Trellix

APJ Partner Summit'24

Partnering for a Secure Future

Join us at the APJ Partner Summit

Phuket, Thailand

10-12 JULY 2024

Trellix

Trellix Endpoint Security Solutions

APJ Partner Summit 2024

July 8, 2024

Speakers for Today

Ron Wang
Sr Director, APJ SE

Hidemitsu Sakurai
Sr Director, Japan SE

Manish Sinha
Director, India SE

Carl Thaw
Global Enablement

What are the key features and capabilities your customers look for in an endpoint security solution?

Agenda

1) **Why the need for Trellix Endpoint solution?**
Challenges it solves

2) **How does Trellix solve the problem?**
How we are different

3) **About the Trellix solution**
Overview & Demo

4) **Personas**
Who to target

5) **Proof Points**
Customer Case Study

6) **Product Packaging**
Product SKUs

7) **Upsell and Cross-Sell**
Positioning the solution to customers

Trellix

Why do we need endpoint solutions?

what are we trying to solve?

Trellix

Current Situation:

More endpoints
More types
Constantly under attack

- Windows, Mac, Linux, Mobile
- Remote workers
- Bring your own devices

- SOC deluged with alerts and incidents
- SOC under pressure and overloaded

- Ransomware attacks continue
- Organizations can’t get ahead of threats

Current Situation: Endpoints are Constantly Under Attack

Ransomware

54%

Organizations reported ransomware blocked access to systems / data[1]

Organizations need modern endpoint security **before, during, and after** to stay resilient from sophisticated attackers.

Gaps in Visibility

21 days

Average attacker dwell time before discovery[2]

Insufficient preparation **before an attack** allows attackers to evade detection

Ignored Alerts

35%

Security analysts who say alerts are ignored when the queue is full[3]

Security teams face a deluge of alerts that they cannot properly triage **during an attack**

Recurring Attacks

43%

Organizations hit by ransomware were hit more than once[4]

Organizations face repeated attacks due insufficient response and not improving security maturity **after recovering from an attack**

[1] Future Enterprise Resiliency and Spending Survey - Wave 11, IDC, December 2021
[2] Infosecurity magazine / [3] IDC Survey 2021 / [4] 2022 Third-party breach report, Black Kite

Trellix

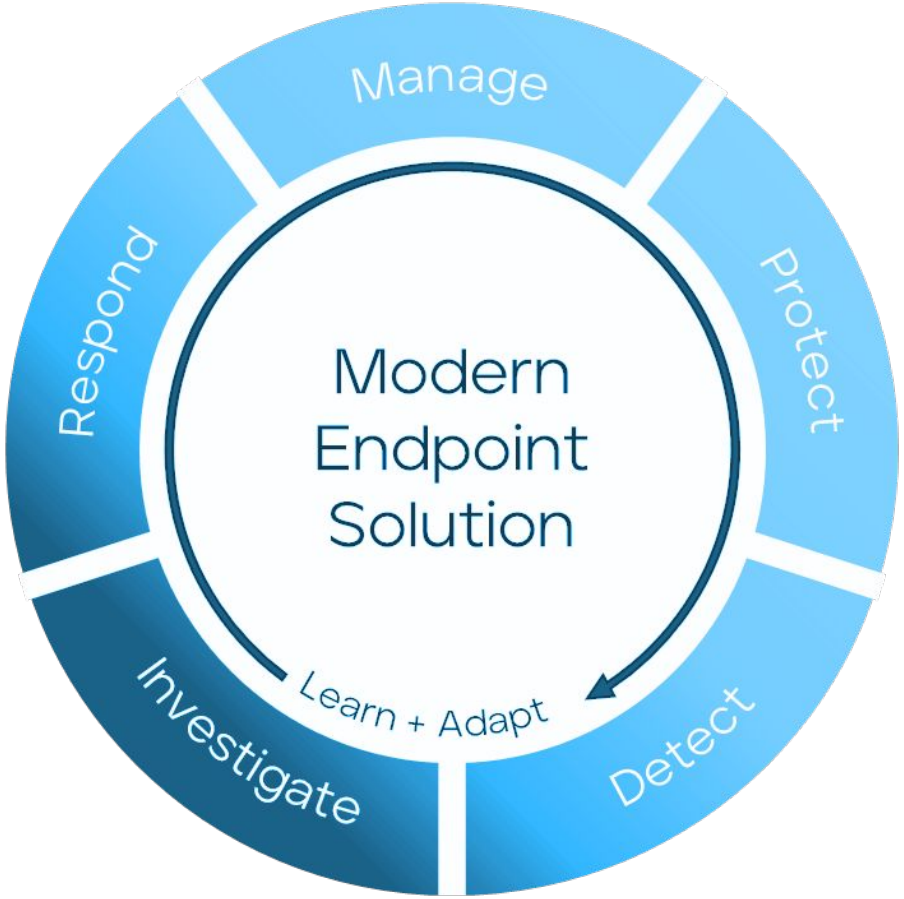
Customers Need Modern Endpoint Security

Trellix Endpoint Security Platform

Reduce Endpoint Complexity:
Optimize *protection and prevent threats* ***proactively***

Increase SOC Efficiency:
Simplifies and improves *alerts triage, investigation, and response*

Reduce Impact from Incident:
Identify ***scope and root cause*** *and improve* ***security maturity***



Required Capabilities

Reduce Endpoint Complexity

- Fill gaps in coverage and fix misconfigurations
- Reduce the attack surface
- Leverage a fully featured protection stack

Increase SOC Efficiency

- Reduce alerts deluge
- Identify and act quickly on attacks
- Speed up investigations and response

Reduce Impact from Incidents

- Understand scope and root cause
- Remediate and prevent reoccurrence
- Improve security posture and prevent attacks

Improving Endpoint Security Maturity Leads to Success with XDR

ePO – SaaS and On-premises Security Management Platform

Endpoint Protection (ENS)

Endpoint Detection and Response (EDR)

Endpoint Forensics (HX)

But what if we dont change - status quo?

What if companies don’t change?

Before Scenarios

- Lack of visibility and unsure of endpoint security readiness
- No true understanding of security posture
- Too many resources spent chasing false positives endpoint alert
- IT tickets for endpoint security incidents like ransomware or a breach
- Numerous products and consoles drive up complexity
- Uncertain ROI on tools

Negative Consequences

- Difficult to quantify, assess, and convey risk toward endpoint security
- Unclear efficacy of endpoint security investments
- Recurrence of similar endpoint attacks such as ransomware
- Higher chance for cyber risk exposure equates to fines / negative reputations
- Increased staff turnover equals no strategic approach to security

Trellix

How Trellix Solves it

Before

During

After

Attack

- ✓ Are we protected?
- ✓ How do we minimize the attack surface?
- ✓ How do we improve our security posture?

Trellix Endpoint Security (ENS)

- Proactively manage attack surface
- Rich and fully-featured threat prevention stack

What differentiates Trellix ENS?

Comprehensive Protection Stack

On-client and cloud ML, behavioral analytics, exploit prevention, signatures

Adaptable aggressiveness and containment based on reputation and connectivity

Host Firewall, Web Control

Ransomware Rollback

Proprietary enhanced remediation leveraging machine learning

More effective than Volume Shadow Copy Service (SentinelOne) or Microsoft's OneDrive that are vulnerable

Some doesn't have any restore capability

Broad Third-party Validation

Consistent solid results in AV-Test, AV-Comparatives, and SE Labs

Outperforms the competition, CrowdStrike, for protection, false positives, and comparable performance despite the competitor's claims.

What differentiates Trellix ENS?

Comprehensive Protection Stack

Customer Values

This multi-layered approach delivers more accurate protection for a range of threats and reduces false positives, reducing alert fatigue in the SOC.

Ransomware Rollback

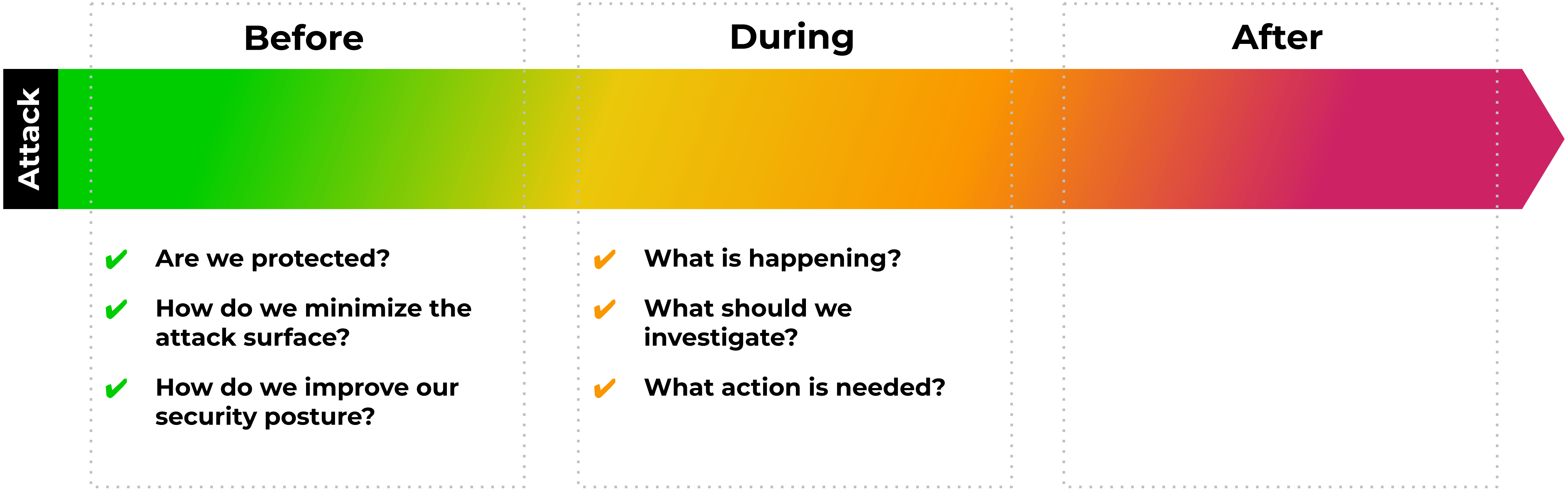
Customer Values

Our automated rollback remediation swiftly remediates unauthorized changes, minimizing disruption and maximizing productivity.

Broad Third-party Validation

Customer Values

Demonstrated value in public independent tests provide confidence that Trellix ENS delivers on security outcomes in a range of platforms and environments.



Before

- ✓ Are we protected?
- ✓ How do we minimize the attack surface?
- ✓ How do we improve our security posture?

During

- ✓ What is happening?
- ✓ What should we investigate?
- ✓ What action is needed?

After

Trellix Insights, Threat Intelligence Exchange (TIE) and EDR

- Efficient and effective alerts and incidents triage
- Fast response and containment
- AI-guided investigation

What differentiates Trellix Insights?

Proactive Threat Intelligence

Threat intel relevant to industry and country

Extensive, actionable threat campaign dossiers

Security Posture Recommendations

Recommendations to improve endpoint configurations

Proactive and threat specific countermeasures before attacks

Threat Hunting Guidance

Pivot to EDR with indicators in Trellix Insights threat intelligence

Campaign connections maps tools and CVEs to threat actors

What differentiates Trellix Insights?

Proactive Threat Intelligence

Customer Values

Increases readiness for relevant risks to focus defensive preparations relevant to threat landscape.

Security Posture Recommendations

Customer Values

Organizations have confidence their endpoint configuration is optimized.
Minimize preventable attacks and focus on strategic security initiatives

Threat Hunting Guidance

Customer Values

Threat hunters focus on threats that matter before they cause damage.

What differentiates Trellix Threat Intelligence Exchange?

Flexible Deployment

Cloud, on-premises and hybrid deployments

Centrally managed in ePO

Platform Integrations

Automated submission to IVX (sandbox)

Integrates with Endpoint, Network IPS, Skyhigh Web Gateway, etc.

Real-time Response

Share reputation and actions across the ecosystem

Fast, reliable, and scalable communication fabric (DXL)

What differentiates Trellix Threat Intelligence Exchange?

Flexible Deployment

Customer Values

Trellix empowers organizations with complex, constrained and on-prem networks to leverage the Trellix connected security platform with flexible deployment options.

Platform Integrations

Customer Values

Automatic threat intelligence sharing and actionability across the ecosystem beyond just endpoints, including industry leading sandbox with IVX.

Real-time Response

Customer Values

Organizations respond to threats in real-time across the security ecosystem

What differentiates Trellix EDR?

AI Guided Investigations

AI Investigations expertly steer analysts to faster and more effective responses.

Relevant questions asked and answered reducing time spent by analysts to triage

Direct Endpoint Queries at Scale

Quickly execute hunting queries directly on endpoints to speed investigations

Disrupt evasive attackers with direct client access

Integrated EDR and Forensics

Unified deployment and updates for EDR and Forensics (HX)

Added enrichment with deep endpoint visibility

What differentiates Trellix EDR?

AI Guided Investigations

Customer Values

Security analysts' skills are upleveled for faster investigations

Direct Endpoint Queries at Scale

Customer Values

Faster MTTD and MTTR through real-time data directly from endpoints at scale

Integrated EDR and Forensics

Customer Values

Deploying and updating EDR and Forensics (HX) software is effortless, saving you valuable time and resources.

Before

- ✓ Are we protected?
- ✓ How do we minimize the attack surface?
- ✓ How do we improve our security posture?

During

- ✓ What is happening?
- ✓ What should we investigate?
- ✓ What action should we take?

After

- ✓ What is the scope? Are other endpoints affected?
- ✓ How did the attacker get in?
- ✓ How do we make sure it does not happen again?

Trellix Endpoint Forensics (HX)

- Forensics and root cause analysis
- Real-time and historical artifacts search
- Long-term remediation

Trellix

What differentiates Trellix Endpoint Forensics (HX)?

Flexible Deployment

AI Investigations expertly steer analysts to faster and more effective responses.

Relevant questions asked and answered reducing time spent by analysts to triage

Forensics at Scale

Quickly execute hunting queries directly on endpoints to speed investigations

Disrupt evasive attackers with direct client access

Advanced Forensic Data Acquisition

Unified deployment and updates for EDR and Forensics (HX)

Added enrichment with deep endpoint visibility

What differentiates Trellix Endpoint Forensics (HX)?

Flexible Deployment

Customer Values

Uncover hidden threats, investigate security incidents, and safeguard your endpoints with confidence, regardless of your network configuration.

Forensics at Scale

Customer Values

Improved security posture across large and complex environments when the root cause of an incident is understood

Advanced Forensic Data Acquisition

Customer Values

Ability to root out sophisticated attackers to prevent them from reusing footholds in the organization.

Summary - Trellix Endpoint Solutions

Trellix Endpoint Security (ENS)

- Pro-active attack surface management
- Rich and fully-featured threat prevention stack

What's The Value?

- Consistent solid results in AV-Test, AV-Comparatives, and SE Labs while outperforming competition for protection and false positives all with comparable performance
- Enhanced remediation intelligently rolls back ransomware changes and retains suspicious artifacts
- Protection in cloud connected AND disconnected networks

Trellix Insights, TIE, Trellix EDR

- Efficient and effective alerts and incidents triage
- Fast response and containment

What's The Value?

- Highest fidelity and AI-prioritized alerting for faster investigations
- Faster MTTD and MTTR through real-time data directly from endpoints at scale
- Automatically provide answers to SOC analysts with visualization and guidance

Trellix Endpoint Forensics (HX)

- Forensics and root cause analysis
- Real-time and historical artifacts search

What's The Value?

- Flexible and unified deployment from ePO for seamless pivot into adv. Forensics for incident responders
- Forensic investigations at scale to 100k systems with automated forensic data and file acquisition
- Pre-configured expert data acquisition libraries with customizable point and click data acquisition for incident responders

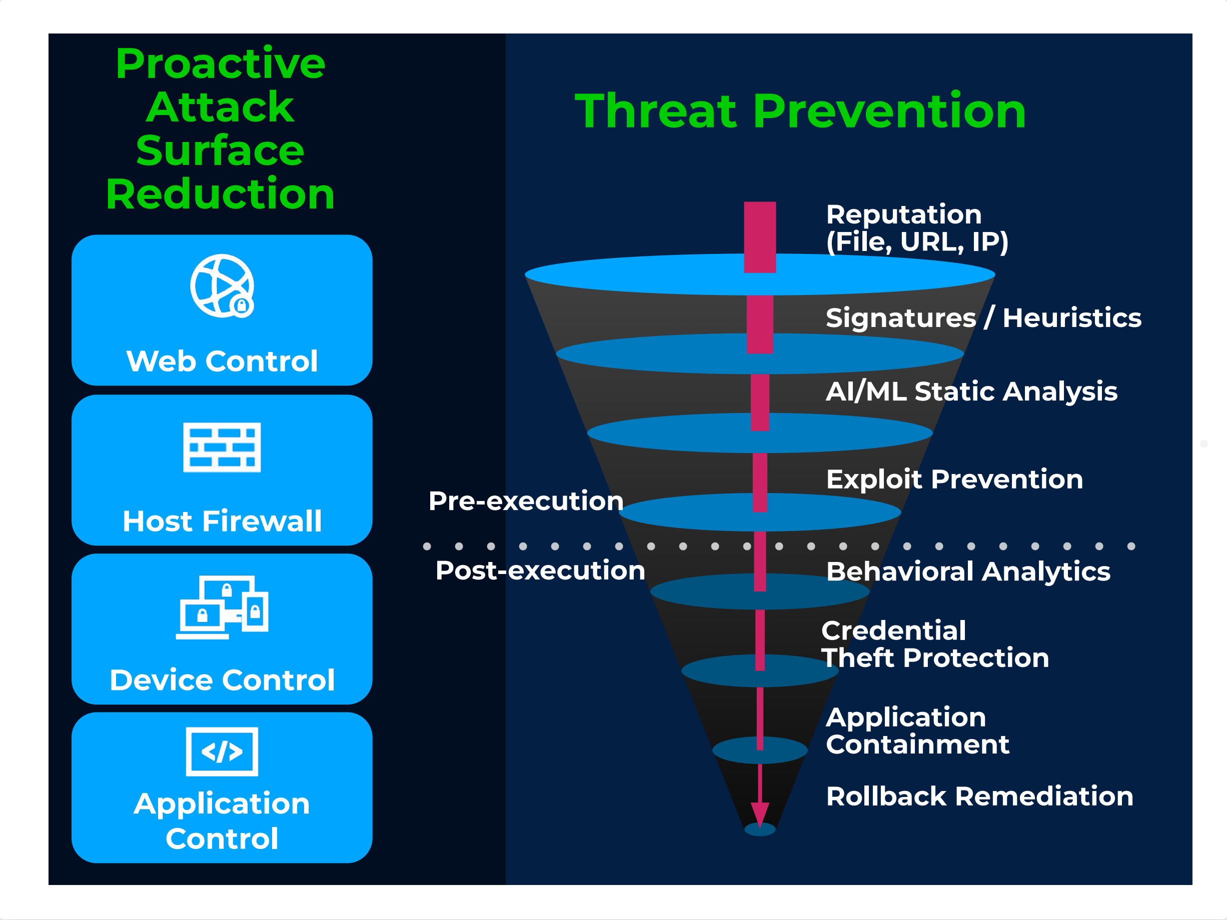
Trellix

About Trellix Endpoint Solutions

Overview and Product Tour

Trellix Endpoint Security (ENS)

- Multi-Platform, Multi-Device
- Multi-Layered Defense
- Multi-Stage Detection and Response



Proactive Attack Surface Reduction

Web Control

Host Firewall

Device Control

Application Control

Threat Prevention

Reputation (File, URL, IP)

Signatures / Heuristics

AI/ML Static Analysis

Exploit Prevention

Pre-execution

Post-execution

Behavioral Analytics

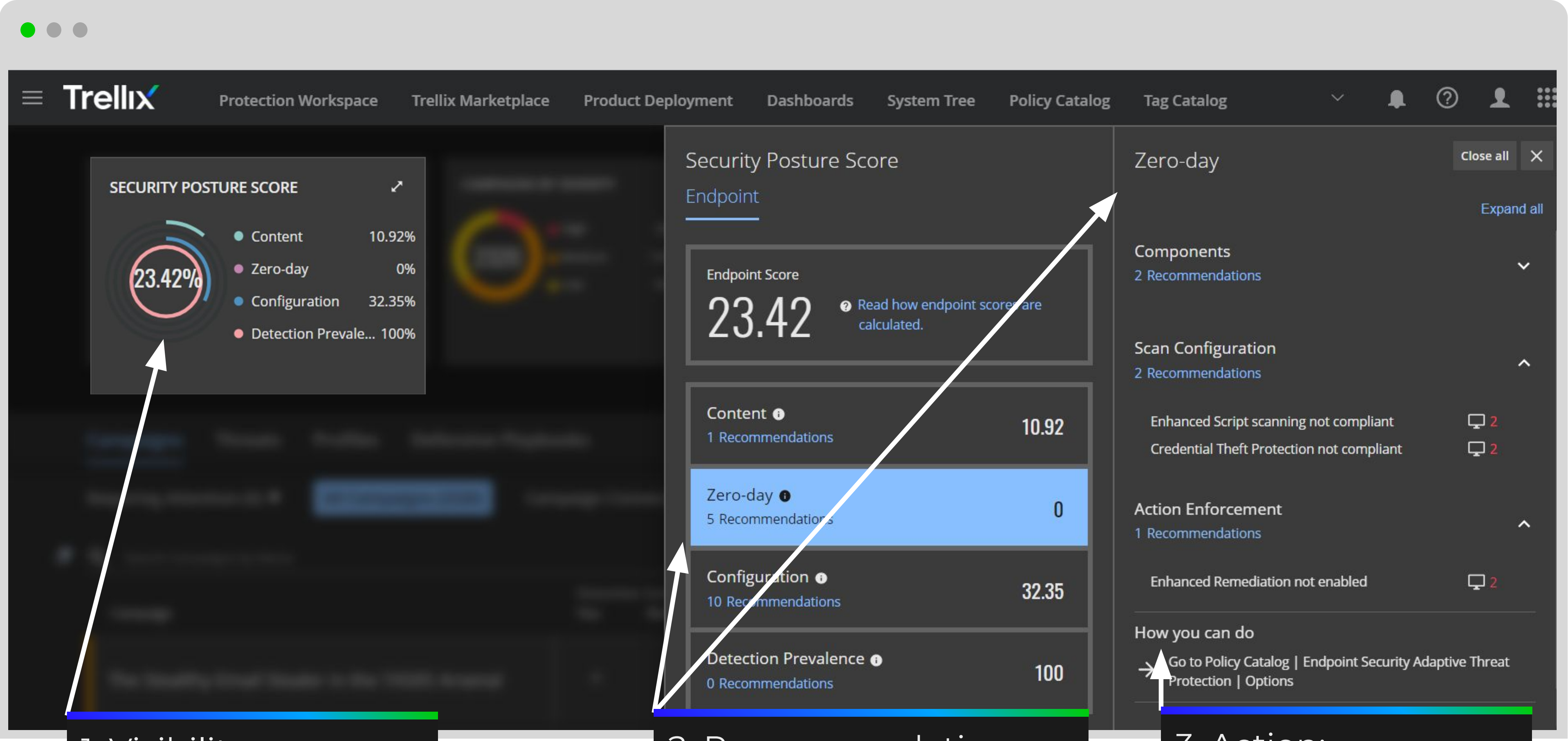
Credential Theft Protection

Application Containment

Rollback Remediation

Trellix

Trellix Insights



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

Close all

Expand all

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

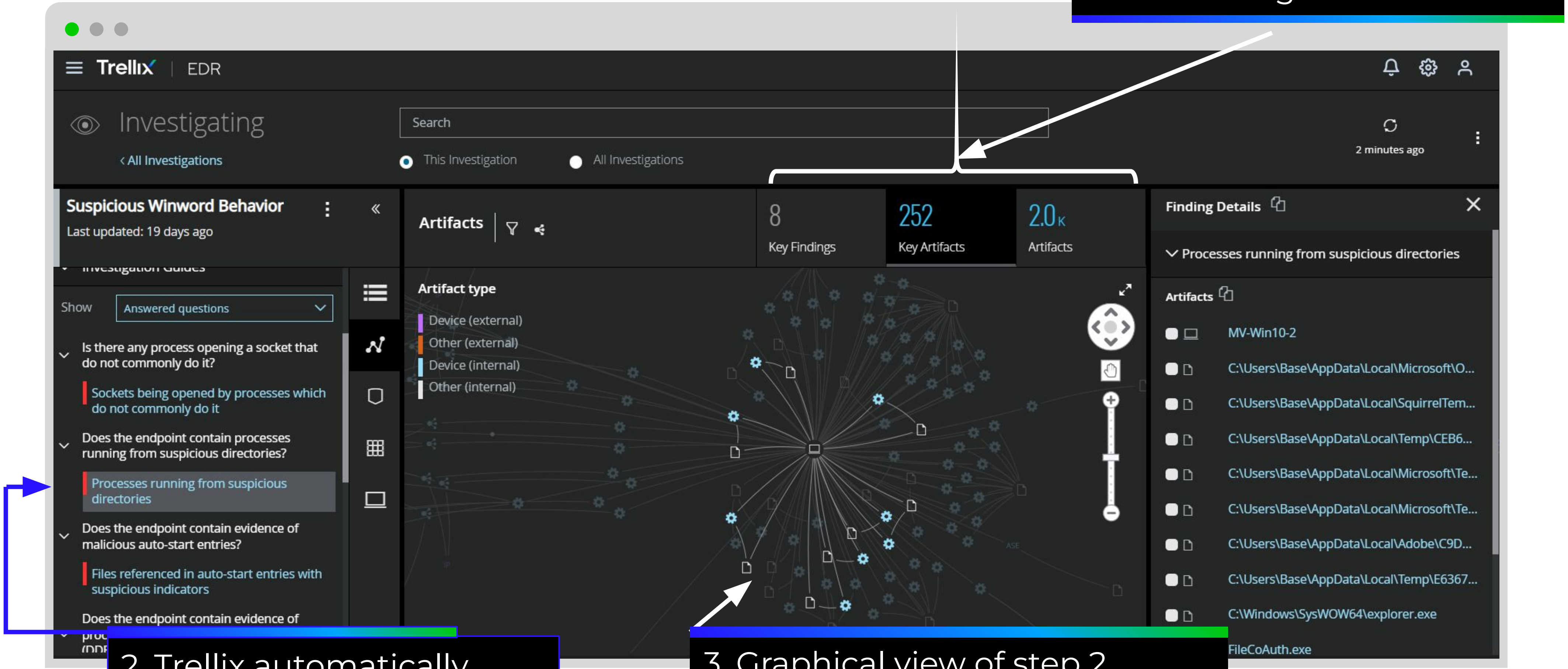
2. Recommendations:
five actions to improve Zero-day protection

3. Action:
jump to Policy Catalog

Trellix

Trellix Endpoint Detection and Response (EDR)

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



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

Processes running from suspicious directories

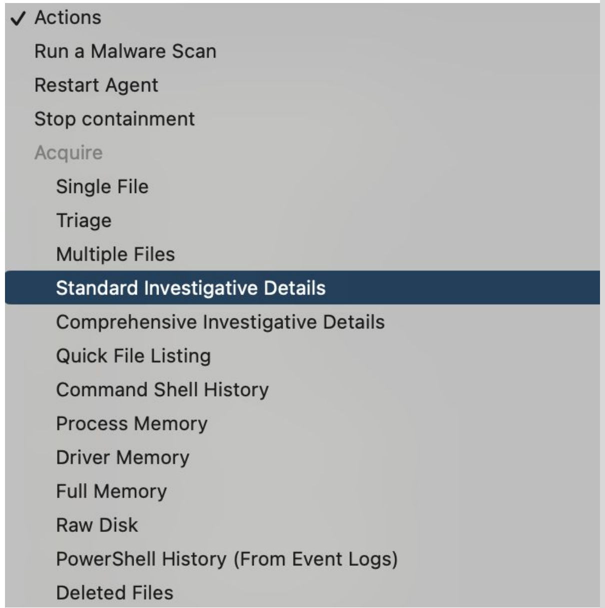
- MV-Win10-2
- C:\Users\Base\AppData\Local\Microsoft\O...
- C:\Users\Base\AppData\Local\SquirrelTem...
- C:\Users\Base\AppData\Local\Temp\CEB6...
- C:\Users\Base\AppData\Local\Microsoft\Te...
- C:\Users\Base\AppData\Local\Microsoft\Te...
- C:\Users\Base\AppData\Local\Adobe\C9D...
- C:\Users\Base\AppData\Local\Temp\E6367...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

2. Trellix automatically provides answers to the SOC analysts

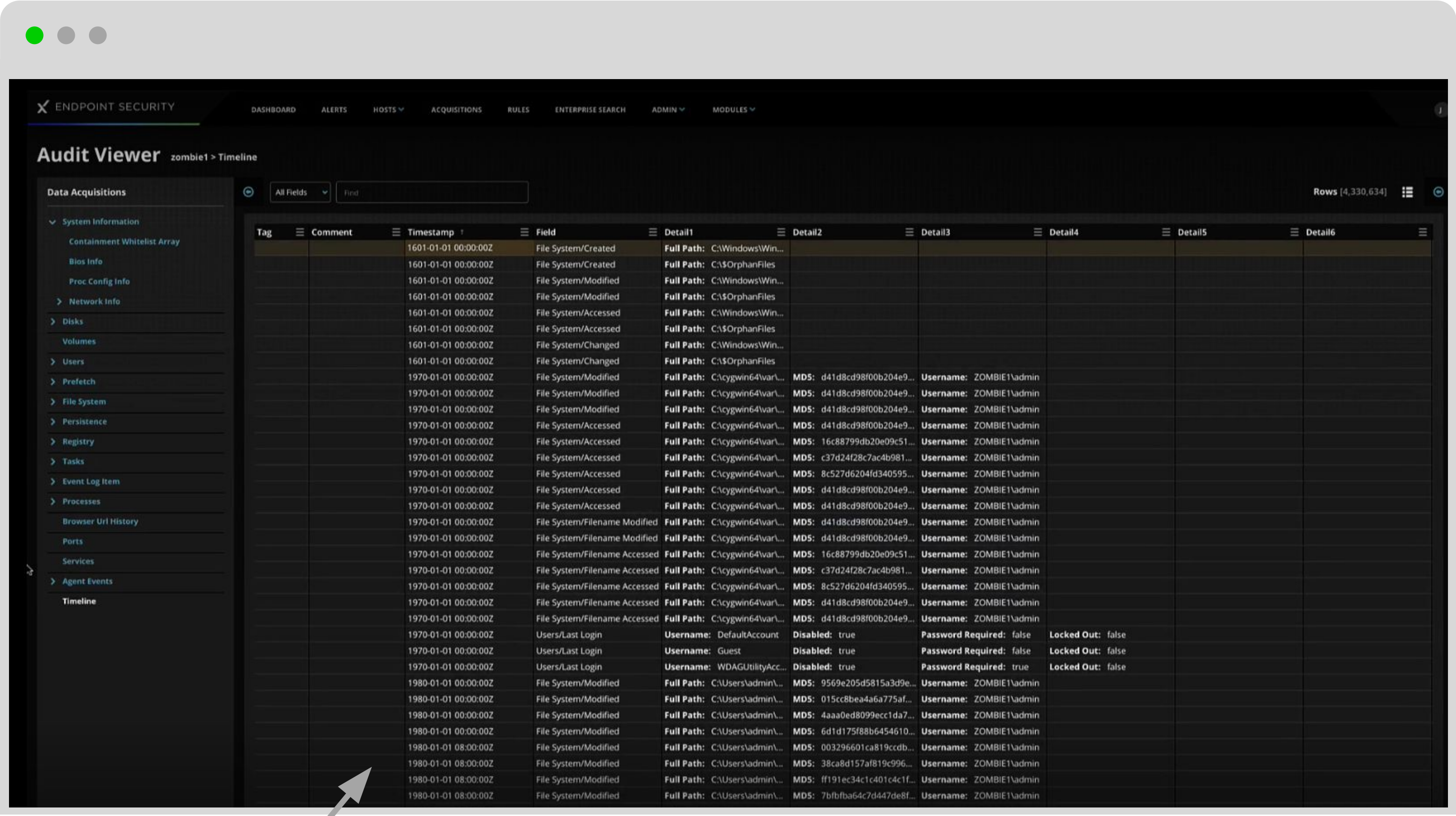
3. Graphical view of step 2 results to guide the analyst to get further details

Trellix

Trellix Endpoint Forensics (HX)



- ✓ Actions
- Run a Malware Scan
- Restart Agent
- Stop containment
- 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)
  - Deleted Files



Audit Viewer zombie1 > Timeline

Data Acquisitions

- System Information
  - Containment Whitelist Array
  - Bios Info
  - Proc Config Info
  - Network Info
- Disks
- Volumes
- Users
- Prefetch
- File System
- Persistence
- Registry
- Tasks
- Event Log Item
- Processes
- Browser Url History
- Ports
- Services
- Agent Events
- Timeline

All Fields | Find

Rows [4,330,634]

Tag	Comment	Timestamp ↑	Field	Detail1	Detail2	Detail3	Detail4	Detail5	Detail6
		1601-01-01 00:00:00Z	File System/Created	Full Path: C:\Windows\Win...					
		1601-01-01 00:00:00Z	File System/Created	Full Path: C:\$OrphanFiles					
		1601-01-01 00:00:00Z	File System/Modified	Full Path: C:\Windows\Win...					
		1601-01-01 00:00:00Z	File System/Modified	Full Path: C:\$OrphanFiles					
		1601-01-01 00:00:00Z	File System/Accessed	Full Path: C:\Windows\Win...					
		1601-01-01 00:00:00Z	File System/Accessed	Full Path: C:\$OrphanFiles					
		1601-01-01 00:00:00Z	File System/Changed	Full Path: C:\Windows\Win...					
		1601-01-01 00:00:00Z	File System/Changed	Full Path: C:\$OrphanFiles					
		1970-01-01 00:00:00Z	File System/Modified	Full Path: C:\cygwin64\var\...	MD5: d41d8cd98f00b204e9...	Username: ZOMBIE1\admin			
		1970-01-01 00:00:00Z	File System/Modified	Full Path: C:\cygwin64\var\...	MD5: d41d8cd98f00b204e9...	Username: ZOMBIE1\admin			
		1970-01-01 00:00:00Z	File System/Modified	Full Path: C:\cygwin64\var\...	MD5: d41d8cd98f00b204e9...	Username: ZOMBIE1\admin			
		1970-01-01 00:00:00Z	File System/Accessed	Full Path: C:\cygwin64\var\...	MD5: d41d8cd98f00b204e9...	Username: ZOMBIE1\admin			
		1970-01-01 00:00:00Z	File System/Accessed	Full Path: C:\cygwin64\var\...	MD5: 16c88799db20e09c51...	Username: ZOMBIE1\admin			
		1970-01-01 00:00:00Z	File System/Accessed	Full Path: C:\cygwin64\var\...	MD5: c37d24f28c7ac4b981...	Username: ZOMBIE1\admin			
		1970-01-01 00:00:00Z	File System/Accessed	Full Path: C:\cygwin64\var\...	MD5: 8c527d6204fd340595...	Username: ZOMBIE1\admin			
		1970-01-01 00:00:00Z	File System/Accessed	Full Path: C:\cygwin64\var\...	MD5: d41d8cd98f00b204e9...	Username: ZOMBIE1\admin			
		1970-01-01 00:00:00Z	File System/Accessed	Full Path: C:\cygwin64\var\...	MD5: d41d8cd98f00b204e9...	Username: ZOMBIE1\admin			
		1970-01-01 00:00:00Z	File System/Filename Modified	Full Path: C:\cygwin64\var\...	MD5: d41d8cd98f00b204e9...	Username: ZOMBIE1\admin			
		1970-01-01 00:00:00Z	File System/Filename Modified	Full Path: C:\cygwin64\var\...	MD5: d41d8cd98f00b204e9...	Username: ZOMBIE1\admin			
		1970-01-01 00:00:00Z	File System/Filename Accessed	Full Path: C:\cygwin64\var\...	MD5: 16c88799db20e09c51...	Username: ZOMBIE1\admin			
		1970-01-01 00:00:00Z	File System/Filename Accessed	Full Path: C:\cygwin64\var\...	MD5: c37d24f28c7ac4b981...	Username: ZOMBIE1\admin			
		1970-01-01 00:00:00Z	File System/Filename Accessed	Full Path: C:\cygwin64\var\...	MD5: 8c527d6204fd340595...	Username: ZOMBIE1\admin			
		1970-01-01 00:00:00Z	File System/Filename Accessed	Full Path: C:\cygwin64\var\...	MD5: d41d8cd98f00b204e9...	Username: ZOMBIE1\admin			
		1970-01-01 00:00:00Z	File System/Filename Accessed	Full Path: C:\cygwin64\var\...	MD5: d41d8cd98f00b204e9...	Username: ZOMBIE1\admin			
		1970-01-01 00:00:00Z	Users/Last Login	Username: DefaultAccount	Disabled: true	Password Required: false	Locked Out: false		
		1970-01-01 00:00:00Z	Users/Last Login	Username: Guest	Disabled: true	Password Required: false	Locked Out: false		
		1970-01-01 00:00:00Z	Users/Last Login	Username: WDAGUtilityAcc...	Disabled: true	Password Required: true	Locked Out: false		
		1980-01-01 00:00:00Z	File System/Modified	Full Path: C:\Users\admin\...	MD5: 9569e205d5815a3d9e...	Username: ZOMBIE1\admin			
		1980-01-01 00:00:00Z	File System/Modified	Full Path: C:\Users\admin\...	MD5: 015cc8bea4a6a775af...	Username: ZOMBIE1\admin			
		1980-01-01 00:00:00Z	File System/Modified	Full Path: C:\Users\admin\...	MD5: 4aaa0ed8099ecc1da7...	Username: ZOMBIE1\admin			
		1980-01-01 00:00:00Z	File System/Modified	Full Path: C:\Users\admin\...	MD5: 6d1d175f88b6454610...	Username: ZOMBIE1\admin			
		1980-01-01 08:00:00Z	File System/Modified	Full Path: C:\Users\admin\...	MD5: 003296601ca819ccdb...	Username: ZOMBIE1\admin			
		1980-01-01 08:00:00Z	File System/Modified	Full Path: C:\Users\admin\...	MD5: 38ca8d157af819c996...	Username: ZOMBIE1\admin			
		1980-01-01 08:00:00Z	File System/Modified	Full Path: C:\Users\admin\...	MD5: ff191ec34c1c401c4c1f...	Username: ZOMBIE1\admin			
		1980-01-01 08:00:00Z	File System/Modified	Full Path: C:\Users\admin\...	MD5: 7bfbfba64c7d447de8f...	Username: ZOMBIE1\admin			

1. Create and customize data acquisition profiles across multiple endpoints

2. Get a time-based comprehensive audit report

DEMO

Trellix

Trellix

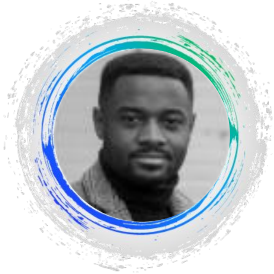
Personas

Targets

Personas

Job Title

Positive Business Outcomes



CISO

Economic Buyer

-Minimize Risk

-Minimize Cost

Leverage existing Investment to reduce risk

- Reduce risk with greater endpoint visibility
- Better positioned for strategic SOC initiatives
- Improve SOC efficiency, within resource constraints

SOC Manager

Champion

- Operational Efficiency
- Metrics: MTTD, MTTR

Streamline operational efficiencies

- Maturing endpoint risk management with EDR and forensics improves security posture to reduce incidents
- Improved SOC efficiencies, MTTD / MTTR metrics
- Reduced incidents, improved staff morale

Security Architect

Champion

- Define technical criteria
- Validate solution outcomes

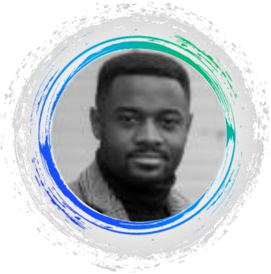
More actionable visibility and control

- Optimized prevention, minimize alerts
- Can prioritize response and remediation effectively
- Better visibility and control to execute daily tasks

Discovery Questions

Job Title

Suggested Discovery Questions



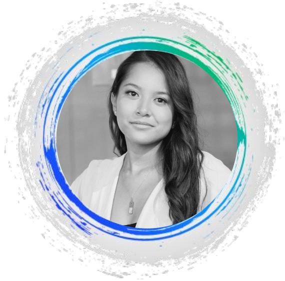
CISO

Economic Buyer

-Minimize Risk

-Minimize Cost

- Have you encountered any challenges or limitations in achieving comprehensive endpoint visibility?
- Are there any specific SOC objectives or goals that you feel could be better achieved with enhanced endpoint visibility and security controls?
- Do you see opportunities for leveraging technology or process improvements to enhance SOC efficiency while working within existing resource constraints?



SOC Manager

Champion

- Operational Efficiency

- Metrics: MTTD, MTTR

- Describe any specific challenges or gaps in your current endpoint risk management strategy?
- Have you identified any areas where your SOC could improve in terms of incident response time or resource utilization?
- Can you describe your current Security Operations Center (SOC) setup and its effectiveness in handling security incidents?

Security Architect

Champion

- Define technical criteria

- Validate solution outcomes

- How do you currently manage and prioritize security alerts within your organization?
- Have you encountered any difficulties in effectively prioritizing response efforts based on the severity and impact of incidents?
- Are there any specific areas where you feel you lack sufficient visibility or control to execute daily security tasks effectively

Trellix

Proof Points

Customer Use Case

Strengthening Trust with Intelligence-Based Trellix Solutions

Customer Success Story: Proactive defense against cyberattacks

Industry: Banking and Finance | Trellix Products: Trellix Endpoint Security, Endpoint Detection and Response, ePO

Challenges

- Increased number and sophistication of cyber threats from bad actors and nation states
- Maintain customer's trust that their data is safe
- Implementation of effective security controls wherever customer data resides and whenever it is accessed

Solutions

- **Trellix Endpoint Security** incorporates mixture of next generation antivirus protection and data encryption, providing proactive defense against intrusion
- **Trellix Endpoint Detection and Response** provides AI-guided threat investigation
- **Trellix Intelligent Virtual Execution** helps catch zero-day malware
- **Trellix ePolicy Orchestrator** offers centralized endpoint security management

Results

- Achieved security compliance for 99.6% of endpoints.
- Enabled isolation of infected devices within minutes of detection
- Improved incident response efficiency of SOC teams.

> "Trellix provides us with actionable intelligence that helps our SOC analysts work through the entire process of identification, response, and remediation." — Chief Information Security Officer, AU Small Finance Bank

Trellix

3rd Party Validation

- Strongest protection in multiple 3rd party tests
- Low false positives
- Low impact on performance

	AV-TEST		AV-Comparatives			
	2023 Award (Corporate) [1]	**Protection / Performance / Usability (max 6)** [2]	**2023 Award - Approved** [3]	**False Positives** [4]	**Malware Protection Rate** [4]	**Impact Score (lower is better)** [4]
Trellix	**Best Protection Corporate Windows**	**6/6/6**	**Business Security, Mac Security**	**Very Low**	**99.7%**	**14.8**
CrowdStrike	-	-	Business Security, Mac Security	Medium Average	99.6%	20.9
Microsoft	-	6/6/6	Business Security, Security Product	Very Low	99.5%	18.5

Product Packaging

What SKUs

Trellix Endpoint Security Offerings

Meeting Customers Where They Are on Their Security Maturity Journey

Endpoint Security Maturity to XDR

SKU	Capabilities	Endpoint Protection	Attack Surface Reduction		Threat Intel	Threat Response at Scale	Cloud EDR	EDR and Advanced Forensics
		ENS	Device Control	App. Control for Desktops	Insights	Threat Intelligence Exchange (TIE)	EDR	Forensics (HX)
MV1	Baseline EPP (ENS)	X	X					
MV2	EPP Plus (ASR, TIE & 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 + EDR + Forensics (on-premises)	X	X	X	X	X		X

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

Trellix

Upsell and Cross Sell

How to position

Upselling to TRXE Value

Decision Criteria to advance endpoint security maturity journey

Step-up SKU	Components	Value Messaging	Customer Positive Outcomes	Discovery Questions
MV2	**Insights**	• Proactive Threat Intelligence • Security Posture Recommendations	• Increased readiness for threat landscape • Optimized existing ENS investment	• Do you know who is targeting you? • How are you getting value from ENS?
	Threat Intelligence Exchange (TIE)	• Take immediate action on unknown processes • Automate file submission to sandbox (IVX)	• Contain new threats immediately at scale • Automated sandbox analysis on unknown files	• How quickly can you block newly discovered threat? • How do you submit unknown files for sandbox analysis?
MV6/7	**EDR**	• AI-guided investigations • Faster investigation and response with direct client query	• Uplevel SOC analyst skills for faster and more efficient investigations • Faster investigations and responses mitigate attack damage	• How do you measure SOC efficiency (MTTD? MTTR?) • How long does it take to query multiple endpoints in investigations?
TRXE	**Endpoint Forensics (HX)**	• Forensics investigations at scale • Advanced data acquisition libraries	• Identify scope of evasive attacker presence in an incident • Forensics provides insights to improve security posture and prevents future attacks	• Are you impacted by repeated incidents? • How did your SOC conduct root-cause analysis in a recent incident?
TRXHX	**MV2 + HX**	• Comprehensive endpoint capabilities, ENS, EDR, and Forensics in on-prem and air-gapped environments	• Endpoint management and protection on-premises • Advanced EDR hunting, detection, response and forensics on-prem	• Do you have visibility and control of endpoints in on-prem environments? • Can you investigate and respond to threats in on-prem environments?

Trellix