

Chapter 13 Trustees MDR Overview

Mark Ponte and Matt Chapman

September 22, 2026

Meet the team



Mark Ponte

Account Executive



Matt Chapman

Consulting
Systems Engineer



Matt Monacelli

Director, Public
Sector Channels
and Alliances

Global Enterprise Cybersecurity **Leader**

Trusted
**Global Security
Leader**

\$1.3B

in ARR* and consistently profitable

*2025, constant currency

6,000

Employees in 75 countries,
headquartered in Japan

Broadest
**Enterprise Security
Platform**

25k

Enterprise organizations
protected

185

Countries with TrendAI™
customers

Leading
**Innovator and
Cybersecurity Expert**

Market leader across

**AI, XDR, Cloud, EPP,
Email, Network***

with over 1,000 global patents

#1 in Public
Vulnerability
Disclosure

With 14 global threat research centers

Recognized Enterprise Leader

Gartner

Leader in
Endpoint Security
Q3 2025



FORRESTER

Leader in Network
Analysis & Visibility
Q4 2025



FORRESTER

Leader in Attack Surface
Management
Q3 2024

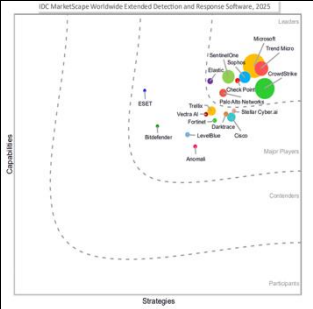


The Customer Choice



IDC

Leader in Extended
Detection & Response
Q3 2025



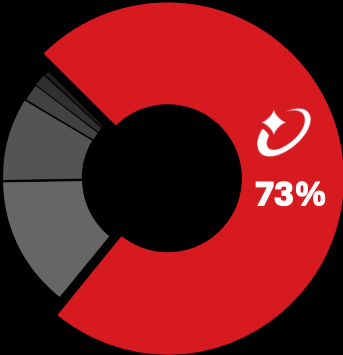
IDC

Leader in Cloud-Native
Application Protection Platform
Q2 2025



OMDIA

Ranked #1 in Public
Vulnerability Disclosure
(2025)



The Partner Choice



Trusted by Leading Enterprises

FORTUNE
GLOBAL
500

As of the end of 2025



**7 of
Top 10**
Banking



**7 of
Top 10**
Automotive



**5 of
Top 10**
Healthcare



**5 of
Top 10**
Petroleum



**4 of
Top 10**
Telecom



**4 of
Top 10**
Technology

Does this sound familiar?

“We’re responsible for IT and security, but we don’t have a dedicated security team watching for threats around the clock.”

“We have security tools in place, but when something suspicious happens, we need to know what matters, what to do, and who can help us respond.”

“We want to make sure bringing in a third party to monitor our environment doesn’t mean giving up control of our systems or data.”



Managed Detection and Response (MDR)

- **It is a SERVICE**
 - **24/7 outsourced cybersecurity service** that combines advanced security technologies with human expertise to monitor an organization's network, detect threats, and actively respond to eliminate them in real time.
- **MDR addresses a major operational challenge:**
 - Many companies buy capable security software but lack the round-the-clock staffing or specialized skills required to run an internal, full-time **Security Operations Center (SOC)**.

How MDR Works

- 1. Continuous Telemetry & Monitoring:** The MDR provider collects and monitors data from endpoints (laptops/servers), cloud environments, network traffic, and user identities.
- 2. Advanced Analytics:** Rather than relying purely on simple, signature-based alerts, MDR uses artificial intelligence, machine learning, and behavioral analytics to catch subtle, unusual activity.
- 3. Human Expertise & Threat Hunting:** When a suspicious anomaly is flagged, human analysts step in to investigate. Experts proactively "hunt" through the system to uncover hidden attackers who may have bypassed automated filters.
- 4. Active Containment & Mitigation:** Unlike traditional alert-only services, an MDR provider has pre-authorized permission to act immediately. They can remotely isolate a compromised laptop, block malicious traffic, or kill a ransomware process before it spreads.

Key Differences: MDR vs. EDR vs. MSSP

Service Type	Scope & Focus	Human Component
EDR (Endpoint Detection & Response)	Software tool focused purely on individual devices (laptops, desktops, servers).	None by default; it is a tool your own team must manage.
MSSP (Managed Security Service Provider)	Broad security management, focusing on compliance, firewalls, and forwarding high volumes of log alerts.	Primarily administrative; they notify your team when something goes wrong but rarely hunt or contain threats directly.
MDR (Managed Detection & Response)	Holistic coverage across endpoints, network, and cloud, explicitly focused on finding and stopping active attackers.	High; backed by a fully staffed, 24/7 outsourced SOC that actively mitigates incidents on your behalf.

Legal Services firms are being hit from four directions at once

The threat is high-tempo, multi-vector, and escalating.

01 Organized extortion crews

UNC3753 / Silent Ransom Group and BlackFile (UNC6671 / “The Com”). Vishing and IT-support impersonation → remote access → data theft → leak-site extortion. No encryptor needed.

02 Access brokers → ransomware

Brokers (ProfessorKliq, Asian_Baddie) sell footholds for \$700–\$6,000; Qilin & Akira buy in and deploy. A live pipeline turning cheap access into extortion within 30–90 days.

03 Nation-state

Chinese state-linked actors breached Williams & Connolly, a top US firm (client notice 2025-10-07). A distinct, higher tier for firms with government or national-security clients.

04 Physical intrusion

Russian-linked actors outsource burglaries to plant USB implants; insiders paid ~\$500. A vector no purely-cyber control can address, now a front-desk and facilities problem too.

Why Trustee Offices Are High-Value Targets

A concentrated risk environment

- Sensitive data
 - SSNs
 - Tax returns
 - Bank information
 - Addresses and employer data
- Critical operations
 - Payment processing
 - Disbursements
 - Case administration
 - Creditor and debtor communications
- Common security challenges
 - Limited IT resources
 - Remote staff
 - Fragmented tools
 - Incomplete logging
 - Unvalidated recovery procedures

Why "Legal Services" are a priority, not opportunistic, target

- **Premium data**
 - Privileged communications, M&A details, client financials and litigation strategy, high extortion leverage and high resale value.
- **Theft alone is enough**
 - Extortion crews steal and threaten to publish without ever encrypting, so backups are not a sufficient defense.
- **Soft attack surface**
 - Historically thin endpoint defenses and reliance on legacy remote access (RDWeb, SonicWall VPN); brokers pre-screen for weak or absent EDR.
- **A distinct top tier**
 - Firms with government, national-security or high-profile corporate clients face nation-state interest on top of the criminal threat.
- **The shift.**
 - The sector has moved from opportunistic ransomware target to a deliberate, repeatedly-targeted one, confirmed by a dedicated FBI advisory to law firms (2026-05-26).



Industry-Leading
AI Security Platform

Cyber Risk Exposure Management

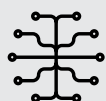
Vulnerability Management, Risk, ASM, EASM, CSPM

Security Operations

XDR, Agentic SIEM, Agentic SOAR

Threat Intelligence

Threat Intelligence Platform, Threat Intel Feed, Adversary Research



**AI App
Security**



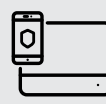
**Cloud
Security**



**Data
Security**



**Email
Security**



**Endpoint
Security**



**Identity
Security**



**Network
Security**

Services



**Industry-Leading
AI Security Platform**

Cyber Risk Exposure Management
Vulnerability Management, Risk, ASM, EASM, CSPM

Security Operations
XDR, Agentic SIEM, Agentic SOAR

Threat Intelligence
Threat Intelligence Platform, Threat Intel Feed, Adversary Research



**AI App
Security**



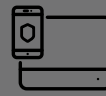
**Cloud
Security**



**Data
Security**



**Email
Security**



**Endpoint
Security**

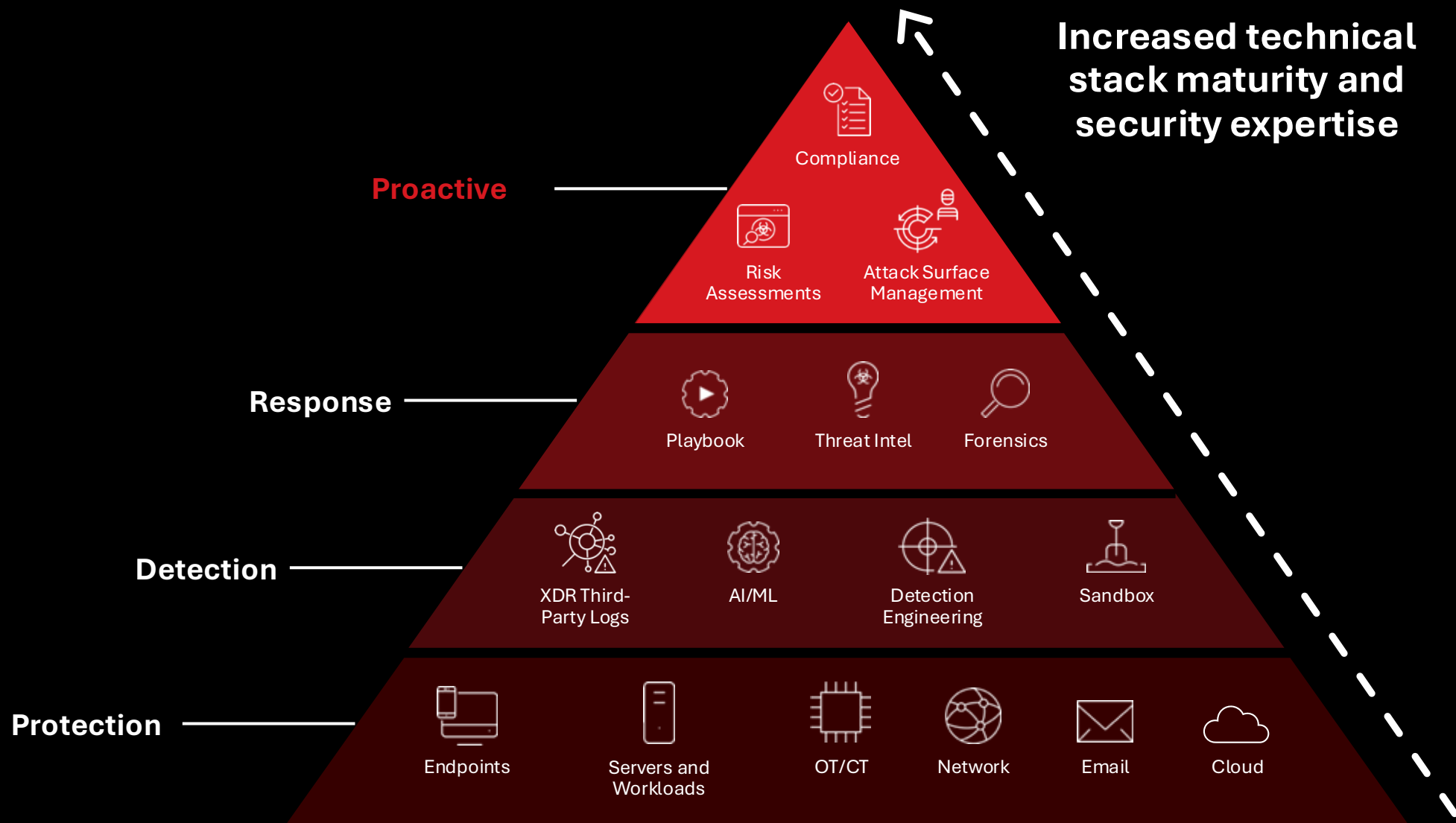


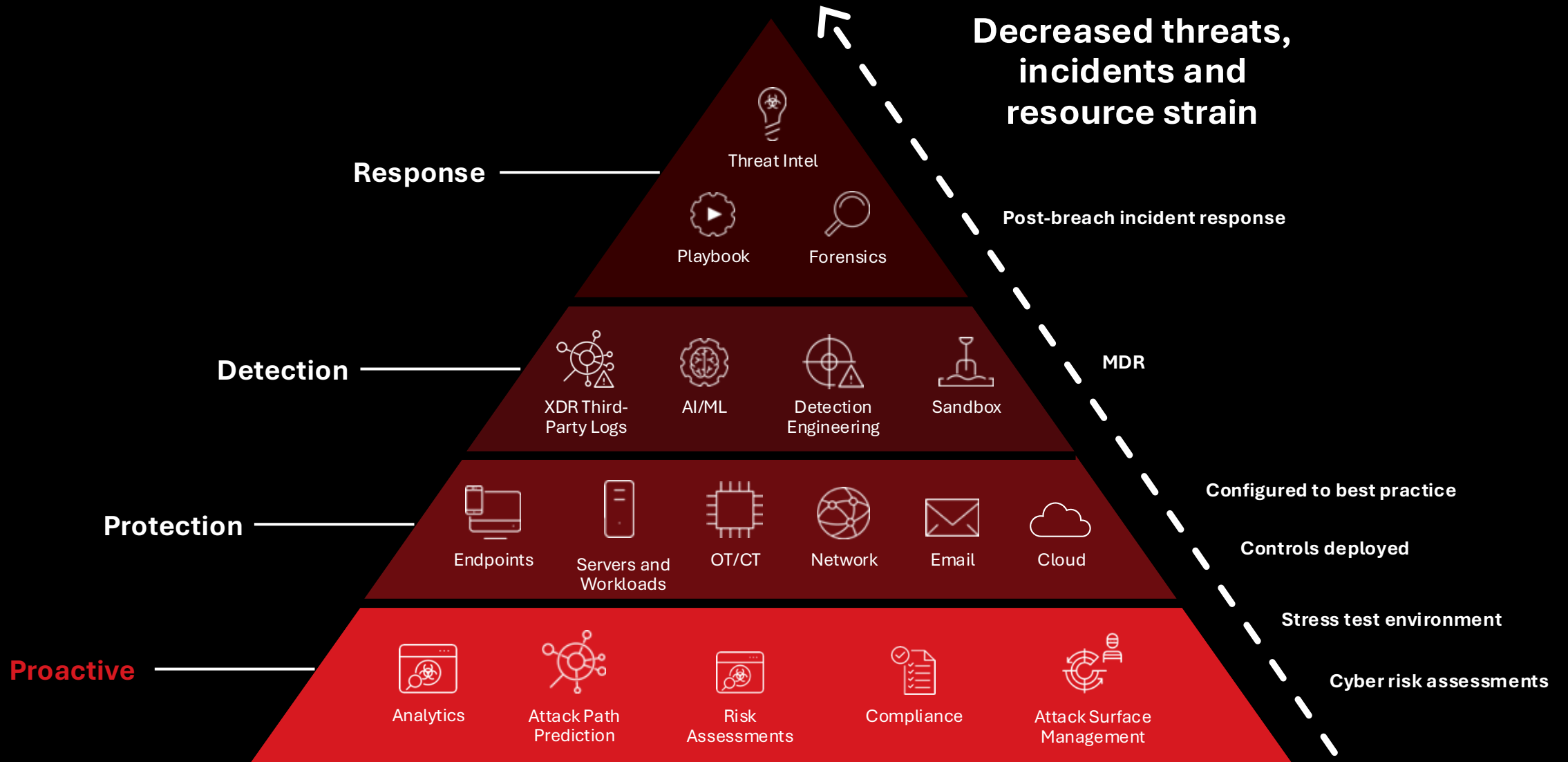
**Identity
Security**



**Network
Security**

Services





Proactive security starts here

What this means for Chapter 13 Trustee Offices

Confidence in your defenses



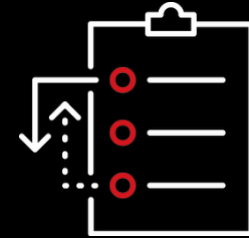
Know your security controls are working and better prepared to withstand real-world threats

Operational resilience



Keep critical operations and business continuity

Freedom to focus on what matters



Extend your team with trusted specialists, while you focus on the highest priorities.

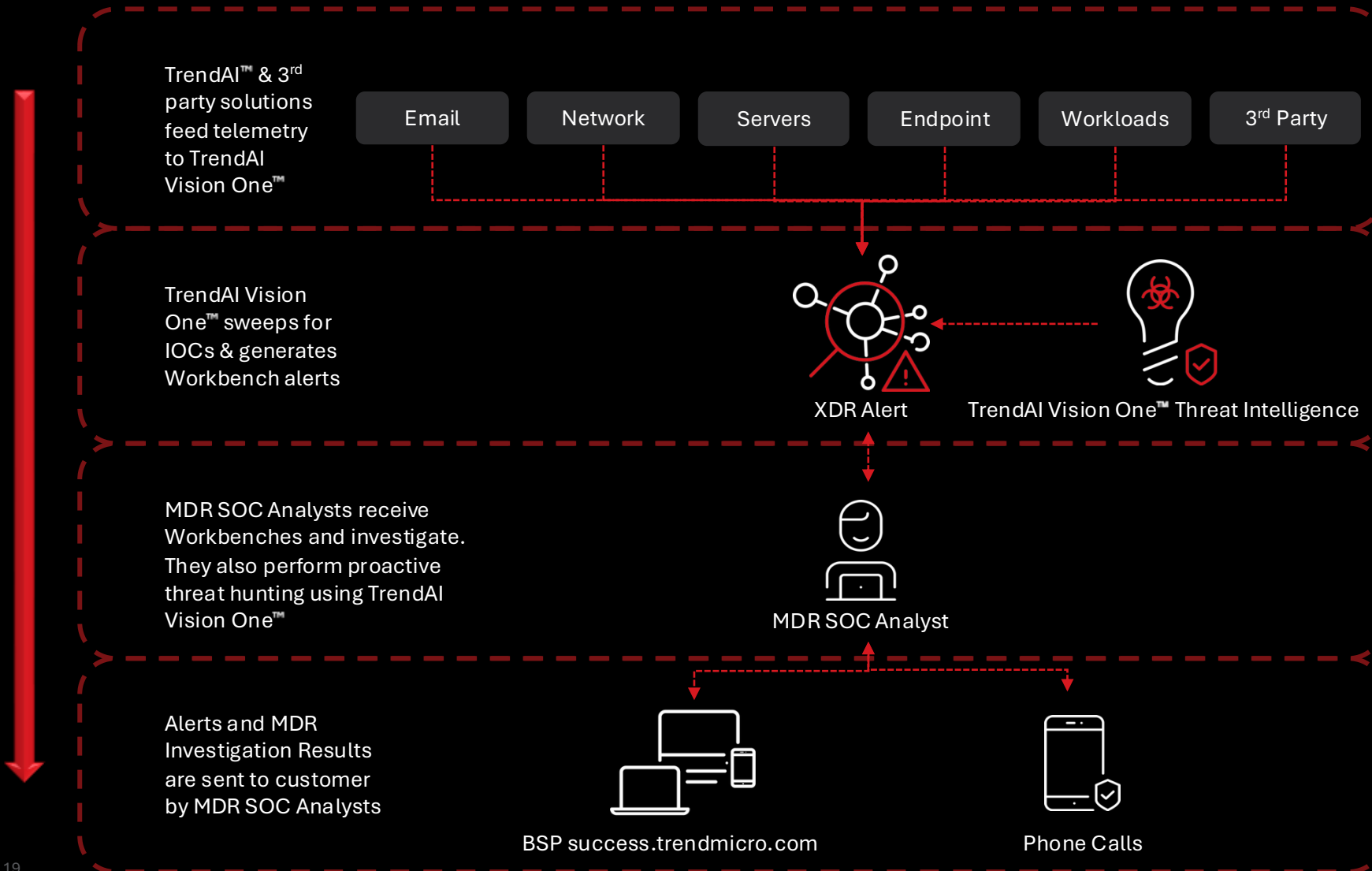
Extend your team with trusted 24/7 cybersecurity experts

What this means for Chapter 13 Trustee Offices



Extend your team with trusted 24/7 cybersecurity experts

Adaptive MDR across native and third-party telemetry



MDR investigation triggers:

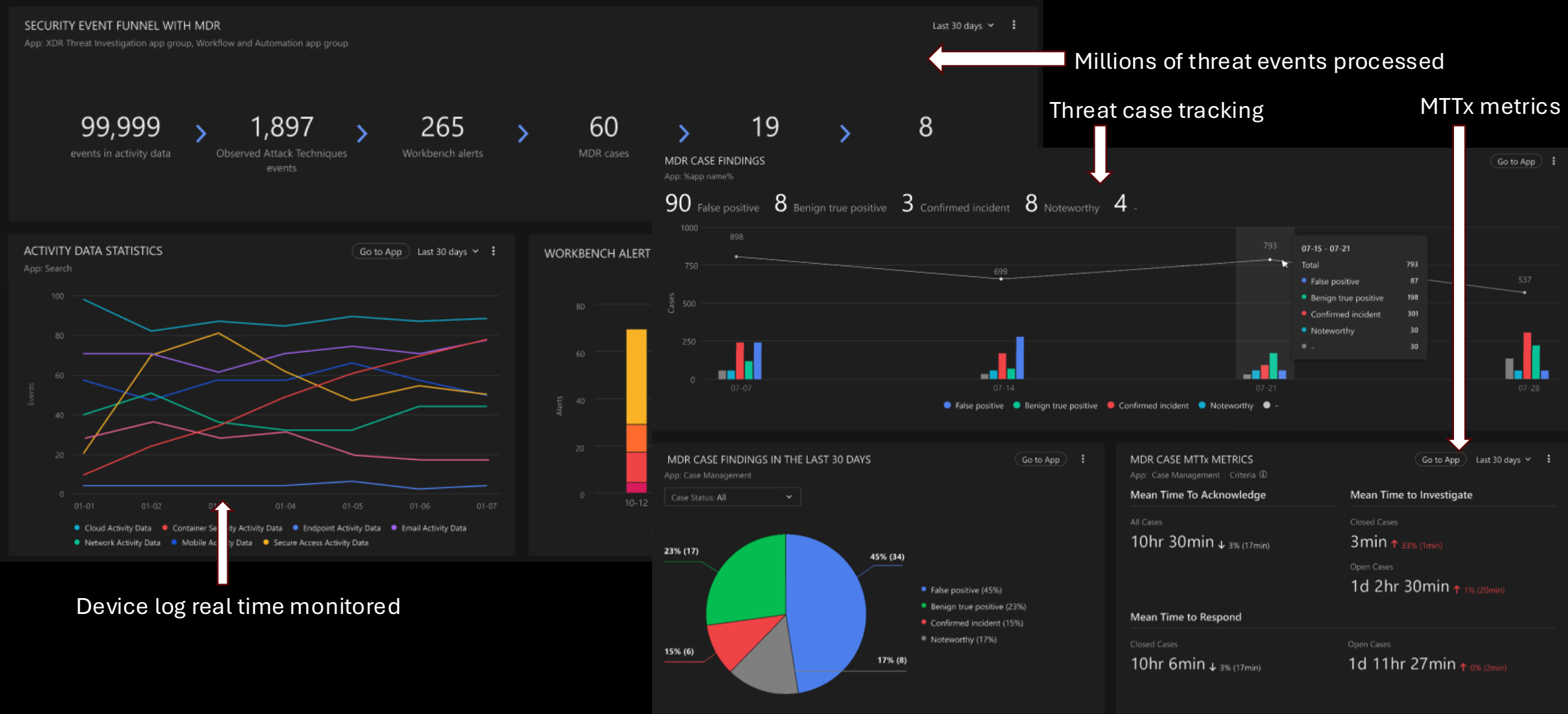
- **TrendAI Vision One™ Workbenches (XDR Alert)**
 - Telemetry
 - IOC Sweep + hit (*TrendAI Vision One™ Intelligence Report*)
- **Threat Hunting**
 - OAT, Workbench, or Other Telemetry
- **Customer inbound via BSP**
 - Request investigation
 - Declare an incident
 - Request quarterly service review



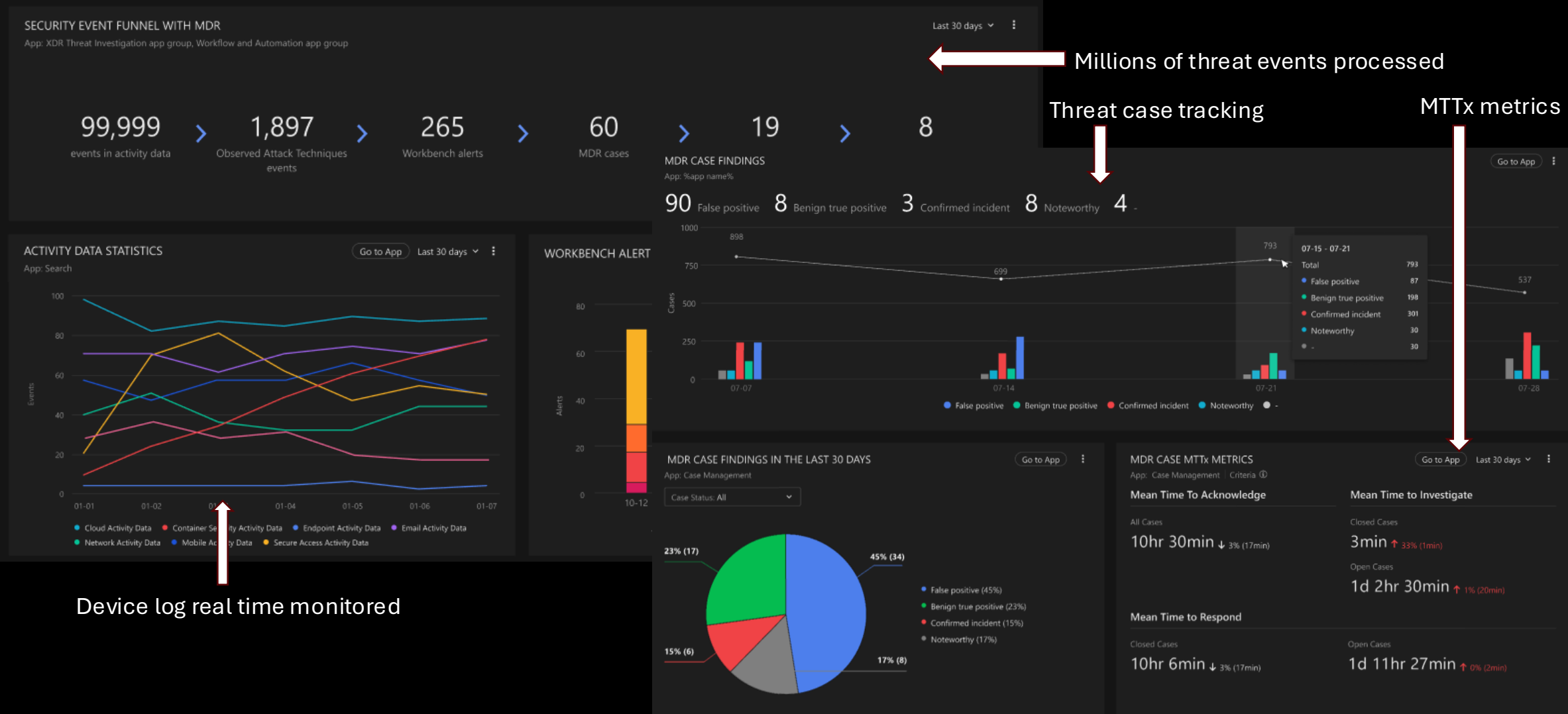
Security results delivered at scale

- **Faster investigation and response** through AI-assisted analysis and expert-led investigation and response workflows.
- **Earlier awareness of emerging threats** through threat research and intelligence that informs detection and investigation before threats reach your environment.
- **Reduced security risk and incident impact** through earlier prioritization, cross-domain correlation, and threat hunting.
- **Consistent MDR across regions and environments** through standardized, platform-driven investigation and response.
- **Clear visibility into MDR activity and outcomes** through case management, audit trails, and reporting.

See what MDR is doing for your organization



See what MDR is doing for your organization



Understand your security activity over time

TrendAI

TrendAI Managed Detection and Response (MDR) - Monthly Report

Reporting period from March 1, 2026 to March 31, 2026

Executive Summary

MDR Security Event Funnel

During this reporting period, Trend Vision One identified **211,279** security events. Of these events, **41** were classified as MDR incidents. The MDR security analysts reviewed **106** Workbenches.

- Trend Vision One identified **211,279** security events
- These events generated **106** Workbenches
- The MDR security analysts reviewed **41** incidents
- Of these cases, **0** were classified as MDR incidents

For more information, see the **24x7 Critical Incident Response Center**.

Activity data	Observed Attack Techniques	Workbenches alerts
62,741,341	211,279	106

Generated: 2026-04-02 03:04:04 UTC

Executive Summary

TrendAI

MDR Security Event Funnel

During this reporting period, Trend Vision One processed **62,741,341** activity data from your organization for the time period between March 1, 2026 and March 31, 2026. From these events:

- Trend Vision One identified **211,279** Observed Attack Techniques events
- These events generated **106** Workbench alerts
- The MDR security analysts reviewed the Workbench alerts and opened **4** cases
- Of these cases, **0** were classified as noteworthy and **1** were confirmed as actual security incidents

For more information, see the **24x7 Critical Alerting and Monitoring** section of this report.

Activity data	Observed Attack Techniques	Workbench alerts	MDR cases	Noteworthy cases	Confirmed incident
62,741,341	211,279	106	4	0	1

Page 5 of 15

Executive Summary



Monitoring sources

This graph shows the distribution of security events by monitoring source for the reporting period:



24/7 Critical Alerting and Response

This section summarizes all MDR cases and ongoing cases.

MDR case findings in the last 24 hours



Case findings

- Benign True Positive
- True Positive
- False Positive
- Noteworthy
- Other Findings
- -

Confirmed incident

1

Incident details

Incident details

Page 11 of 15

TrendAI

24/7 Critical Alerting and Monitoring

This section summarizes all MDR security cases during this reporting period, including closed and ongoing cases.

MDR case findings in the last 30 days

4
MDR case findings

Case findings	% of total cases	Cases
Benign True Positive	50%	2
True Positive	25%	1
False Positive	25%	1
Noteworthy	0%	0
Other Findings	0%	0
-	0%	0

Case findings	% of total cases	Cases
Benign True Positive	50%	2
True Positive	25%	1
False Positive	25%	1
Noteworthy	0%	0
Other Findings	0%	0
-	0%	0

Page 11 of 15

Incident report from MDR analyst

TrendAI Vision One™
Services – Managed
Detection and Response
(MDR)



TrendAI Incident Report

TM-03922047

March 27, 2026

Executive Summary

TrendAI Vision One™ Services – Managed Detection and Response (MDR) responded to an incident on 2026-03-17 19:06:15 and 2026-03-26 22:12:26. TrendAI experienced a targeted phishing attack that resulted in malware execution and sustain days, the attacker escalated privileges, compromised the domain, and gained control of critical file server. Sensitive data from a central project share (C:\Shares\projectAI) was then exfiltrated and confidentiality. Several mitigations have been recommended for your organization to perform to reduce the risk.

Service Details

Engagement Commencement	2026/03/17 UTC
Incident Case Reference	TM-03922047
Entitlement	TrendAI Vision One™ Services – Complete
Response Phase	Remediation & Recovery
Incident Trigger	TrendAI Vision One™
Incident Severity	Critical

Report Versioning

Version	Version Date	
Initial Draft (0.1)	2026/03/27	Initial draft – Pending pr

1. Incident Scope

Scope of Compromise

The tables below delineate the extent of compromise, encapsulating details regarding impacted hosts and user accounts throughout the investigation.

Hosts	
Hostname (IP)	Remarks
us-mdr-vm1 (172.16.0.19)	Regular user workstation, initial compromised host. Evidence of user execution (v1AI.credential dumping (mimikatz.exe)
use-mdr-vm2 (172.16.0.20)	Regular user workstation, evidence of collection using aliautomation2.exe (renamed via potential exfiltration via havoc beacon.
mlw-mdr-dc01 (172.16.0.31)	Domain controller, evidence of AD database credential dumping (ntds.dit), AD recon Bloodhound (20260325110817_BloodHound.zip), potential Kerberos golden ticket abuse creation of new domain user malware/solomon.
mlw-mdr-fs01 (172.16.0.13)	File server, evidence of exfiltration using automation3.exe (rename rclone.exe).

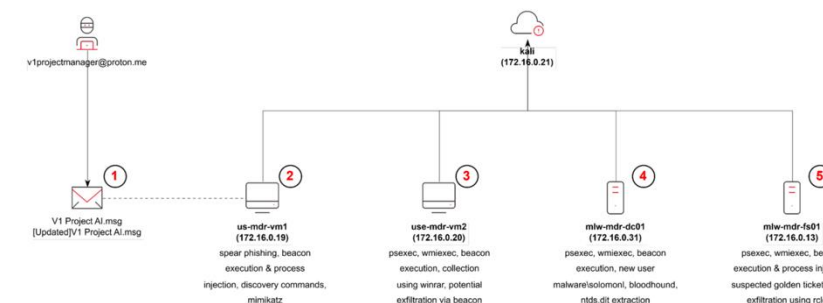
Users	
Domain\Username	Remarks
us-mdr-vm1\ryans	User who was spear-phished that lead to initial access on us-mdr-vm1.
malware/administrator	Built-in domain administrator, creds suspected to have been dumped via mimikatz and impactet psexec/wmiexec, and other malicious activities.
malware/benji-a	Domain administrator, creds suspected to have been dumped via mimikatz and used psexec/wmiexec, and other malicious activities.
malware/solomon	New domain user that was created likely for the purpose of persistence.

2. Adversarial Tactics

Initial Access

The intrusion began with a phishing campaign leveraging email-delivered malicious links. At 2026-03-17 19:06:15, the user ph_mdr@trendmicro-update.org received an email labeled **V1 Project AI** that directed them to download an executable payload **v1AI.exe**. Shortly after, additional emails were sent between 19:17:32 and 19:19:01 containing an updated archive version of the payload. This sequence aligns with ATT&CK technique T1566.002 (Spearphishing Link) highlighting the adversary's reliance on social engineering and user interaction to deploy the initial payload.

3. Incident Diagram



Page 5 of 19

TrendAI Vision One™ Services – Managed Detection and Response (MDR) – Incident Report

Page 8 of 19

TrendAI Vision One™ Services – Managed Detection and Response (MDR) – Incident Report

Page 6 of 19

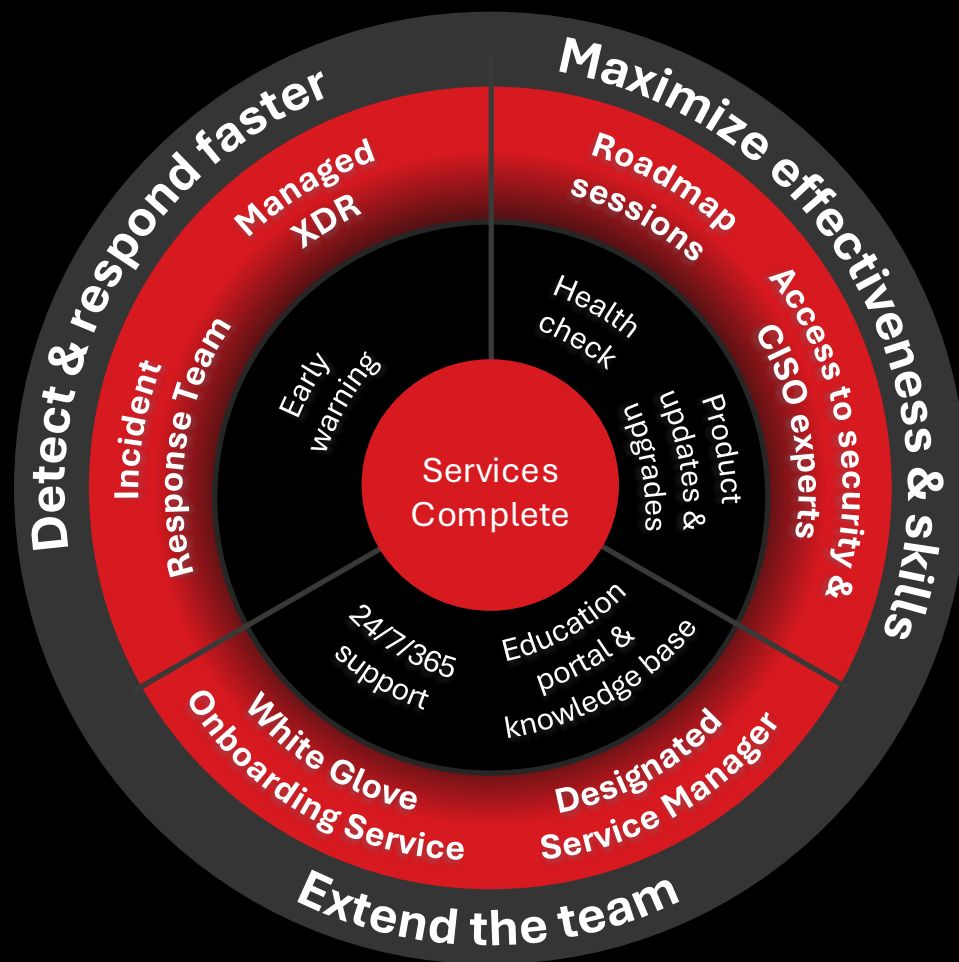
TrendAI Vision One™ Services – Managed Detection and Response (MDR) – Incident Report

Page 3 of 19

TrendAI Vision One™ Services – Managed Detection and Response (MDR) – Incident Report

TrendAI Vision One™ Services – Complete

MANAGED DETECTION and RESPONSE (MDR)
Onboarding
Proactive IoA hunting
24/7 alert monitoring
Critical events: Notify & investigate
Agreed response activities
Monthly reporting
Quarterly service review
Priority access to incident response
Prioritized case-handling
3 rd party data coverage**
Support to co-exist with non-Trend endpoint protection***



INCIDENT RESPONSE
Initial triage call / Qualification
First action & Initial set-up
Incident response plan execution

PREMIUM SUPPORT PLAN
Designated technical acct manager*
Onboarding
Installation / Update planning
Regular health check-ins
Security roadmap planning
Education recommendations
Quarterly business review
Prioritized case-handling

*Designated Customer Service Manager

**3rd party data supported by TrendAI Vision One™

Why TrendAI™ MDR

 **24/7 expert monitoring:** Continuous monitoring, investigation and response by experienced security analysts.

 **Broad visibility:** Native telemetry across endpoint, email, identity, cloud, network, and more through Vision One

 **Threat intelligence that feeds into detection:** TrendAI™ Zero Day Initiative (ZDI) provides early intelligence on emerging vulnerabilities, helping inform what our MDR team looks for and investigates.

 **Security expertise without permanent headcount:** Extend your team with experienced security analysts without building and staffing a dedicated security operation.

 **Global coverage:** In-house SOC operations across the Americas, Europe and APAC provide continuous coverage around the clock.

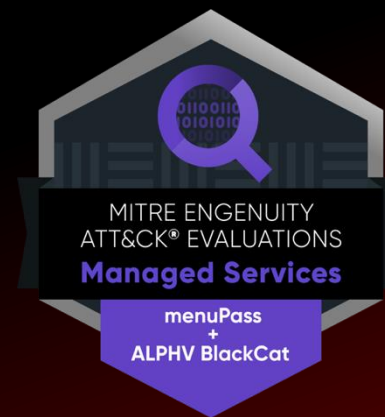
Proven threat protection

100% detection coverage
MITRE Engenuity™ ATT&CK® Evaluations

Pre-disclosure protection
up to 115 days before patch, powered by TrendAI™ Zero Day Initiative™ (ZDI)

Proven at scale
Thousands of customers protected worldwide by TrendAI Vision One™ Services –
Managed Detection and Response (MDR)

Broad visibility
Native and third-party telemetry across the attack surface



Security
expertise
backed
by industry
certifications and
company
compliance

SANS | GIAC
CERTIFICATIONS



Average **7 years** of TrendAI™ experience,
5 years in a SOC environment, and at least
4 security certifications from SANS | GIAC

Expert-led MDR, 24×7×365

- Continuous quality assessment programs improve investigation accuracy and consistency.
- Human-led decision-making across the full detection-to-response lifecycle.



Recognized by IDC

“TrendAI™ is positioned in the Major Players category in the 2025 IDC MarketScape: Worldwide Managed Detection and Response Service for MidMarket 2026 Vendor Assessment”

“The Zero Day Initiative provides TrendAI MDR with pre-disclosure vulnerability intelligence that informs detection engineering and attack path modeling before public CVE assignment, offering a protective advantage window against exploitable vulnerabilities that is structurally unavailable to providers without an equivalent vulnerability research program.”



Breadth of TrendAI Vision One™ Services

Address skills shortage and augment security operations with 24/7 threat monitoring

**MANAGED DETECTION
AND RESPONSE (MDR)**

Build resilient strategies and test real-world defenses

RED / PURPLE TEAMING

Contain, eradicate, and recover from a major incident

INCIDENT RESPONSE

Deploy, configure, and optimize Trend solutions for maximum effectiveness with dedicated resources

PREMIUM SUPPORT



AI Fearlessly

