



Proactive Security
Starts Here

Trend Vision One™

Enterprise Cybersecurity Platform

Jesper Mikkelsen



**AI is reshaping the
threat landscape.
Being reactive isn't enough.**



Complex defense is **expensive**

Disjointed teams

Too many tools

Delayed response

AI risks

Alert overload

Data exposure risks

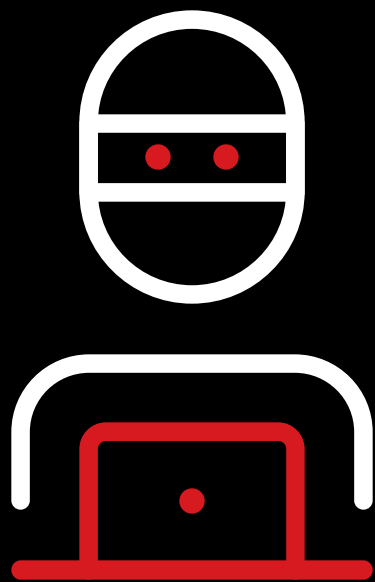


Attackers thrive on **complexity**



How can I move
What's the in the network?
easiest way in?

And **compromise** the
most valuable assets



TREND Vision OneTM

AI-Powered Enterprise
Cybersecurity Platform



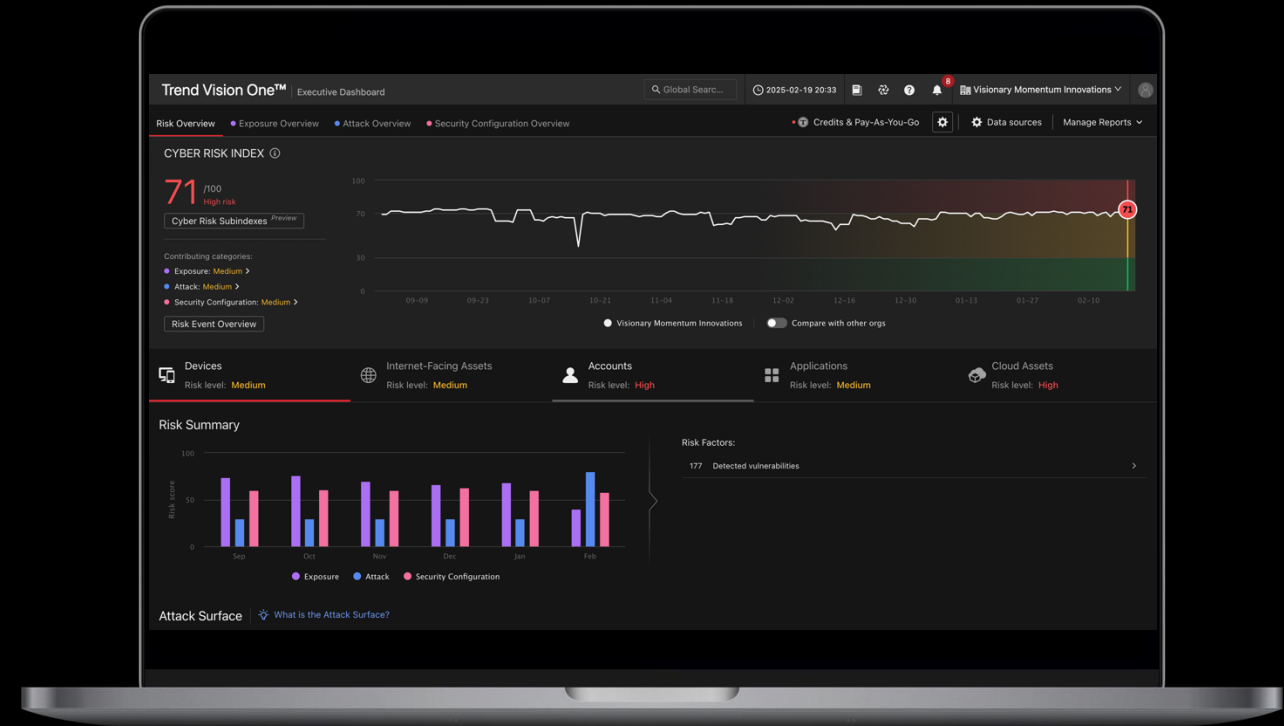
How can Trend Vision One help you?

65% Reduction in dwell time

99.6% Fewer alerts

\$1.3M Avg. savings from risk reduction

Source: Analyzing the Economic Benefits of Trend Vision One, ESG, Jan. 2024



Proactive security starts here

Visibility • Prioritization • Mitigation



VISIBILITY

Eliminate security
blind spots



Visibility

USING

Native Telemetry



Endpoints



Network



Cloud



Email



Identity



Server



Third-Party Sources

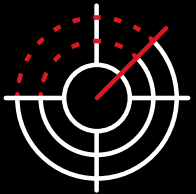


tenable



Visibility

TO



Continuously
discover known and
unknown assets



Centralize asset
inventory and
management



Map IT
infrastructure gaps



Assess risk across
your digital estate



Visibility



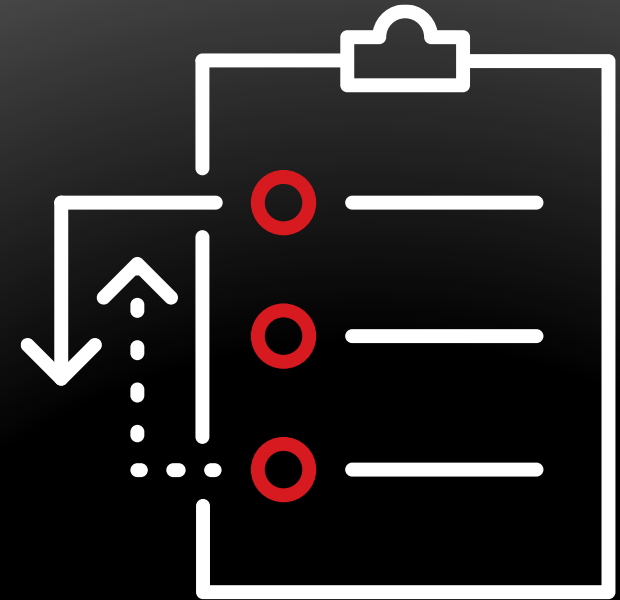
With Trend, we have been able to **eliminate silos and visibility gaps** [through] centralized visibility, analysis, and a deeper understanding of what is happening...

Head of New Technologies
European Government



PRIORITIZATION

Focus on what
matters most



Prioritization

USING

Trend Cybertron powered by:

Industry's first proactive cybersecurity AI

Wisdom

Decades of institutional knowledge

Context from 3,000+ technical engineers

Vertical expertise plus local data insights

Knowledge

1000+ patents, documentation, and logs

147B threats blocked in 2024

500k+ enterprises & 250M+ sensors in 175+ countries

Intelligence

450+ Trend researchers

14 global threat research centers

20+ year industry leading bug bounty program

90-120 days of advanced protection before vendor patches

60% of all global public vulnerability disclosures

Prioritization

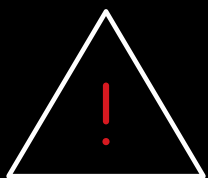
TO



Identify which issues need attention



Focus resources on critical risks



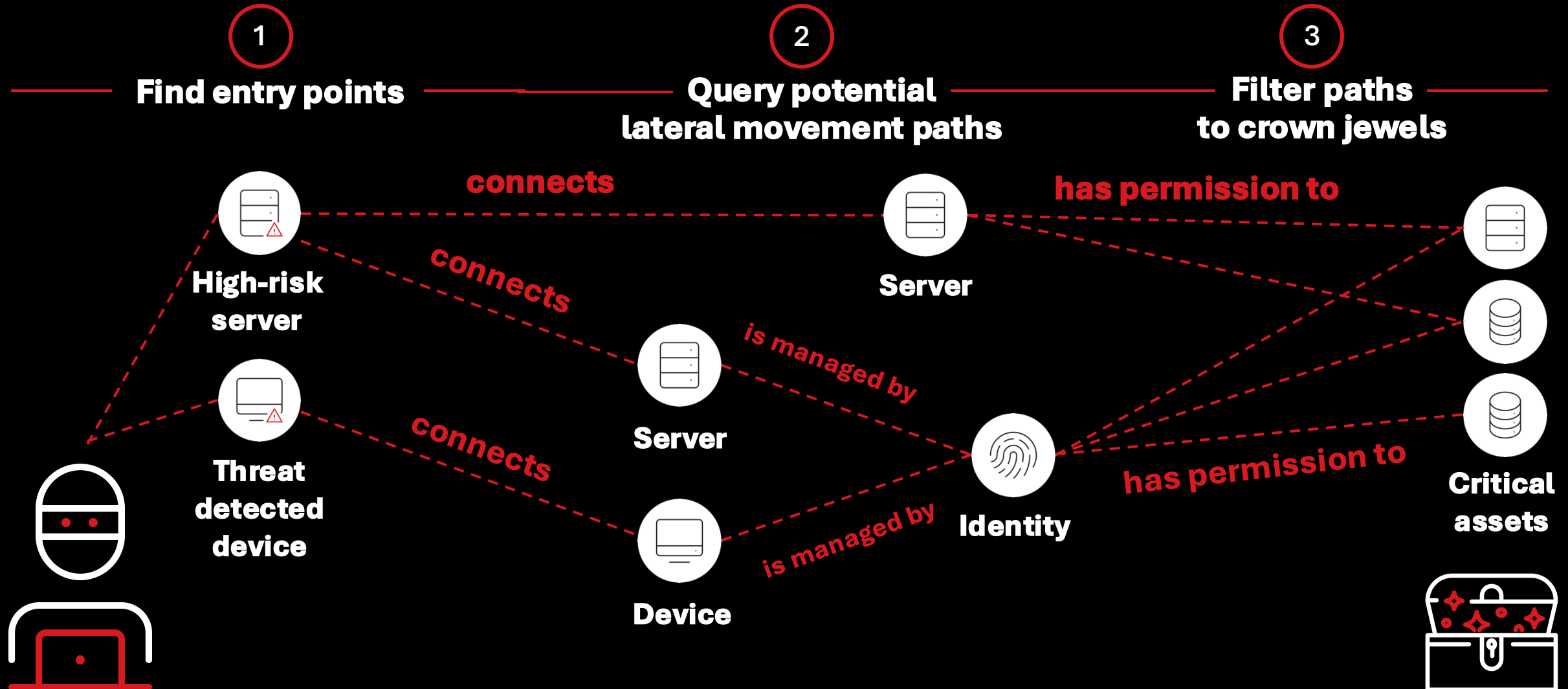
Rank issues based on business impact



Provide clear guidance



Predict from attacker's point of view



Prioritization



Trend Vision One is brilliant because it provides a single-pane-of-glass approach. It's refreshing — I can jump on and use security alerts at a glance and **focus on what requires the most attention.**

Jack Smith, IT Manager
ROC Oil Company Limited



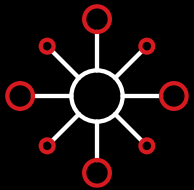
MITIGATION

Elevate security into
a strategic partner
for innovation



Mitigation

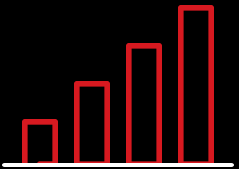
USING



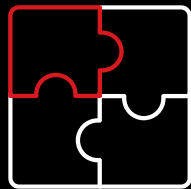
Contextual
awareness



Risk insights



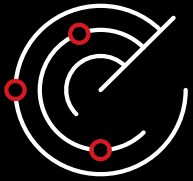
Predictive
analytics



Automation and
Integration

Mitigation

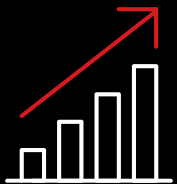
TO



Actively preempt threats



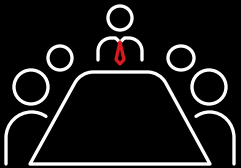
Prevent attacks before they happen



Reduce risk to accelerate business growth

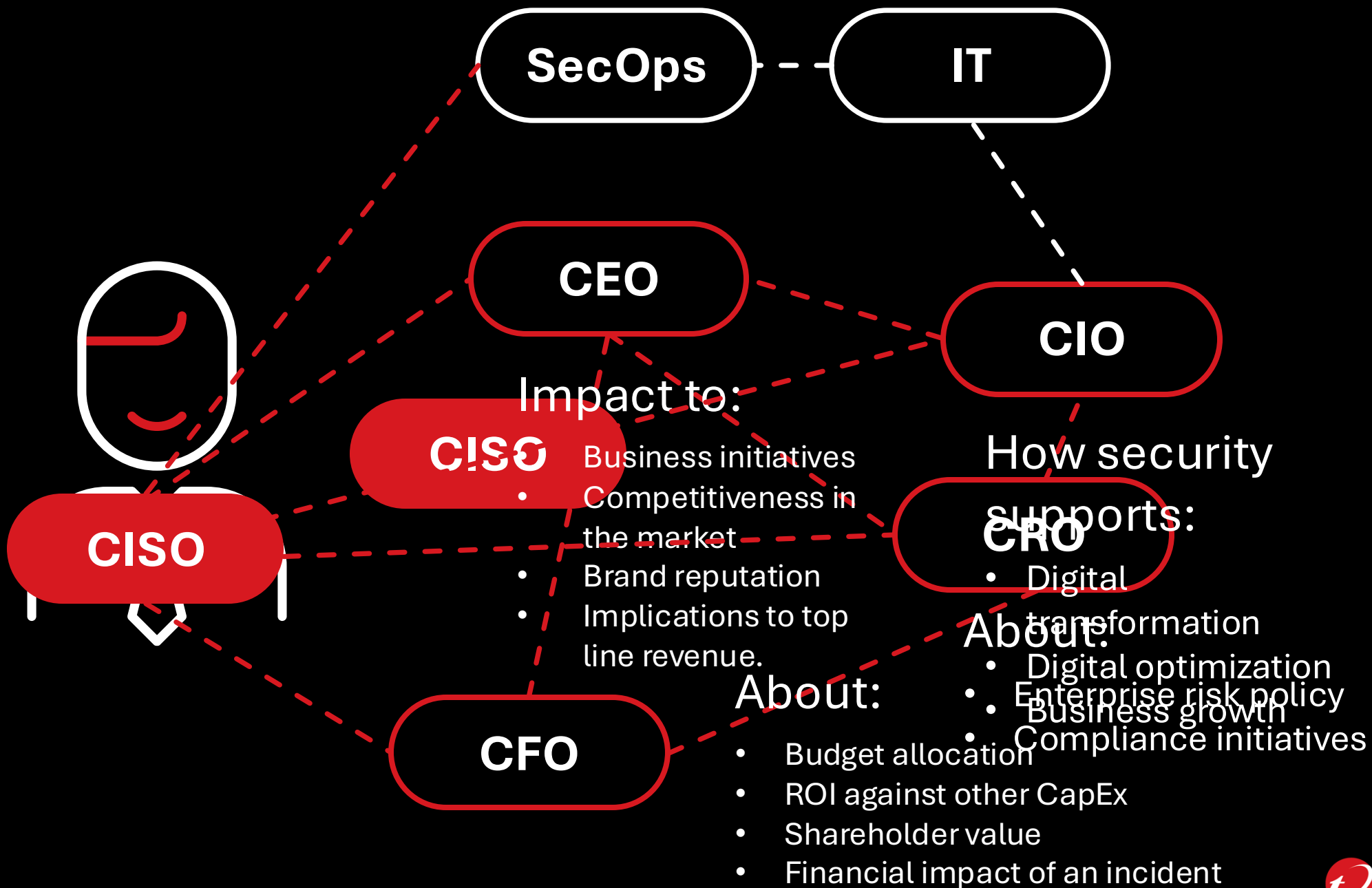


Optimize teams and security investments



Communicate among executive leadership





Mitigation

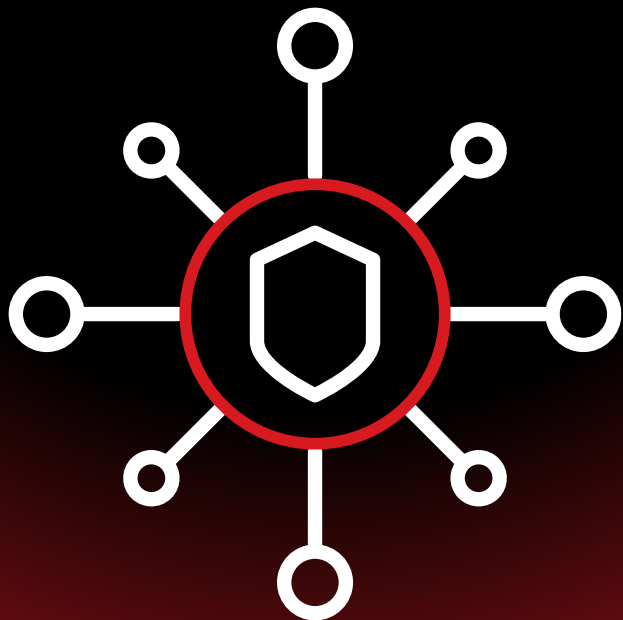


The Trend Vision One platform accelerates our business because it gives us the information we need to **take action before any threats even start.**

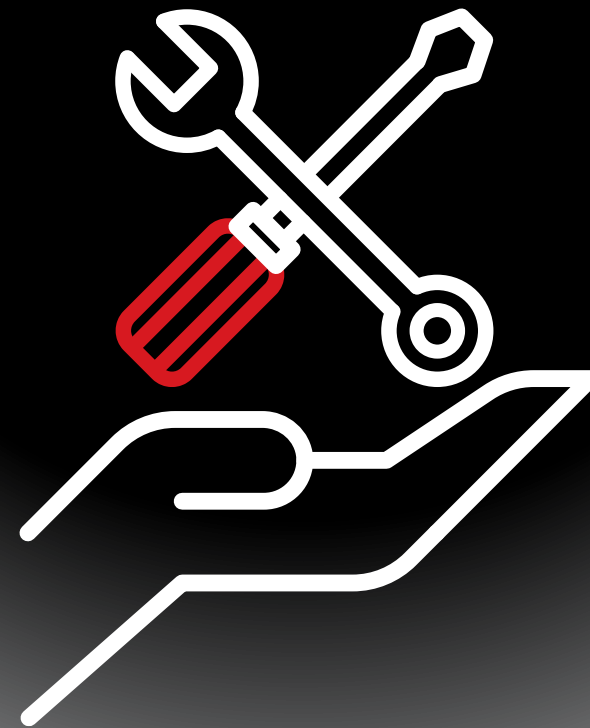
Cybersecurity Specialist
Leading Auto Parts Manufacturer



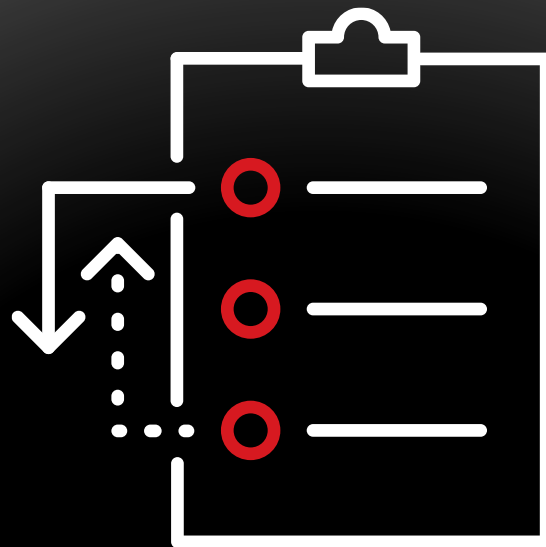
VISIBILITY



MITIGATION



PRIORITIZATION



VISIBILITY

ELIMINATE
SECURITY
BLIND SPOTS

FOCUS
ON WHAT
MATTERS MOST

MITIGATION

ELEVATE
SECURITY INTO A
STRATEGIC PARTNER
FOR INNOVATION

PRIORITIZATION

**Proactive security
starts here**



Proactive Security
Starts Here

Trend Vision One™ Cyber Risk Exposure Management



**Cyber risk is
business risk**

**Are you effectively
managing it?**



75%

of organizations
suffered at least one
ransomware attack
last year

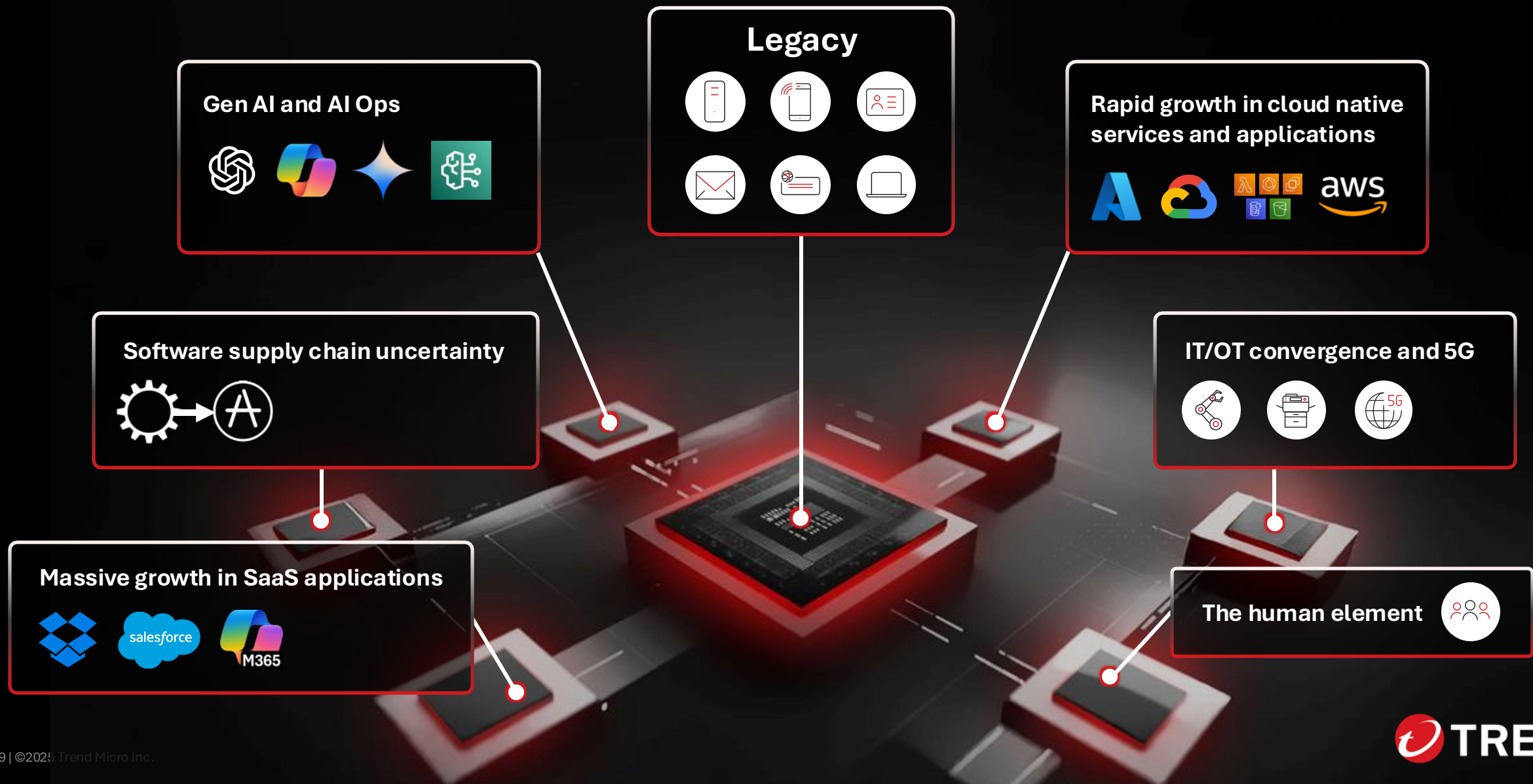
70%

of organizations
have been compromised
via an unknown, unmanaged,
or poorly managed
internet-facing asset

52%

of Trend Micro
IR incidents start
with phishing

Complexity and Scale of Attack Surface



→ "Do I have **complete visibility of risks** in my environment?"

→ "What steps should/could I take to **lessen chances of an attack**?"

→ "How can I **communicate risk effectively** to my board and internal stakeholders?"

→ "How do I make the **best use of my team, technology and time**?"

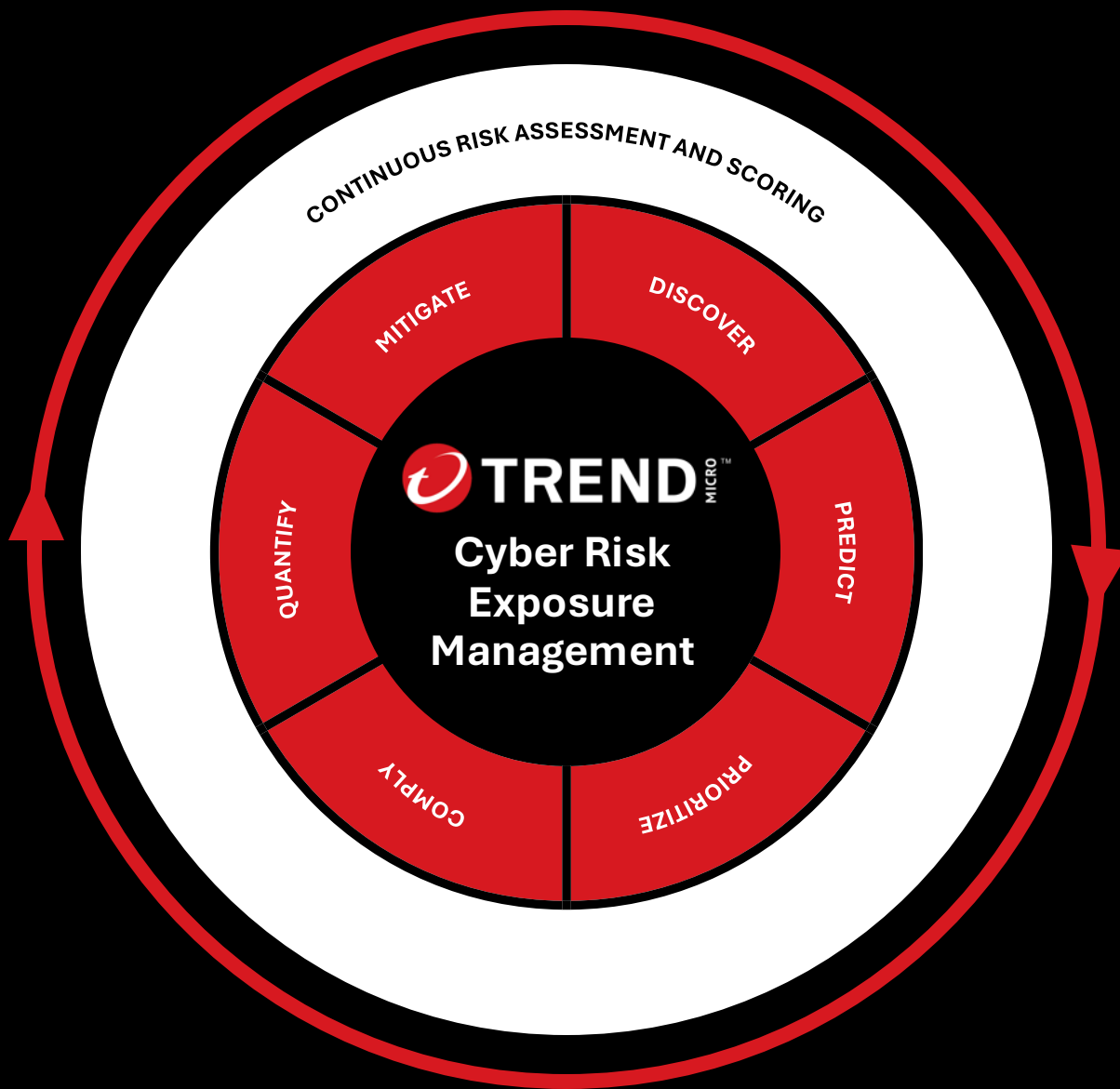
→ "**Are we compliant?** If not, how do we get and stay there?"



Cyber Risk Exposure Management (CREM)

- Unified experience for better understanding of your cyber risk posture
- Centralized visibility across identities, devices, network, cloud, APIs, and more
- Continuous risk assessment to prioritize and mitigate risks in real time
- Predict and neutralize threats before they have a chance to materialize
- Optimize compliance and security configuration with risk-based insights

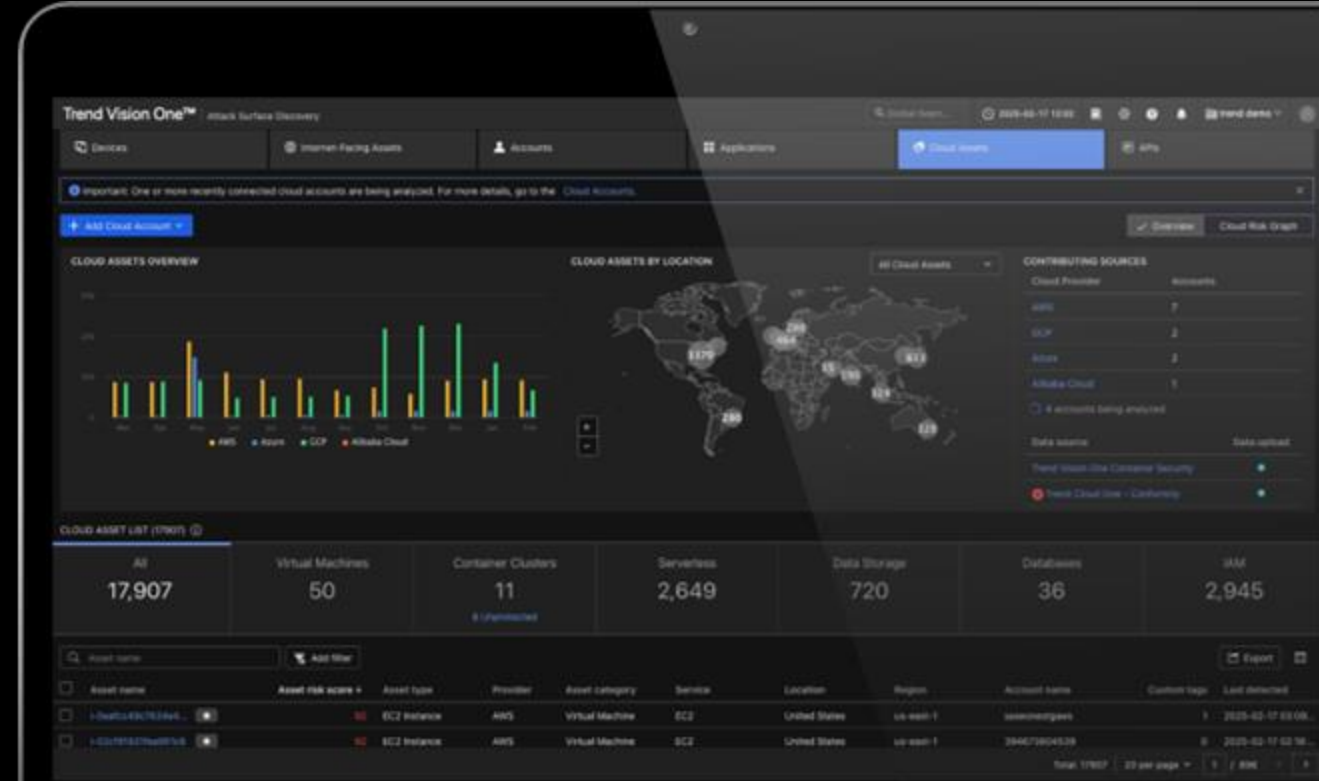
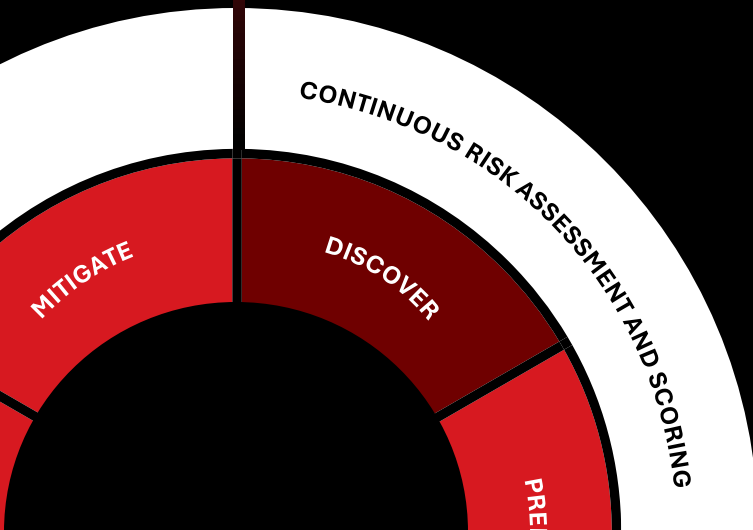




Let's get **proactive.**

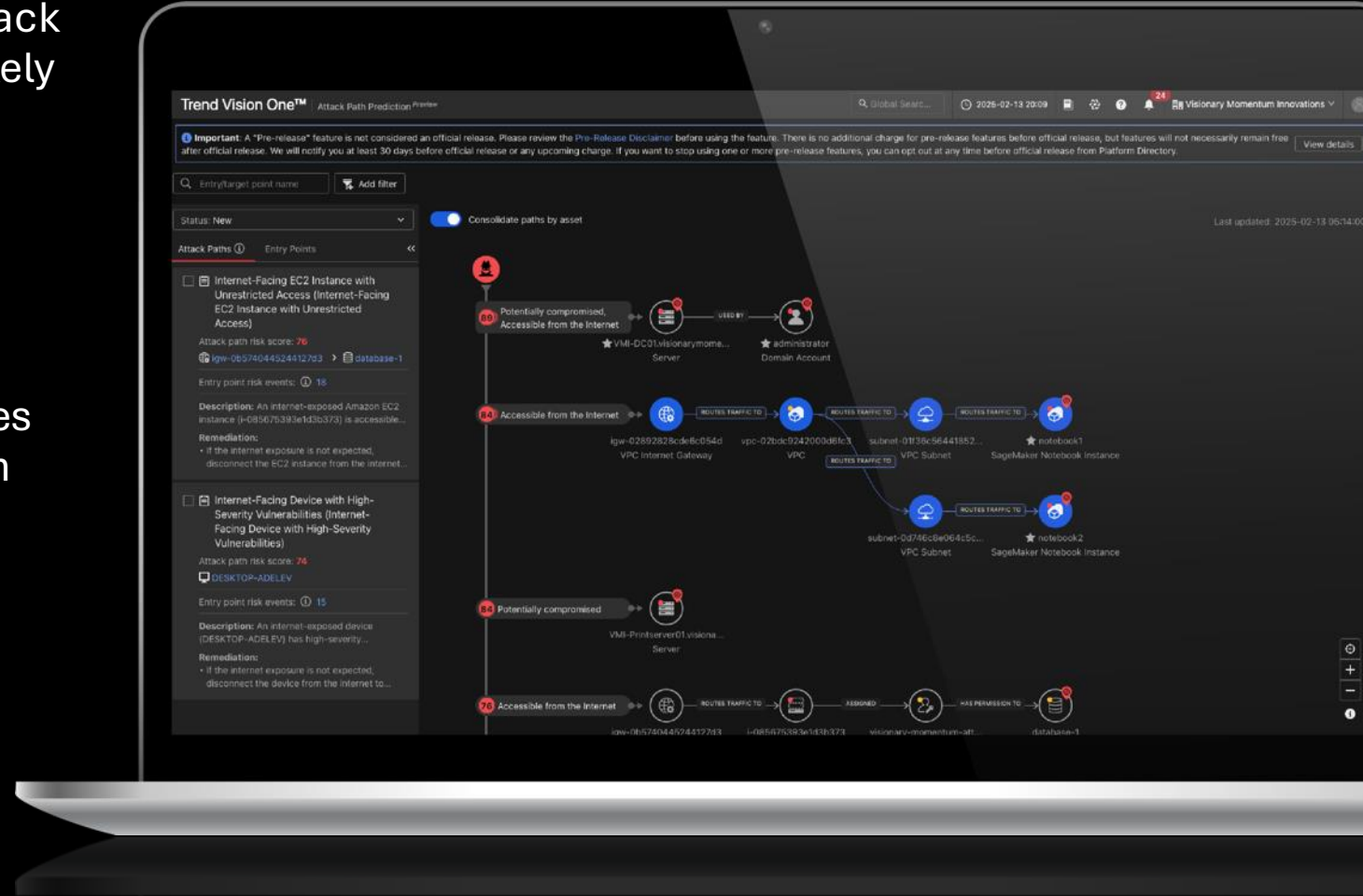
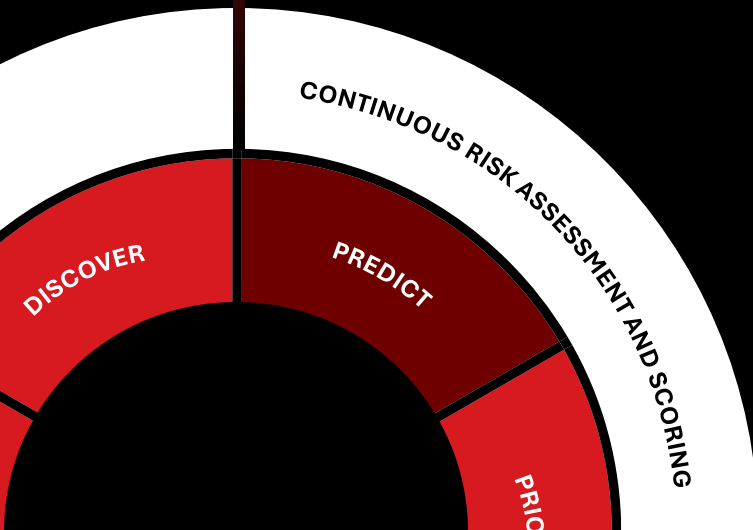
Discover

- Discover and inventory all assets internal, external and in the cloud
- Use native telemetry from Trend Micro and integrate third-party tools
- Leverage powerful risk-based vulnerability management
- See in-depth, AI-powered asset profiles



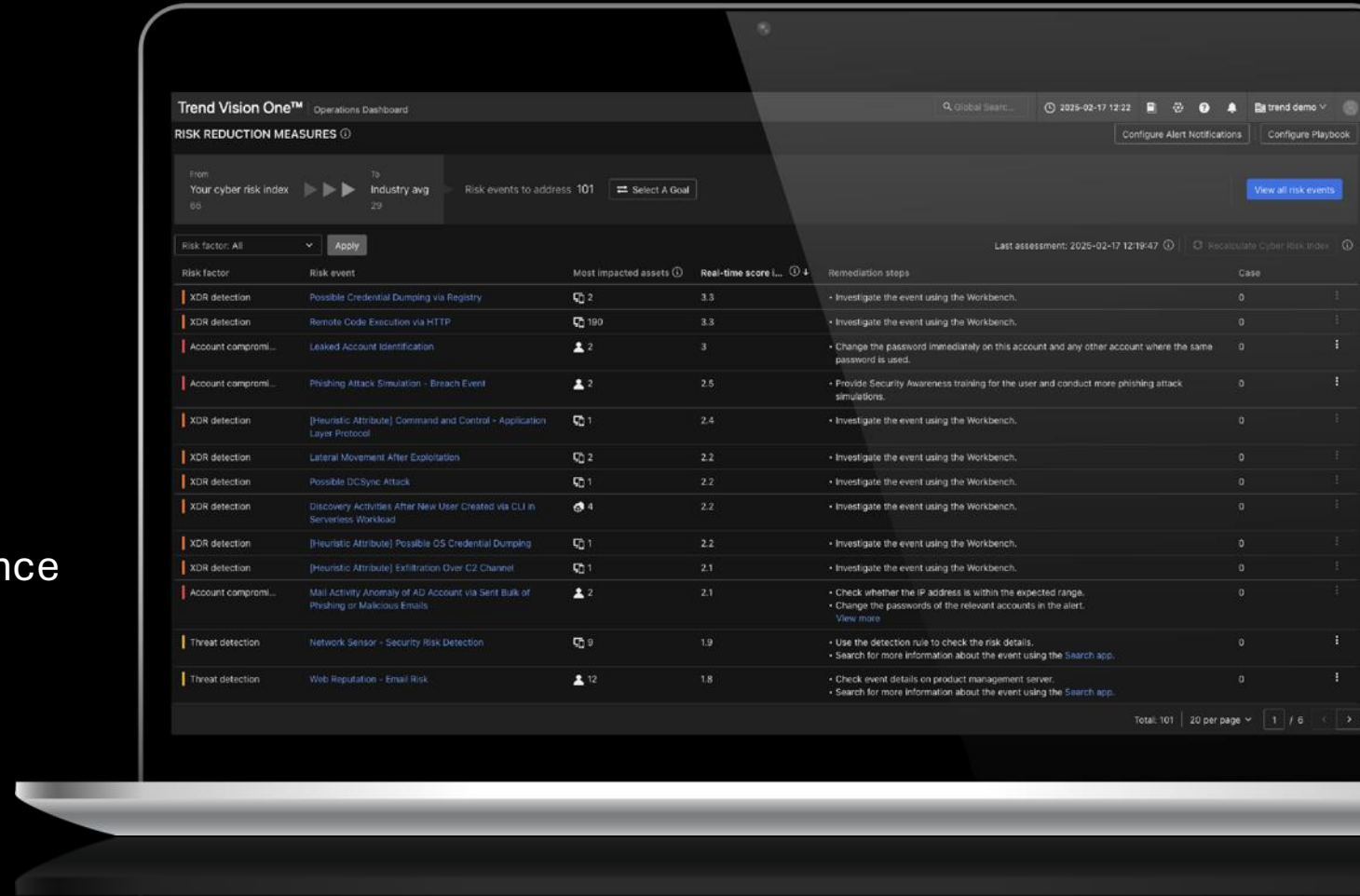
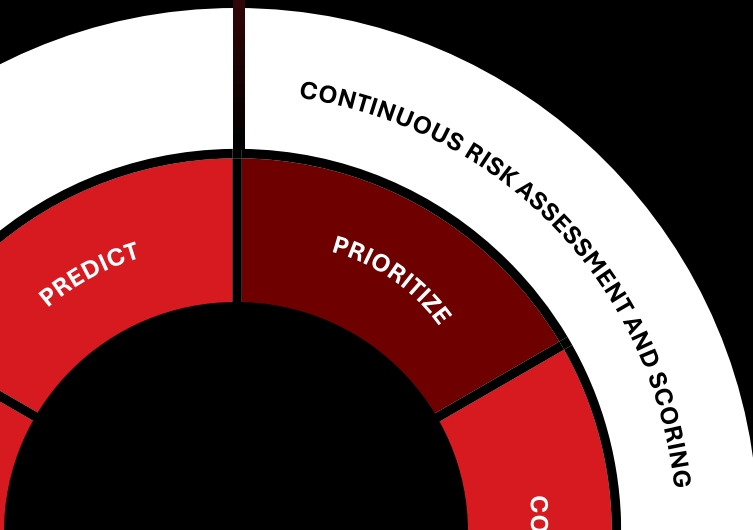
Predict

- Correlate discovered risks to map attack paths to critical assets and predict likely exploitation using Threat Intelligence
- Visualize attack paths to pinpoint choke points that could enable multiple attack vectors
- Deliver effective remediation strategies to prevent attacks before they happen



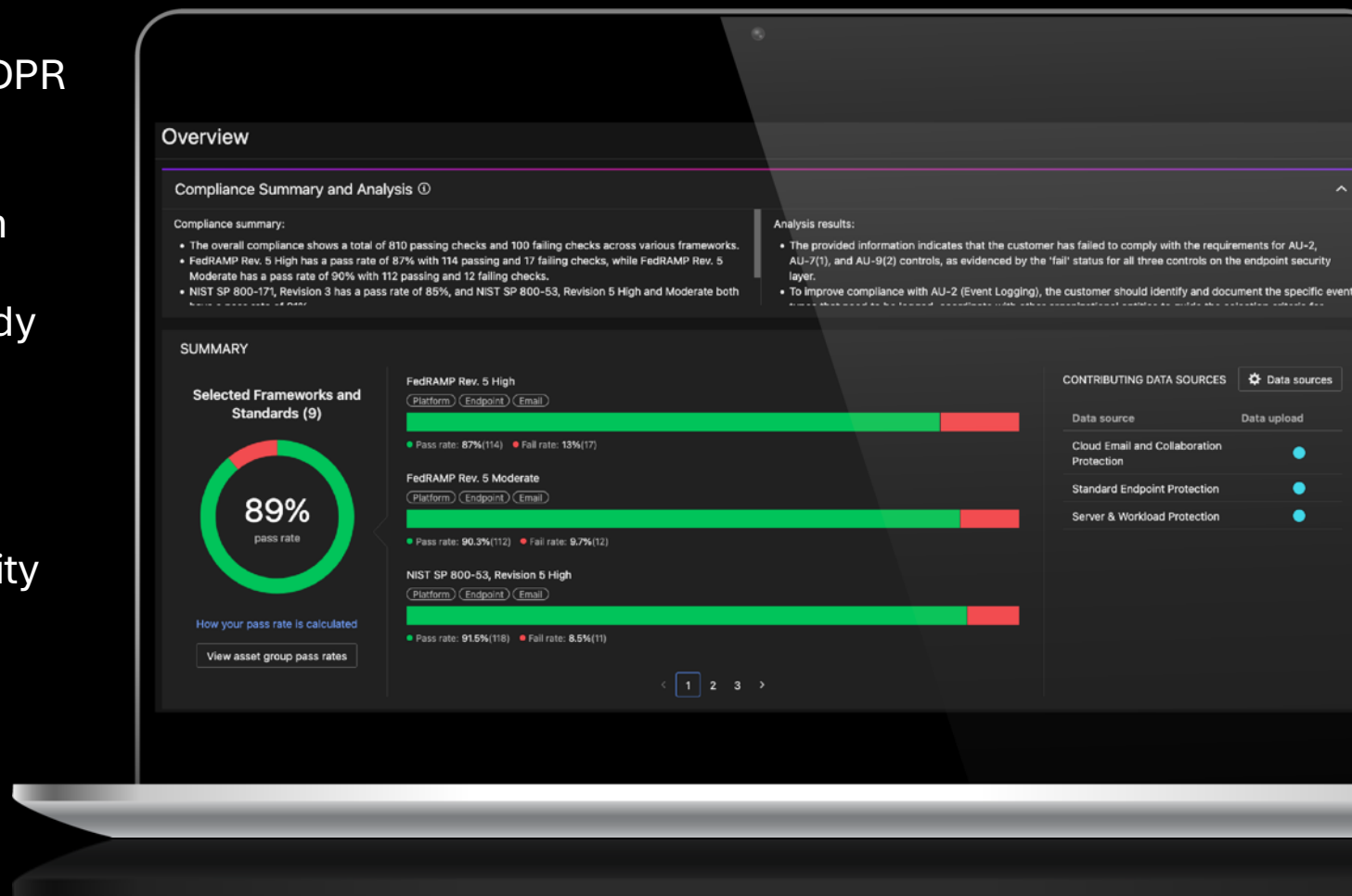
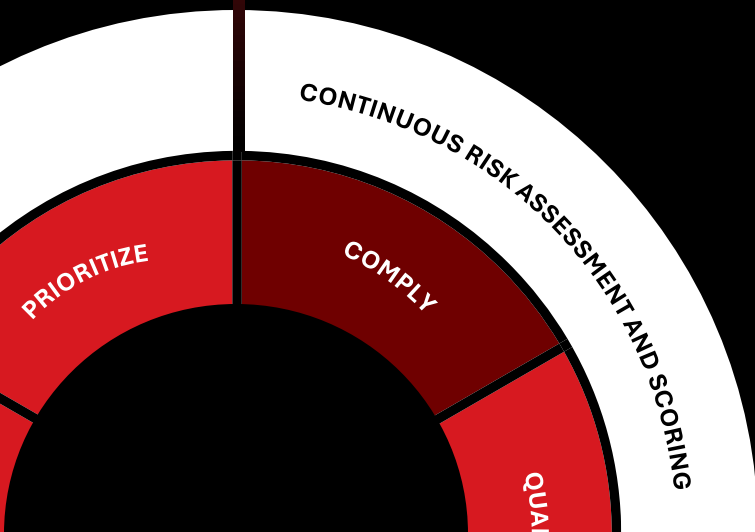
Prioritize

- Quickly identify high-impact risks to the organization
- Early threat indicators alert security teams before an attack or breach can materialize
- Prioritize CVEs with more context beyond CVSS scores
- Synthesize all risk factors to deliver intelligent custom remediation guidance



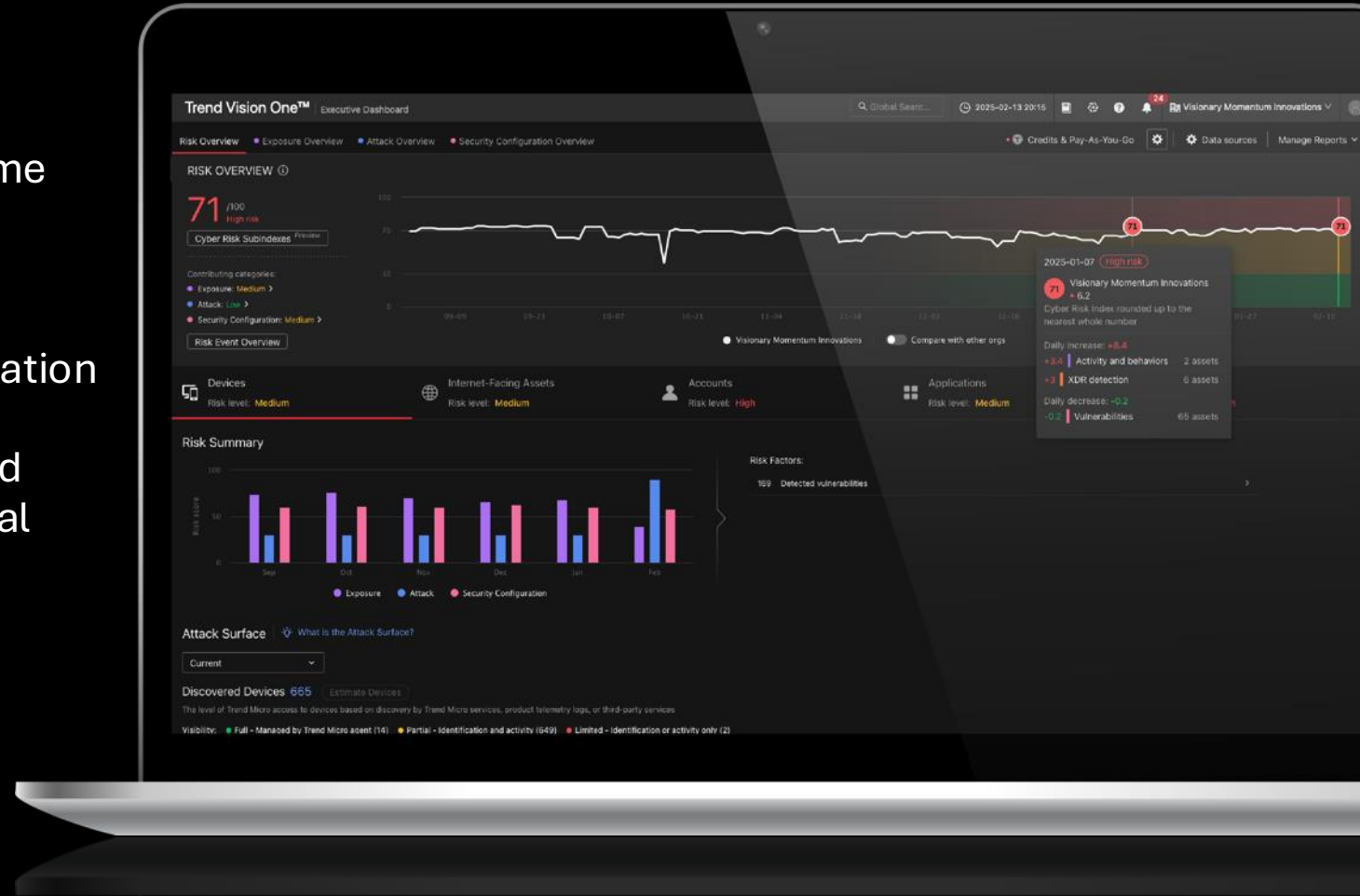
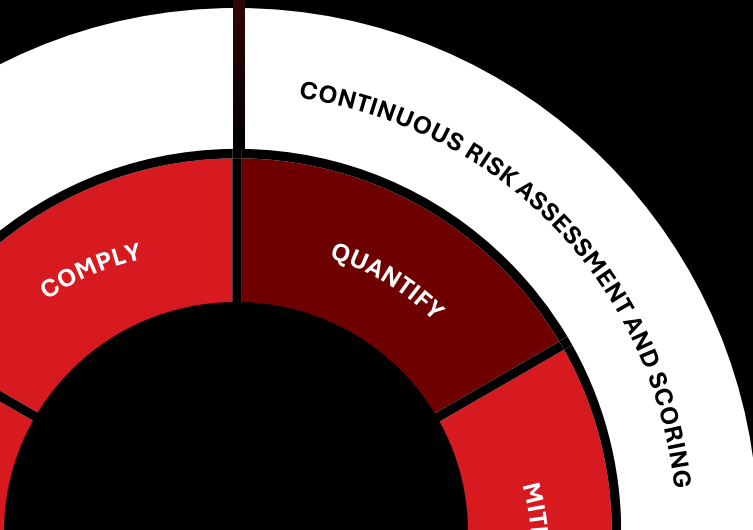
Comply

- Map compliance efforts to global standards like NIST, FedRAMP, and GDPR
- Automate compliance processes for a proactive approach to risk reduction
- Generate comprehensive auditor-ready reports instantly, drastically reducing manual effort
- Facilitate clear risk communication, prove due diligence, and reduce liability



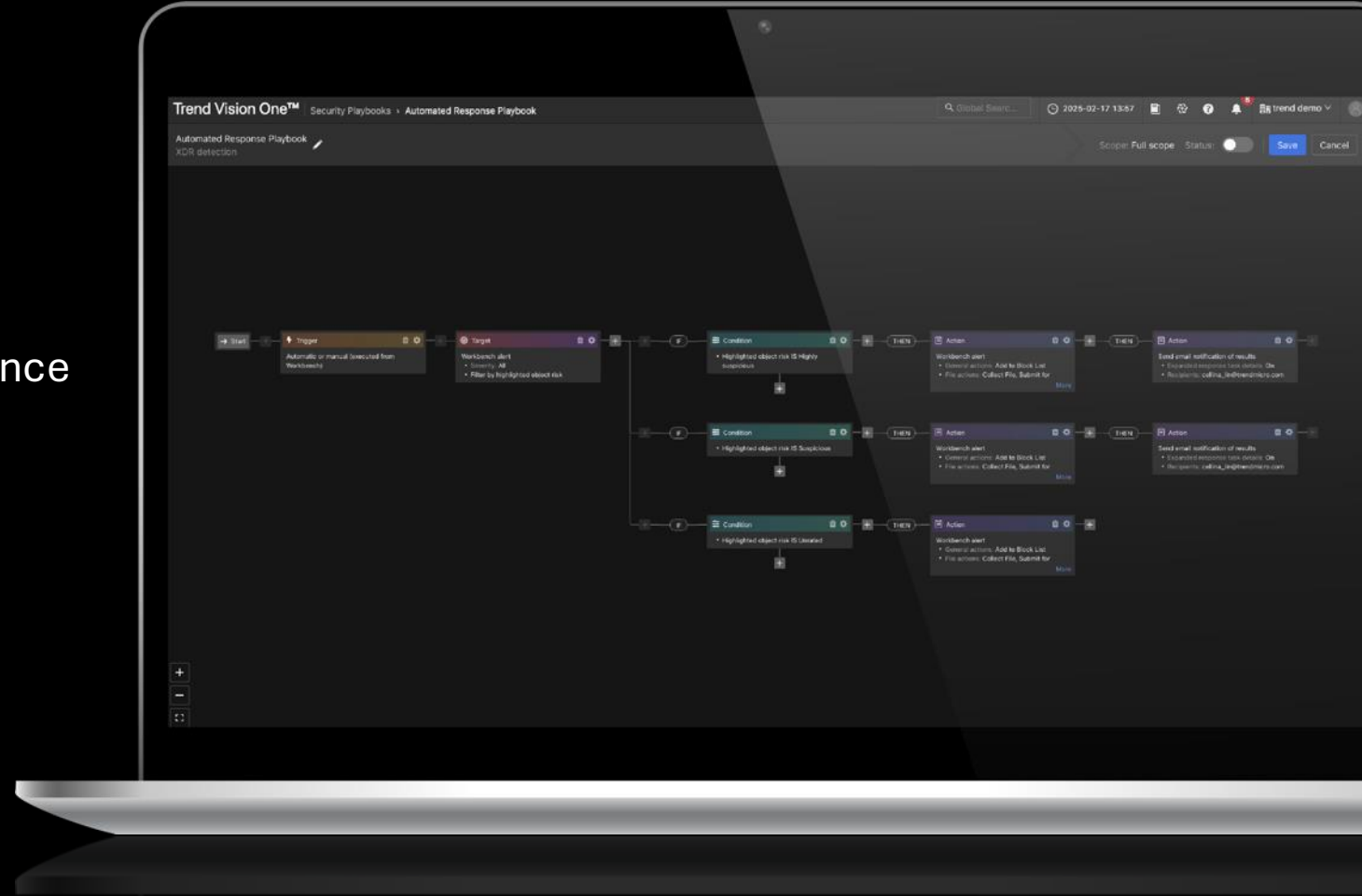
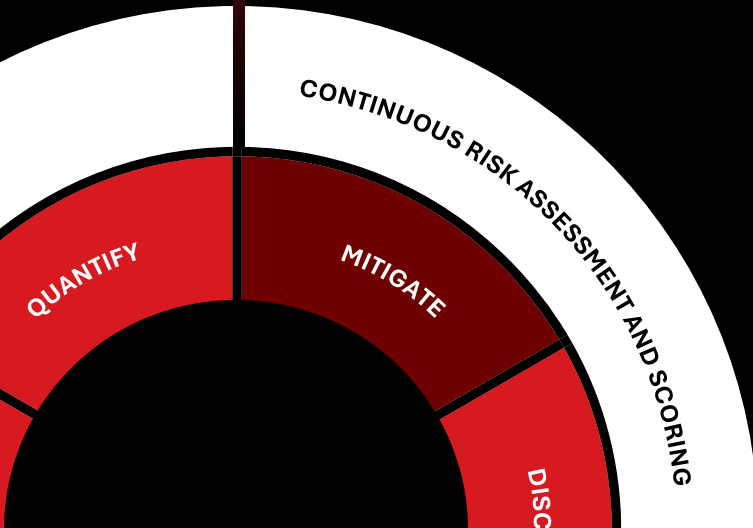
Quantify

- Understand the business impact of cyber threats and prioritize response
- Improve decision-making with real-time insights and situational awareness
- Enhance regulatory compliance with structured, defensible risk/loss estimation
- Communicate cyber risk exposure and security effectiveness to non-technical stakeholders



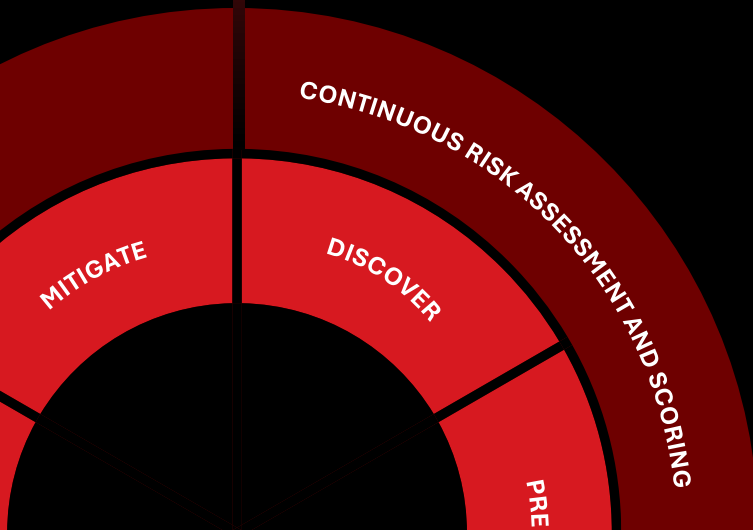
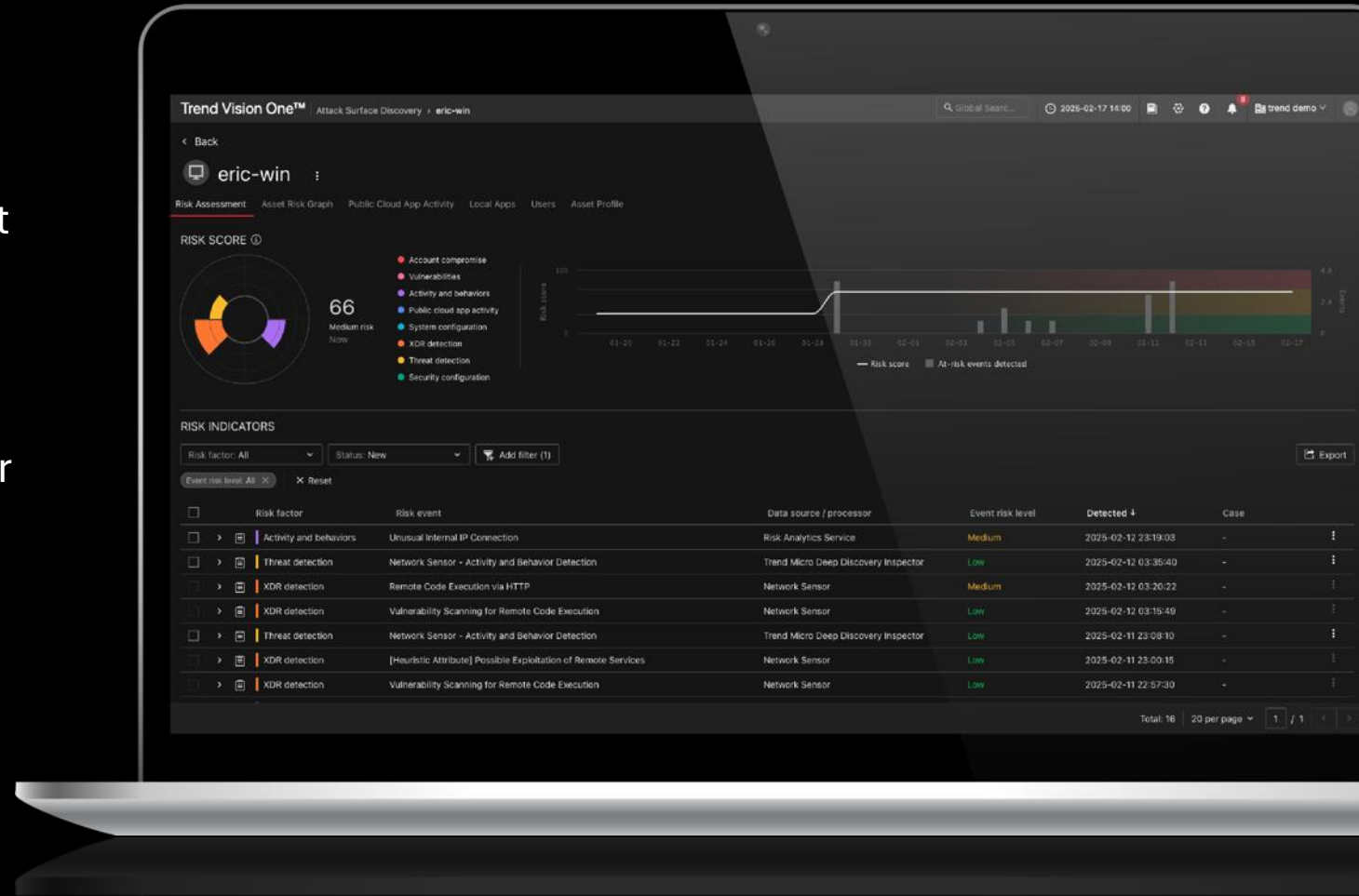
Mitigate

- Respond automatically to changes in risk posture
- Configure playbooks with bespoke response actions across multiple security controls
- Remediate with GenAI guided assistance

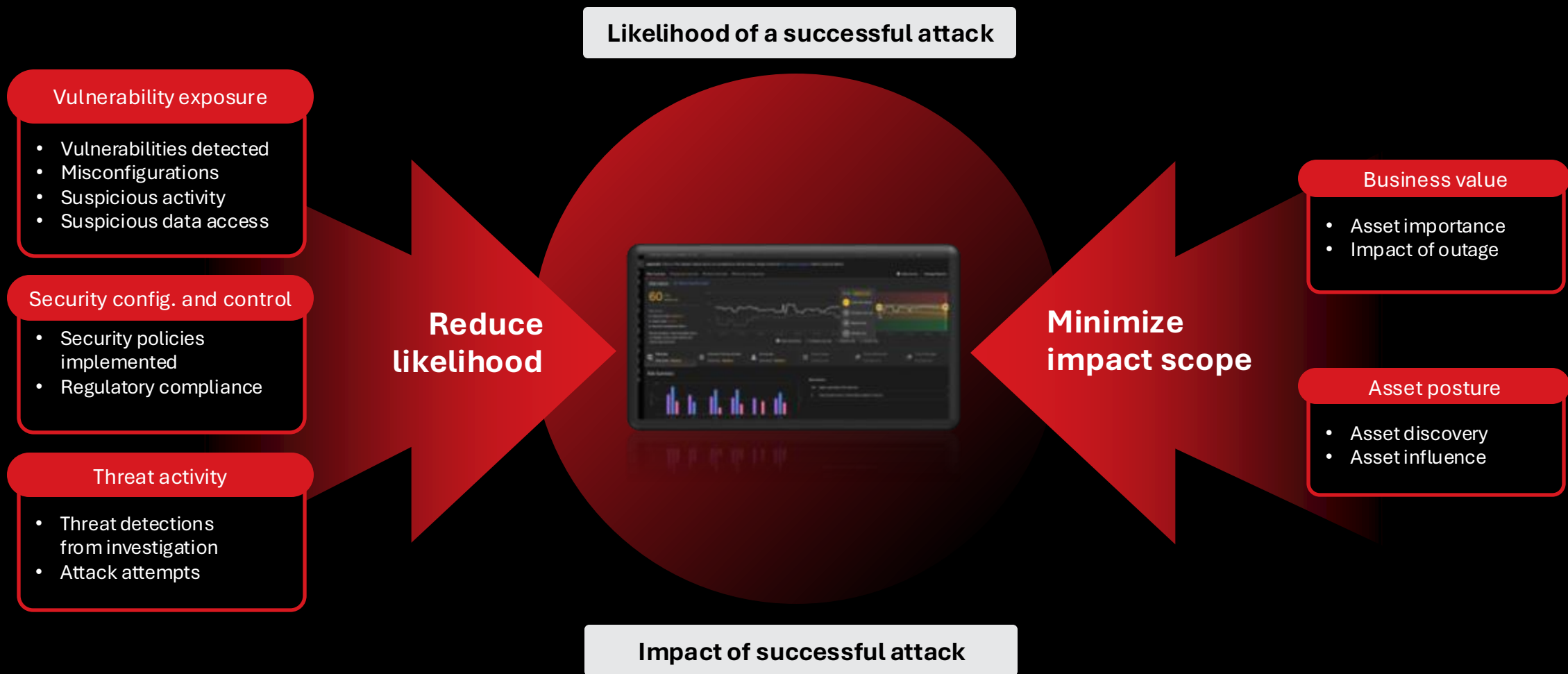


Continuous Risk Assessment and Scoring

- Dynamically assess risk in real-time and prioritize mitigation with per-asset scores
- Risk-based vulnerability management goes beyond just discovering vulnerabilities
- Benchmark the company-wide risk against peers of the same size, similar industry, or same region



Continuous Risk Assessment and Scoring



Based on NIST 800-30 and NIST 800-60

One Solution, One Risk Picture

Cyber Risk Exposure Management

Attack surface discovery

Attack surface management (ASM)

Cyber asset attack surface management (CAASM)

External attack surface management (EASM)

Risk assessment

Vulnerability risk management (VRM)

Compliance management

Security posture management

- Cloud (CSPM)
- Identity (ISPM)
- Data (DSPM)
- SaaS (SSPM)
- AI-SPM
- API-SPM

Cloud infrastructure entitlement management (CIEM)

Risk mitigation

Automation and orchestration of mitigation actions (SOAR capabilities)

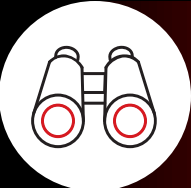
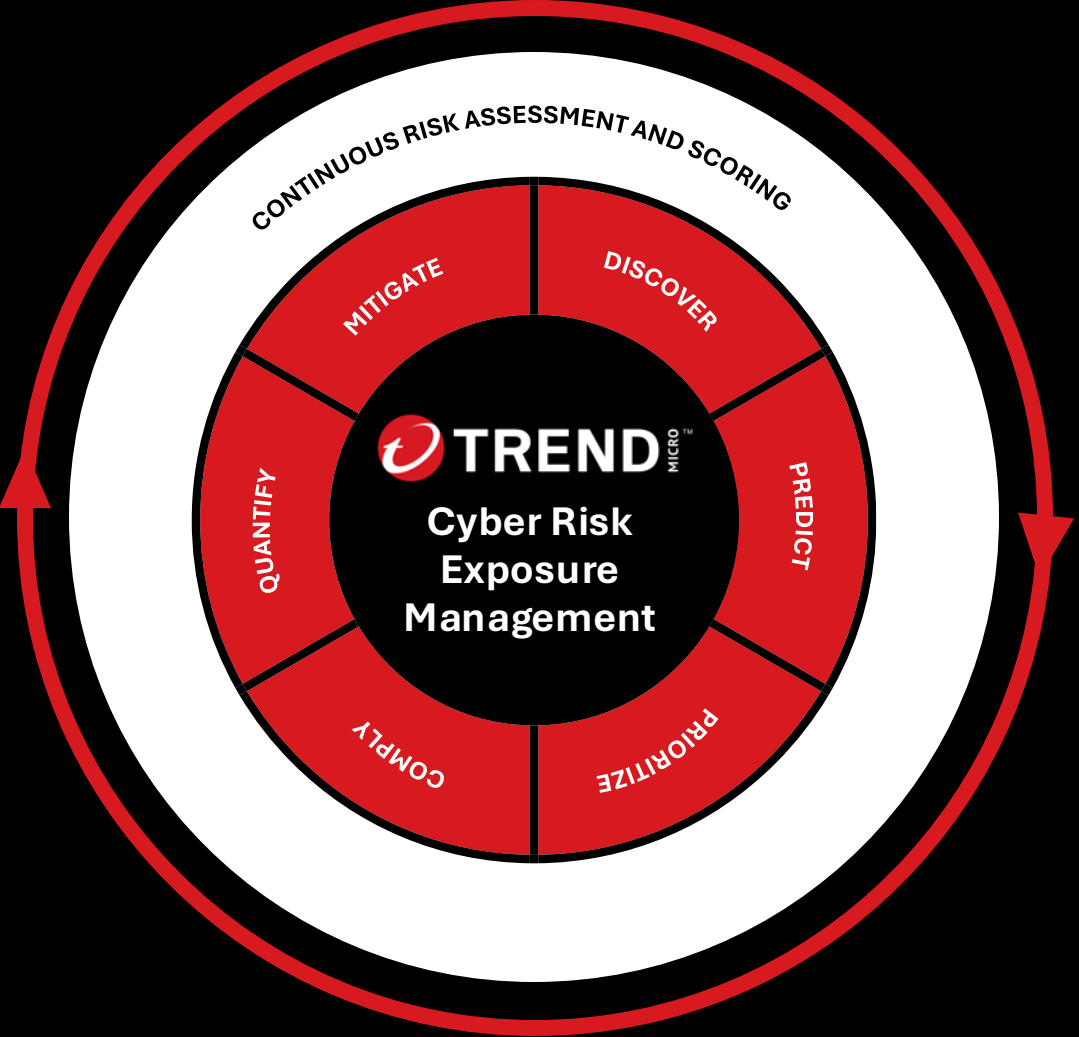
Streamlined workflows with prevention and protection solutions from Trend

Security Awareness

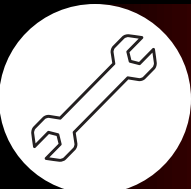
Extended detection and response (XDR) • Endpoint • Cloud • Email • Network • Identities • Third parties

Risk scoring, dashboards, and reporting

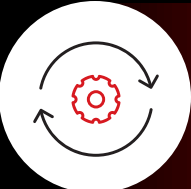
Unrivalled Cyber Risk Exposure Management



See everything, secure everything



Fix what matters first



Automate to stay ahead



One solution, one risk picture

Recognized in the Industry as a Leader

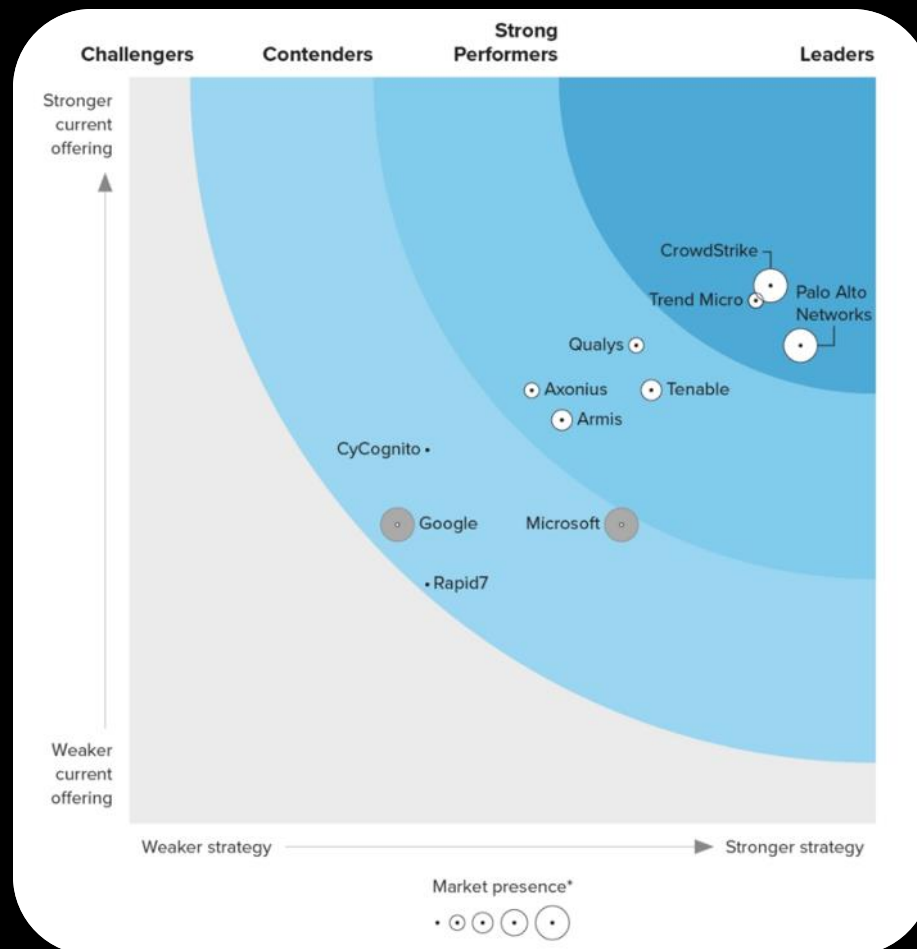
The Forrester Wave™: Attack Surface Management Solutions, Q3, 2024

FORRESTER®

WAVE
LEADER 2024

Attack Surface
Management Solutions

Forrester does not endorse any company, product, brand, or service included in its research publications and does not advise any person to select the products or services of any company or brand based on the ratings included in such publications. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change. For more information, read about Forrester's objectivity [here](#).





Trend not only offers us **unrivalled risk scoring, but also makes sense of telemetry better than anyone else**. This allows us to contextualize and prioritize risk to take rapid remedial action and build cyber-resilience. As a leader in our use of AI in health technology, **Trend puts us at the forefront of security as well, enabling us to reduce breach risk proactively** rather than being forced to react to incidents.



Zach Evans
CTO, Xsolis

Proactive security starts here





Proactive Security
Starts Here

Trend Vision One™ AI Security





Biggest Security Concerns Related to AI



**Deepfakes and
Next-Gen Phishing**

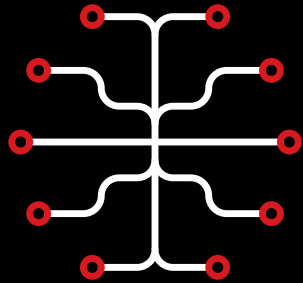
**Risks Caused by
AI Blind Spots**



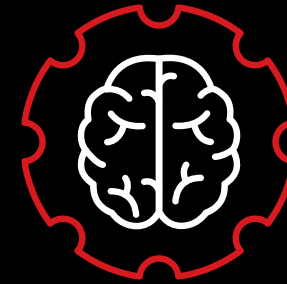
**Data Privacy and
Compliance
Issues**

Trend Vision One™

AI-Powered Enterprise Cybersecurity Platform



AI Innovation



Securing AI Initiatives

Balances your needs for **AI** innovation with securing those **AI** initiatives

Trend Vision One AI Solution Strategy

AI for Security

enhance your cybersecurity efforts and transform security operations with AI

Security for AI

secure your AI journey and defend against AI-related threats and attacks

AI Ecosystem

Threat and Attack Intelligence

Responsible AI



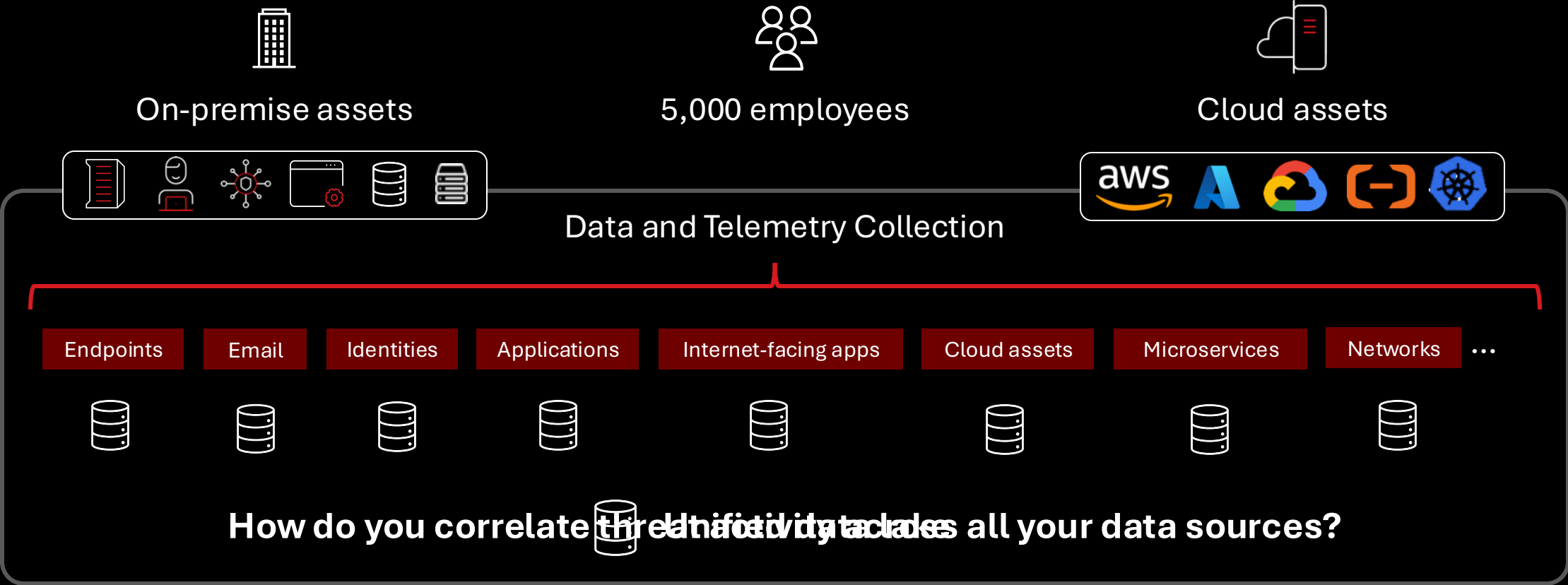
AI-Powered Enterprise Cybersecurity
Platform



Trend Cybertron

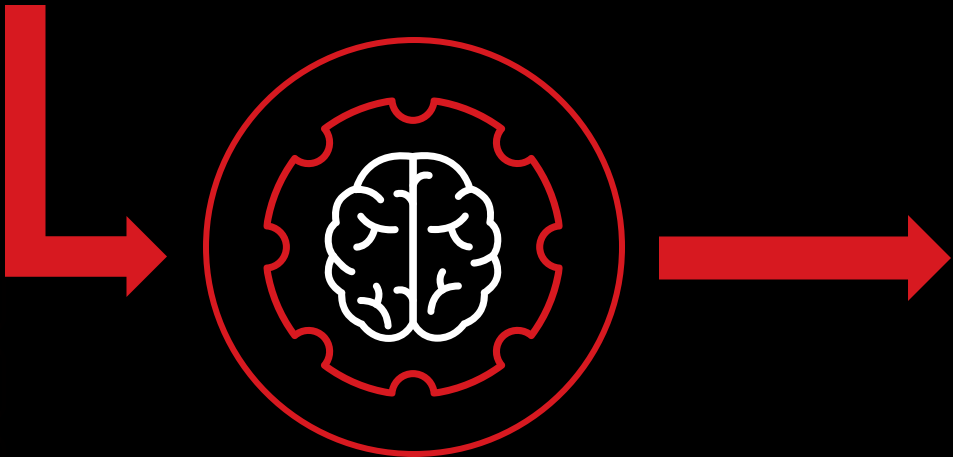
The industry's first **proactive cybersecurity AI**. Within Trend Vision One, Trend Cybertron is a collection of LLM models, datasets, and AI an agent featuring a fine-tuned cybersecurity LLM.

AI for Security - Comprehensive Proactive Protection



AI for Security - Comprehensive Proactive Protection

- Endpoints
- Email
- Identities
- Applications
- Internet Facing Apps
- Cloud Assets
- Microservices
- Networks

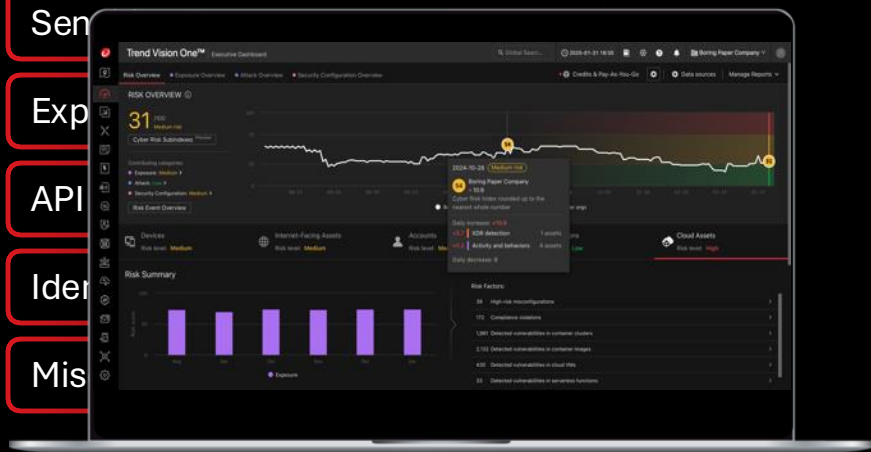


Trend Cybertron

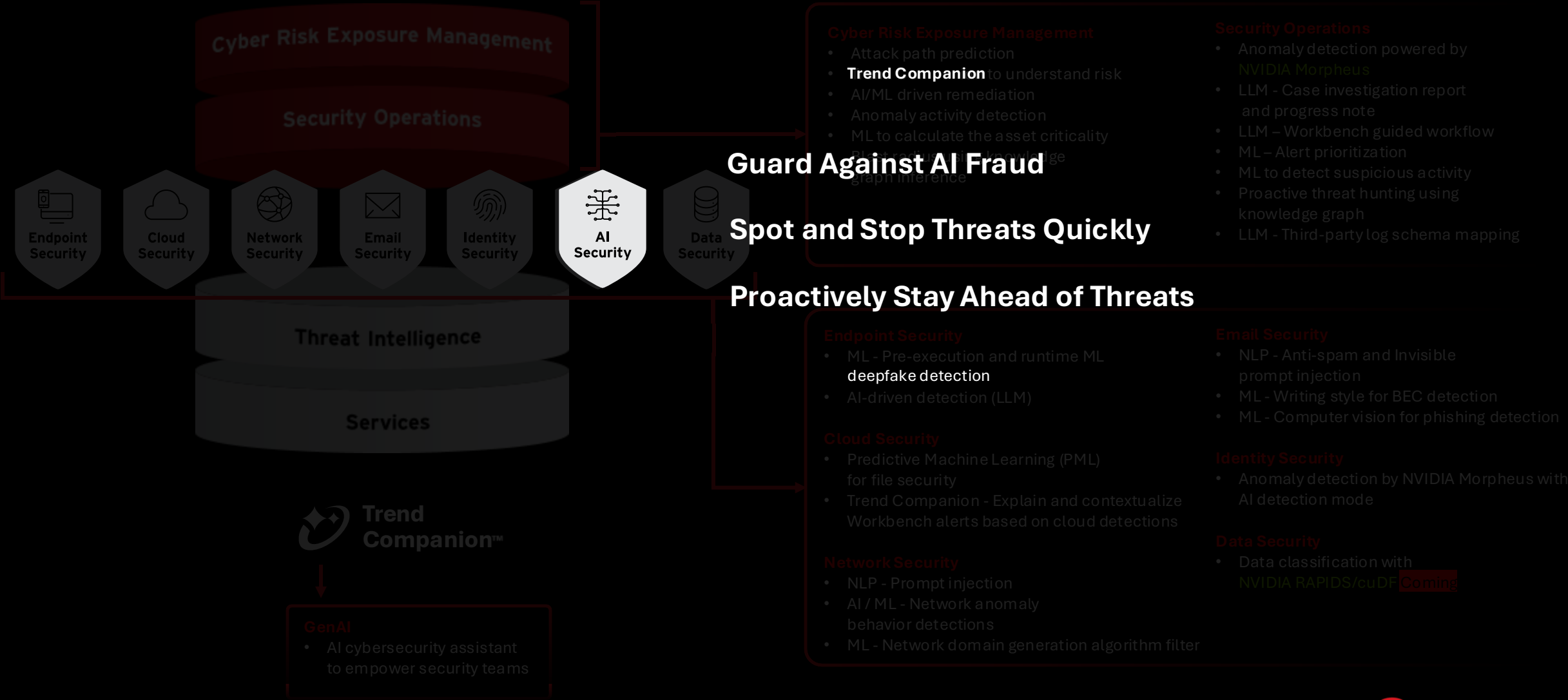
Detect and address security issues, analyze risks, prioritize threats, predict attack paths, and provide remediation

Unified data lake

- Vulnerability
 - Exploitability
 - Exposure & Attack Contextualize Threats
 - Excessive Permissions
 - BEC Attacks
- Trend Vision One** platform processes all risk information



Trend Cybertron – AI Powering Trend Vision One Solutions



Trend Vision One AI Solution Strategy

AI for Security

enhance your cybersecurity efforts and transform security operations with AI

Security for AI

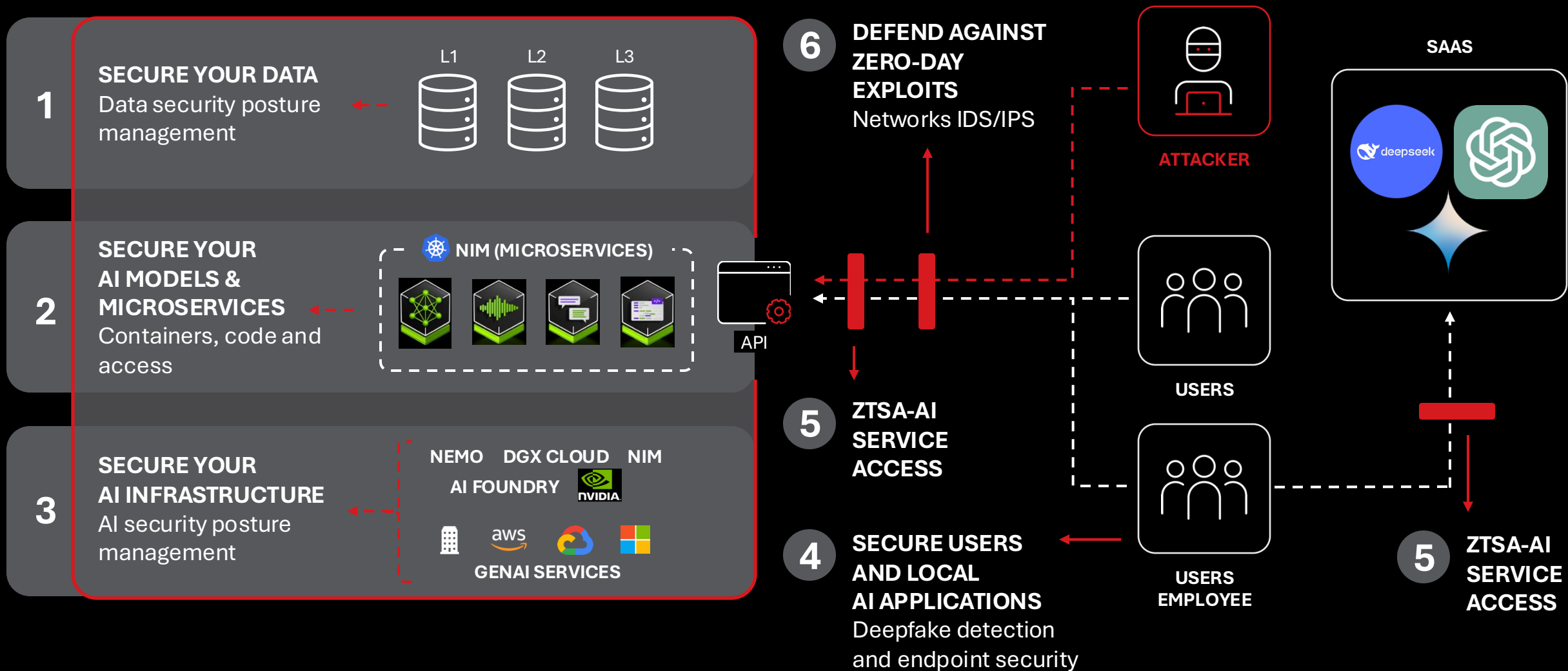
secure your AI journey and defend against AI-related threats and attacks

AI Ecosystem







Threat and Attack Intelligence

Responsible AI








Customer Use Case – Securing Your AI Stack



Security for AI • End-to-End Protection

		SECURITY CHALLENGES	SECURITY CONTROLS	TREND VISION ONE
Data		Sensitive information blind spots	Data Security	Data Security posture management
Models		Model poisoning and improper model usage	Implement guardrails for AI API's request/prompt (inbound) & responses (outbound)	ZTSA AI Service Access
Microservices		Vulnerabilities in AI supply chains and microservices architecture	Security validation on CI/CD pipeline and implement container controls	Code security Container security
Infrastructure		Security risks in AI model deployment and resource exhaustion attacks	Infrastructure posture management	AI-SPM API Security AI-DR
Network		Exploiting vulnerabilities in AI infrastructure and hybrid cloud environments	Network Security	Network IDS/IPS TippingPoint
Users		Insecure design and mismanagement leading to sensitive data exposure by AI	AI application access control and protect local AI application configurations	ZTSA AI Service Access V1ES - Deepfake detection AI app guard

Security for AI • End-to-End Protection

		SECURITY CHALLENGES	SECURITY CONTROLS	TREND VISION ONE
Data		Sensitive information blind spots	Data Security	 <p>Trend Vision One AI-Powered Enterprise Cybersecurity Platform</p>
Models		Model poisoning and improper model usage	Implement guardrails for AI API's request/prompt (inbound) & responses (outbound)	
Microservices		Vulnerabilities in AI supply chains and microservices architecture	Security validation on CI/CD pipeline and implement container controls	
Infrastructure		Security risks in AI model deployment and resource exhaustion attacks	Infrastructure posture management	
Network		Exploiting vulnerabilities in AI infrastructure and hybrid cloud environments	Network Security	
Users		Insecure design and mismanagement leading to sensitive data exposure by AI	AI application access control and protect local AI application configurations	

Trend Micro in AI Standards and Policies

AI Standards



AI Policy Development



AI Alliance





The evolution of AI in the Trend platform is unique as it calculates our constantly changing risk profile. **This cyber brain has made it possible to be more proactive than reactive with our entire security strategy.**



**South London
and Maudsley**
NHS Foundation Trust

Stuart MacLellan

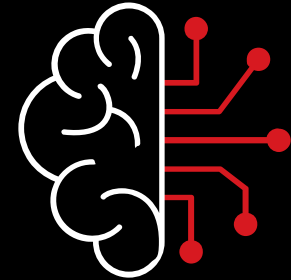
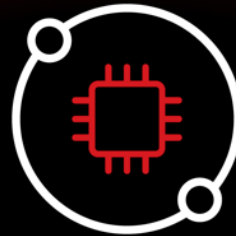
CTO, South London and Maudsley NHS Foundation Trust

AI Security for AI Innovation



**AI Security
Trailblazers**

**Proactive Security
for Your AI Stacks**



**Trusted
Intelligence
Behind Our AI**

**Proactive security
starts here**



Trend Research

Platform Marketing







ANTICIPATE

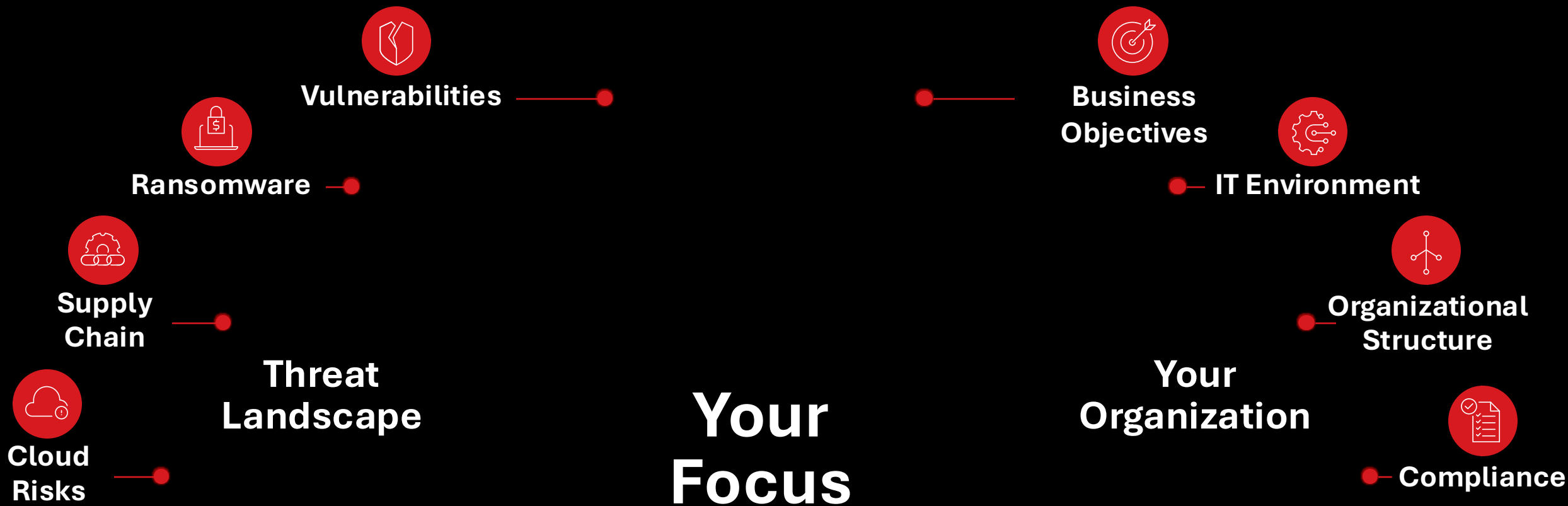
Proactive security starts with foresight



BLINDSPOT

Your risk is not knowing before the attackers

“Operation Anywhere”



Pivot and shift tried-and-true
attacks in surface



BACKED BY
**PASSIONATE
THREAT
EXPERTS**

TAKE THE LEAD
**VULNERABILITY
DISCLOSURE
AND THREAT
HUNTING**

INTEGRATE
**PROACTIVE
SOLUTIONS**



Cybersecurity : A 360 View *Past, Present, Future*

Cyber Risk Exposure Management



Targeted Attacks



Threats



Cloud



IoT and OT



AI and ML

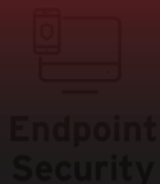


Cybercriminal Undergrounds



Future Threat Landscapes

Trend
Research



Endpoint Security



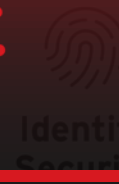
Cloud Security



Network Security



Email Security



Identity Security



AI Security



Data Security

Threat intelligence and research for consumers, businesses, and governments

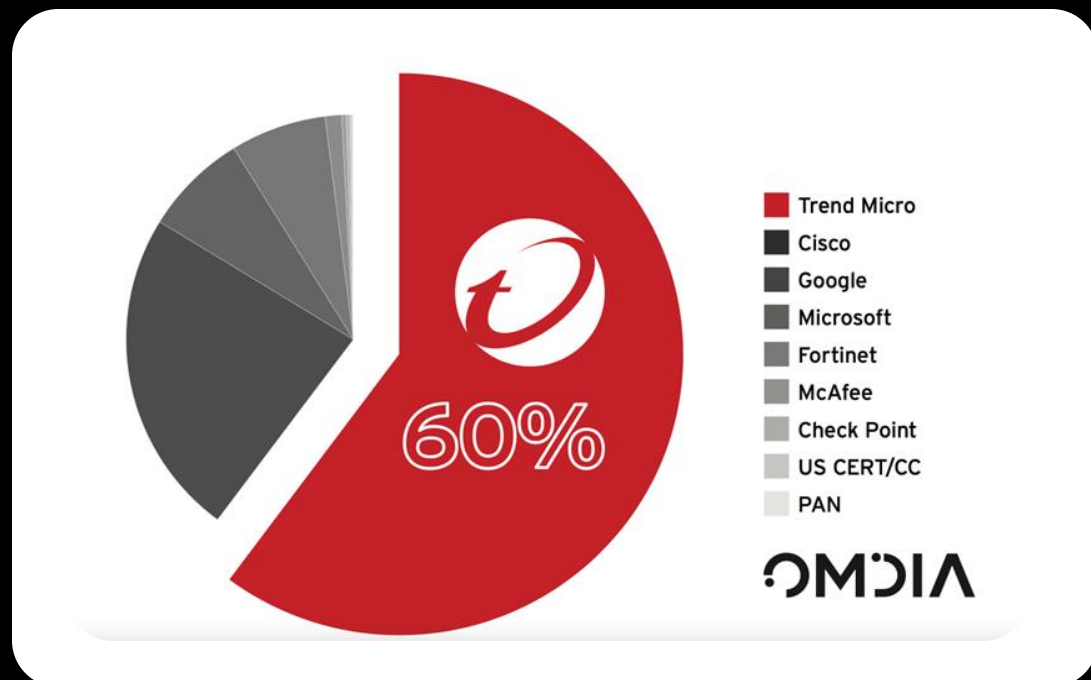
Trend Micro core technology and Trend Vision One™ AI-powered enterprise cybersecurity platform

Public/private partnerships (e.g. global enforcement)

Services



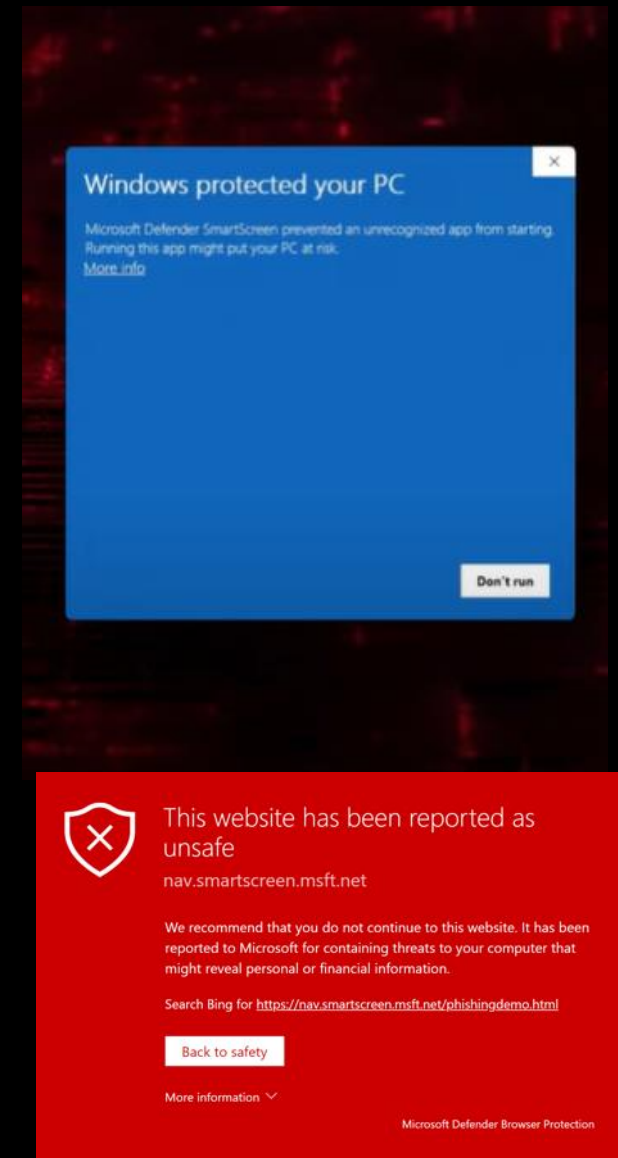
Securing a safer connected world



Source : OMDIA Vulnerability Report

OMDIA REPORT:
Trend disclosed
60%
of vulnerabilities

The Trend ZDI team recently discovered CVE-2024-21412 and alerted Microsoft of a Windows Defender SmartScreen bypass used in a zero-day attack by the advanced persistent threat (APT) group Water Hydra.



Turning attack knowledge into powerful enterprise defense

- Adversarial AI allows us to identify and mitigate vulnerabilities
- Understand how AI is weaponized, such as exposed containers
- New criminal LLMs, criminal services

Silent Sabotage: Weaponizing AI Models in Exposed Containers

How can misconfigurations help threat actors abuse AI to launch hard-to-detect attacks with massive impact? We reveal how AI models stored in exposed container registries could be tampered with—and how organizations can protect their systems.

December 04, 2024

Trend Vision One™ Workbench - WB-9002-20230627-00063

Summary

Possible Vulnerable LOG4J for CVE-2021-44228 File Compromise - BETA Only

This incident means an application vulnerable to CVE-2021-44228 in the Log4j library was exploited and malware was observed on the target. For BETA testing only.

Score: 66
Impact scope: 3
Created: 2023-06-27 12:53:40
Owner: None Assign owner
Automated responses: View Execution Result

Highlights

Possible HTTP Header OGNL Expression Exploit

Technique: T1190 - Exploit Public-Facing Application
Rule name: Unsuccessful login to Kerberos
Data source / processor: Trend Micro Deep Discovery Inspector

2022-04-20 11:06:17 | View event
(interestedip) 46.166.139.111
(dst) 198.71.247.91
(uid) yoda\$
(deviceDirection) outbound

46.166.139.111 10.0.2.71 yoda\$ 198.71.247.91

Companion

The recommended response to an alert related to unauthorized access to the Unix shadow file would be to investigate the alert further and determine if it is a legitimate threat. This may involve reviewing logs, analyzing network traffic, and conducting interviews with users. If the threat is confirmed, appropriate action should be taken to mitigate the threat, such as revoking user access, changing passwords, or implementing additional security measures. It is also important to document the incident and take steps to prevent similar incidents from occurring in the future.

This response is generated by generative AI. You should check the accuracy of the response as appropriate for your use case.

Explain this alert

Generating reply...

Type your question here

TREND MICRO

2024



Silent Sabotage: Weaponizing AI Models in Exposed Containers

2023



API Security Exposed: The Role of API Vulnerabilities in Real-World Data Breaches

2023



A Deep Dive into the Packet Reflection Vulnerability Allowing Attackers to Plague Private 5G Networks

2022



Supply Chain as Kill Chain: Security in the Era of Zero Trust

2021



Identifying Cybersecurity Focus Areas in Connected Cars Based on WP.29 UNR155 Attack Vectors and Beyond

2021



Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them

Fast Facts

51M

ransomware
threats blocked

92%

reduction in
ransomware

**Proactive security
starts here**

- By reducing risk, ransomware infection can be **reduced by 92% ***
- By actively hunting vulnerabilities we offer Trend Vision One customers protection up to **96 days ahead*** of a vendor patch
- **147 billion threats *** blocked in 2024

Source : Trend Research



Securing a safer connected world

Cybersecurity failures increasing

Global threats up by **24%**

73%

digital attack surface spiraling

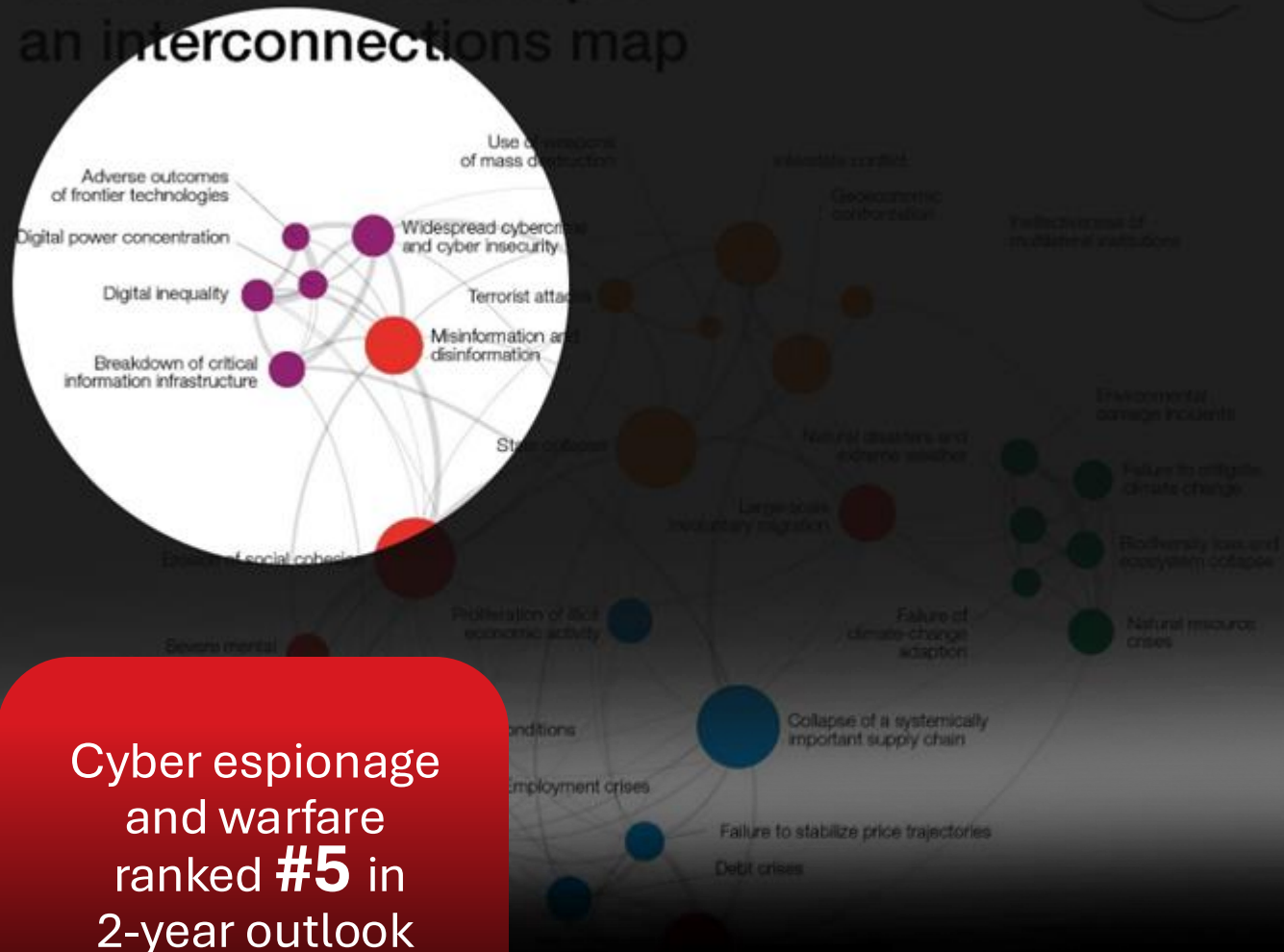
7/10

CROs expressed intense cyber risks concern

Cyber espionage and warfare ranked **#5** in 2-year outlook

Global Risks Report 2023

Global risks landscape: an interconnections map



WORLD
ECONOMIC
FORUM

Source : World Economic Forum
Global Risk Report

Unmasking cybercrime operations



Operation Killer Bee

Interpol. Nigeria Eco. OPEC
oil and gas industry (OPEC);
disguise
Petroleum company;
credential theft

Operation Cyclone Clop

Ransom arrest of mules
2019–21, 4 RFIs on
Clop TA505 group

TM Op. Quicksand Gandcrab
ransom arrest Intel and data
sets 19 law enforcement
agencies in 17 countries

Operation Chronos

Largest ransomware group
in terms of impact globally,
responsible for 25% of
ransomware attacks in
the last year (2023–24)



**Proactive security
starts here**



Proactive Security
Starts Here

Trend Micro™ Threat Intelligence



Understanding Risks

Am I at risk
of being
targeted?

Am I protected against
the latest threats and
exploits in the news?

What should
I do next for
this attack?

Did I catch everything
about this attack?



Outcomes

**Better prepared
for advanced,
emerging threats**

**Confidence to
hunt threats and
pre-empt alerts**

**Align security
investments with
business goals**

Where Does Our Data Come From?

Cyber Risk Exposure Management



Targeted Attacks



Threats



Cloud



IoT and OT



AI and ML



Cybercriminal Undergrounds



Future Threat Landscapes



Vulnerabilities



Endpoint Security



Cloud Security



Network Security



Email Security



Identity Security



AI Security



Data Security

Trend
Research

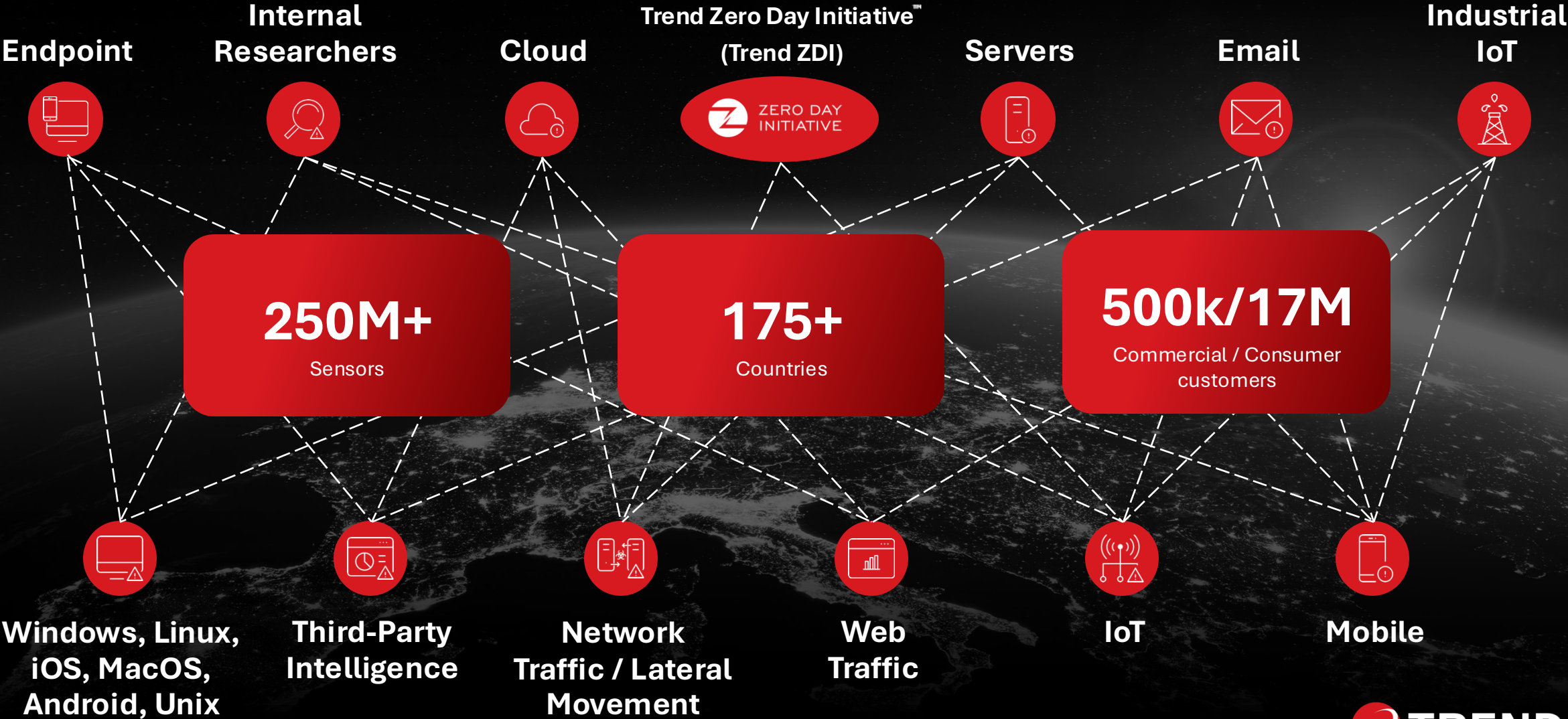


Threat intelligence and research for consumers, businesses, and governments

Trend Micro core technology and Trend Vision One™ AI-powered enterprise cybersecurity platform

Public/private partnerships (e.g. global enforcement)

Unprecedented Intelligence Gathering



Trend Zero Day Initiative™ Leadership

50% of bugs found
by internal
Trend ZDI
researchers

Over **1,900**
vulnerabilities disclosed
in 2023

Discloses
2.5x more vulnerabilities
than its nearest rival

Protects up to
96 days ahead
of the industry
before a breach can occur on
zero-day vulnerabilities

\$1M by Trend Micro
customers
who applied all virtual
patches in 2023
saved on average

Discovered
60%
of vulnerabilities
worldwide in 2023
(disclosed by vendors mentioned in Omdia report)

16,000 External
researchers
supporting
Trend ZDI



Two Paths | Threat Intelligence

Have Existing Platform/Tool

Within Trend Vision One

Trend Micro™ Threat Intelligence Feed

- A comprehensive repository of IOCs, including vulnerabilities with enriched context
- Can be imported into third-party tools

Trend Vision One™ – Threat Insights

- Deep insights into threats, CVEs, attackers
- Standalone or with Trend Vision One™ Cyber Risk Exposure Management (CREM) and/or Trend Vision One™ Security Operations (SecOps)

Trend Vision One™ Sandbox Analysis

- Protection from unknown threats
- Local threat intelligence

Know What You're Up Against

- Deep insights on emerging threats and threat actors within reach
- Get to know your adversaries; who they are, what they want, and how they plan to get it

TargetCompany's new variant with Mallox and Fargo ransomware extensions

Type

AKA

Targeted countries

Targeted industries

Motivation

First seen

Last seen

Last updated

Emerging Threat

AVAST, FARGO, MALLOX, Malla...

▼

Bolivia, Brazil, China, France, German...

▼

Education, Energy, Entertainment, ...

▼

Financial Gain

June 2022

May 2024

2024-05-06 18:28:13

Overview

Risk Management Guidance

Threat Hunting Queries (2)

Overview

TargetCompany Ransomware was initially spotted in June 2021, using the affected company as its appended extension name and mostly targets vulnerable Database servers. But earlier this year, Avast Cybersecurity firm was able to develop a free decryptor for the encrypted files to help victims recover their important files. But that did not stop the Threat Actors in their bad acts and was able to improve their malware and later on changed their encryption. They started to employ Reflective Loading technique for its defense evasion where it connects to an IP address to load the encrypted ransomware. The contents of the IP address change periodically, giving a hard time for Threat Analysts to replicate the infection.

Recently, Threat Hunting Team found a TargetCompany Ransomware infection case with a much different

Intelligence Data

Intelligence Reports (25)

Tactics, Techniques, and Procedures

Tools (7)

Malware (5)

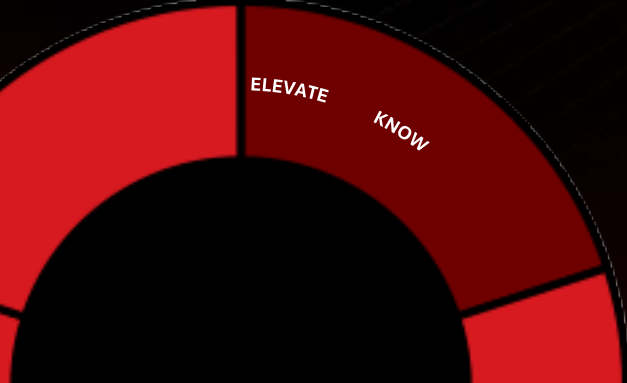
CVEs (2)

Indicators (341)

Associated Threat Actors (1)

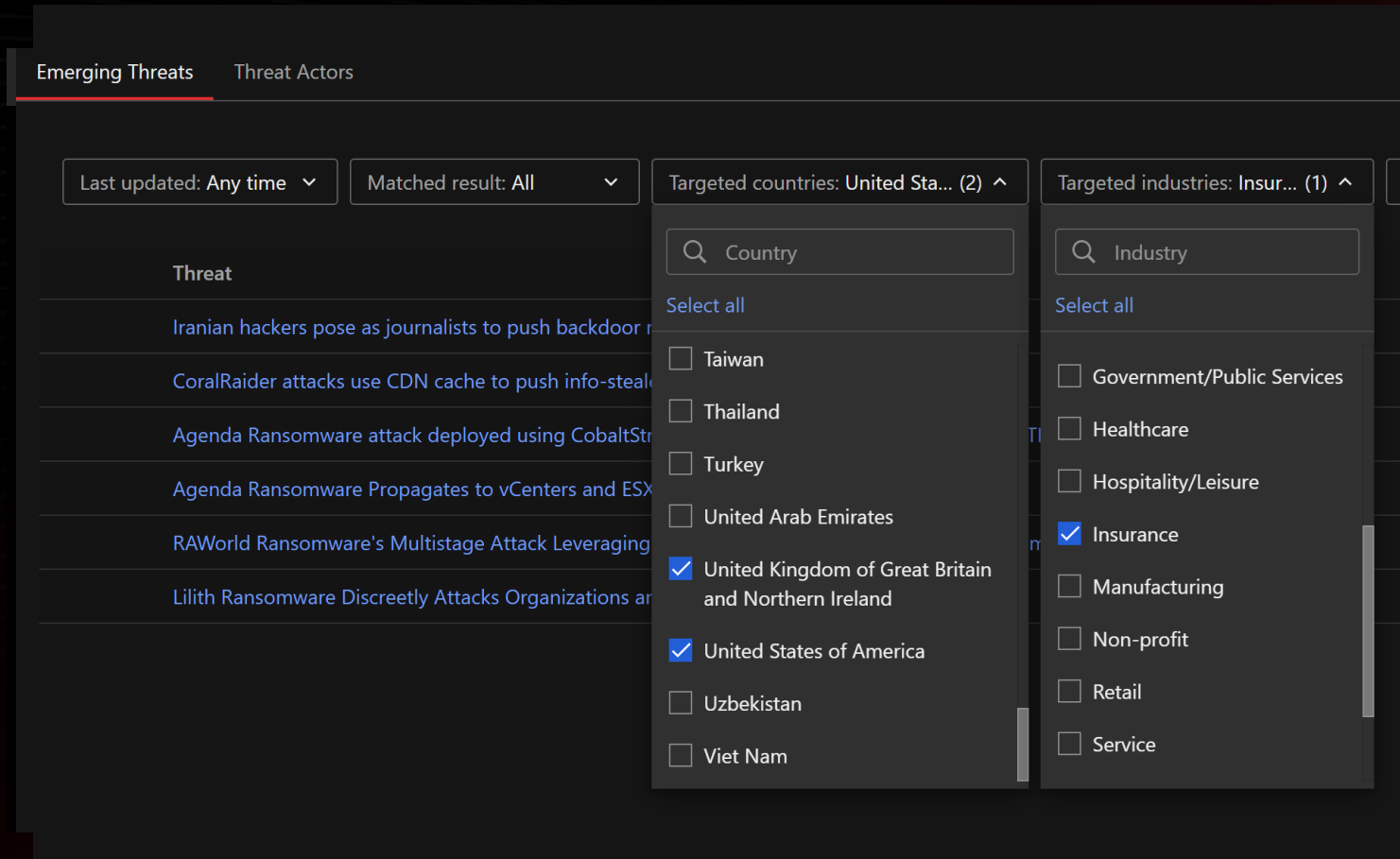
Note: You can view sweeping results for these reports in [Intelligence Report](#).

Report name	Source	Last updated ↓
[Ransomware New Infections] TargetCompany Ransomware Recurring Infection in JP due to vulnerable SQL	Trend Micro	2024-05-18 12:26:04
Mallox ranomware affiliate leverages PureCrypter in MS-SQL exploitation campaigns	Security vendors	2024-05-15 22:25:31
[Ransomware New Infections] TargetCompany Ransomware New Variant (.rmallox) Ransomware Incident	Trend Micro	2024-05-11 11:26:23



See Threats Coming from Miles Away

- Filter emerging threats and actors in your region and industry
- Take actions ahead of upcoming threats



The screenshot displays the Trend Micro Threat Intelligence dashboard. At the top, there are two tabs: "Emerging Threats" (selected) and "Threat Actors". Below the tabs, there are four filter sections:

- Last updated:** Any time (dropdown)
- Matched result:** All (dropdown)
- Targeted countries:** United Sta... (2) (dropdown with a list of countries)
- Targeted industries:** Insur... (1) (dropdown with a list of industries)

The "Threat" table lists several threats:

Threat
Iranian hackers pose as journalists to push backdoor r...
CoralRaider attacks use CDN cache to push info-steal...
Agenda Ransomware attack deployed using CobaltStr...
Agenda Ransomware Propagates to vCenters and ESX
RAWorld Ransomware's Multistage Attack Leveraging
Lilith Ransomware Discreetly Attacks Organizations ar...

The "Country" dropdown menu is open, showing a list of countries with checkboxes. The "Industry" dropdown menu is also open, showing a list of industries with checkboxes.

Enrich XDR Alert Investigation

- Enhance XDR workbench alerts with detailed threat intelligence
- Know the "who, why and how" behind the attack

New Threat2024-06-12Type: Cybercrime AKA: AlphaV, AlphaVM, ALPHV

BlackCat Rans...Campaign Overview:

- BlackCat Ransomware (aka AlphaVM, AlphaV, or ALPHV) was first observed in mid-November 2021 by researchers from the MalwareHunterTeam....

Emerging ThreatsThreat Actors

Last updated: Any ti...Matched result: AllType: AllTargeted countries: AllTargeted industries: AllSearch

Threat actor

StatusAKA

BlackCat Ransomware

ActiveAlphaV, AlphaVM, ALPHV

Workbench ID

Report name

WB-10797-20240301-00003

[Targeted Attack] Top malicious IOC found in company possibly attacked by BlackCat - 2024-02-29

APT-Viper

ActiveAPT-C-23, Desert Falcon

BlackCat Ransomware

TypeCybercrime

AKAALPHV, AlphaV, AlphaVM

Targeted countriesAustralia, Canada, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Netherlands, Philippines, Singapore, Spain, Thailand, United Kingdom of Great Bri...

Targeted industriesEducation, Energy, Financial Services, Government/Public Services, Hospitality, Leisure, Insurance, Manufacturing, Retail, Service, Technology, Transportation, Utilities

MotivationFinancial Gain

First seenNovember 2021

Last seenJune 2024

Last updated2023-02-17 13:53:33

Overview

Campaign Overview:

- BlackCat Ransomware (aka AlphaVM, AlphaV, or ALPHV) was first observed in mid-November 2021 by researchers from the MalwareHunterTeam.
- BlackCat swiftly gained notoriety for being the first major professional ransomware family to be written in Rust language.
- Since it first came out in 2021, BlackCat has victimized organizations from a variety of industries that include construction, retail, manufacturing, technology, and energy.
- BlackCat's attacks have been detected in multiple locations globally, but organizations based in the US lead the victim count, followed by some in Europe and Asia-Pacific.

Linked Groups:

- According to the FBI's advisory published on April 19, 2022, several developers and money launderers for BlackCat have links to two defunct ransomware-as-a-service (RaaS) groups - DarkSide and Bl...

Intelligence Data

Intelligence Reports (57)Tactics, Techniques, and ProceduresTools (13)Malware (4)CVEs (4)Indicators (194)

Note: You can view sweeping results for these reports in Intelligence Report.

Report name

Source

Last updated

IcedID Brings ScreenConnect and CSharp Streamer to ALPHV Ransomware Deployment

Security vendors

2024-06-12 02:26:38

[Targeted Attack] Top malicious IOC found in company possibly attacked by BlackCat - 2024-05-23

Trend Micro

2024-05-22 17:26:12

SEE

ENRICH

TREND MICRO

Unlock Vulnerabilities Intelligence

- Fueled by Trend Zero Day Initiative
- Quickly search CVEs to see details, exploit actors, targets, and required actions

Emerging ThreatsThreat Actors

Last updated: Any ti...

Matched result: All

Targeted countries: All

Targeted industries: All

CVE-2021-44...

Reset

Threat	Targeted countries	Targeted industries	Impact scope
Karakurt	-	Communications, Energy, Hea...	000

Intelligence Data

Intelligence Reports (0)

Tactics, Techniques, and Procedures

Tools (4)

Malware (3)

CVEs (1)

Indicators (0)

Associated Threat Actors (0)

CVE ID

CVE ID ↑	Description	CVSS v3.0	CVSS v2.0	OS / App
CVE-2021-44228	Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.	0	9.3	emergen

ENRICH

UNLOCK

TREND MICRO

Elevate Cyber Risk Exposure Management

- Deep context on vulnerabilities in your environment
- Enables faster, more proactive decisions

CVE-2021-44228

Basic

Devices



Threat Intelligence

Status: New

Device

Apply

Add filter

<input type="checkbox"/>	Device name	Operating system	IP address
<input type="checkbox"/>	 rs-win10-wrk01	Windows 10 10.0 (Build 19041)	10.44.52.101
<input type="checkbox"/>	 rs-app03	Windows Server 2016 10.0 (Build 14393)	10.44.52.4

Basic

Devices

Threat Intelligence

ASSOCIATED EMERGING THREATS

Report name

Karakurt

ASSOCIATED THREAT ACTORS

Threat actor	Status	AKA
Kimsuky	Active	Black Banshee, Earth Kumiho, Kims...
Earth Smilodon	Active	APT 27, BRONZE UNION, Budworm, ...
Water Goblin	Active	Conti

PROACTIVE SECURITY STARTS BY

Operationalizing Threat Intelligence



Faster decisions
Lower risk exposure

“

I can bring IOCs **very quickly**
and search across my organization.
I used to spend up to a week just
to answer the question of ‘**are we
affected by this?**’

Executive director,
Large university in USA



**Proactive security
starts here**



Proactive Security
Starts Here

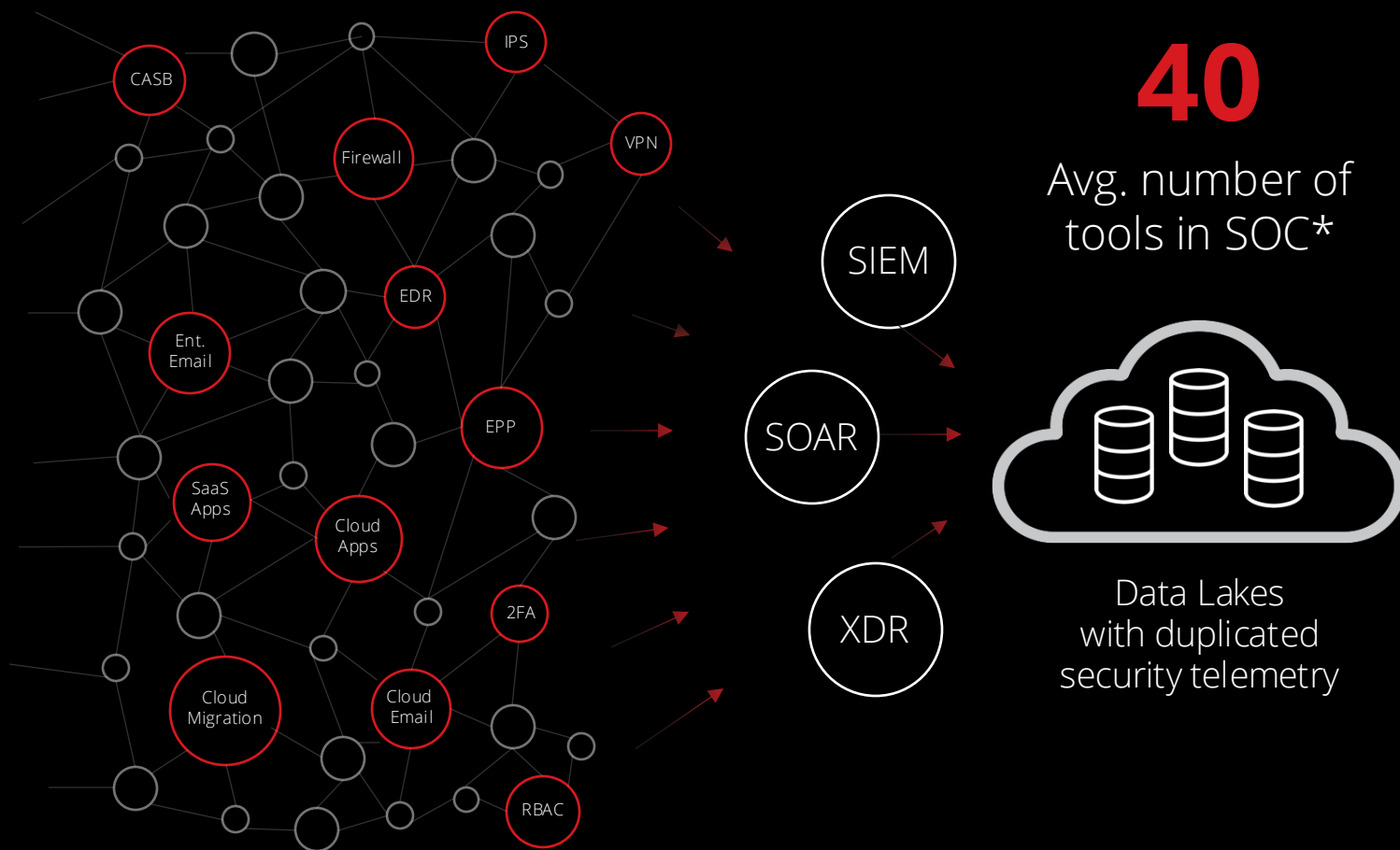
Trend Vision One™ Security Operations (SecOps)





Here's the reality

Overwhelmed SOC teams experience



Alert fatigue

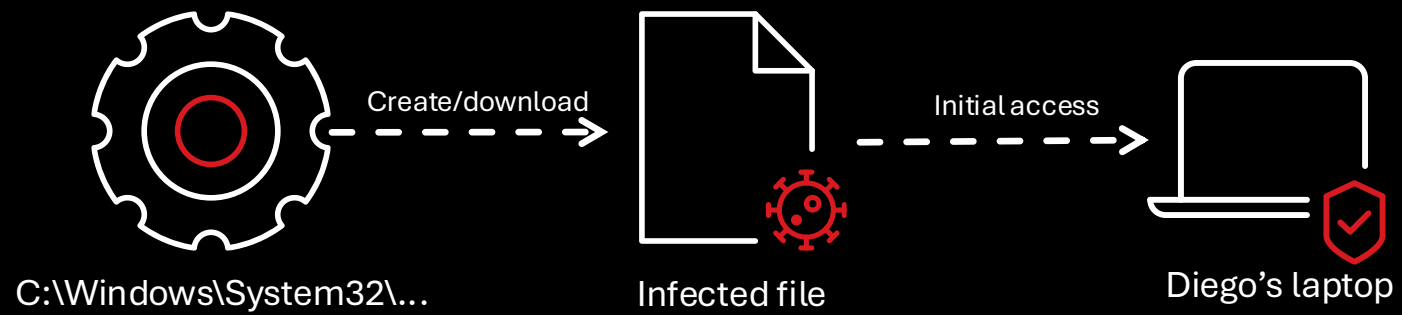
Overlapping solutions

Data lake and cost proliferation

Siloed data

Takes time to correlate

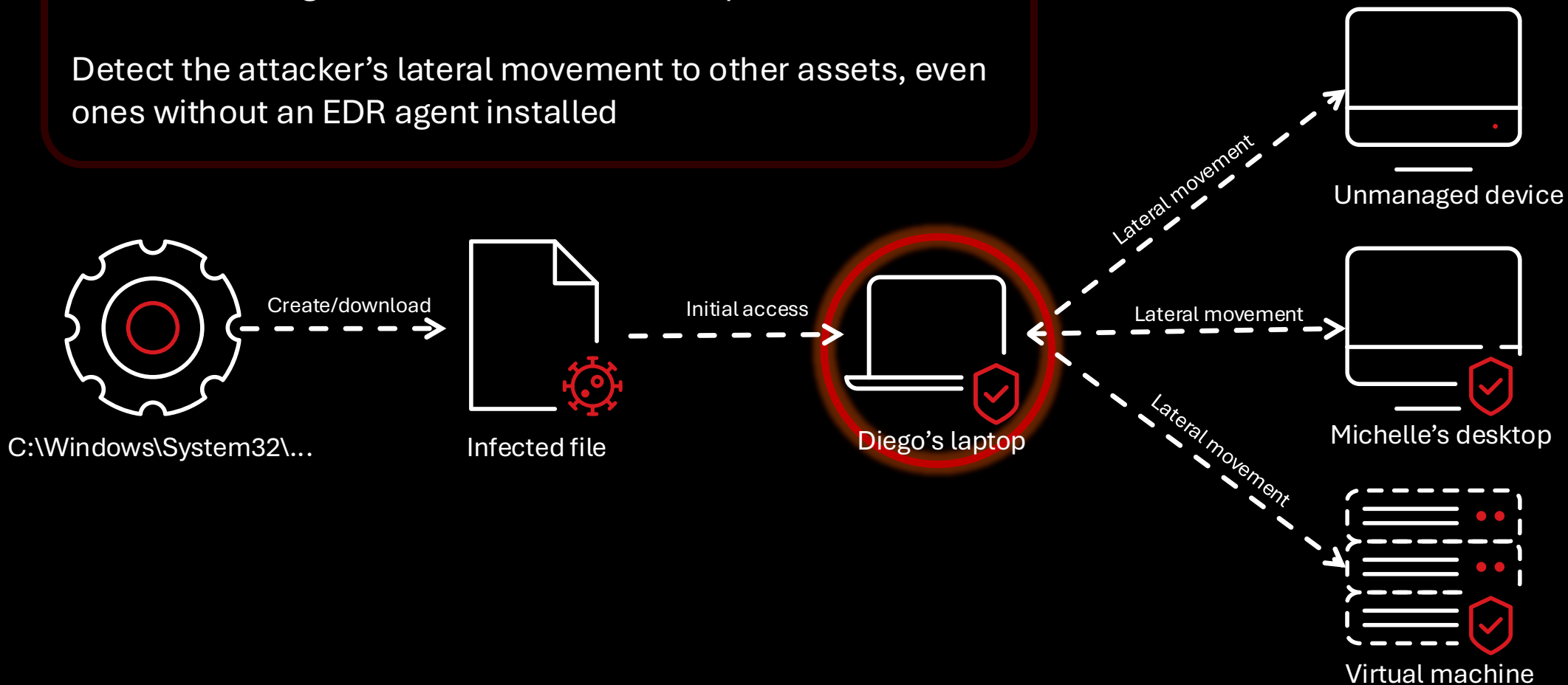
Challenging to measure effectiveness



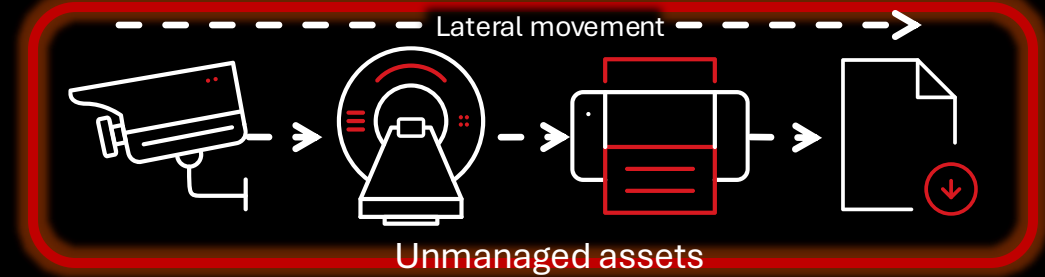
Endpoint Detection and Response

Detect that Diego's machine has been compromised

Detect the attacker's lateral movement to other assets, even ones without an EDR agent installed

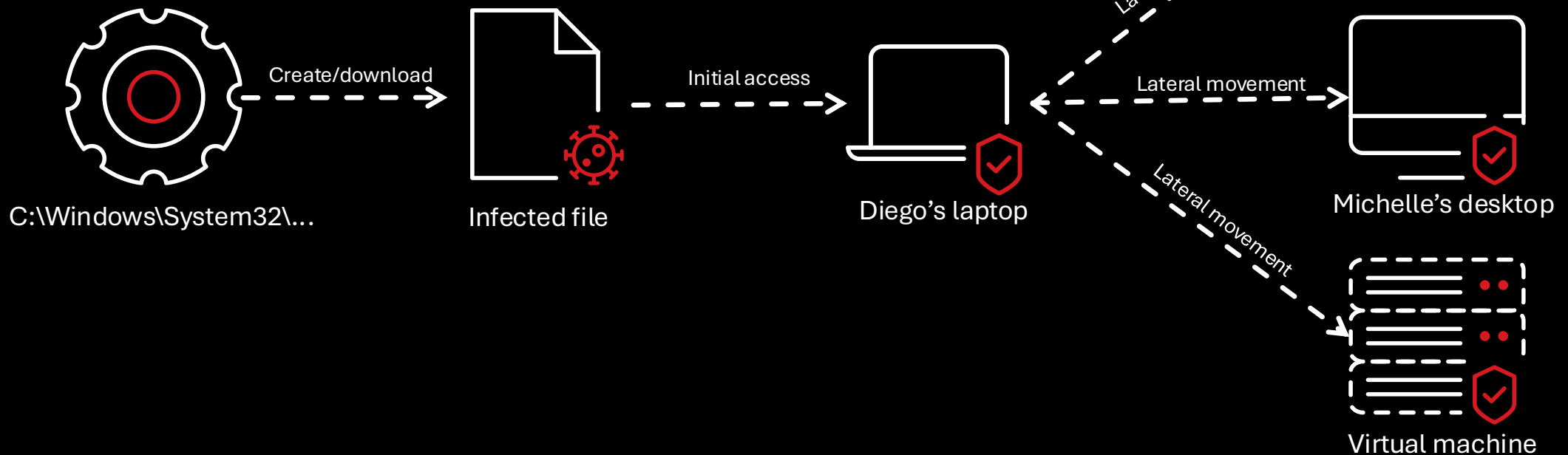


Network Detection and Response

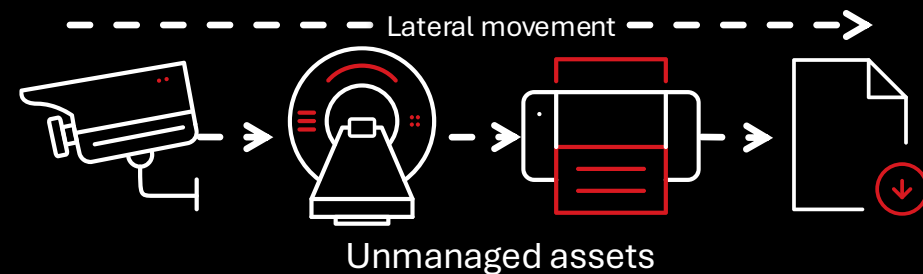


Not all assets have an agent installed

Detect the attacker's movements between unmanaged assets, and their C&C communication

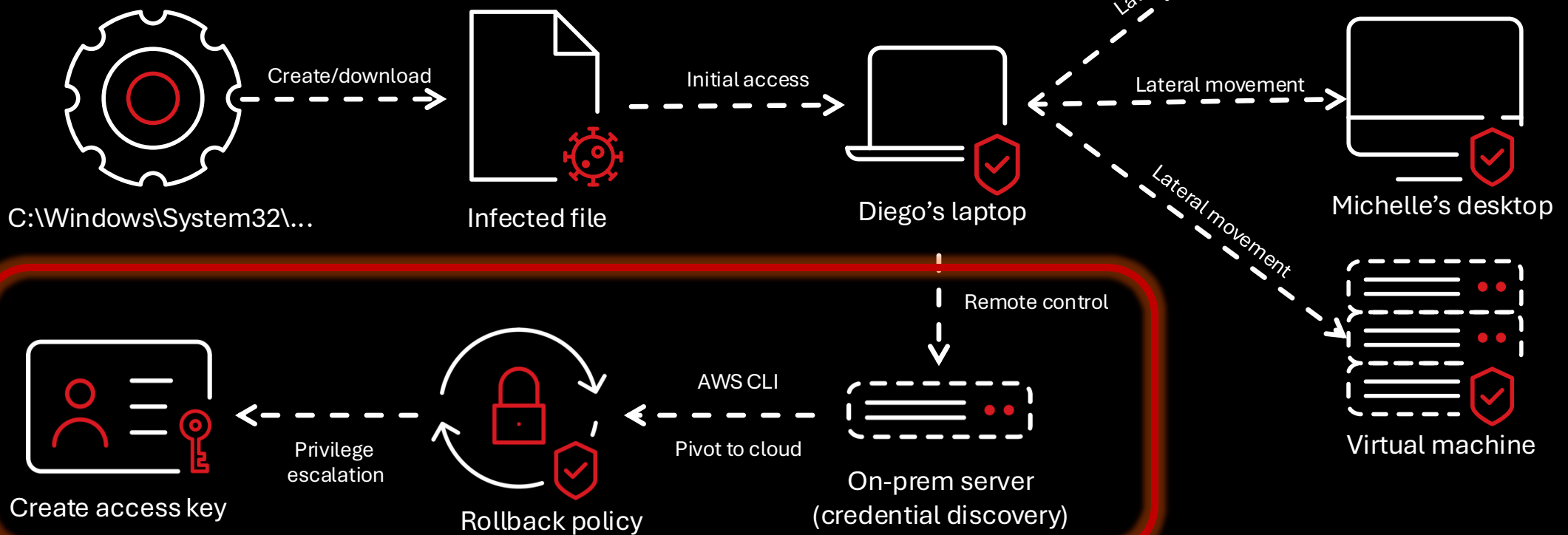


Cloud Detection and Response



Attacker gets access to AWS credentials saved on the machine (AWS credential discovery)

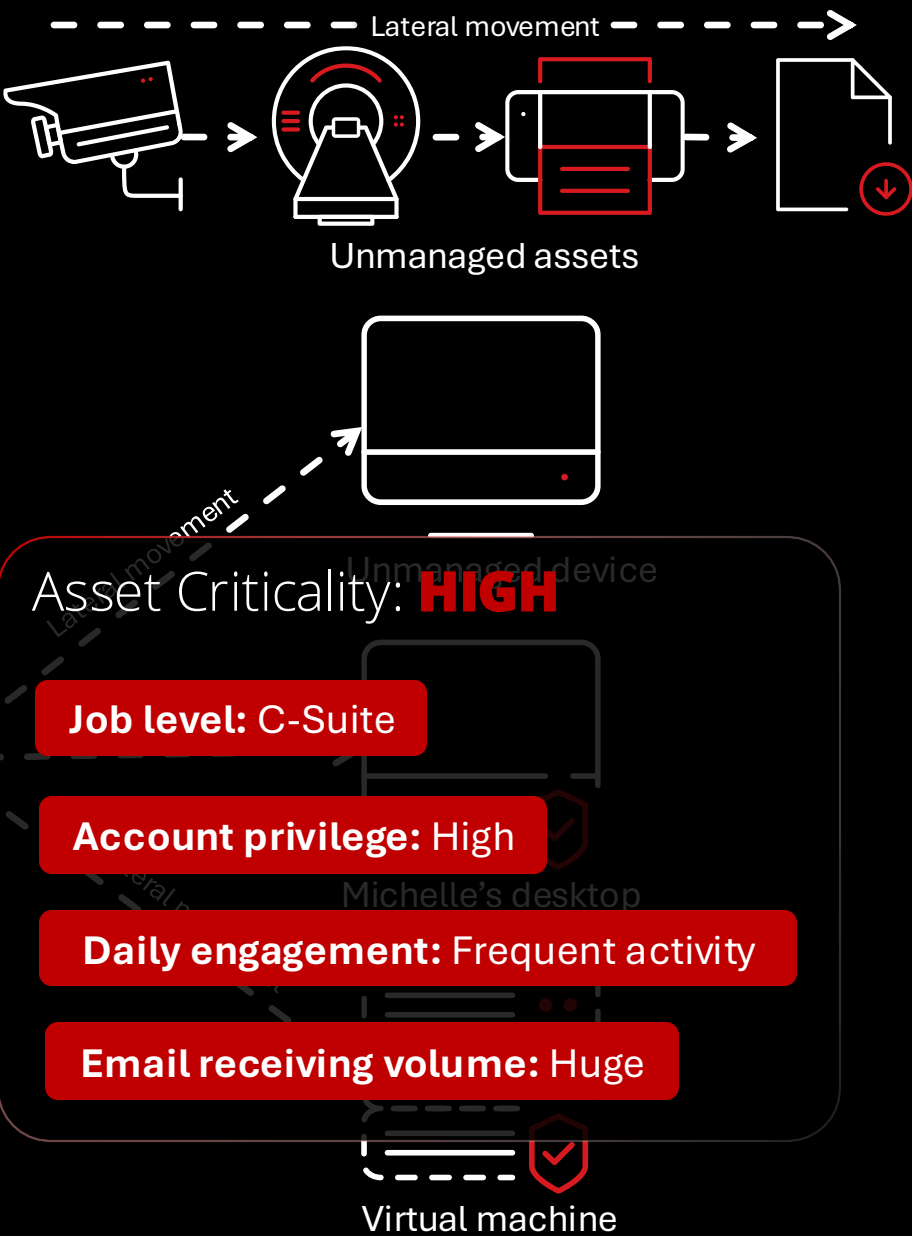
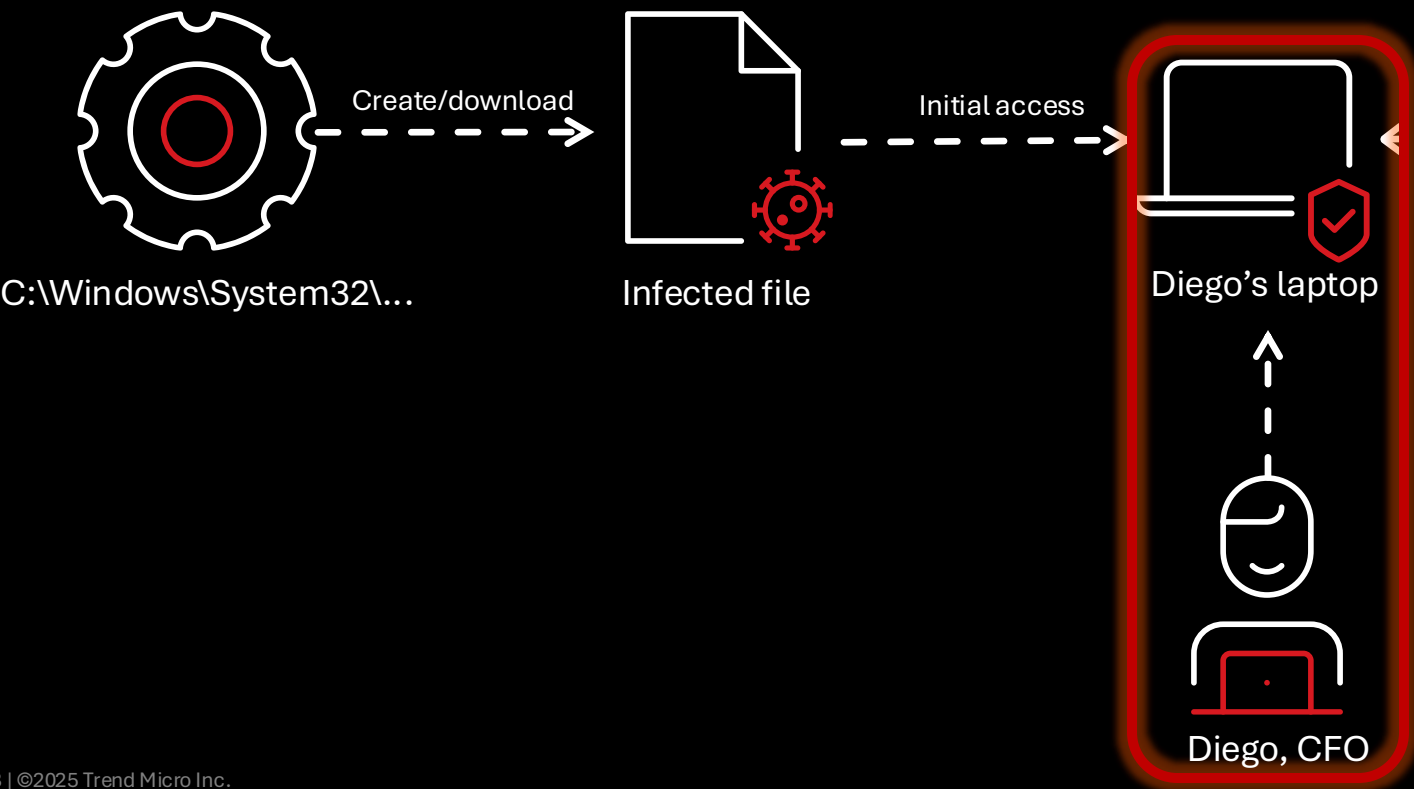
Attacker uses rolled back policy to generate access key



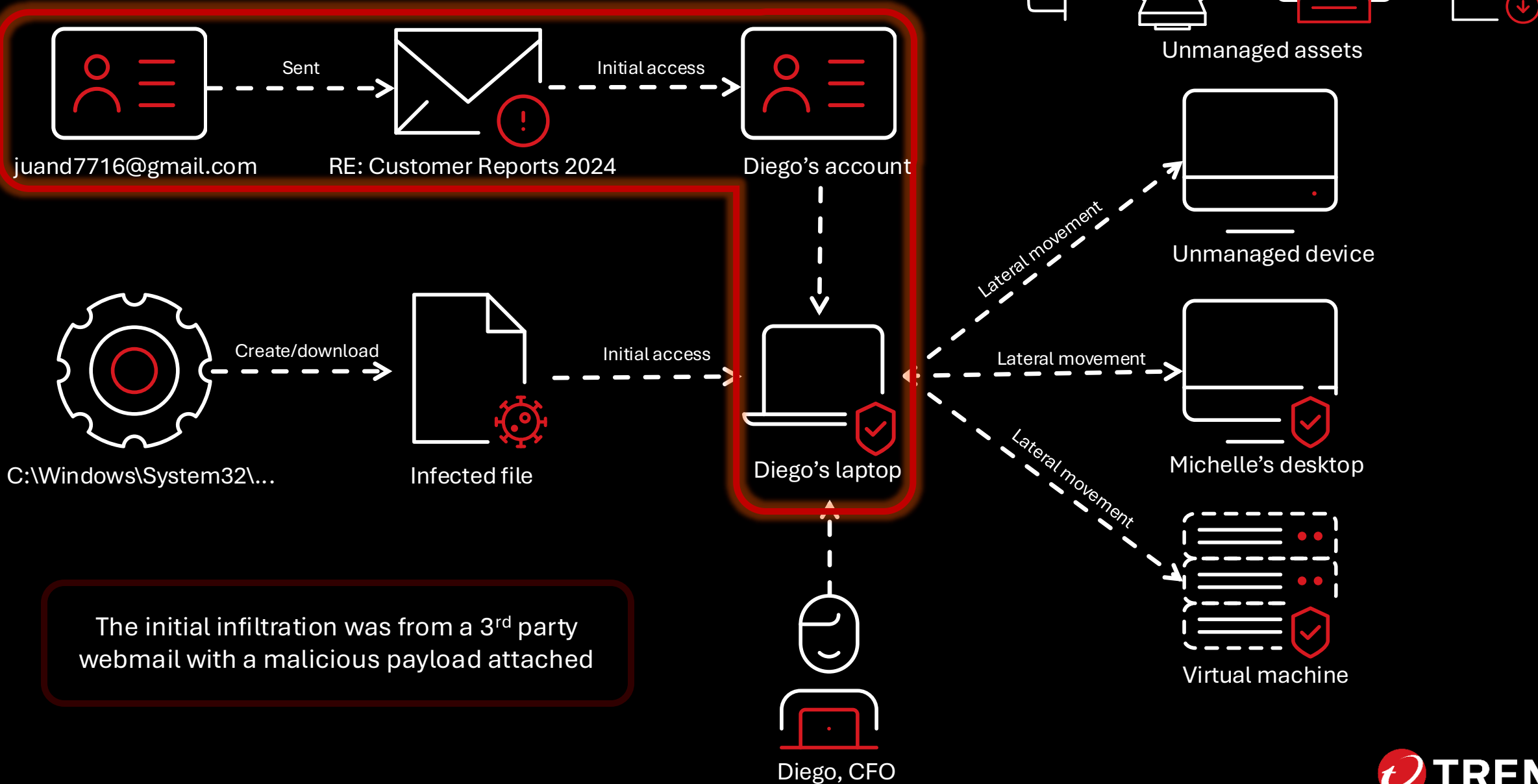
Identity Threat Detection and Response

Detect whether a user has been compromised

Without ITDR, we have no way of knowing that a high-profile user like Diego was compromised until it's too late...



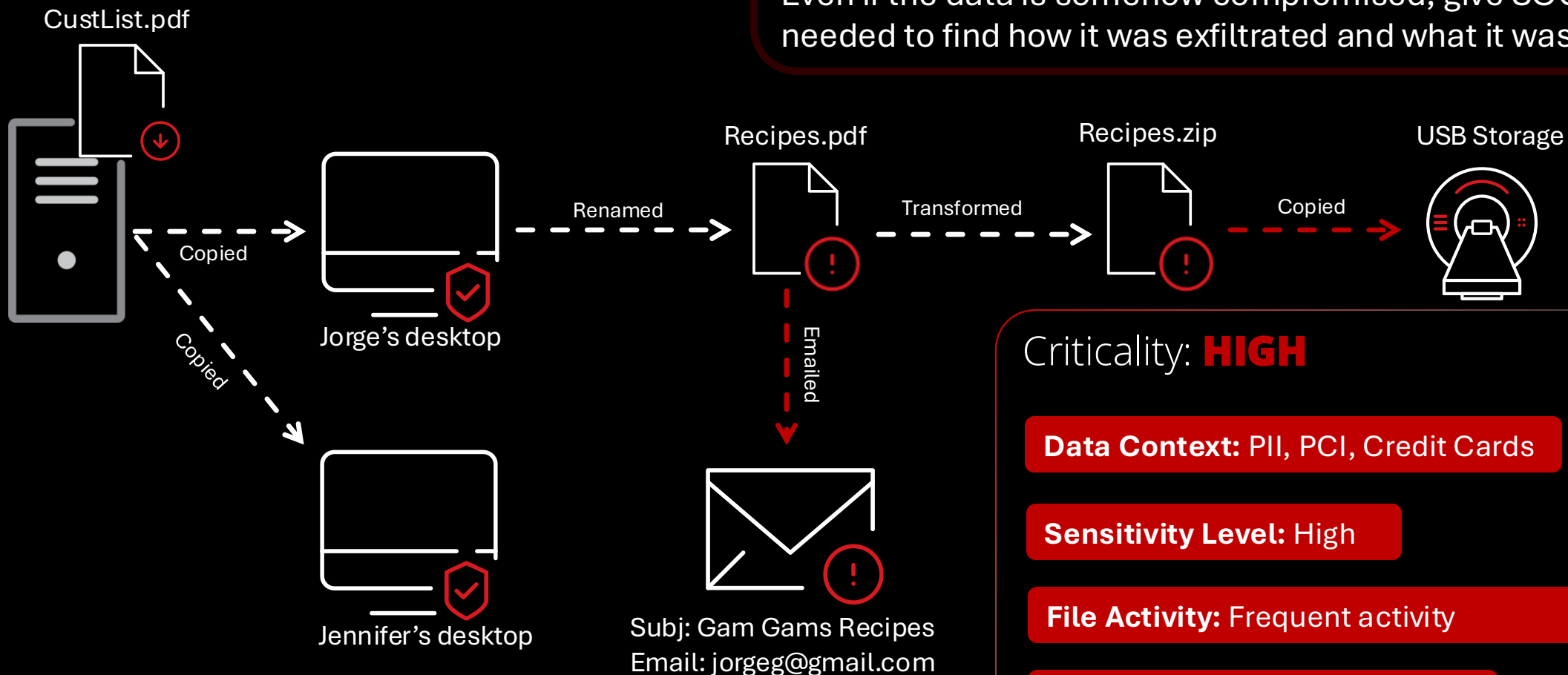
Email Detection and Response



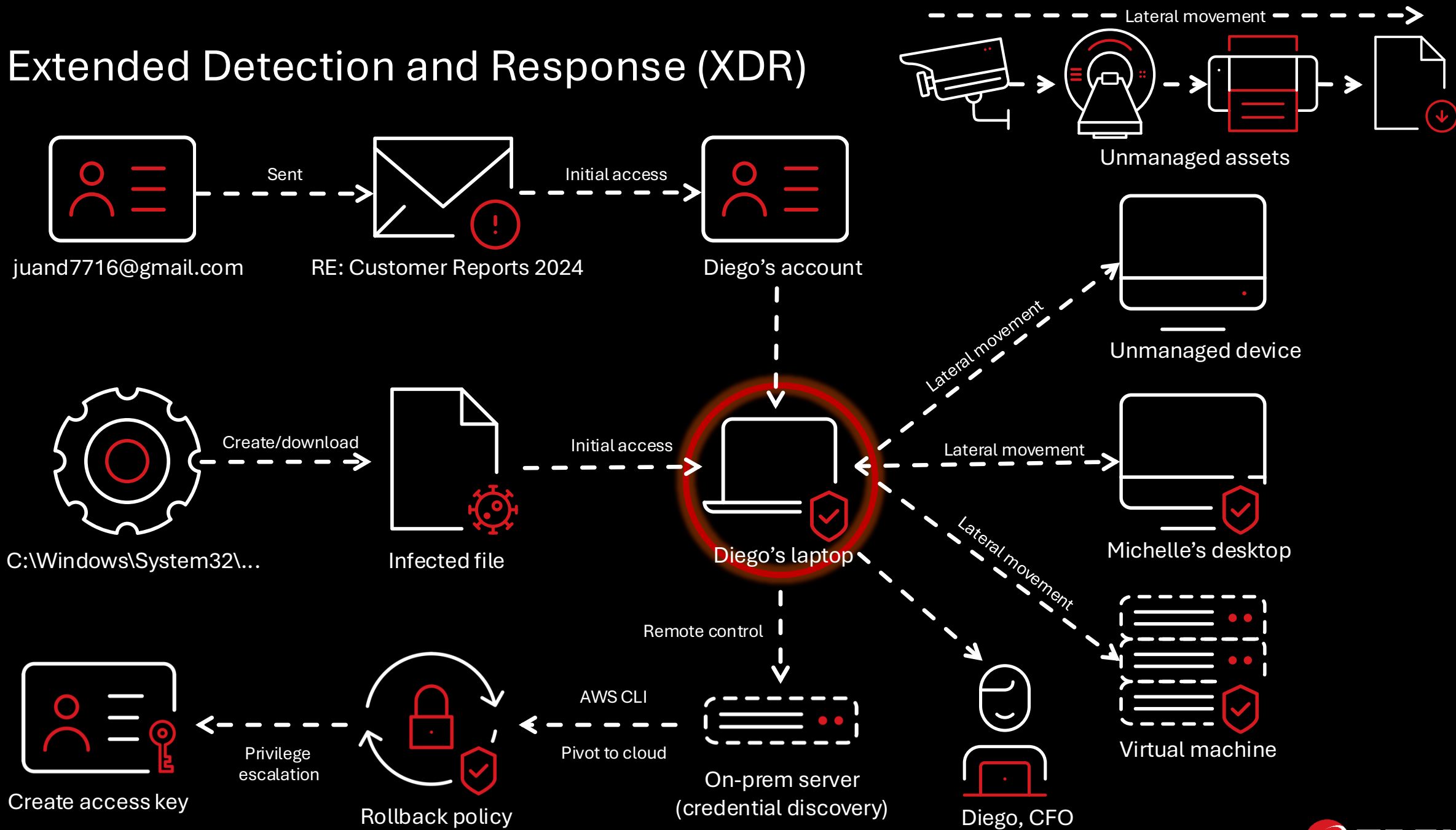
Data Detection and Response

Gain visibility, context, and response to sensitive data as it moves throughout the environment

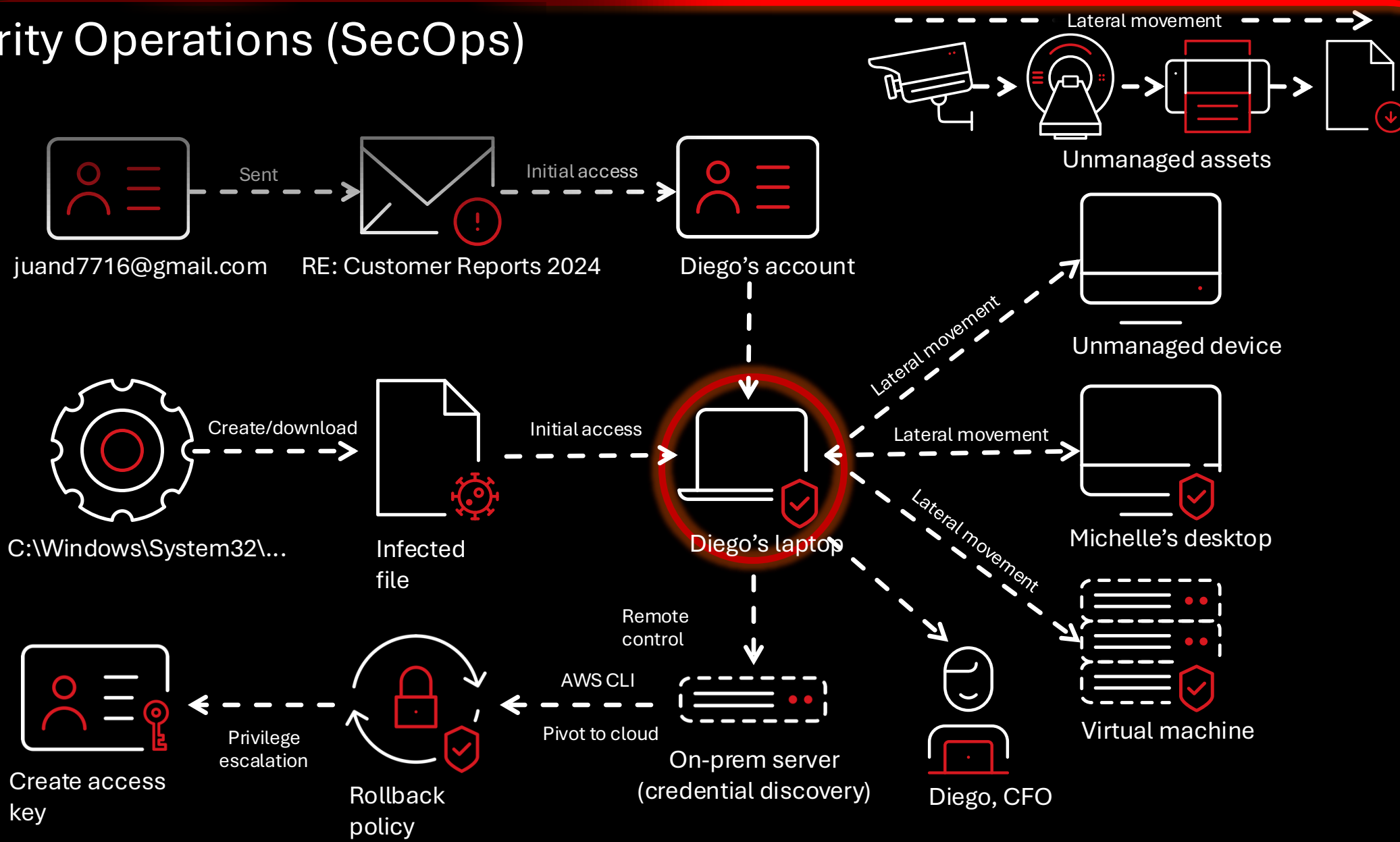
Even if the data is somehow compromised, give SOC the tools needed to find how it was exfiltrated and what it was before



Extended Detection and Response (XDR)



Security Operations (SecOps)



+ Third-Party Telemetry

One Home For All Your Security Telemetry

Trend Micro Native Sensors

Endpoint

Email and Collaboration

Network

Cloud

Identity

Data

Trend Micro Native Telemetry



Third-Party Log Collectors

paloalto NETWORKS

FORTINET

SONICWALL

CHECK POINT

Barracuda

FORCEPOINT

f5

CISCO

okta

Network / Identity / Application Logs



AWS CloudTrail

Amazon VPC

AWS Lambda

Amazon EKS

Amazon S3

Amazon Route53

AWS WAF

Azure Activity Logs

Azure Virtual Network

Google Cloud Audit Logs

Cloud Activity Data



Microsoft

aws

CROWDSTRIKE

Azure

zscaler

Google Cloud

netskope

Third-Party Security Logs



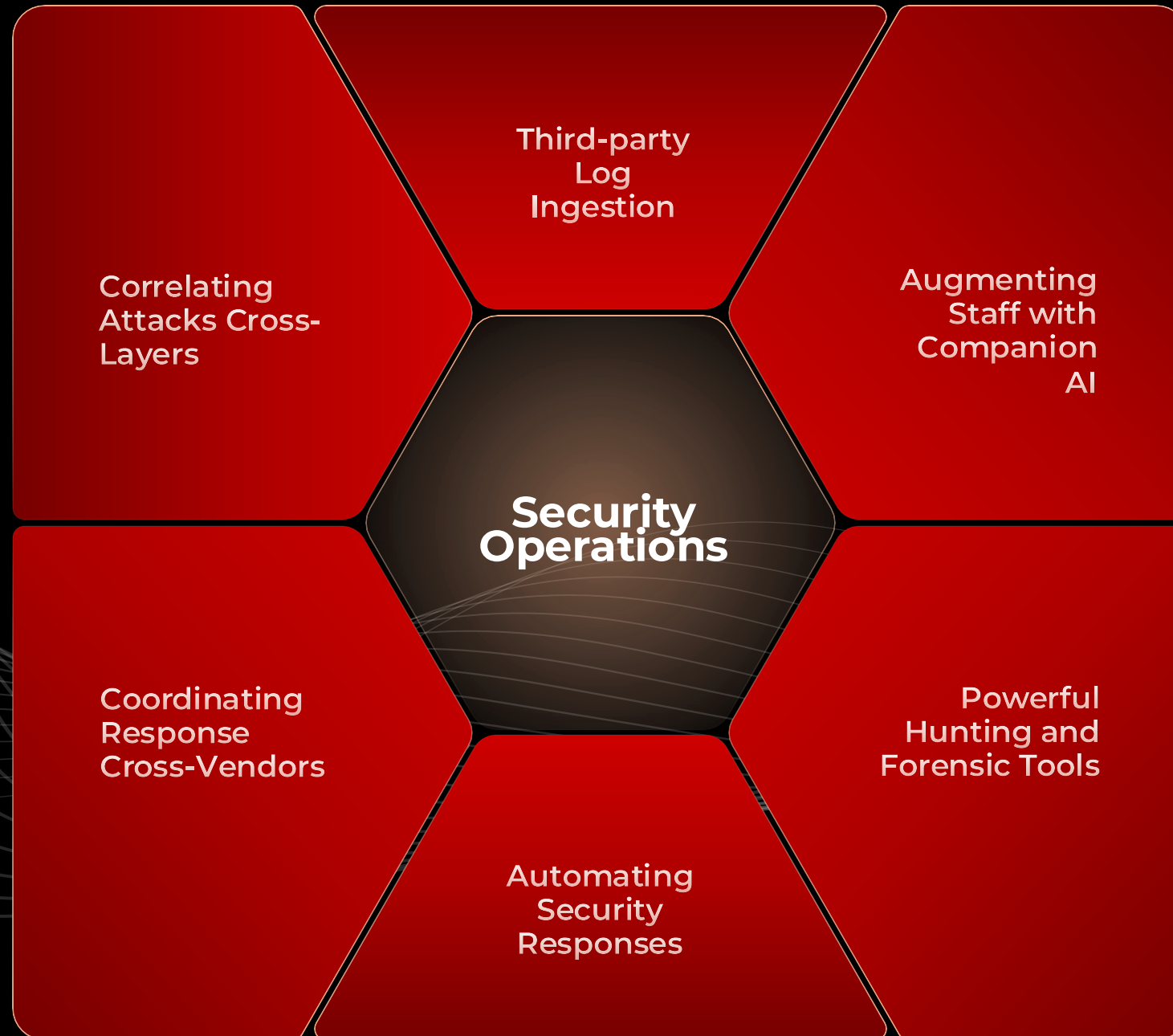
Data Lake | AI-Powered Data Ingestion and Analysis

Data Collection

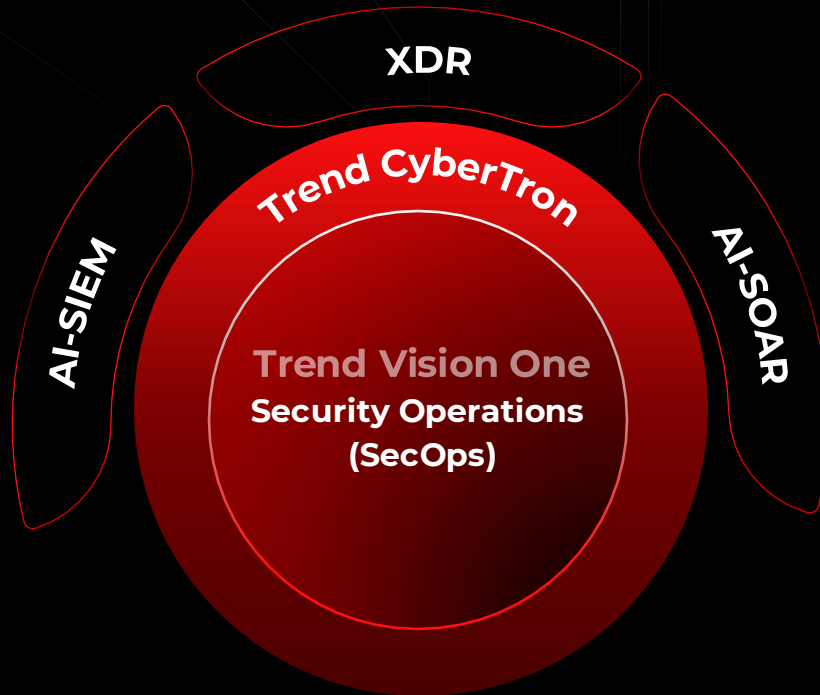
Data Cleaning

Data Transformation

Data Integration



Extend beyond the traditional



powered with

Threat Intelligence

Native Sensors

Global Research

Third-Party Telemetry

Understand Your Data. Act with Intent.
The first AI-SIEM that thinks in language — not just logs

Built for the future

Modern technology at a lower cost, designed for the new digital age.

Trend's LLM Advantage

Treat your schema like a language, using AI to understand the *intent* behind the data.

Unmatched XDR foundation

The first AI-SIEM built on award-winning native sensors, filling in the gaps a SIEM cannot cover.

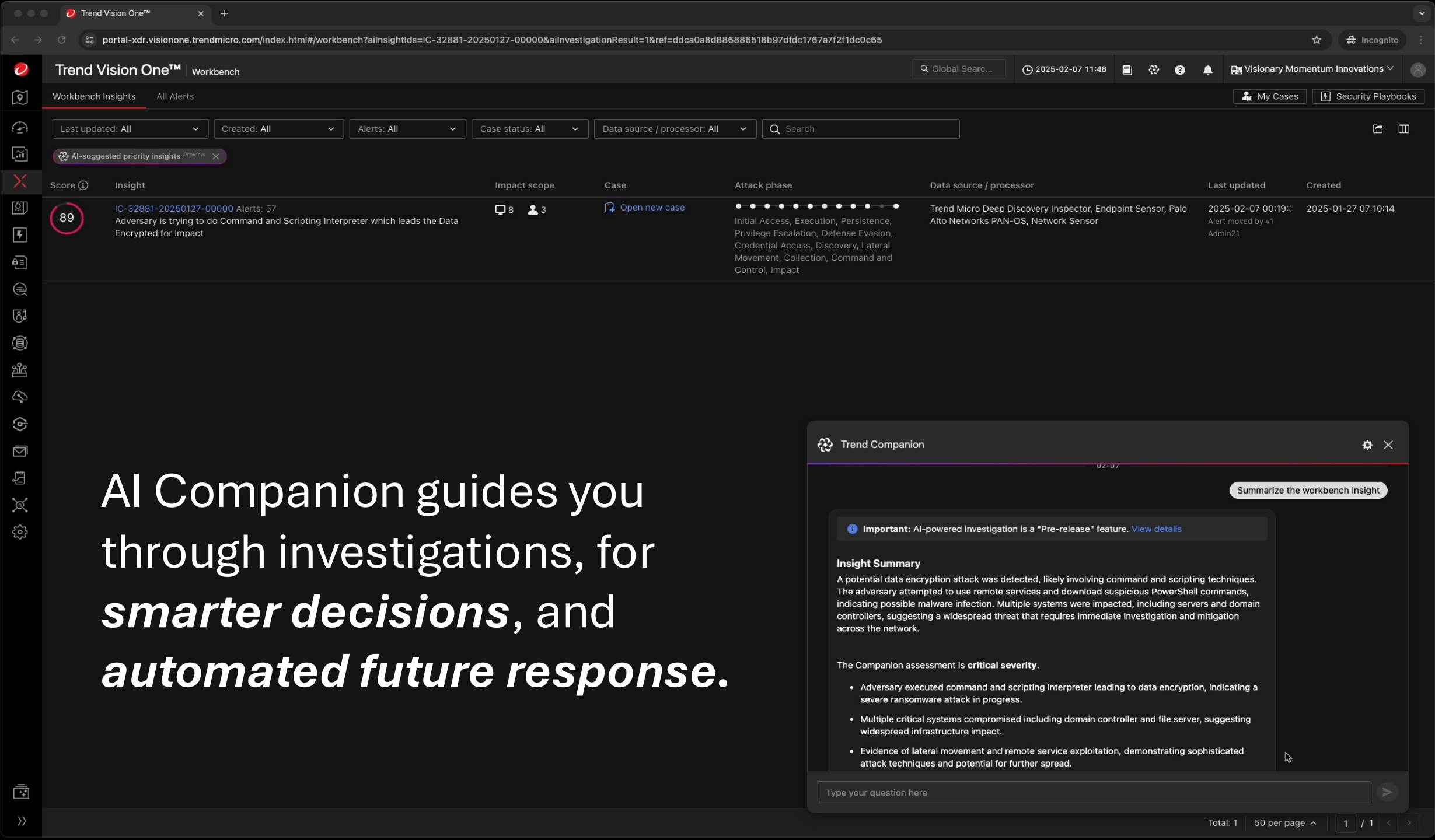
Effortless Threat Hunting

Cut the manual work – let Trend Companion take you on an AI-driven threat hunting journey, delivering actionable insights at every step of the way.

2025-01-17 00:34:27

Last updated: All		Created: Last 30 days		Alerts: All		Case status: All		Q Search		
Score ⓘ	Insight	Impact scope			Case	Attack phase			Last updated	Created
100	IC-31023-20250116-00000 Alerts: 39 Detection avoidance by Data Encrypted for Impact	10	5	2	Open new case	Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Command and Control, Impact			2025-01-16 15:54:04 Alert moved by v1 Admin9	2025-01-16 15:35:4
75	IC-31023-20250117-00000 Alerts: 7 Environment probing(Transfer Data to Cloud Account) has been detected	1			Open new case	Initial Access, Persistence, Privilege Escalation, Defense Evasion, Discovery, Collection, Exfiltration			2025-01-17 18:42:52 New alert correlated	2025-01-17 17:15:0
70	IC-31023-20250108-00000 Alerts: 34 Environment probing(Cloud Service Discovery) has been detected	1			Open new case	Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Discovery			2025-01-22 06:39:55 New alert correlated	2025-01-08 08:07:3

Workbench gives you a single, prioritized view of all alerts –
So, you know *exactly where to start*



AI Companion guides you
through investigations, for
smarter decisions, and
automated future response.

Trend Companion

02-07

Summarize the workbench insight

Important: AI-powered investigation is a "Pre-release" feature. [View details](#)

Insight Summary

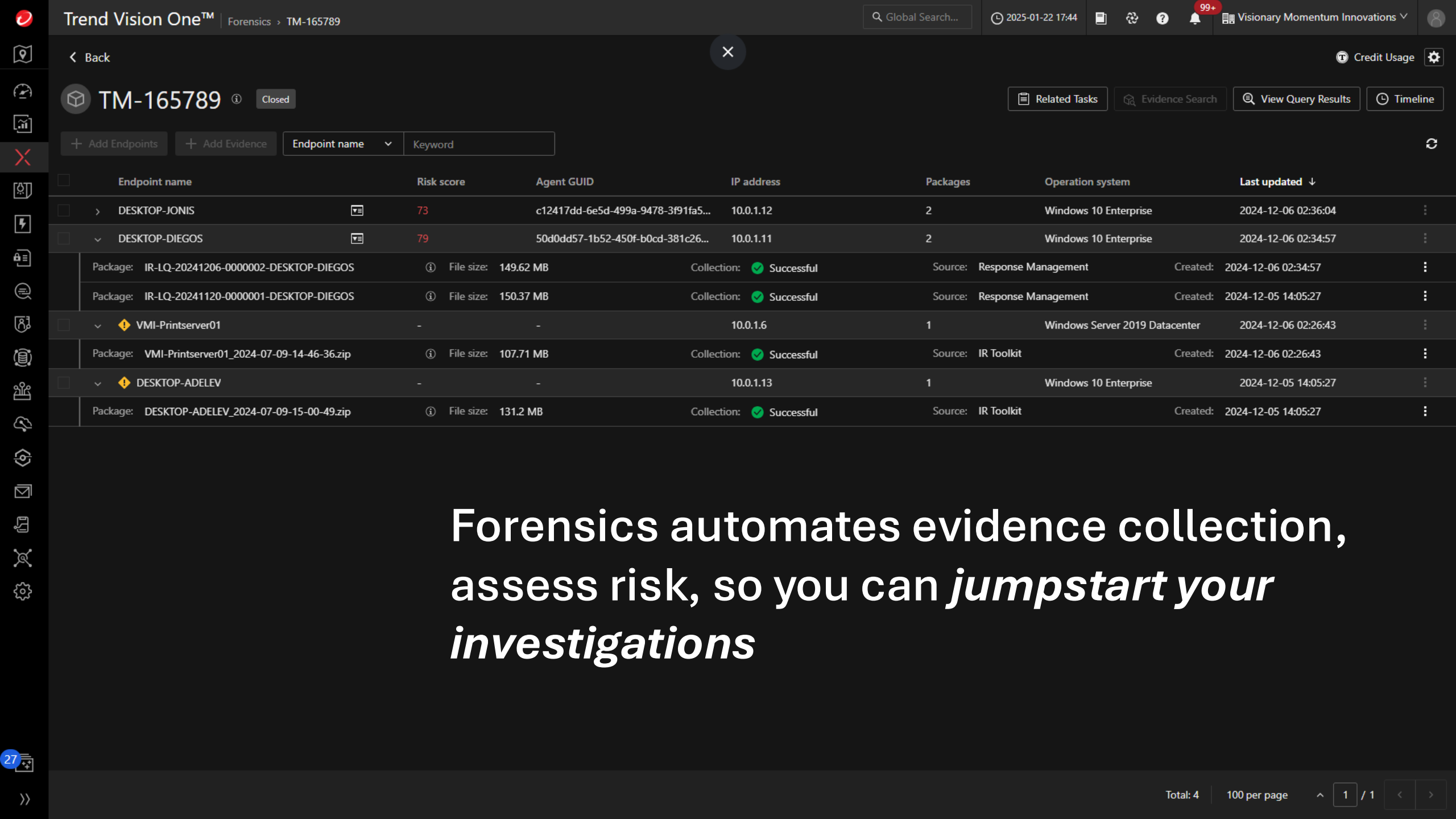
A potential data encryption attack was detected, likely involving command and scripting techniques. The adversary attempted to use remote services and download suspicious PowerShell commands, indicating possible malware infection. Multiple systems were impacted, including servers and domain controllers, suggesting a widespread threat that requires immediate investigation and mitigation across the network.

The Companion assessment is **critical severity**.

- Adversary executed command and scripting interpreter leading to data encryption, indicating a severe ransomware attack in progress.
- Multiple critical systems compromised including domain controller and file server, suggesting widespread infrastructure impact.
- Evidence of lateral movement and remote service exploitation, demonstrating sophisticated attack techniques and potential for further spread.

Type your question here

Total: 150 per page1 / 1



< Back

Credit Usage

TM-165789

Closed

Related Tasks

Evidence Search

View Query Results

Timeline

+ Add Endpoints

+ Add Evidence

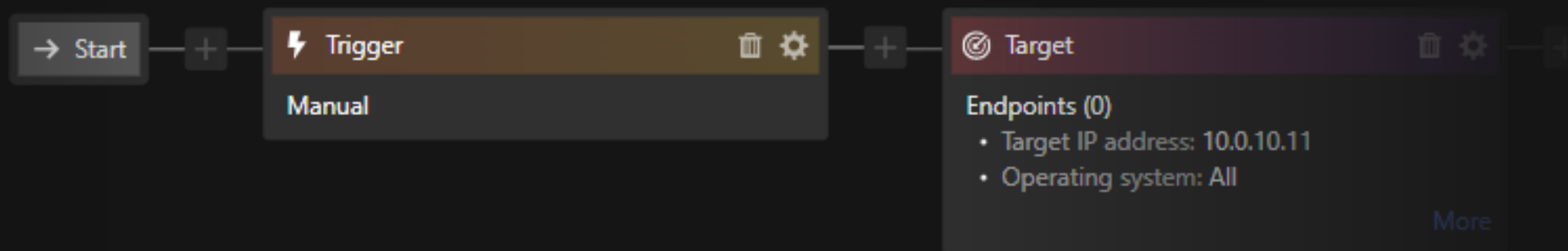
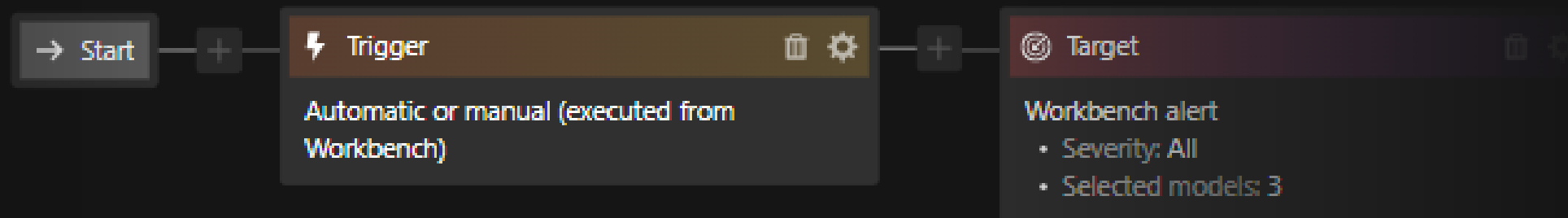
Endpoint name

Keyword

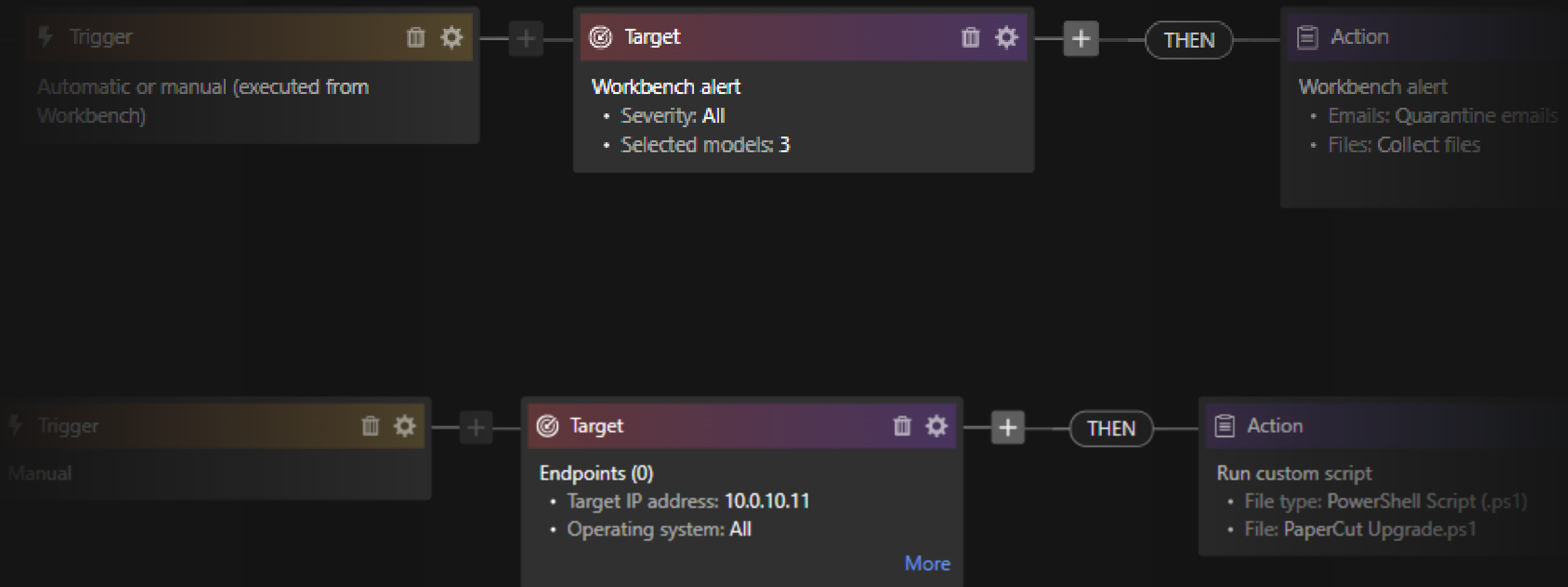
<input type="checkbox"/>	Endpoint name	Risk score	Agent GUID	IP address	Packages	Operation system	Last updated	↓
<input type="checkbox"/>	> DESKTOP-JONIS	73	c12417dd-6e5d-499a-9478-3f91fa5...	10.0.1.12	2	Windows 10 Enterprise	2024-12-06 02:36:04	
<input type="checkbox"/>	▼ DESKTOP-DIEGOS	79	50d0dd57-1b52-450f-b0cd-381c26...	10.0.1.11	2	Windows 10 Enterprise	2024-12-06 02:34:57	
	Package: IR-LQ-20241206-0000002-DESKTOP-DIEGOS	File size: 149.62 MB	Collection: Successful	Source: Response Management	Created: 2024-12-06 02:34:57			
	Package: IR-LQ-20241120-0000001-DESKTOP-DIEGOS	File size: 150.37 MB	Collection: Successful	Source: Response Management	Created: 2024-12-05 14:05:27			
<input type="checkbox"/>	▼ VMI-Printserver01	-	-	10.0.1.6	1	Windows Server 2019 Datacenter	2024-12-06 02:26:43	
	Package: VMI-Printserver01_2024-07-09-14-46-36.zip	File size: 107.71 MB	Collection: Successful	Source: IR Toolkit	Created: 2024-12-06 02:26:43			
<input type="checkbox"/>	▼ DESKTOP-ADELEV	-	-	10.0.1.13	1	Windows 10 Enterprise	2024-12-05 14:05:27	
	Package: DESKTOP-ADELEV_2024-07-09-15-00-49.zip	File size: 131.2 MB	Collection: Successful	Source: IR Toolkit	Created: 2024-12-05 14:05:27			

Forensics automates evidence collection,
assess risk, so you can *jumpstart your
investigations*

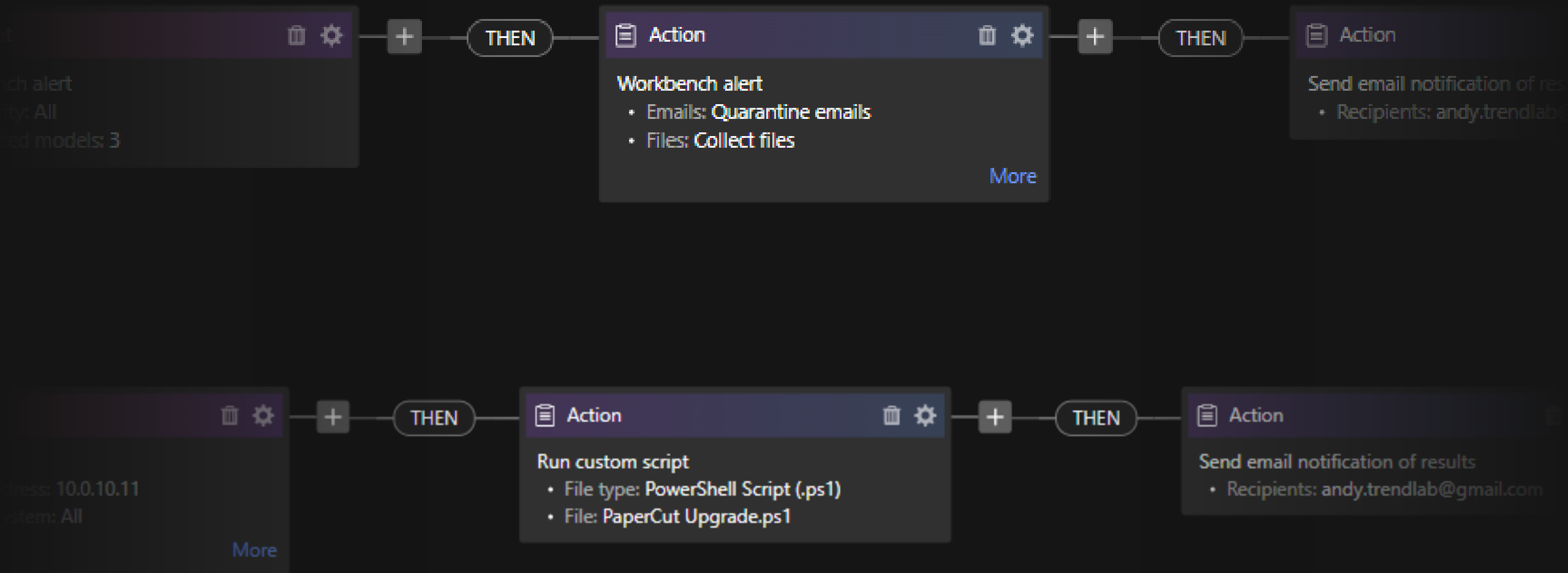
Automated playbooks— so you can work less, respond faster, and ***stop more threats.***



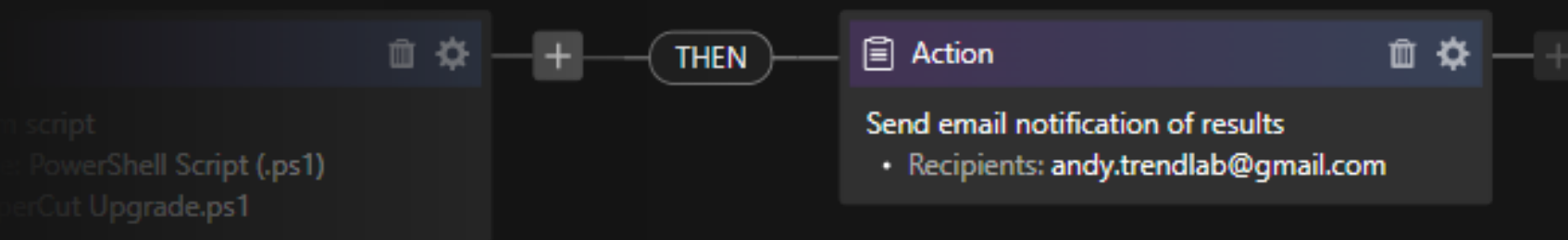
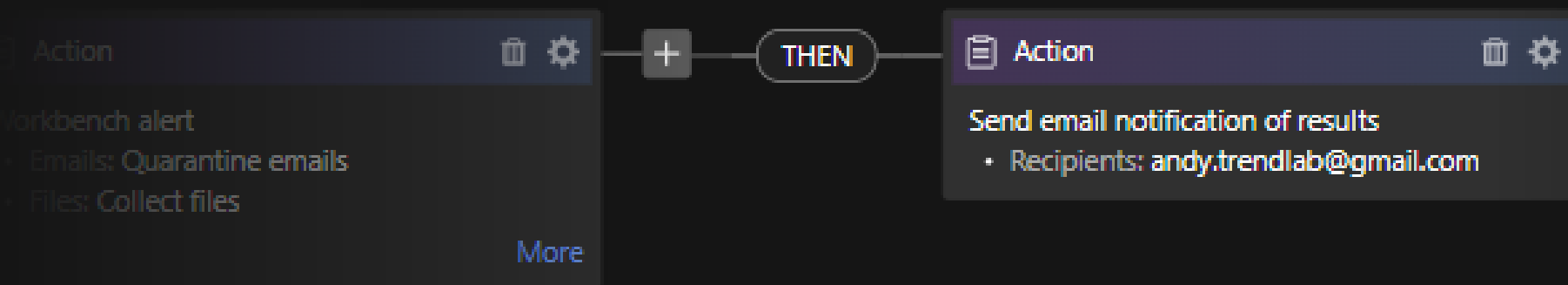
Automated playbooks— so you can work less, respond faster, and ***stop more threats.***



Automated playbooks— so you can work less, respond faster, and ***stop more threats.***



Automated playbooks— so you can work less, respond faster, and ***stop more threats.***



Cut through the noise and empower your SecOps to focus on what matters most – stopping threats before they surface and reducing risk.



Recognized by Gartner®

Magic Quadrant™ for Endpoint Protection Platforms (EPP)



Gartner, Magic Quadrant for Endpoint Protection Platforms, Evgeny Mirolyubov, Franz Hinner, et al., 23 September 2024

Magic Quadrant™ for Email Security Platforms (ESP)



Gartner, Magic Quadrant for Email Security Platforms, Max Taggett, Nikul Patel, et al., 16 December 2024

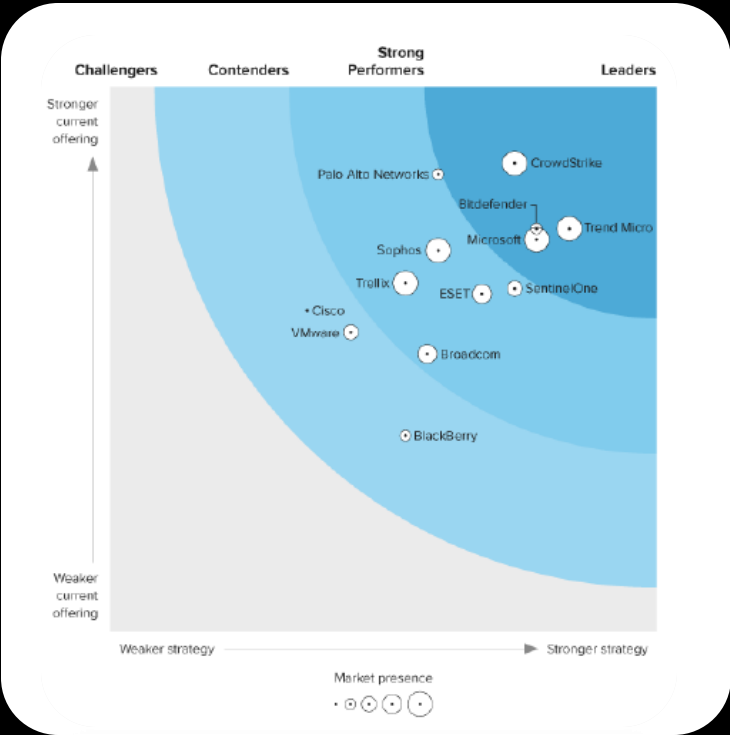
These graphics were published by Gartner, Inc. as part of larger research documents and should be evaluated in the context of the entire documents. The Gartner documents are available upon request from Trend Micro.

Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.

Strength Across the Enterprise

The Forrester Wave™:
Endpoint Security
Q4, 2023



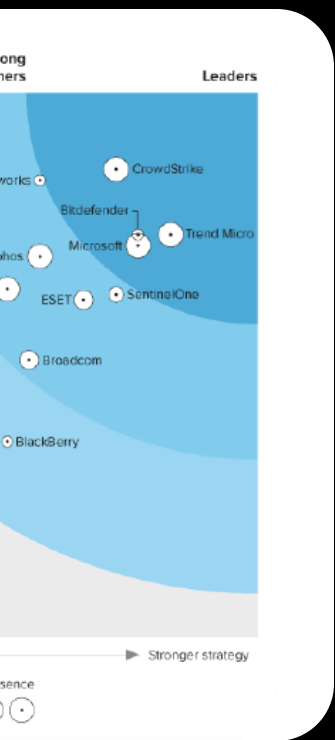
The Forrester Wave™: Network
Analysis And Visibility
Q2, 2023



The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and ForresterWave 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.

Strength Across the Enterprise

Wave :
Security
23



The Forrester Wave™ : Network
Analysis And Visibility
Q2, 2023



The Forrester Wave™ : Attack
Surface Management Solutions
Q3, 2024



100%

analytic coverage
for all major steps (16/16)

100%

analytic coverage in Linux
and macOS for all sub-steps

100%

analytic coverage in server
platform (Windows/Linux)
for all sub-steps

99%

analytic coverage
for all sub-steps (79/80)



“

The Trend Vision One platform afforded us the opportunity to **ingest all the information in one place** and allowed our cyber security team to **act on offenses and events across the board** without the need to cross borders between the different IT organizations.

Panasonic

Samer Mansour
Vice President, CISO
Panasonic North America





Trend Vision One[™] Network Security

Network Detection
and Response



Cyber Risk Exposure Management

Security Operations



Endpoint
Security



Cloud
Security



Network
Security



Email
Security



Identity
Security



AI
Security



Data
Security

Threat Intelligence

Services

→ **Detect the
unknown, protect
the unmanaged**

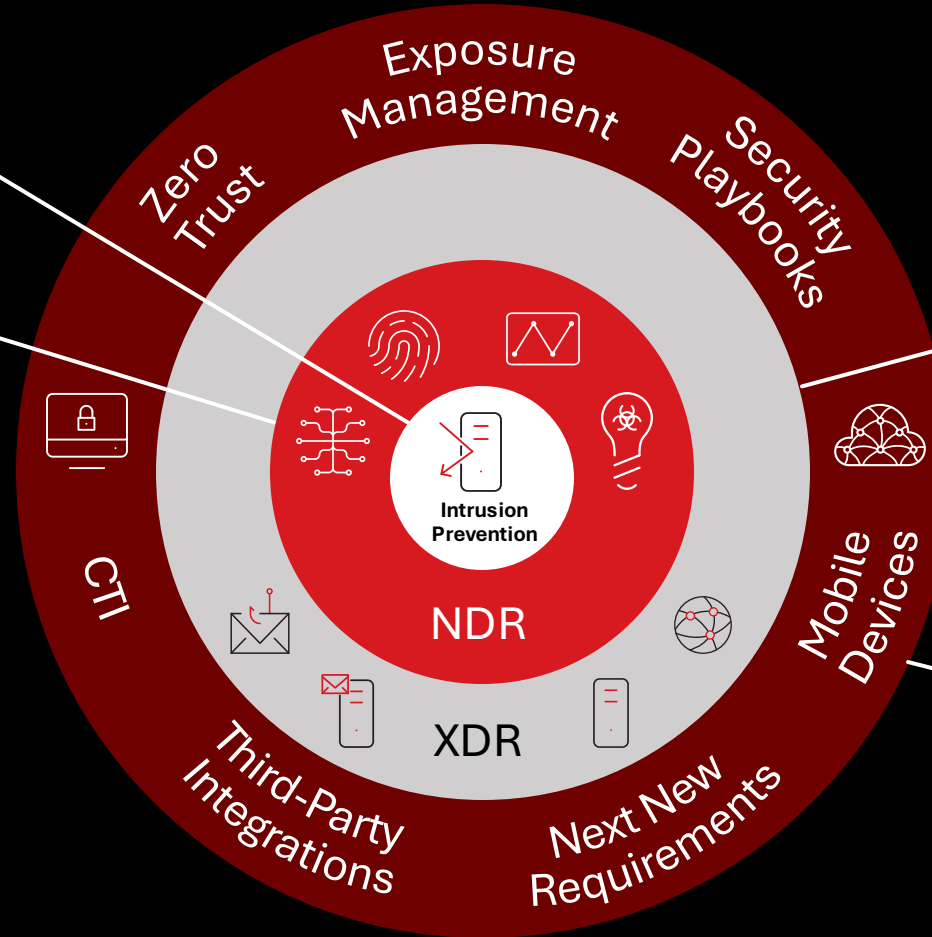
Converging technology

1 Prevention

2 Visibility into network traffic and unmanaged devices

3 Multilayered: Endpoint, Network, Cloud Workloads, and Email Fill the attack gaps that others miss

4 Trend Vision One™ Assess and prioritize risks and enhance security posture



Solution model

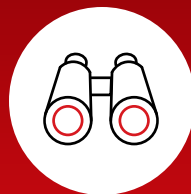
Trend Vision One™ Network Detection and Response



Accelerating protection

Network Detection and Response

Trend Vision One



Visibility



Automated
Remediation



Prioritization

From Network
to Endpoint

See everything,
miss nothing

Prioritize and
Mitigate Risks

Automatic
Defense Against
Zero Day Threats

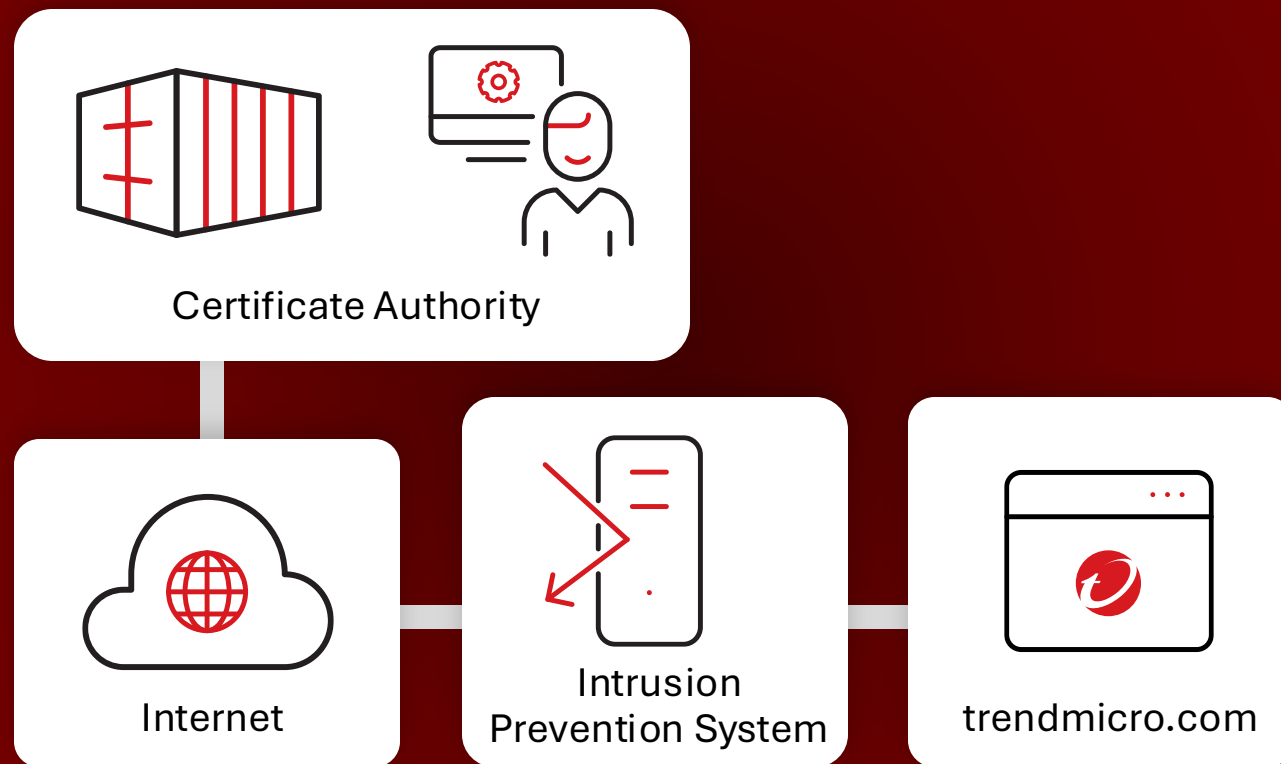
Powered by XDR and Cyber Risk Exposure Management

Comprehensive visibility

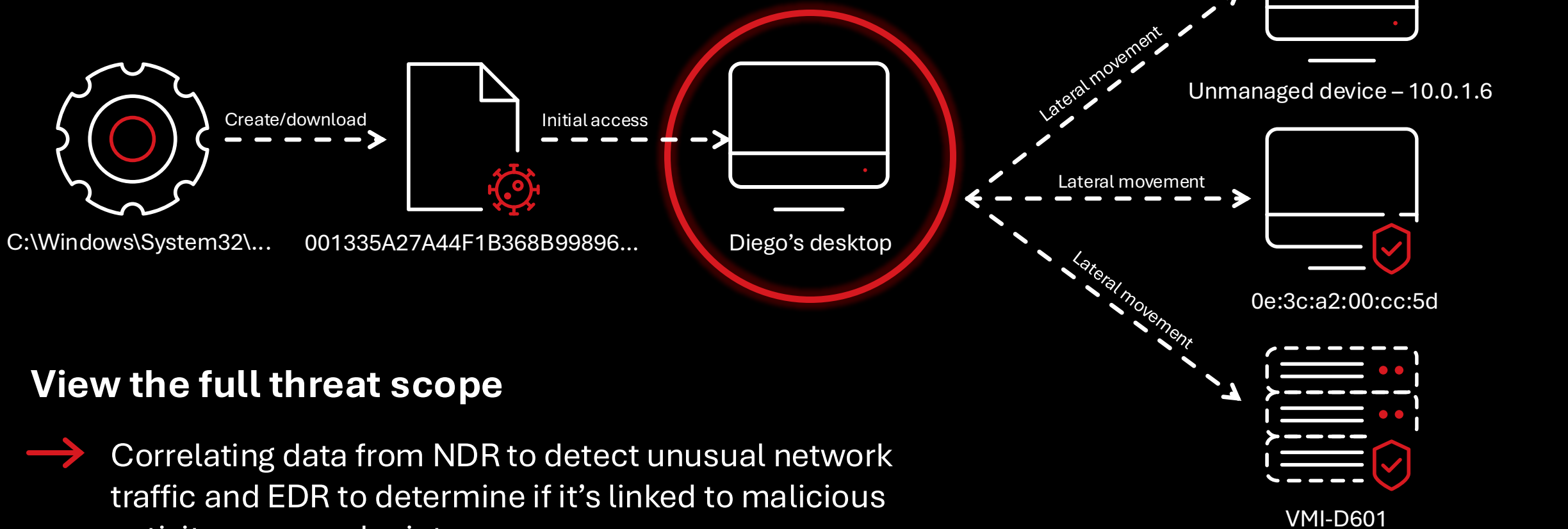
→ Transport Layer Security (TLS)

- Inbound and outbound TLS decryption
- Automated ACME certificate management
- Support advanced cipher suites
- (Advanced Encryption Standard, Rivest Cipher 4, Data Encryption Standard, Triple Data Encryption Standard)

Automated Certificate Management Environment



Cross-layer detection and response → Complete Visibility

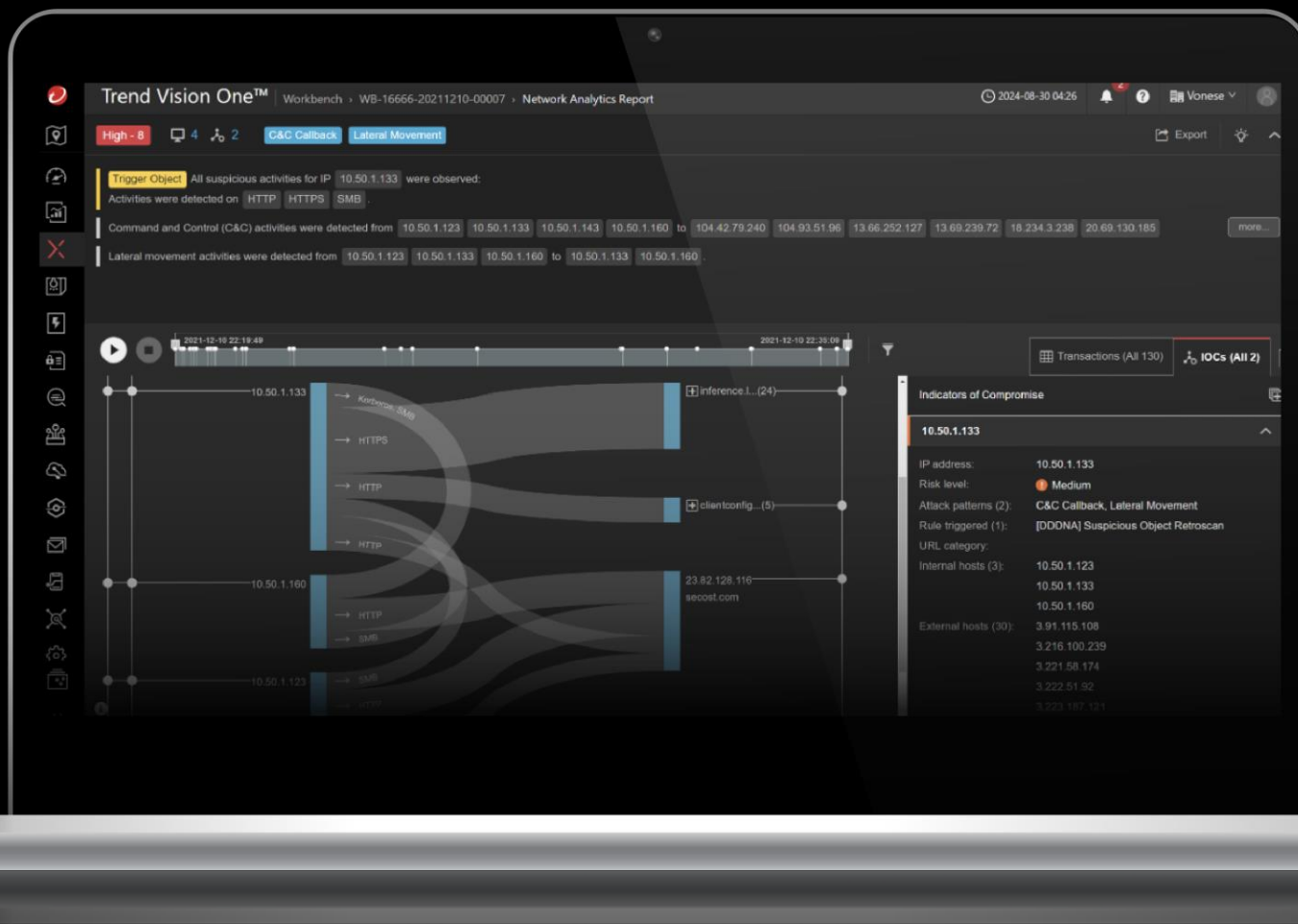


View the full threat scope

- Correlating data from NDR to detect unusual network traffic and EDR to determine if it's linked to malicious activity on an endpoint

Powered by XDR

- **Cross-layer XDR detection and correlation**
- **Network layer analytics report**
- **Leveraging Threat Intelligence for IOCs**
- **Threat investigation/hunting**
- **Remediation and investigation actions (manual/auto playbook)**

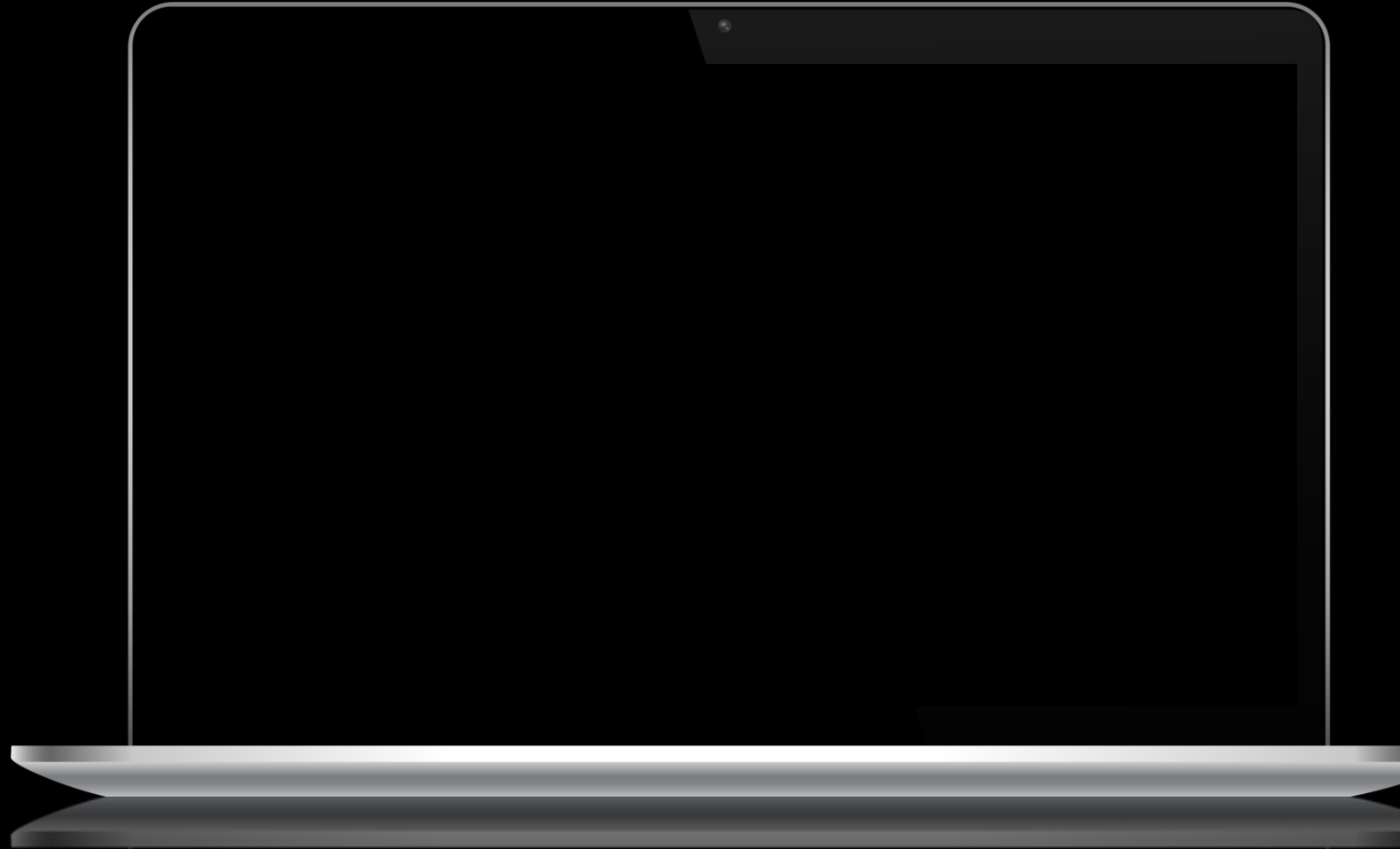


Automate, respond, and improve overall security posture

Network Detection and Response + Playbooks

Through XDR:

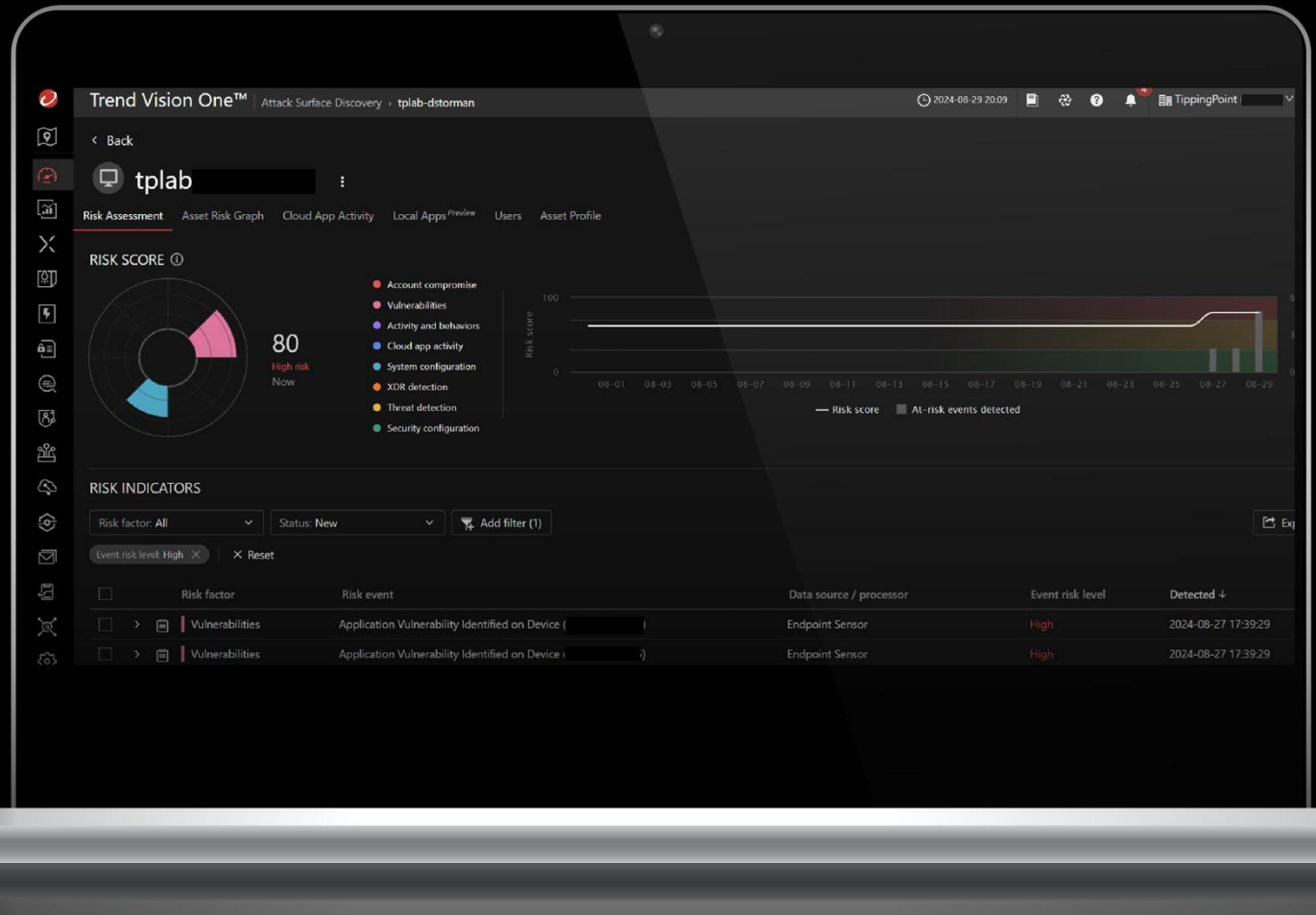
- Investigate incidents
- Set up and run playbooks
- Automatically detect and respond to risky events
- Enforce remediation action in real-time



Gain insights with Network Detection and Response

Enriched by Cyber Risk Exposure Management

- Proactively identify threats
- Unmanaged device discovery
- Risk assessment of the network



Identify unmanaged assets with Network Detection and Response

Enriched by Cyber Risk Exposure Management

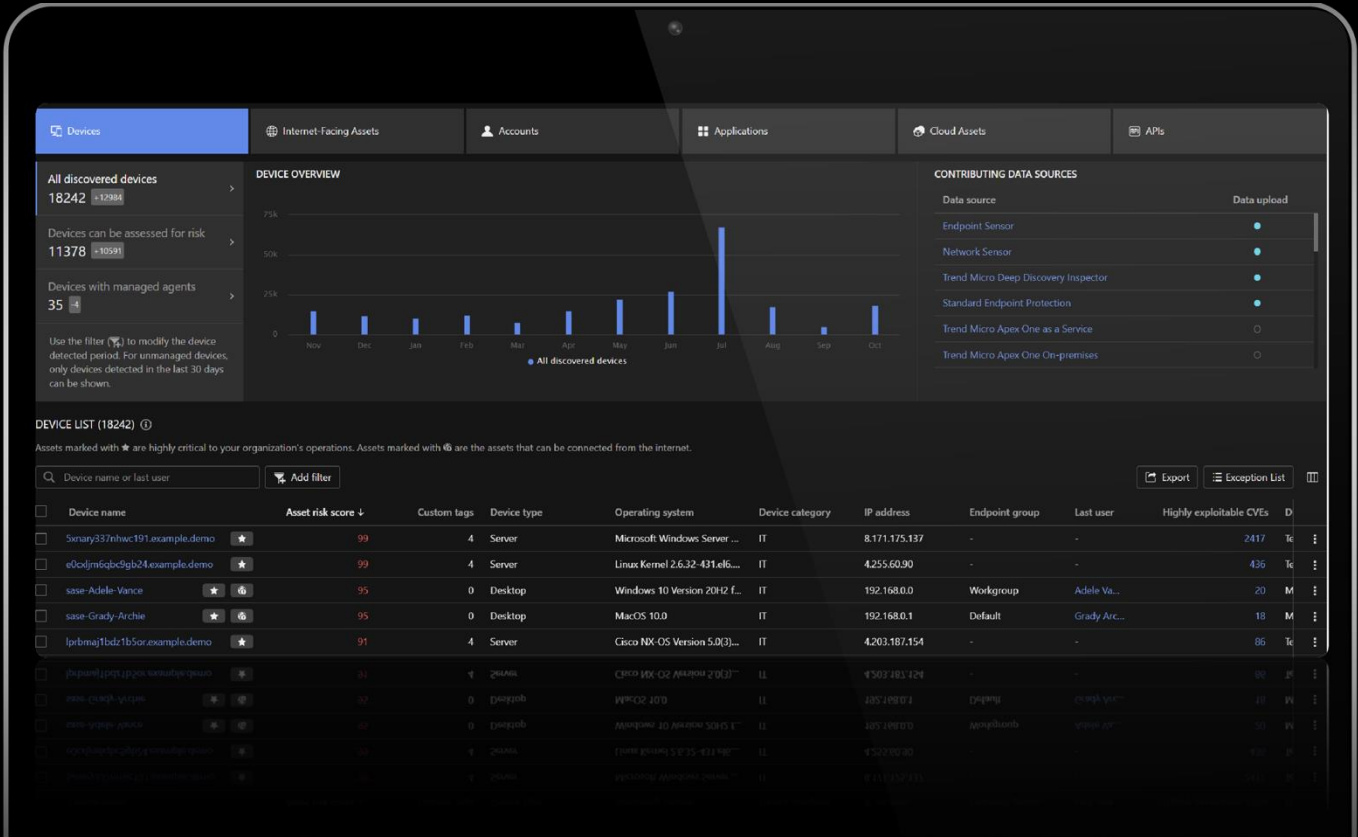
Integration



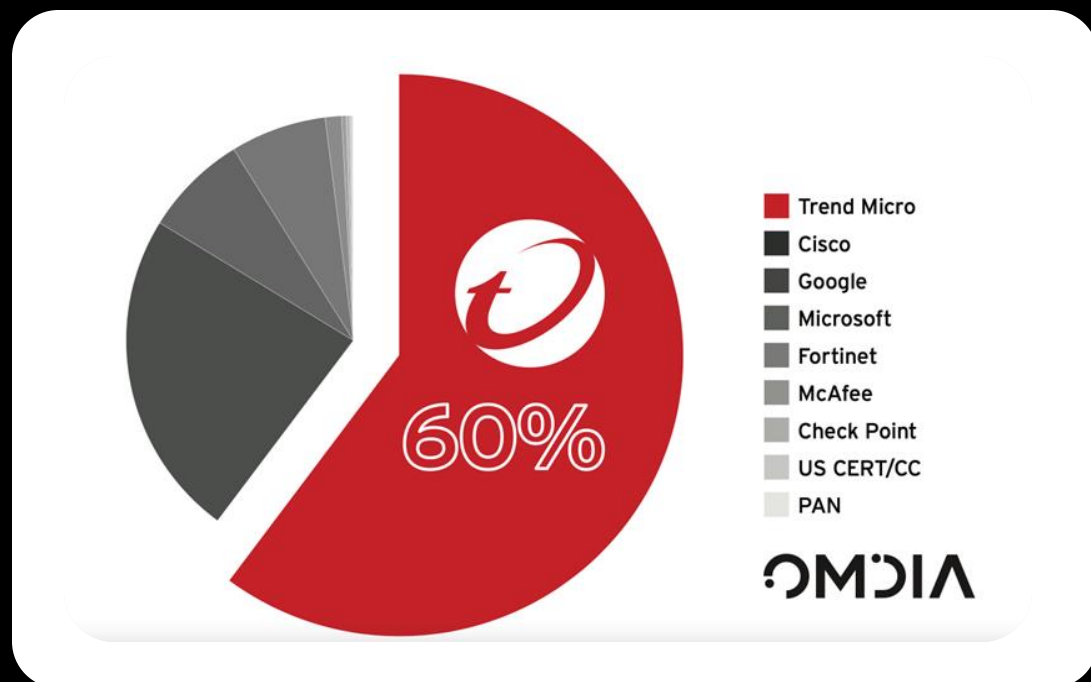
Correlation



Recommendation



Recognized threat research leadership



OMDIA REPORT:

#1 Public vulnerability disclosure market

A leader every year since 2007 — **2.5x more bugs** disclosed than anyone else

Source: Quantifying the Public Vulnerability Market, Omdia, June 2024



Trend Vision One™

Network Detection and Response

- Detect the unknown, protect the unmanaged
- Leave nothing uncovered with Network Detection and Response

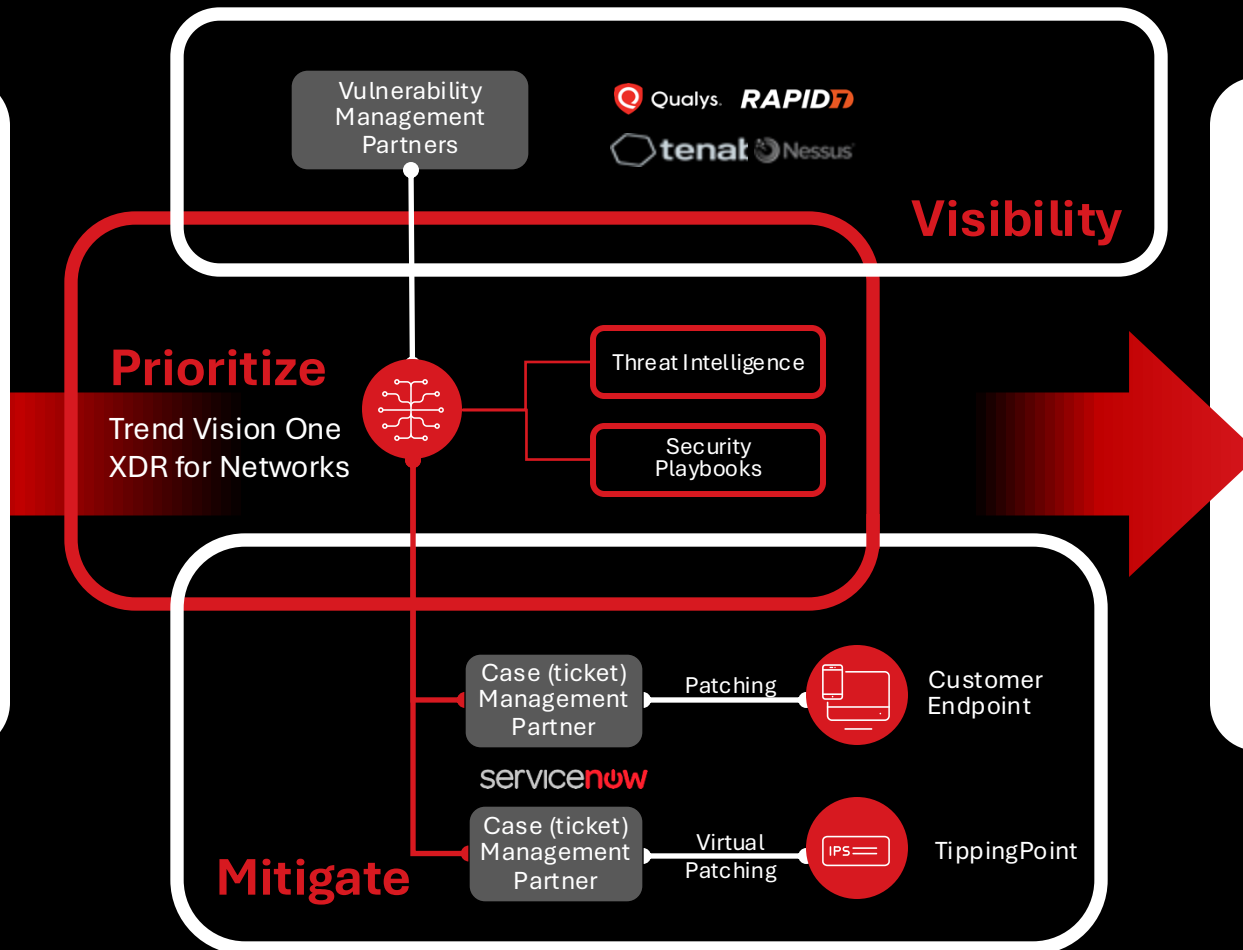
Customer success

A global pharmaceutical company

More than 24,000 employees — Inline NDR with mature SOC

Before

- IT silos
- No business process for vulnerabilities
- Monthly patch management



After

- Instant risk reduction
- Visibility into known and unknown threats
- Optimized operations
- Unified security tools



Seeing the complete picture — from servers, cloud, email, network to endpoints — is crucial to maintaining a healthy network. **Having access to all of this information in one portal really saves time.**



DEKALB COUNTY
SCHOOLS

Dekalb County School District
USA

Strength Across the Enterprise by Forrester

The Forrester Wave™:
Endpoint Security
Q4, 2023



The Forrester Wave™:
Attack Surface Management Solutions
Q3, 2024



Forrester does not endorse any company, product, brand, or service included in its research publications and does not advise any person to select the products or services of any company or brand based on the ratings included in such publications. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change. For more information, read about Forrester's objectivity here.

**Proactive security
starts here**