



Streaming Edition 2021

## 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



Streaming Edition

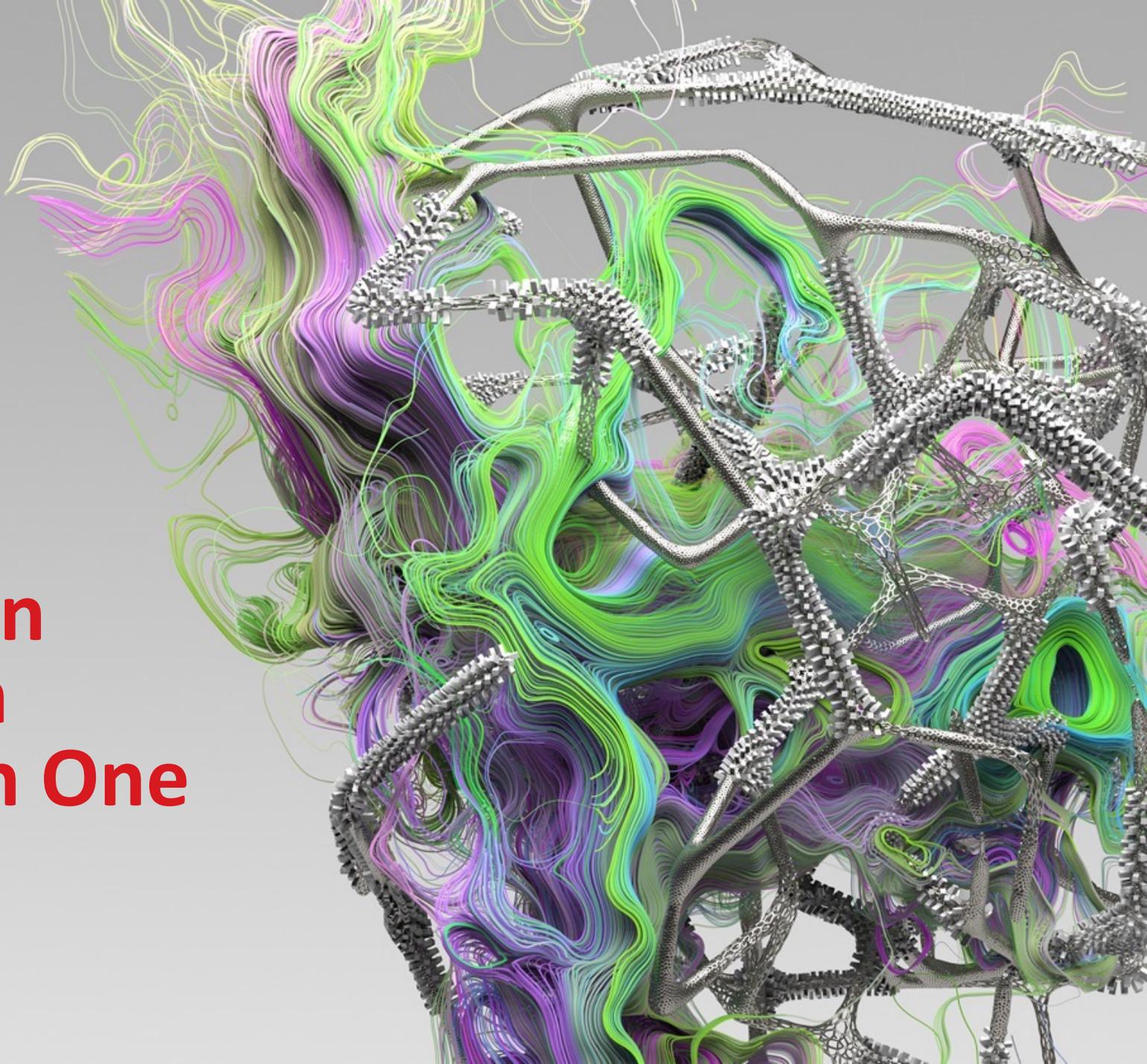
16-17-18  
marzo 2021





# Extended detection and response with Trend Micro Vision One

---



...and little visibility into email traffic and mailboxes

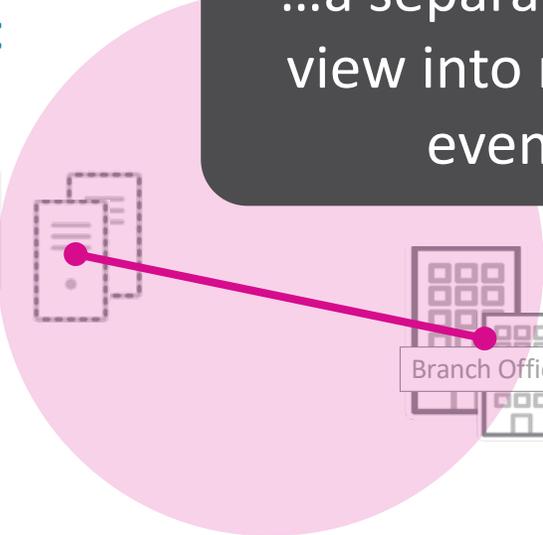
...limited visibility to threats affecting cloud workloads

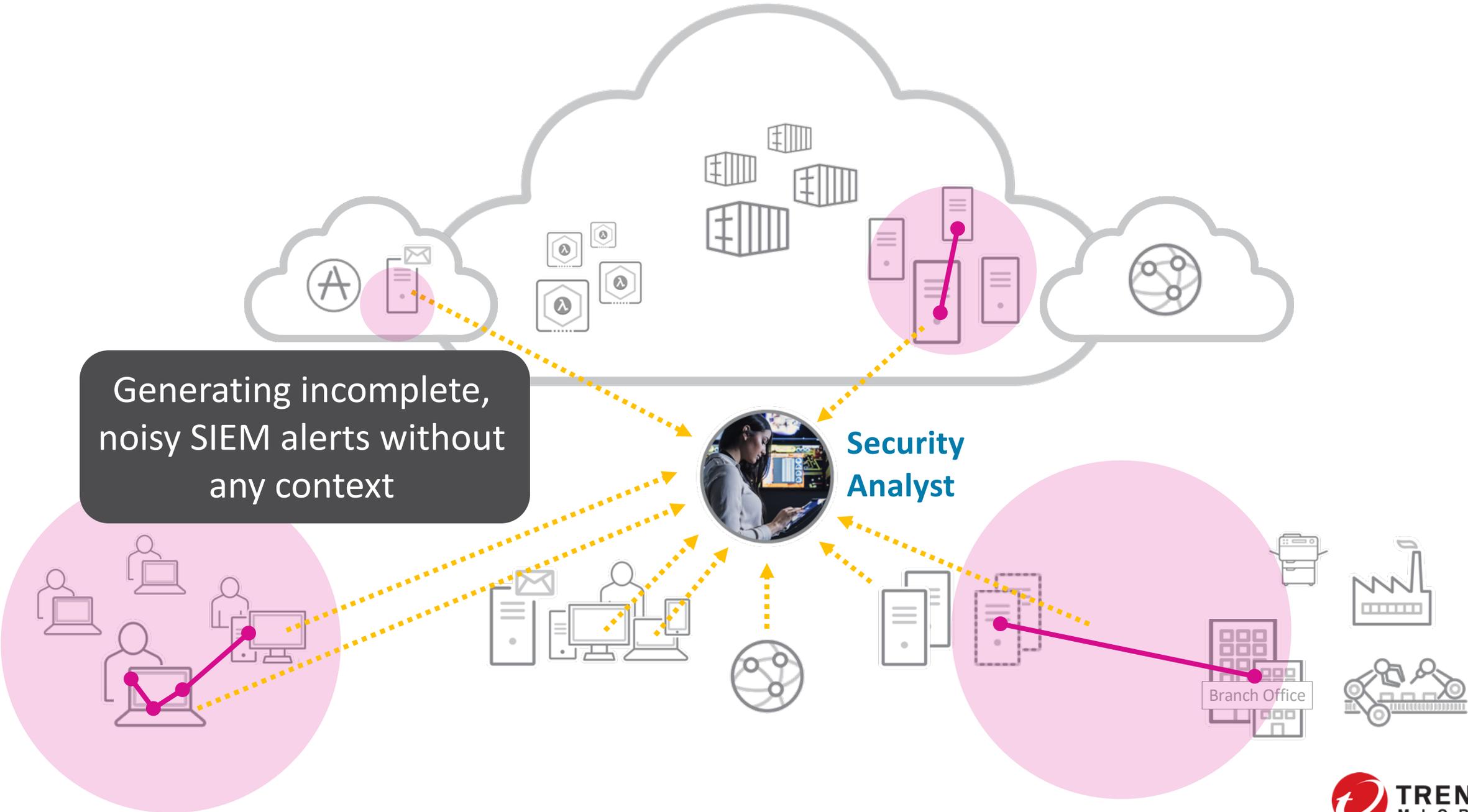
Today, the SOC gets siloed insight into endpoints (EDR)...



Security Analyst

...a separate siloed view into network events,



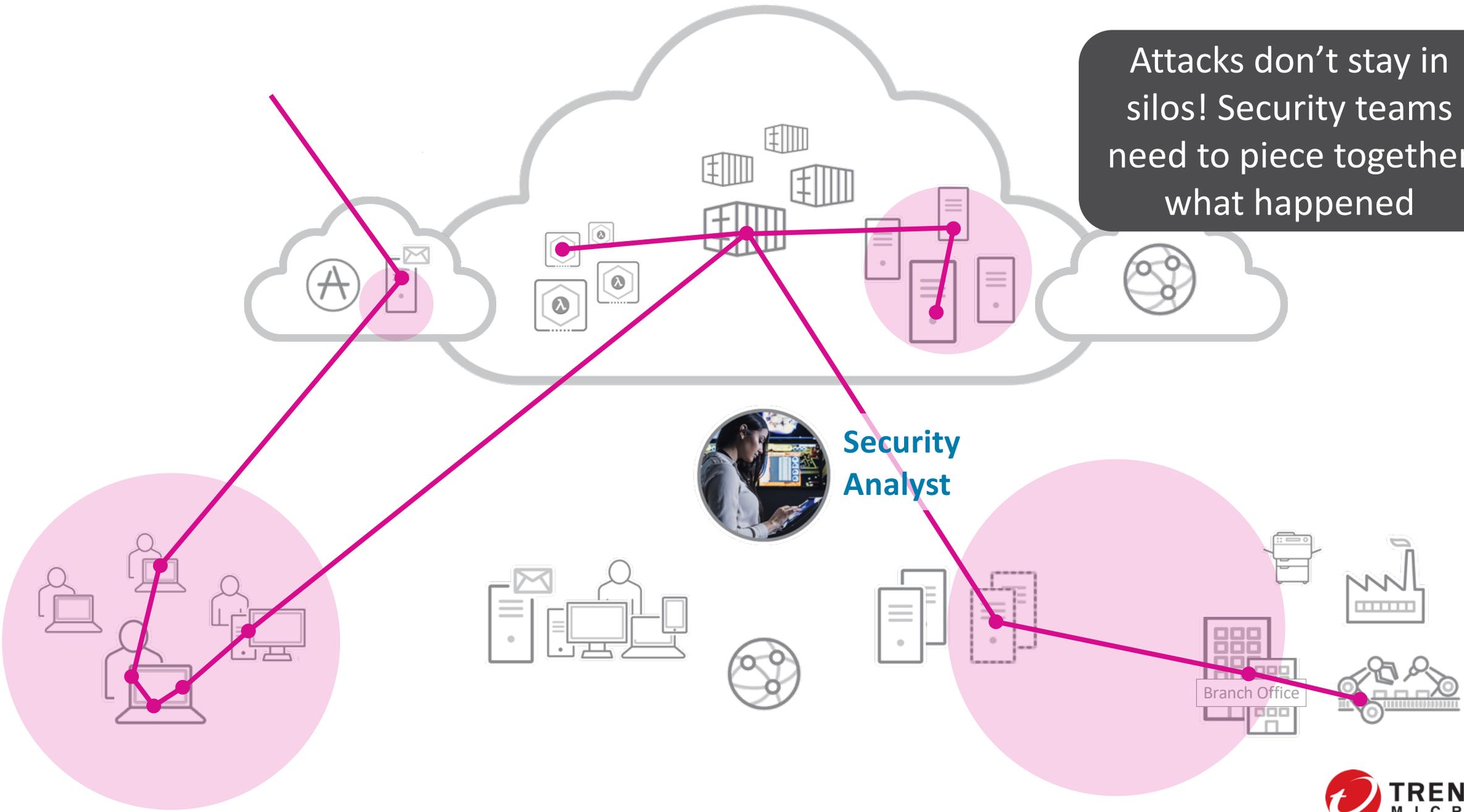


Generating incomplete, noisy SIEM alerts without any context

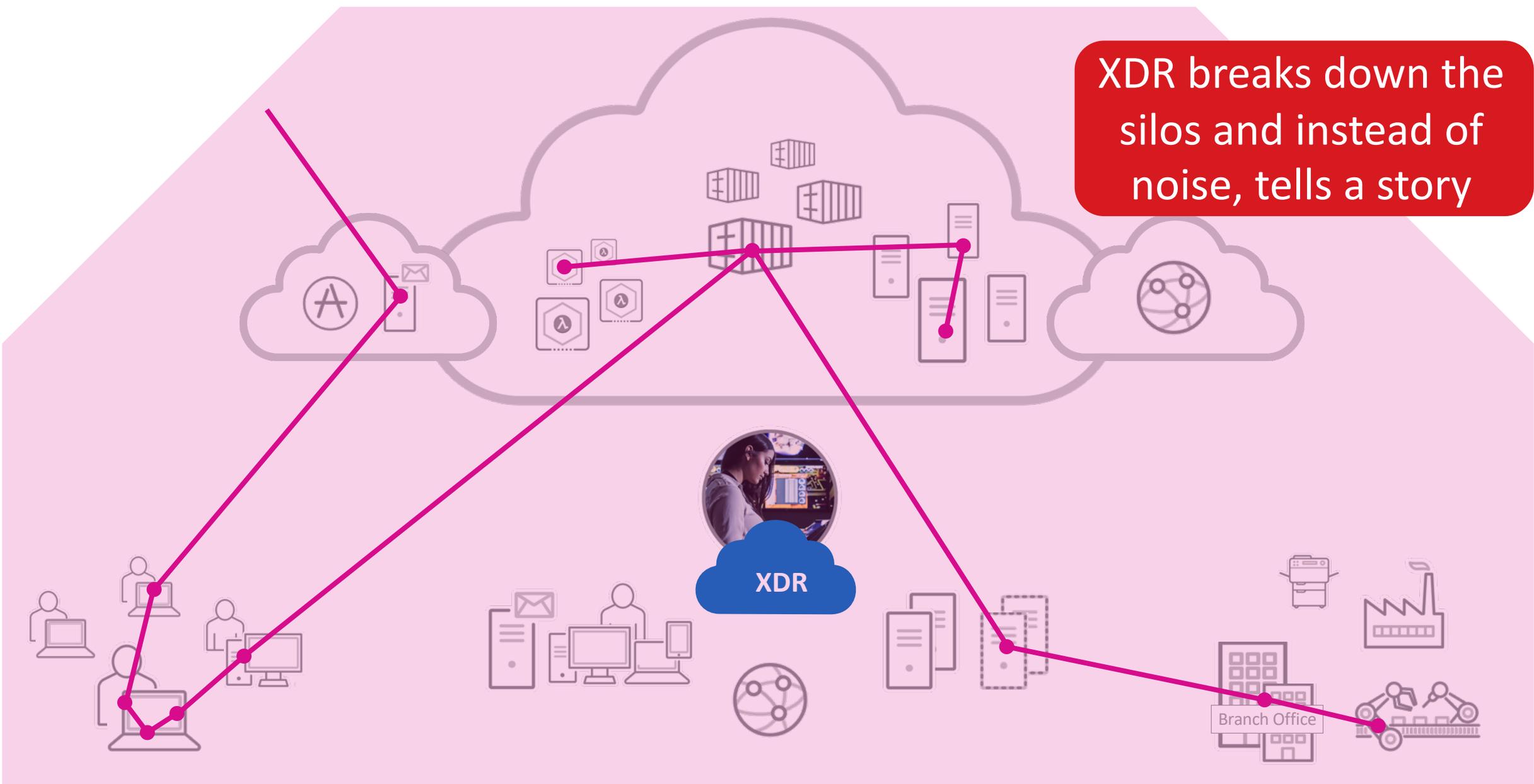
Security Analyst

Branch Office

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

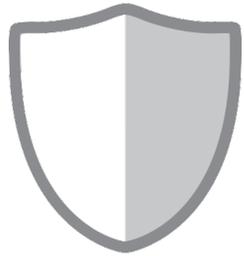


XDR breaks down the silos and instead of noise, tells a story



# Organizations with XDR...

Are better protected



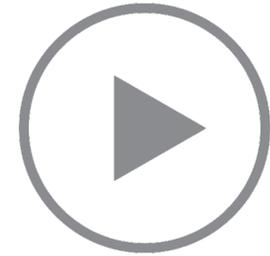
Suffered **half as many successful attacks** over the last 12 months

Detect quicker



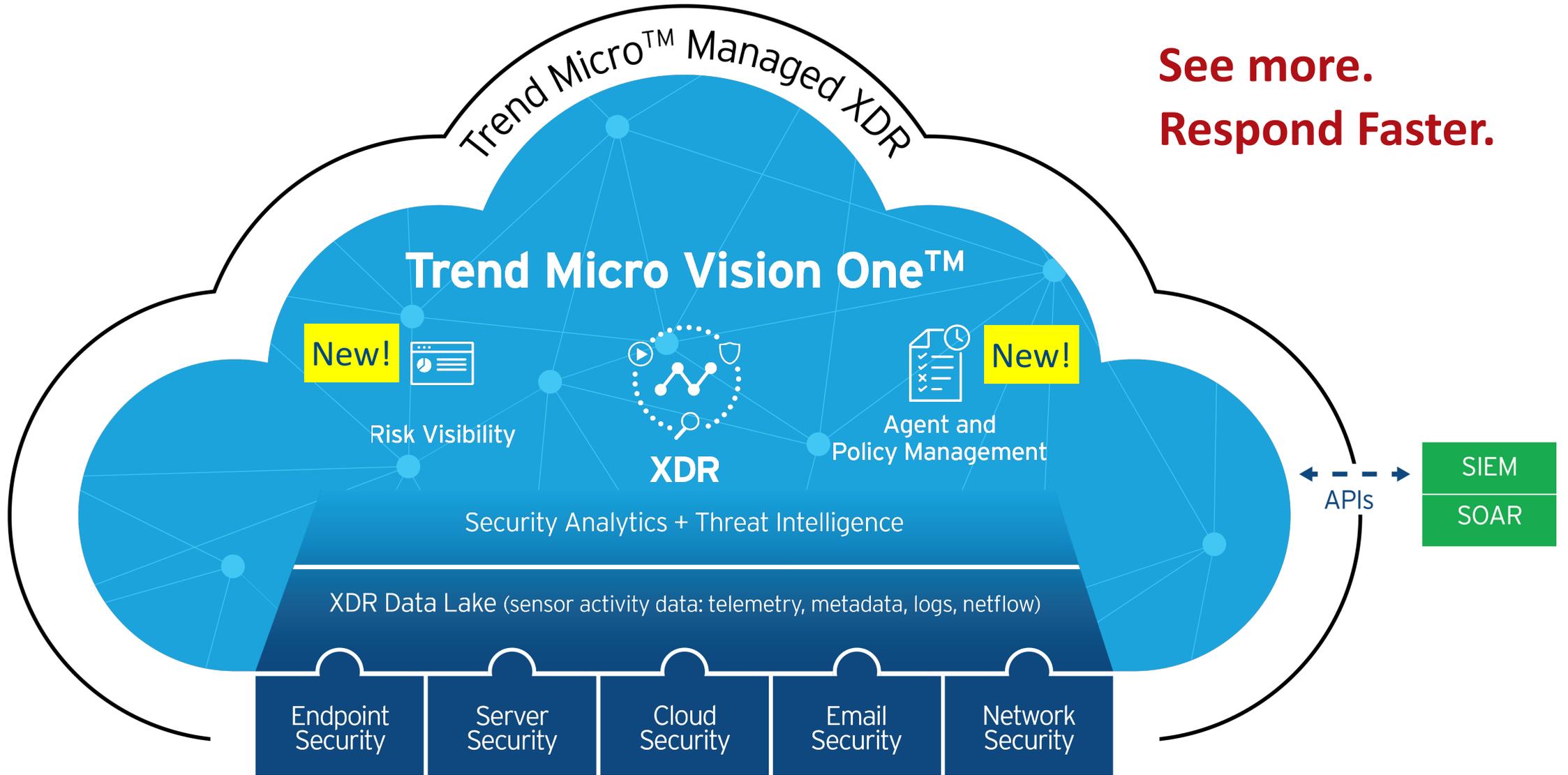
**2.2X more likely to detect** a data breach /successful attack in a **few days or less**

Respond completely

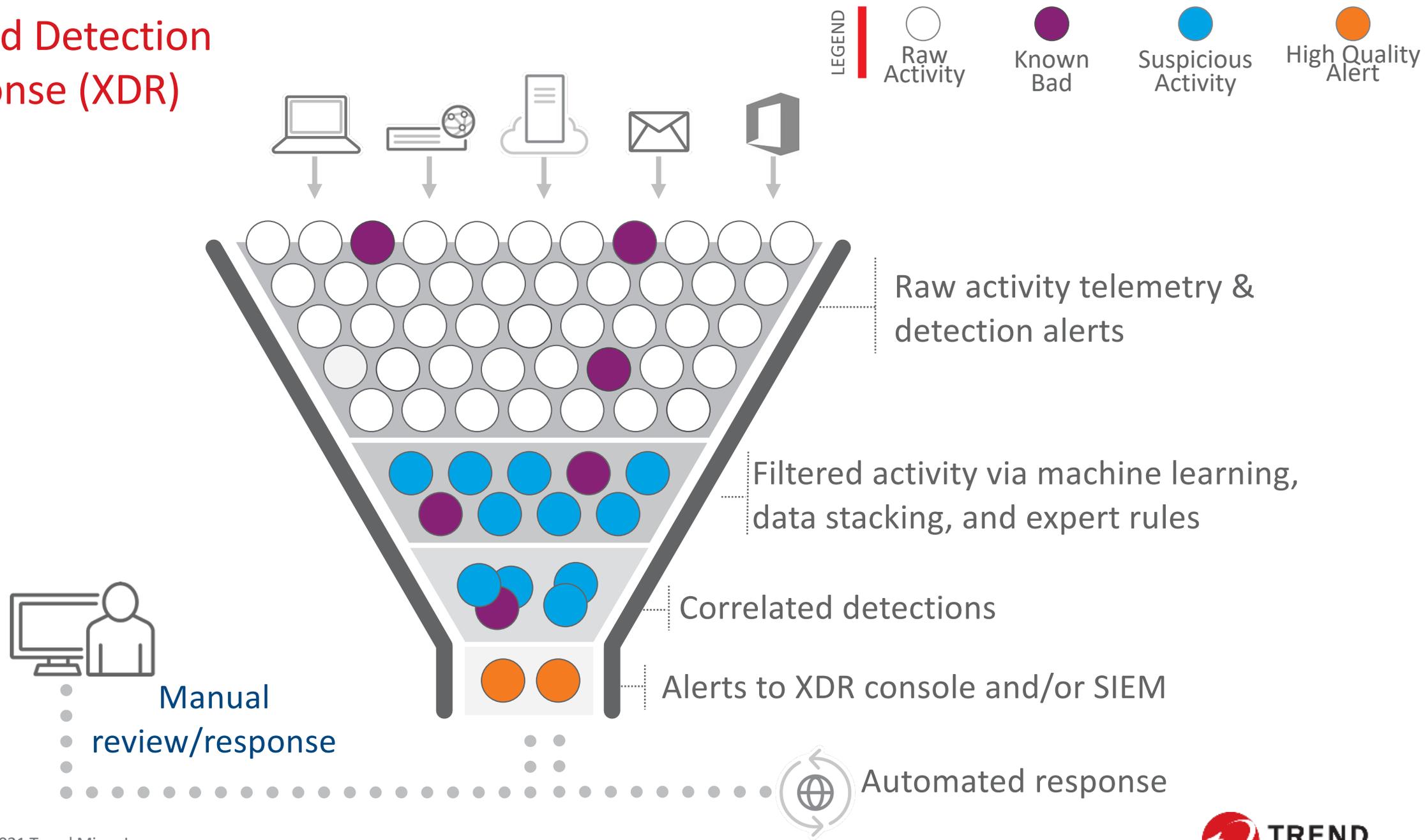


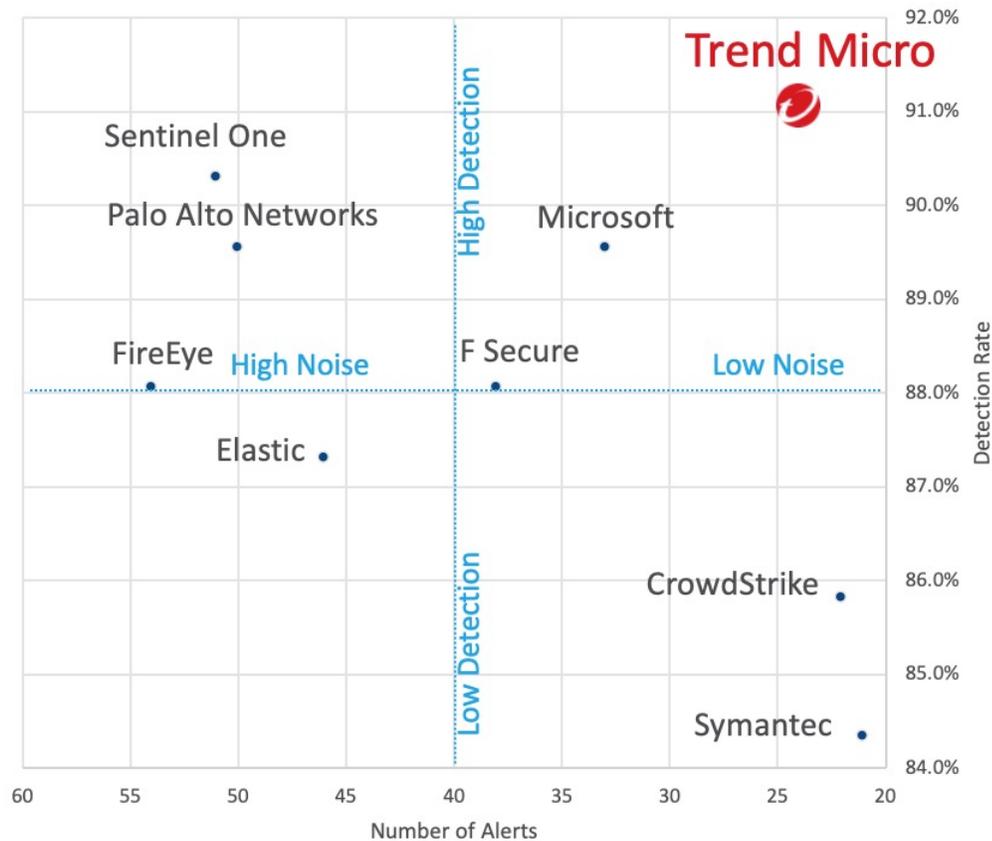
**60% less likely** to report that **attack re-propagation** has been an issue.

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



# Extended Detection & Response (XDR)





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.....

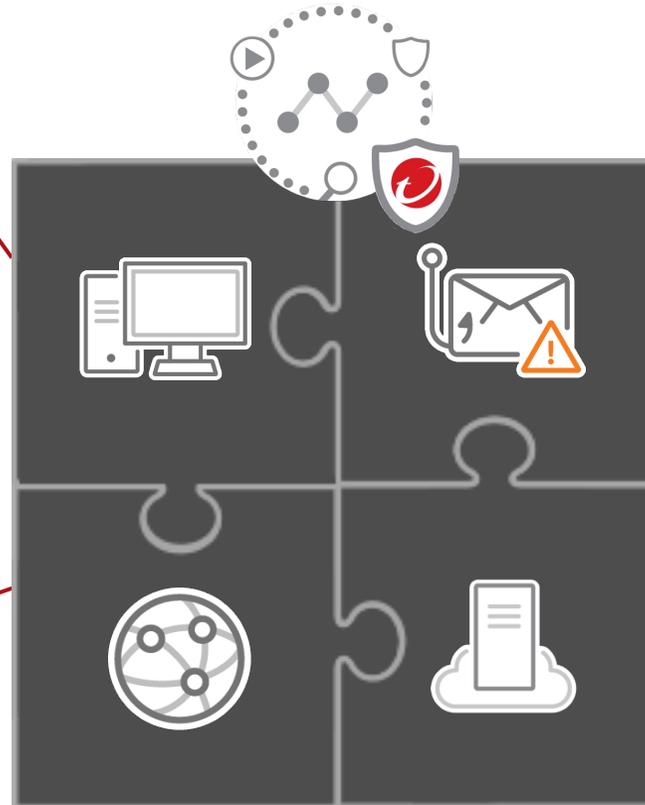
# Each Layer Adds Value

**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?



# Discover More with Correlated Detection

Security Analytics Engine finds Zero-day and Targeted Attacks

The screenshot displays the 'Detection Model Management' interface in Trend Micro Vision One. It features a table of detection models with columns for Severity, Model, Description, and Applicable products. The interface includes filters for Severity, Applicable products, Status, and Last updated, along with a search bar for Model name or description. A mouse cursor is visible over the table.

Severity	Model	Description	Applicable products
	Suspicious Script Execution Using Normal Application	A local or remote scriptlet file was executed using Regsvr.	Apex One / Apex One (Mac), Cloud One - Workload Security
	Suspicious SDB Installation	Detect someone tries to install .sdb file on the host to keep persistence	Apex One / Apex One (Mac), Cloud One - Workload Security
	Initial Access via Browser Leading to Script Execution	A user have clicked a link which led to script execution and access to a suspicious IP or domain.	Apex One / Apex One (Mac), Cloud One - Workload Security
	Suspicious DLL Execution Using Normal Application	A windows utility was abused to be used as a proxy for the execution of a suspicious Dynamic-link library.	Apex One / Apex One (Mac), Cloud One - Workload Security
	Script Execution via Misnamed Executable	Detect suspicious script execution launched by misnamed executable file	Apex One / Apex One (Mac), Cloud One - Workload Security
	Repetitive Web Reputation Services Detection by a Non-Browser Application	A repetitive connection to a Dangerous website was detected by WRS on an endpoint which may signify that an unmitigated threat is beaconing to a malicious host.	Apex One / Apex One (Mac), Cloud One - Workload Security
	Suspicious Web Access via MS Office	A suspicious web access was made from MS office application.	Apex One / Apex One (Mac), Cloud One - Workload Security
📌	Possible SpearPhishing Attack via Link	Suspicious Phishing URL in Email Attack	Cloud App Security
📌	Suspicious Double Extension LNK File Execution	Detect that LNK file with double extension launch suspicious script	Apex One / Apex One (Mac), Cloud One - Workload Security
🚫	Possible APT Attack	A backdoor was implanted in the system after a user has accessed a possible spearphishing link embedded in an email message.	Apex One / Apex One (Mac), Cloud App Security

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

**Summary** Score: 23

**Suspicious Web Access After Suspicious Email**  
A user has accessed a possible spearphishing link embedded in an email message.

Impact scope: 1 1 1

Created: 2020-04-20T09:01:56Z

**Highlights**

**Possible Spearphishing Link**  
Technique: Spearphishing Link [\(T1192\)](#)

2020-04-19T03:38:16Z

[Emergency] Important Information

www.bdfecfitddfg.com

sam@jaguartmpeggy.onmicrosoft.com

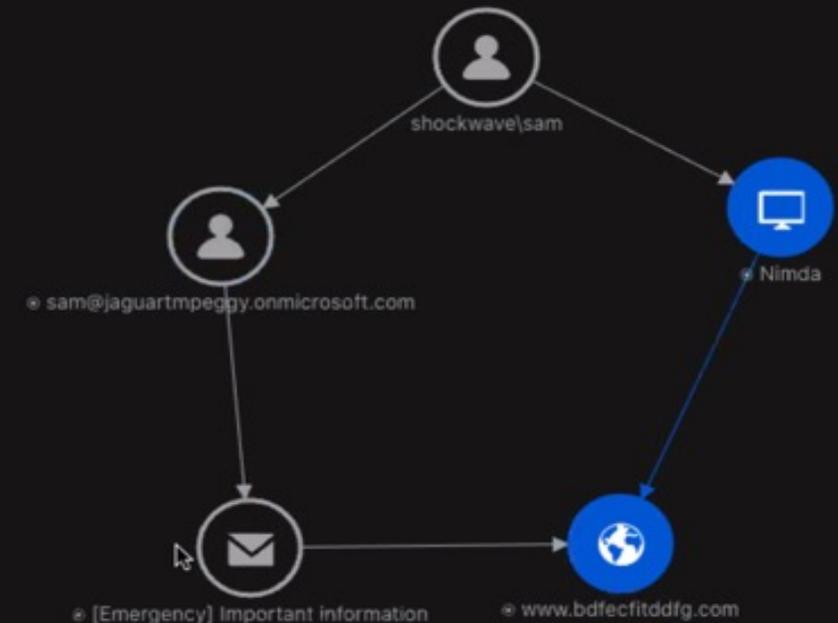
**Rare Web Domain Access (Data Stacking)**  
Technique: Standard Application Layer Protocol [\(T1071\)](#)

2020-04-19T04:43:48Z

www.bdfecfitddfg.com

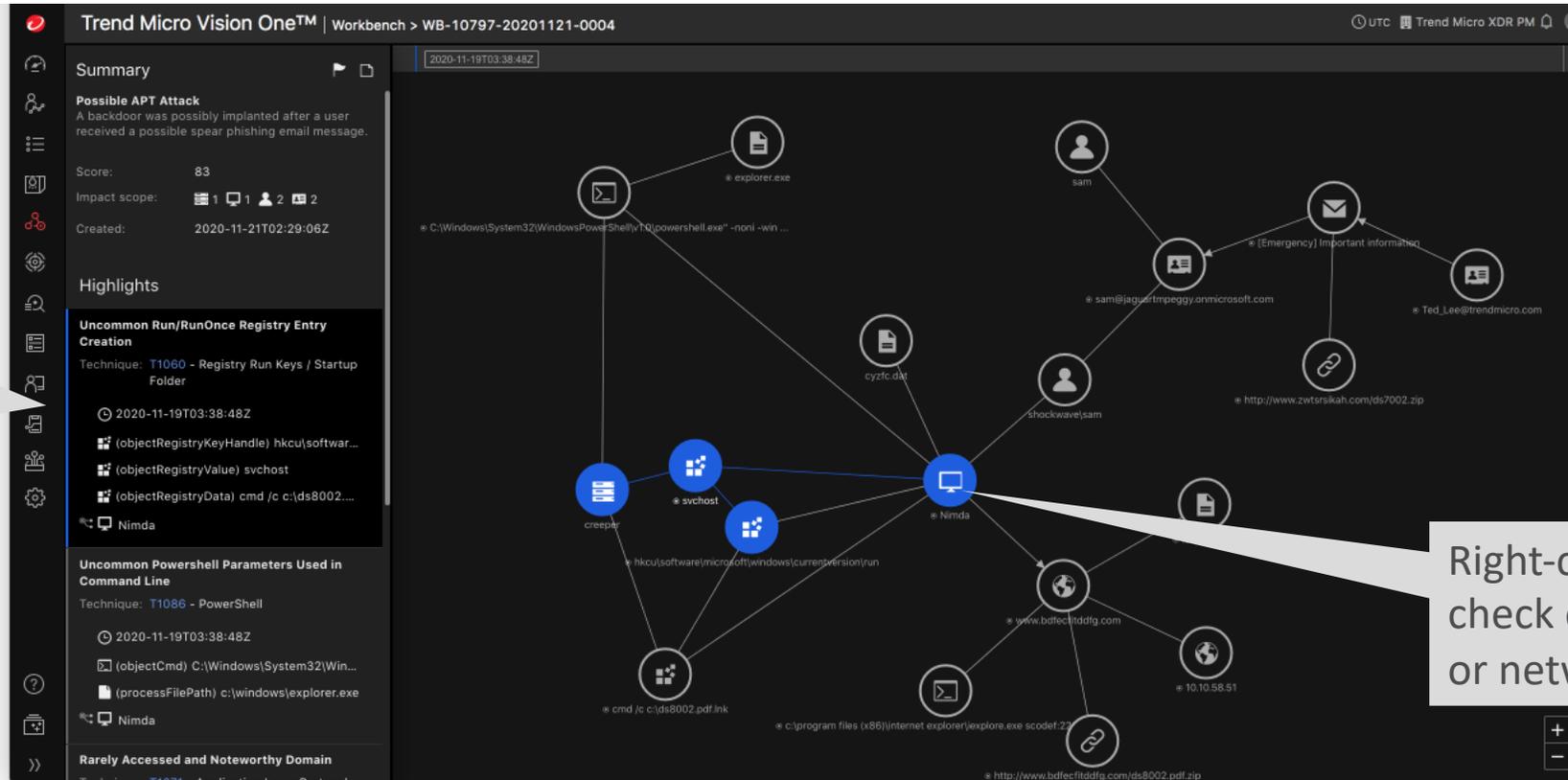
Nimda

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

The screenshot displays the Trend Micro Vision One™ Workbench interface for an analysis chain. The breadcrumb navigation shows 'Workbench > WB-10797-20201121-0004'. The main content area is divided into several panels:

- Target Endpoint:** Host name: server1, IP address: -, Criteria: Command line: bash -c echo \*/1 (curl -fsSL -...
- First Observed Object:** crons, Chain 8, 2020-04-16T23:13:35Z
- Matched Objects (32):** A list of 32 objects, all with the process name 'bash'.
- Noteworthy Objects:** A single object represented by a circle.

Below these panels, a dropdown menu indicates '8 matched chain: Chain 1: 2020-04-20T02:45:25Z'. The main visualization is a process flow diagram starting with a 'crons' node, which branches into multiple 'bash' nodes, illustrating the execution profile of the attack.

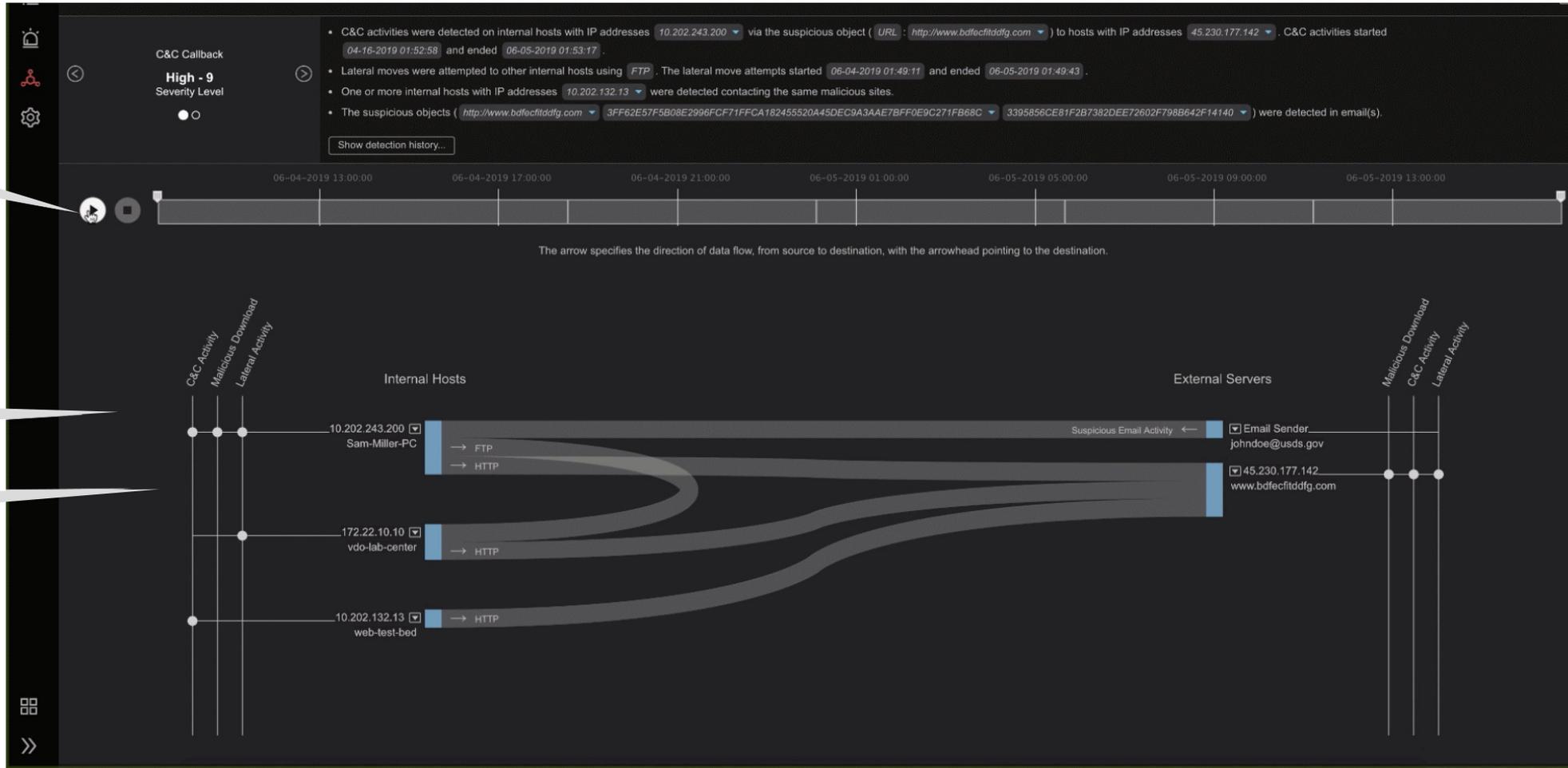
# Integrated Investigation and Response

Quickly visualize the story of an attack

Graphically replay communication activity

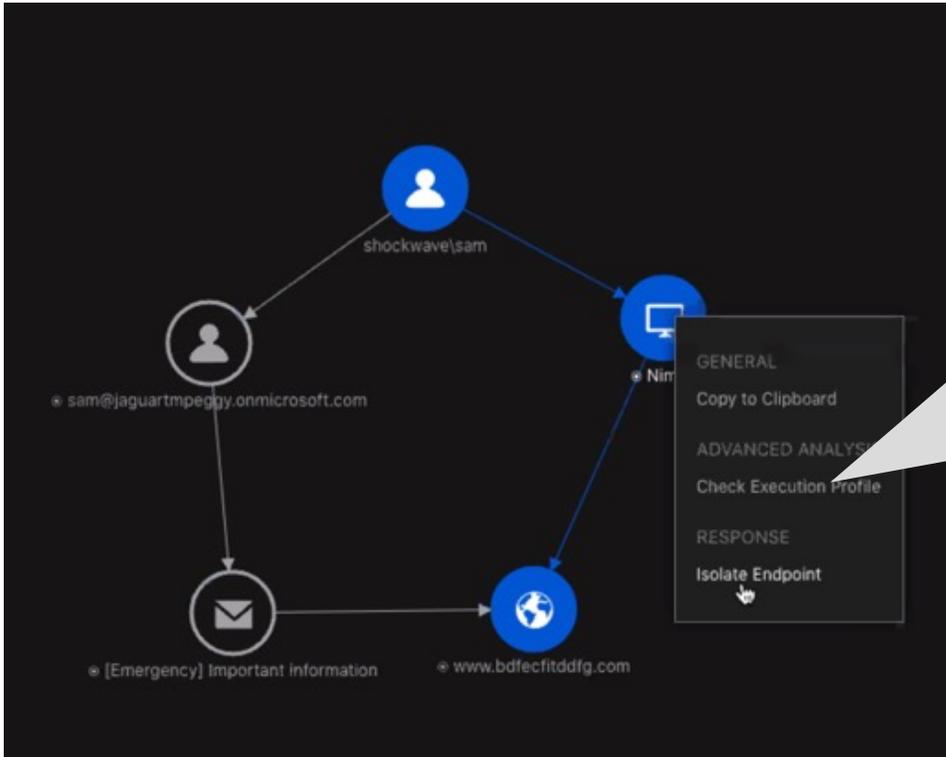
1<sup>st</sup> target and C&C

Lateral movement



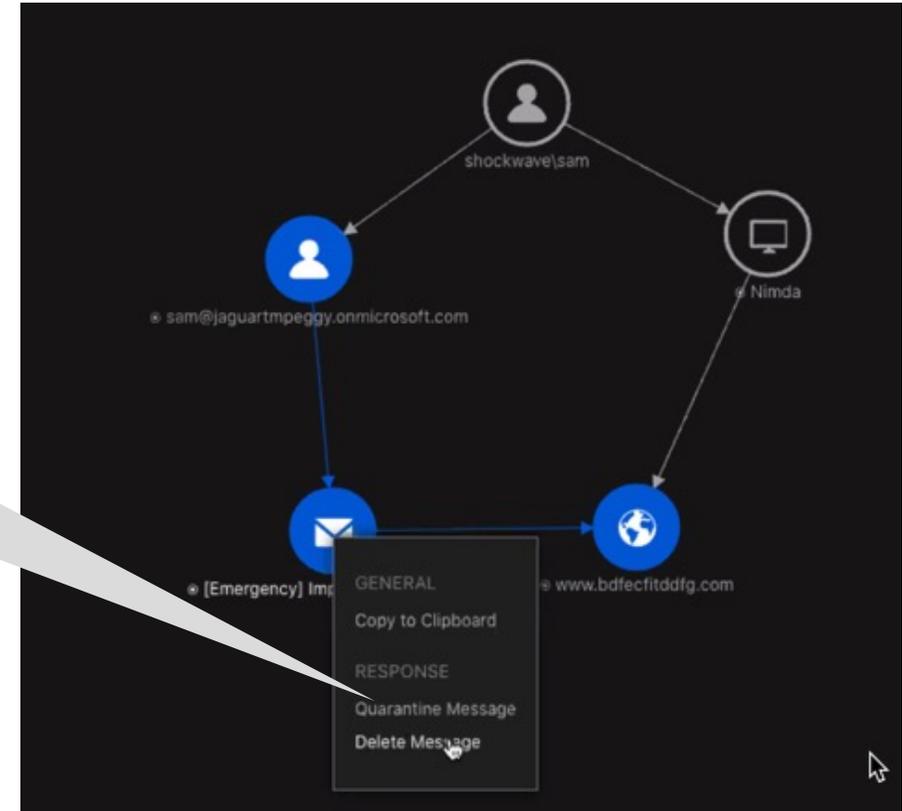
# Respond Faster and More Completely

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 Vision One™ | Intelligence Reports UTC Trend Micro XDR PM

Threat Intelligence integrates up-to-the-minute intelligence reports from Trend Micro and third parties to help you identify threats. When enabled, Threat Intelligence parses your event logs, matches the data against intelligence reports, and generates alerts based on threat detections. To enable or disable Threat Intelligence Sweeping, go to [Detection Model Management](#).

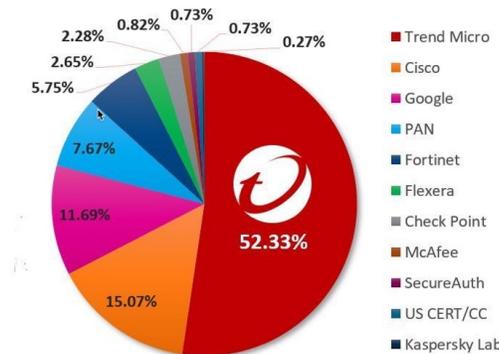
Now: Enabled Last updated: All Report keywords

Intelligence report	Campaign	Target region/country	Target platform	Reference	Last updated ↓
Indicators of compromise reported by third-party sources	-	-	-	-	2021-02-08T18:40:22Z
Operation Spalax: Targeted malware attacks in Colombia	Spalax	Colombia	-	-	2021-02-02T06:40:22Z
Vadokrist: A wolf in sheep's clothing	MSI overload	-	-	-	2021-02-02T06:40:22Z
Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop	-	-	Windows	-	2021-01-27T10:40:21Z
SUNSPOT: An Implant in the Build Process	-	-	-	-	2021-01-27T10:40:21Z
DarkUniverse – the mysterious APT framework #27	-	Iran, Ethiopia, United Arab ...	-	-	2021-01-25T02:40:21Z
Hard Pass: Declining APT34's Invite to Join Their Professional Network	-	-	-	-	2021-01-25T02:40:21Z



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



# Search the XDR Data Lake

Search method: General

General

ADVANCED

Endpoint Activity Data

Message Activity Data

Network Activity Data

Detections

objectCmd:bin/sh AND tags: MITRE.T1105

View History

Saved Queries

Export Result

2020-09-22T16:45:08Z - 2020-10-22T16:45:08Z

Last 30 days

Search

Combine criteria with MITRE framework

Search through all or specific data sources

DATA GROUPING

ENDPOINT ACTIVITY DATA

- dpt 1
- dst 1
- endpointGuid 1
- endpointHostName 1
  - agent1010 1
- hostName 1
- objectHostName 1
- objectIpp 1
- objectPort 1
- objectUser 1
- spt 1
- src 1

DETECTION DATA

- endpointIpp 1
- request 1
- suid 1
- endpointHostName 1
- eventName 1
- endpointGUID 1

Logged

2020-10-01T19:13:56Z

dpt: | dst: | endpointGuid: b4032449-090b-4b36-bc21-e66a9b0f6324 | endpointHostName: Agent1010 | endpointIpp: 192.168.44.136, ::1, 127.0.0.1 | eventId: 7 | eventSubid: 602 | hostName: | logonUser: david | objectCmd: | objectFileHashSha1: | objectFilePath: | objectHostName: ca75-1.winshipway.com | objectIpp: | objectIpps: | objectPort: | objectRegistryData: | objectRegistryKeyHandle: | objectRegistryValue: | objectSigner: | objectSignerValid: | objectUser: | parentCmd: | parentFileHashSha1:...

2020-10-01T19:13:56Z

request: https://ca75-1.winshipway.com | rt: 2020-10-01T19:13:56+00:00 | interestedIpp: 192.168.44.136 | aggregatedCount: 1 | rating: Dangerous | rtHour: 19 | suid: FO REVER\david | score: 49 | senderGUID: 000D3AA5-24B8-5E67-E37B-02FA233C880D | act: Block | endpointHostName: AGENT1010 | mpver: 2019.5299 | blocking: Web r eputation: | deviceGUID: 5a3fc148-a85f-4d95-8d31-53ee347688a1 | dvchost: CU-PRO1-7422-2 | endpointMacAddress: 00-0C-29-80-88-1E | mDeviceGUID: 000D3AA5...

mail\_message\_sender: speardave7@protonmail.com | mail\_message\_recipient: david@xinesys.com | mail\_message\_subject: Last minute | mailbox: david@xinesys.com | mail\_urls: https://ca75-1.winshipway.com, http://www.bdfectitddf.com | source\_domain: protonmail.com | source\_ip: 185.70.40.140 | mail\_message\_delivery\_time: 2020-10-01T17:00:09.000Z | mail\_message\_id: <GaLmp55JXmLV3S-q4C1bv30AKSGriMbAv8OGYA8...>

speardave7@protonmail.com

david@xinesys.com

Last minute

david@xinesys.com

GENERAL

Copy to Clipboard

SEARCH

New search: match field and value

Add Filter: field IS value

Add Filter: field IS NOT value

Google

RESPONSE

Quarantine Message

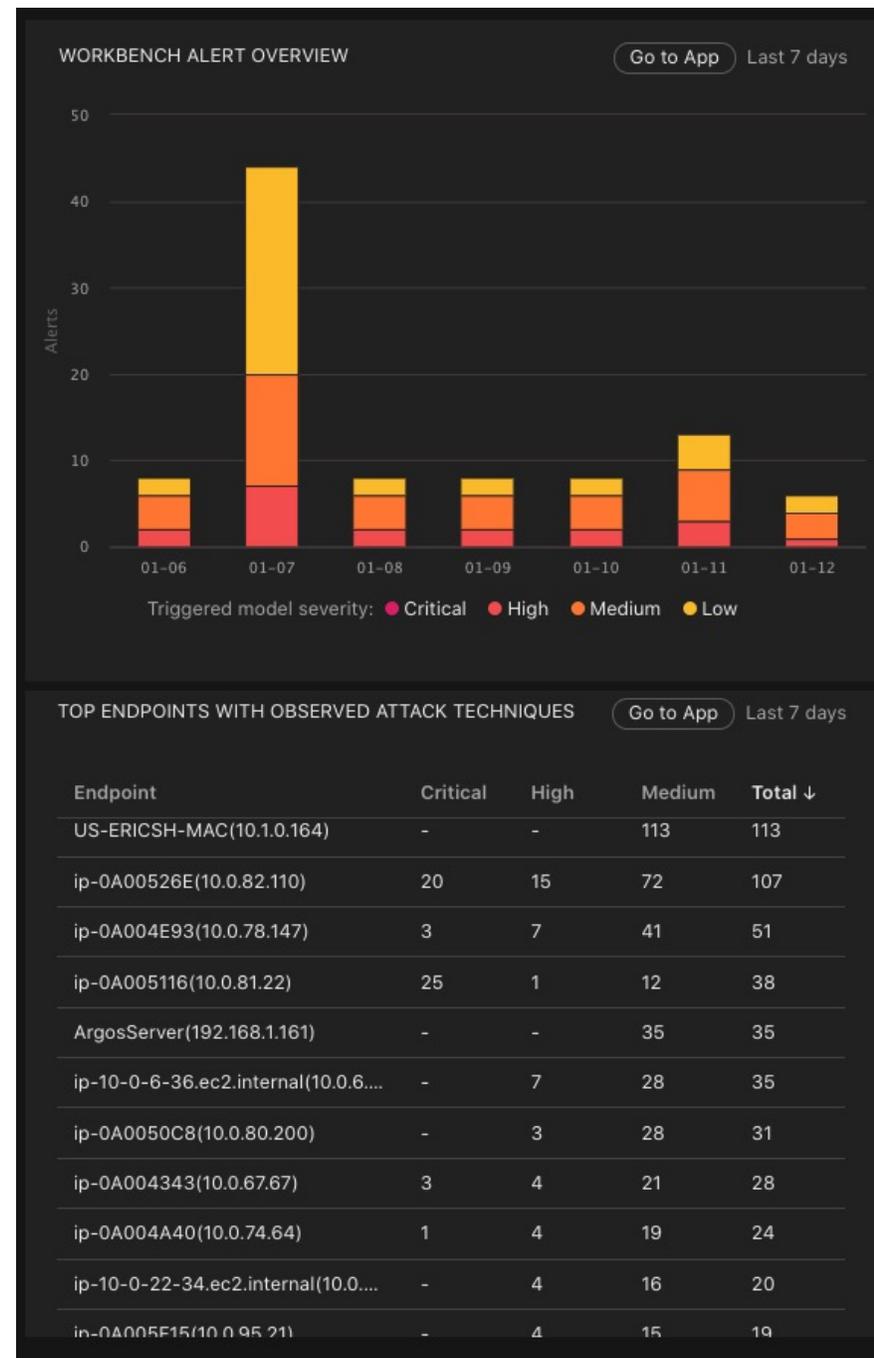
Delete Message

Take actions or open an investigation workbench directly from the results

Filter results

# Risk Visibility

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



# Risk Visibility

## Cloud App App Usage (preview)

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

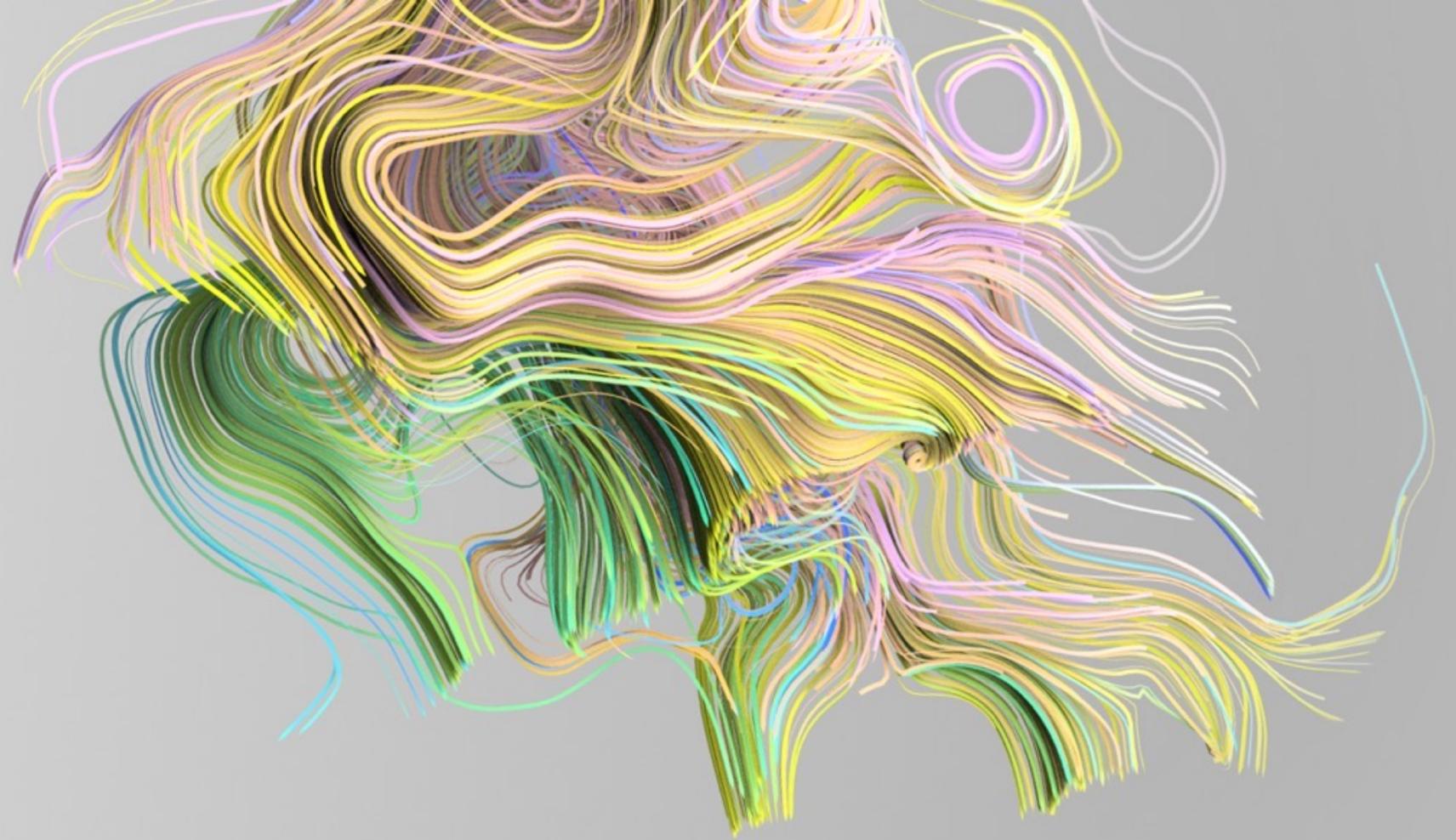
Uses data from existing sensors, Azure AD, or 3<sup>rd</sup> party firewall logs

Trend Micro XDR | Identity and Risk Insights (Preview) UTC Trend Micro

< Back

Source	Data target	Last sync	Data upload st...
Azure AD	User activities on sanctioned cloud apps	-	Off
3rd party logs	User activities on detected cloud apps	-	Off
Endpoint Sensor	Cloud apps detected by monitored endpoints	2021-01-12T23:36:...	Off





# Managed XDR MDR service

# Managed XDR: MDR Service by Trend Experts

## Expert Threat Hunting

Cutting-edge techniques with verification and enrichment by threat experts



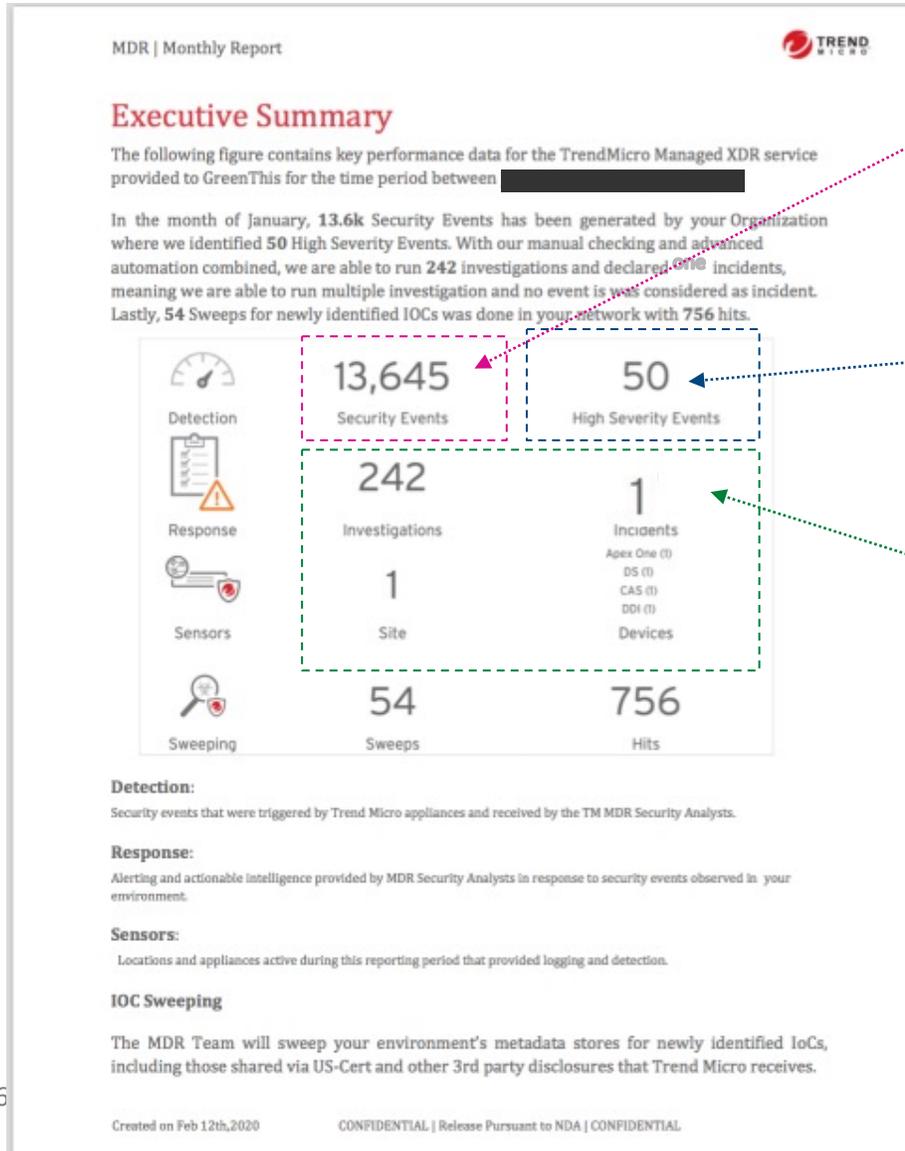
## 24x7 Monitoring & Detection

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

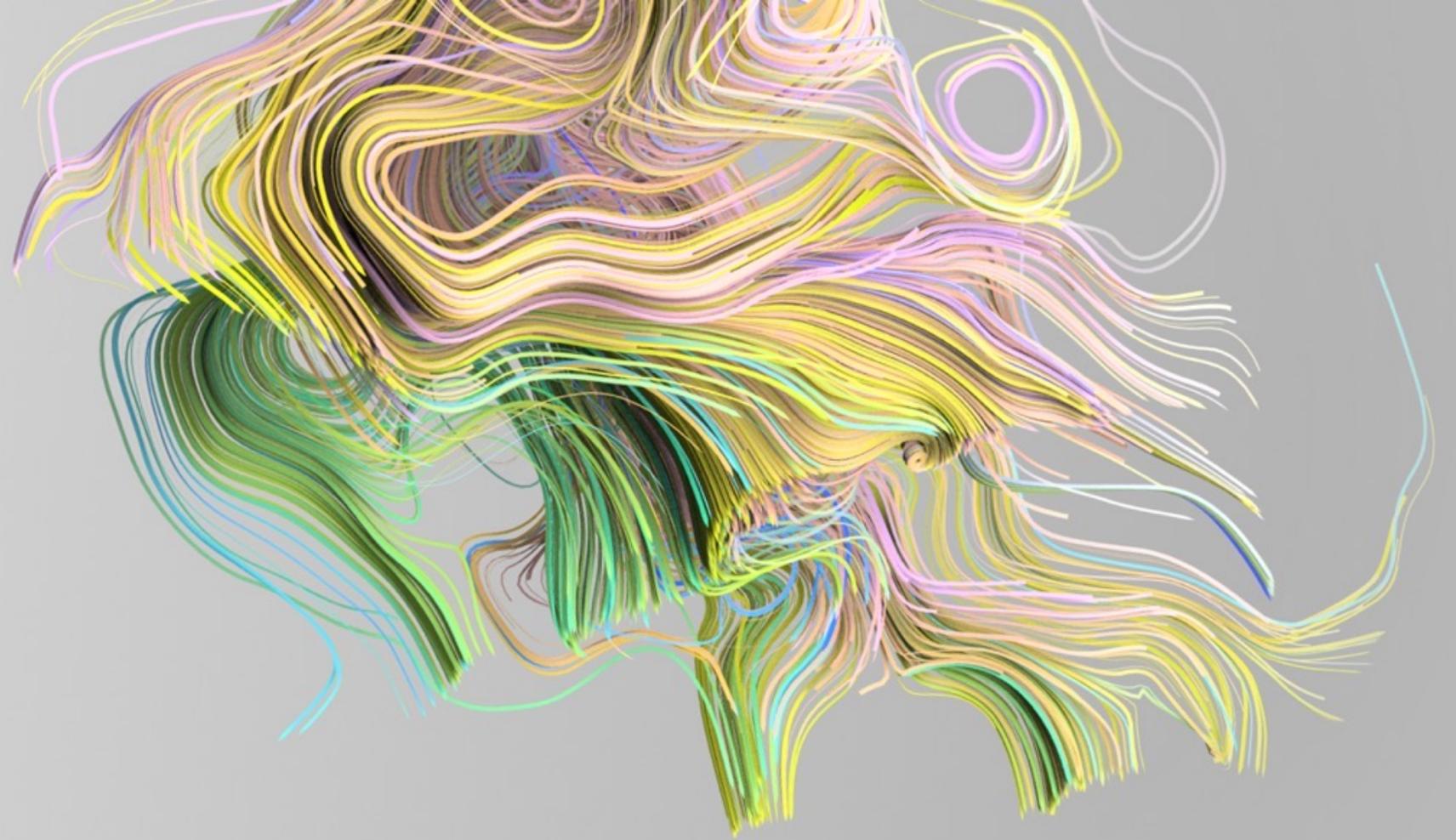
# What it Means for the Customer



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.”*



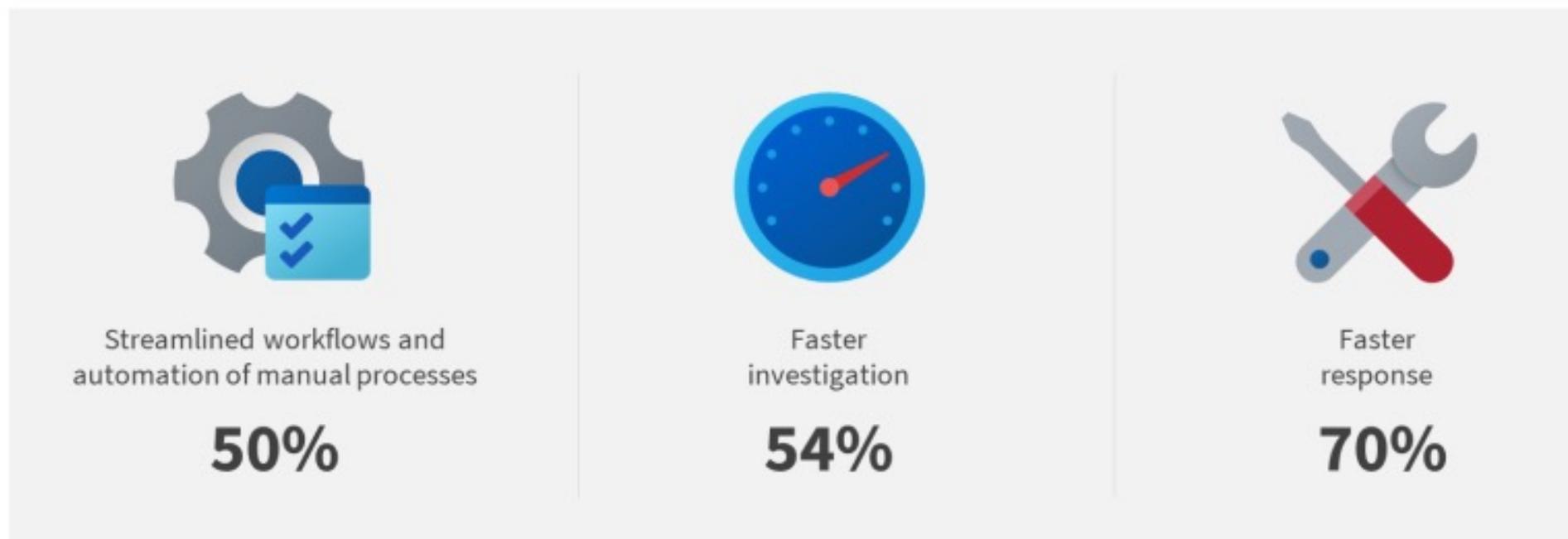
*“The way XDR allows me to drill down is amazing. It literally paints a picture in front of you.”*

# 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	<i>partial</i>
Deep understanding of all data generated by layers	Yes	No	No
Integrated investigations in one console	Yes	No	<i>partial</i>
Integrated response actions across layers	Yes	No	Yes

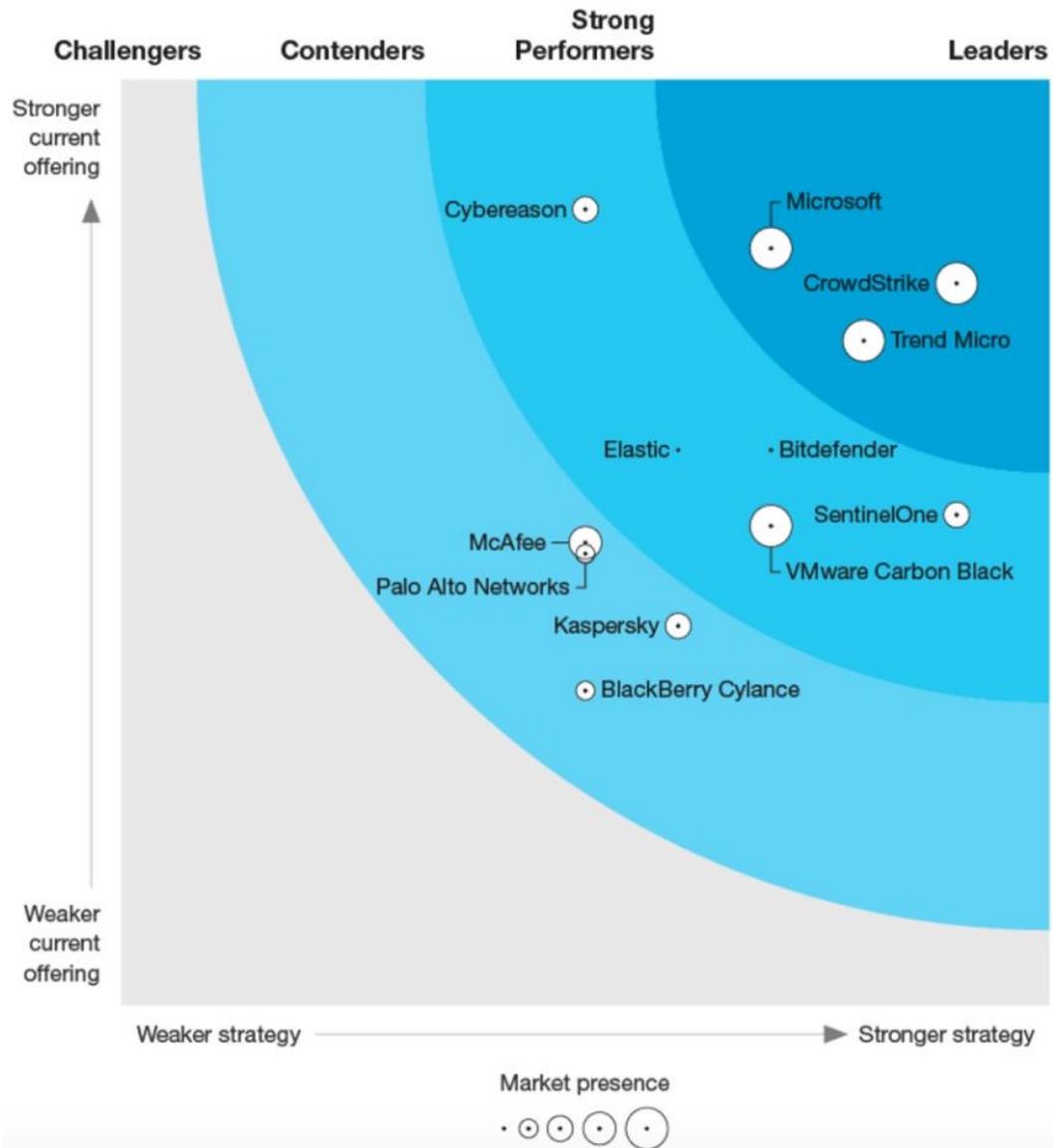
# Correlation is critical, but not possible without XDR

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



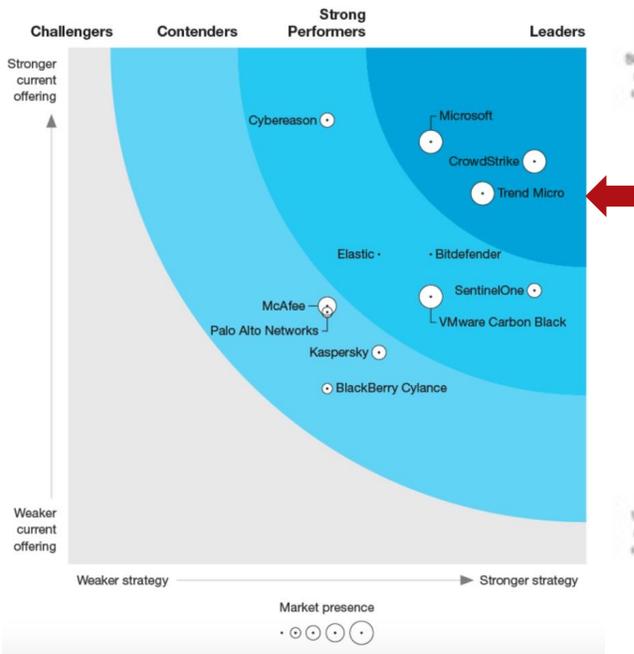
**“Trend Micro delivers XDR functionality that can be impactful today.”**

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



# 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

“The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.”



# Why Trend Micro Vision One?

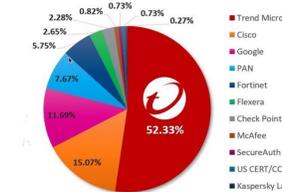
- 1 Purpose-built XDR platform with deep integration into native sensors



- 2 Distinctive data sources

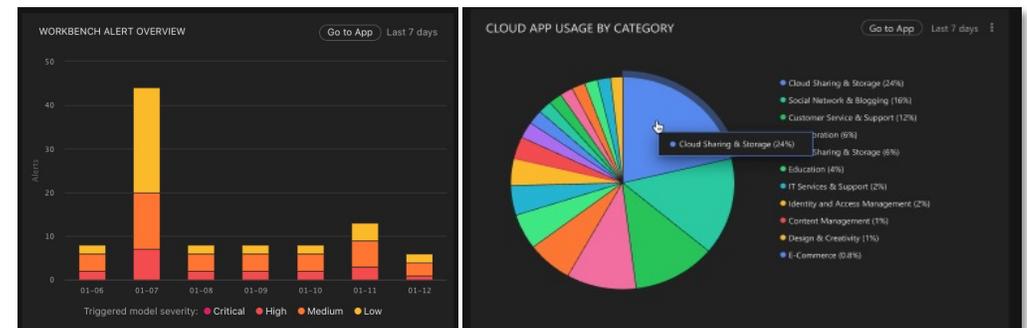
<p><b>Cloud</b> - breadth and timeliness of Linux support</p> <p>Cloud - breadth and timeliness of Linux support</p>	<p><b>Email</b> - visibility + response by integrating at the <i>application layer</i></p>
--	--

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



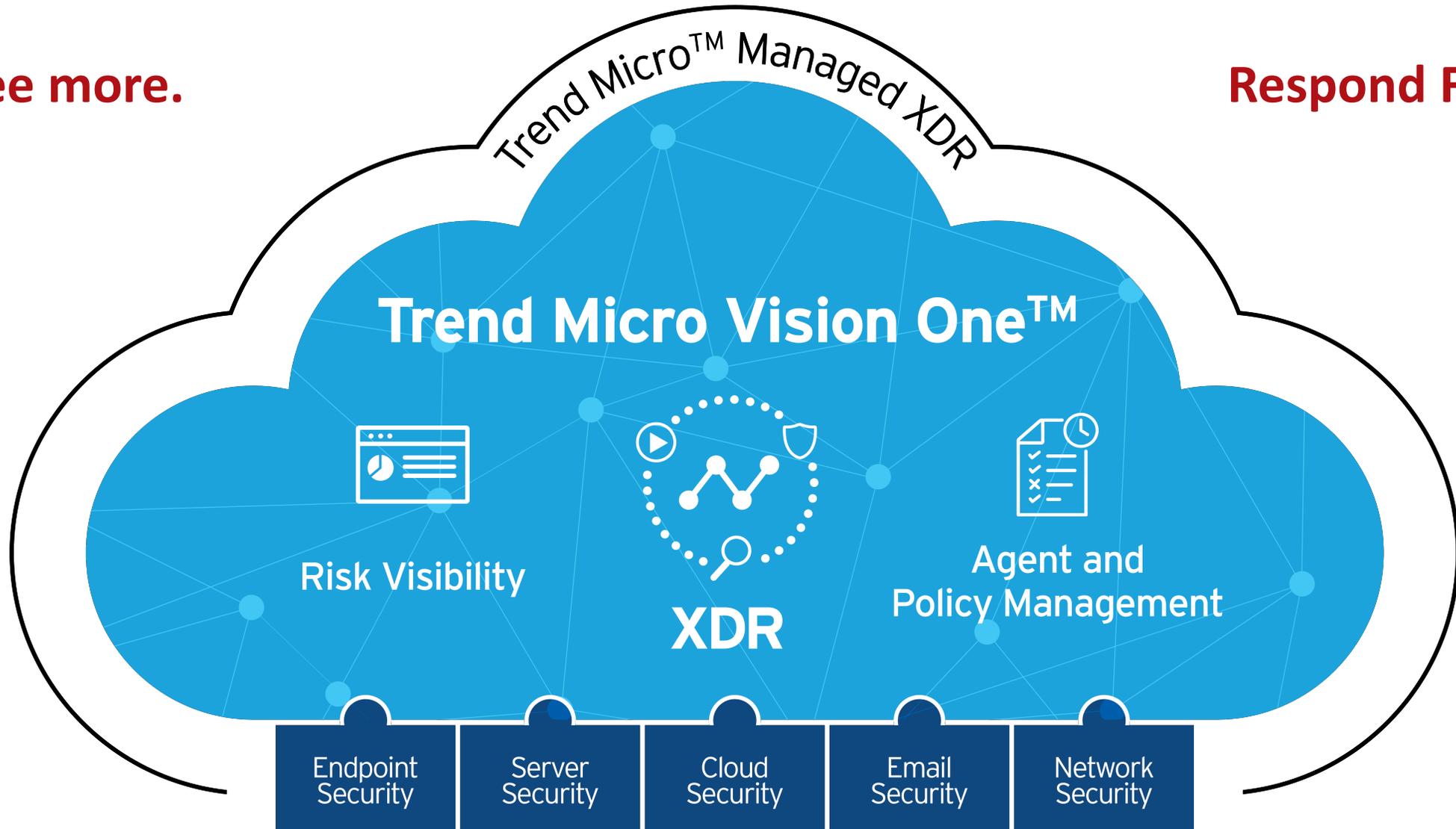
Trend Micro discovered **over half** the disclosed vulnerabilities in 2019

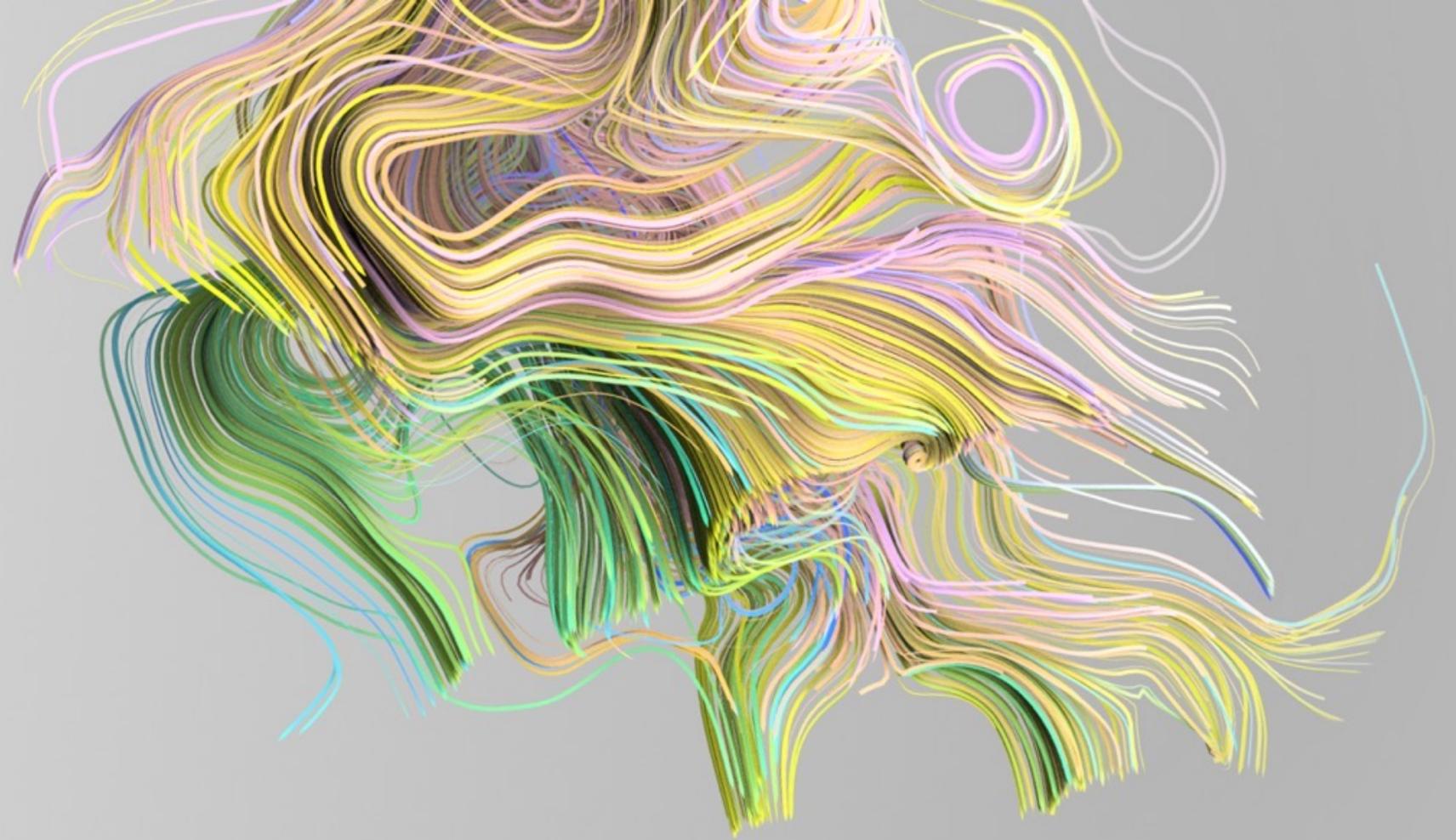
- 4 Additional Risk Insights



See more.

Respond Faster.





# Additional information



# How is XDR different from SIEM? EDR?

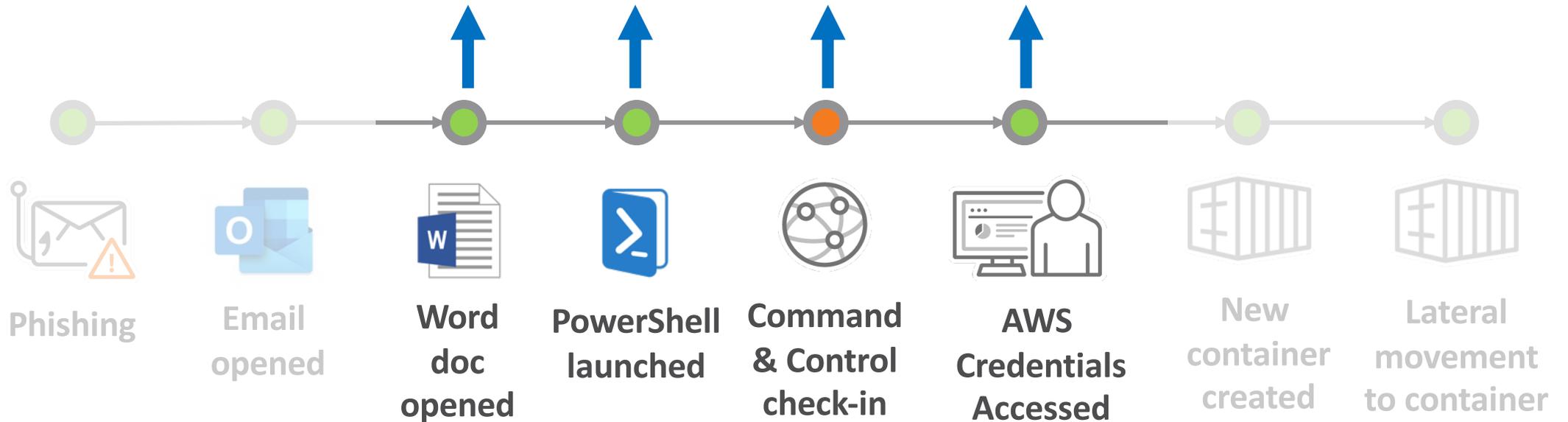
# SIEM (Security Information and Event Management)



# SIEM (Security Information and Event Management)

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

## EDR (Endpoint Detection & Response)

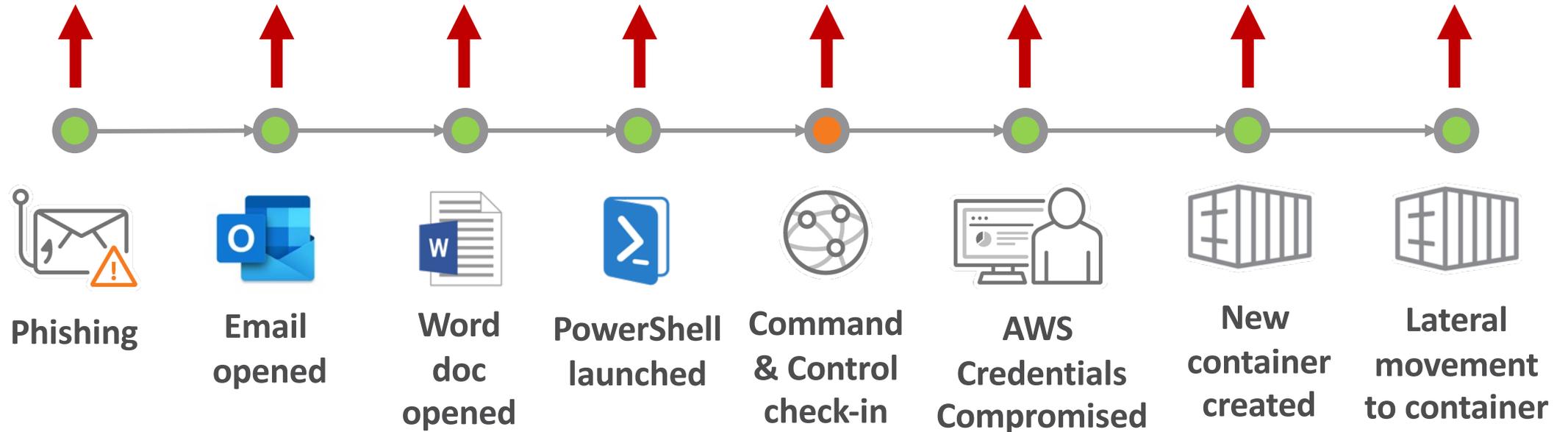


# SIEM (Security Information and Event Management)



Fewer, higher-fidelity alert that tells a story

## XDR (with cloud data lake collecting all activity)



# Q&A

40

Streaming Edition



Streaming Edition

[tiberio\\_molino@trendmicro.com](mailto:tiberio_molino@trendmicro.com)

Vieni a trovarci al nostro virtual desk!

41





# THE ART OF CYBERSECURITY

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