Trellix

24-26 OCTOBER 2023

EMEA Partner Tech Summit 2023

Rome, Italy

Endpoint Security

EMEA Partner Tech Summit 2023

Benjamin Marandel
Diarmuid O'Boyle
November 10, 2023

Use the following WIFI:
SID: **Sheraton_Conference**
Password: **trellix**

Before We Begin

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 before the reception on your right.

Emergency Exits

Familiarize yourself with the nearest emergency exits, located just before the reception on your left. In case of an emergency, follow the exit signs and proceed calmly to the nearest exit.

Q&A

We will have a Q&A session at the end of the presentation. Please save your questions until then.

Session Schedule

The session is expected to last approximately 3 hours with no breaks.

Trellix

Welcome

EMEA Partner Tech Summit 2023

Trellix

Introduction

Endpoint Security - Speakers

“Ben” (Benjamin) Marandel

Solutions Architect

Diarmuid O’Boyle

Solutions Engineer

Trellix

Agenda

Endpoint Security

- Welcome
- Product Line Pitching
- Use cases and Demonstration Guidance
- SE Resources – How to Access
- Trellix Differentiators
- What Next
- Point of Contacts

Trellix

Product Line Pitching

Endpoint Security

Trellix

Endpoint Security is a foundation

Reduce SOC workloads and improve effectiveness

Support **all your Endpoints** in complex environment

Pro-actively protect against sophisticated threats, like Ransomware

Effective and accurate **alerts & incidents triage and prioritization**

Immediate **response, root cause** understanding, and **remediation**

Endpoints are Constantly Under Attack

Ransomware

54%

Organizations reported ransomware blocked access to systems / data*

Gaps in visibility

21days

Average attacker dwell time before being discovered**

Ignored Alerts

35%

Security analysts who say alerts are ignored when the queue is full***

Reoccurring Attacks

43%

Organizations hit by ransomware were hit more than once****

* Future Enterprise Resiliency & Spending Survey - Wave 11, IDC, December 2021
** Infosecurity magazine
*** IDC Survey 2021
**** 2022 Third-party breach report, Black Kite

Trellix

Endpoint Security Requirements are changing

Expanding Attack Surface

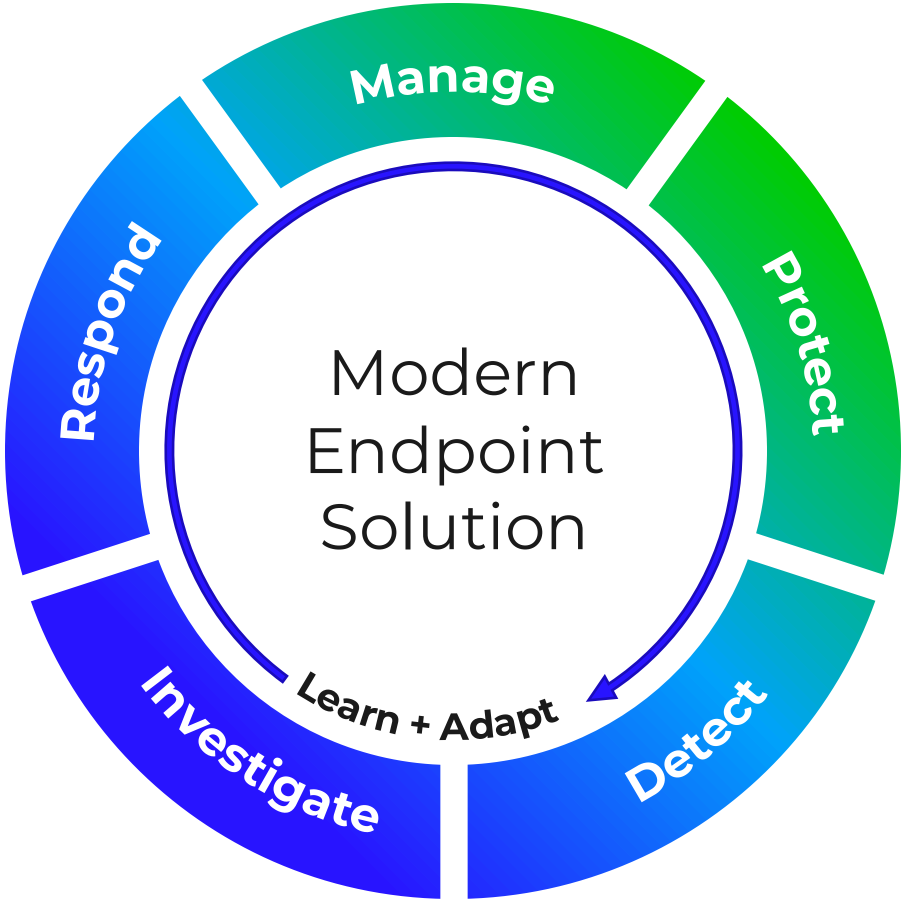
Increasingly sophisticated threats, more endpoints constantly under attack

Act before, during and after the attack

Endpoint solutions need to cover protection, detection and response and be effective before, during and after the attack

SOC is highly impacted

Increasing workloads due to alerts and incidents deluge leads to inability to respond fast enough



Trellix

You Need a Comprehensive Solution

What if you could have a solution that...

- **Optimizes** Protection on all Endpoints **Proactively**
- **Simplifies & Improves** Endpoint Alerts Triage, Investigation, and Response
- **Minimizes Impact** from Endpoint Incidents & Threat Campaigns

Trellix Endpoint Security Products

Trellix Endpoint Security (ENS)

Malware Protection

Trellix Endpoint Security (HX)

Endpoint Forensics

Trellix Application and Change Control

Deny/Allow Lists

Trellix Host Data Loss Prevention

Protecting the Data

Trellix Desktop Encryption

Protecting the device

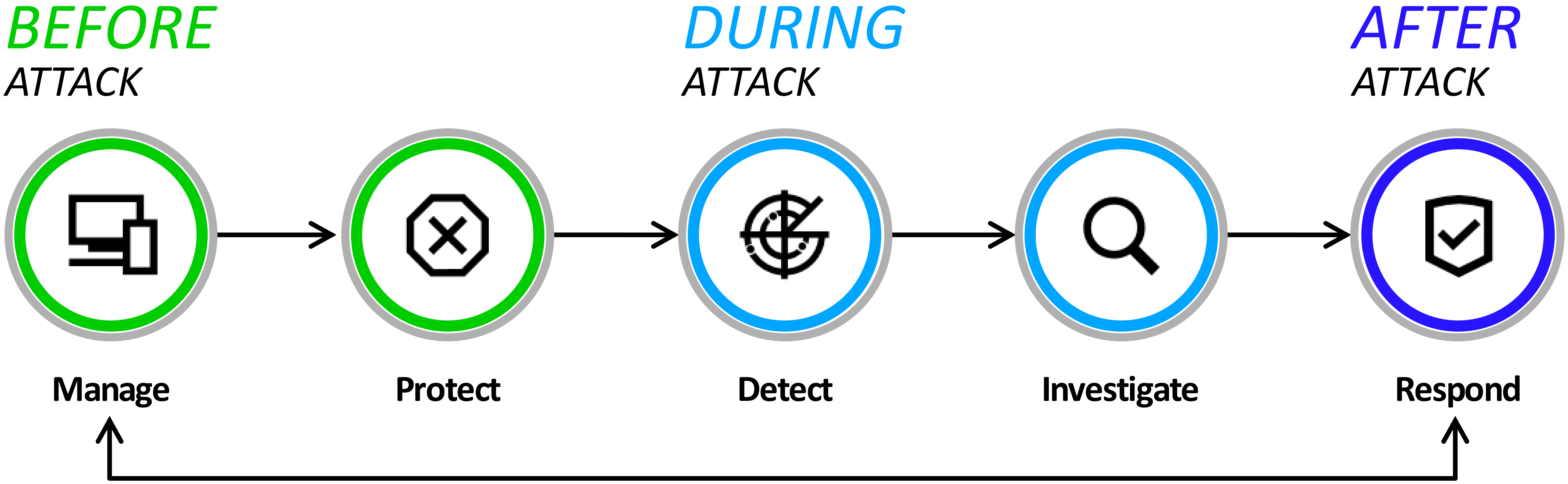
Trellix EDR

Threat Mitigation

Trellix Mobile Security

Protecting the mobile device

Foundational Endpoint Security



Visibility & Control over the full life cycle of all your Endpoints

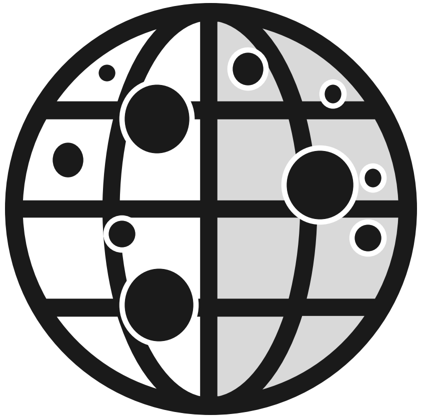
Trellix

BEFORE
THE ATTACK

Machine Learning and Advanced Remediatio

Real Protect

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



Real Protect Static (Pre-Execution)

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

Real Protect Dynamic (Post-Execution)

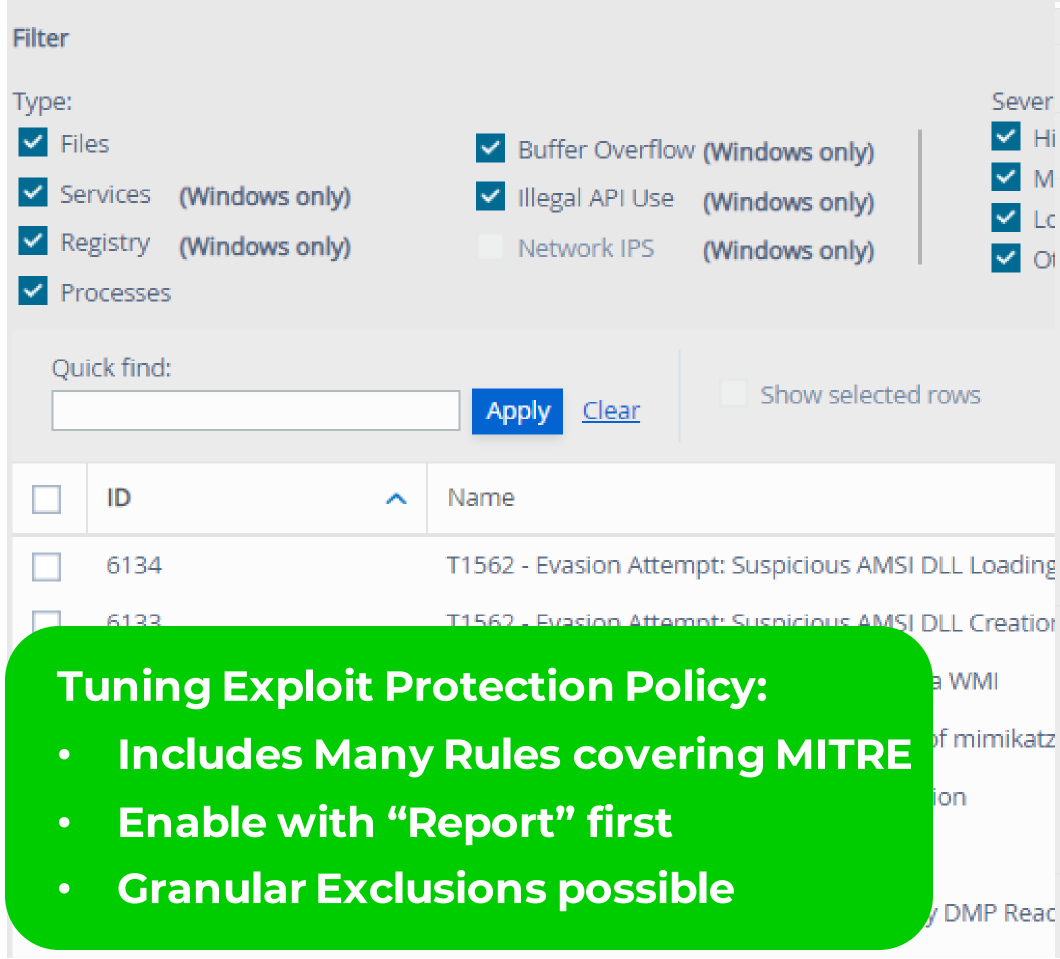
Detect dynamic behavior of Greyware on the endpoint, compare to known malware behaviors for a match via behavioral cloud-based machine learning

Pre-and Post Execution is critical to maximize your detection capabilities.

Trellix

BEFORE
THE ATTACK

Optimize Endpoint Security Posture – Exploit Protection



Filter

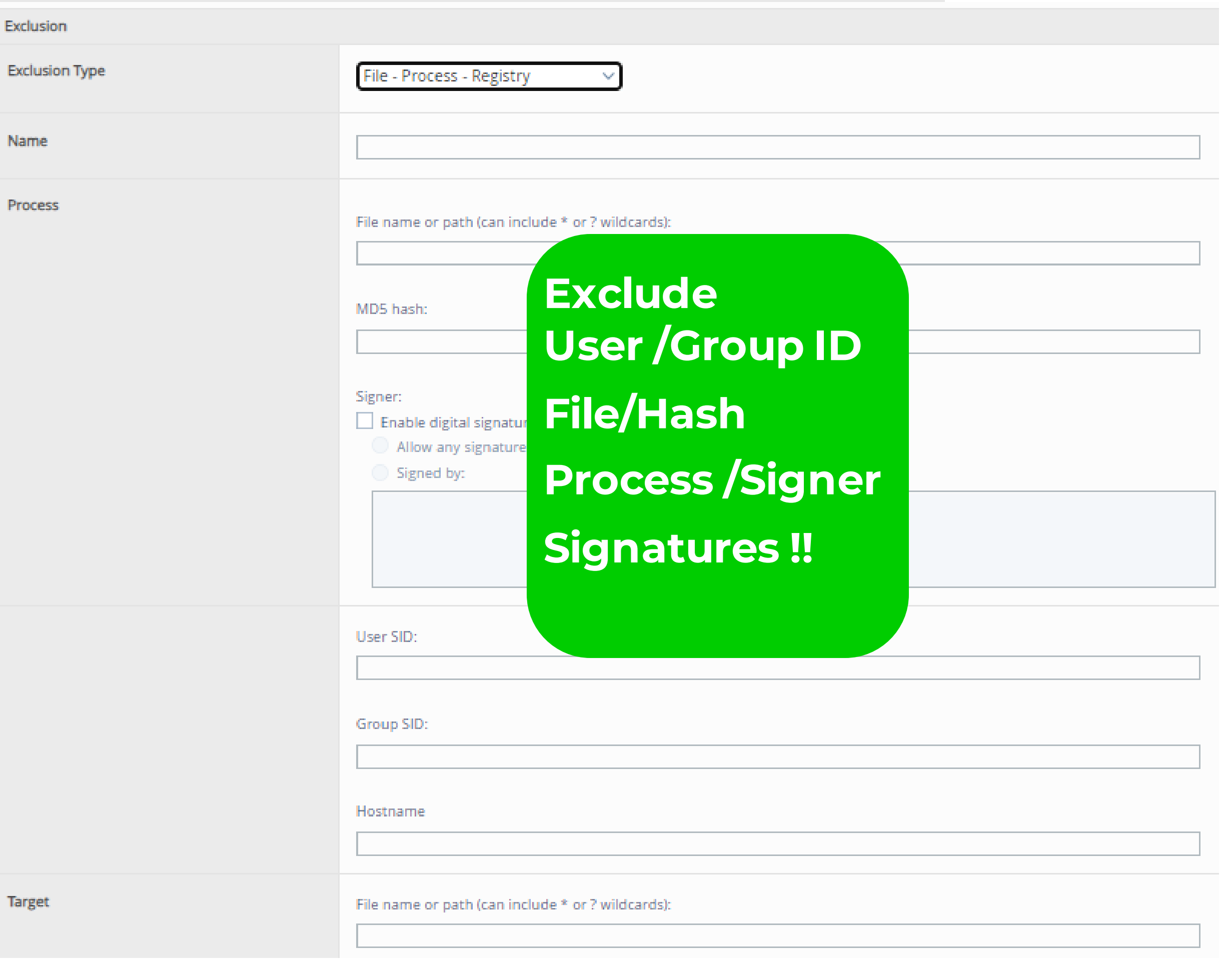
Type:

☑ Files
☑ Services (Windows only)
☑ Registry (Windows only)
☑ Processes
☑ Buffer Overflow (Windows only)
☑ Illegal API Use (Windows only)
□ Network IPS (Windows only)

Sever
☑ Hi
☑ M
☑ Lo
☑ O

Quick find: Apply Clear □ Show selected rows

□	ID	Name
□	6134	T1562 - Evasion Attempt: Suspicious AMSI DLL Loading
□	6133	T1562 - Evasion Attempt: Suspicious AMSI DLL Creation
		a WMI
		of mimikatz
		ion
		y DMP Reac



Exclusion

Exclusion Type: File - Process - Registry

Name:

Process:
File name or path (can include * or ? wildcards):
MD5 hash:
Signer:
□ Enable digital signatur
○ Allow any signature
○ Signed by:
User SID:
Group SID:
Hostname

Target:
File name or path (can include * or ? wildcards):

Exclude
User /Group ID
File/Hash
Process /Signer
Signatures !!

Tuning Exploit Protection Policy:

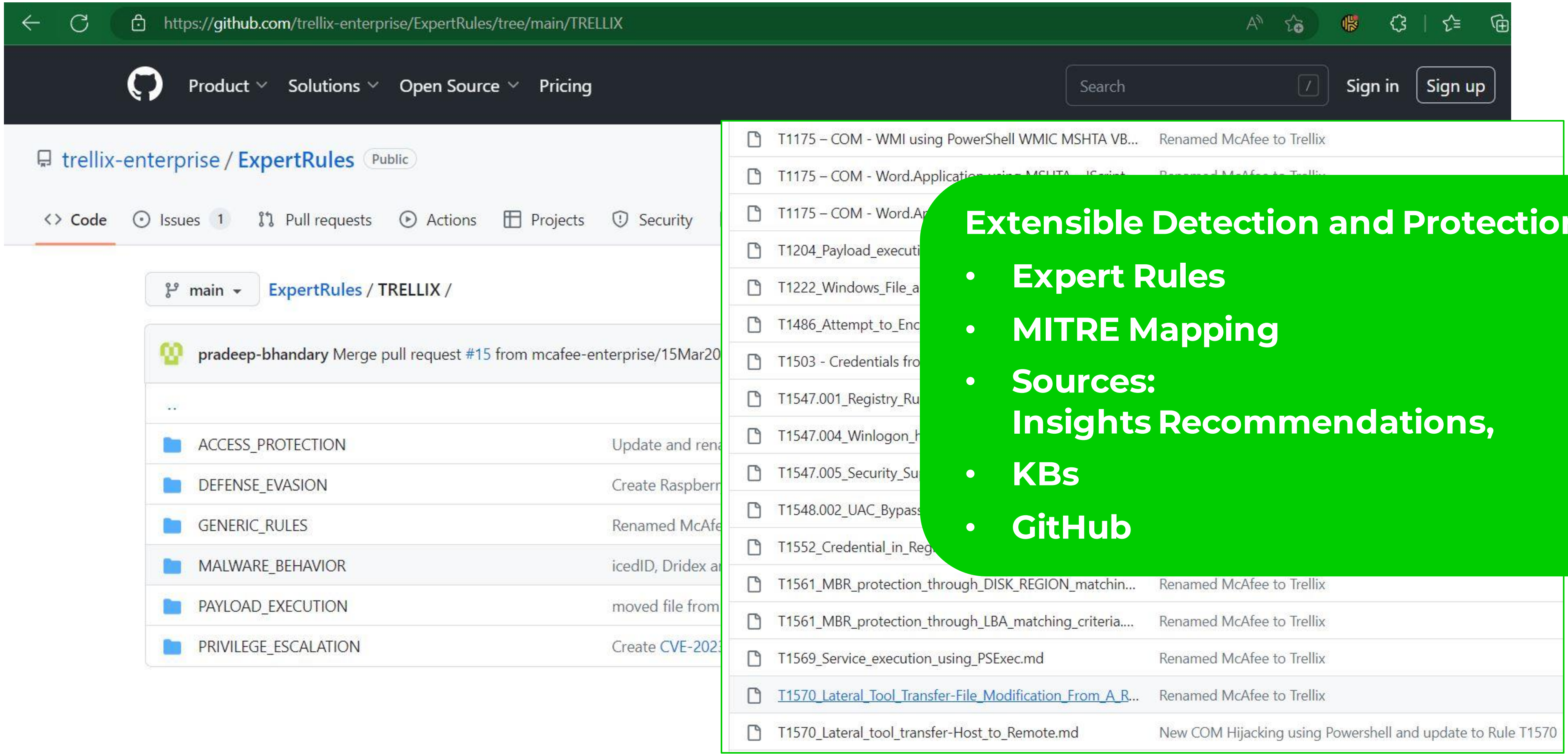
- **Includes Many Rules covering MITRE**
- **Enable with “Report” first**
- **Granular Exclusions possible**

Countermeasures for entry vector threats
https://kcm.trellix.com/corporate/index?page=content&id=KB91836

BEFORE

THE ATTACK

Optimize Endpoint Security Posture – Expert Rules



https://github.com/trellix-enterprise/ExpertRules/tree/main/TRELLIX

trellix-enterprise / ExpertRules Public

ExpertRules / TRELLIX /

pradeep-bhandary Merge pull request #15 from mcafee-enterprise/15Mar20

..	
ACCESS_PROTECTION	Update and rena
DEFENSE_EVASION	Create Raspberr
GENERIC_RULES	Renamed McAfe
MALWARE_BEHAVIOR	icedID, Dridex ar
PAYLOAD_EXECUTION	moved file from
PRIVILEGE_ESCALATION	Create CVE-202

T1175 – COM - WMI using PowerShell WMIC MSHTA VB...	Renamed McAfee to Trellix
T1175 – COM - Word.Application using MSHTA – JScript...	Renamed McAfee to Trellix
T1175 – COM - Word.Ap	
T1204_Payload_executi	
T1222_Windows_File_a	
T1486_Attempt_to_Enc	
T1503 - Credentials fro	
T1547.001_Registry_Ru	
T1547.004_Winlogon_H	
T1547.005_Security_Su	
T1548.002_UAC_Bypass	
T1552_Credential_in_Reg	
T1561_MBR_protection_through_DISK_REGION_matchin...	Renamed McAfee to Trellix
T1561_MBR_protection_through_LBA_matching_criteria....	Renamed McAfee to Trellix
T1569_Service_execution_using_PSExec.md	Renamed McAfee to Trellix
T1570_Lateral_Tool_Transfer-File_Modification_From_A_R...	Renamed McAfee to Trellix
T1570_Lateral_tool_transfer-Host_to_Remote.md	New COM Hijacking using Powershell and update to Rule T1570

Extensible Detection and Protection:

- **Expert Rules**
- **MITRE Mapping**
- **Sources:**
  Insights Recommendations,
- **KBs**
- **GitHub**

Expert Rules GitHub Repository - https://github.com/mcafee-enterprise/ExpertRules

BEFORE
THE ATTACK

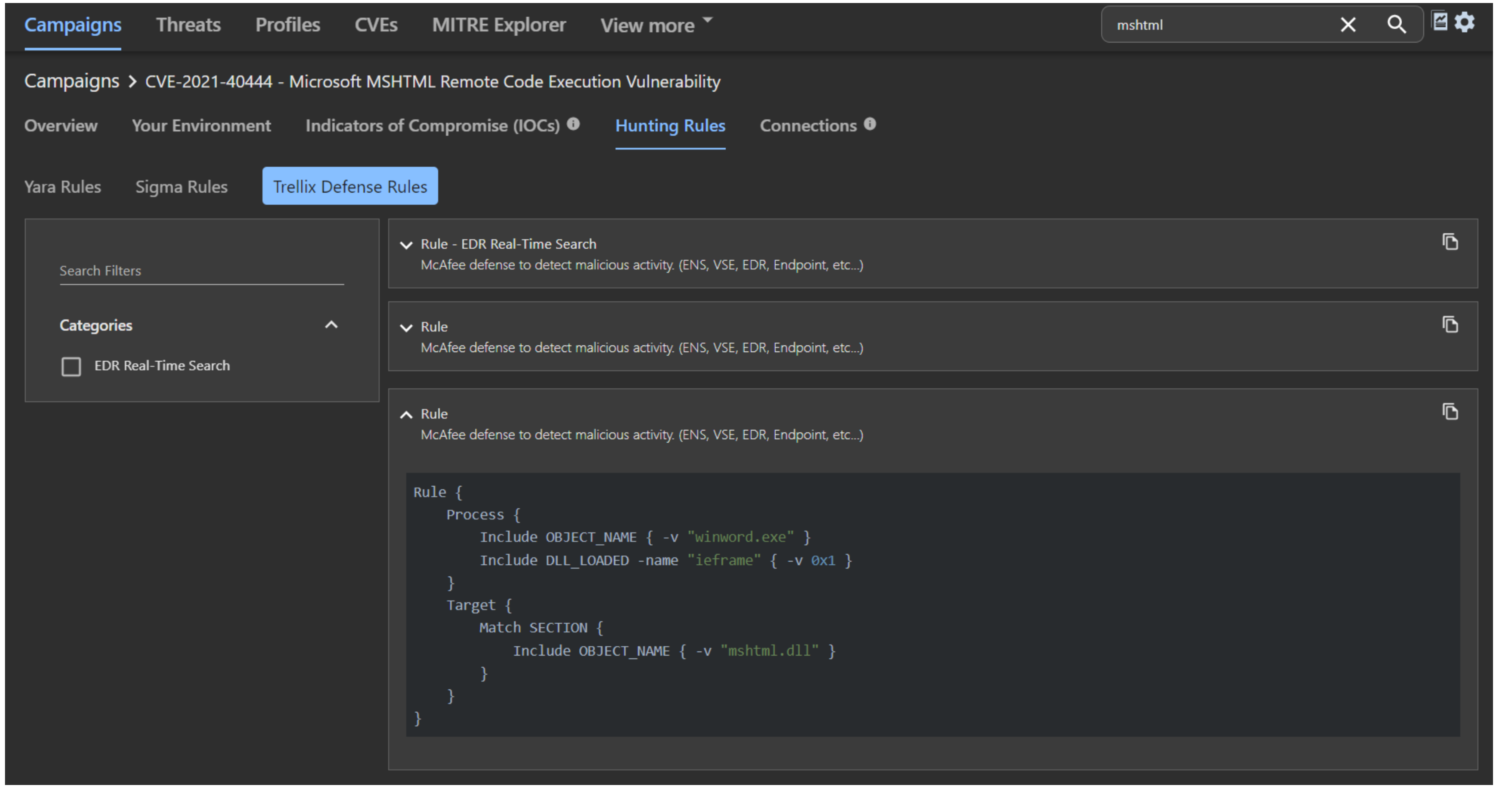
Optimize Endpoint Security Posture

Protection against entry vector Threats (KB91836)

Below are the countermeasures. Click to advance to the section that you want to view:

- ENS Adaptive Threat Protection (ATP)
- ENS Dynamic Application Containment (DAC)
- ENS Threat Prevention Antimalware Scan Interface (AMSI)
- ENS Exploit Prevention
- ENS Exploit Prevention Expert Rules
- ENS Access Protection default rules
- ENS Access Protection custom rules
- ENS Firewall Rules
- VSE Access Protection default rules
- VSE Access Protection custom rules
- Host IPS signatures
- MSME antispam and on-access scan policies
- More user recommendations

Trellix Insights



Rule - EDR Real-Time Search
McAfee defense to detect malicious activity. (ENS, VSE, EDR, Endpoint, etc...)

Rule
McAfee defense to detect malicious activity. (ENS, VSE, EDR, Endpoint, etc...)

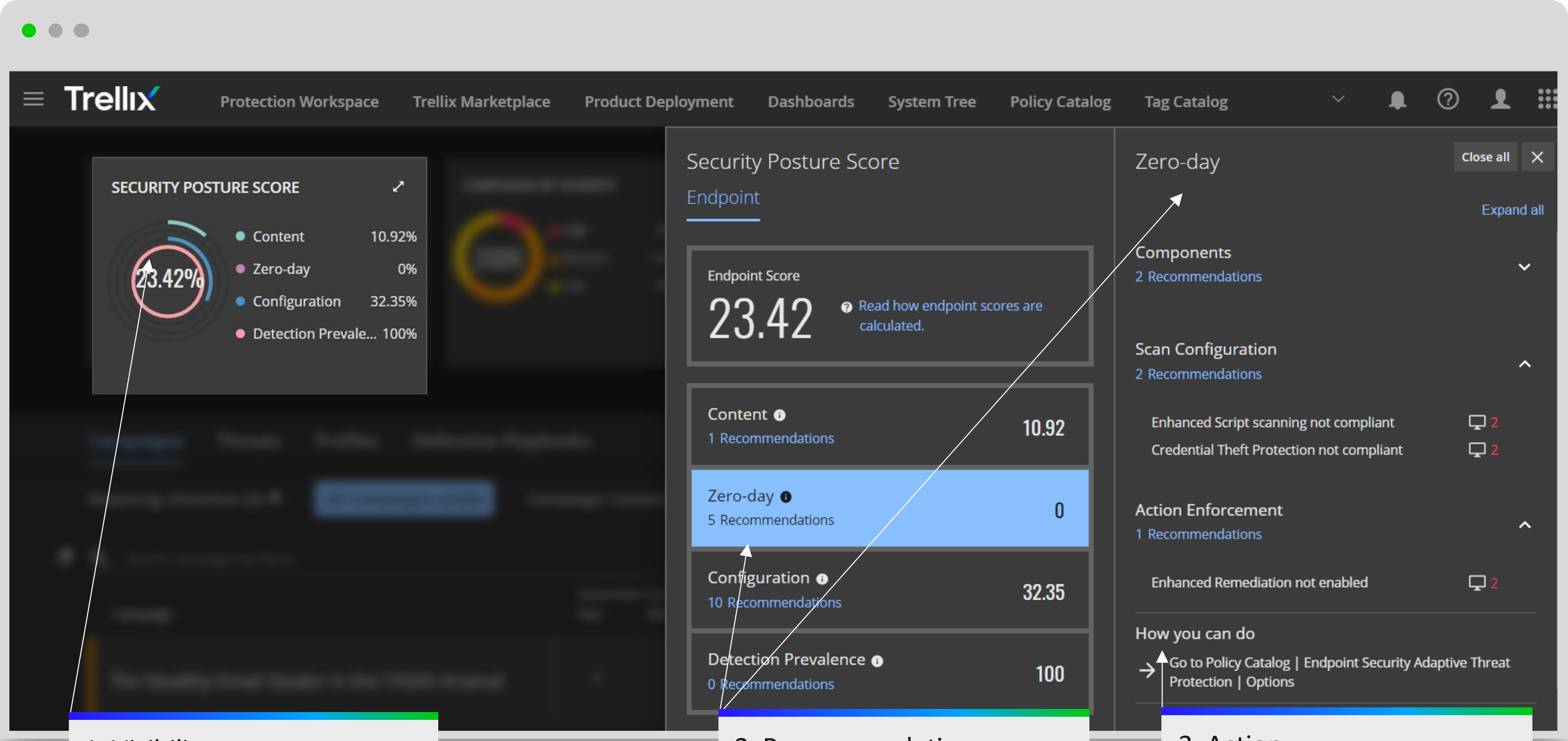
Rule
McAfee defense to detect malicious activity. (ENS, VSE, EDR, Endpoint, etc...)

```
Rule {
    Process {
        Include OBJECT_NAME { -v "winword.exe" }
        Include DLL_LOADED -name "ieframe" { -v 0x1 }
    }
    Target {
        Match SECTION {
            Include OBJECT_NAME { -v "mshtml.dll" }
        }
    }
}
```

Countermeasures for entry vector threats
https://kcm.trellix.com/corporate/index?page=content&id=KB91836

BEFORE
THE ATTACK

Optimize Endpoint Security Posture



SECURITY POSTURE SCORE

23.42%

● Content	10.92%
● Zero-day	0%
● Configuration	32.35%
● Detection Prevale...	100%

Security Posture Score

Endpoint

Endpoint Score

23.42 Read how endpoint scores are calculated.

Content 1 Recommendations	10.92
Zero-day 5 Recommendations	0
Configuration 10 Recommendations	32.35
Detection Prevalence 0 Recommendations	100

Zero-day

Components
2 Recommendations

Scan Configuration
2 Recommendations

Enhanced Script scanning not compliant	2
Credential Theft Protection not compliant	2

Action Enforcement
1 Recommendations

Enhanced Remediation not enabled	2

How you can do

→ Go to Policy Catalog | Endpoint Security Adaptive Threat Protection | Options

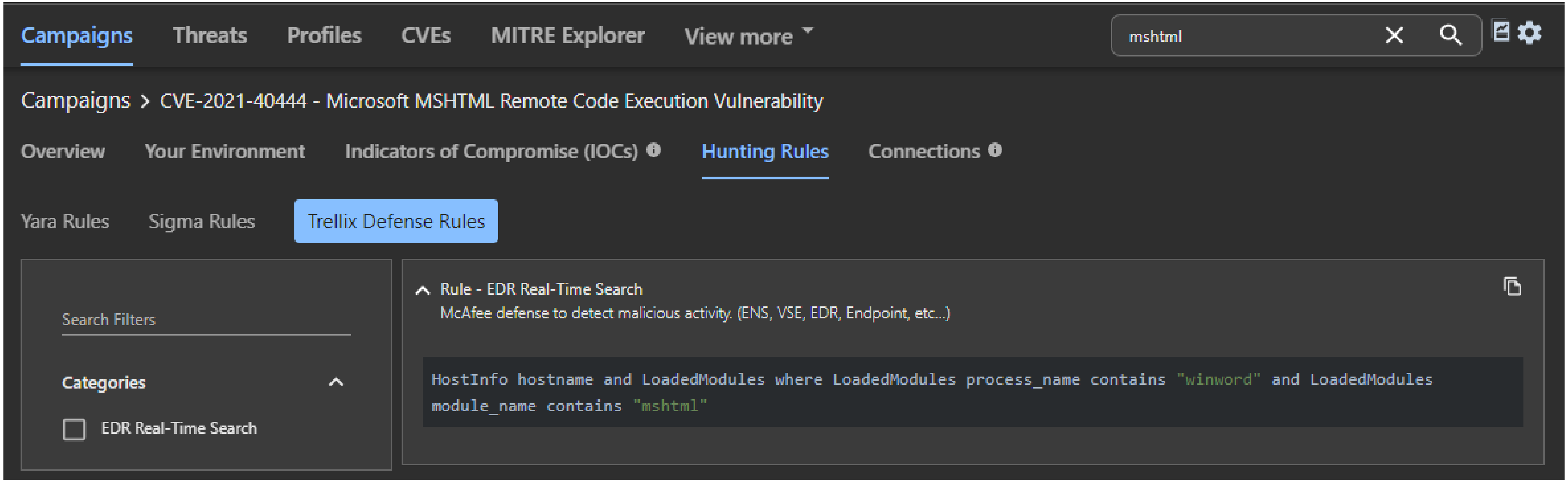
1. Visibility:
Zero-day protection not enabled

2. Recommendations:
five actions to improve Zero-day protection

3. Action:
jump to Policy Catalog

BEFORE *THE ATTACK*

Determine Potential Impact



Campaigns > CVE-2021-40444 - Microsoft MSHTML Remote Code Execution Vulnerability

□ EDR Real-Time Search

Rule - EDR Real-Time Search

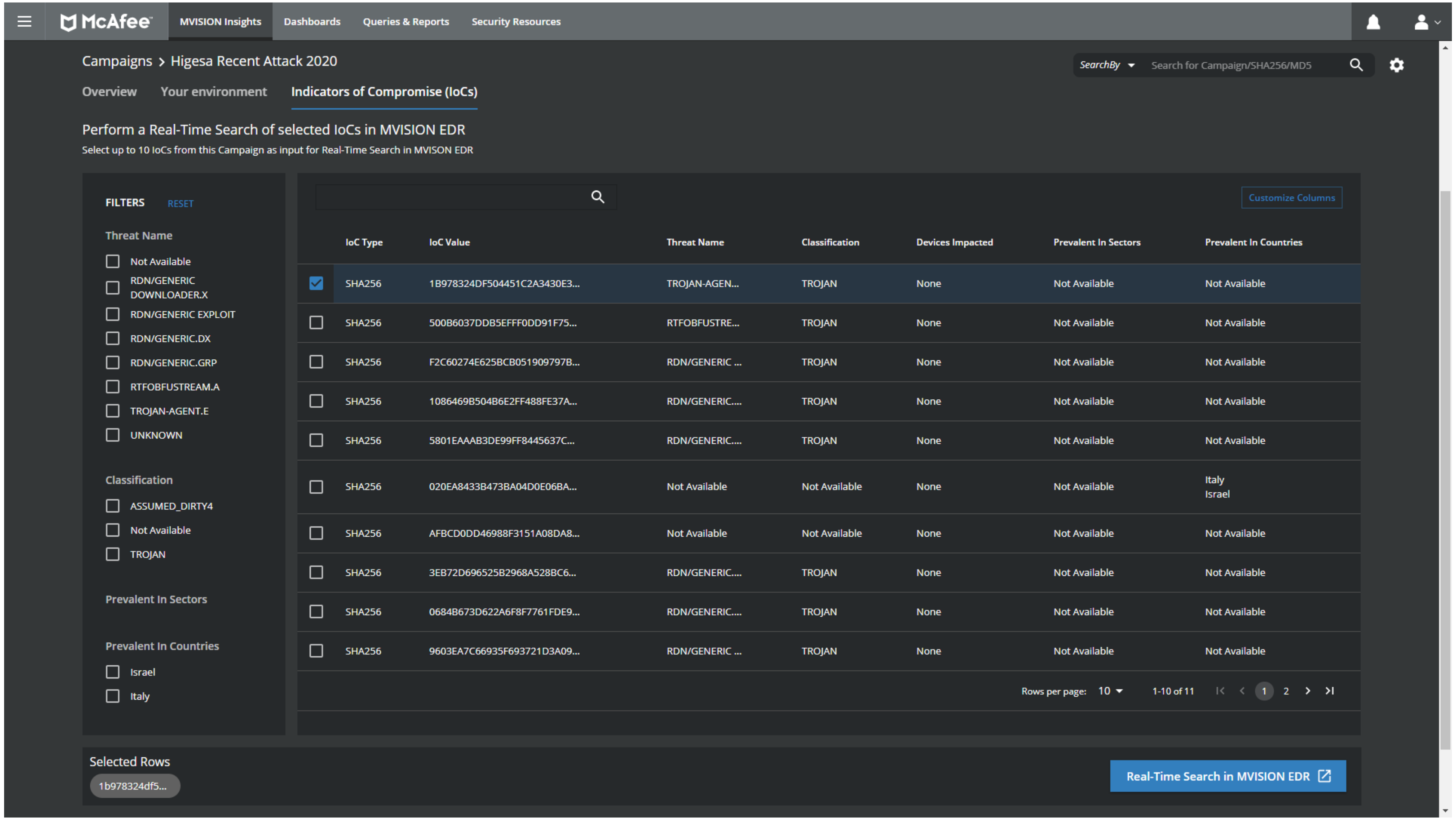
McAfee defense to detect malicious activity. (ENS, VSE, EDR, Endpoint, etc...)

```
HostInfo hostname and LoadedModules where LoadedModules process_name contains "winword" and LoadedModules
module_name contains "mshtml"
```

- Proactive Search
- Realtime queries from Insights to EDR
- Identify devices on risk

BEFORE
THE ATTACK

Dormant Threats



McAfee MVISION Insights | Dashboards | Queries & Reports | Security Resources

Campaigns > Higesa Recent Attack 2020

SearchBy ▾ Search for Campaign/SHA256/MD5

Overview | Your environment | Indicators of Compromise (IoCs)

Perform a Real-Time Search of selected IoCs in MVISION EDR

Select up to 10 IoCs from this Campaign as input for Real-Time Search in MVISION EDR

FILTERS RESET

Threat Name

- □ Not Available
- □ RDN/GENERIC DOWNLOADER.X
- □ RDN/GENERIC EXPLOIT
- □ RDN/GENERIC.DX
- □ RDN/GENERIC.GRP
- □ RTFOBFUSTREAM.A
- □ TROJAN-AGENT.E
- □ UNKNOWN

Classification

- □ ASSUMED_DIRTY4
- □ Not Available
- □ TROJAN

Prevalent In Sectors

Prevalent In Countries

- □ Israel
- □ Italy

Customize Columns

	IoC Type	IoC Value	Threat Name	Classification	Devices Impacted	Prevalent In Sectors	Prevalent In Countries
☑	SHA256	1B978324DF504451C2A3430E3...	TROJAN-AGEN...	TROJAN	None	Not Available	Not Available
□	SHA256	500B6037DDB5EFFF0DD91F75...	RTFOBFUSTRE...	TROJAN	None	Not Available	Not Available
□	SHA256	F2C60274E625BCB051909797B...	RDN/GENERIC ...	TROJAN	None	Not Available	Not Available
□	SHA256	1086469B504B6E2FF488FE37A...	RDN/GENERIC....	TROJAN	None	Not Available	Not Available
□	SHA256	5801EAAAB3DE99FF8445637C...	RDN/GENERIC....	TROJAN	None	Not Available	Not Available
□	SHA256	020EA8433B473BA04D0E06BA...	Not Available	Not Available	None	Not Available	Italy Israel
□	SHA256	AFBCD0DD46988F3151A08DA8...	Not Available	Not Available	None	Not Available	Not Available
□	SHA256	3EB72D696525B2968A528BC6...	RDN/GENERIC....	TROJAN	None	Not Available	Not Available
□	SHA256	0684B673D622A6F8F7761FDE9...	RDN/GENERIC....	TROJAN	None	Not Available	Not Available
□	SHA256	9603EA7C66935F693721D3A09...	RDN/GENERIC ...	TROJAN	None	Not Available	Not Available

Rows per page: 10 ▾ 1-10 of 11 |< < 1 2 > >|

Selected Rows

1b978324df5...

Real-Time Search in MVISION EDR

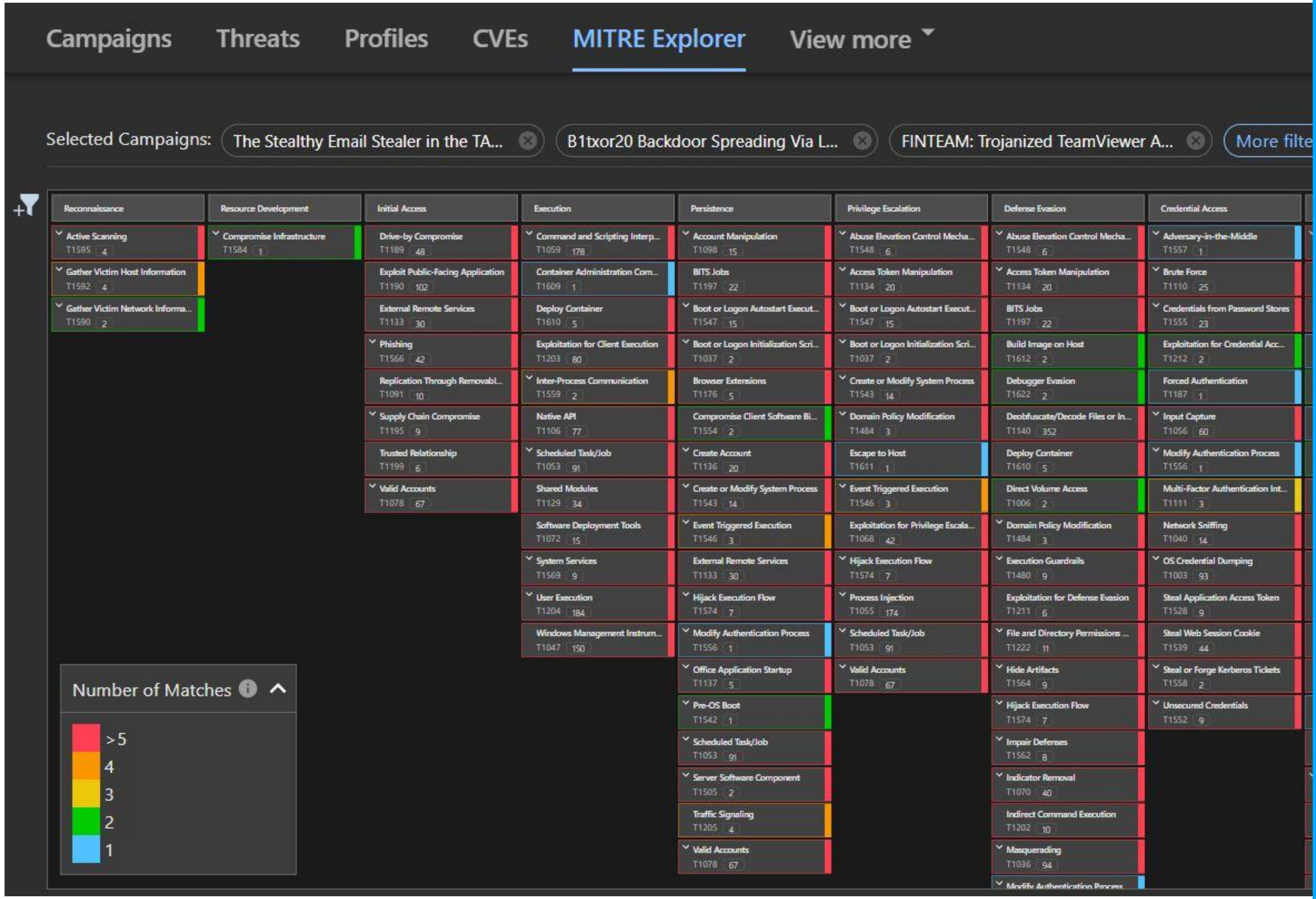
- Proactive Search
- Realtime queries from Insights to EDR
- Identify devices on risk

Trellix

BEFORE

THE ATTACK

Trellix Insights - MITRE Explorer

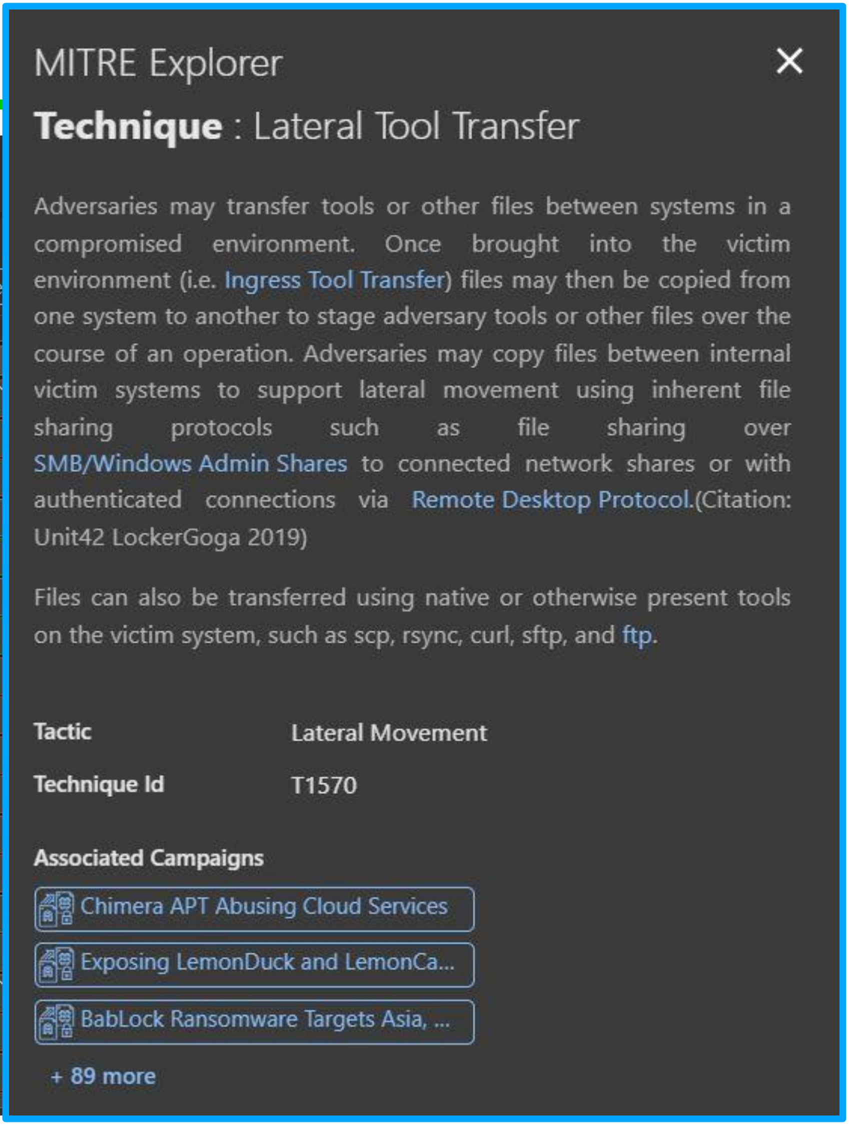


Selected Campaigns: The Stealthy Email Stealer in the TA... ⊗ B1txor20 Backdoor Spreading Via L... ⊗ FINTEAM: Trojanized TeamViewer A... ⊗ More filte

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Active Scanning T1595 4	Compromise Infrastructure T1584 1	Drive-by Compromise T1189 48	Command and Scripting Interp... T1059 178	Account Manipulation T1098 15	Abuse Elevation Control Mecha... T1548 6	Abuse Elevation Control Mecha... T1548 6	Adversary-in-the-Middle T1557 1
Gather Victim Host Information T1592 4		Exploit Public-Facing Application T1190 102	Container Administration Com... T1609 1	BITS Jobs T1197 22	Access Token Manipulation T1134 20	Access Token Manipulation T1134 20	Brute Force T1110 25
Gather Victim Network Informa... T1590 2		External Remote Services T1133 30	Deploy Container T1610 5	Boot or Logon Autostart Execut... T1547 15	Boot or Logon Autostart Execut... T1547 15	BITS Jobs T1197 22	Credentials from Password Stores T1555 23
		Phishing T1566 42	Exploitation for Client Execution T1203 80	Boot or Logon Initialization Scri... T1037 2	Boot or Logon Initialization Scri... T1037 2	Build Image on Host T1612 2	Exploitation for Credential Acc... T1212 2
		Replication Through Removabl... T1091 10	Inter-Process Communication T1559 2	Browser Extensions T1176 5	Create or Modify System Process T1543 14	Debugger Evasion T1622 2	Forced Authentication T1187 1
		Supply Chain Compromise T1195 9	Native API T1106 77	Compromise Client Software Bi... T1554 2	Domain Policy Modification T1484 3	Deobfuscate/Decode Files or In... T1140 352	Input Capture T1056 60
		Trusted Relationship T1199 6	Scheduled Task/Job T1053 91	Create Account T1136 20	Escape to Host T1611 1	Deploy Container T1610 5	Modify Authentication Process T1556 1
		Valid Accounts T1078 67	Shared Modules T1129 34	Create or Modify System Process T1543 14	Event Triggered Execution T1546 3	Direct Volume Access T1006 2	Multi-Factor Authentication Int... T1111 3
			Software Deployment Tools T1072 15	Event Triggered Execution T1546 3	Exploitation for Privilege Escala... T1068 42	Domain Policy Modification T1484 3	Network Sniffing T1040 14
			System Services T1569 9	External Remote Services T1133 30	Hijack Execution Flow T1574 7	Execution Guardrails T1480 9	OS Credential Dumping T1003 93
			User Execution T1204 184	Hijack Execution Flow T1574 7	Process Injection T1055 174	Exploitation for Defense Evasion T1211 6	Steal Application Access Token T1528 9
			Windows Management Instrum... T1047 150	Modify Authentication Process T1556 1	Scheduled Task/Job T1053 91	File and Directory Permissions ... T1222 11	Steal Web Session Cookie T1539 44
				Office Application Startup T1137 5	Valid Accounts T1078 67	Hide Artifacts T1564 9	Steal or Forge Kerberos Tickets T1558 2
				Pre-OS Boot T1542 1		Hijack Execution Flow T1574 7	Unsecured Credentials T1552 9
				Scheduled Task/Job T1053 91		Impair Defenses T1562 8	
				Server Software Component T1505 2		Indicator Removal T1070 40	
				Traffic Signaling T1205 4		Indirect Command Execution T1202 10	
				Valid Accounts T1078 67		Masquerading T1036 94	
						Modify Authentication Process	

Number of Matches

🟥	>5
🟧	4
🟨	3
🟩	2
🟦	1



MITRE Explorer

Technique : Lateral Tool Transfer

Adversaries may transfer tools or other files between systems in a compromised environment. Once brought into the victim environment (i.e. Ingress Tool Transfer) files may then be copied from one system to another to stage adversary tools or other files over the course of an operation. Adversaries may copy files between internal victim systems to support lateral movement using inherent file sharing protocols such as file sharing over SMB/Windows Admin Shares to connected network shares or with authenticated connections via Remote Desktop Protocol.(Citation: Unit42 LockerGoga 2019)

Files can also be transferred using native or otherwise present tools on the victim system, such as scp, rsync, curl, sftp, and ftp.

Tactic	Lateral Movement
Technique Id	T1570

Associated Campaigns

- Chimera APT Abusing Cloud Services
- Exposing LemonDuck and LemonCa...
- BabLock Ransomware Targets Asia, ...

+ 89 more

Trellix

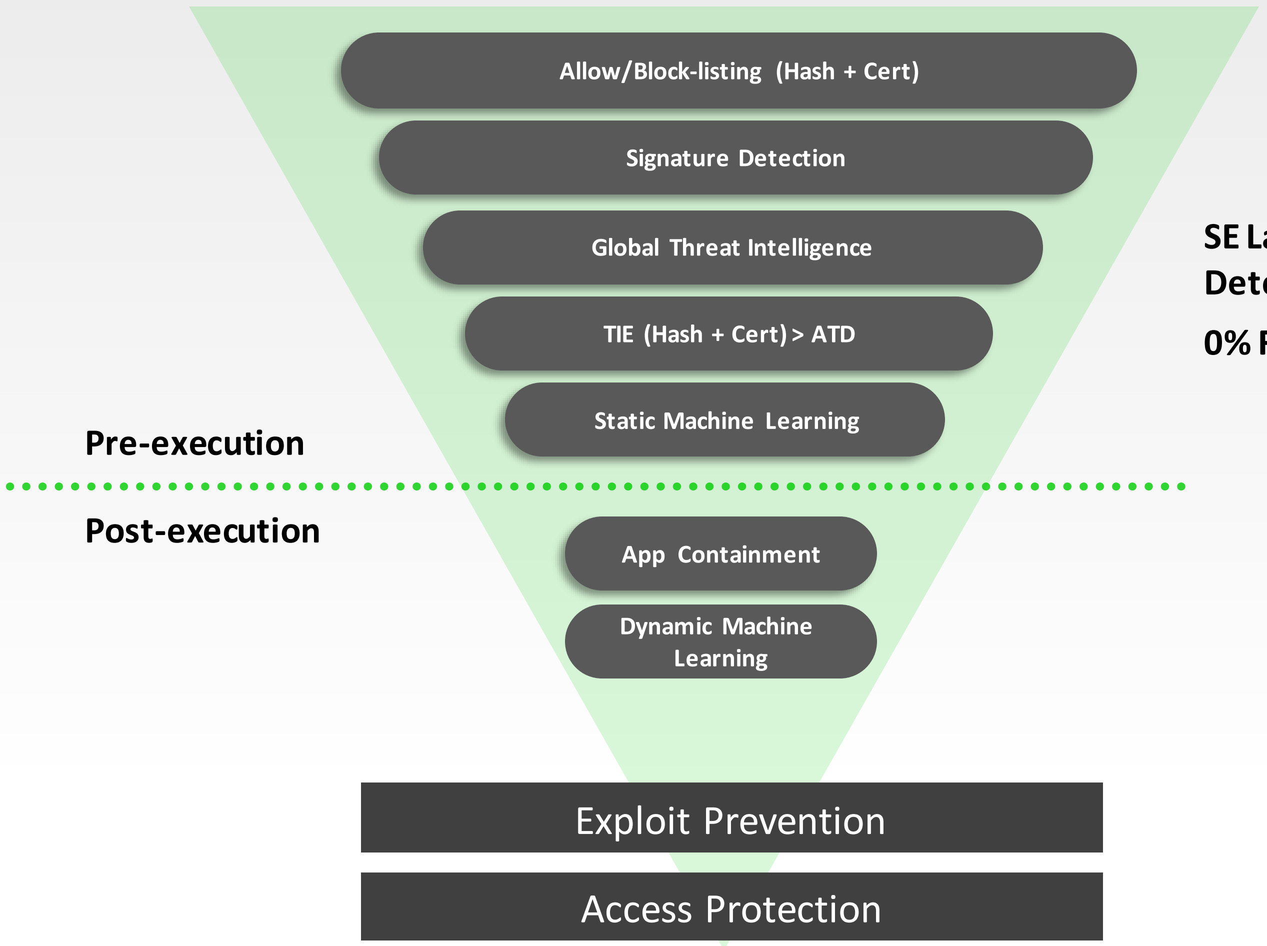
BEFORE
THE ATTACK

Proactive protection against sophisticated threats, like Ransomware

Proactive Attack Surface Reduction

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

Threat Prevention



Pre-execution

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

Post-execution

- App Containment
- Dynamic Machine Learning

Exploit Prevention

Access Protection

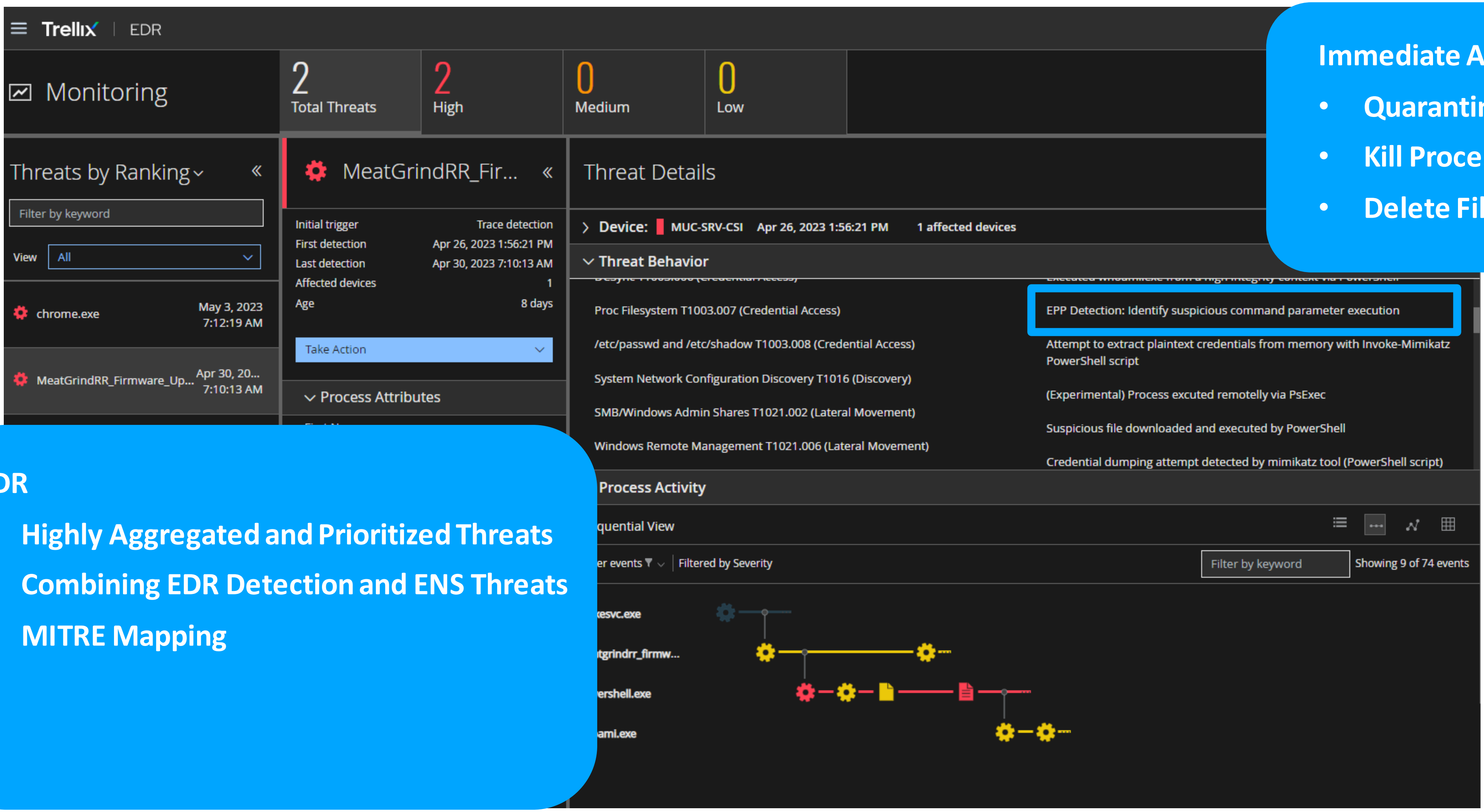
SE Labs 100% Detections

0% False Positives

Trellix

DURING
THE ATTACK

EDR
– Detect hidden threats



2	2	0	0
Total Threats	High	Medium	Low

chrome.exe	May 3, 2023 7:12:19 AM
MeatGrindRR_Firmware_Up...	Apr 30, 20... 7:10:13 AM

MeatGrindRR_Fir...

Initial trigger	Trace detection
First detection	Apr 26, 2023 1:56:21 PM
Last detection	Apr 30, 2023 7:10:13 AM
Affected devices	1
Age	8 days

Device: MUC-SRV-CSI Apr 26, 2023 1:56:21 PM 1 affected devices

Threat Behavior

Proc Filesystem T1003.007 (Credential Access)	EPP Detection: Identify suspicious command parameter execution
/etc/passwd and /etc/shadow T1003.008 (Credential Access)	Attempt to extract plaintext credentials from memory with Invoke-Mimikatz PowerShell script
System Network Configuration Discovery T1016 (Discovery)	(Experimental) Process excuted remotely via PsExec
SMB/Windows Admin Shares T1021.002 (Lateral Movement)	Suspicious file downloaded and executed by PowerShell
Windows Remote Management T1021.006 (Lateral Movement)	Credential dumping attempt detected by mimikatz tool (PowerShell script)

Immediate Actions

- **Quarantine**
- **Kill Process**
- **Delete File**

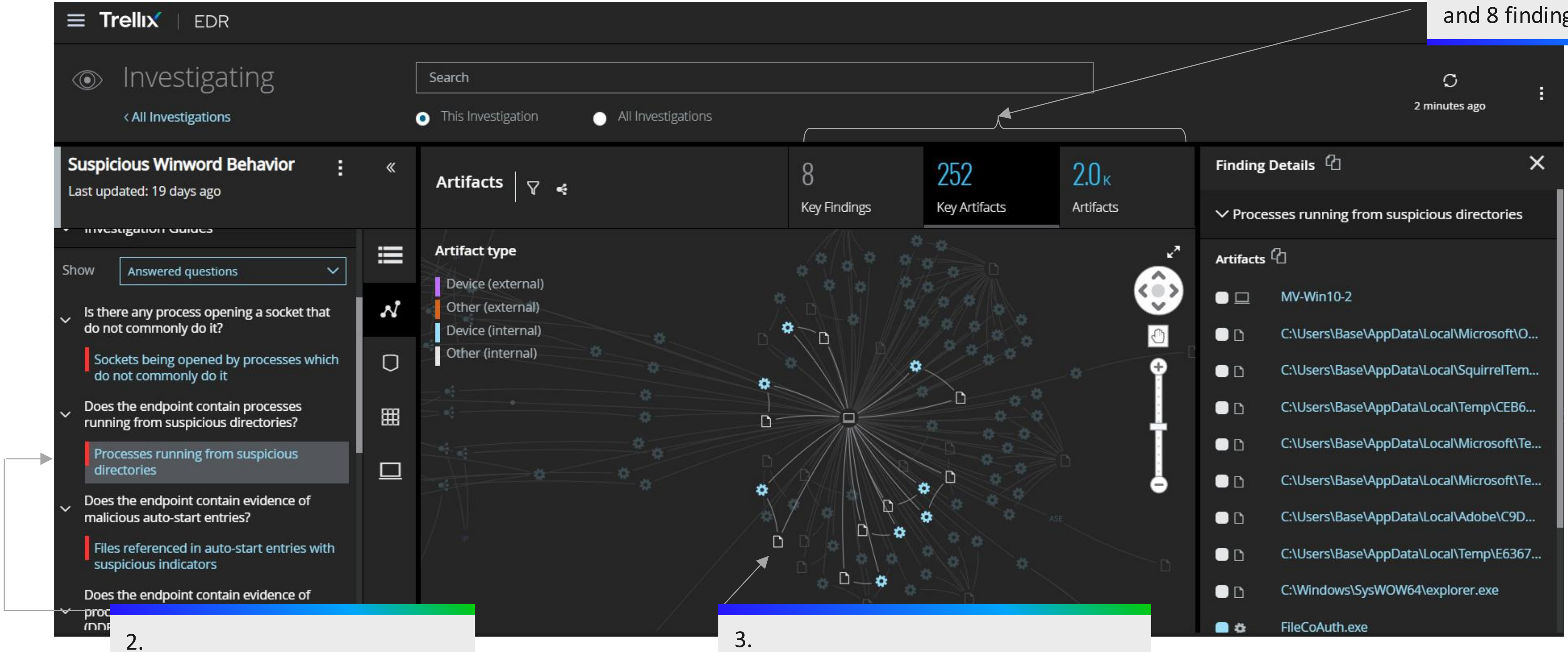
EDR

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

DURING
THE ATTACK

Optimize Alert Triage with AI-guided Investigations

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



Trellix | EDR

Investigating

‹ All Investigations

Search

● This Investigation ○ All Investigations

2 minutes ago

Suspicious Winword Behavior

Last updated: 19 days ago

Investigation Guides

Show: Answered questions

Is there any process opening a socket that do not commonly do it?

- Sockets being opened by processes which do not commonly do it

Does the endpoint contain processes running from suspicious directories?

- Processes running from suspicious directories

Does the endpoint contain evidence of malicious auto-start entries?

- Files referenced in auto-start entries with suspicious indicators

Does the endpoint contain evidence of proc...

Artifacts

8	252	2.0K
Key Findings	Key Artifacts	Artifacts

Artifact type

- Device (external)
- Other (external)
- Device (internal)
- Other (internal)

Finding Details

Processes running from suspicious directories

Artifacts

- MV-Win10-2
- C:\Users\Base\AppData\Local\Microsoft\O...
- C:\Users\Base\AppData\Local\SquirrelTem...
- C:\Users\Base\AppData\Local\Temp\CEB6...
- C:\Users\Base\AppData\Local\Microsoft\Te...
- C:\Users\Base\AppData\Local\Microsoft\Te...
- C:\Users\Base\AppData\Local\Adobe\C9D...
- C:\Users\Base\AppData\Local\Temp\E6367...
- C:\Windows\SysWOW64\explorer.exe
- FileCoAuth.exe

2.
Trellix automatically provides answers to the SOC analysts

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

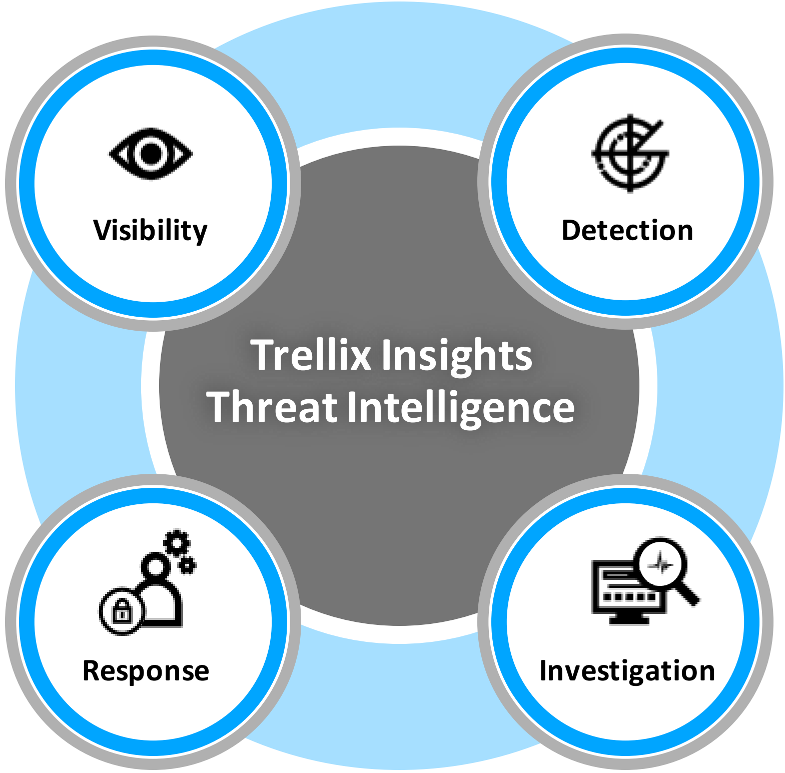
DURING
THE ATTACK

Effective endpoint alert triage and prioritization

Simpler investigation workflows

- Broad Visibility
- Flexible Retention
- Always-on data collection

- Data Visualization & Search
- Robust Response



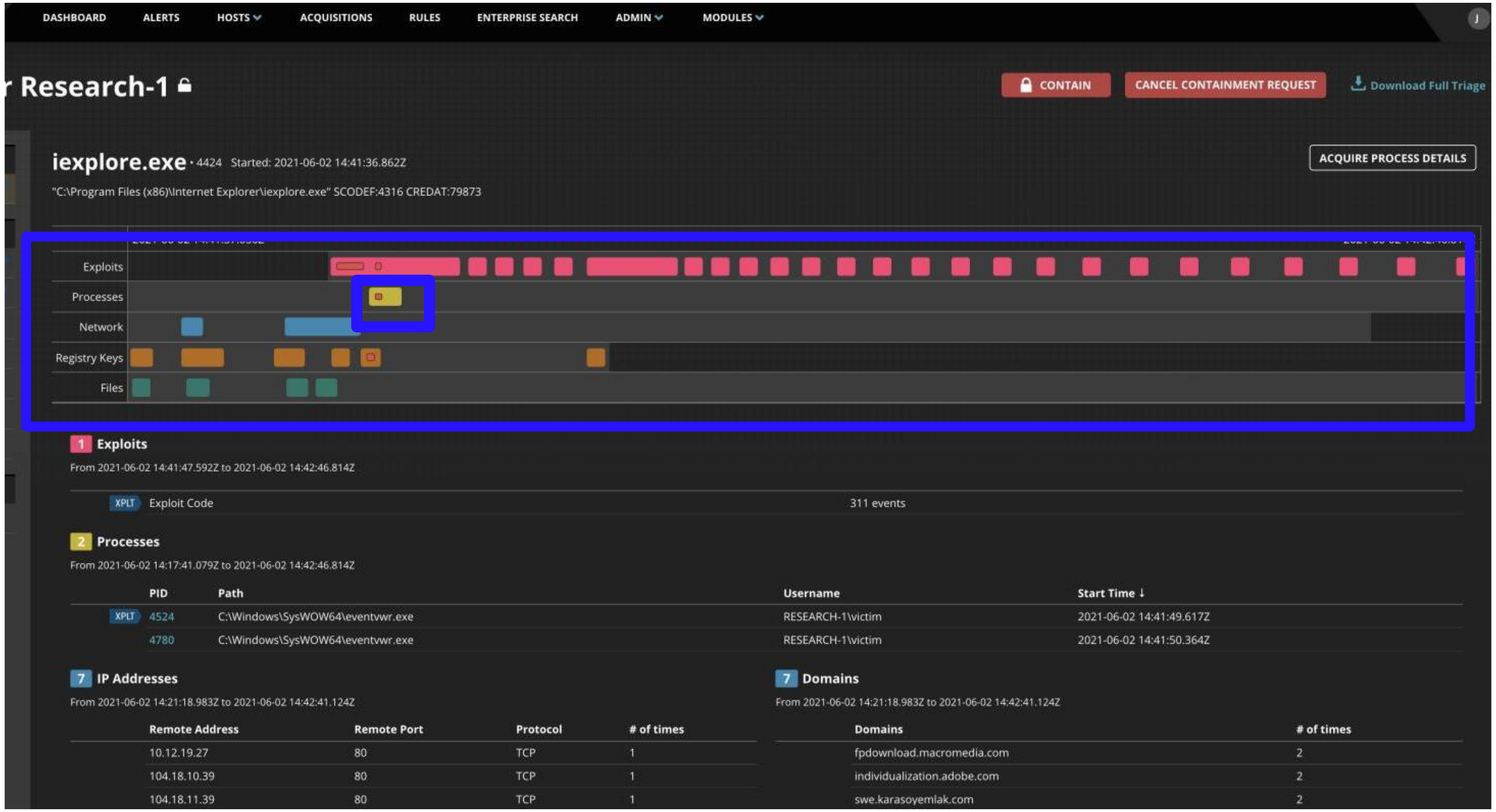
- File and Fileless threats
- MITRE framework driven detection and mapping

- Force-multiply expertise with AI
- Automatic Alert Triage

AFTER *THE ATTACK*

Alert Timeline and Triage Viewer

- Show timeline of alerts
- Simplifies investigation
- Filters results based on selection
- Red Dot shows indicator trigger
- Full triage download for deeper analysis



r Research-1

iexplore.exe · 4424 Started: 2021-06-02 14:41:36.862Z

"C:\Program Files (x86)\Internet Explorer\iexplore.exe" SCODEF:4316 CREDAT:79873

1 Exploits

From 2021-06-02 14:41:47.592Z to 2021-06-02 14:42:46.814Z

XPLT	Exploit Code	311 events

2 Processes

From 2021-06-02 14:17:41.079Z to 2021-06-02 14:42:46.814Z

	PID	Path	Username	Start Time ↓
XPLT	4524	C:\Windows\SysWOW64\eventvwr.exe	RESEARCH-1\victim	2021-06-02 14:41:49.617Z
	4780	C:\Windows\SysWOW64\eventvwr.exe	RESEARCH-1\victim	2021-06-02 14:41:50.364Z

7 IP Addresses

From 2021-06-02 14:21:18.983Z to 2021-06-02 14:42:41.124Z

Remote Address	Remote Port	Protocol	# of times
10.12.19.27	80	TCP	1
104.18.10.39	80	TCP	1
104.18.11.39	80	TCP	1

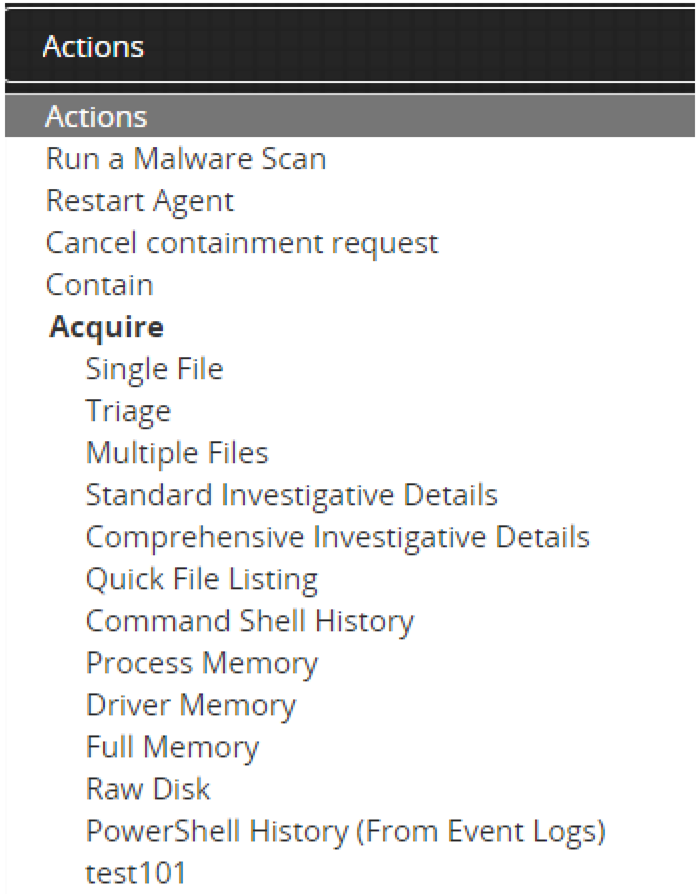
7 Domains

From 2021-06-02 14:21:18.983Z to 2021-06-02 14:42:41.124Z

Domains	# of times
fpdownload.macromedia.com	2
individualization.adobe.com	2
swe.karasoyemlak.com	2

AFTER
THE ATTACK

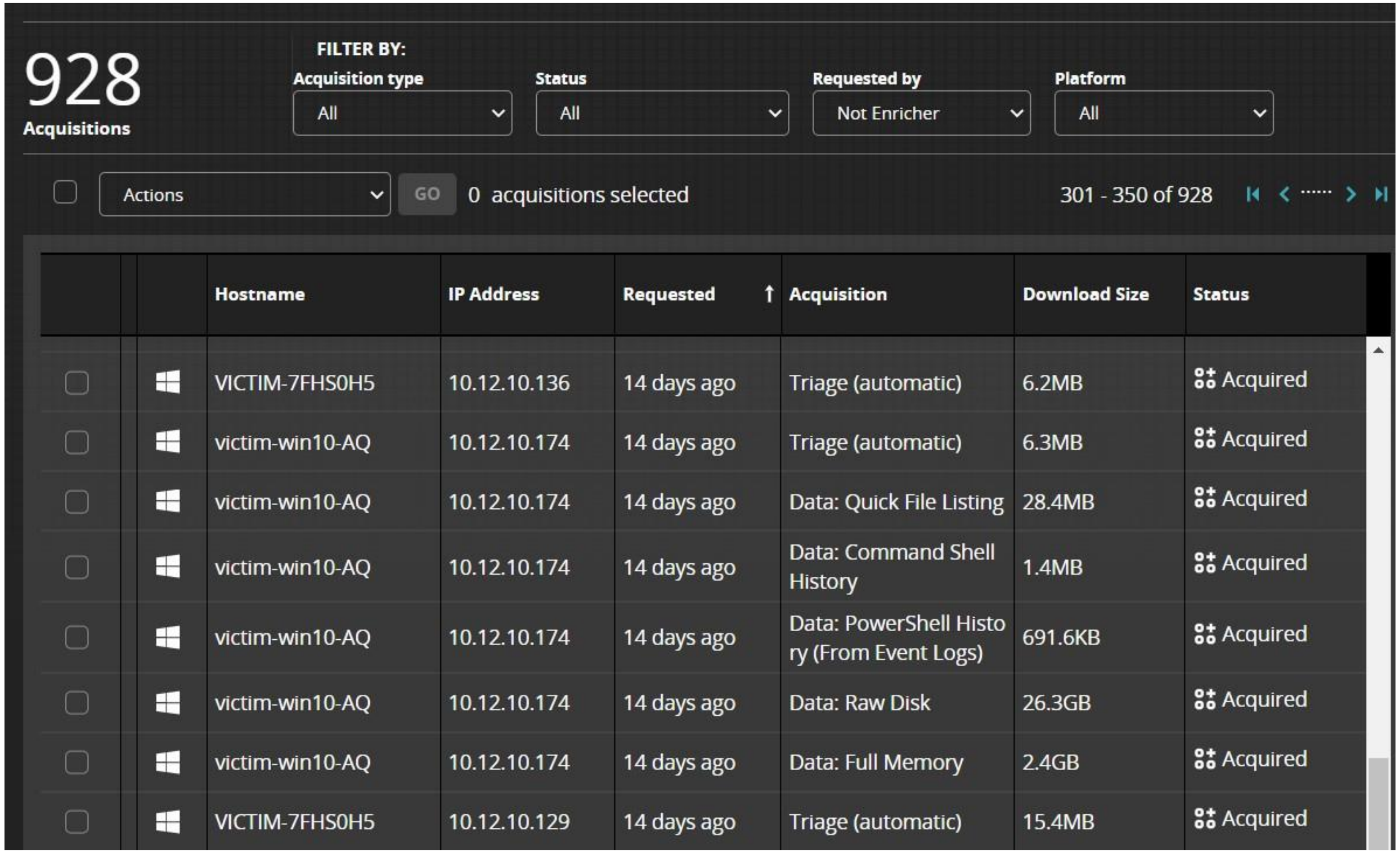
Data Acquisitions



Actions

Actions

- Run a Malware Scan
- Restart Agent
- Cancel containment request
- Contain
- **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)
  - test101



928 Acquisitions

FILTER BY:

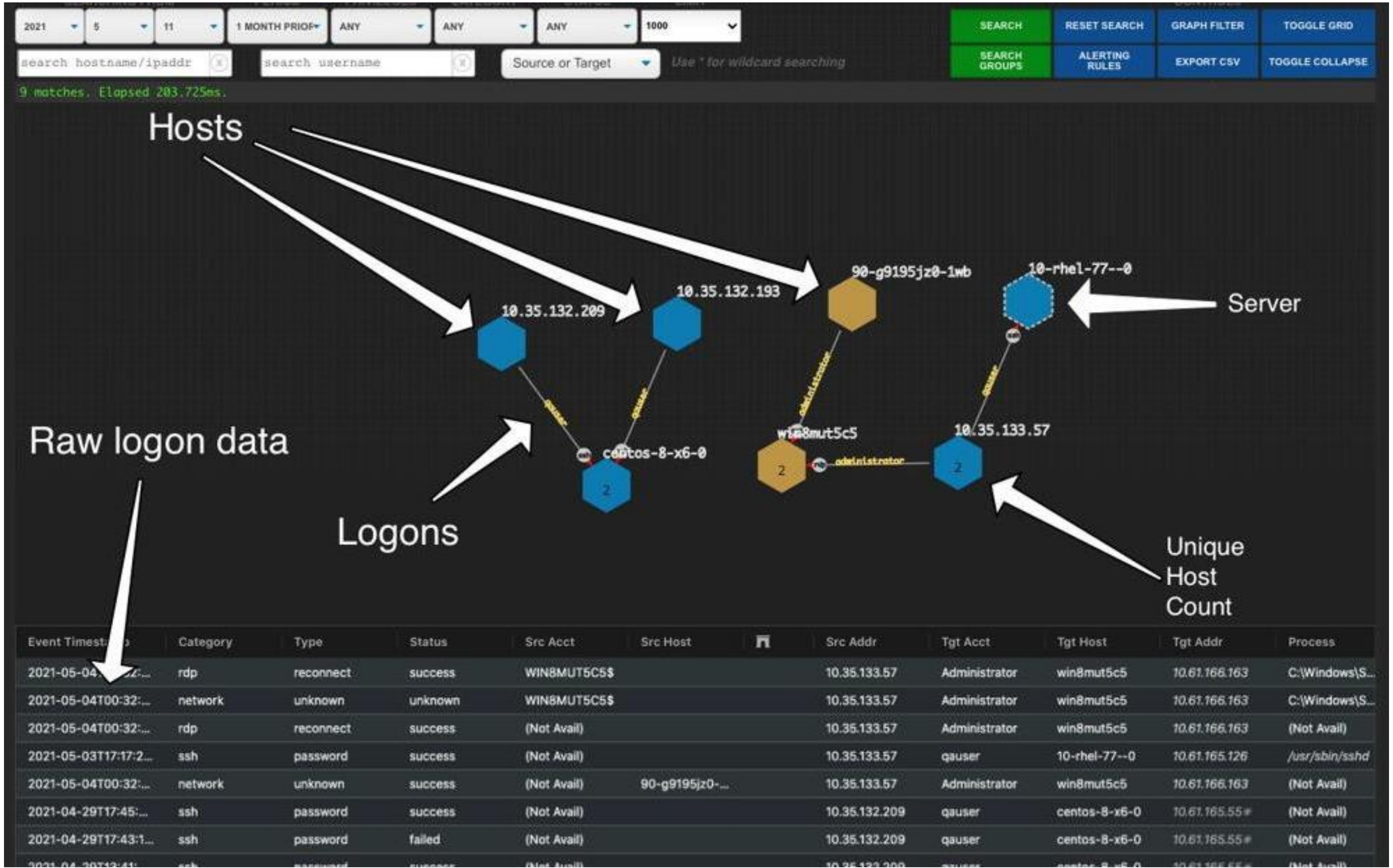
Acquisition type: All
Status: All
Requested by: Not Enricher
Platform: All

☐ Actions GO 0 acquisitions selected 301 - 350 of 928

		Hostname	IP Address	Requested ↑	Acquisition	Download Size	Status
☐		VICTIM-7FHSOH5	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-7FHSOH5	10.12.10.129	14 days ago	Triage (automatic)	15.4MB	Acquired

AFTER
THE ATTACK

Logon Tracker
 - Lateral Movement Detection



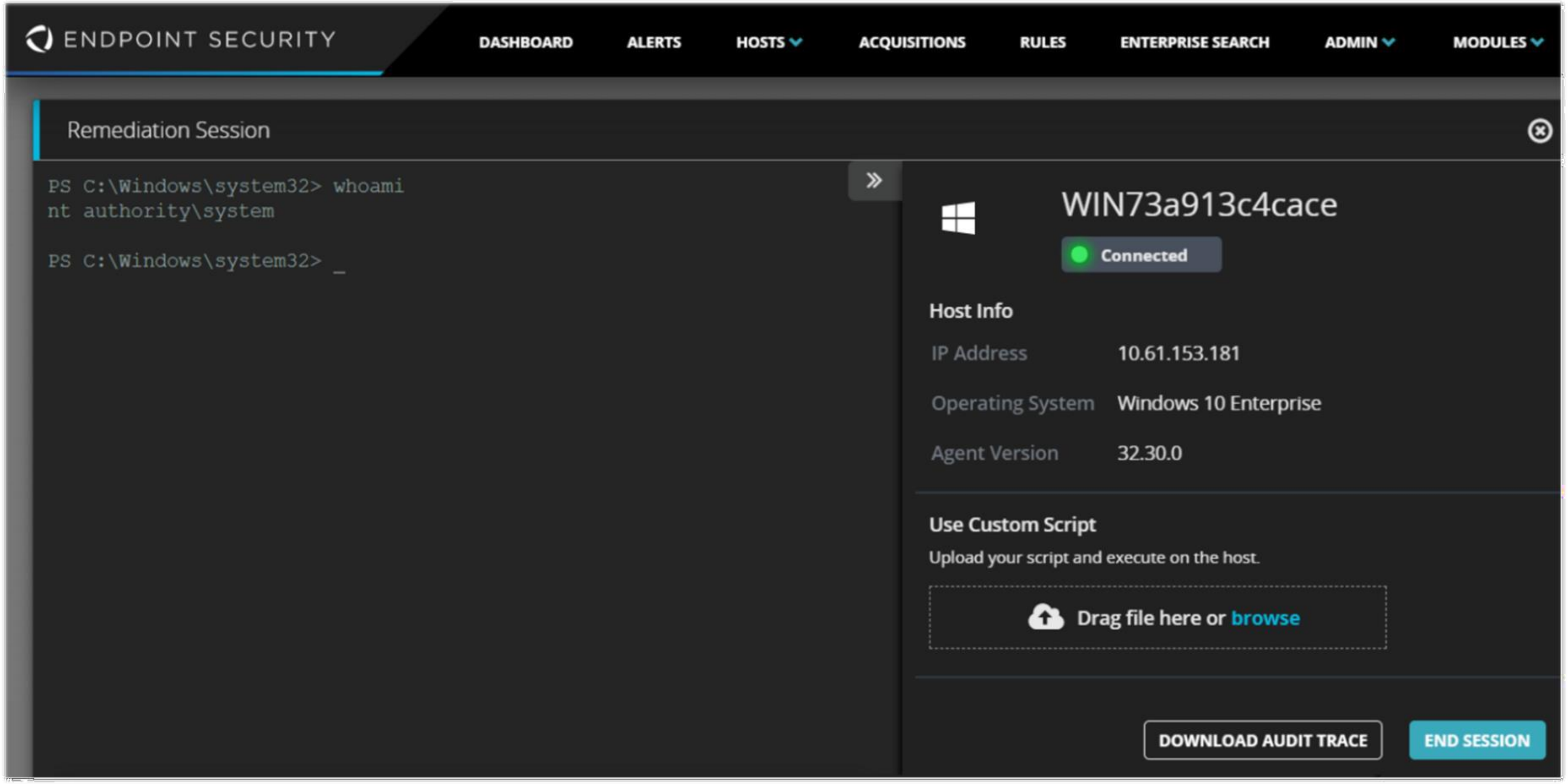
```
9 matches. Elapsed 203.725ms.
```

Event Timestamp	Category	Type	Status	Src Acct	Src Host		Src Addr	Tgt Acct	Tgt Host	Tgt Addr	Process
2021-05-04T00:32:...	rdp	reconnect	success	WIN8MUT5C5$			10.35.133.57	Administrator	win8mut5c5	10.61.166.163	C:\Windows\S...
2021-05-04T00:32:...	network	unknown	unknown	WIN8MUT5C5$			10.35.133.57	Administrator	win8mut5c5	10.61.166.163	C:\Windows\S...
2021-05-04T00:32:...	rdp	reconnect	success	(Not Avail)			10.35.133.57	Administrator	win8mut5c5	10.61.166.163	(Not Avail)
2021-05-03T17:17:2...	ssh	password	success	(Not Avail)			10.35.133.57	qauser	10-rhel-77--0	10.61.165.126	/usr/sbin/sshd
2021-05-04T00:32:...	network	unknown	success	(Not Avail)	90-g9195jz0-...		10.35.133.57	Administrator	win8mut5c5	10.61.166.163	(Not Avail)
2021-04-29T17:45:...	ssh	password	success	(Not Avail)			10.35.132.209	qauser	centos-8-x6-0	10.61.165.55#	(Not Avail)
2021-04-29T17:43:1...	ssh	password	failed	(Not Avail)			10.35.132.209	qauser	centos-8-x6-0	10.61.165.55#	(Not Avail)
2021-04-29T13:41:...	ssh	password	success	(Not Avail)			10.35.132.209	qauser	centos-8-x6-0	10.61.165.55#	(Not Avail)

- Analysis typically starts with a clue (an account or a host)
- Essential to gather historical logon data
- Account, host, and logon metadata speeds up analysis

AFTER THE ATTACK

Host Remediation – Remote Shell



Remediation Session

```
PS C:\Windows\system32> whoami
nt authority\system

PS C:\Windows\system32> _
```

WIN73a913c4cace

Connected

Host Info

IP Address 10.61.153.181

Operating System Windows 10 Enterprise

Agent Version 32.30.0

Use Custom Script

Upload your script and execute on the host.

- Remote Console
- Audited
- Kill processes
- Remove Files
- Scriptable

AFTER
THE ATTACK

Rapid response capabilities to contain attacks

Root cause understanding, and remediation

Investigation

Enterprise Search

Forensic Acquisition

Attack Summary and Audit Viewer

Response

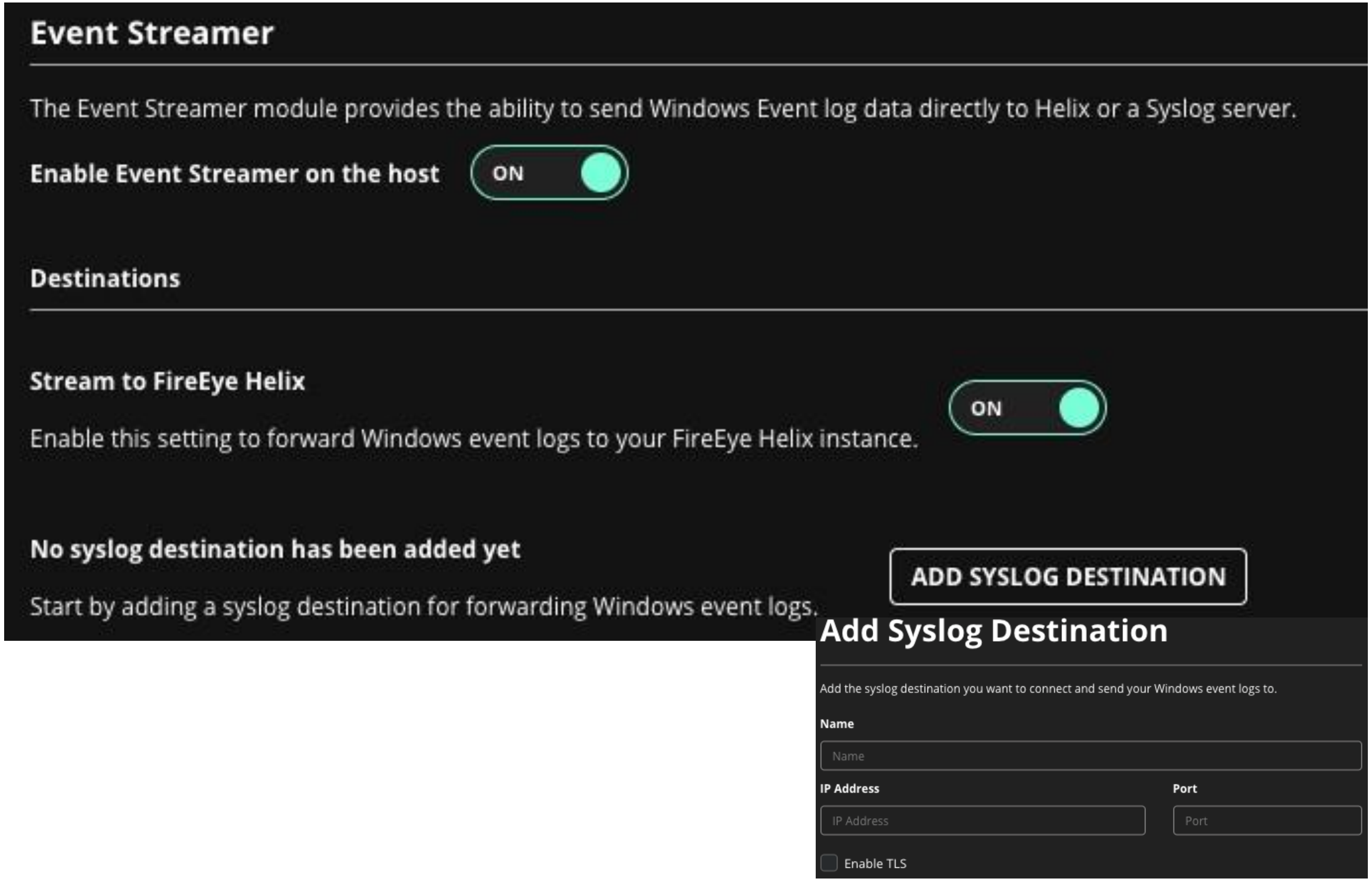
Quick Containment

Scalability

Off Network Investigation

AFTER
THE ATTACK

Windows Event Log Forwarding



Event Streamer

The Event Streamer module provides the ability to send Windows Event log data directly to Helix or a Syslog server.

Enable Event Streamer on the host ON

Destinations

Stream to FireEye Helix

Enable this setting to forward Windows event logs to your FireEye Helix instance. ON

No syslog destination has been added yet

Start by adding a syslog destination for forwarding Windows event logs.

Add Syslog Destination

Add the syslog destination you want to connect and send your Windows event logs to.

Name

Name

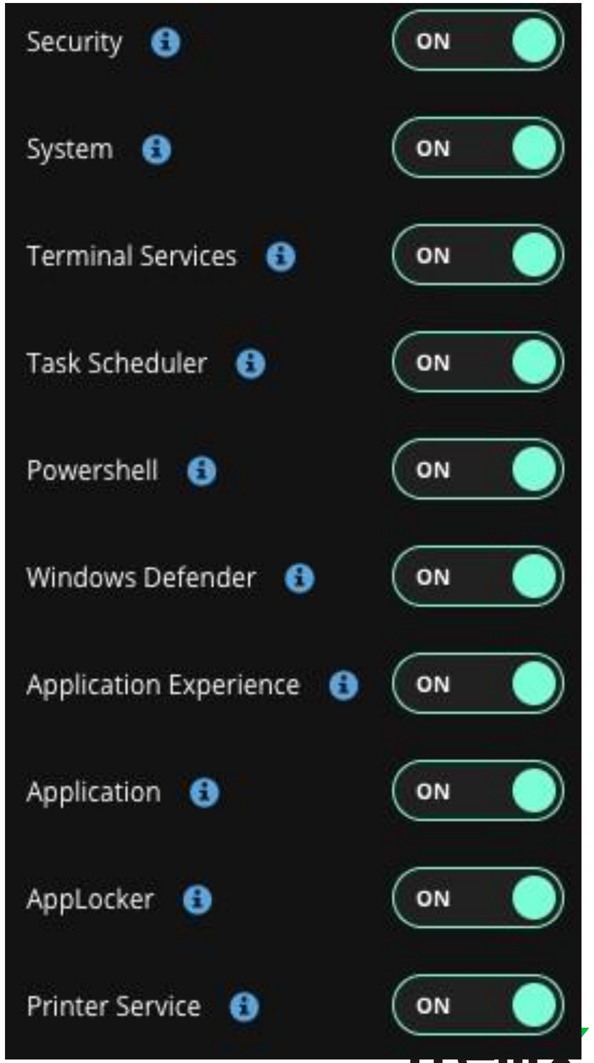
IP Address

IP Address

Port

Port

□ Enable TLS



Security ON

System ON

Terminal Services ON

Task Scheduler ON

Powershell ON

Windows Defender ON

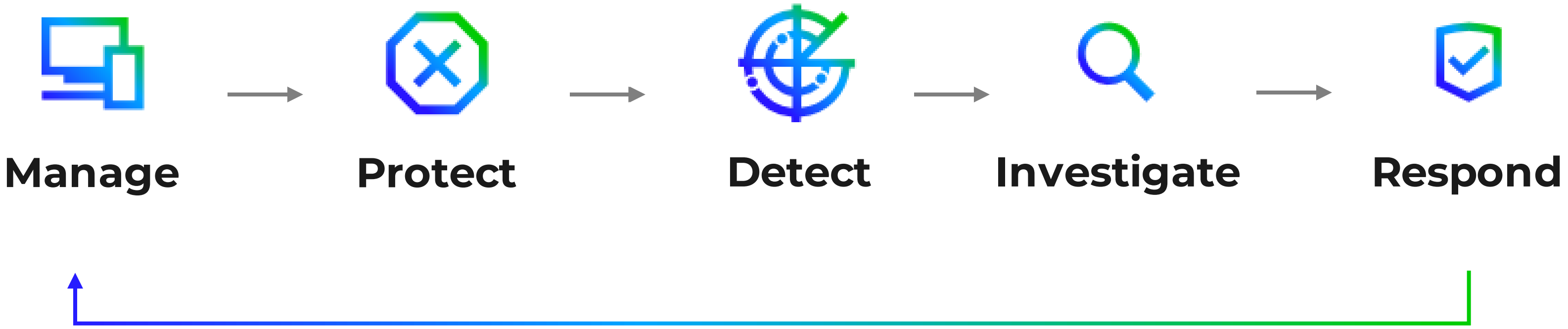
Application Experience ON

Application ON

AppLocker ON

Printer Service ON

Trellix Endpoint Security Solution



Visibility & Control over the full life cycle of all your Endpoints

An Endpoint Security
Powerhouse

Optimize all your Endpoints Protection

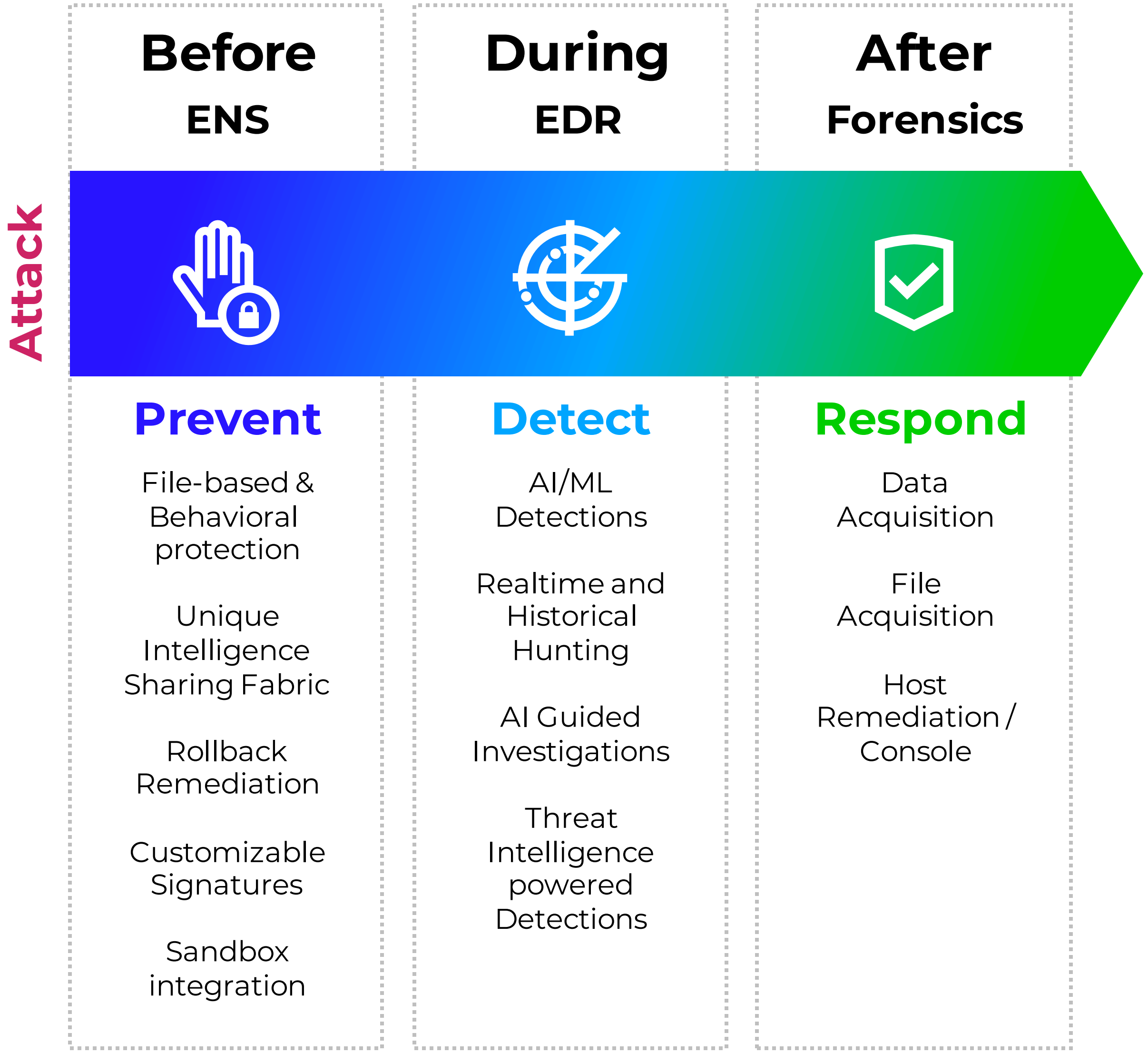
- Manage at Enterprise Scale, on-prem & cloud
- Desktop, Servers & Fixed functions devices
- Proactively Protect against sophisticated threats

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

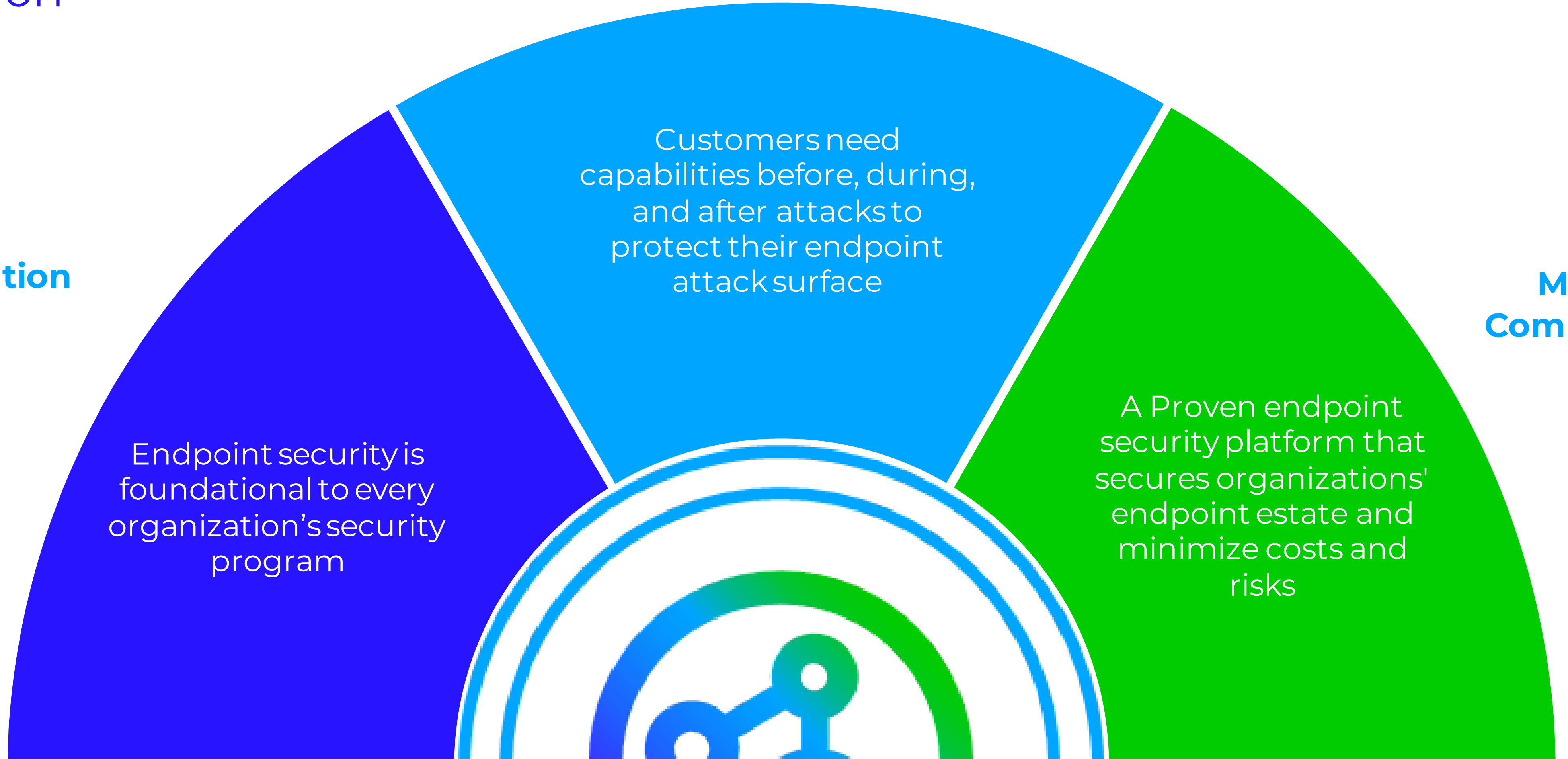


Before	During	After
ENS	EDR	Forensics
Prevent	Detect	Respond
File-based & Behavioral protection Unique Intelligence Sharing Fabric Rollback Remediation Customizable Signatures Sandbox integration	AI/ML Detections Realtime and Historical Hunting AI Guided Investigations Threat Intelligence powered Detections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

Trellix

Endpoints are foundational to cybersecurity

... And we offer a fully-featured solution



Before, During & After the Attack

Customers need capabilities before, during, and after attacks to protect their endpoint attack surface

A Foundation

Endpoint security is foundational to every organization’s security program

Modern & Comprehensive

A Proven endpoint security platform that secures organizations' endpoint estate and minimize costs and risks

Trellix Endpoint

New SKU for Comprehensive Endpoint Coverage

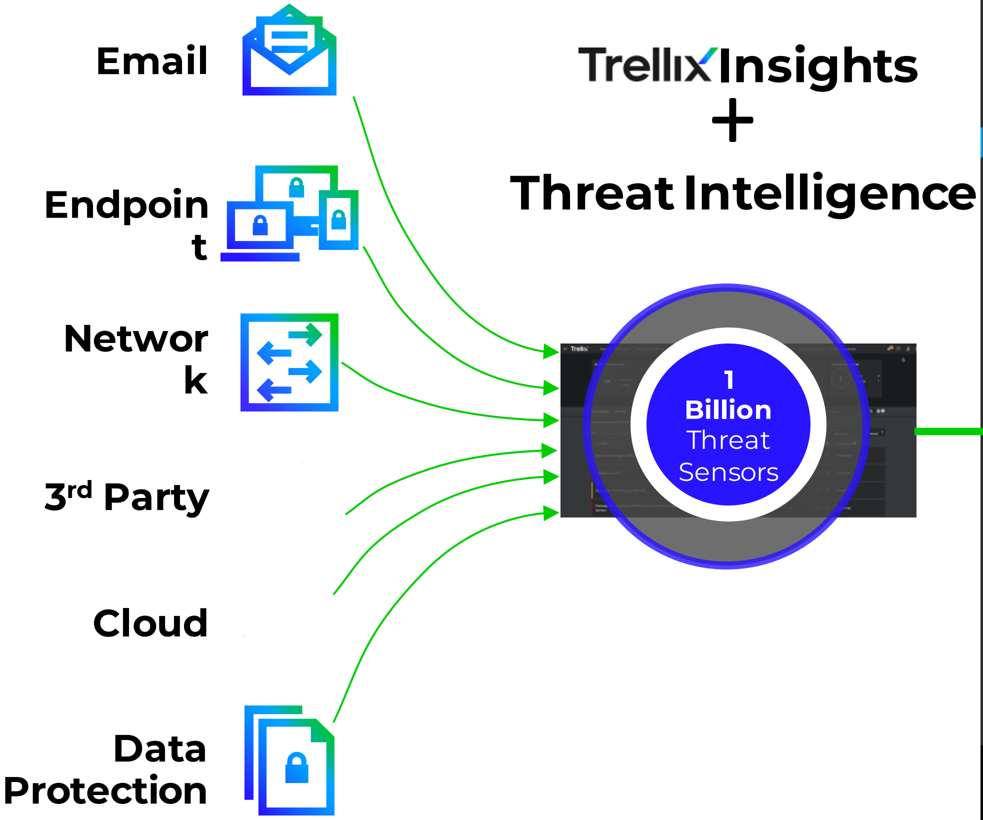
New SKU (TRXE - March 2023)	Rich Protection	Investigation & Response	Adv. Forensics	Threat Intelligence Prioritization	Threat Response at Scale	Attack Surface Reduction
Component	ENS	EDR	Forensics	Insights	TIE	App/Device Control
SaaS and On-prem Mgmt						
Trellix Endpoint	X	X	X	X	X	X

Trellix

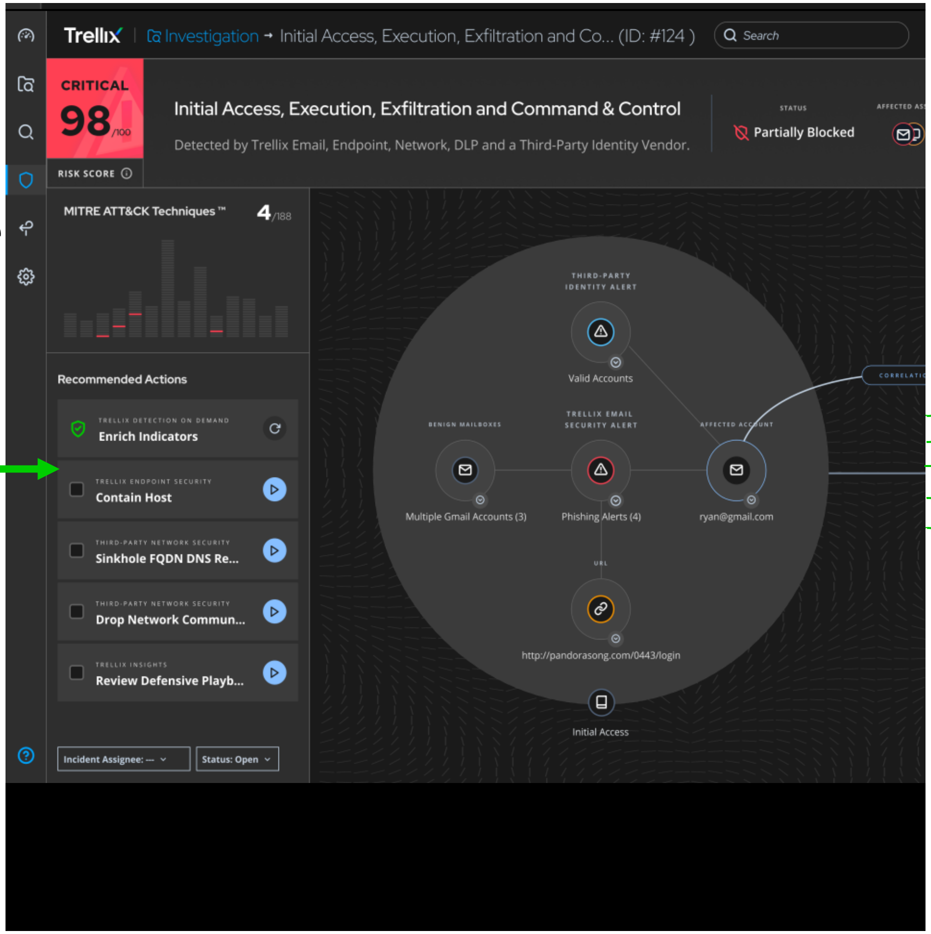
Security Tools

Trellix XDR Platform

Automated Responses and Playbooks



Trellix Insights
+
Threat Intelligence



Investigation → Initial Access, Execution, Exfiltration and Co... (ID: #124)

CRITICAL
98/100
RISK SCORE

Initial Access, Execution, Exfiltration and Command & Control

Detected by Trellix Email, Endpoint, Network, DLP and a Third-Party Identity Vendor.

STATUS
Partially Blocked

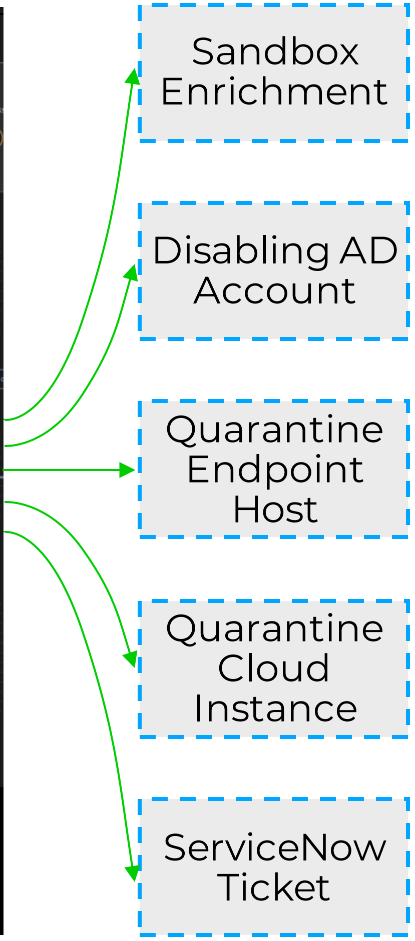
AFFECTED AS

MITRE ATT&CK Techniques ™ 4/188

Recommended Actions

- TRELLIX DETECTION ON DEMAND
  Enrich Indicators
- □ TRELLIX ENDPOINT SECURITY
  Contain Host
- □ THIRD-PARTY NETWORK SECURITY
  Sinkhole FQDN DNS Re...
- □ THIRD-PARTY NETWORK SECURITY
  Drop Network Commun...
- □ TRELLIX INSIGHTS
  Review Defensive Playb...

Incident Assignee: — ⌄ Status: Open ⌄



Trellix

Use Cases

Endpoint Security

Key Use Cases

Endpoints are a constant target for attackers

1 **Complex Endpoint Attack Surface**

Gaps in coverage and misconfigurations can lead to increasing cost and risk of attacker dwell time and costly incidents

2 **Ransomware attacks cause damage**

Ransomware quickly blocks access to systems and data causing impact to users and organizations

3 **Inefficient Endpoint Alert Triage**

Noisy alerting and false positives increases alert fatigue and the risk of critical alerts being ignored, leading to costly incidents.

4 **Impactful Endpoint Incidents**

Endpoint incidents must be contained, and scope and root cause must be understood to resolve and prevent incidents from reoccurring

Who Cares?

Foundational Endpoint Security for Strategic Security Initiatives

Organization Profiles:

Low to Medium Maturity – Manage and Protect Focus

- Minimal resources dedicated to security
- SLAs and business uptime the priority
- Industries/geos with on-prem mandate
- Starting a SOC initiative

High Maturity – Detect, Investigate, and Respond Focus

- Considers endpoints as fundamental to the SOC
- Seeking SOC excellence
- Striving for more proactive security posture

Key Persona Concerns:

CISO

Economic Buyer

- Minimize Risk
- Minimize Cost

SOC Manager / Security Architect

Technical Buyer

- Operational Efficiency
- Metrics: E.g. MTTD, MTTR
- Staff Effectiveness

SOC Analyst

Influencer

- Daily successful execution
  - Deploy and Configure
  - Detect and Respond

Trellix

Complex Endpoint Attack Surface

1

Optimize Protection on Endpoints

Trellix Promise

CISO

Economic Buyer

Minimize cost and risk protecting endpoints in complex environments with consistent security baselines.

SOC Manager / Security Architect

Technical Buyer

Manage and protect the entire endpoint estate efficiently and effectively.

Why Trellix?

- Broad endpoint coverage, on-prem and cloud management
- Enterprise management and automation at scale
- Security posture optimization with threat intelligence

Trellix

Use Case: Complex Attack Surface

1

Optimize Protection

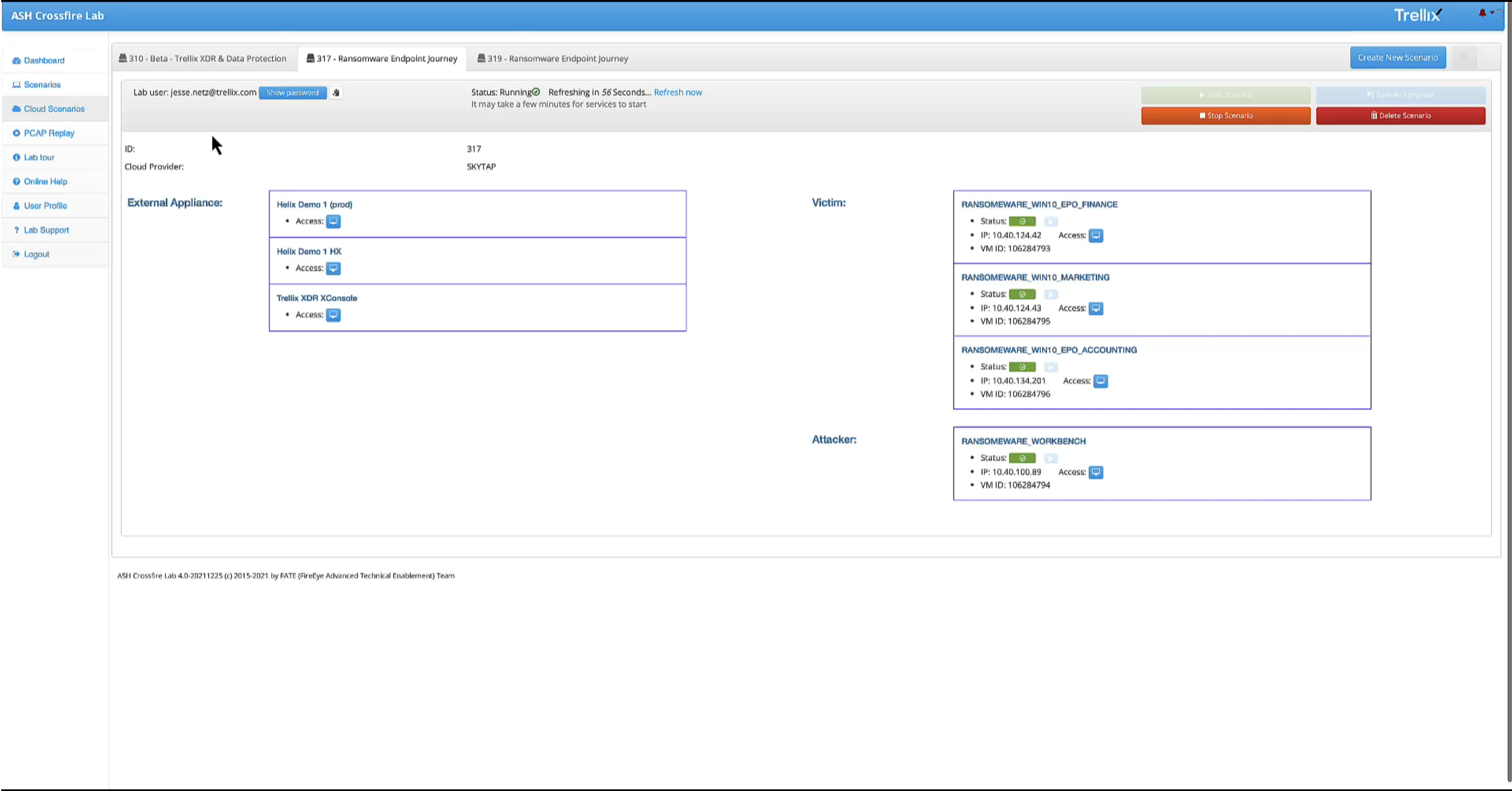
Scenario	Result	Solution
An organization isn't aware of what protection controls have been configured in their endpoint estate. They haven't enabled zero-day protection in ENS.	An organization is hit by ransomware and deals with costly impact due to insufficient security being enabled.	Trellix Insights shows security posture status and guides customers to where they can enable advanced protections that are part of ENS.

Trellix

Demo

Complex Attack Surface

Trellix



Lab user: jesse.netz@trellix.com

Status: Running Refreshing in *56* Seconds... Refresh now
It may take a few minutes for services to start

ID: 317

Cloud Provider: SKYTAP

External Appliance:

Helix Demo 1 (prod)
- Access:

Helix Demo 1 HX
- Access:

Trellix XDR XConsole
- Access:

Victim:

RANSOMWARE_WIN10_EPO_FINANCE
- Status:
- IP: 10.40.124.42 Access:
- VM ID: 106284793

RANSOMWARE_WIN10_MARKETING
- Status:
- IP: 10.40.124.43 Access:
- VM ID: 106284795

RANSOMWARE_WIN10_EPO_ACCOUNTING
- Status:
- IP: 10.40.134.201 Access:
- VM ID: 106284796

Attacker:

RANSOMWARE_WORKBENCH
- Status:
- IP: 10.40.100.89 Access:
- VM ID: 106284794

ASH Crossfire Lab 4.0-20211225 (c) 2015-2021 by FATE (FireEye Advanced Technical Enablement) Team

Ransomware Attacks Cause Damage

Solution: Rapid Response Process Blocking and Rollback

2

Trellix Promise

CISO

Economic Buyer

Minimize cost and risk from ransomware with advanced rapid response and rollback

SOC Manager / Security Architect

Technical Buyer

Quickly block new ransomware variants and avoid costly impact with automated remediation.

Why Trellix?

TIE – Rapid Response Process Blocking

- Rapidly block new attacks across endpoint estate with Threat Intelligence Exchange
- Ransomware Rollback

Trellix

Use Case: Complex Attack Surface

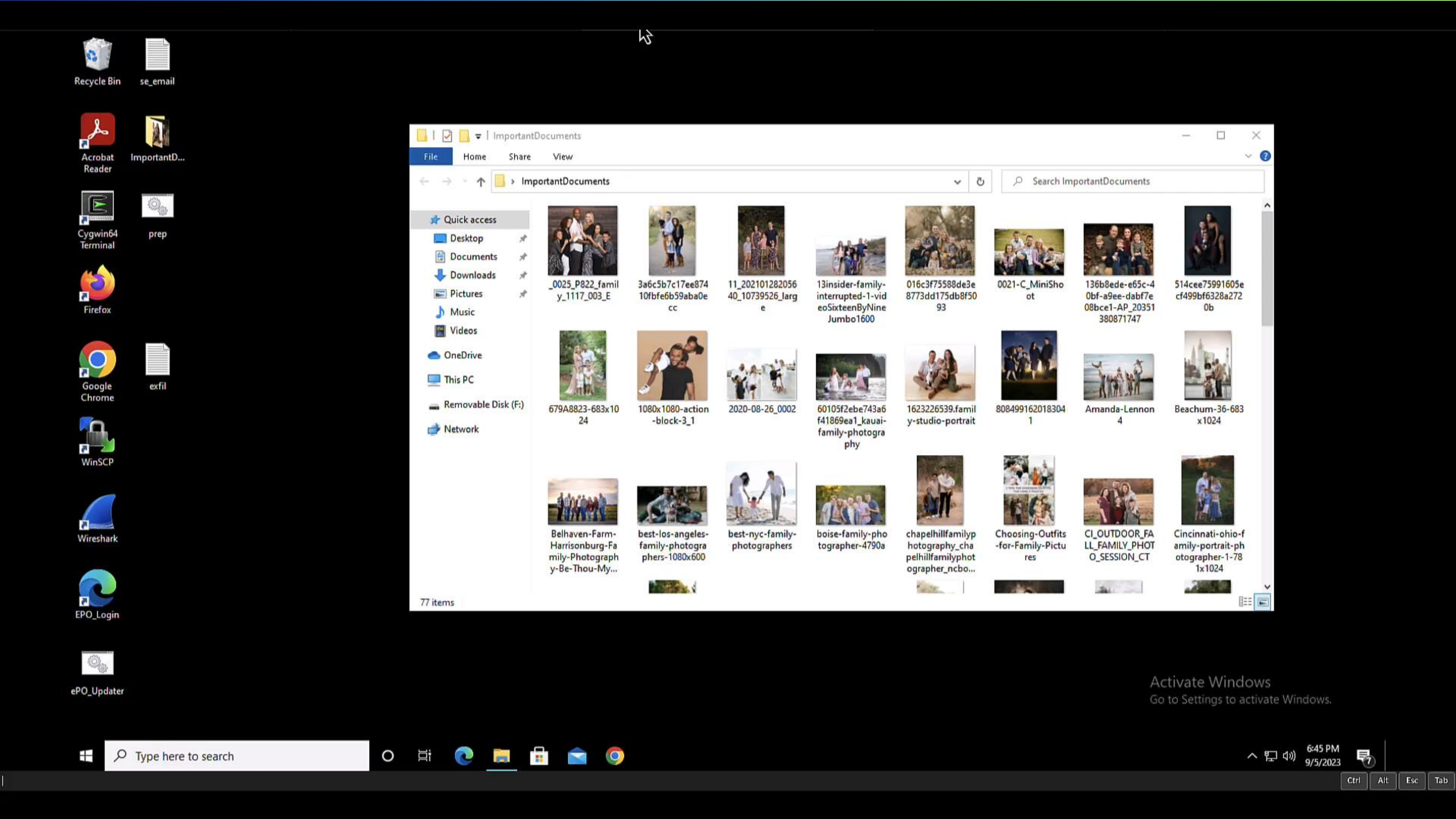
2

Optimize Protection

Scenario	Result	Solution
A new ransomware variant is executed on an endpoint.	Endpoint data is encrypted and the organization is at risk of increased scope of damage.	Trellix Threat Intelligence Exchange allows admins to immediately block new process throughout an estate and enhanced remediation automatically restores encrypted data.

Demo

Ransomware Attacks Cause Damage


Recycle Bin
se_email
Acrobat Reader
ImportantD...
Cygwin64 Terminal
prep
Firefox
Google Chrome
exfil
WinSCP
Wireshark
EPO_Login
ePO_Updater
ImportantDocuments
File
Home
Share
View
ImportantDocuments
Search ImportantDocuments
Quick access
Desktop
Documents
Downloads
Pictures
Music
Videos
OneDrive
This PC
Removable Disk (F:)
Network
_0025_P822_family_1117_003_E
3a6c5b7c17ee87410fbfe6b59aba0ecc
11_20210128205640_10739526_large
13insider-family-interrupted-1-videoSixteenByNineJumbo1600
016c3f75588de3e8773dd175db8f5093
0021-C_MiniShoot
136b8ede-e65c-40bf-a9ee-dabf7e08bce1-AP_20351380871747
514cee75991605ecf499bf6328a2720b
679A8823-683x1024
1080x1080-action-block-3_1
2020-08-26_0002
60105f2ebe743a6f41869ea1_kauai-family-photography
1623226539.family-studio-portrait
8084991620183041
Amanda-Lennon4
Beachum-36-683x1024
Belhaven-Farm-Harrisonburg-Family-Photography-Be-Thou-My...
best-los-angeles-family-photographers-1080x600
best-nyc-family-photographers
boise-family-photographer-4790a
chapelhillfamilyphotography_chapelhillfamilyphotographer_ncbo...
Choosing-Outfits-for-Family-Pictures
CI_OUTDOOR_FALL_FAMILY_PHOTO_SESSION_CT
Cincinnati-ohio-family-portrait-photographer-1-781x1024
77 items
Activate Windows
Go to Settings to activate Windows.
Type here to search
6:45 PM
9/5/2023
Ctrl
Alt
Esc
Tab

Inefficient Endpoint Alert Triage

3

Simplify Endpoint Alert Triage

Trellix Promise

SOC Manager / Security Architect

Technical Buyer

Improve endpoint team efficiency and MTTD/MTTR for endpoint investigations

SOC Analyst

Influencer

Minimize alert fatigue and time spent investigating endpoint alerts.

CISO

Economic Buyer

Minimize risk of incidents resulting from unattended endpoint alerts

Why Trellix?

- High-fidelity detections, low false positives
- MITRE Tactic and Technique
- AI Guided Investigations

Trellix

Use Case: Inefficient Alert Triage

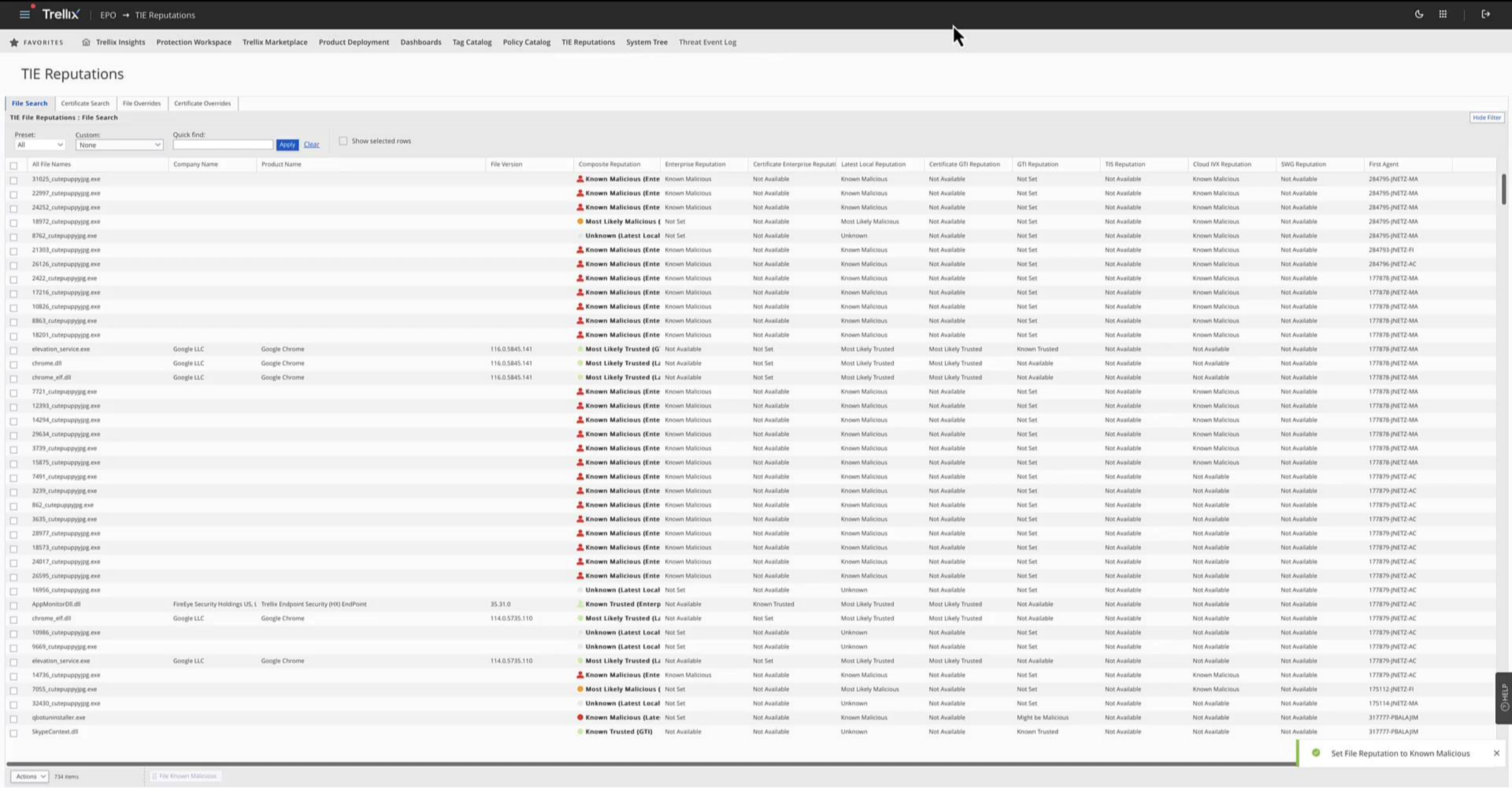
3

AI Guided Investigations

Scenario	Result	Solution
SOC analysts who need to triage endpoint alerts are overwhelmed and don’t know how to efficiently investigate alerts where they might need to take action.	An organization is hit by ransomware and deals with costly impact due to inefficient alert triage and investigation.	Trellix EDR AI guided investigations answer questions for the SOC Analysts and allow them to quickly contain incidents..

Demo

Inefficient Endpoint Alert Triage



TIE Reputations

TIE File Reputations : File Search

Preset: All

Custom: None

Quick find: Apply Clear

□ Show selected rows

All File Names	Company Name	Product Name	File Version	Composite Reputation	Enterprise Reputation	Certificate Enterprise Reputati	Latest Local Reputation	Certificate GTI Reputation	GTI Reputation	TIS Reputation	Cloud IVX Reputation	SWG Reputation	First Agent
31025_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	284795-JNETZ-MA
22997_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	284795-JNETZ-MA
24252_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	284795-JNETZ-MA
18972_cutepuppyjpg.exe				Most Likely Malicious (	Not Set	Not Available	Most Likely Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	284795-JNETZ-MA
8762_cutepuppyjpg.exe				Unknown (Latest Local	Not Set	Not Available	Unknown	Not Available	Not Set	Not Available	Known Malicious	Not Available	284795-JNETZ-MA
21303_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	284793-JNETZ-FI
26126_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	284796-JNETZ-AC
2422_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	177878-JNETZ-MA
17216_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	177878-JNETZ-MA
10826_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	177878-JNETZ-MA
8863_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	177878-JNETZ-MA
18201_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	177878-JNETZ-MA
elevation_service.exe	Google LLC	Google Chrome	116.0.5845.141	Most Likely Trusted (G'	Not Available	Not Set	Most Likely Trusted	Most Likely Trusted	Known Trusted	Not Available	Not Available	Not Available	177878-JNETZ-MA
chrome.dll	Google LLC	Google Chrome	116.0.5845.141	Most Likely Trusted (La	Not Available	Not Set	Most Likely Trusted	Most Likely Trusted	Not Available	Not Available	Not Available	Not Available	177878-JNETZ-MA
chrome_elf.dll	Google LLC	Google Chrome	116.0.5845.141	Most Likely Trusted (La	Not Available	Not Set	Most Likely Trusted	Most Likely Trusted	Not Available	Not Available	Not Available	Not Available	177878-JNETZ-MA
7721_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	177878-JNETZ-MA
12393_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	177878-JNETZ-MA
14294_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	177878-JNETZ-MA
29634_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	177878-JNETZ-MA
3739_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	177878-JNETZ-MA
15875_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	177878-JNETZ-MA
7491_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Not Available	Not Available	177879-JNETZ-AC
3239_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Not Available	Not Available	177879-JNETZ-AC
862_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Not Available	Not Available	177879-JNETZ-AC
3635_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Not Available	Not Available	177879-JNETZ-AC
28977_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Not Available	Not Available	177879-JNETZ-AC
18573_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Not Available	Not Available	177879-JNETZ-AC
24017_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Not Available	Not Available	177879-JNETZ-AC
26595_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Not Available	Not Available	177879-JNETZ-AC
16956_cutepuppyjpg.exe				Unknown (Latest Local	Not Set	Not Available	Unknown	Not Available	Not Set	Not Available	Not Available	Not Available	177879-JNETZ-AC
AppMonitorDll.dll	FireEye Security Holdings US, L	Trellix Endpoint Security (HX) EndPoint	35.31.0	Known Trusted (Enterp	Not Available	Known Trusted	Most Likely Trusted	Most Likely Trusted	Not Available	Not Available	Not Available	Not Available	177879-JNETZ-AC
chrome_elf.dll	Google LLC	Google Chrome	114.0.5735.110	Most Likely Trusted (La	Not Available	Not Set	Most Likely Trusted	Most Likely Trusted	Not Available	Not Available	Not Available	Not Available	177879-JNETZ-AC
10986_cutepuppyjpg.exe				Unknown (Latest Local	Not Set	Not Available	Unknown	Not Available	Not Set	Not Available	Not Available	Not Available	177879-JNETZ-AC
9669_cutepuppyjpg.exe				Unknown (Latest Local	Not Set	Not Available	Unknown	Not Available	Not Set	Not Available	Not Available	Not Available	177879-JNETZ-AC
elevation_service.exe	Google LLC	Google Chrome	114.0.5735.110	Most Likely Trusted (La	Not Available	Not Set	Most Likely Trusted	Most Likely Trusted	Not Available	Not Available	Not Available	Not Available	177879-JNETZ-AC
14736_cutepuppyjpg.exe				Known Malicious (Ente	Known Malicious	Not Available	Known Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	177879-JNETZ-AC
7055_cutepuppyjpg.exe				Most Likely Malicious (	Not Set	Not Available	Most Likely Malicious	Not Available	Not Set	Not Available	Known Malicious	Not Available	175112-JNETZ-FI
32430_cutepuppyjpg.exe				Unknown (Latest Local	Not Set	Not Available	Unknown	Not Available	Not Set	Not Available	Not Available	Not Available	175114-JNETZ-MA
qbotuninstaller.exe				Known Malicious (Late:	Not Set	Not Available	Known Malicious	Not Available	Might be Malicious	Not Available	Not Available	Not Available	317777-PBALAJIM
SkypeContext.dll				Known Trusted (GTI)	Not Available	Not Available	Unknown	Not Available	Known Trusted	Not Available	Not Available	Not Available	317777-PBALAJIM

Actions 734 items

File Known Malicious

Set File Reputation to Known Malicious

Impactful Endpoint Incidents

Minimize Impact from Endpoint Incidents

Trellix Promise

SOC Manager / Security Architect

Technical Buyer

Minimize impact from incidents and understand root cause

SOC Analyst

Influencer

Contain incidents quickly and verify incident is resolved

CISO

Economic Buyer

Ensure endpoint incidents don't lead to costly outages or headlines

Why Trellix?

- Rapidly block new attacks across endpoint estate
- Contain and investigate endpoints at scale
- Understand scope with adv. Forensics
- MDR options for added expertise

Trellix

Use Case: Impactful Incidents Reoccur

4

Root cause analysis to prevent reoccurring incidents

Scenario	Result	Solution
An organization is hit by ransomware but doesn't investigate with forensics for root cause analysis and just reimages systems to recover.	The organization gets hit by ransomware again because they never understood the attack vector and didn't improve their security posture.	Trellix Forensics provides advanced tools for responders to understand the scope of an attack and root cause analysis to understand how to improve controls and prevent attacks from reoccurring.

Demo

Impactful Endpoint Incidents

Demonstration Guidance

Endpoint Security

Trellix

Endpoint Demo

How to

In this demo you will be able set up a demo in CrossFire. Please start this process 1 hour prior to your demo.

Note: you can configure it before then as well.

Accessing Crossfire Labs.

You can use any of these:

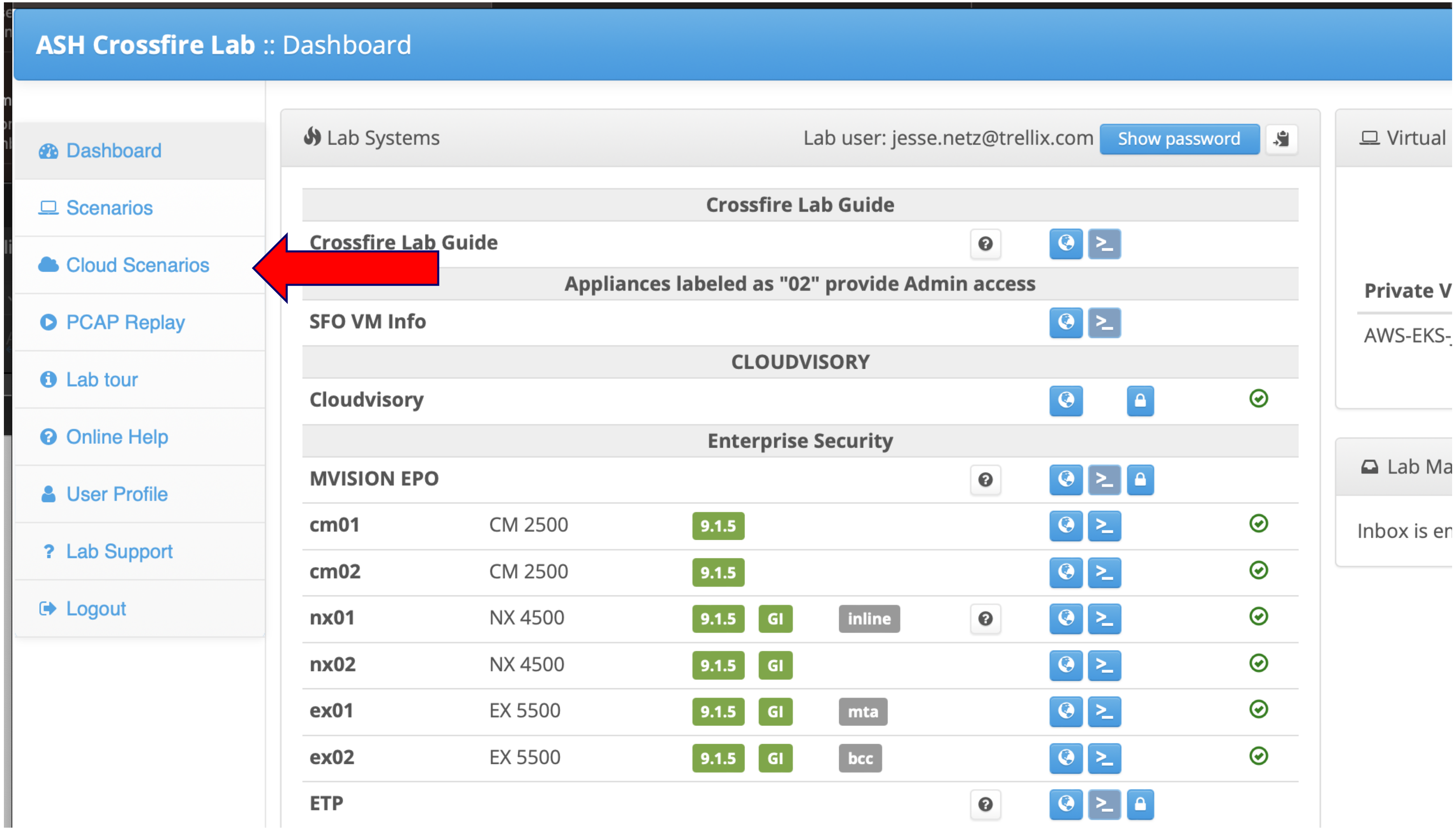
Alliances Crossfire Lab (fireeye.com)

SFO Crossfire Lab (fireeye.com)

Or

ASH Crossfire Lab (fireeye.com)

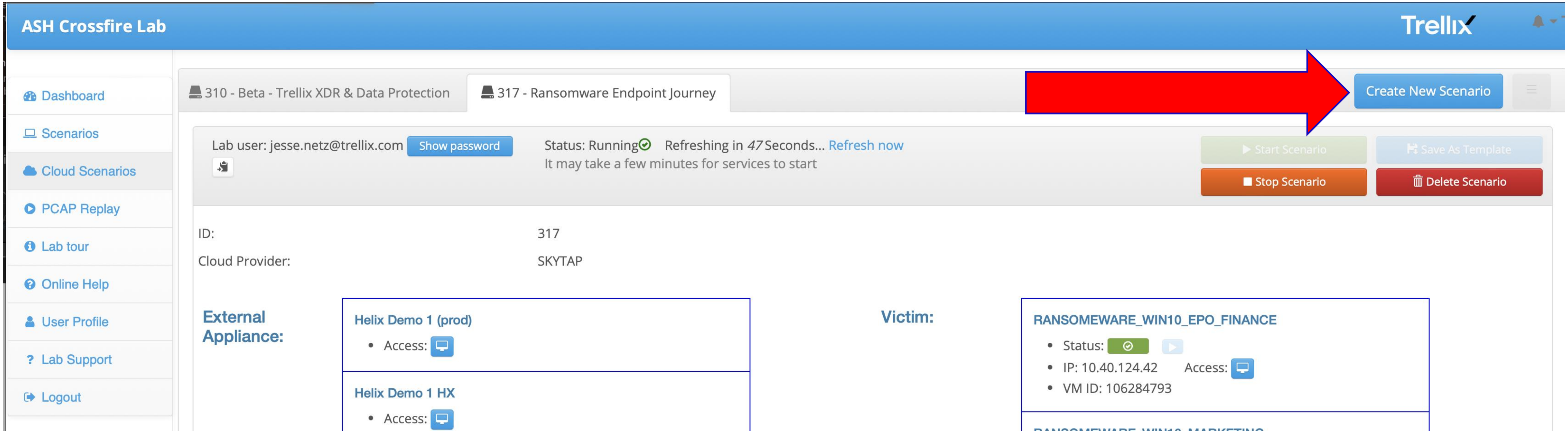
Scenarios



Lab user: jesse.netz@trellix.com

Crossfire Lab Guide						
Crossfire Lab Guide					?	
Appliances labeled as "02" provide Admin access						
SFO VM Info						
CLOUDVISORY						
Cloudvisory						✓
Enterprise Security						
MVISION EPO					?	
cm01	CM 2500	9.1.5				✓
cm02	CM 2500	9.1.5				✓
nx01	NX 4500	9.1.5	GI	inline	?	✓
nx02	NX 4500	9.1.5	GI			✓
ex01	EX 5500	9.1.5	GI	mta		✓
ex02	EX 5500	9.1.5	GI	bcc		✓
ETP					?	

Create new scenario



Lab user: jesse.netz@trellix.com

Status: Running Refreshing in *47* Seconds... Refresh now

It may take a few minutes for services to start

ID: 317

Cloud Provider: SKYTAP

External Appliance:

Helix Demo 1 (prod)

- Access:

Helix Demo 1 HX

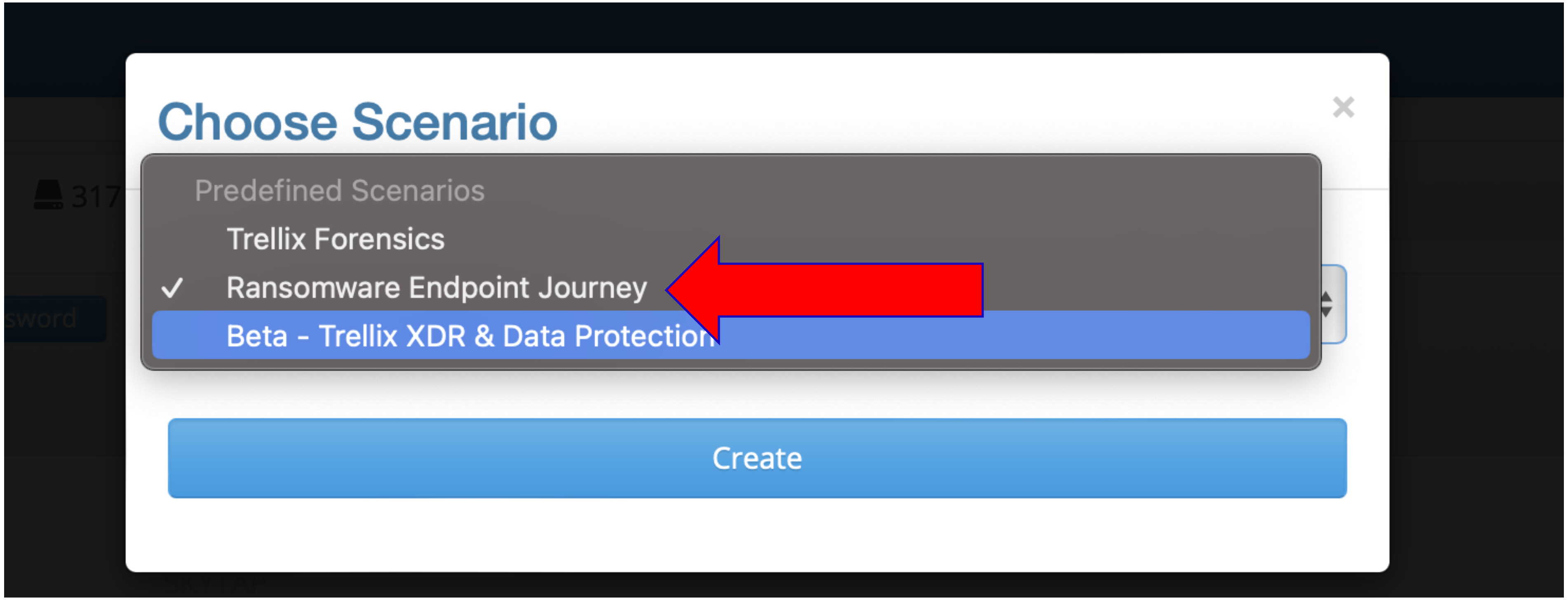
- Access:

Victim:

RANSOMWARE_WIN10_EPO_FINANCE

- Status:
- IP: 10.40.124.42 Access:
- VM ID: 106284793

Choose new scenario



Choose Scenario

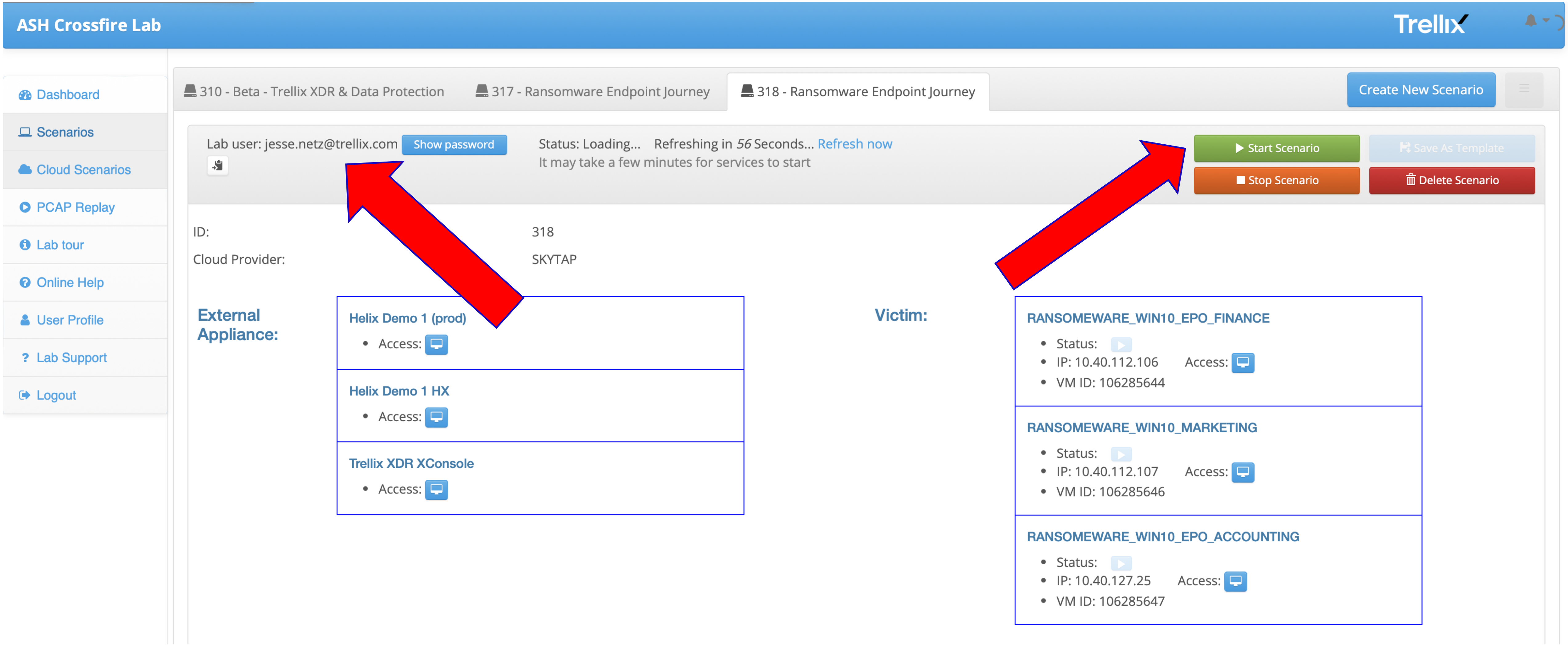
Predefined Scenarios

Trellix Forensics

✓ Ransomware Endpoint Journey

Beta - Trellix XDR & Data Protection

Start the new scenario.
Be sure to note your lab user name and password.



ASH Crossfire Lab

Lab user: jesse.netz@trellix.com

Status: Loading... Refreshing in *56* Seconds...

It may take a few minutes for services to start

ID: 318

Cloud Provider: SKYTAP

External Appliance:

Helix Demo 1 (prod)

- Access:

Helix Demo 1 HX

- Access:

Trellix XDR XConsole

- Access:

Victim:

RANSOMEWARE_WIN10_EPO_FINANCE

- Status:
- IP: 10.40.112.106 Access:
- VM ID: 106285644

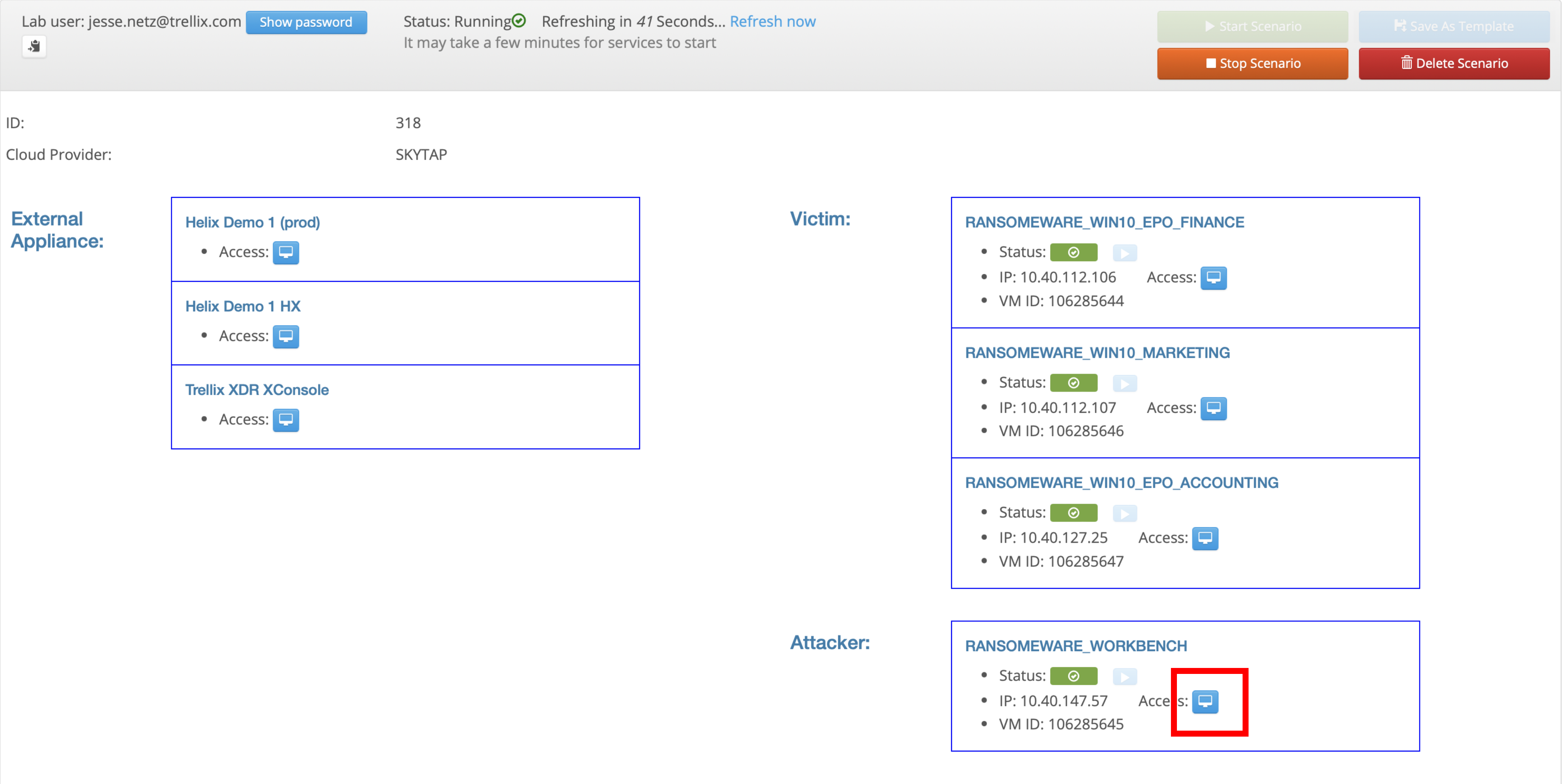
RANSOMEWARE_WIN10_MARKETING

- Status:
- IP: 10.40.112.107 Access:
- VM ID: 106285646

RANSOMEWARE_WIN10_EPO_ACCOUNTING

- Status:
- IP: 10.40.127.25 Access:
- VM ID: 106285647

Launch the Ransomware workbench system



Lab user: jesse.netz@trellix.com Show password

Status: Running✓ Refreshing in *41* Seconds... Refresh now

It may take a few minutes for services to start

ID: 318

Cloud Provider: SKYTAP

External Appliance:

Helix Demo 1 (prod)

- Access:

Helix Demo 1 HX

- Access:

Trellix XDR XConsole

- Access:

Victim:

RANSOMEWARE_WIN10_EPO_FINANCE

- Status:
- IP: 10.40.112.106 Access:
- VM ID: 106285644

RANSOMEWARE_WIN10_MARKETING

- Status:
- IP: 10.40.112.107 Access:
- VM ID: 106285646

RANSOMEWARE_WIN10_EPO_ACCOUNTING

- Status:
- IP: 10.40.127.25 Access:
- VM ID: 106285647

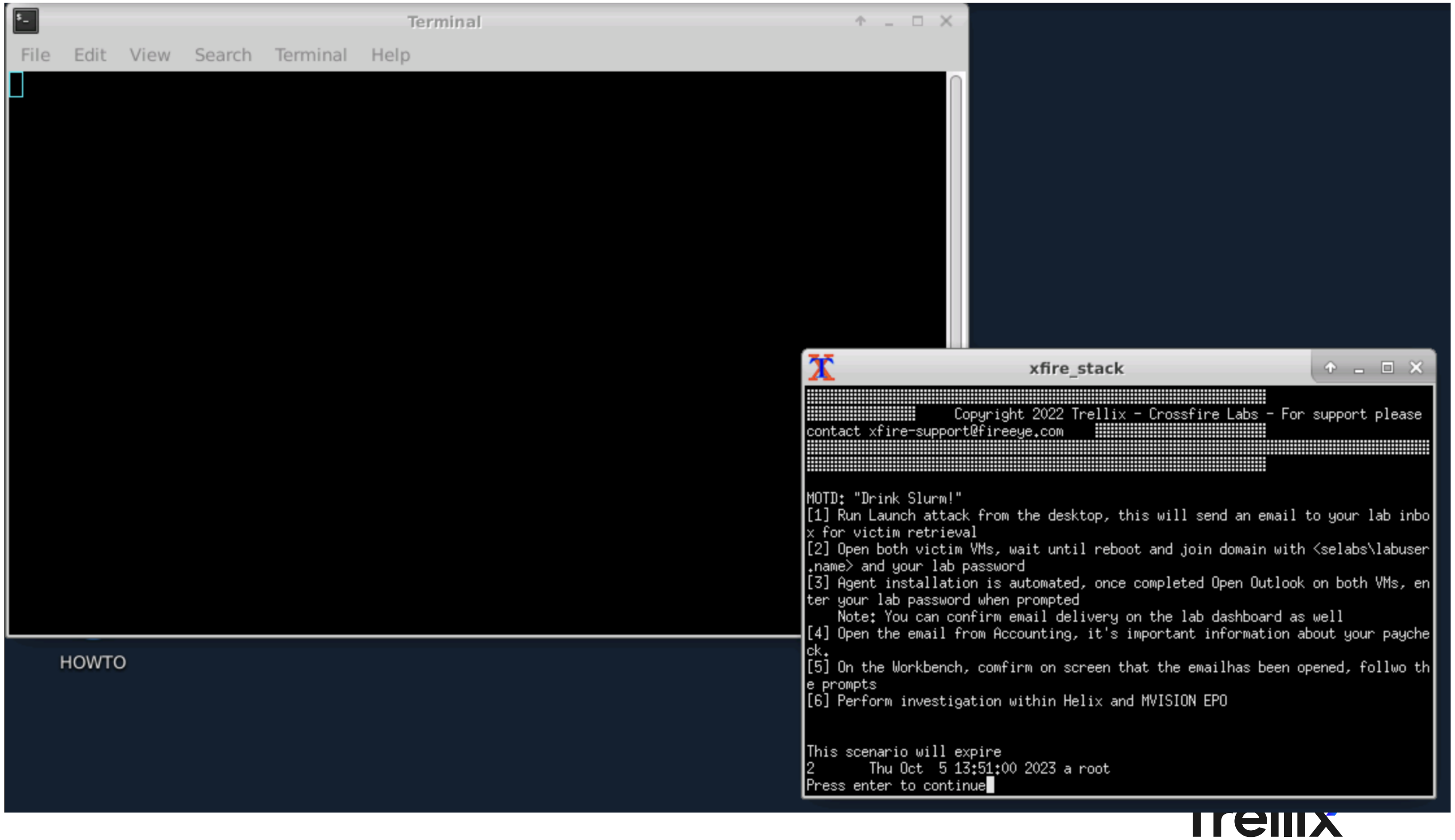
Attacker:

RANSOMEWARE_WORKBENCH

- Status:
- IP: 10.40.147.57 Access:
- VM ID: 106285645

Complete your scenario

- Press enter to continue
- Close the workbench



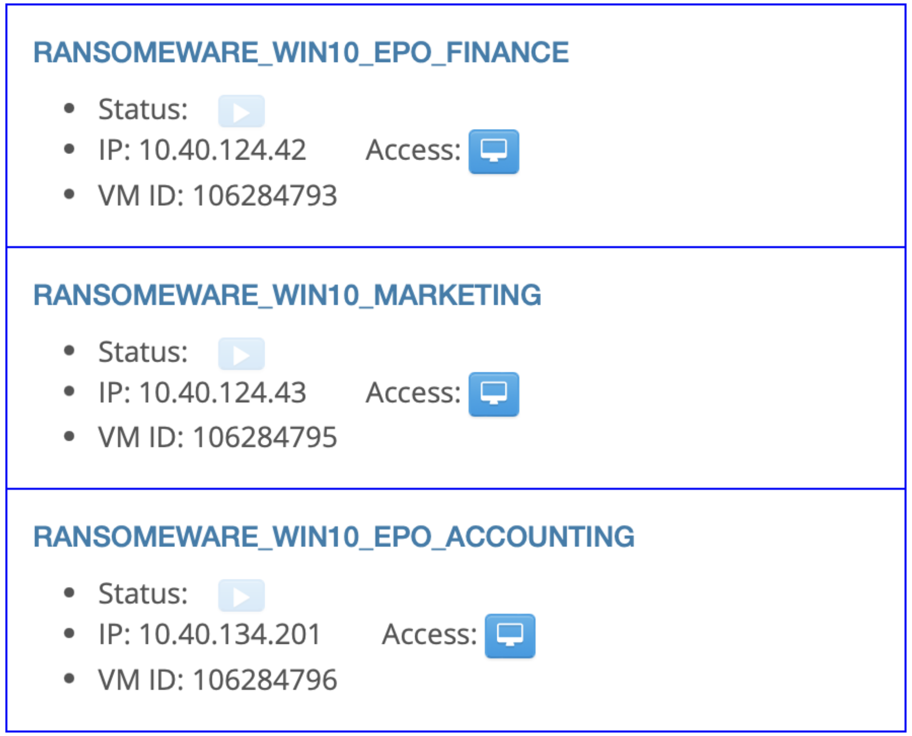
```
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
▒▒▒▒▒▒▒▒▒▒▒▒▒     Copyright 2022 Trellix - Crossfire Labs - For support please
contact xfire-support@fireeye.com    ▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒


MOTD: "Drink Slurm!"
[1] Run Launch attack from the desktop, this will send an email to your lab inbo
x for victim retrieval
[2] Open both victim VMs, wait until reboot and join domain with <selabs\labuser
.name> and your lab password
[3] Agent installation is automated, once completed Open Outlook on both VMs, en
ter your lab password when prompted
    Note: You can confirm email delivery on the lab dashboard as well
[4] Open the email from Accounting, it's important information about your payche
ck.
[5] On the Workbench, comfirm on screen that the emailhas been opened, follwo th
e prompts
[6] Perform investigation within Helix and MVISION EPO


This scenario will expire
2       Thu Oct  5 13:51:00 2023 a root
Press enter to continue
```

Available systems.

There are 3 available systems and all have HX, ENS, ATP, and the same policies installed

- Marketing
- Finance
- Accounting

Victim:



RANSOMEWARE_WIN10_EPO_FINANCE

- Status: ▶
- IP: 10.40.124.42 Access: 🖥
- VM ID: 106284793

RANSOMEWARE_WIN10_MARKETING

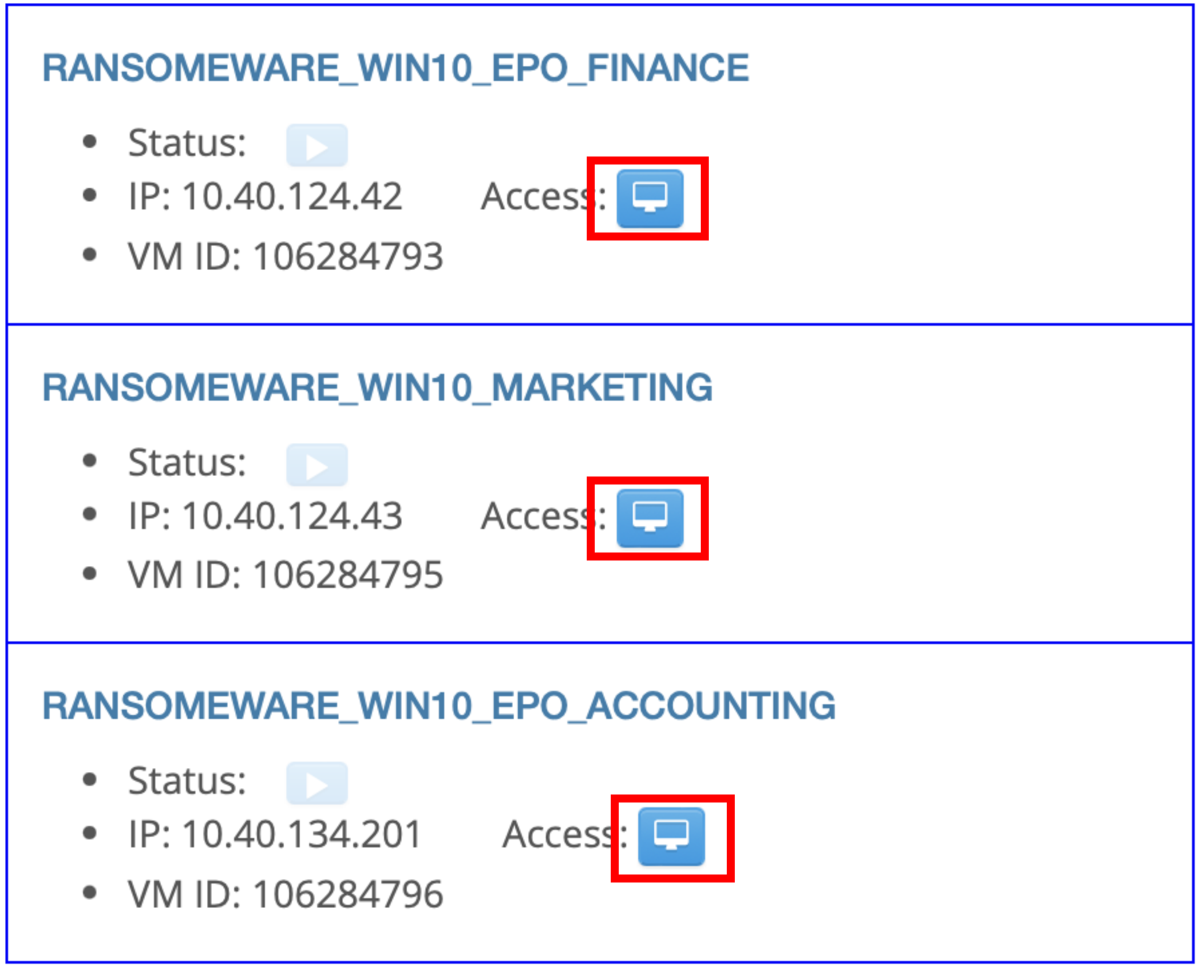
- Status: ▶
- IP: 10.40.124.43 Access: 🖥
- VM ID: 106284795

RANSOMEWARE_WIN10_EPO_ACCOUNTING

- Status: ▶
- IP: 10.40.134.201 Access: 🖥
- VM ID: 106284796

Launch all systems to begin bootstrapping

Victim:



RANSOMEWARE_WIN10_EPO_FINANCE

- Status: ▶
- IP: 10.40.124.42 Access: 🖥
- VM ID: 106284793

RANSOMEWARE_WIN10_MARKETING

- Status: ▶
- IP: 10.40.124.43 Access: 🖥
- VM ID: 106284795

RANSOMEWARE_WIN10_EPO_ACCOUNTING

- Status: ▶
- IP: 10.40.134.201 Access: 🖥
- VM ID: 106284796

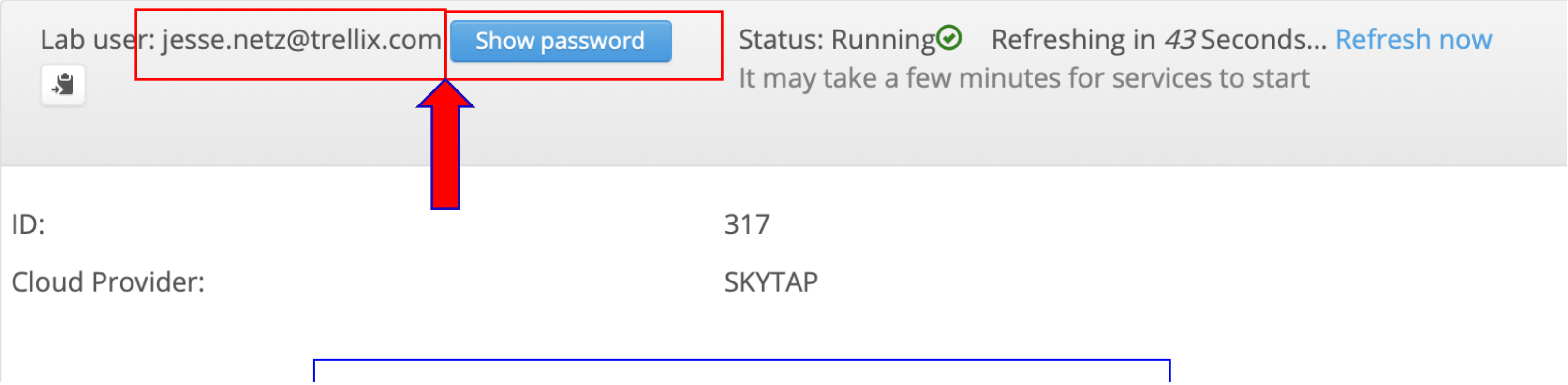
This will take a while...

1. The system will launch automatically and you will see the login scripts run to prep the system.
2. You will be logged out for set up to complete.
3. When it is time to log back in, you will need your credentials provided on the CrossFire landing page.

The End-User Experience.

The first time you log into the endpoint systems, it will need to completed the setup process.

- After this set up, the system will reboot.
- You will log in with your CrossFire credentials.



Lab user: jesse.netz@trellix.com

Status: Running ✓ Refreshing in *43* Seconds... Refresh now

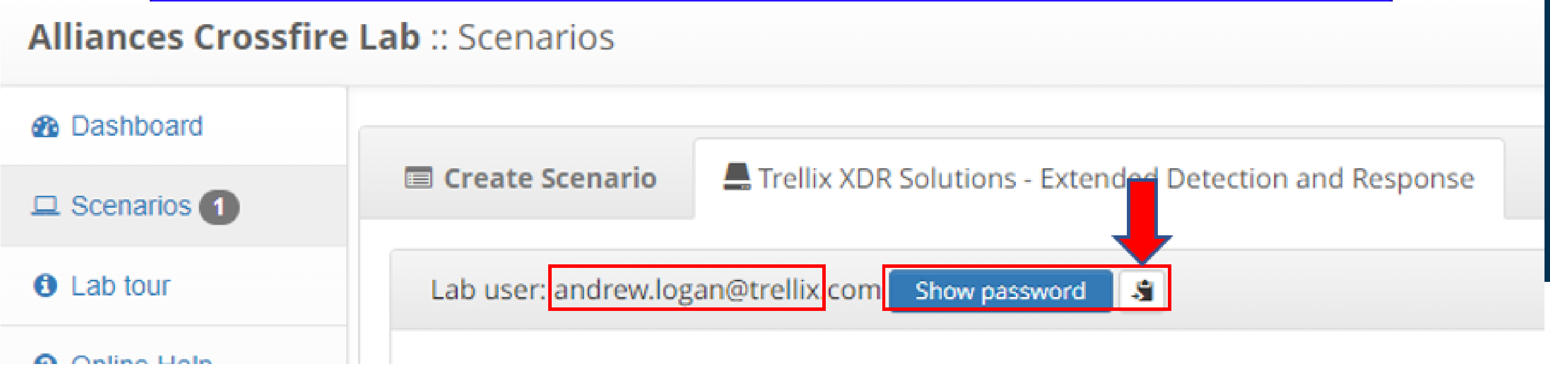
It may take a few minutes for services to start

ID: 317

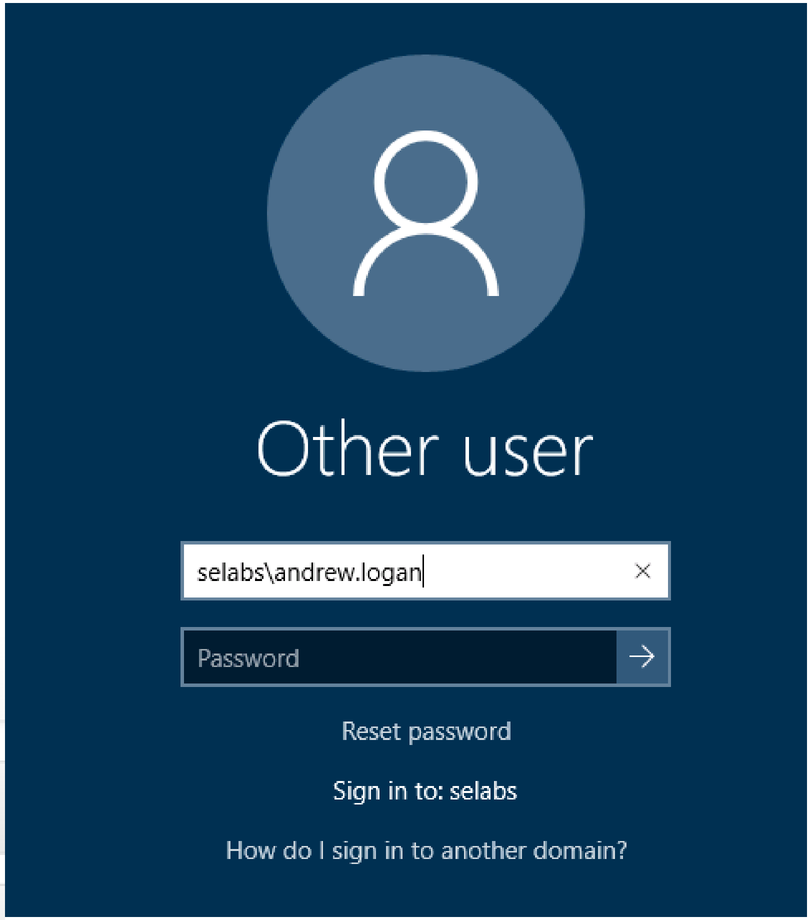
Cloud Provider: SKYTAP

The End-User Experience.

When logging into the endpoints, you will be prompted for your CrossFire credentials.
For example:
Selabs\first name.last name
Password:


Alliances Crossfire Lab :: Scenarios
Dashboard
Scenarios 1
Lab tour
Create Scenario
Trellix XDR Solutions - Extended Detection and Response
Show password

Lab user: andrew.logan@trellix.com



selabs\andrew.logan

After the reboot….

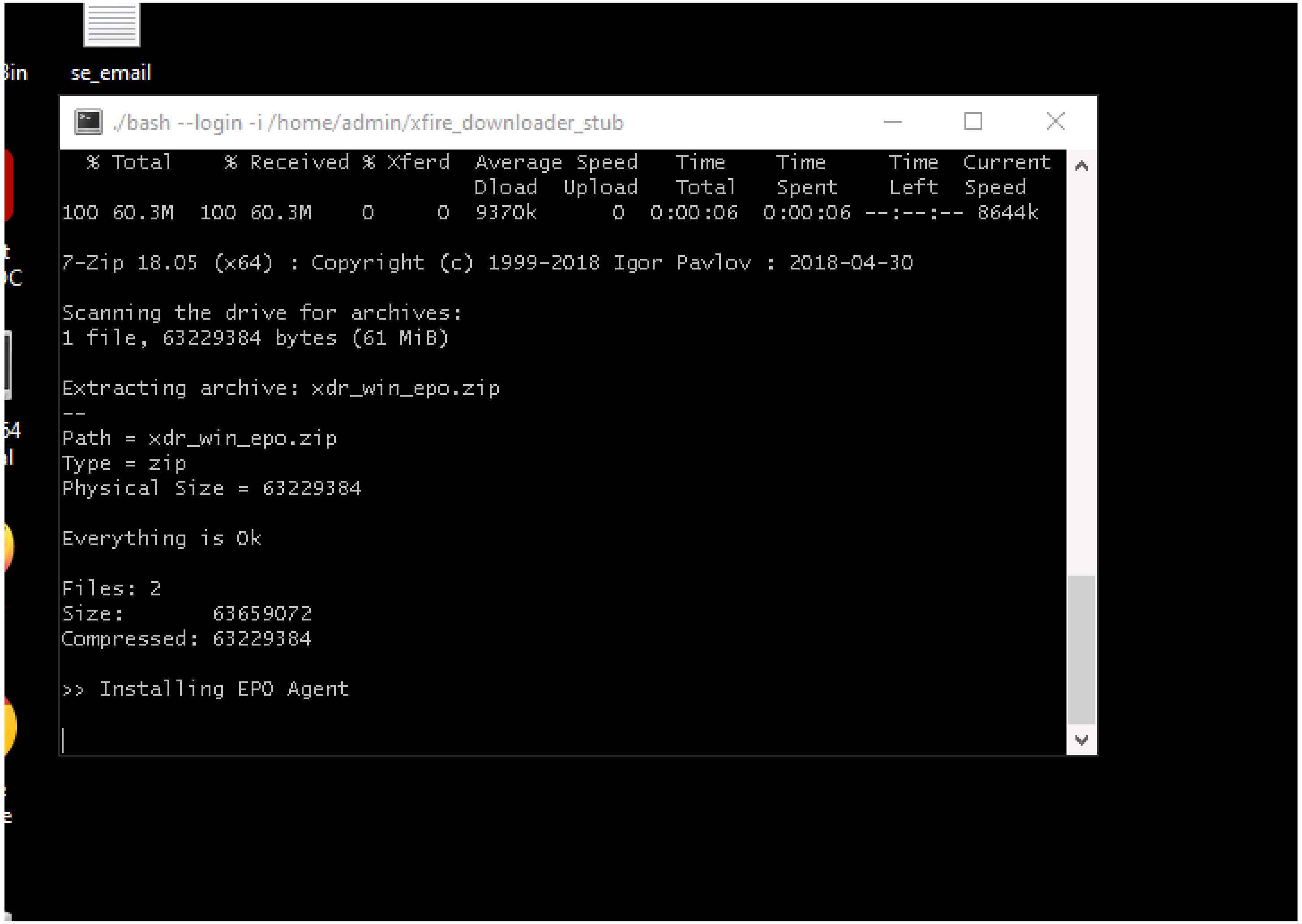
Once you log back in, you will see your desk top.

It will take a few minutes to install the ePO Agent (Trellix Agent).

(get a cup of coffee ☺).

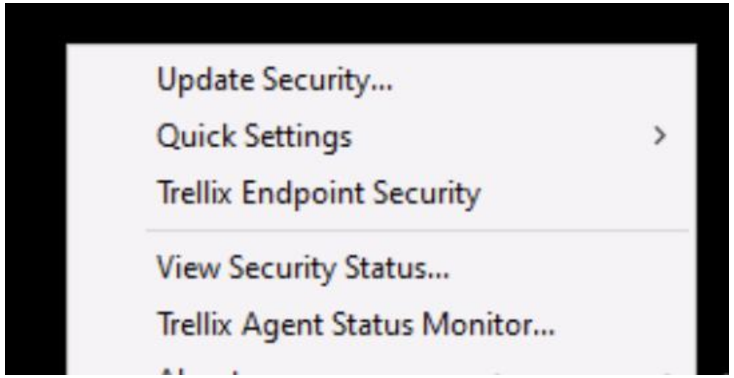
Check the icon tray to see if Trellix Agent is there.

Reboot this system again.



```
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 60.3M  100 60.3M    0     0  9370k      0  0:00:06  0:00:06 --:--:-- 8644k

7-Zip 18.05 (x64) : Copyright (c) 1999-2018 Igor Pavlov : 2018-04-30

Scanning the drive for archives:
1 file, 63229384 bytes (61 MiB)

Extracting archive: xdr_win_epo.zip
--
Path = xdr_win_epo.zip
Type = zip
Physical Size = 63229384

Everything is Ok

Files: 2
Size:       63659072
Compressed: 63229384

>> Installing EPO Agent
```

... after the reboot you should see this in the tray.



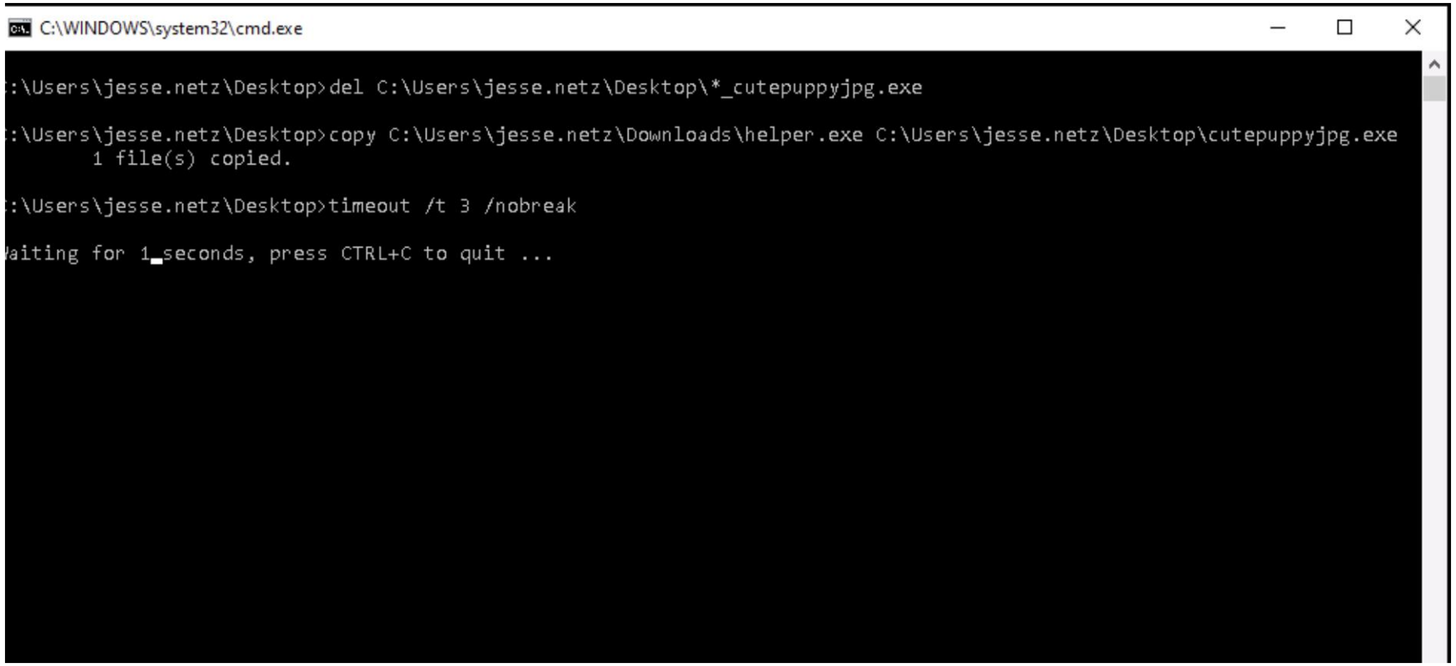
Launch prep.bat

You’ll notice a sample will get created on the desktop

%random%_cutepuppyjpg.exe

This is the sample used to launch the ransomware scenario

The End-User Experience.



C:\WINDOWS\system32\cmd.exe

```
:\Users\jesse.netz\Desktop>del C:\Users\jesse.netz\Desktop\*_cutepuppyjpg.exe

:\Users\jesse.netz\Desktop>copy C:\Users\jesse.netz\Downloads\helper.exe C:\Users\jesse.netz\Desktop\cutepuppyjpg.exe
        1 file(s) copied.

:\Users\jesse.netz\Desktop>timeout /t 3 /nobreak

aiting for 1 seconds, press CTRL+C to quit ...
```

Choose your scenario

Creating the following files will change the sample's behavior:

- sample/sample.txt – Cause the cutepuppy ransomware to download a copy of the DarkPower ransomware and trigger a correlated Trellix Insights Campaign

- exfil/exfil.txt – Cause the cutepuppy ransomware to behave poorly after the encryption. This will cause an automatic rollback of the encrypted files.

Endpoint Demo

At this point you will be ready to demonstrate the Ransomware Endpoint use cases

Trellix

Partner and SE Tools

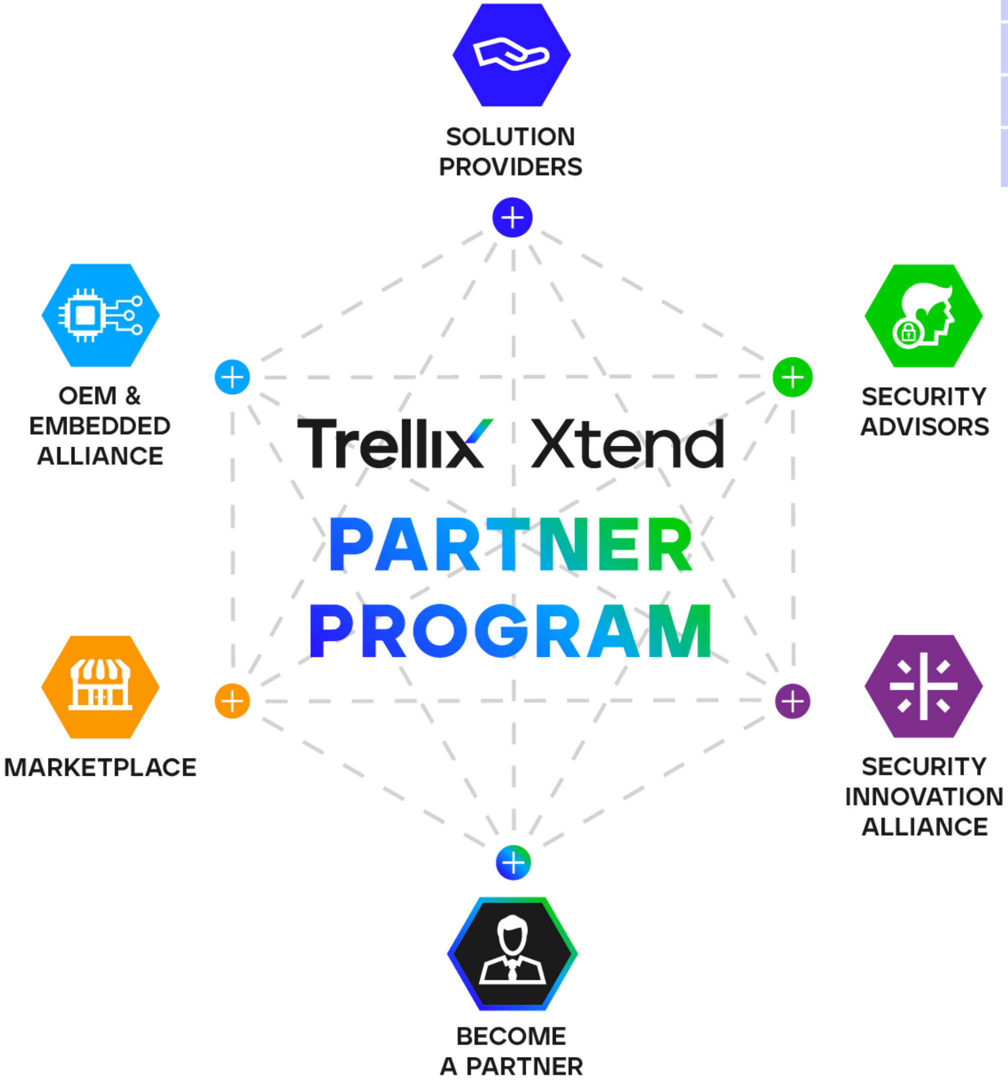
How to Access

Diarmuid O’Boyle

Senior Sales Engineer
November 10, 2023

Types of Partners

Partner Levels	Sales Certifications	Architect Certifications
Collaborate	4	4
Momentum	2	2
Growth	1	1
Distribution	4	4
MSSP	4	4



Trellix Xtend

Trellix

Partner Success Engines

Profitability Programs

Demand Generation & Marketing Support

Trellix University

Dedicated Technical & Sales Resources

The Hive

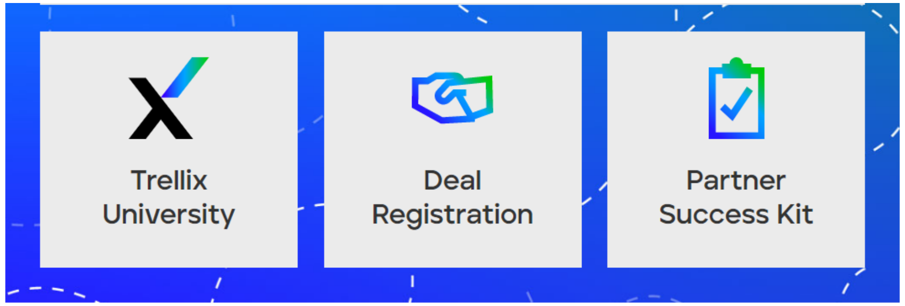
Tools & Resources

Partner Care

Trellix

The HIVE

Call to Action Buttons

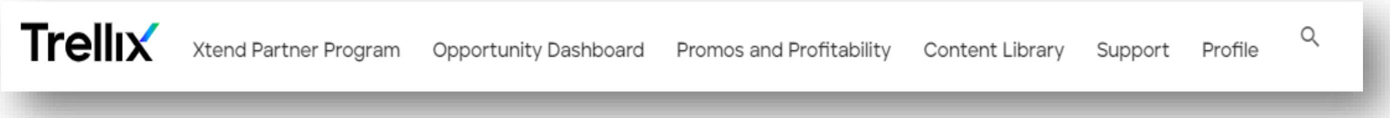


Trellix University

Deal Registration

Partner Success Kit

Updated Navigation



Trellix

Xtend Partner Program

Opportunity Dashboard

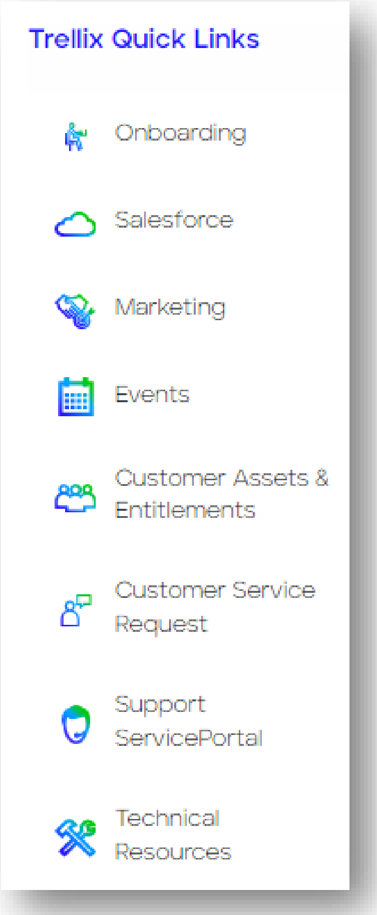
Promos and Profitability

Content Library

Support

Profile

Updated Quick Links

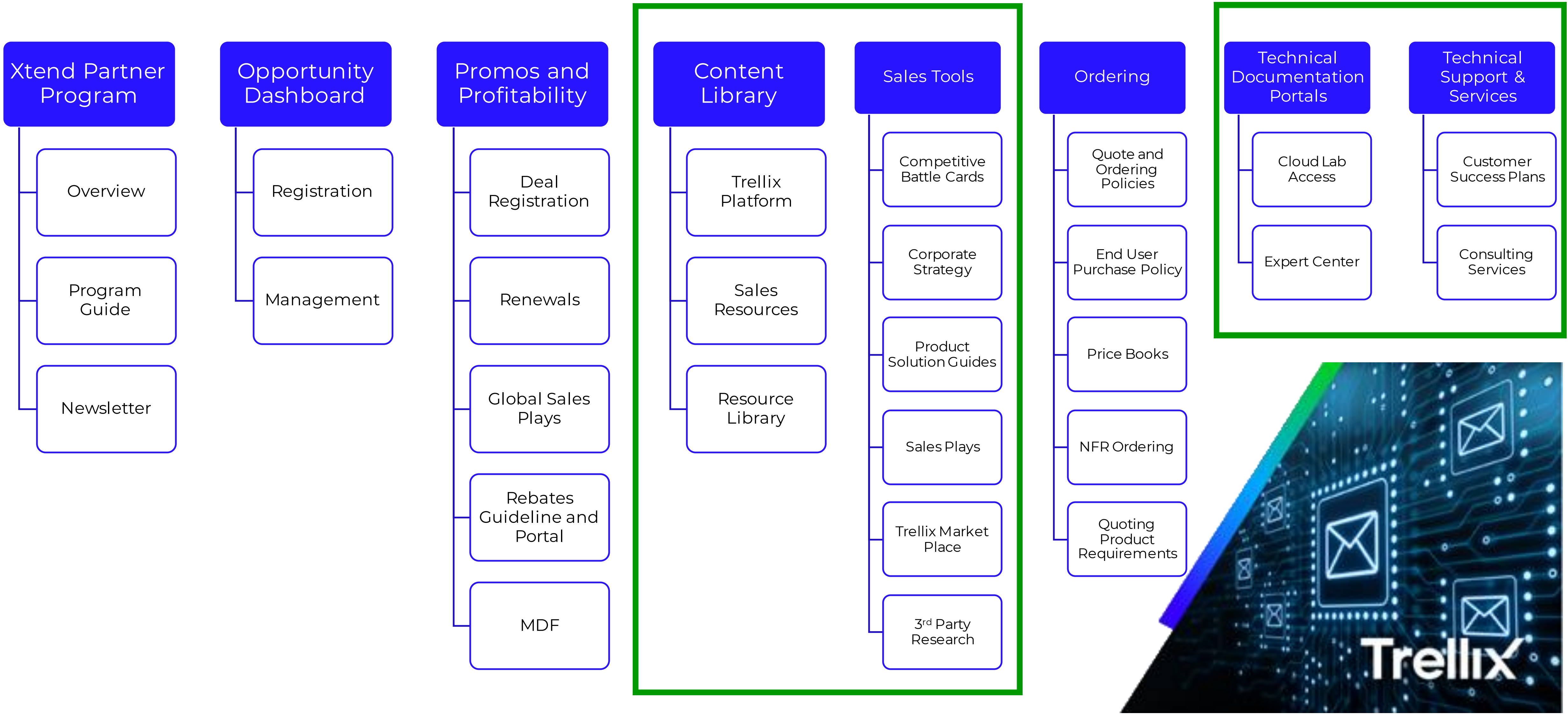


Trellix Quick Links

- Onboarding
- Salesforce
- Marketing
- Events
- Customer Assets & Entitlements
- Customer Service Request
- Support ServicePortal
- Technical Resources

Partner Portal

https://partners.trellix.com



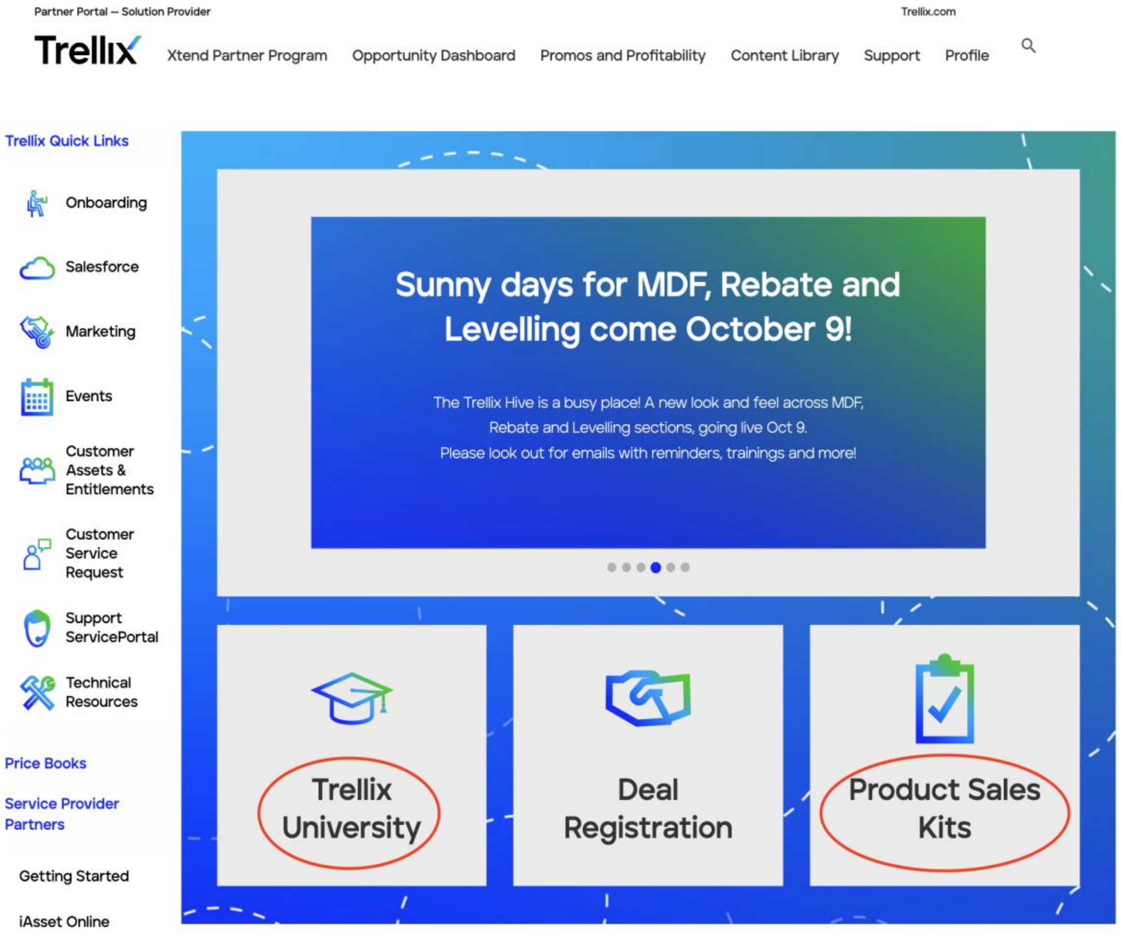
- Xtend Partner Program
  - Overview
  - Program Guide
  - Newsletter
- Opportunity Dashboard
  - Registration
  - Management
- Promos and Profitability
  - Deal Registration
  - Renewals
  - Global Sales Plays
  - Rebates Guideline and Portal
  - MDF
- Content Library
  - Trellix Platform
  - Sales Resources
  - Resource Library
- Sales Tools
  - Competitive Battle Cards
  - Corporate Strategy
  - Product Solution Guides
  - Sales Plays
  - Trellix Market Place
  - 3rd Party Research
- Ordering
  - Quote and Ordering Policies
  - End User Purchase Policy
  - Price Books
  - NFR Ordering
  - Quoting Product Requirements
- Technical Documentation Portals
  - Cloud Lab Access
  - Expert Center
- Technical Support & Services
  - Customer Success Plans
  - Consulting Services

Trellix

Partner Portal – Sales Kits

https://partners.trellix.com/partner/en-us/solution-provider/product-sales-kits.html

Product Sales Kits will be updated frequently



Partner Portal — Solution Provider

Trellix.com

Trellix

Xtend Partner Program | Opportunity Dashboard | Promos and Profitability | Content Library | Support | Profile

Trellix Quick Links

- Onboarding
- Salesforce
- Marketing
- Events
- Customer Assets & Entitlements
- Customer Service Request
- Support ServicePortal
- Technical Resources

Price Books

Service Provider Partners

Getting Started

iAsset Online

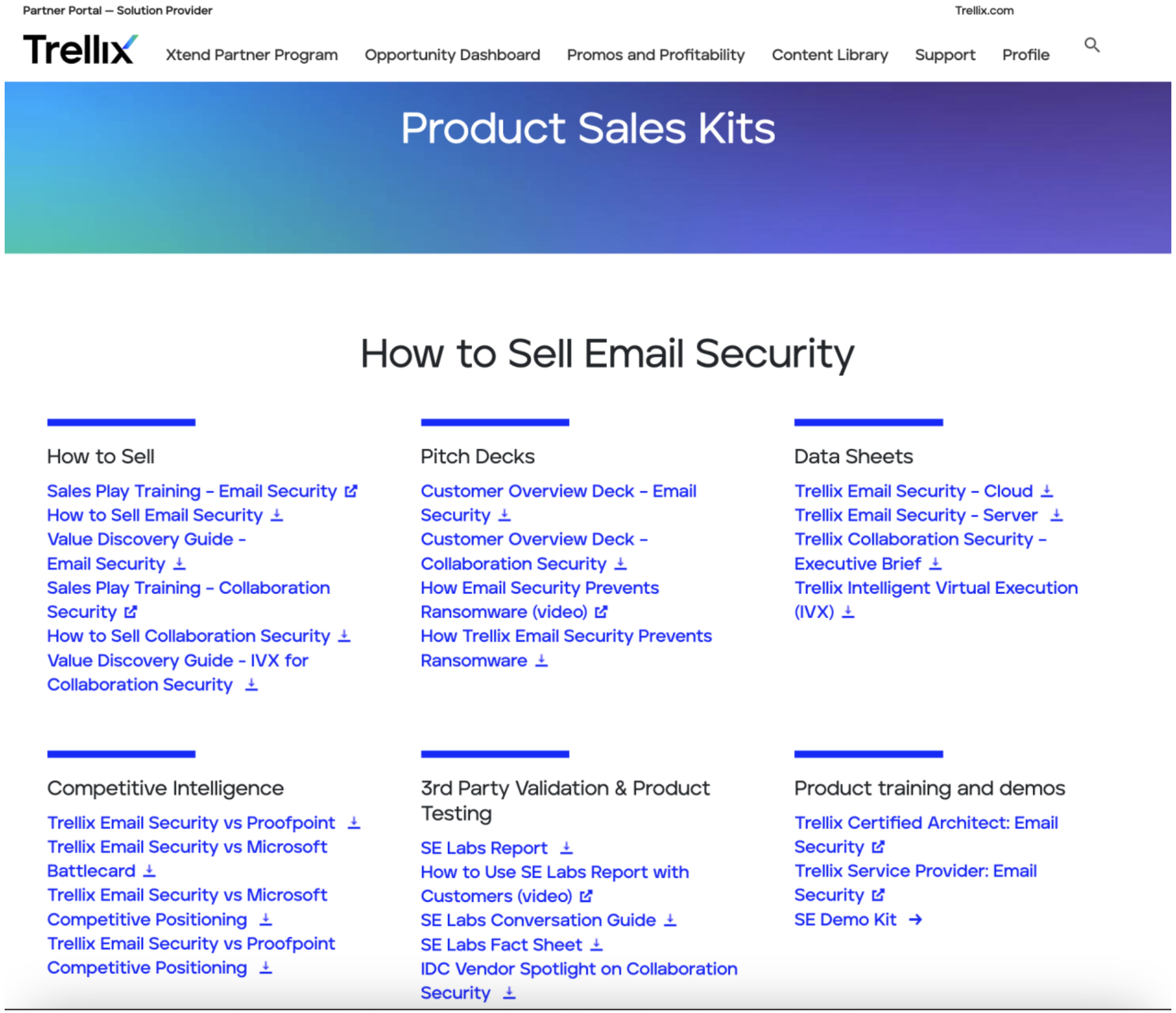
Sunny days for MDF, Rebate and Levelling come October 9!

The Trellix Hive is a busy place! A new look and feel across MDF, Rebate and Levelling sections, going live Oct 9. Please look out for emails with reminders, trainings and more!

Trellix University

Deal Registration

Product Sales Kits



Partner Portal — Solution Provider

Trellix.com

Trellix

Xtend Partner Program | Opportunity Dashboard | Promos and Profitability | Content Library | Support | Profile

Product Sales Kits

How to Sell Email Security

How to Sell

- Sales Play Training – Email Security ↗
- How to Sell Email Security ⤓
- Value Discovery Guide - Email Security ⤓
- Sales Play Training – Collaboration Security ↗
- How to Sell Collaboration Security ⤓
- Value Discovery Guide - IVX for Collaboration Security ⤓

Pitch Decks

- Customer Overview Deck – Email Security ⤓
- Customer Overview Deck - Collaboration Security ⤓
- How Email Security Prevents Ransomware (video) ↗
- How Trellix Email Security Prevents Ransomware ⤓

Data Sheets

- Trellix Email Security – Cloud ⤓
- Trellix Email Security – Server ⤓
- Trellix Collaboration Security – Executive Brief ⤓
- Trellix Intelligent Virtual Execution (IVX) ⤓

Competitive Intelligence

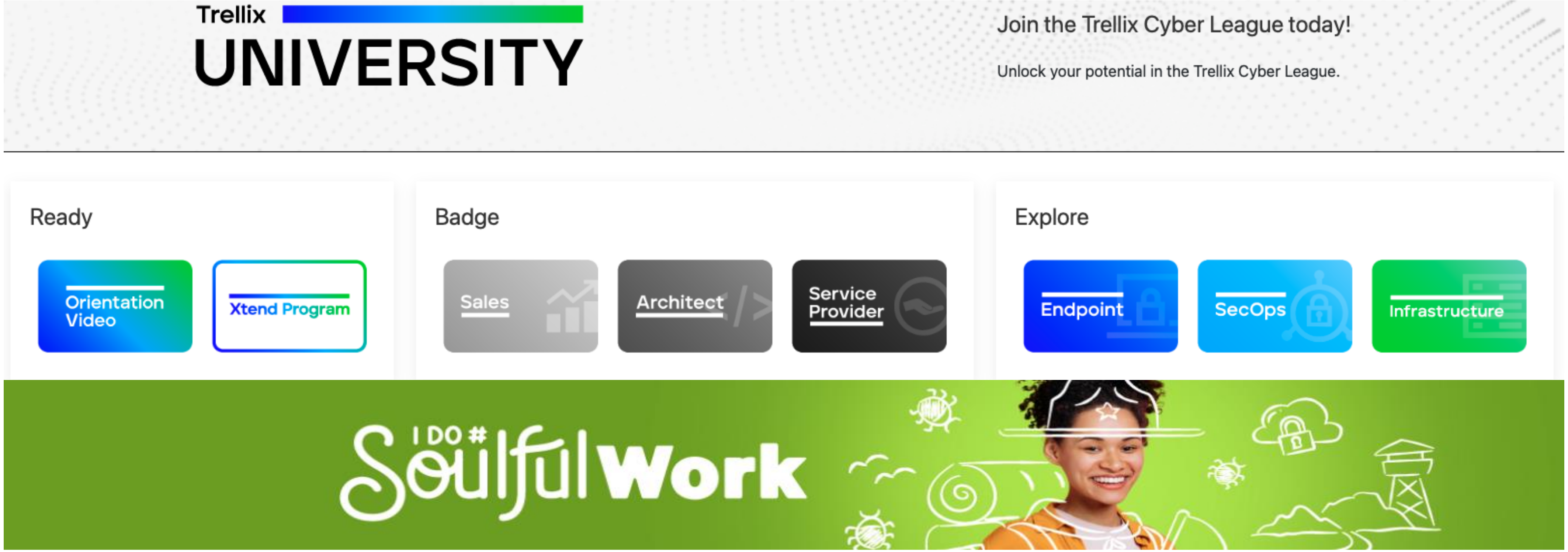
- Trellix Email Security vs Proofpoint ⤓
- Trellix Email Security vs Microsoft Battlecard ⤓
- Trellix Email Security vs Microsoft Competitive Positioning ⤓
- Trellix Email Security vs Proofpoint Competitive Positioning ⤓

3rd Party Validation & Product Testing

- SE Labs Report ⤓
- How to Use SE Labs Report with Customers (video) ↗
- SE Labs Conversation Guide ⤓
- SE Labs Fact Sheet ⤓
- IDC Vendor Spotlight on Collaboration Security ⤓

Product training and demos

- Trellix Certified Architect: Email Security ↗
- Trellix Service Provider: Email Security ↗
- SE Demo Kit →



Join the Trellix Cyber League today!

Unlock your potential in the Trellix Cyber League.

All Badges are valid for 1 year or until a new version is released (whichever comes first)
Must meet enablement requirements within 90 days of joining program

Access through Partner Portal or https://training.trellix.com

Same login and password as the Trellix Partner Portal

Contact PartnerCare@Trellix.com with login issues

Partner SE Technical Bookmarks

Product Technical Documentation Portal

- Product Documentation:
- https://docs.trellix.com/

- Administration Guides
- Deployment Guides
- System Security Guides
- Release Notes
- Hardware Guides
- Reference Guides

Cloud Lab

- CrossFire (ASH):
- https://login.trellix.com/

- MDemo:
- https://trellix-mdemo.skytap-portal.com/

- Consolidation in progress…

Communication

Partner Care Team

- partnercareemea@trellix.com

- MSP Partner Care Team
- msppartnercare@trellix.com

Expert Center

Knowledge Base

Forum

- Trellix-F Community:
- https://community.fireeye.com/
- Trellix-M Community:
- https://communitym.trellix.com/
  Consolidation in progress…

Differentiators

Endpoint Security

Trellix

Top Endpoint Competitors

Microsoft

CROWDSTRIKE

SentinelOne

Endpoint Customer Alternatives

Microsoft

What they say

- Endpoint Protection is built-in to Windows with advanced protection, nothing to deploy
- Inspired by the "assume breach" mindset with their EDR
- Prevent and detect attacks across your identities, endpoints, apps, email, data, and cloud apps with XDR capabilities

The Reality

- Difficult to manage and configure, especially at enterprise scale
- Complex for responders, search is limited to cloud telemetry, and generic alerting
- The path to XDR has limited integrations and requires their SIEM integrations

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 open and native XDR with native integration of endpoint, email & network security

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 2022 MITRE Round 4 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

Trellix

Endpoint Customer Alternatives

SentinelOne

What they say

- SentinelOne promotes a single agent and cloud console or on-prem based
- Achieve greater cross-surface visibility and take action in real-time
- Welcome to Native and Open XDR
- Position Trellix as “legacy” that “relies on signatures”

The Reality

- Unproven prevention capability in 3rd party testing and limited configurable controls
- Relies on cloud telemetry and access for hunting and control of endpoints
- Relies on 3rd party integrations for visibility and context beyond the endpoint

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

How our Competition Increase Risk and Cost

THE REALITY

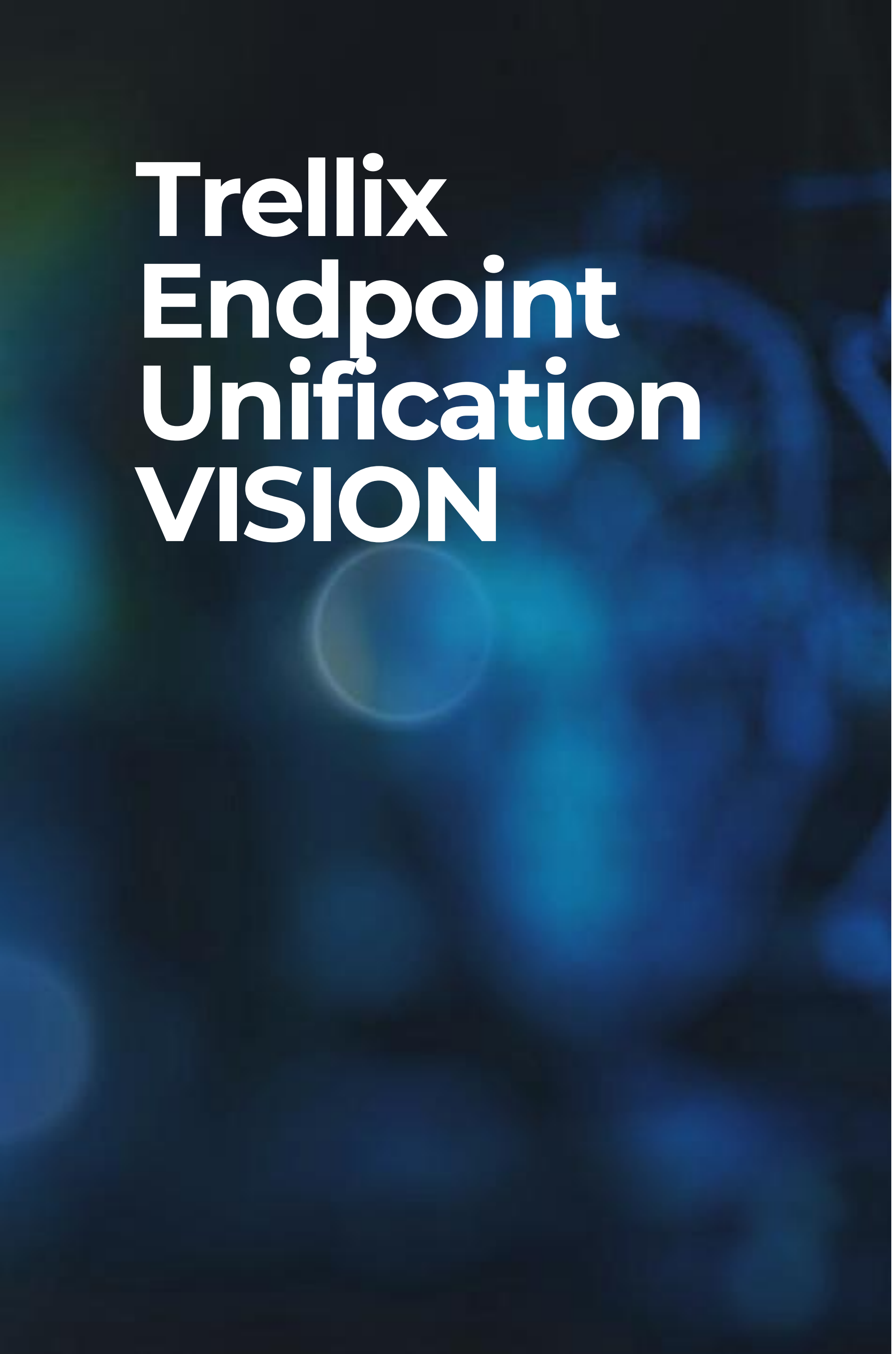
	Microsoft	CROWDSTRIKE		
	“Built-in endpoint and nothing to deploy.”	“Single lightweight agent and cloud console”	“Superior visibility and endpoint security”	
BEFORE THE ATTACK	GAPS ON-PREM AND LEGACY WIN	GAPS ON-PREM AND MAC COVERAGE	UNPROVEN ENDPOINT “CHECKLIST” FEATURES	INCREASED RISK
DURING THE ATTACK	GENERIC ALERTING, COMPLEX INVESTIGATIONS	HIGH FALSE POSITIVE AND DELAYED DETECTIONS	NO INTEGRATED THREAT CAMPAIGN INTEL	INCREASED TIME
AFTER THE ATTACK	LIMITS TO MANAGEMENT, RESPONSE AND DATA COLLECTION AT SCALE			INCREASED COST

Trellix Differentiation: Optimized operational efficiencies and proven enterprise scale protection, advanced visibility and control for rapid response AT SCALE.

Trellix

What next

Endpoint Security



Trellix Endpoint Unification VISION

XConsole

- SaaS, Multi-tenant
- Built on MVISION + Helix technology
- Easy to deploy, easy to use
- One console for all experiences

Unified Agent

- EDR + Forensics capabilities
- Best of both companies' technologies
- Lightweight and performance optimized
- Composable Apps (Modules)
- Simple to deploy, upgrade and manage

Unified Endpoint

North Star Themes & Outcomes

Deployment Simplification

- Simplified deployment
- Install status Observability
- Agent updates & ease of transition from other EPP

Unified Management Console

- Zero context switching
- Unified portfolio policy management
- Rich alert workflows (visualization, context, actionability)

Comprehensive Endpoint Security

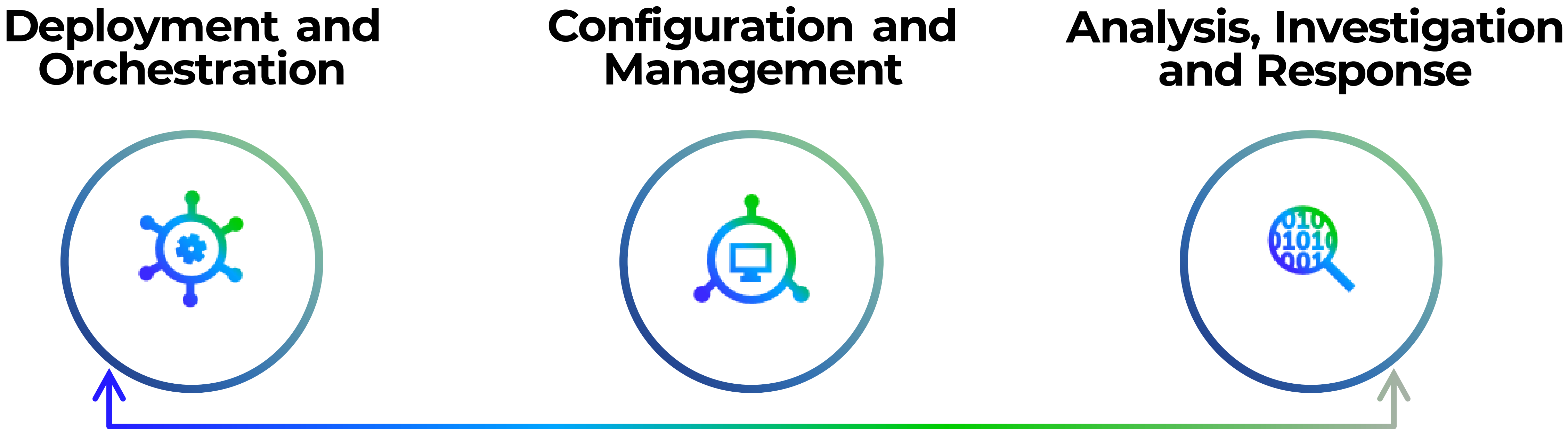
- Best in class Protection, Detection & Remediation
- Rapid Triage & Deep Investigations
- Full spectrum Incident Response
- Reduced footprint
- Improved performance

Improved Extensibility & Scalability

- Modular platform
- Extensible for XDR
- Accelerated release cadence
- API based
- COGS reduction

Trellix

XConsole Vision: Unified Experience



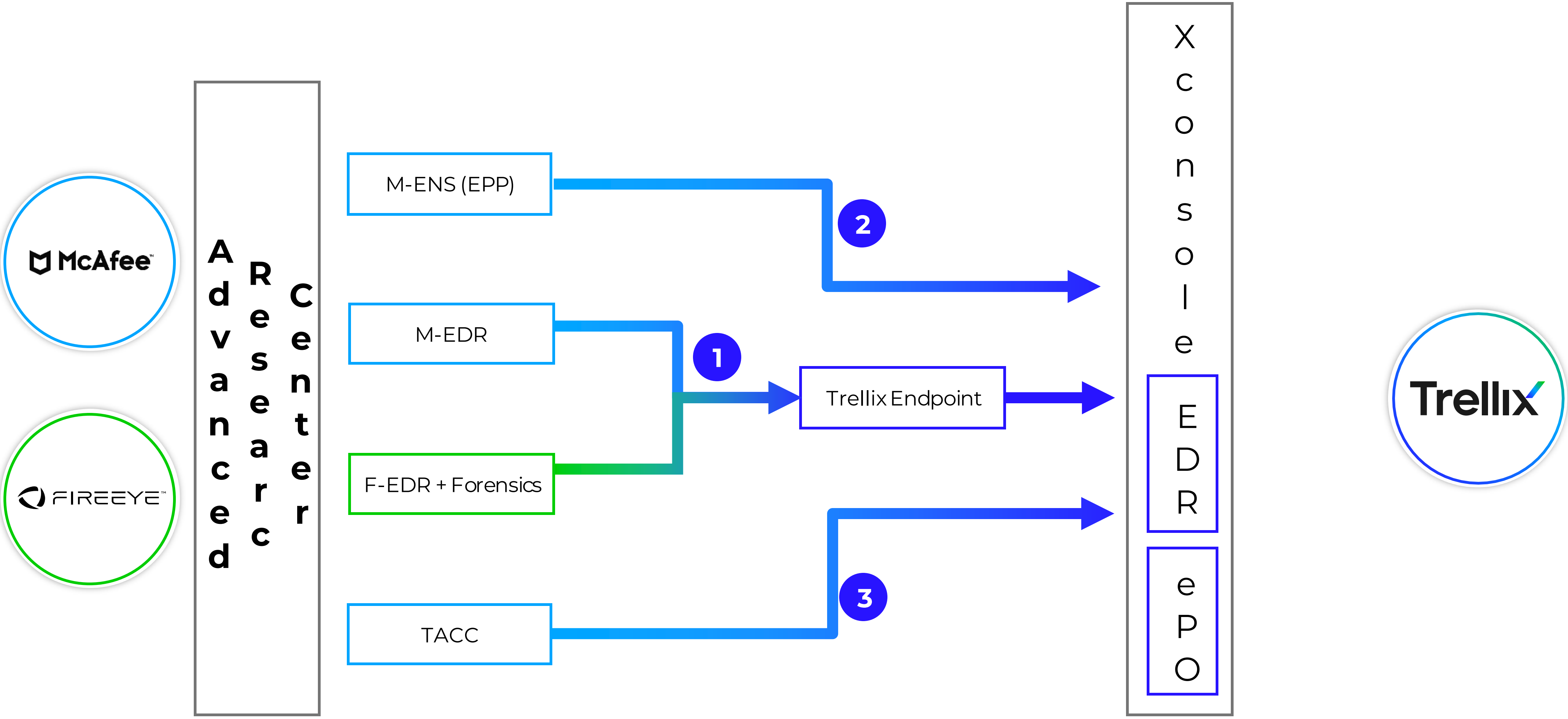
Deployment and Orchestration

Configuration and Management

Analysis, Investigation and Response

Enables customers to use Trellix **SaaS** services and **on-prem** products in **unified hybrid experience**

Trellix Endpoint Security Stack



Trellix

Endpoint Security Journey

Enhanced EDR
Q2 2023

SECURITY EXCELLENCE: EDR + forensics

- Expanded alerting on Indicators of Compromise (IoC) AMSI & Logon Tracker
- Forensic Alert threats in EDR

EASE OF DEPLOY: Integrated Deployment

- Integrated agent deployment via ePO

Endpoint/Datacenter Security

- HYBRID CLOUD: Mac (M1/M2) native support

EDR with Advanced Response
2H 2023

EASE OF MANAGEMENT: EDR + forensics

- Simplified Auth for EDR & HX (Forensics)
- Integrated user experience across ePO, EDR & HX (Forensics)
- XConsole architecture for UI and workflows
- Policy management

SECURITY EXCELLENCE: Advanced response actions

- Host Remediation
- File/Memory/Process Acquisitions
- Forensic (Enterprise) Search (also new depth from EDR vantage)

EASE OF DEPLOY: Integrated Deployment

- Integrated agent deployment via ePO
- Mac M1/M2 native support in HX

Endpoint/Datacenter Security

- ePO SaaS for App Control
- CWS support for GCP

EDR Advanced Forensics
2024 +

SECURITY EXCELLENCE : Investigation Workflows

- Cross-App Alert Workflow with Storytime View to understand sequence of events
- Alert Enrichment for rich context and behavior analysis
- Evidence Acquisition at scale
- Automated response options
- Assisted investigations through playbooks
- Auto Evidence Capture (Acquisitions)
- Seamless detection to forensic workflows
- XConsole Interface (Modern UI)

EASE OF MANAGEMENT:

- Enterprise centric security through behavioral analytics at user & org level

Endpoint/Datacenter Security

HYBRID CLOUD: Platform support & Certifications

- ARM support on Win & Linux
- Advanced security for Containers
- FedRAMP & IL5

Demo

Unified Endpoint – H2 2023

Trellix

A Unified Endpoint Experience

The information contained in this presentation is for informational purposes only and should not be deemed an offer by Trellix, create obligations for Trellix, or create expectations of future releases which impact your current purchase decision. Trellix reserves the right to modify, discontinue, add or subtract features or functionality to its existing products and planned future releases at any time at its sole discretion.

Point of Contacts

Endpoint Security

Contact us

Email

partnercareemea@trellix.com

Trellix

Thank You!