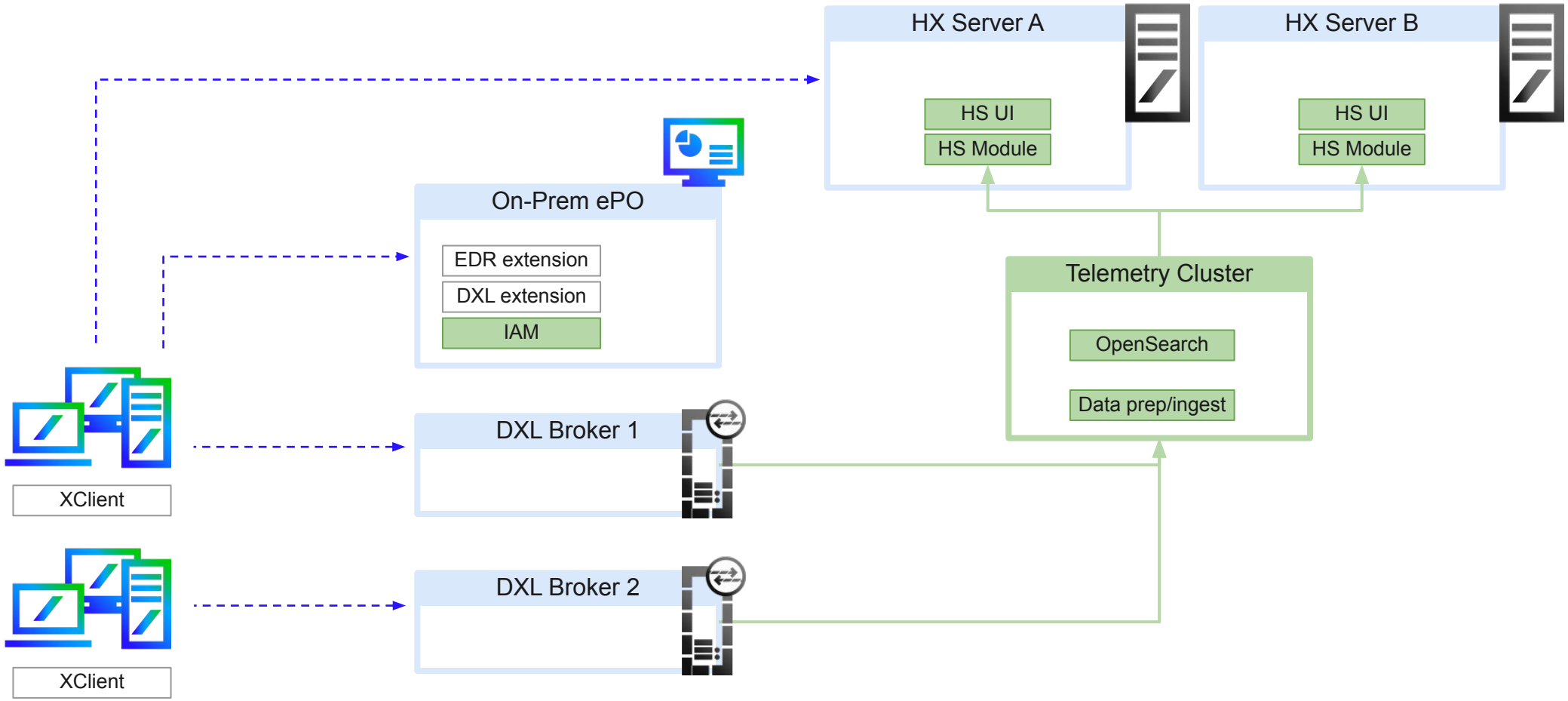
Trellix

ENS and EDRF - On Prem Managed – Intended for 18 Nov 2025



Trellix

EDRF On-Prem Architecture: Historical Search



Green is new

Trellix

HX Agent Events by Operating System

Event Type	Windows	Mac OS X	Linux
File write events	✔	✔	
IPv4 network events	✔	✔	✔
DNS lookup events	✔	✔	
URL events	✔		
Image load events	✔	✔	
Process life cycle events	✔	✔	✔
Registry key events	✔		
IP address change events	✔	✔	

Event Visibility with EDRF - Windows

Telemetry Feature Category	Event
Process Activity	Process Creation
	Process Refreshed
	Process Forked
	Process Reputation changed
	Process Termination/Deleted
	Process Access
	Image/Library Loaded
	Remote Thread Creation/Injection
	Process Tampering Activity
File Manipulation (Executable & Non-Executable)	**File Created**
	File Attribute Changed
	File Modified
	File Deleted
	File Moved
	File Executed
	File Read/Write
	File Reputation Changed
User Account Activity	User Login
	User Logout
	Account Changed
	Password Changed
	Password Reset
	Account Disabled
	Account Deleted
	Account Enabled
	Account Locked
	Account Unlocked
	ACL on Admin Group
	Username Changed
	Admin Pass Restored
	Successful RDP Logon
	Credential Backup
	Credential Restored

Telemetry Feature Category	Event
Network Activity	TCP Connection Open /Close
	UDP Connection Open
	Port Open /Close
	HTTP/S/URL
	DNS Lookup
	File Downloaded
	IP Address Change Notification
Hash Algorithms	MD5
	SHA
Registry Activity	Key/Value Creation
	Key/Value Replaced
	Key/Value Restored
	Key/Value Queried
	Key/Value Enumerated
	Key/Value Modification
	Key/Value Read
	Key/Value Deletion
Schedule Task Activity	Scheduled Task Creation
	Scheduled Task Execution
	Scheduled Task Modification
	Scheduled Task Deletion
Service Activity	Service Creation
	Service Started
	Service Modification
	Service Deletion

Telemetry Feature Category	Event
Driver/Module Activity	**Driver Loaded**
	Loaded DLLs/Images
	Driver Modification
	Driver Unloaded
Device Operations	**Virtual Disk Mount**
	USB Device Unmount
	USB Device Mount
Other Relevant Events	Group Policy Modification
Named Pipe Activity	**Pipe Creation**
	Pipe Connection
EDR SysOps	Agent Start
	Agent Stop
	Agent Install
	Agent Uninstall
	Agent Keep-Alive
	Agent Errors
WMI Activity	**WmiEventConsumerToFilter**
	WmiEventConsumer
	WmiEventFilter
BIT JOBS Activity	**BIT JOBS Activity**
PowerShell Activity	Script-Block Activity
APIs	**COM API**
	Write to Memory
	Code Injection

Trellix

BOLD is not available in HX

Event Visibility with EDRF - Linux

Telemetry Feature Category	Event
Process Activity	Process Creation
	Process Termination
File Manipulation	**File Creation**
	File Modification
	File Moved
	File Symbolic Link
	File Deletion
	File Read
User Activity	Logon Success
	Logon Failed
Network Activity	Network Connection Outbound
	Network Connection Inbound
	Additional L7 Information
Scheduled Task Activity	Scheduled Task
Kernel Module Events	Loaded
	Unloaded
User Account Activity	User Account Created
	User Account Modified
	User Account Deleted
	SSH Logon (Success/Failure)
Driver/Module Activity	Kernel Module Load
	Kernel Module Unload
Service Activity	Service Start
	Service Modification
	Service Restart
	Service Stop
EDR SysOps	Agent Start
	Agent Stop

Event Visibility with EDRF - Mac

Telemetry Feature Category	Event
Files	**Create**
	Read
	Write
	Hardlinked
	Delete
	Rename
	Move
	Modified
Process	Created
	Image / Library loaded
	Fork/Exec
	Stop
Network	Accept
	Connect
	DNS Lookup
	IP Address Change Notification
	Network access
User Activity	SSH & Apple Remote Desktop
Sysinfo	
Service Activity	**Service Start**
	Service Modification
	Service Restart
	Service Stop

BOLD is not available in HX

Trellix

On-prem historical Search - compare

On-prem capabilities today compare to next generation

Current: HX + XClient or XAgent

- Only available when endpoint is online
- Only a few days of events are available
- Can cause performance issues when hunting for files outside event buffer
- Search Request is distributed to many endpoints
- Have to pull full event buffer for further analyze

Next: HX + XClient + Data Store

- Trace Data / Telemetry pushed every 30 seconds
- Search is available even if the endpoint is offline or wiped out
- No performance impact on endpoints when searching
- Many search can be initiated and analyzed with no endpoint performance impacted
- Retention period is weeks or months based on storage
- More telemetry data points with EDRF/Xclient than HX/Xagent

Trellix

Trellix

Rapid Response with Wise

Trellix EDR with Wise AI

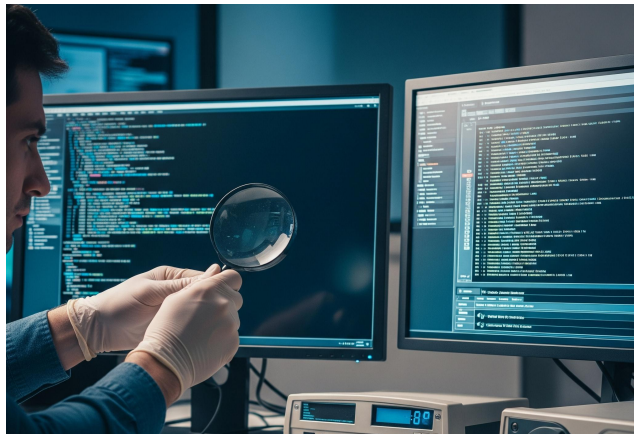
Deep integration with tangible benefits

- **Enable analysts of all skill levels** with *natural language query builder*
- **Increase efficacy and reach** with *multi-lingual threat hunting*
- **Rapidly create executive summaries** of threats and artifacts with *Dossier Mode*
- **Decrease time to resolve** with *Interactive Mode* to drill down into threat and artifact details
- **Rapidly assess** the depth and breadth of an attack with *Knowledge Graph*
- **Reduce time to remediate** with *detailed recommendations for next steps*

Trellix

Boost response w/ Generative AI Assistance

Enable analysts of all skill levels with automated triage analysis and report generation



Rapidly test hypothesis with AI assessment of leads uncovered by analysts

Reduce time to remediate with detailed recommendations for next steps

Trellix Wise reduces time to detect and response w/ Generative AI

Trellix

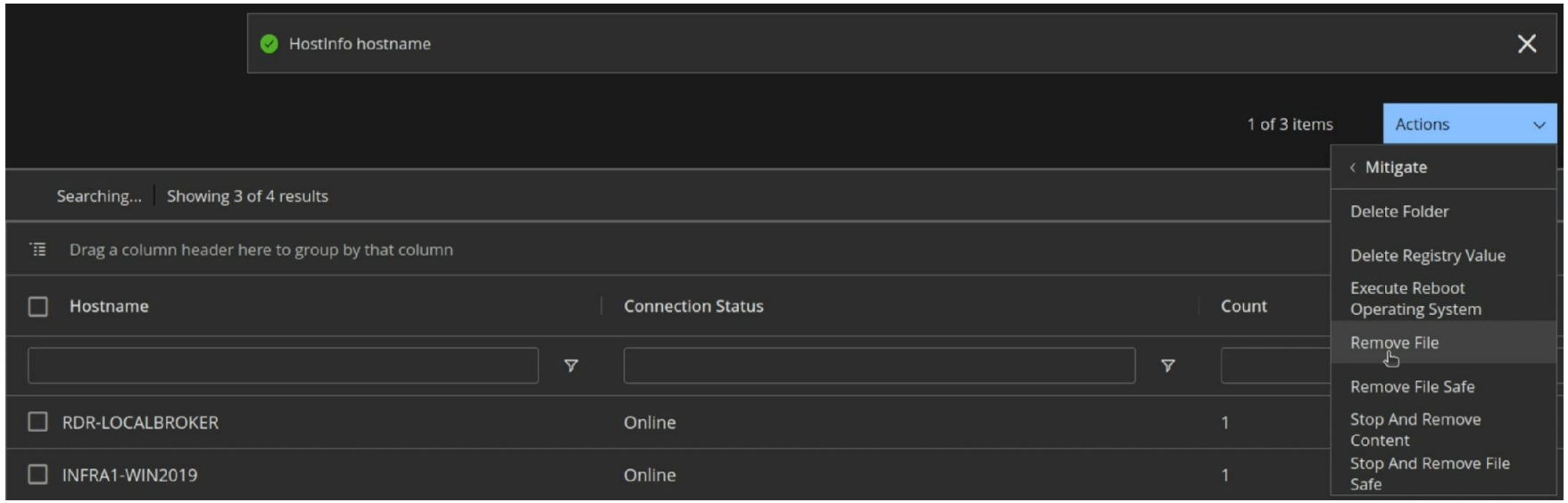
Hunt and Remediate with Natural Language Query

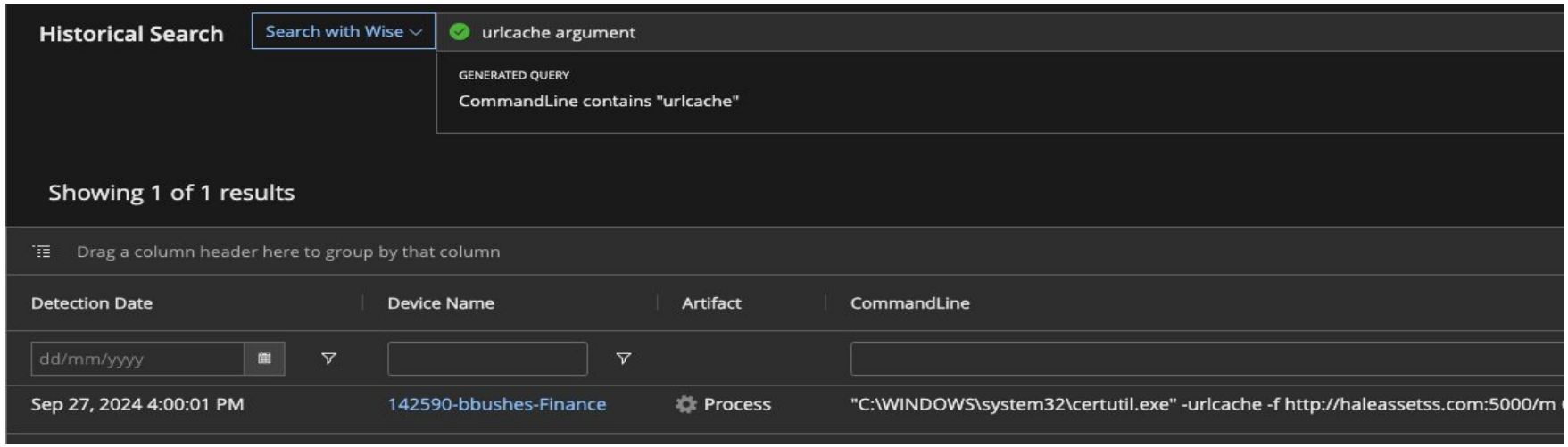
Search and Response

- Search in native language
- Respond w/ Built-in and Custom Actions

Outcome

- Undiscovered Threats revealed with hunt queries
- Threats contained and remediated
- Analysts can communicate w/ tool from Day 1





Trellix

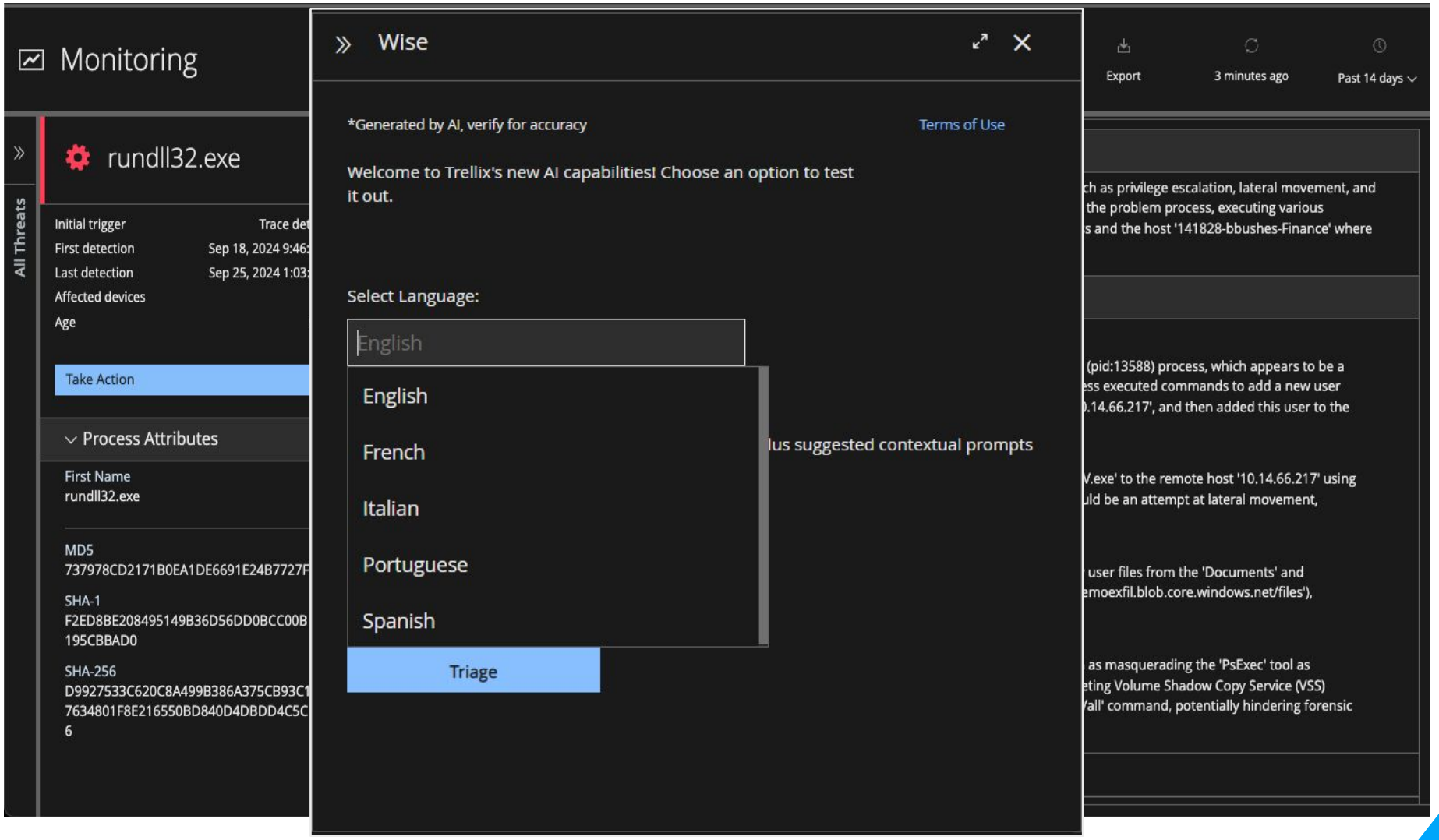
Disrupt Ongoing Attacks Faster with AI

AI-Guided Investigation

- 1-Click Threat analysis & reporting
- Actionable key findings w/ context

Outcome

- Save 8 hours per 100 alerts
- Consistent analysis and reporting
- Guidance to improve analyst skill-sets at all levels



Trellix

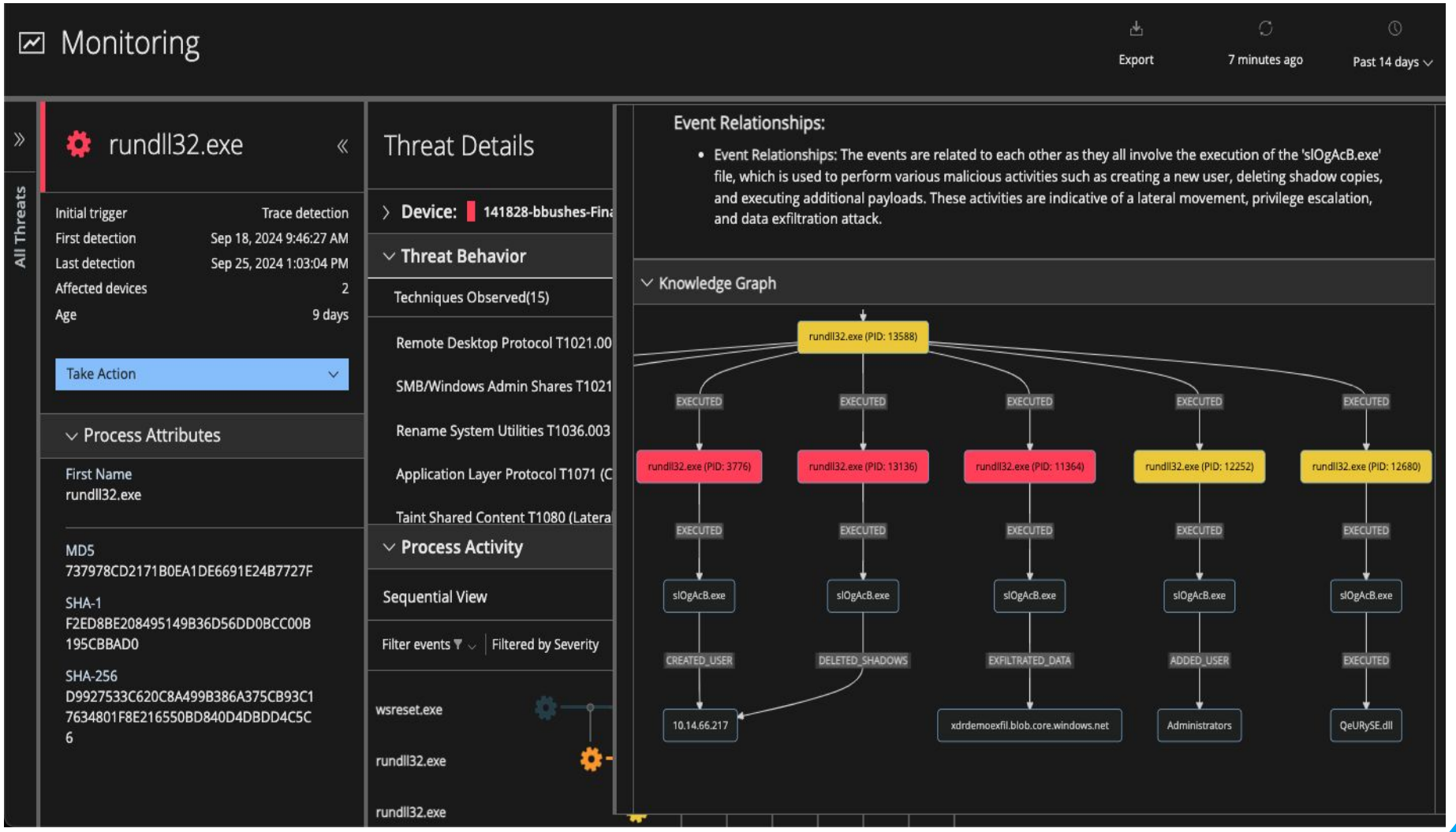
Disrupt Ongoing Attacks Faster with AI

Knowledge graph

- 1-Click Event relationship graph
- Actionable key findings w/ context

Outcome

- Save hours per week by leveraging Wise to summarize and visualize threats on the analysts behalf.



Trellix

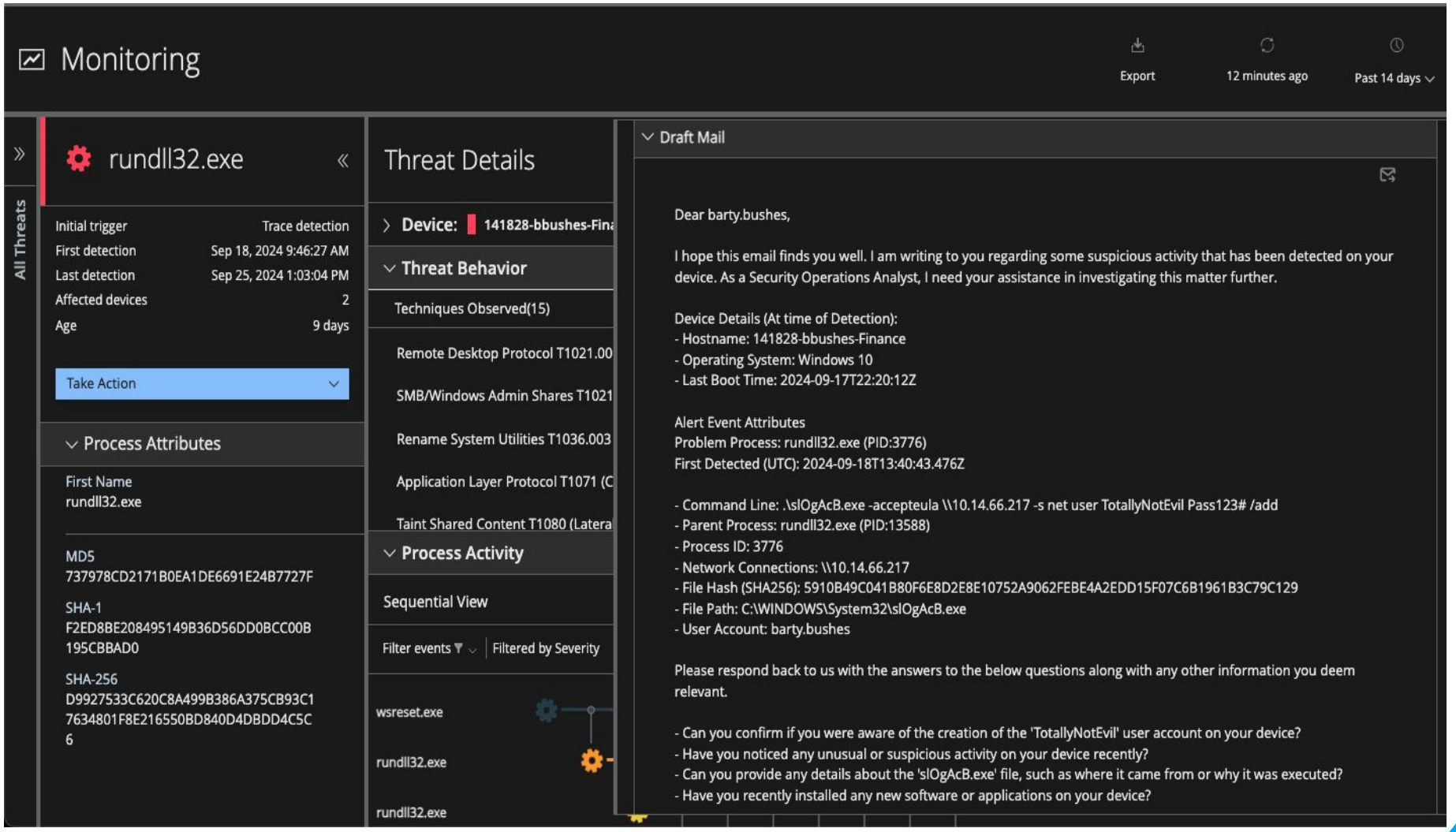
Disrupt Ongoing Attacks Faster with AI

Email Drafting

- 1-Click Threat Draft email
- Time saved on summaries

Outcome

- Save hours per week on common tasks like email summaries
- Accurate and concise email summaries to other stake holders



Trellix

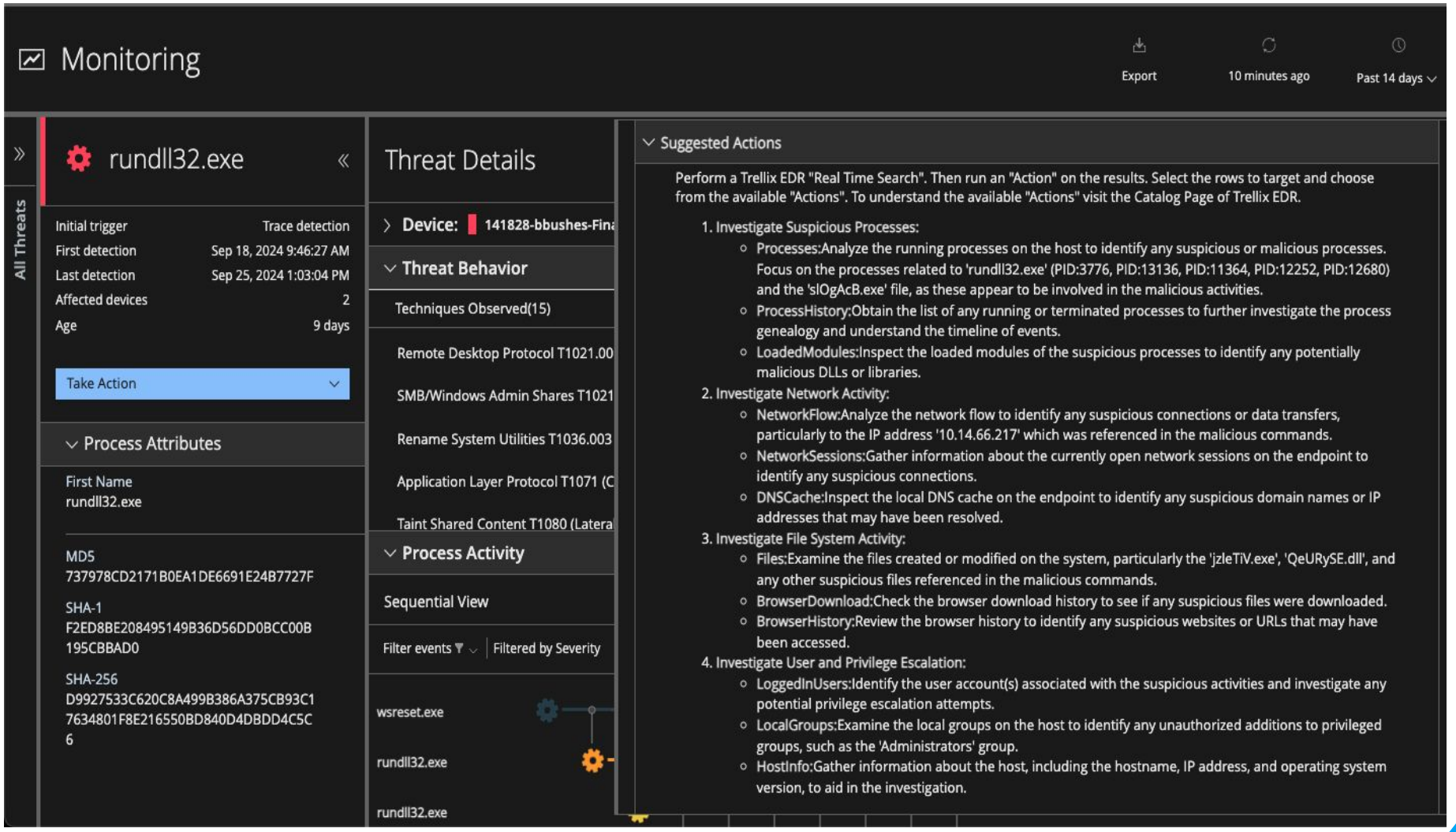
Disrupt Ongoing Attacks Faster with AI

Suggested actions

- 1-Click recommendations on remediation
- Actionable key findings w/ context

Outcome

- Help analysts of all skill levels understand what actions they should be taking to contain and remediate



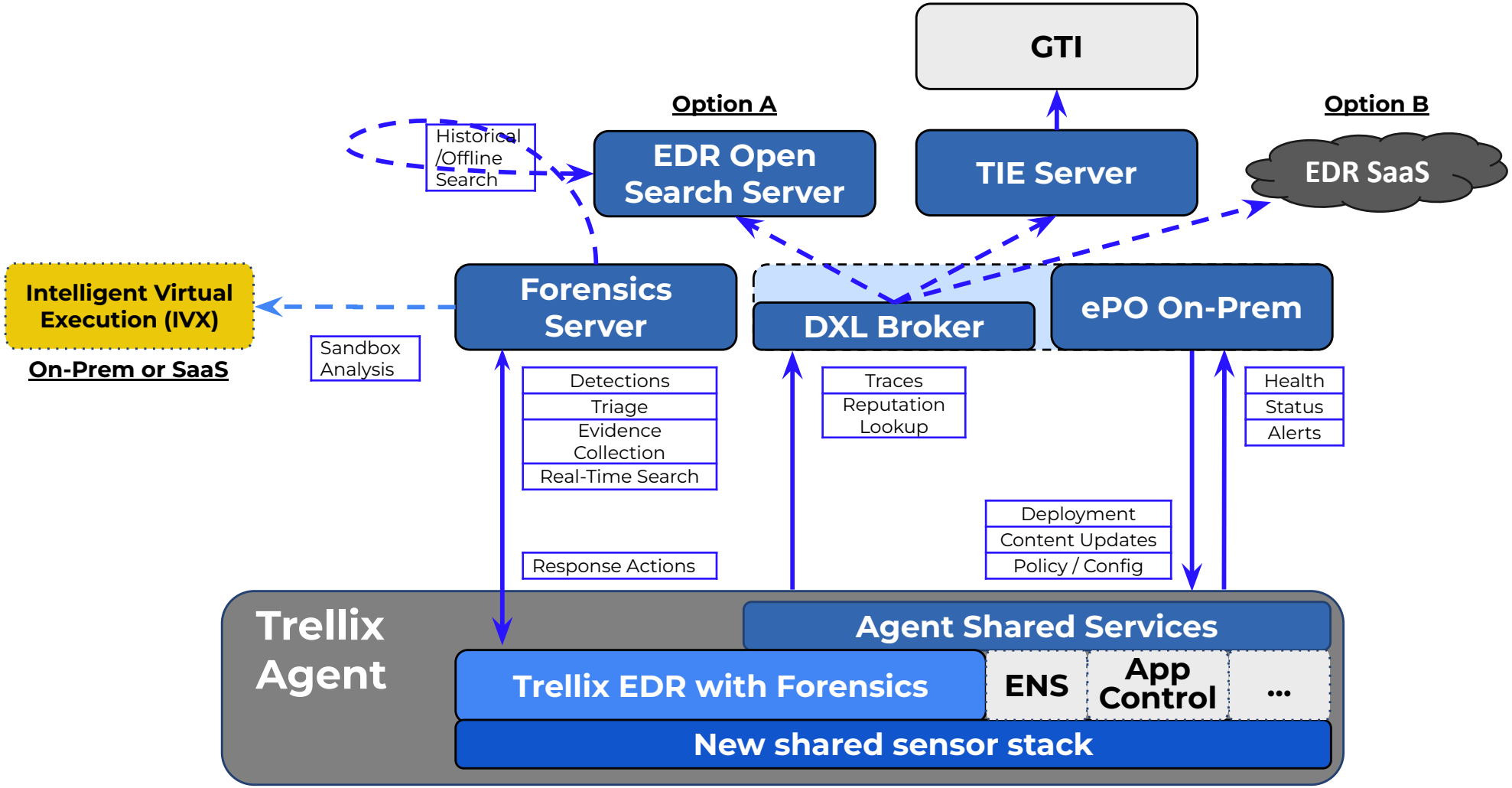
Trellix

Trellix

Endpoint Security Architecture and Integration

Hybrid and On-Prem Deployments

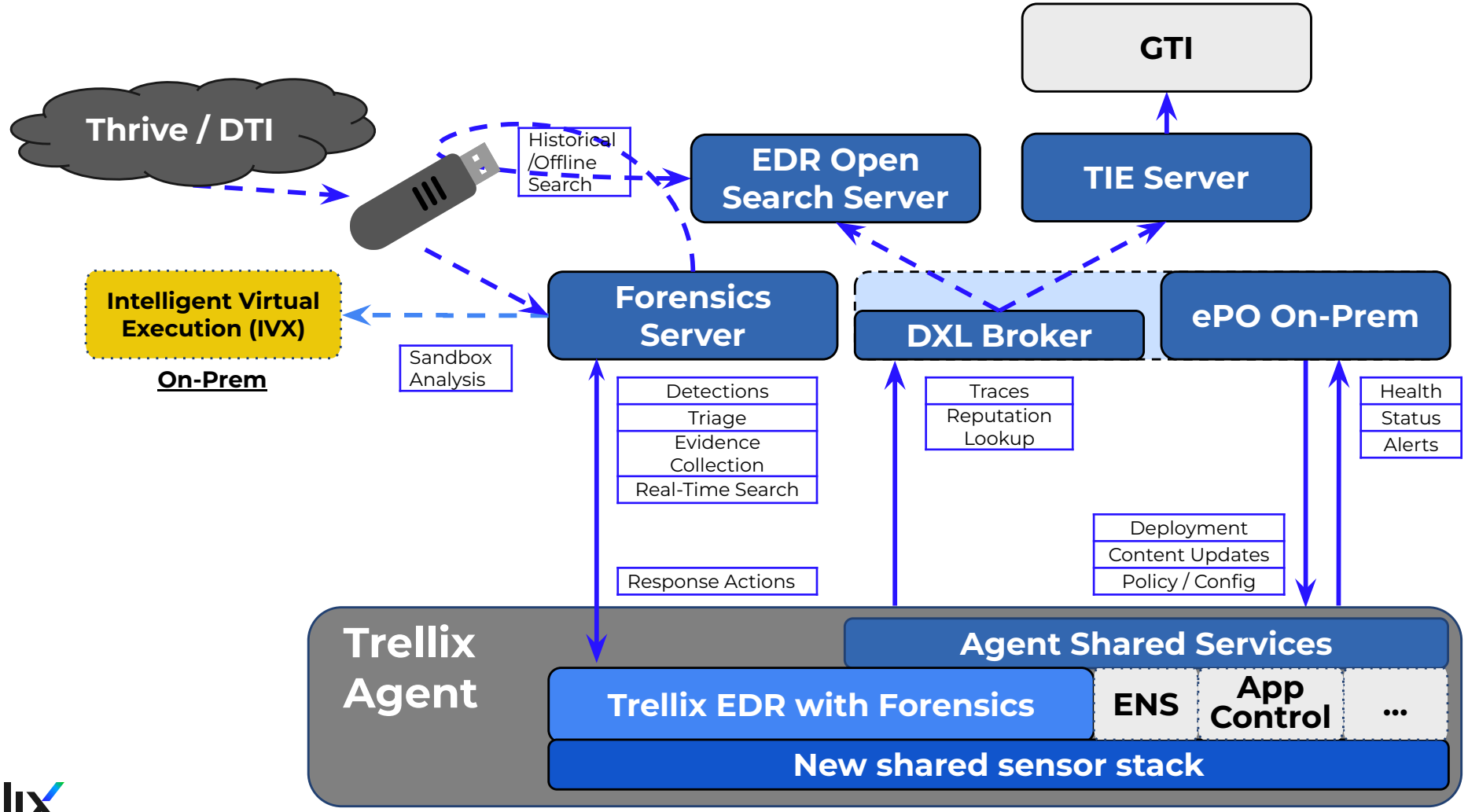
Trellix ENS and EDR w/ Forensics with On-Premise ePO



Trellix

Air-Gapped Deployments

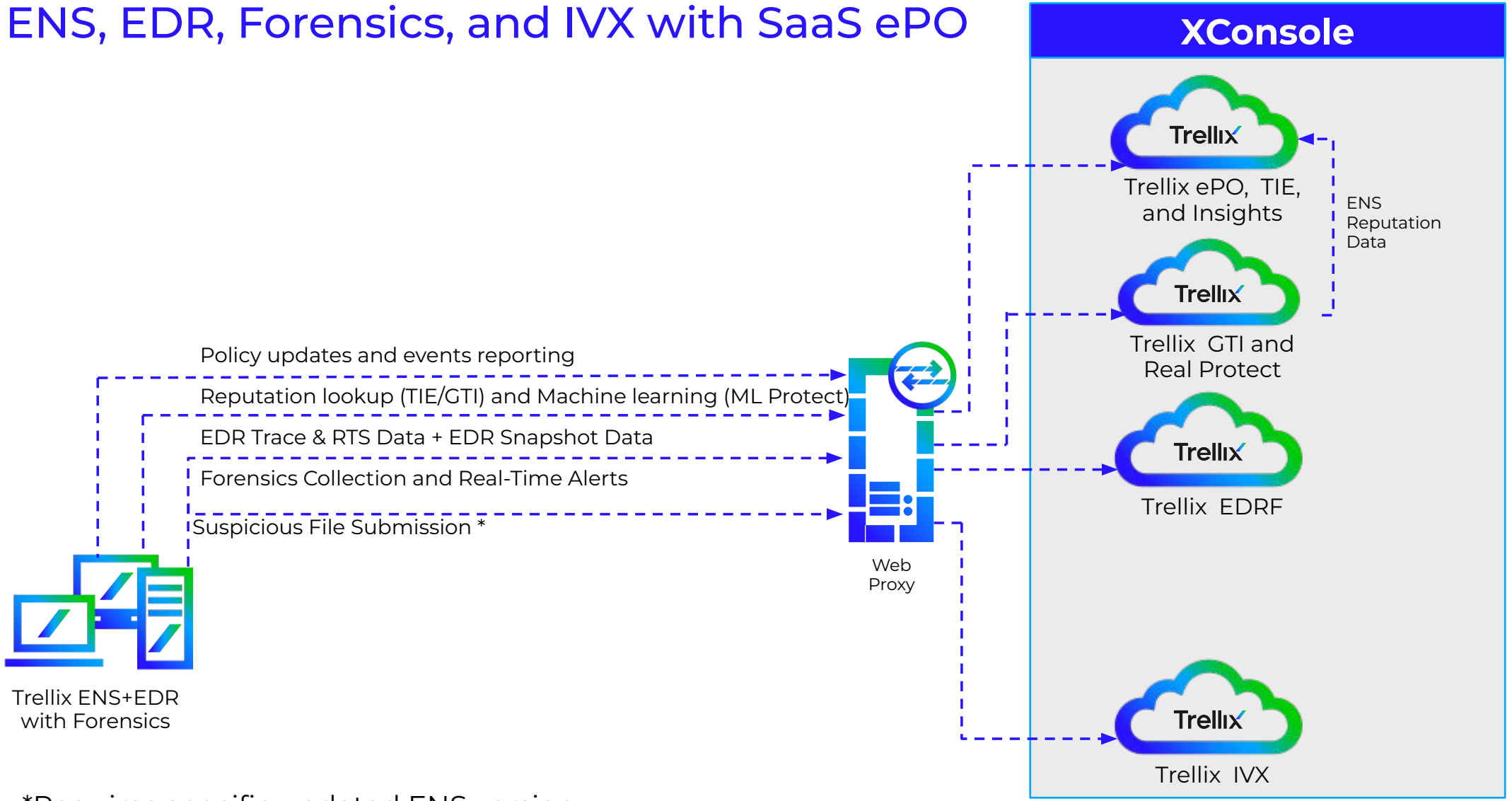
Trellix ENS and EDR w/ Forensics with On-Premise ePO



Trellix

EDRF Cloud

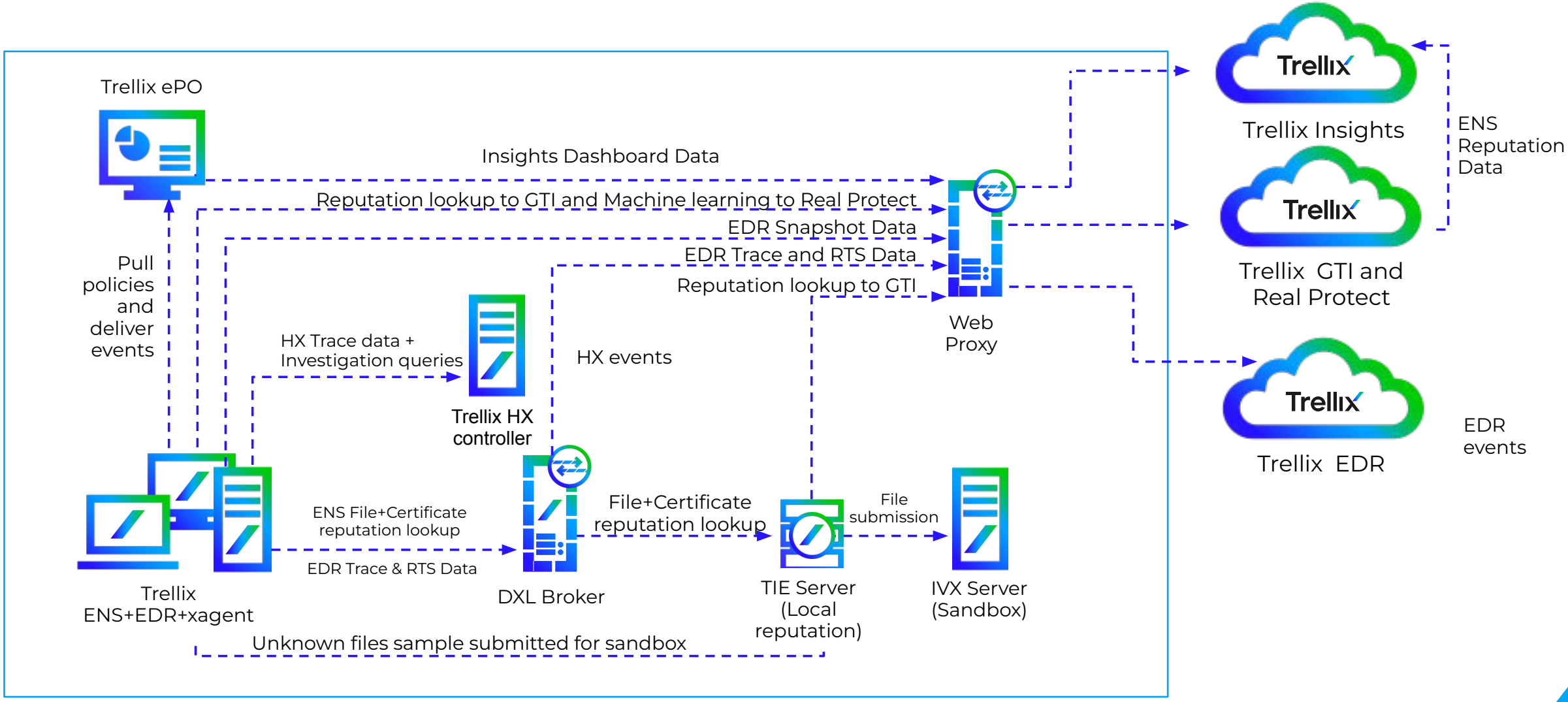
Trellix ENS, EDR, Forensics, and IVX with SaaS ePO



Trellix

*Requires specific updated ENS version

Example Hybrid TRXE Architecture



Trellix

System information reporter (SIR)

Key Use Cases

Systems Information Reporter (SIR)

Collecting Properties from Critical Systems:

The following properties can be collected from critical systems:
Installed software, Processes, Location, Operating system, Hardware configuration, Network configuration, Security configuration, Patch level (Logs file retrieval Next Release)
Once collected, this information can be used to:

- System Information Report
- File search support
- Registry key modification support
- Backup and restore registry keys
- Identify and mitigate security vulnerabilities
- Identify and Improve system performance,
- Troubleshoot problems supports compliance with regulations
- Expired Certs Report

System Information Reporter

Overview

System Information Reporter integrates with ePolicy Orchestrator 5.10 (or later) to provide a flexible, policy-driven method for querying system properties, environment variables, registry key values, and other installed software on your managed nodes.

For example, your managed nodes may have common names or conflicting IP addresses. This complicates the task of managing them from a single server. System Information Reporter tags such nodes and allows you to identify and group them based on the query results such as installed software, services, and registry keys.

System Information Reporter is installed as part of the Trellix Agent install process.

System Information Reporter

Features

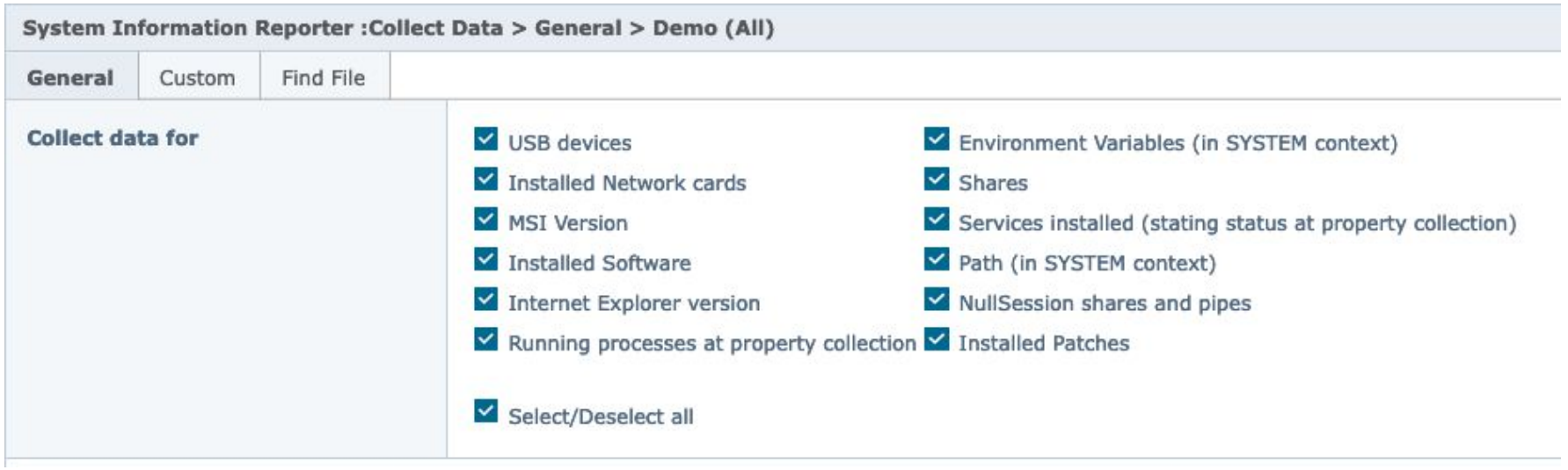
- **Centralized management** — Allows you to enforce System Information Reporter policies on managed nodes using ePolicy Orchestrator management software version 5.10.
- **Query system properties** — Allows you to query the managed nodes to collect:
  - System properties such as versions, patches, and hotfixes
  - Custom environment variable value
  - Registry key values
- **File search support** — Allows you to query the managed nodes to search files.
- **Registry key modification support** — Allows you to query the managed nodes to create, edit, or delete registry keys.
- **Backup and restore registry keys** — Creates a backup of registry keys before modifying and restores registry backup file using Set Registry policy.

System Information Reporter

Collect Data - General

Collect information as system properties:

- Hardware information
- Services
- Software
- Running processes
- Environment variables



Trellix

System Information Reporter

Custom Query & Report

You can build your report based on all values collected by the product as properties.

Trellix

Trellix

Key use cases

Key use cases and demos

1. Cloud UI: Endpoint detection / NEW actions
2. Cloud UI: IOC rule creator
3. Cloud UI: Forensic capabilities / collections
4. Cloud UI: EDR and Trellix WISE
5. On Premise UI: Historical search - on premise
6. System information reporter (SIR)
7. Self service performance metrics (Extended capabilities in development of this feature) - Slides only
8. Trellix in OT - SLIDES ONLY

Trellix

Visibility Across Lifecycle

- Detect, investigate and respond in real time
- High-fidelity alerts and detections
- One-click analysis and reporting with AI-guidance from Wise for EDR
- Enriched with Insights Threat Intelligence

Trellix

Endpoint Detection and Response

1. Collect Data

- Always-on, flexible retention
- Broad visibility
- Cloud-centric

2. Surface Threats

- Suspicious behavior
- File-based and fileless
- MITRE ATT&CK mapping

3. investigation

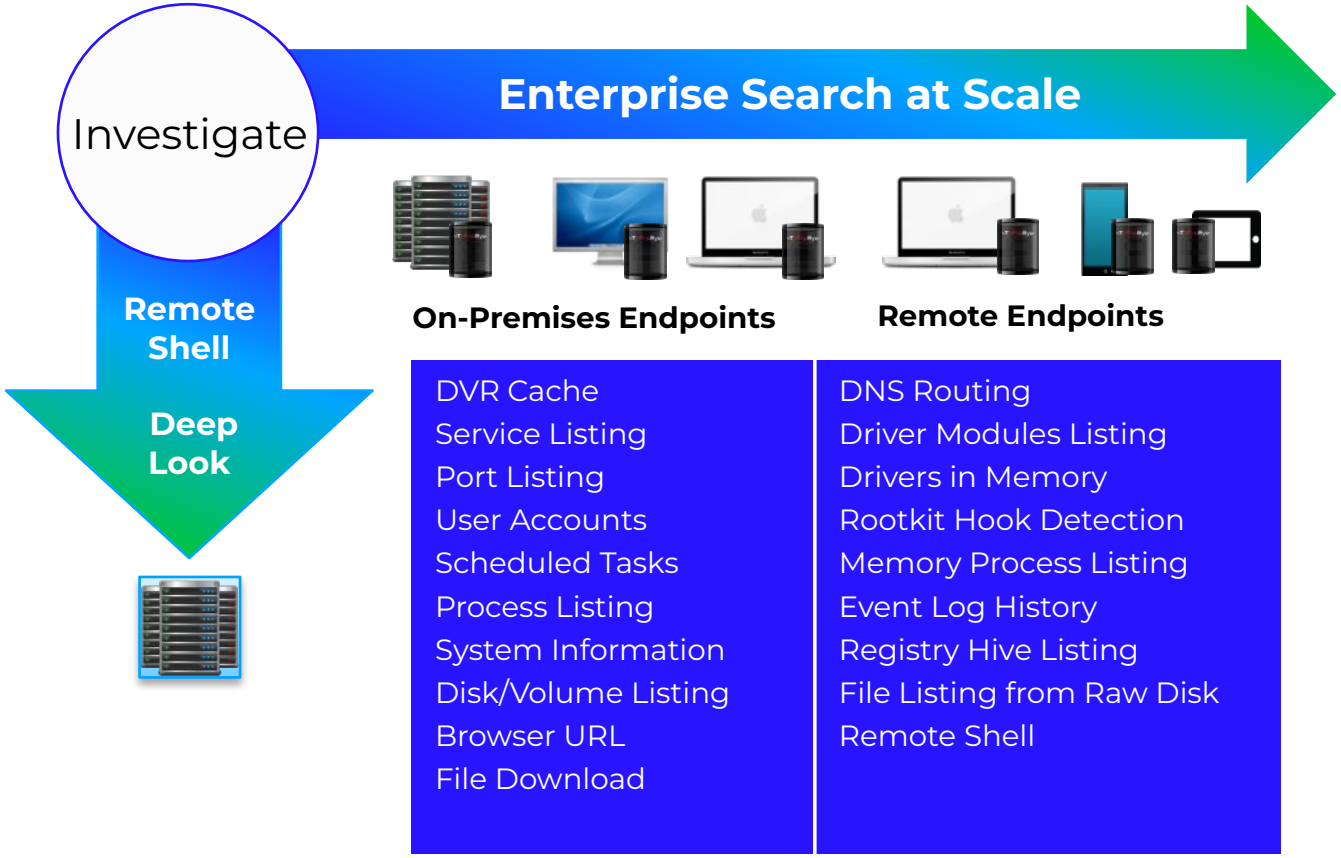
- AI/ML-driven
- Automation
- Correlation at enterprise scale
- Forensic data captures

4. Respond

- Search & visualize
- Robust & effective actions
- API integration

Use Case: Uncover key evidence for resolution

EDR with Forensics prevents recurrent attacks



Recurring Attacks

43%

Organizations hit by ransomware were hit more than once

Endpoint Forensics Outcomes:

- Automated forensics data acquisition
- Visibility into scope and root cause
- Root out evasive attackers
- Prevent recurring attacks

Trellix

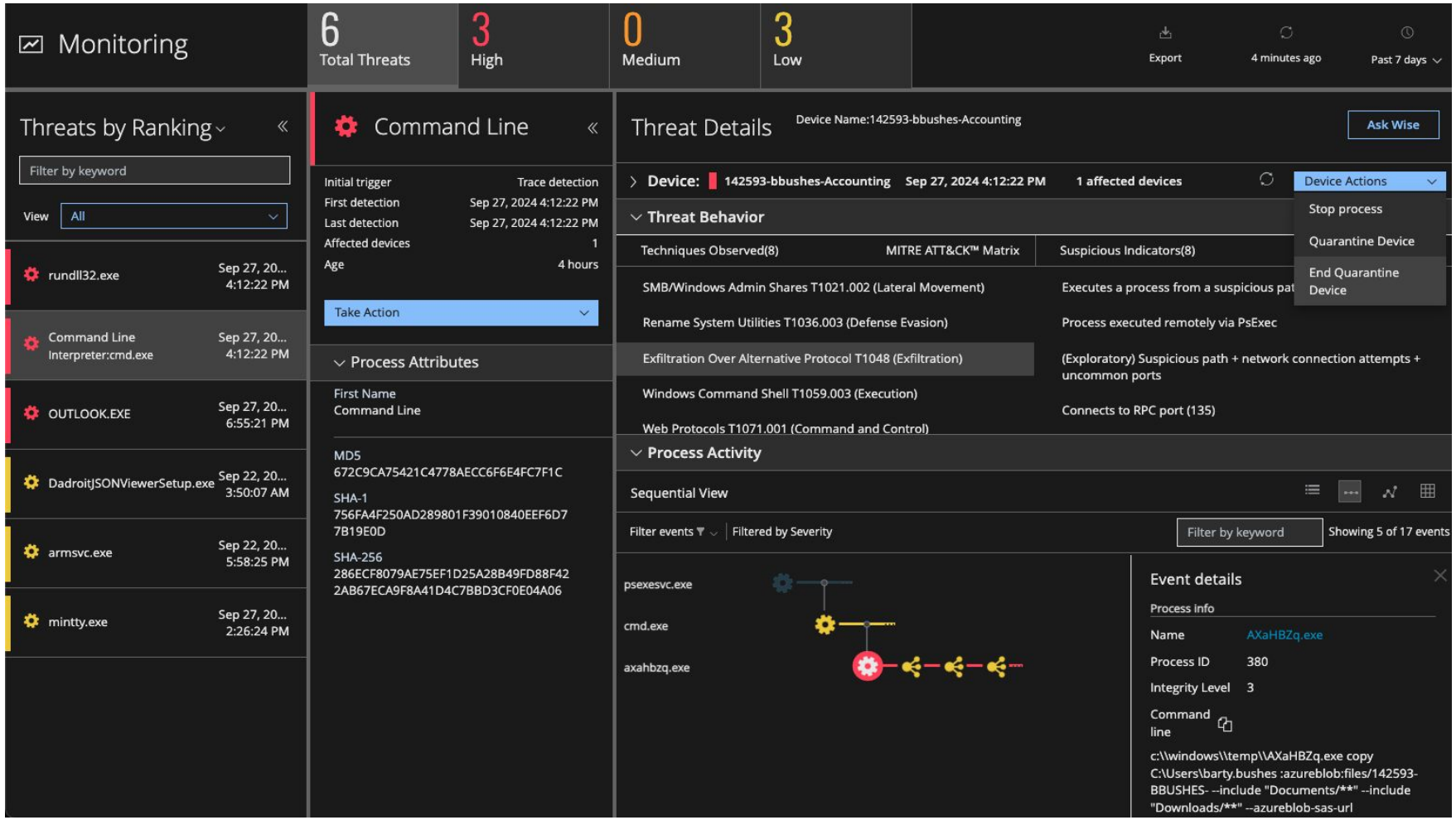
Cloud : Threat Detection Mapped to MITRE ATT&CK

Detection & Response

- Prioritized, correlated threat detection
- Visualization, contextual threat intel, and response actions

Outcome

- Identify evasive threats hiding in user behavior
- Response actions isolate and remove threats
- Reduce MTTD and MTTR to prevent harm



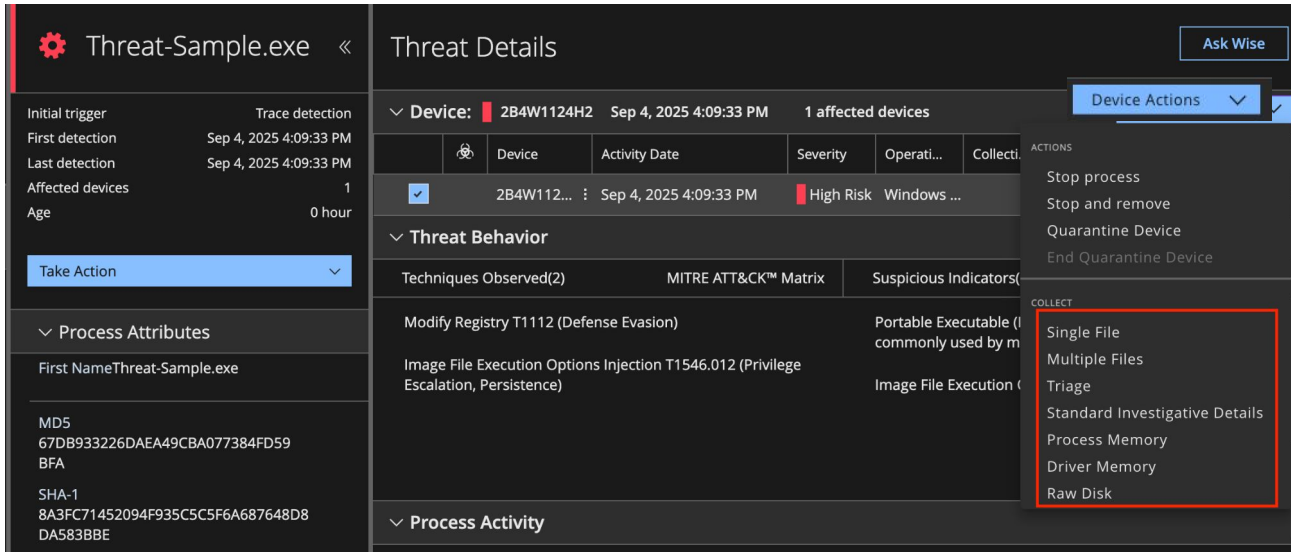
Trellix

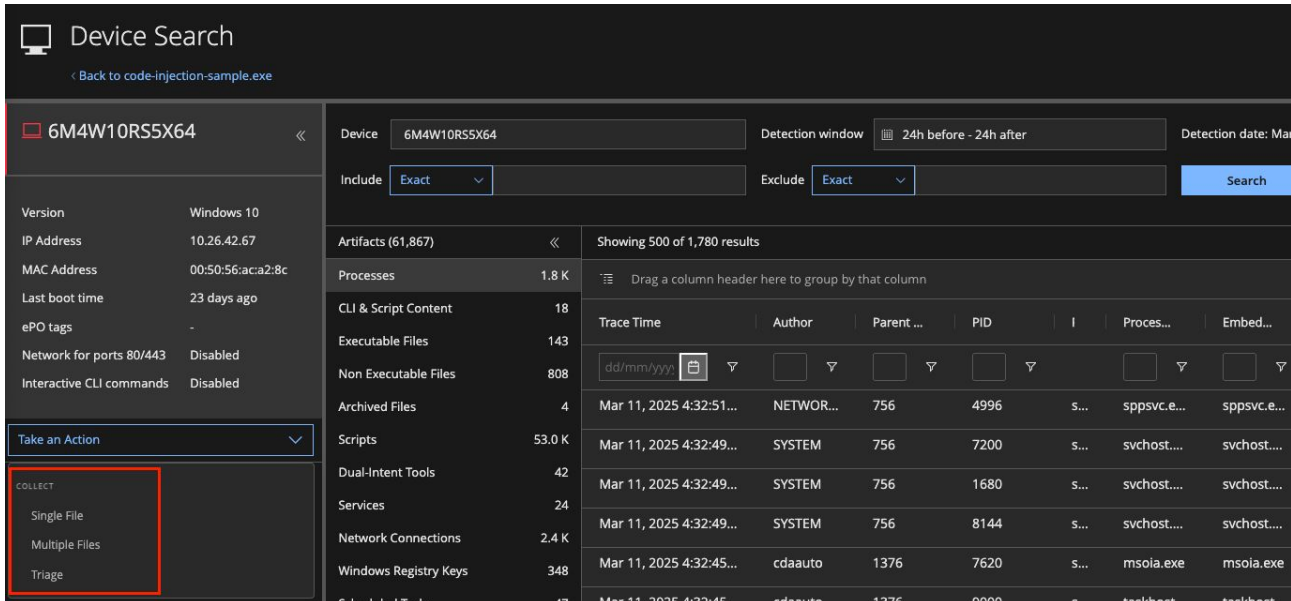
Cloud : Simplified Forensics Workflow - Acquisitions

Faster Investigations: Streamlined forensics workflows and fewer clicks save time.

Accelerated Response: Contextual collections/forensics speed up incident response.

Easy Collection Access: Initiate actions from multiple EDR workspace locations.





Trellix

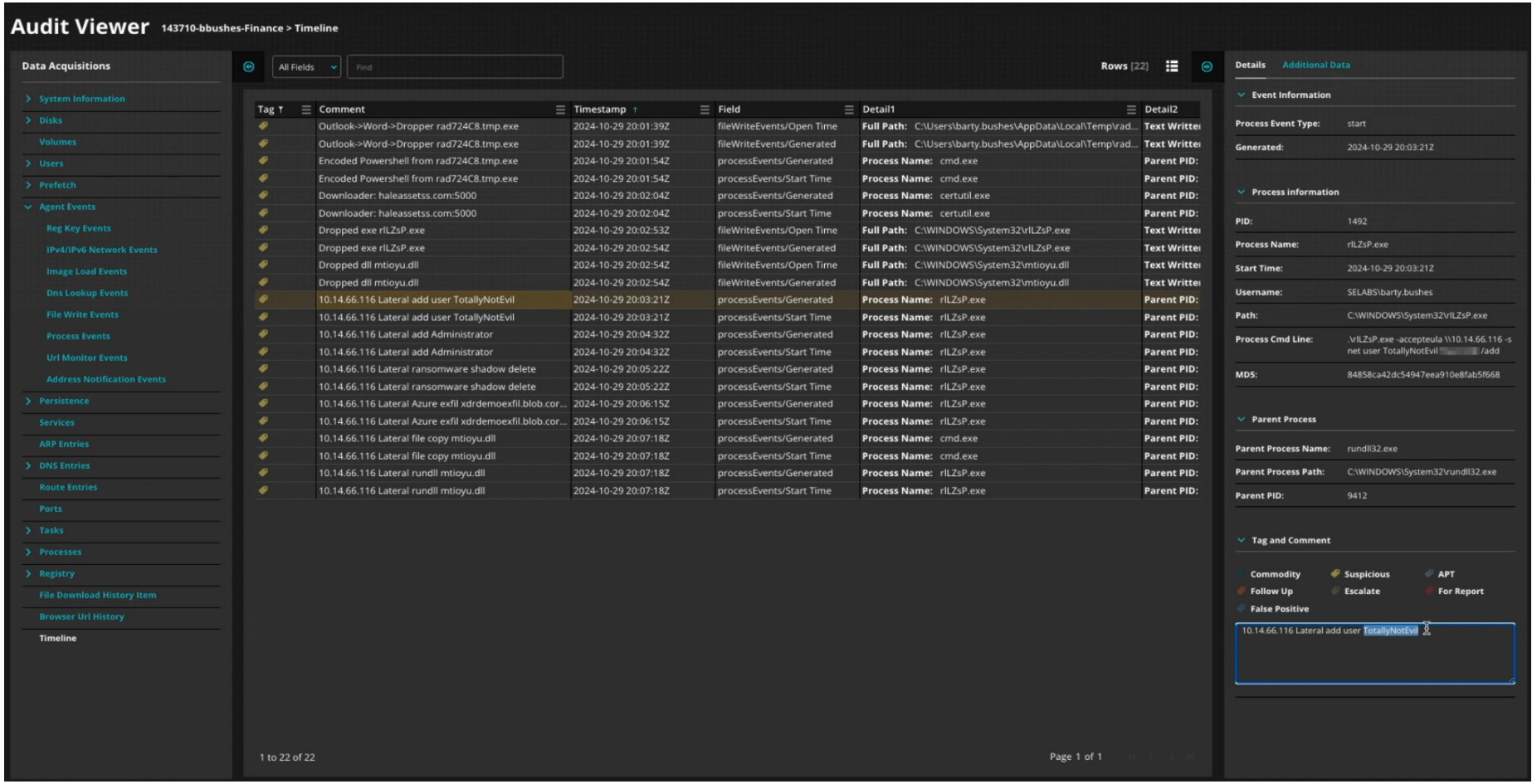
Both: Enabling Defenders with Live Response

Forensic Response

- Uncover evidence of attacker footholds
- Evict attacker with remediation

Outcome

- Reduce MTTR with live forensics
- Prevent attacker's return which happens to 43% of organizations



Trellix

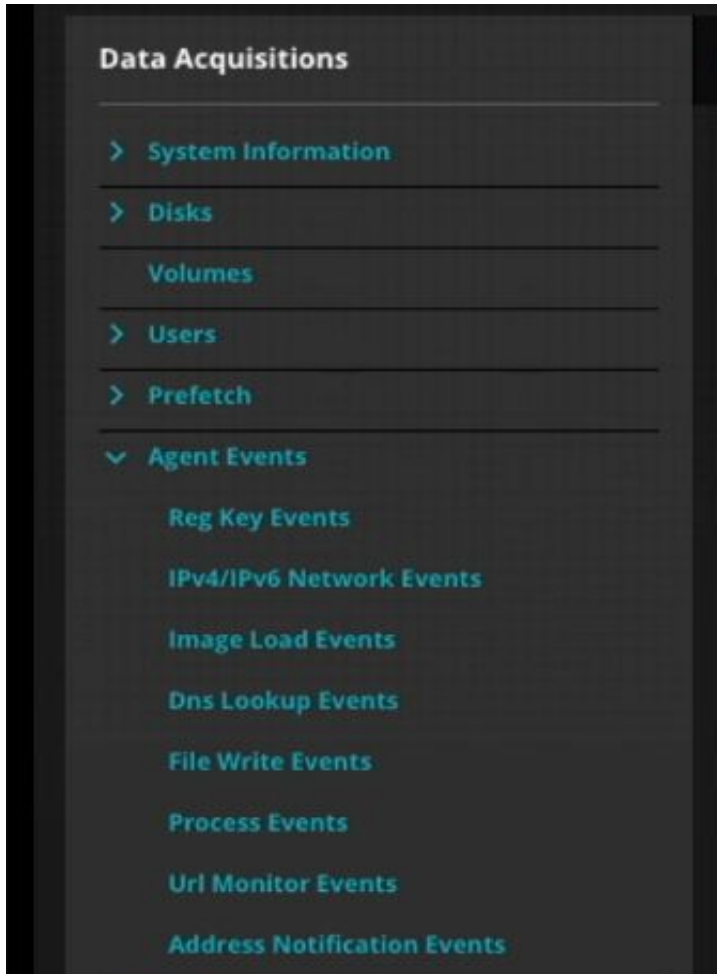
Both: Enabling Defenders with Live Response

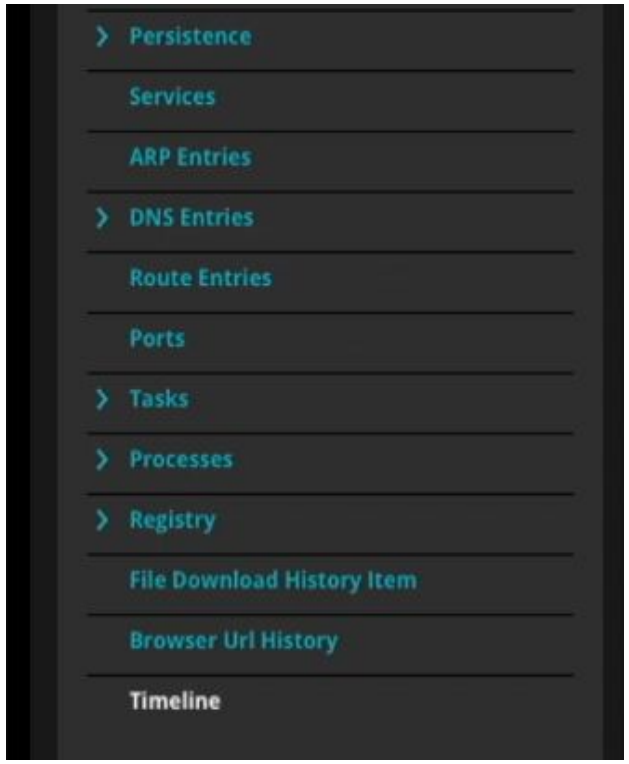
Forensic Response

- Uncover evidence of attacker footholds
- Evict attacker with remediation

Outcome

- Reduce MTTR with live forensics
- Prevent attacker's return which happens to 43% of organizations





Trellix

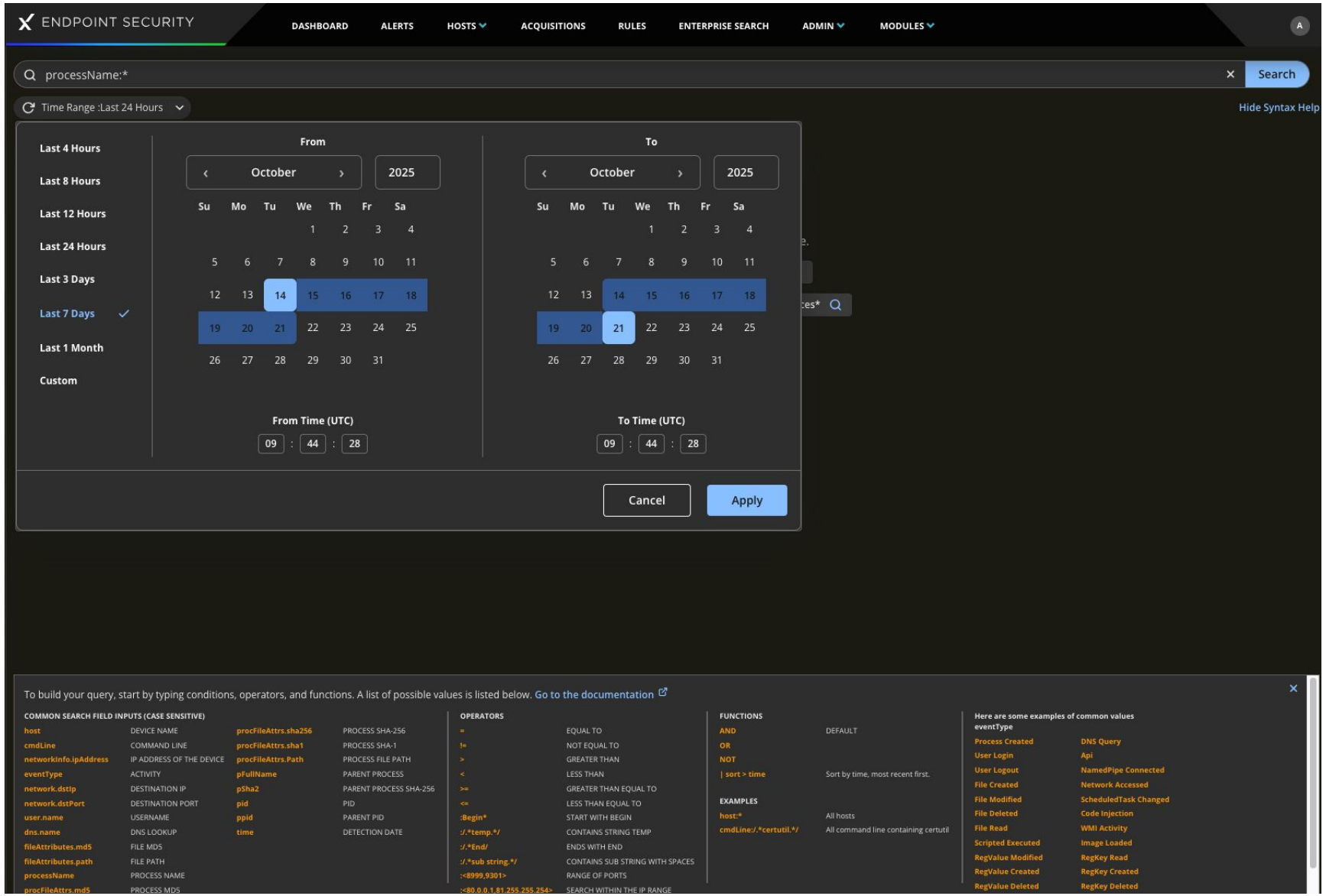
On prem: Historical Search - time based retention

Forensic Response

- Uncover evidence of attacker days/weeks/months before

Outcome

- Reduce MTTR with additional historical data
- Search system even if they offline



Trellix

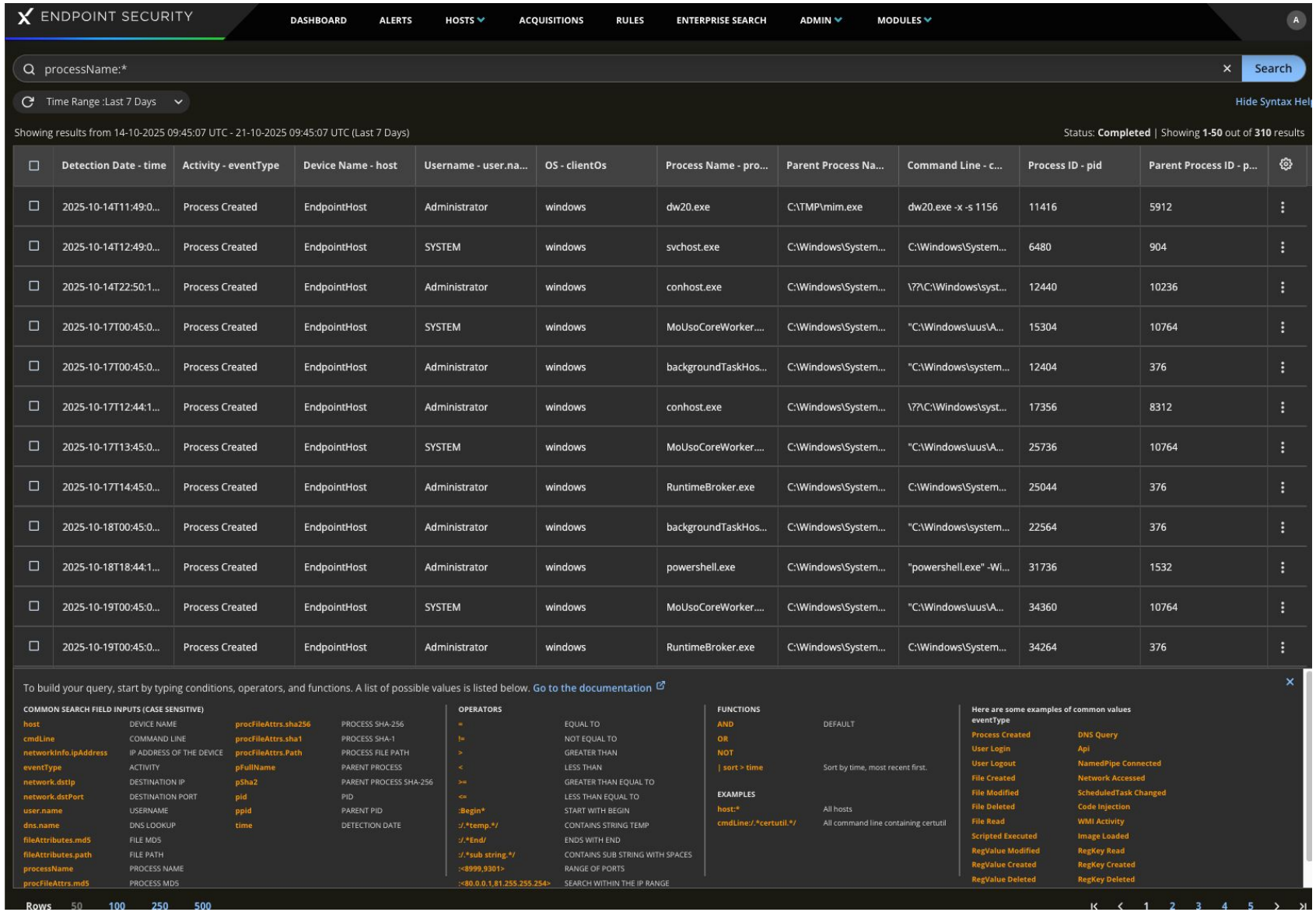
On Prem: Historical Search - enterprise wide visibility

Forensic Response

- Uncover evidence of attacker days/weeks/months before

Outcome

- Reduce MTTR with additional historical data
- Search system even if they offline



Trellix

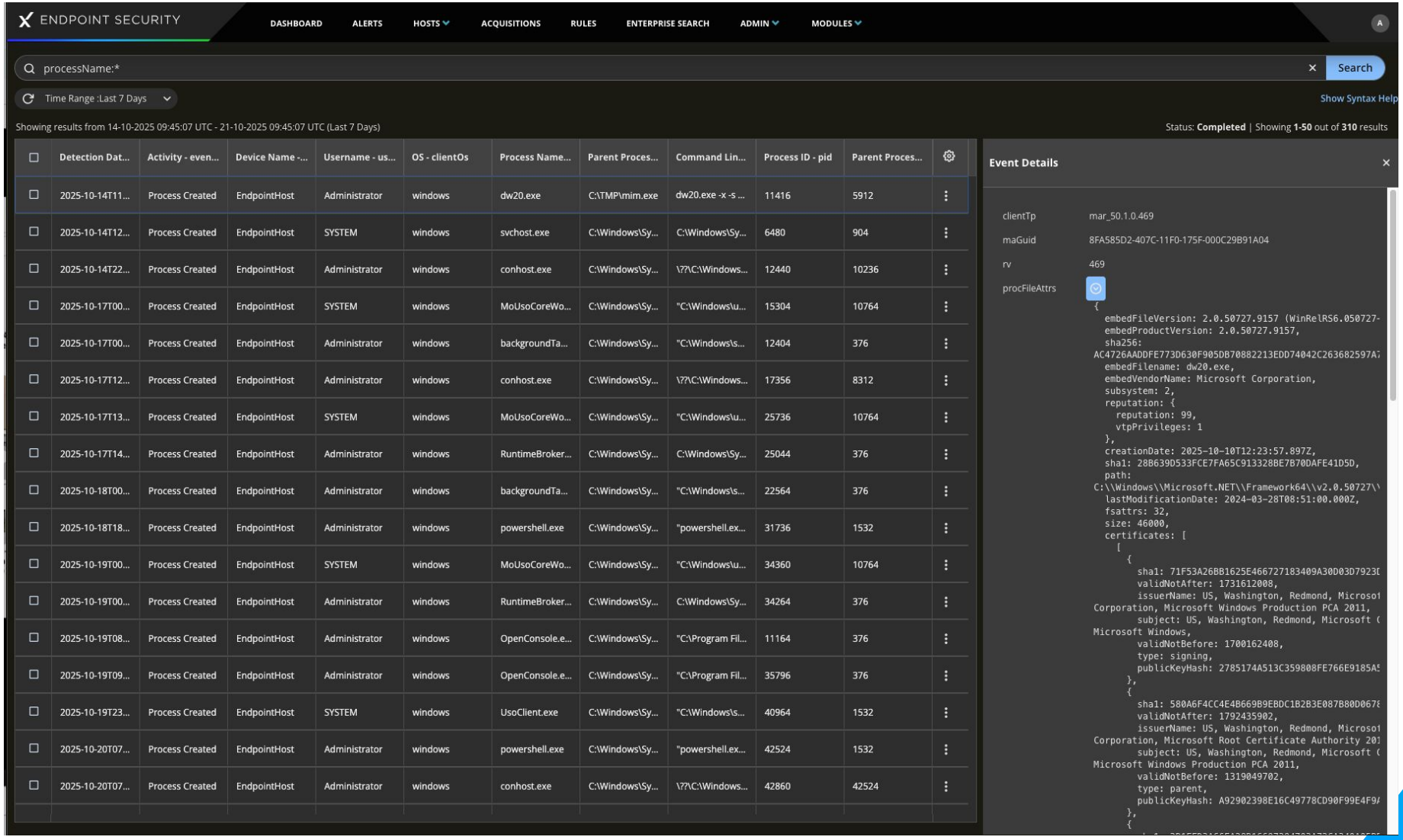
On Prem: Historical Search - in depth details

Forensic Response

- Uncover evidence of attacker days/weeks/months before

Outcome

- Reduce MTTR with additional historical data
- Search system even if they offline



Trellix

Key Trellix Security Solutions for OT

Trellix Endpoint for OT

- Centralized Management
- Anti-Malware
- Device Control
- Application Whitelisting
- Custom Intelligence
- Sandboxing
- Asset Discovery
- Compliance Audit
- EDR/Forensics

Trellix NDR for OT

- **Advanced Threat Detection on IPS or NX sensors**
- **Anomaly Detections**
- HW, Virtual, Cloud
- Asset Discovery and Visibility
- 3rd Party integrations
- **Nozomi integrations**
- Network Forensic

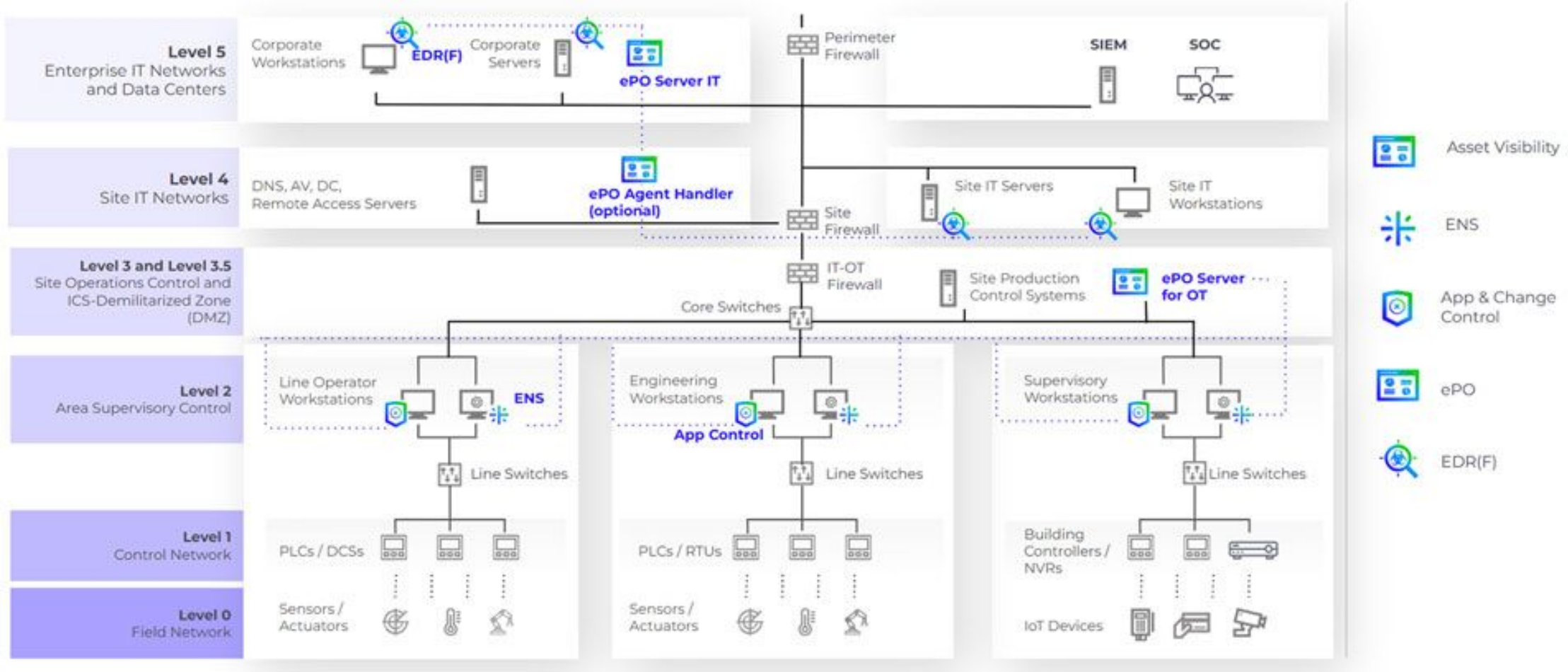
Trellix Helix XDR for OT

- On-Site log forwarding through SIEM, ePO and Comm Broker
- On-Site log collection and storage through ESM
- **IT-OT Threat Detection and Risk Assessments**
- **Integrated GenAI for alert analysis and investigations**
- **Nozomi and other 3rd Party integrations**

Trellix

Endpoint Security for OT Architecture

Operate Anywhere



Trellix

Trellix

Demo

Trellix

Licensing

Simplify Selling and Streamline Endpoint Offerings

Technology/Suite	MV1	MV2	MV3	MV4	MV5	MV6	MV7	SS1	SS2	SS3	SSE4	TRXE	Add-on

From 12 to 4

Endpoint Essentials

- Single install
- Basic Protection
- Ransomware Resilience

New in Q3!

Endpoint Core

- Single install
- Full protection
- EDR for 5% critical assets
- Ransomware Resilience

Endpoint Enterprise

- Single agent
- Integrated detection & forensics

Endpoint Complete

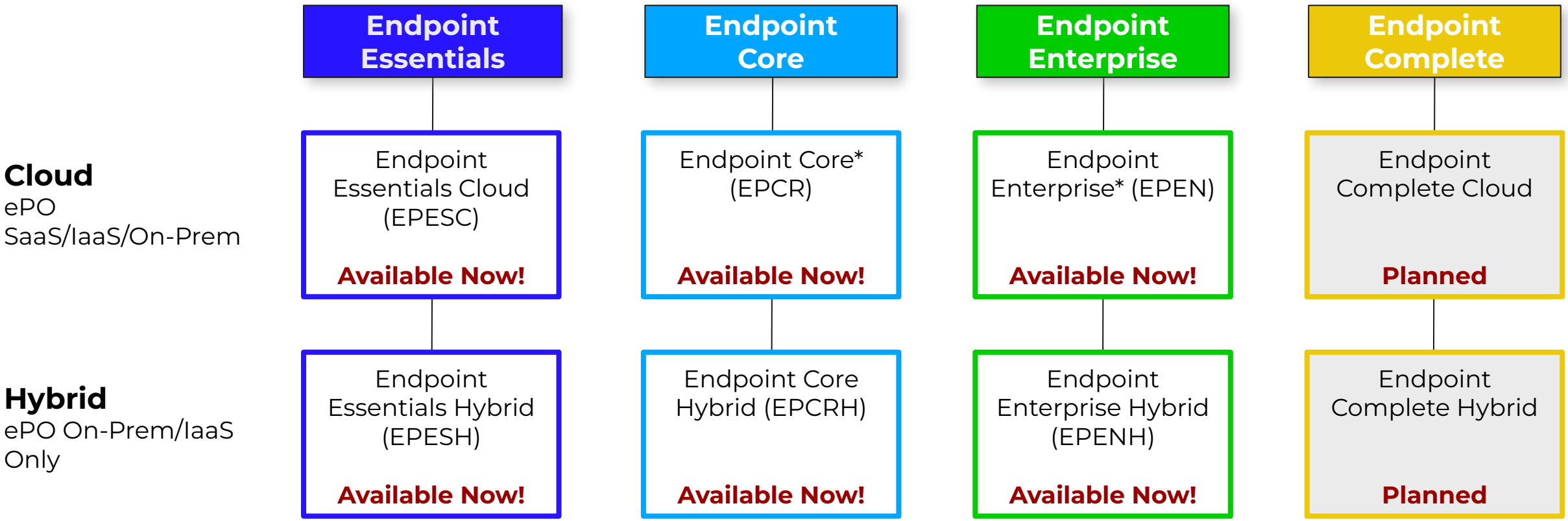
- Risk posture & reduction
- Attack Path Discovery
- MDR

FUTURE

Trellix

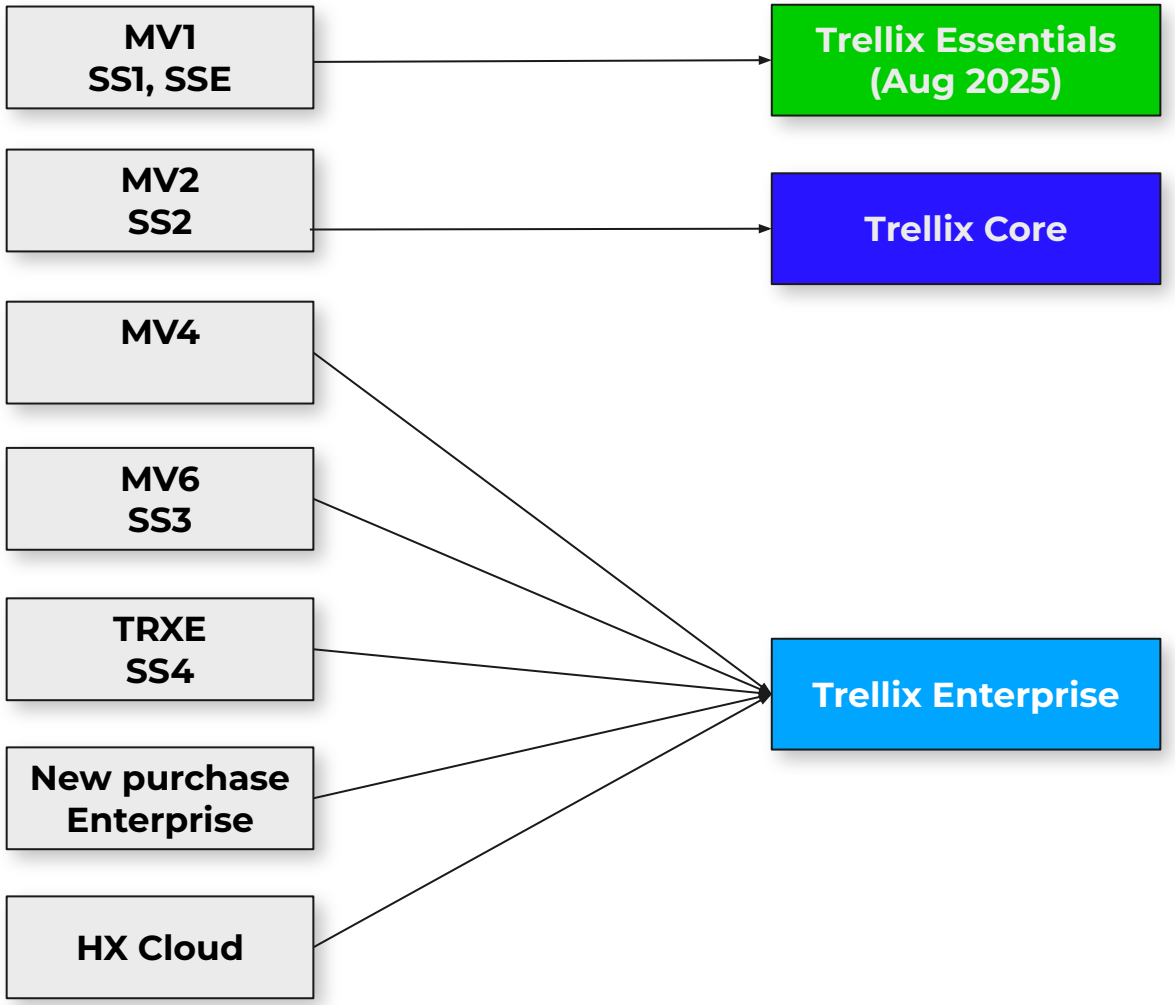
Reduce SKU Complexity, Increase Customer Value!

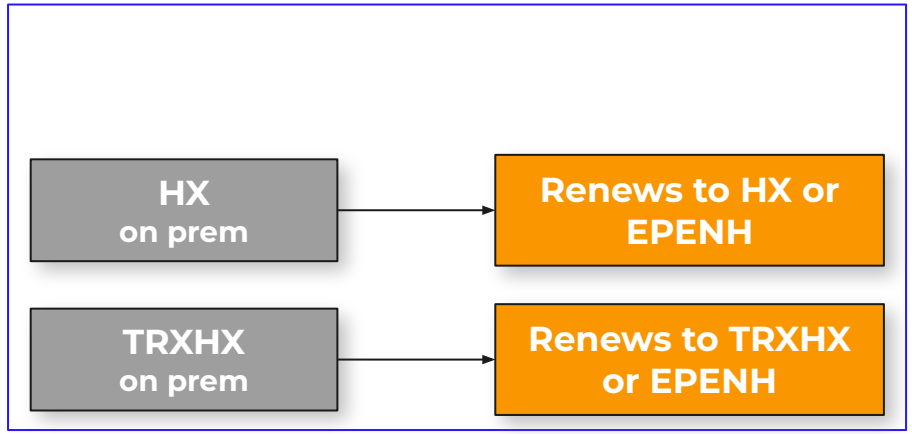
Trellix Endpoint Security Packages



Trellix

Endpoint - Simplified Sales, increased value





Trellix

Trellix Essentials (Any size)

Trellix Essentials Cloud (EPESC)
ePO SaaS, On-Prem, IaaS
Next Gen AV
Host Firewall
Web & Device Control
Adaptive Threat Protection
Native Security Protection

- MV1 Customers that don't want to upgrade to Core
- New New Entry Level security customers
- For ePO On-Prem customers use Essentials Hybrid

Trellix Essentials Hybrid (EPESH)
ePO On-Prem/IaaS
Next Gen AV
Host Firewall
Web & Device Control
Adaptive Threat Protection
Native Security Protection

Trellix

Trellix Core (Medium to large)

Trellix Core Cloud (EPCR)
ePO SaaS, On-Prem, IaaS
Next Gen AV
Host Firewall
Web & Device Control
Adaptive Threat Protection
Native Security Protection
Insights
Threat Intelligence Exchange
IVX Cloud Submissions
Application Control for PCs
EDR for Critical Assets (5%)

- MV1 customers with maturing security programs
- Existing MV2 Customers
- Net new customers with enhanced security needs and compliance requirements
- For ePO On-Prem customers use Core Hybrid

Trellix Core Hybrid (EPCRH)
ePO On-Prem/IaaS
Next Gen AV
Host Firewall
Web & Device Control
Adaptive Threat Protection
Native Security Protection
Insights
Threat Intelligence Exchange
IVX Cloud Submissions
Application Control for PCs
EDR for Critical Assets (5%)

Trellix

Endpoint Enterprise Cloud

Enterprise Cloud (EPEN)
ePO SaaS, On-Prem, IaaS
Next Gen AV
Host Firewall
Web & Device Control
Adaptive Threat Protection
Native Security Protection
Insights
Threat Intelligence Exchange
IVX Cloud Submissions
Application Control for PCs
Trellix EDR + Forensics

- Upgrade MV4 and MV6 Customers
- Migrate TRXE Customers
- Can use on premise components if required
- Net new customers with mature security programs and dedicated Security Operations Centers

Trellix

Endpoint Enterprise Hybrid

Enterprise Hybrid (EPENH)
ePO SaaS, On-Prem, IaaS
Next Gen AV
Host Firewall
Web & Device Control
Adaptive Threat Protection
Native Security Protection
Insights
Threat Intelligence Exchange
IVX Cloud Submissions
Application Control for PCs
On-Prem EDR + Forensics

- **Primary difference from EPEN Cloud is EPENH does not offer EDR or HX as a service**
- Upgrade HX Customers
- Migrate TRXHX Customers
- Net new customers with mature security programs and dedicated Security Operations Centers who need on-prem EDR
- ePO is a new Requirement for HX customers. ePO SaaS is being made available as an option to simplify the addition of ePO.
- If customer chooses to use ePO SaaS - all ePO manageable modules are entitled to be managed by ePO SaaS.

Trellix

Trellix

OVERVIEW

Todays key takeaways

1. Trellix has a robust and mature endpoint and management offering for IT and OT

2. EDRF for cloud and on premise delivers a new EDR + forensics capabilities and is the new EDR and forensics offering

3. Trellix Wise for EDRF augments and enhances SOC teams efficiency and skill sets

4. Trellix is fully focused on delivering capabilities for on premise and cloud customers

5. New endpoint bundle suites designed to protect customers and simplify offerings

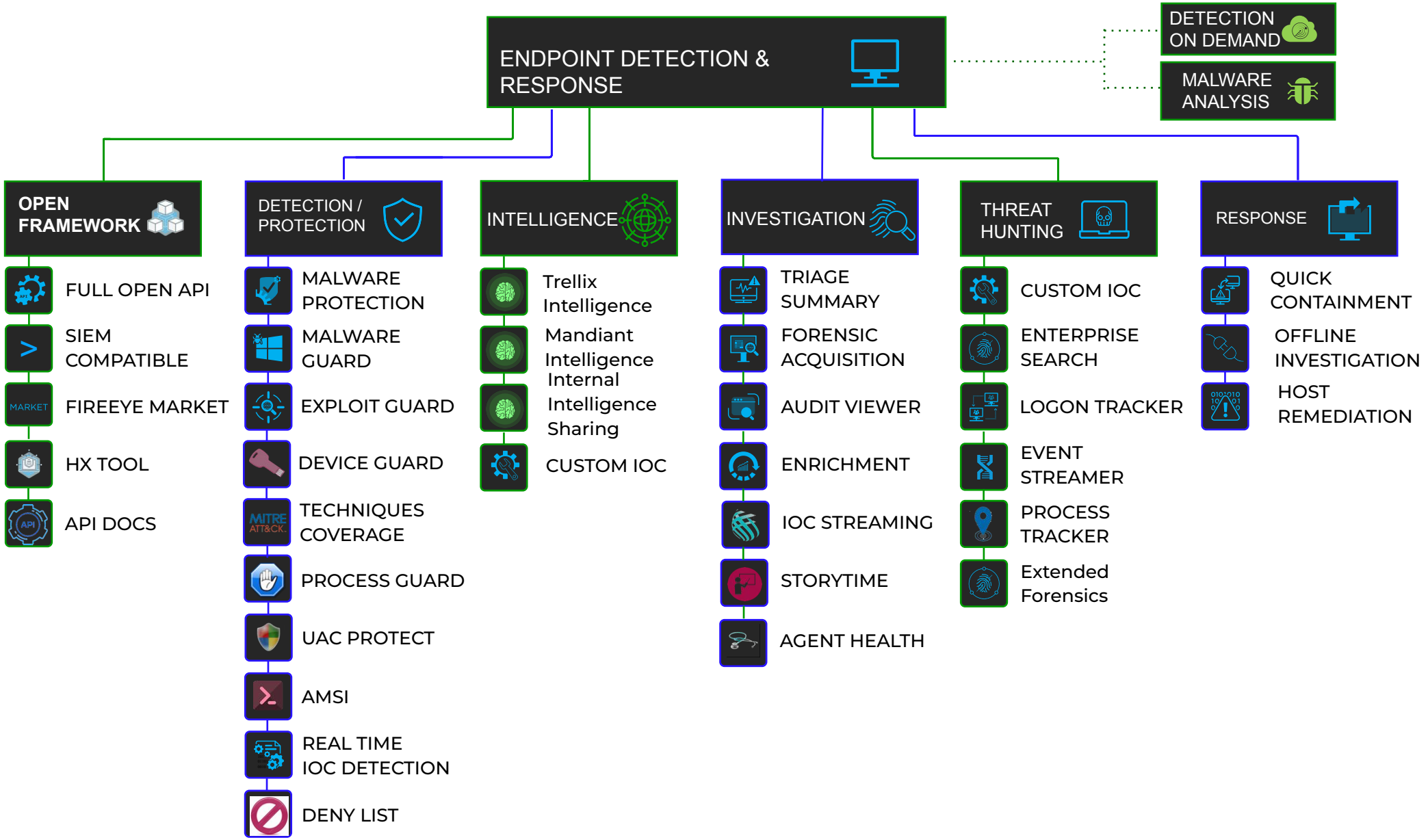
Trellix


Trellix

Trellix

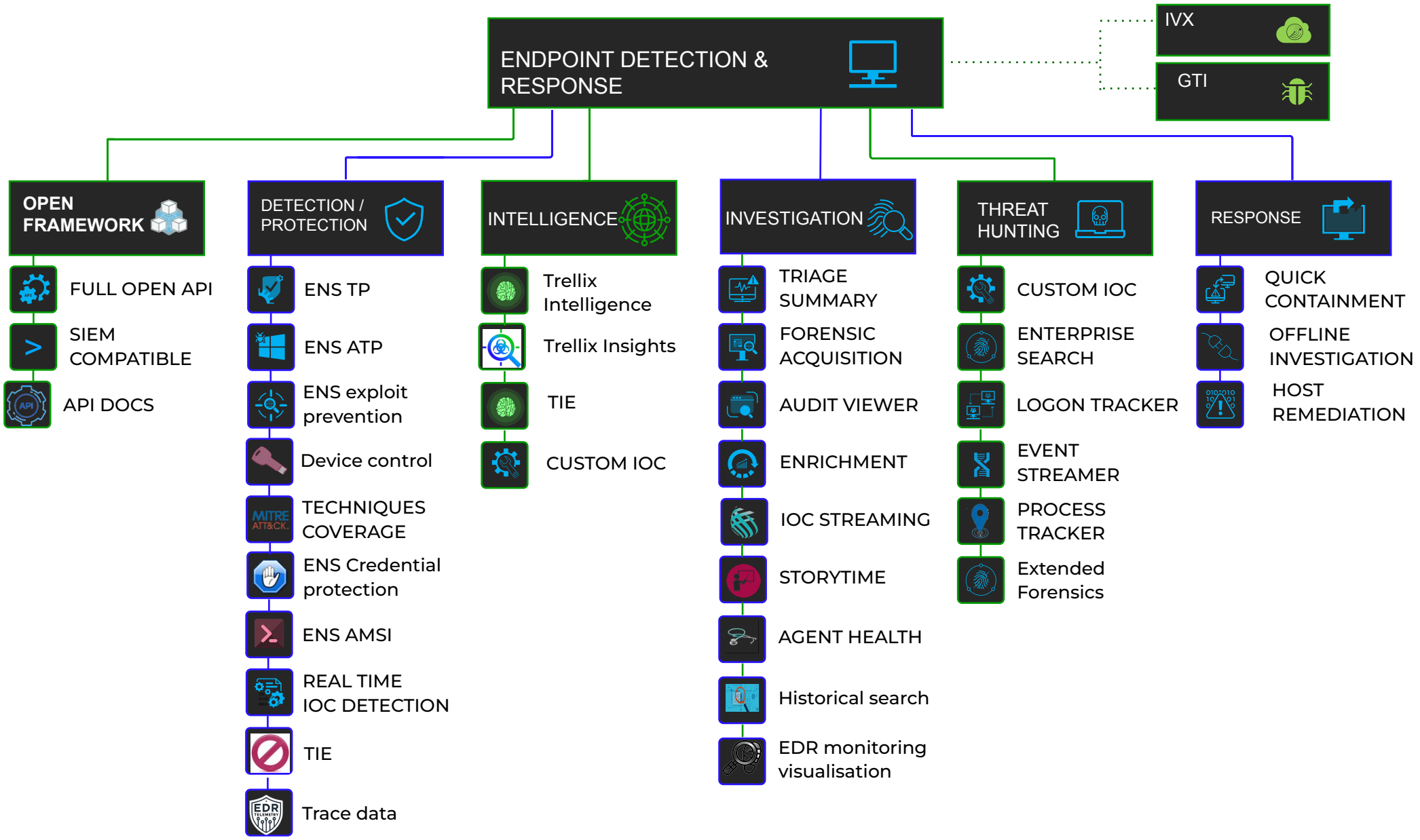
A quick EDR and HX recap

HX capabilities



Trellix

EDRF capabilities



Trellix

The Trellix Approach

Reduces
Endpoint Complexity

- Reduce the attack surface
- Fill gaps in coverage and fix misconfigurations
- Uncover and stop advanced threats

Before the Attack

Increases
SOC Efficiency

- Reduce alerts deluge
- Spot and address critical incidents easily
- Speed up investigations and response

During the Attack

Reduces
Endpoint Incident Impact

- Contain incidents
- Understand scope and root cause
- Remediate and prevent reoccurrence

After the Attack

Reduce SOC workloads and improve SOC effectiveness and response

Trellix

Trellix

Trellix differentiators

Trellix Top Differentiators for Endpoint security

- live memory analysis (w/o a full dump)
- Deep scriptable acquisitions
- Non-exhaustive live searches for arbitrary data patterns (we can hunt for unknown patterns/strings directly inside any file, even if that data hasn't been previously collected/indexed by the agent)
- Same technology for workstations/servers on premise or cloud

Endpoint Customer Alternatives

Microsoft

What they say	• Endpoint Protection is built-in to Windows with advanced protection, nothing to deploy • Inspired by the "assume breach" mindset with their EDR • Prevent and detect attacks across your identities, endpoints, apps, email, data, and cloud apps with XDR capabilities
The Reality	• Difficult to manage and configure, especially at enterprise scale • Complex for responders, search is limited to cloud telemetry, and generic alerting • The path to XDR has limited integrations and requires their SIEM integrations • Hidden costs
Trellix Differentiation	• Easy to configure and manage comprehensive and customizable modern protection technologies at scale, cloud and on-prem. Layered security options. • Quickly hunt, detect, and respond to new threats at scale with differentiated direct client communication architecture. • Fast path to Trellix open and native XDR with native integration of endpoint, email & network security • No surprise Hidden costs

Endpoint Customer Alternatives

CROWDSTRIKE

What they say	• CrowdStrike combines the most effective prevention technologies and full attack visibility with built-in threat intelligence — all in a single lightweight agent • Comprehensive visibility that spans detection, investigation, and response to ensure nothing is missed and potential breaches are stopped • XDR is the future as long as you have the right endpoint security (EDR) • Position Trellix as “legacy” that “relies on signatures”
The Reality	• 3rd party testing shows high rates of false positives, which increases SOC workloads • Relies on cloud telemetry and access for hunting and control of endpoints • Delayed detections in MITRE testing • Relies on 3rd party integrations for visibility and context beyond the endpoint • No on-prem solution
Trellix Differentiation	• Easy to configure and manage comprehensive and customizable modern protection technologies at scale, cloud and on-prem • Quickly hunt, detect, and respond to new threats at scale with differentiated direct client communication architecture. • Fast path to Trellix XDR with native integration of endpoint, email & network security