Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Streaming Edition 2021

ASTREA Advanced Security, Training Research, Events Agency

Percorso Gestione Sicurezza

Da soluzione o prodotto a piattaforma + servizi, come cambia la pelle della cybersecurity per vedere di più e vedere prima

Tiberio Molino, Senior Sales Engineer, Trendmicro

16 marzo 2021 / 16.40-17.40 - StreamingEdition

#securitysummit #streamingedition

Tiberio Molino

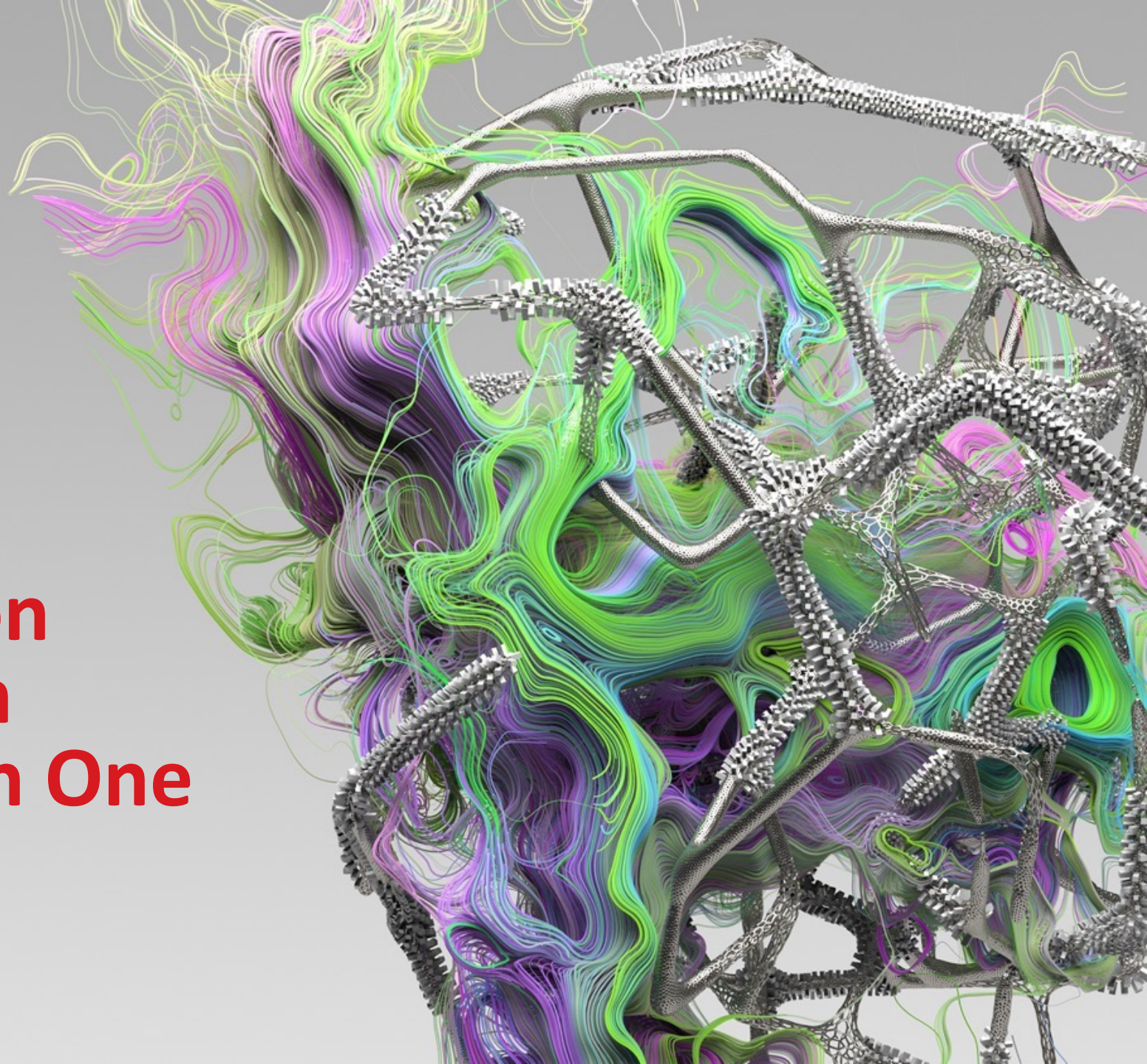
SENIOR SALES ENGINEER

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT
Streaming Edition
16-17-18 marzo 2021

TREND MICRO™

TREND MICRO™

Extended detection and response with Trend Micro Vision One



…and little visibility into email traffic and mailboxes

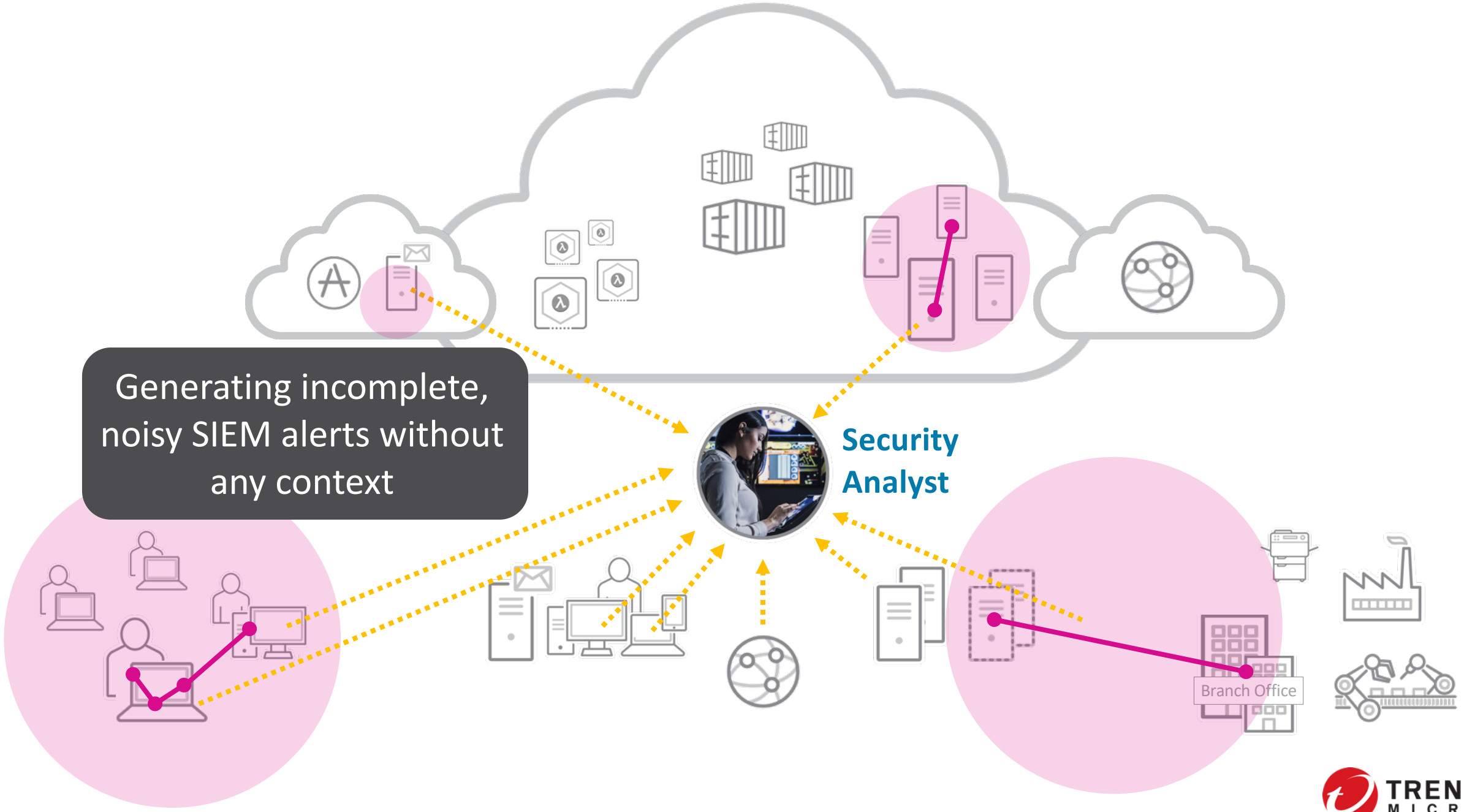
…limited visibility to threats affecting cloud workloads

Today, the SOC gets siloed insight into endpoints (EDR)…

Security Analyst

…a separate siloed view into network events,

Branch Office

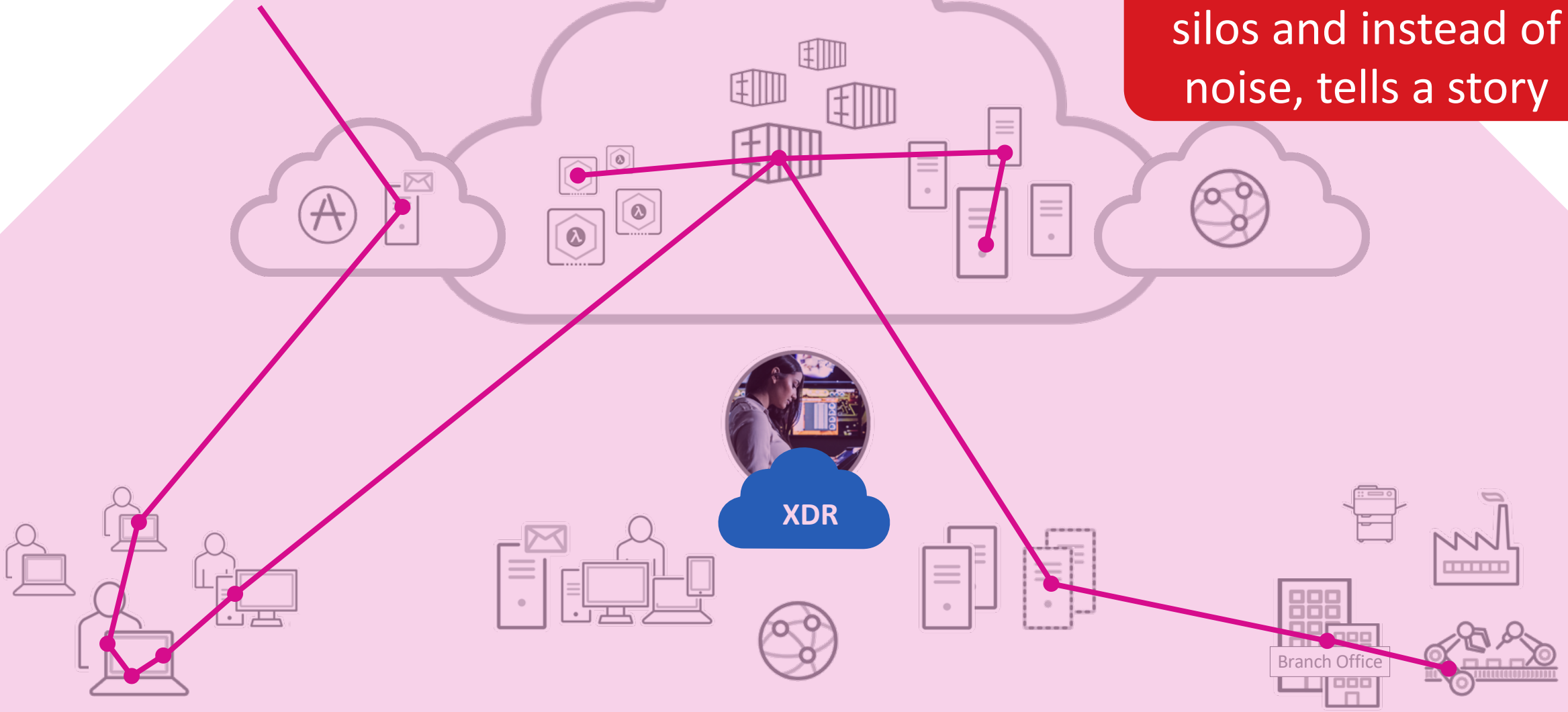

Generating incomplete, noisy SIEM alerts without any context
Security Analyst
Branch Office

Attacks don’t stay in silos! Security teams need to piece together what happened

Security Analyst

Branch Office

XDR breaks down the silos and instead of noise, tells a story



Organizations with XDR…

Are better protected

Suffered **half as many successful attacks** over the last 12 months

Detect quicker

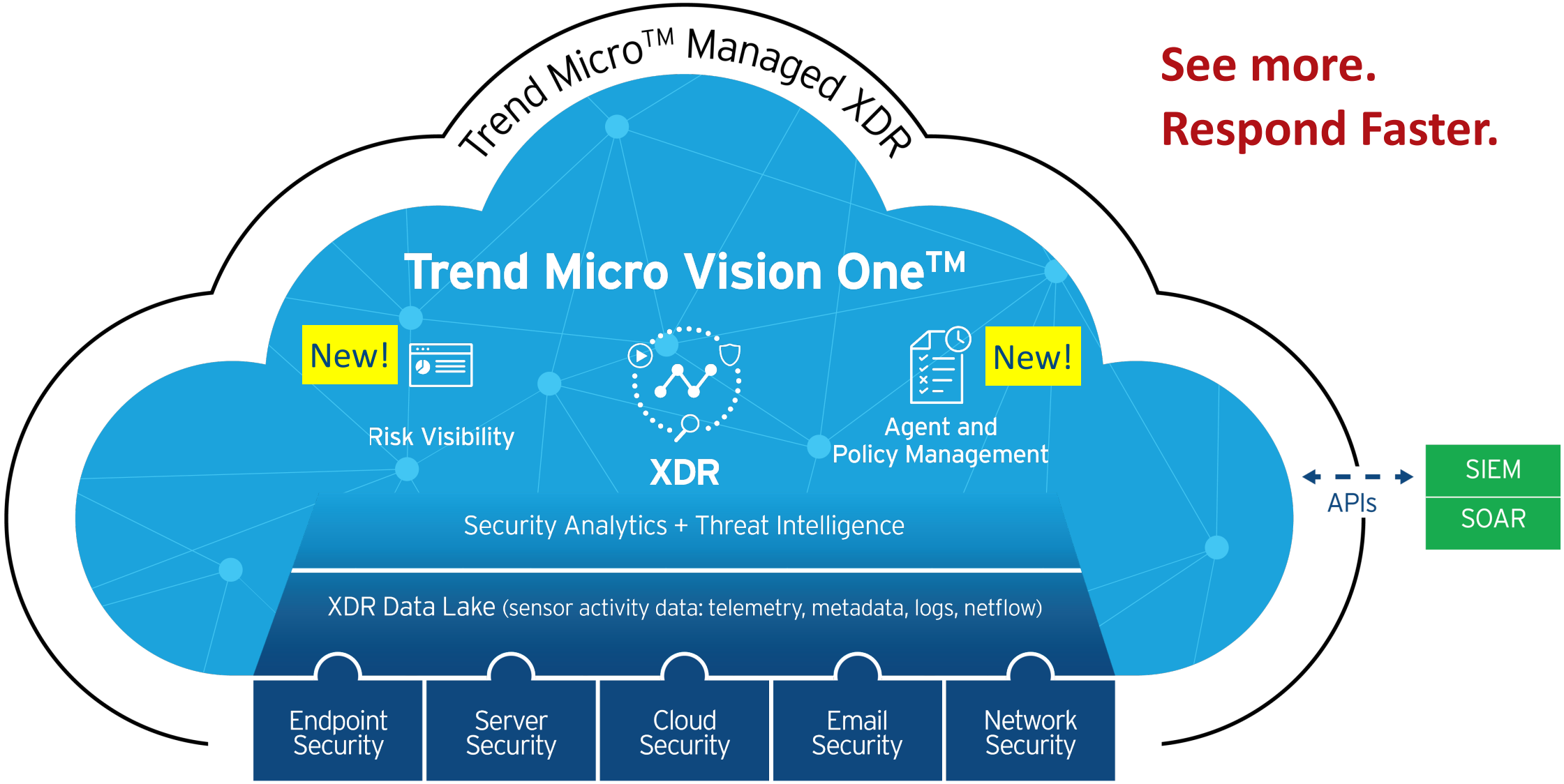
2.2X more likely to detect a data breach /successful attack in a **few days or less**

Respond completely

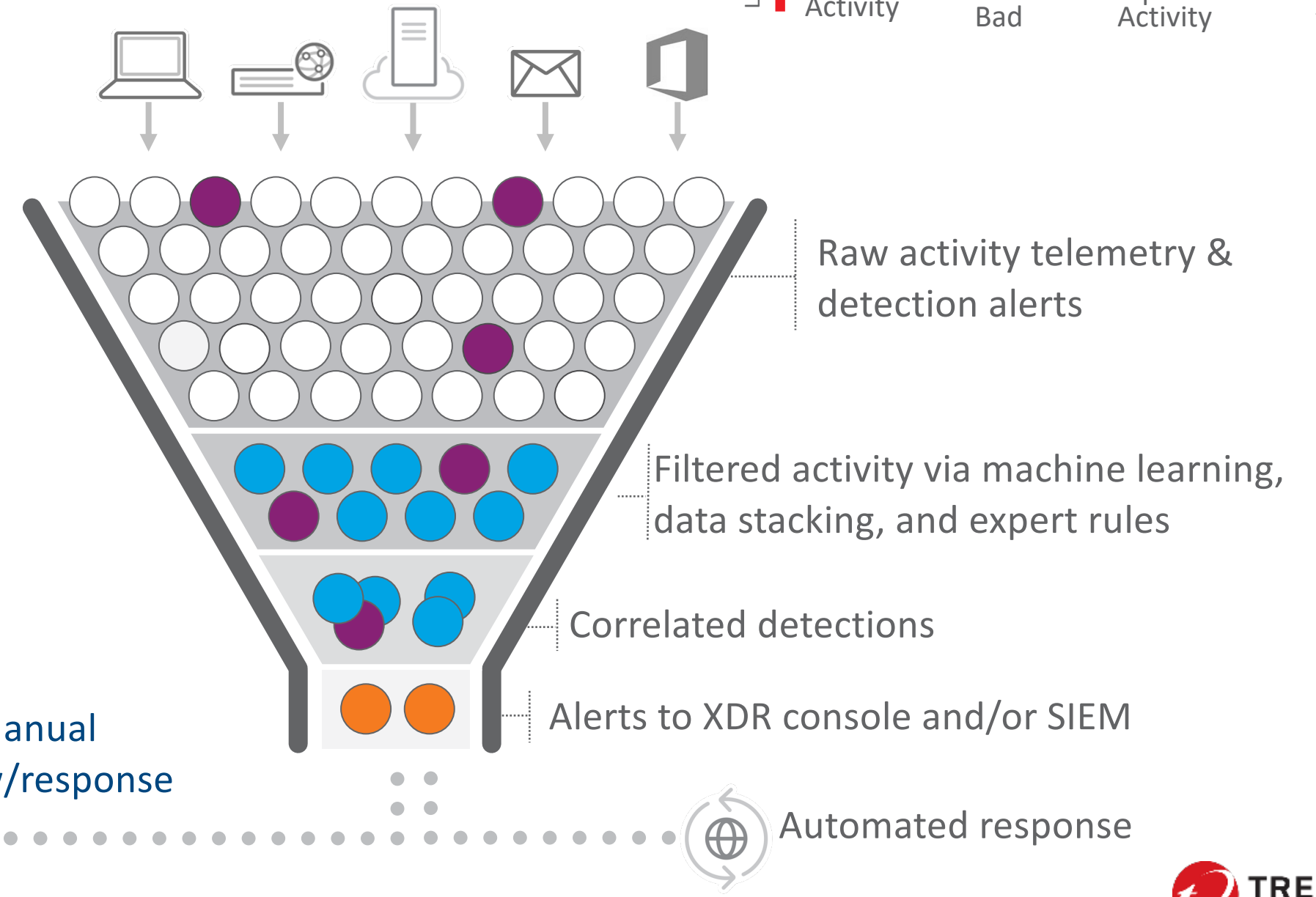
60% less likely to report that **attack re-propagation** has been an issue.

Source: The XDR Payoff: Better Security Posture, ESG Research, Sep 2020

See more.
Respond Faster.



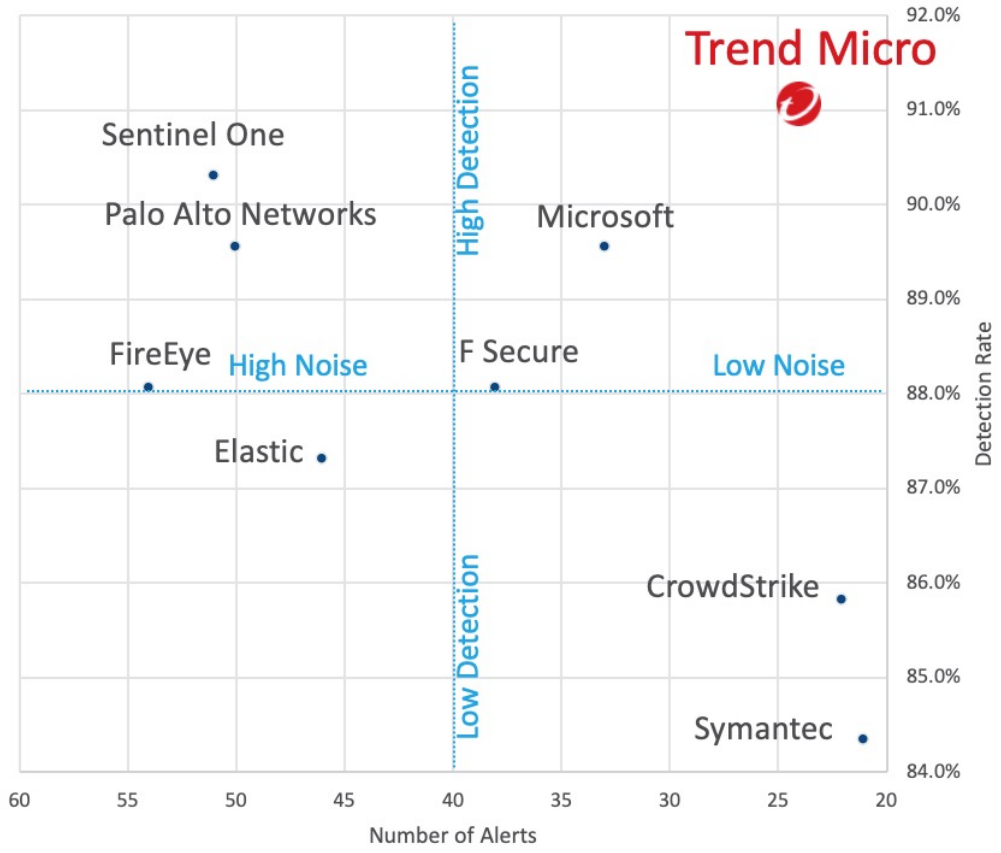
Extended Detection & Response (XDR)



MITRE | ATT&CK®

APT29

Tradecraft and operational flows followed by the group APT29.



Customers want:

High detection without alert fatigue

- ✓ Highest Initial Detection
- ✓ Low Noise

*Evaluation conducted Dec 2019 before new XDR platform. With XDR, tracking and correlating attacker behaviors gets even better…..

TREND MICRO™

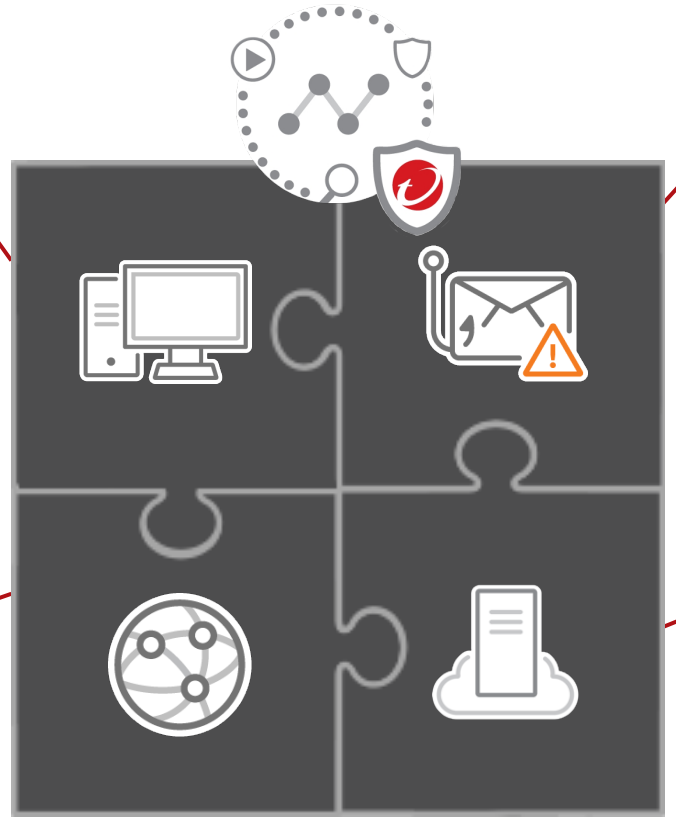
Each Layer Adds Value

Endpoint – most attacks involve users devices

- Find threats hidden amongst endpoint telemetry
- What happened within the endpoint? How did it propagate?

Network - sees EDR blind spots (unmanaged; legacy, IoT, IIoT)

- How is the attacker moving across the organization?
- How is a threat communicating?

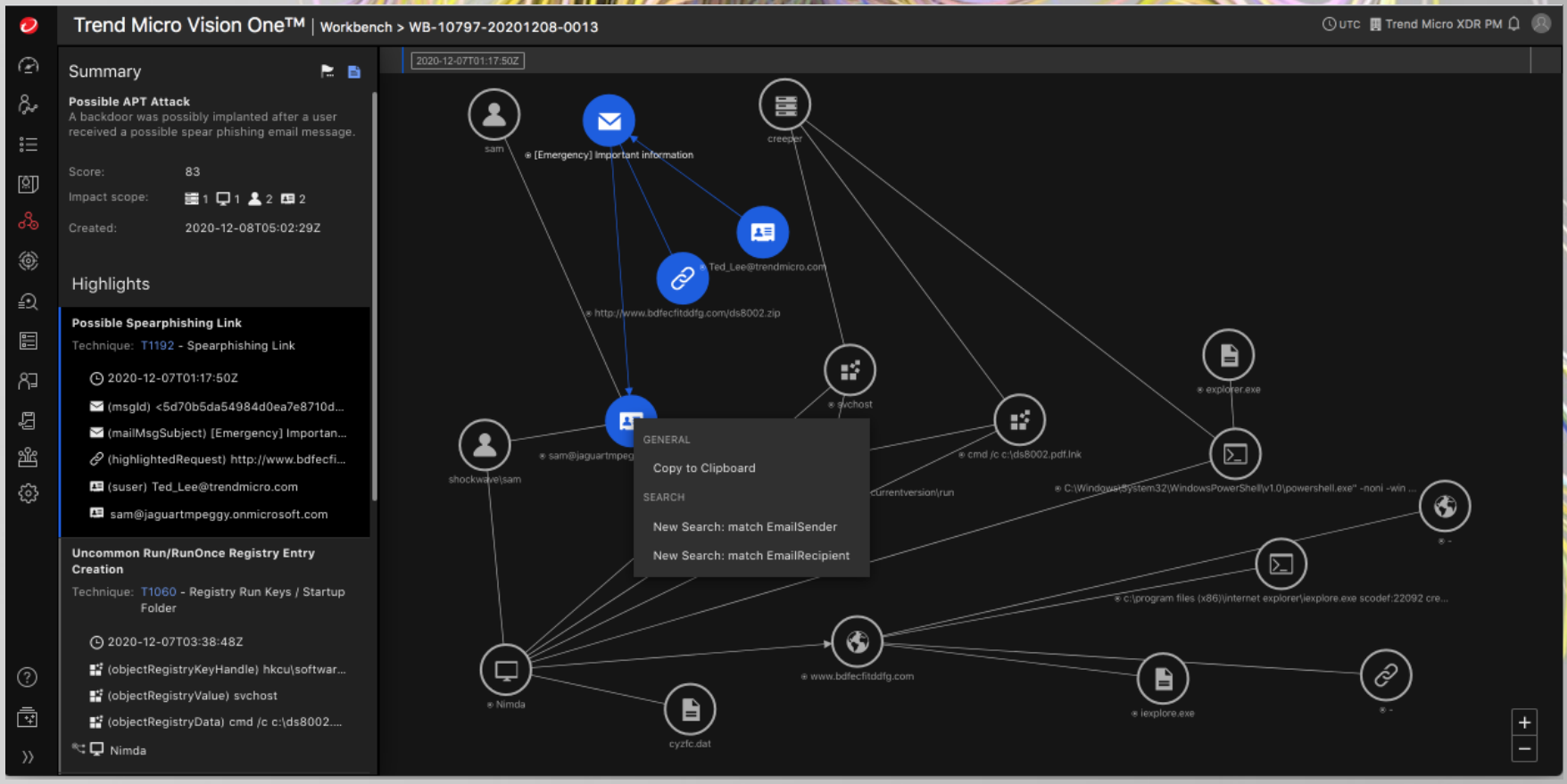


Email - 94% of malware

- Who else received this email or a similar threat?
- API integration for inside view
- Are there compromised accounts sending internal phishing emails?

Cloud/Workloads/Containers - critical to business operations

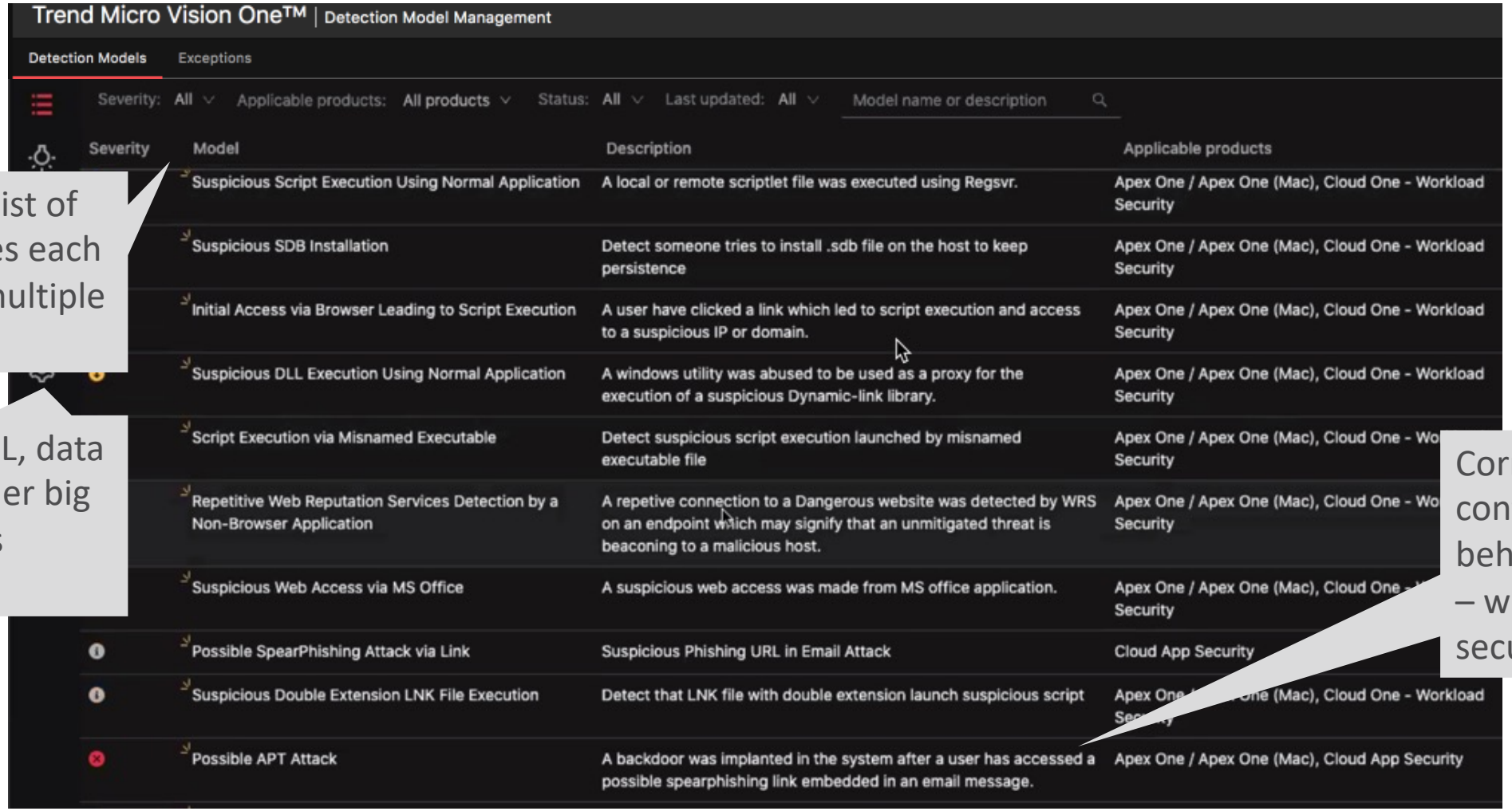
- Correlates data from more security controls than typical EDR to solutions tell a more complete story.
- What happened within the workload?



Let’s see it!

Discover More with Correlated Detection

Security Analytics Engine finds Zero-day and Targeted Attacks



Models consist of multiple rules each containing multiple filters

Combines ML, data stacking, other big data analysis techniques

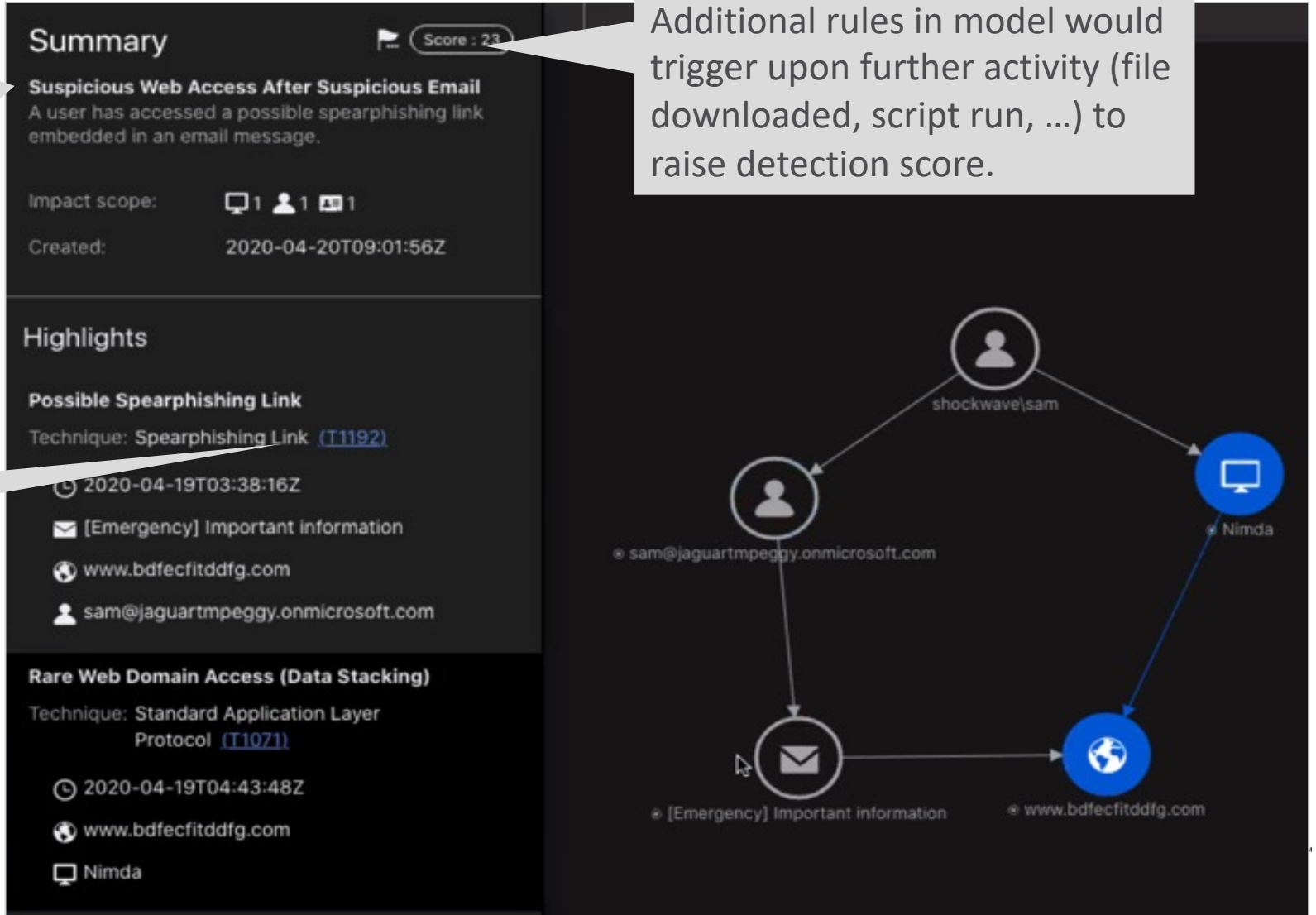
Correlates low confidence events, behaviors, actions – within or across security layers

Discover More with Correlated Detection

Security Analytics Engine finds Zero-day and Targeted Attacks

Correlated Detection Example:
Combines low confidence activities:
1) suspected phishing email
+
2) rare web domain accessed on an endpoint

Mapped to MITRE techniques

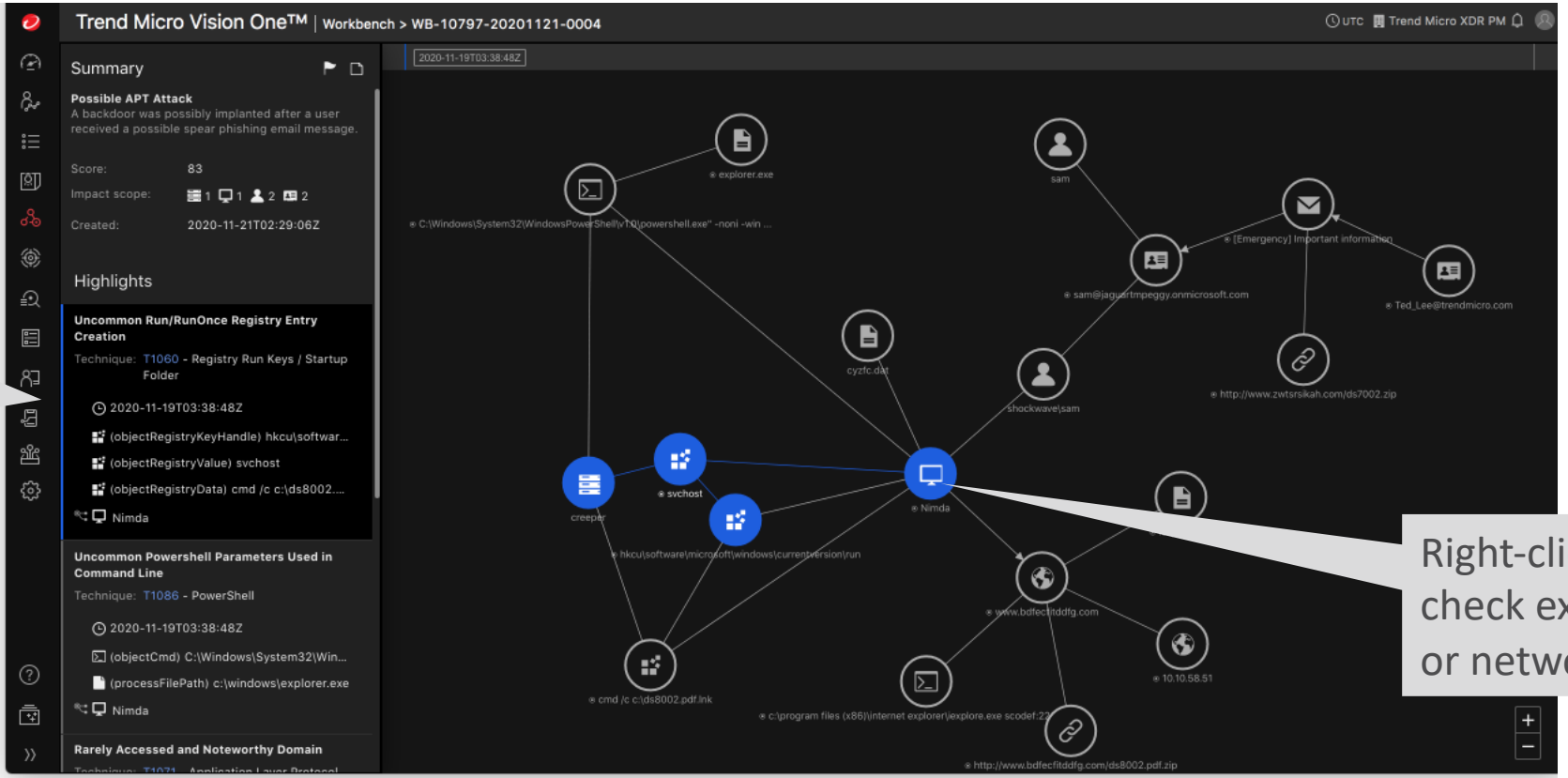


Additional rules in model would trigger upon further activity (file downloaded, script run, …) to raise detection score.

Integrated Investigation and Response

Quickly visualize the story of an attack

Details of selected object



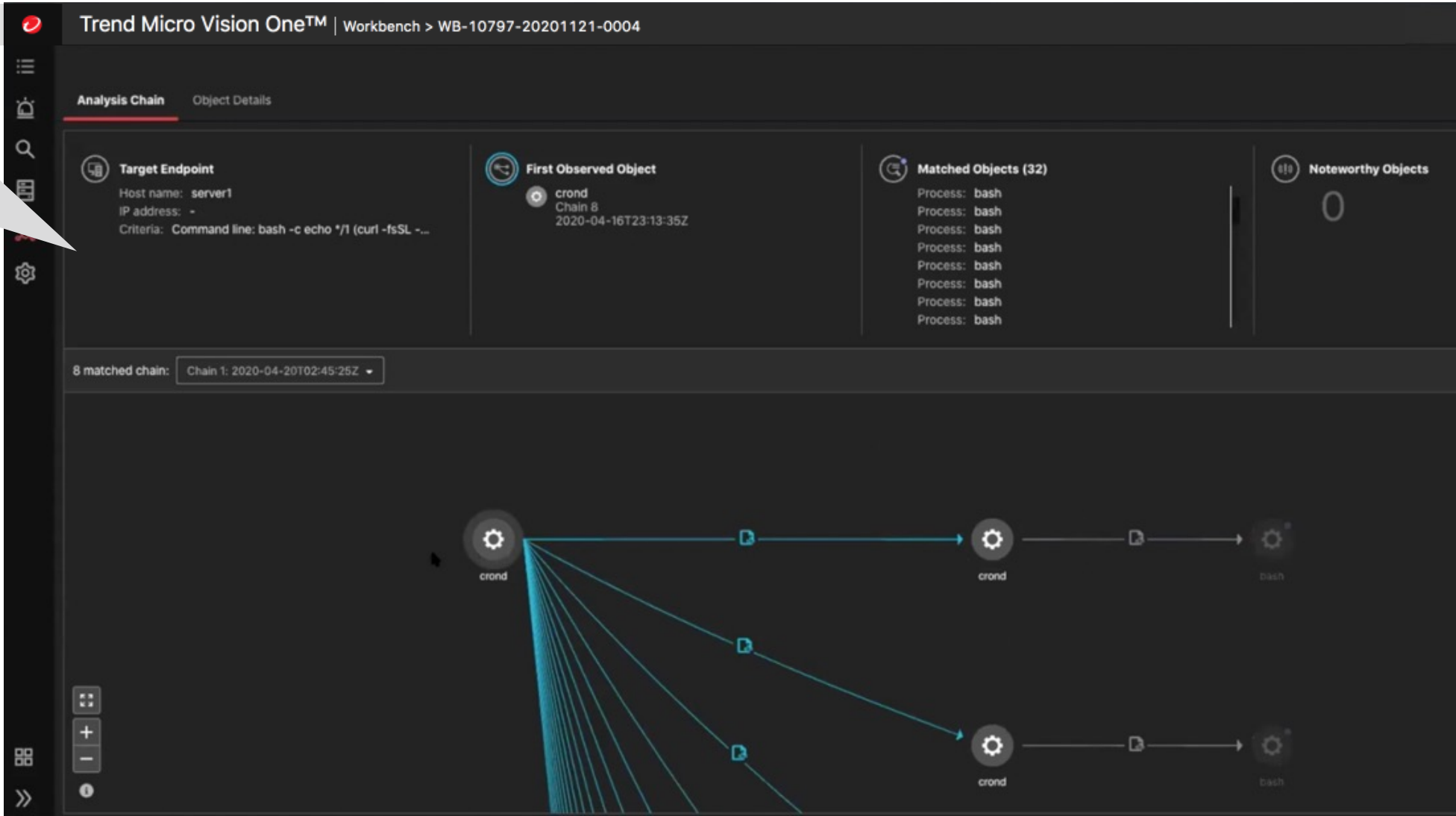
Right-click on objects to check execution profile or network analysis

Integrated Investigation and Response

Quickly visualize the story of an attack

See execution profile of endpoints and cloud / server workloads. Supports 90+ OS versions.

Windows
Mac
Red Hat
debian
CloudLinux
SUSE
ubuntu
CentOS
Oracle Linux
Amazon Linux



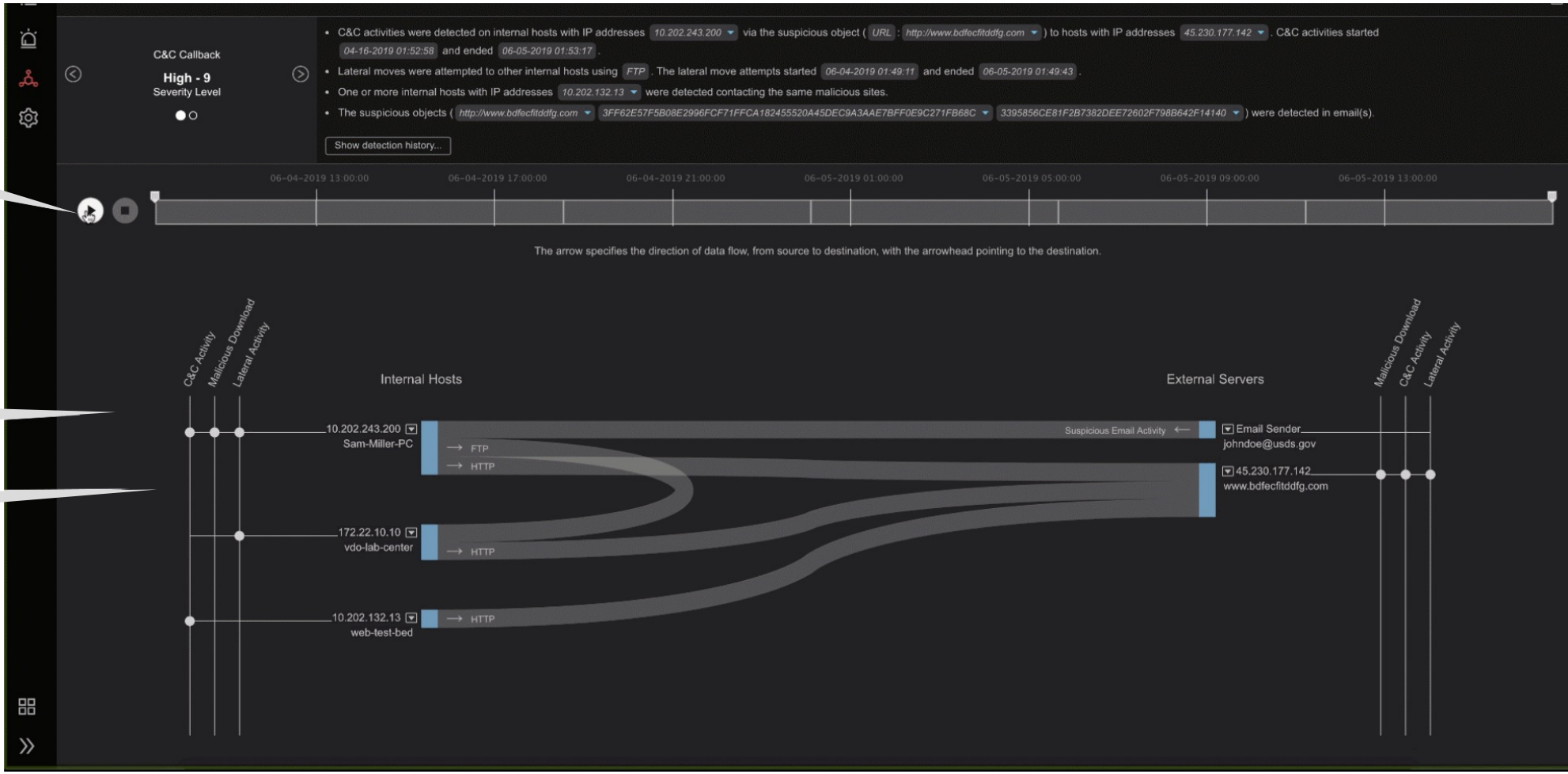
Integrated Investigation and Response

Quickly visualize the story of an attack

Graphically replay communication activity

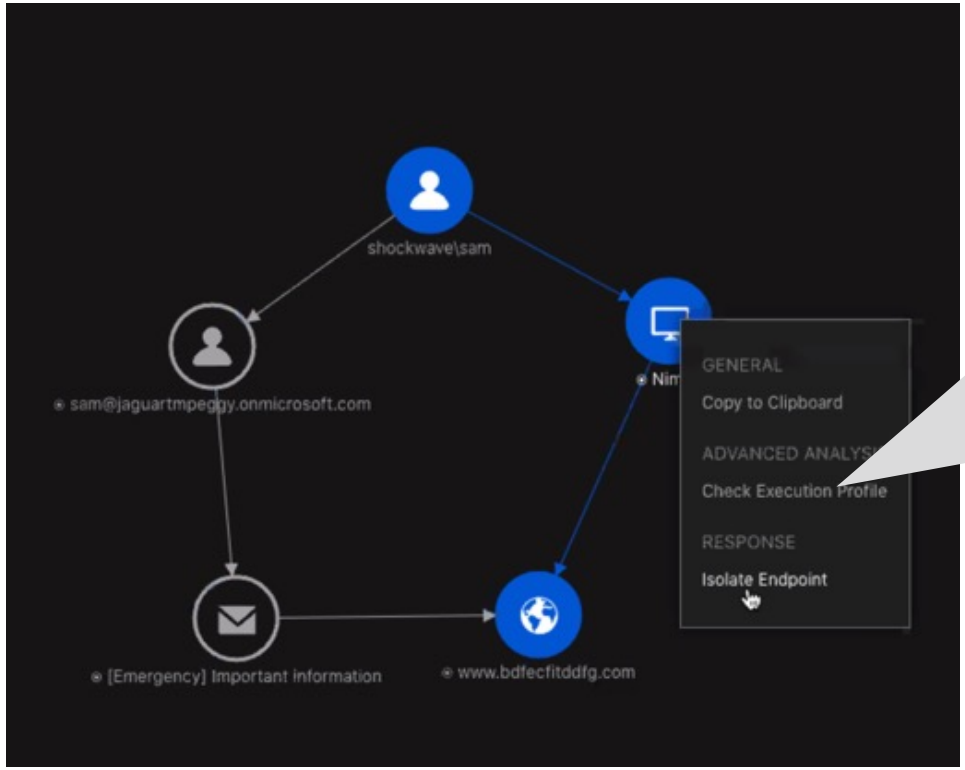
1st target and C&C

Lateral movement



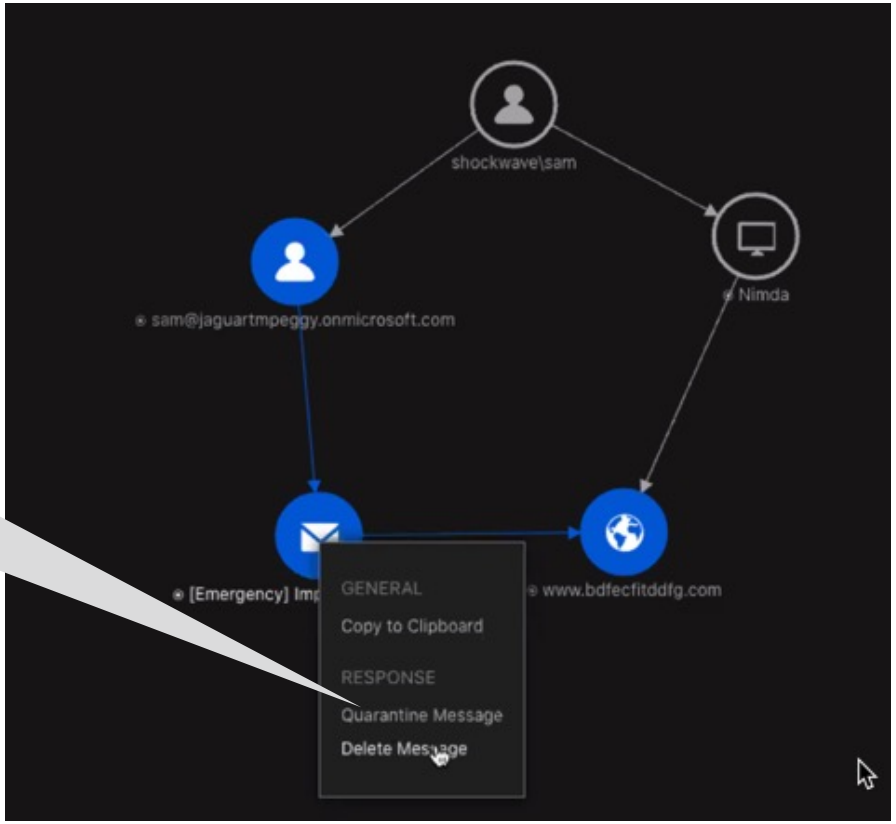
Respond Faster and More Completely

From one place: Endpoint, email, workload, and network response actions



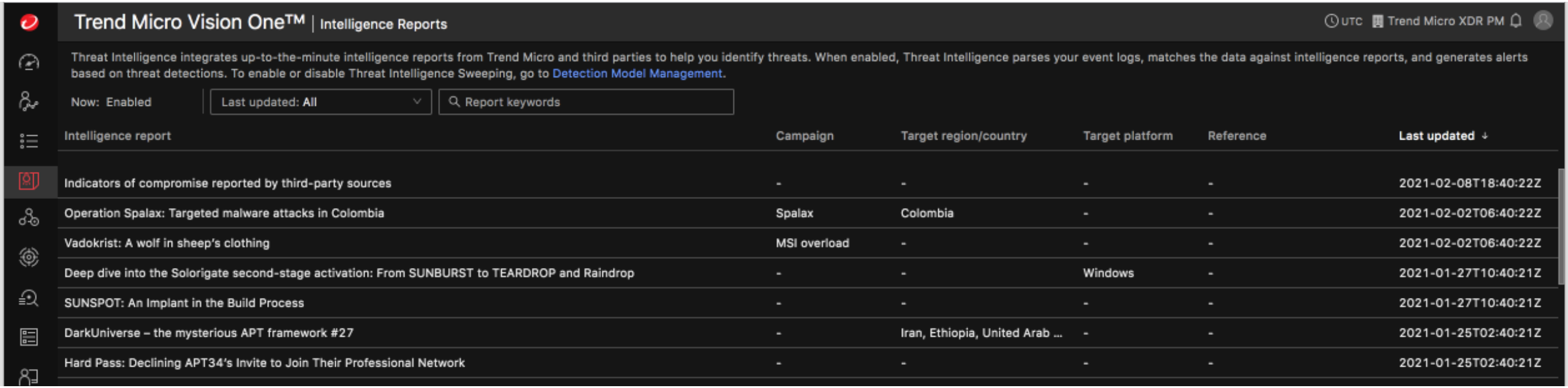
Contextual aware choices for quick response. Actions are carried in multiple security controls.

- Collect file
- Isolate endpoint
- Block filehash, domain, IP, URL
- Terminate process
- Quarantine/delete email
- Remote Shell



Built-in Threat Intelligence

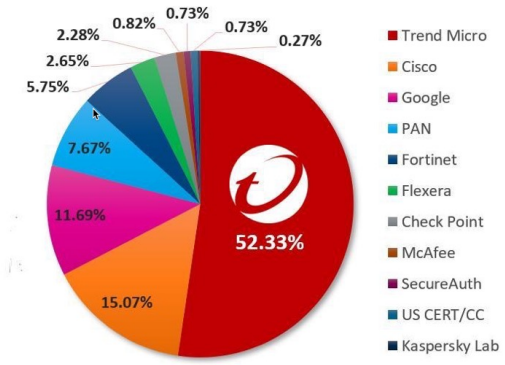
Automatically detect IOCs across your entire environment



TREND MICRO | research

15 threat research centers worldwide

250M sensors globally

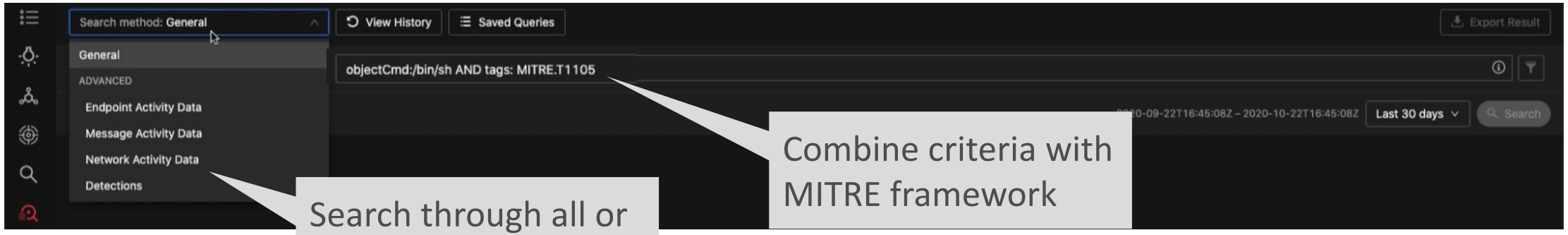


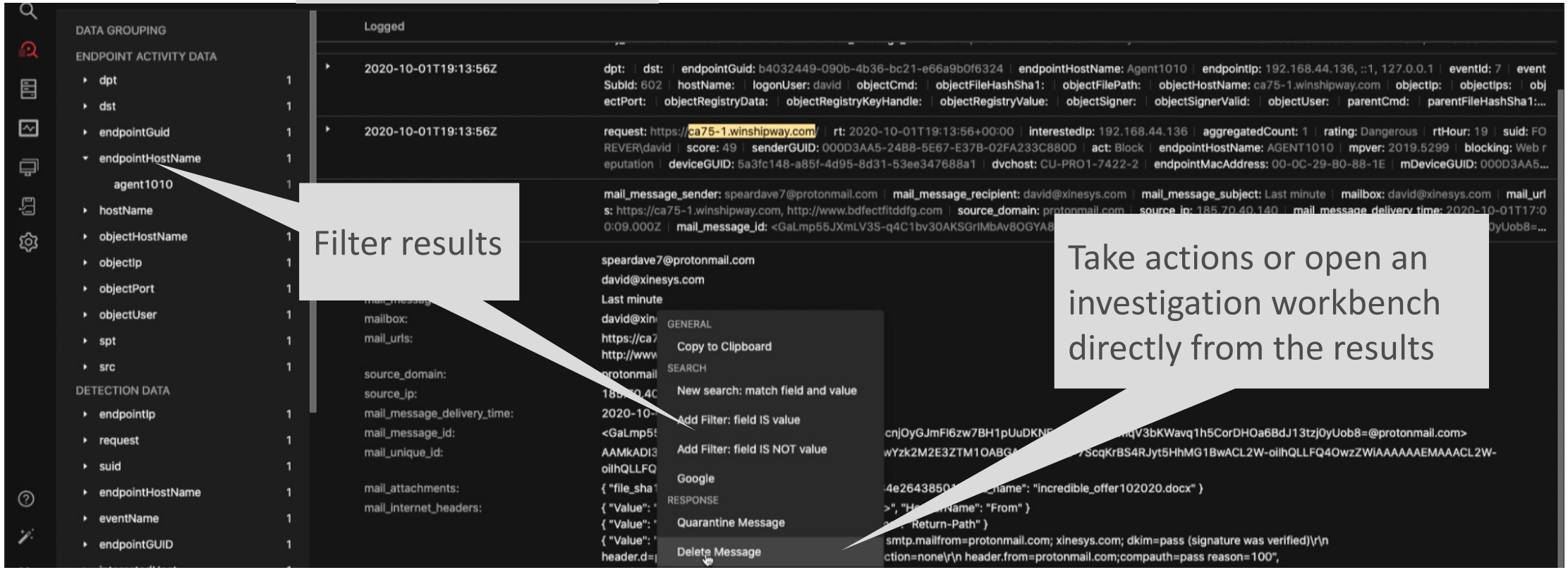
Trend Micro discovered **over half** the disclosed **vulnerabilities** in 2019

Processes Trillions of Queries to the Smart Protection Network yearly

TREND MICRO

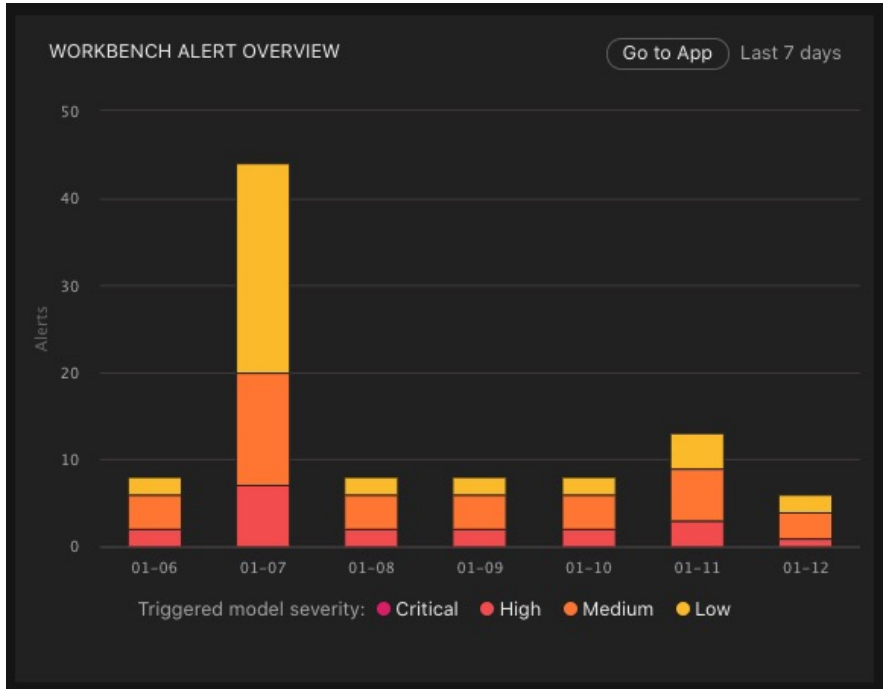
Search the XDR Data Lake





Risk Visibility

See trending of workbench alerts over time and top endpoints with observed techniques



TOP ENDPOINTS WITH OBSERVED ATTACK TECHNIQUES — Go to App — Last 7 days

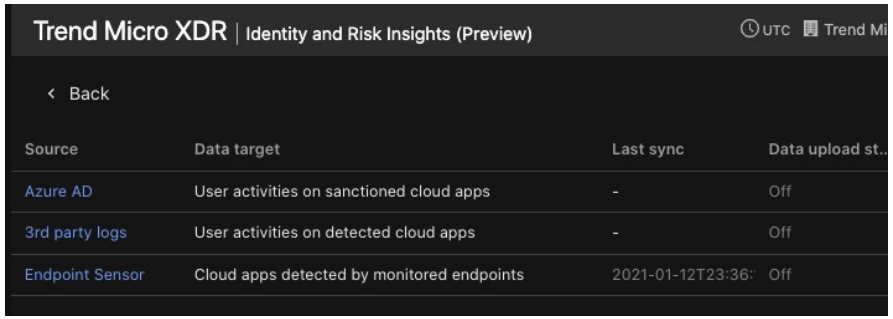
Endpoint	Critical	High	Medium	Total ↓
US-ERICSH-MAC(10.1.0.164)	-	-	113	113
ip-0A00526E(10.0.82.110)	20	15	72	107
ip-0A004E93(10.0.78.147)	3	7	41	51
ip-0A005116(10.0.81.22)	25	1	12	38
ArgosServer(192.168.1.161)	-	-	35	35
ip-10-0-6-36.ec2.internal(10.0.6....	-	7	28	35
ip-0A0050C8(10.0.80.200)	-	3	28	31
ip-0A004343(10.0.67.67)	3	4	21	28
ip-0A004A40(10.0.74.64)	1	4	19	24
ip-10-0-22-34.ec2.internal(10.0....	-	4	16	20
ip-0A005E15(10.0.95.21)	-	4	15	19

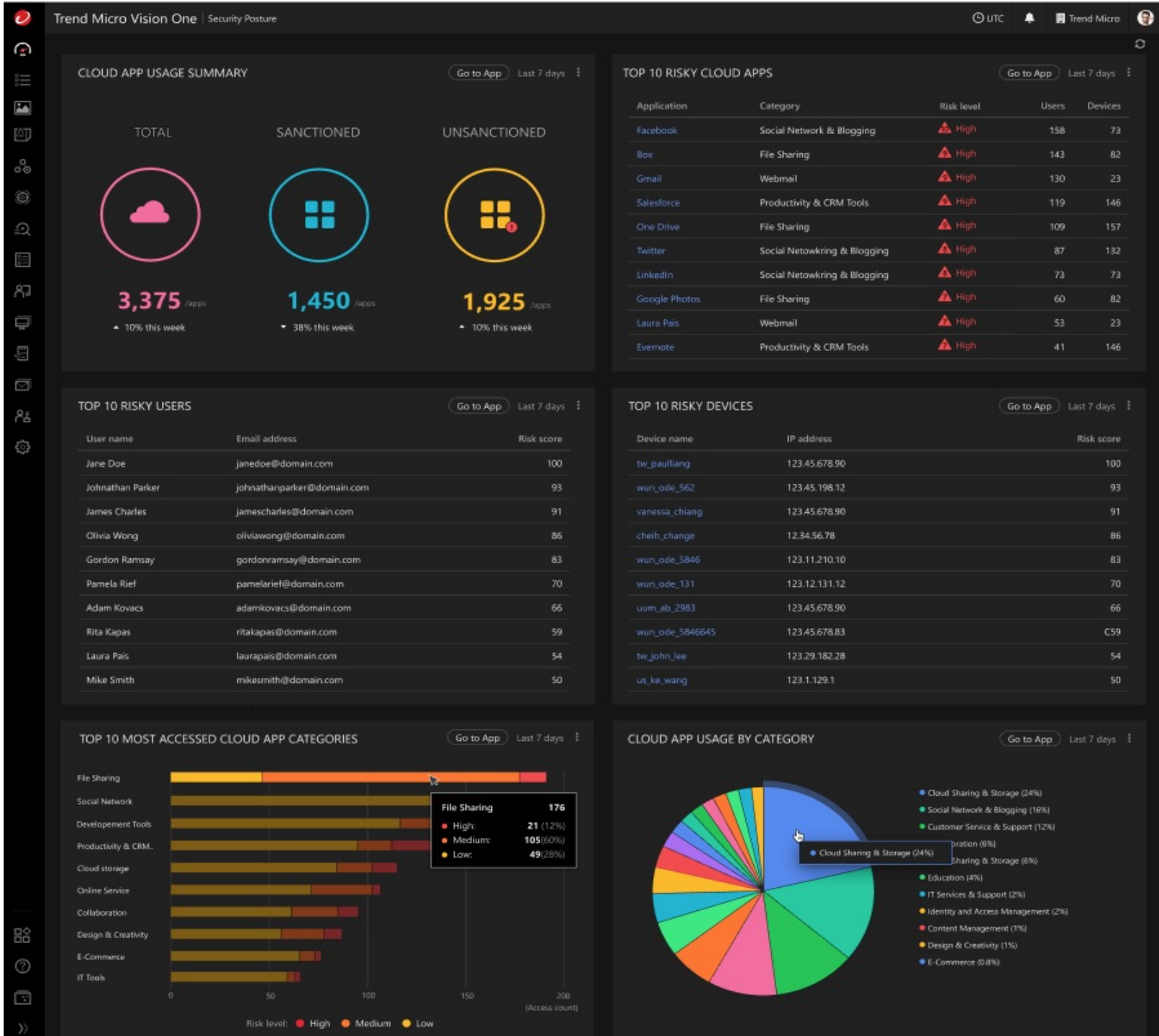
Risk Visibility

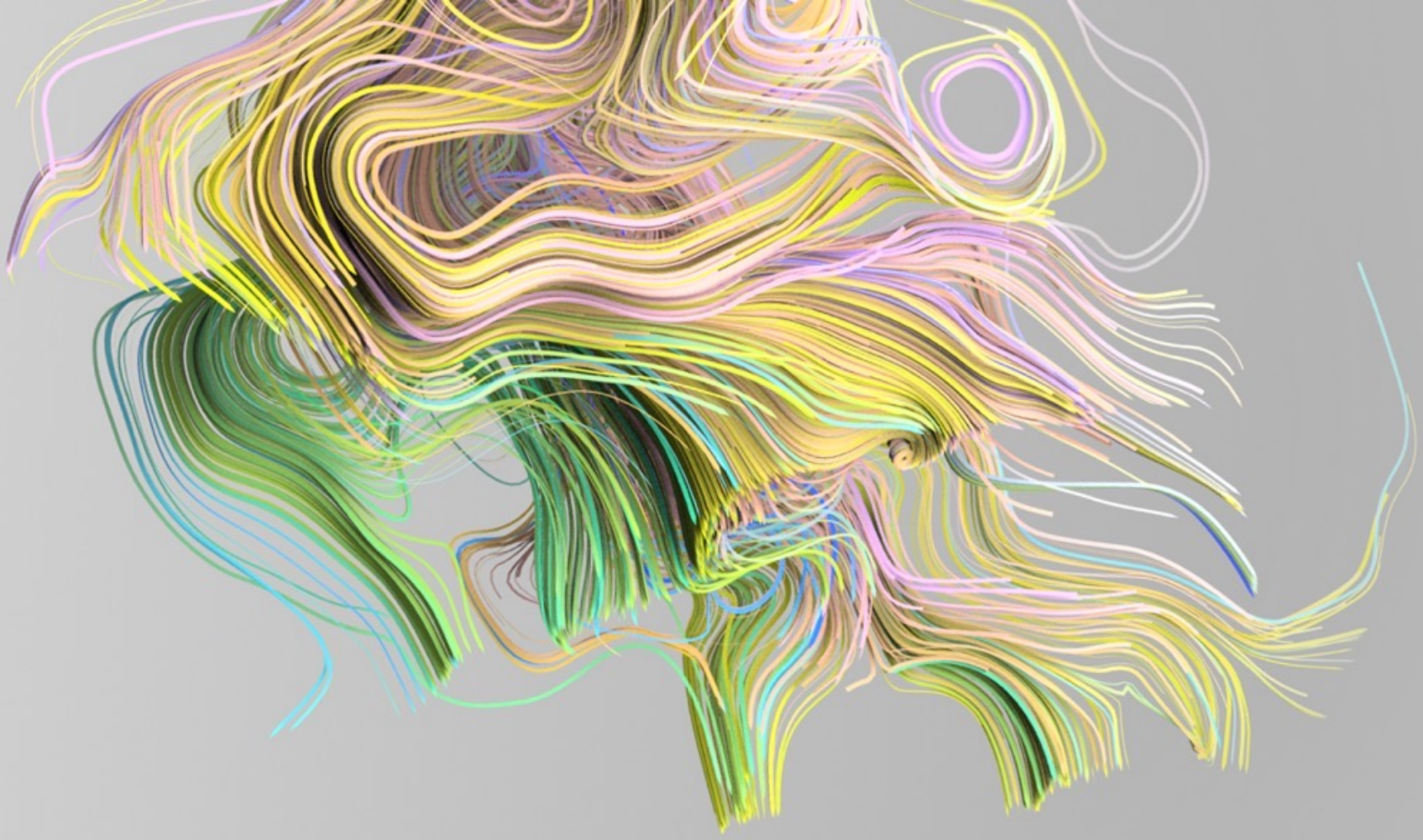
Cloud App App Usage (preview)

Provides insight into cloud applications used in your environment and their risk level.

Uses data from existing sensors, Azure AD, or 3rd party firewall logs







Managed XDR
MDR service

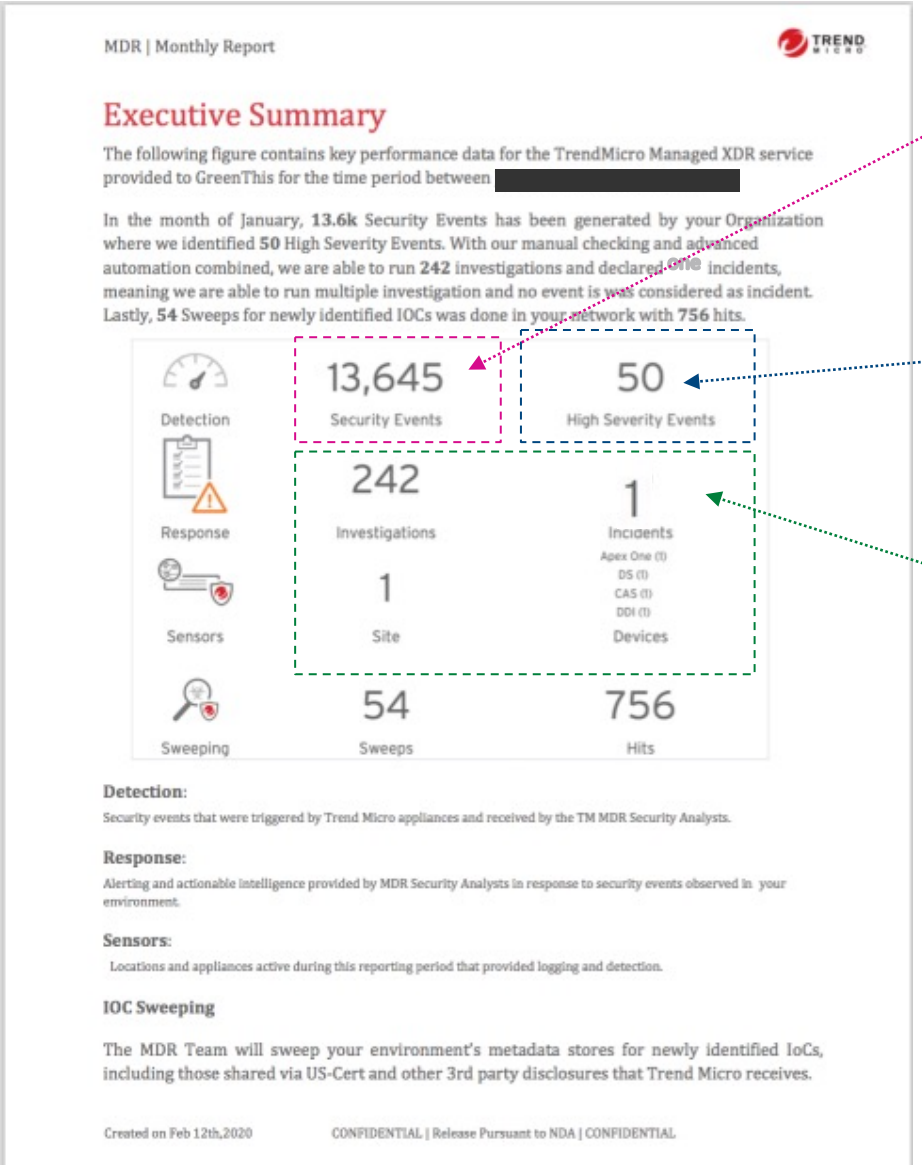
Managed XDR: MDR Service by Trend Experts

Expert Threat Hunting
Cutting-edge techniques with verification and enrichment by threat experts

24x7 Monitoring & Detection
Continuous monitoring and routine sweeping of endpoint, server, network, and email

Rapid Investigation and Mitigation
Detailed response plan and remote actions through Trend Micro products

What it Means for the Customer



MDR | Monthly Report

Executive Summary

The following figure contains key performance data for the TrendMicro Managed XDR service provided to GreenThis for the time period between [redacted]

In the month of January, **13.6k** Security Events has been generated by your Organization where we identified **50** High Severity Events. With our manual checking and advanced automation combined, we are able to run **242** investigations and declared one incidents, meaning we are able to run multiple investigation and no event is was considered as incident. Lastly, **54** Sweeps for newly identified IOCs was done in your network with **756** hits.

Detection	13,645 Security Events	50 High Severity Events	
Response	242 Investigations	1 Incidents	Apex One (1) DS (1) CAS (1) DDI (1)
Sensors	1 Site	Devices	
Sweeping	54 Sweeps	756 Hits	

Detection:
Security events that were triggered by Trend Micro appliances and received by the TM MDR Security Analysts.

Response:
Alerting and actionable intelligence provided by MDR Security Analysts in response to security events observed in your environment.

Sensors:
Locations and appliances active during this reporting period that provided logging and detection.

IOC Sweeping

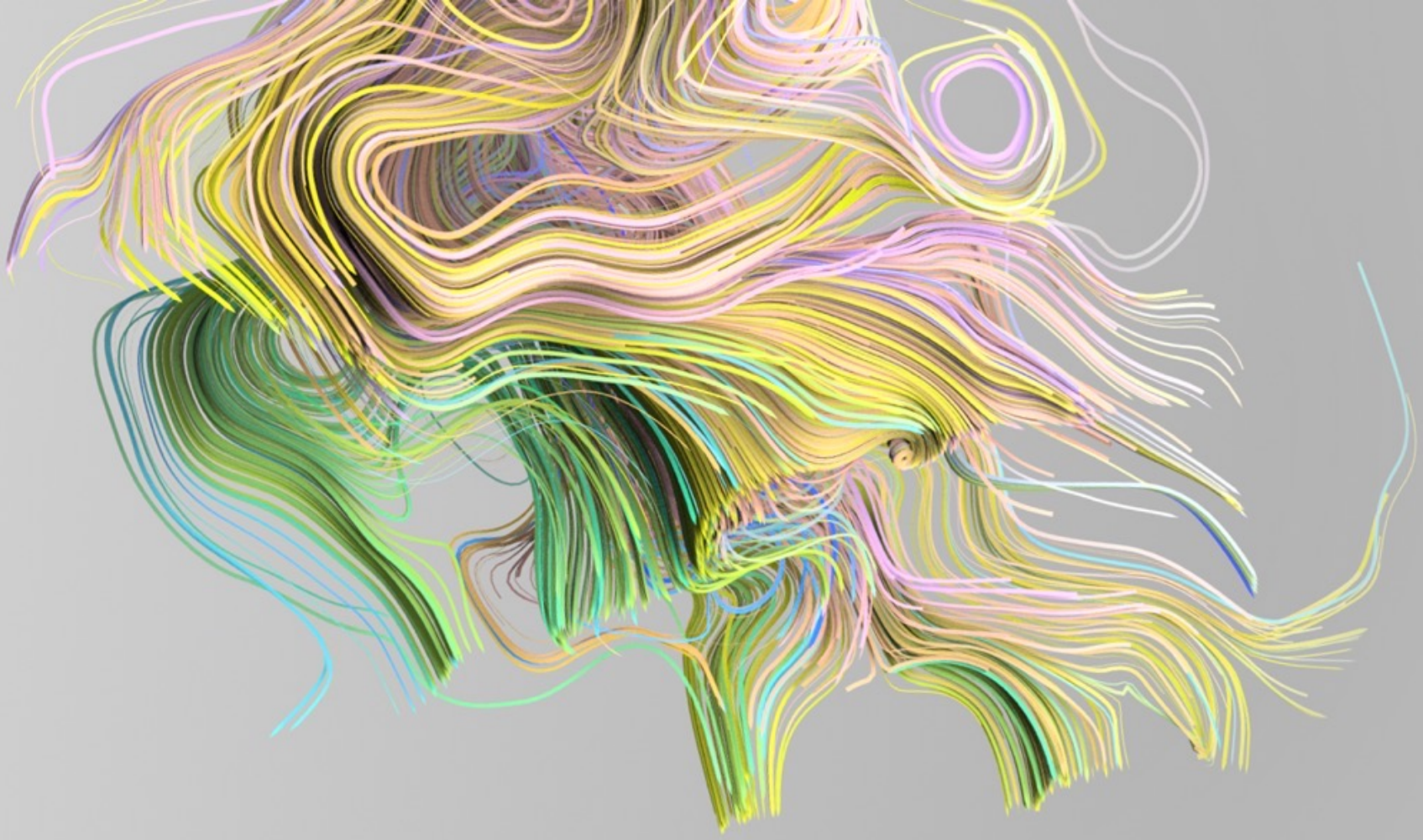
The MDR Team will sweep your environment's metadata stores for newly identified IoCs, including those shared via US-Cert and other 3rd party disclosures that Trend Micro receives.

Created on Feb 12th,2020 CONFIDENTIAL | Release Pursuant to NDA | CONFIDENTIAL

Events generated by Trend Micro products (which are not actionable but needed for compliance / visibility when investigating)

Standard managed service: distills and prioritizes 50 high severity events which require further investigation by the customer's Level II/III security analyst

Advanced managed service: Trend Micro security experts investigate each of the 50 events. Through manual and automated means, they were able to run 242 investigations and declared one incident. For that security incident, the service provides threat response and a detailed remediation plan and incident report.



Why Trend Micro XDR?

Customers Experience with XDR

"It is easier for my team to explain the attack and go through the sequence of events; We aren't breaking things down in all the different tools; *It's like reading a book. Easier to digest."*
"ROI is huge."

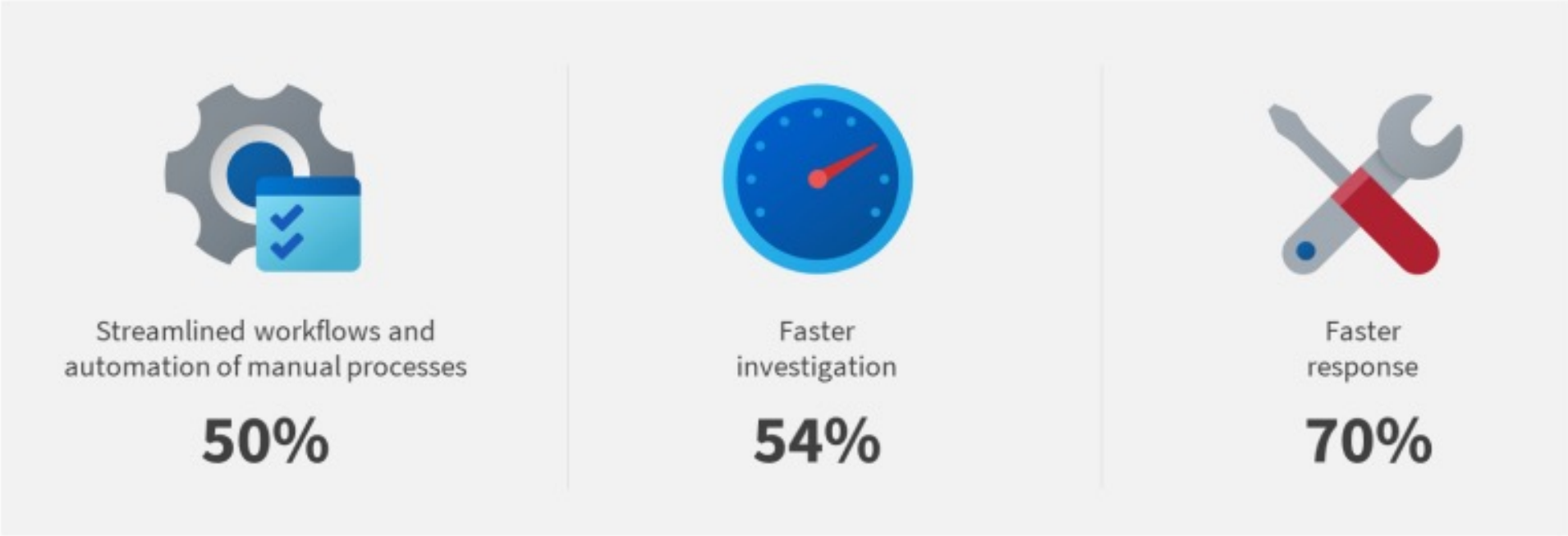
"The way XDR allows me to drill down is amazing. It literally paints a picture in front of you."

How is Trend Micro XDR different than other approaches?

	Trend Micro XDR	Vendor-to-Vendor partnership	SOAR / SIEM
Sharing of IOC's between layers for sweeping	**Yes**	**Yes**	**Yes**
Corelated detection of low confidence events across layers	**Yes**	*No*	*partial*
Deep understanding of all data generated by layers	**Yes**	*No*	*No*
Integrated investigations in one console	**Yes**	*No*	*partial*
Integrated response actions across layers	**Yes**	*No*	**Yes**

Correlation is critical, but not possible without XDR

Survey results: 8 Full Time Employees (FTE) to replace XDR data correlation capabilities



Source: The XDR Payoff: Better Security Posture, ESG Research, Sep 2020

A Leader in the Forrester™ Wave

"Trend Micro delivers XDR functionality that can be impactful today."

–The Forrester Wave™: Enterprise Detection and Response, Q1 2020

FORRESTER®
WAVE
LEADER 2020
Enterprise Detection
And Response

TREND MICRO™

A Leader in 4 Key XDR Building Blocks

Detection & Response

The Forrester Wave™: Enterprise Detection and Response, Q1 2020

Endpoint

The Forrester Wave™: Endpoint Security Suites, Q3 2019

Email

The Forrester Wave™: Enterprise Email Security, Q2 2019

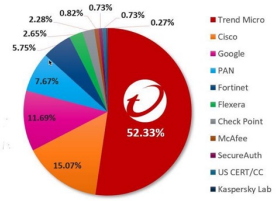
Cloud

The Forrester Wave™: Cloud Workload Security, Q4 2019

Why Trend Micro Vision One?

1 **Purpose-built** XDR platform with deep integration into native sensors

3 **Trend Micro Threat Research** powered threat analytics and automatic IoC sweeping



Trend Micro discovered **over half** the disclosed **vulnerabilities** in 2019

2 **Distinctive data sources**

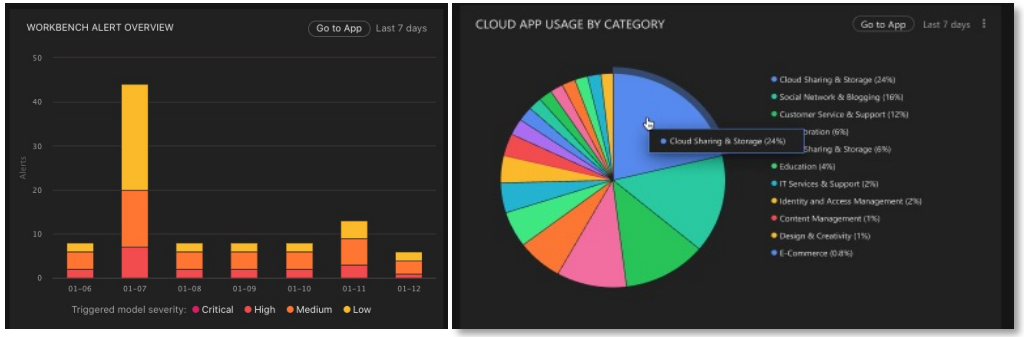
Cloud - breadth and timeliness of Linux support

debian CloudLinux SUSE Amazon

ubuntu CentOS Oracle Red Hat

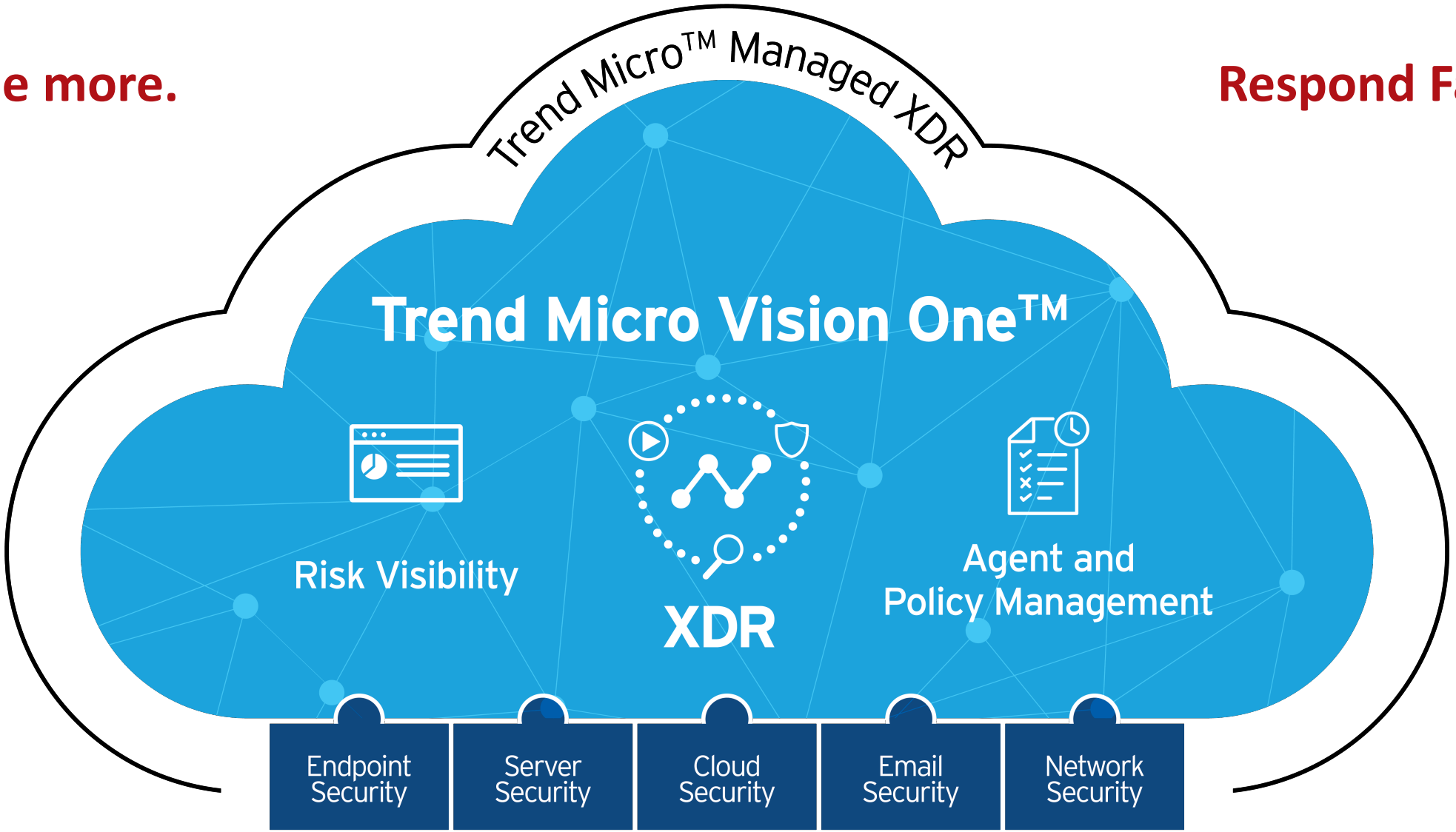
Email - visibility + response by integrating at the *application layer*

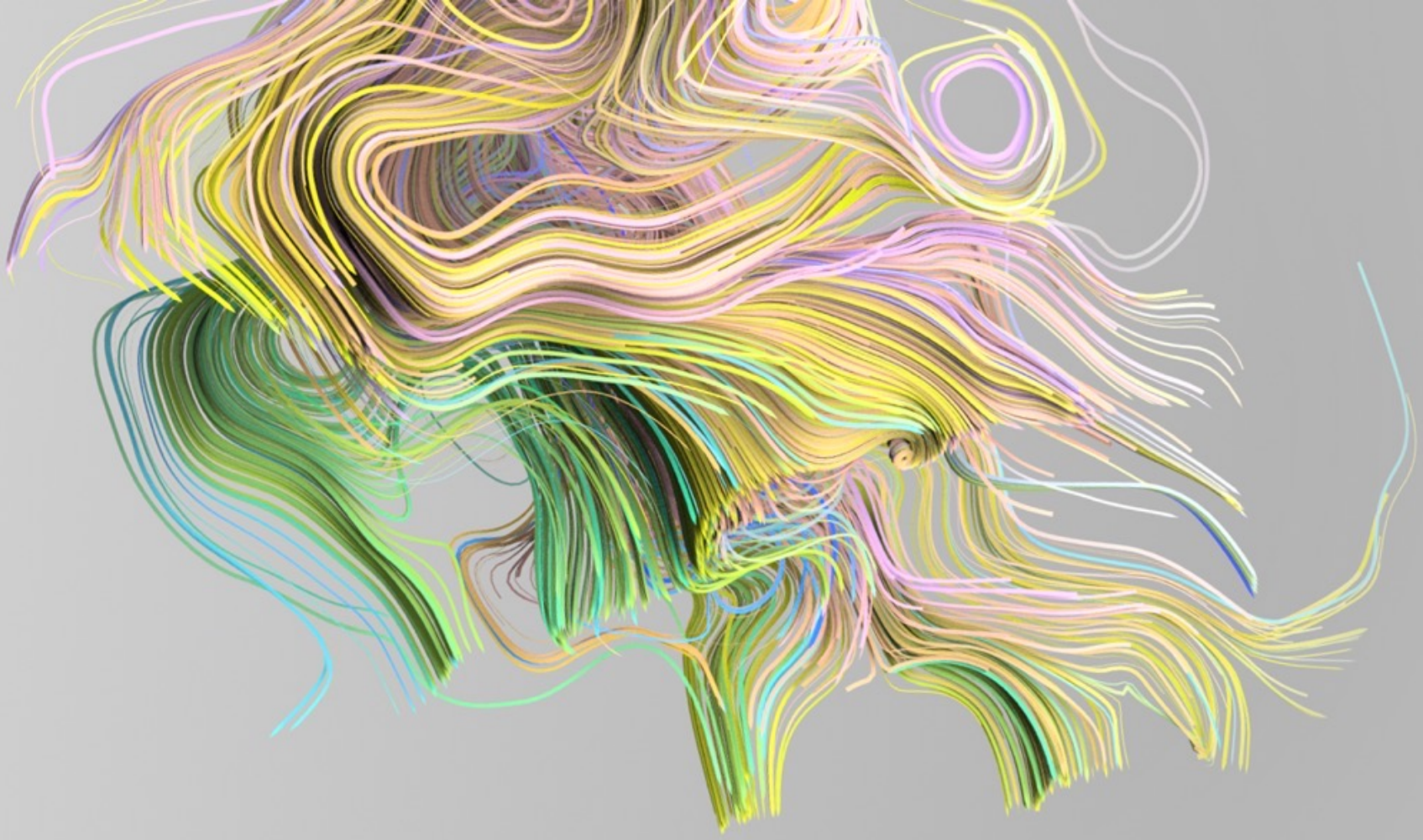
4 **Additional Risk Insights**



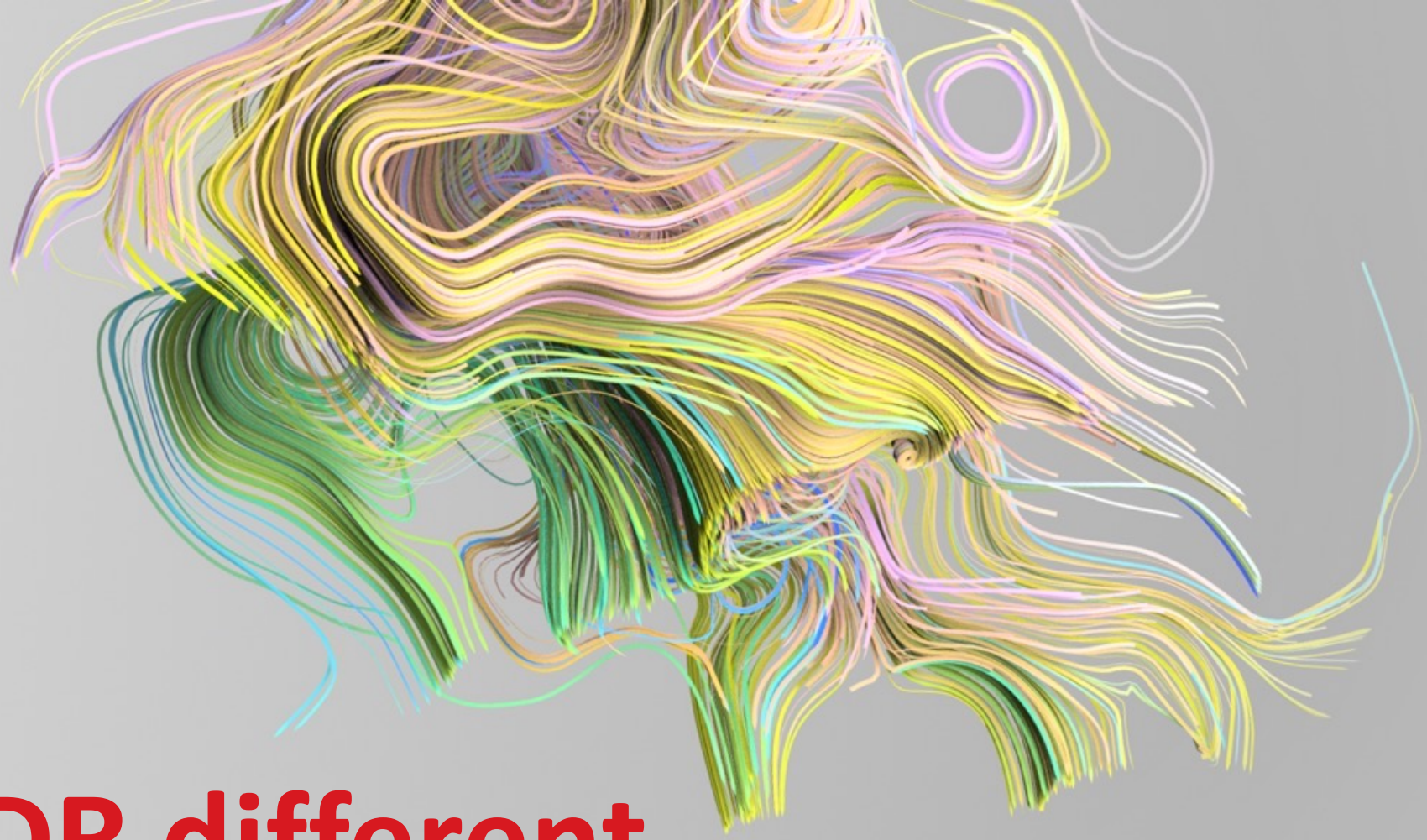
See more.

Respond Faster.



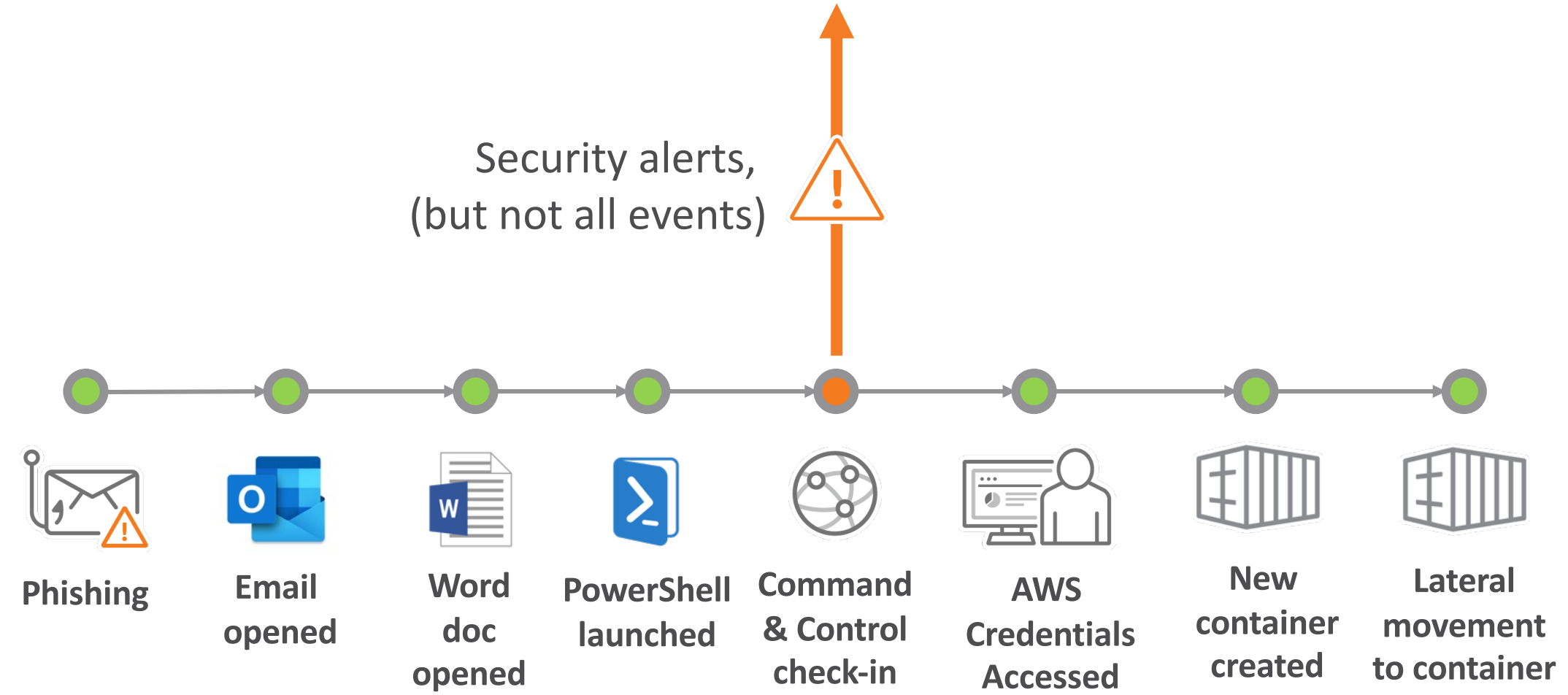


Additional information



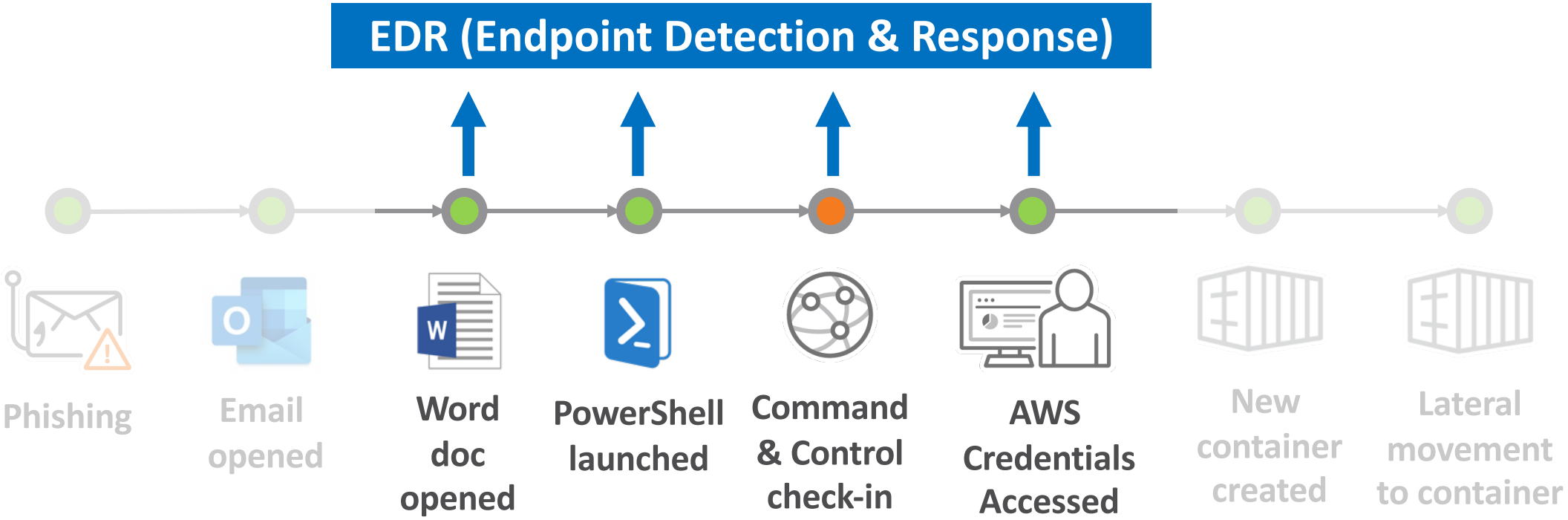
How is XDR different from SIEM? EDR?

SIEM (Security Information and Event Management)



SIEM (Security Information and Event Management)

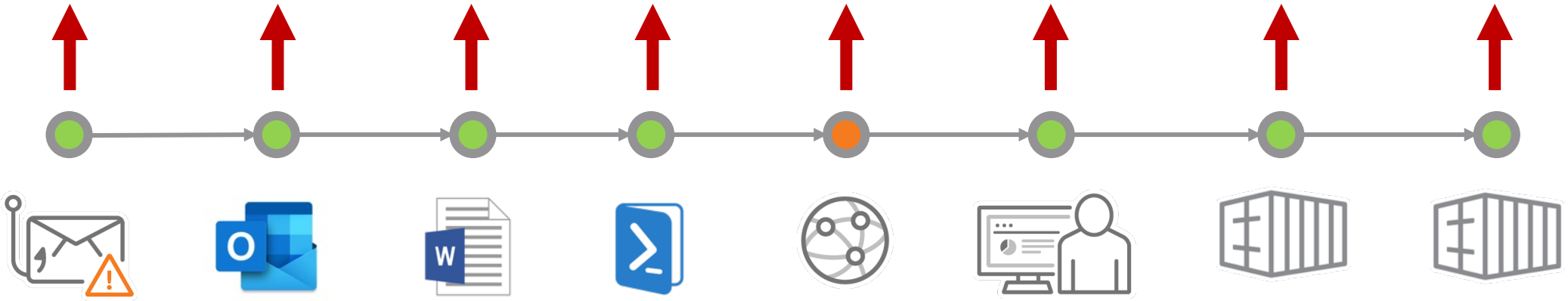
Collecting all **endpoint** activity, not just alerts



SIEM (Security Information and Event Management)

Fewer, higher-fidelity alert that tells a story

XDR (with cloud data lake collecting all activity)



Q&A

tiberio_molino@trendmicro.com

Vieni a trovarci al nostro virtual desk!

TREND MICRO™

THE ART OF CYBERSECURITY

Unknown threats detected and stopped over time by Trend Micro. **Created with real data by artist Brendan Dawes.**