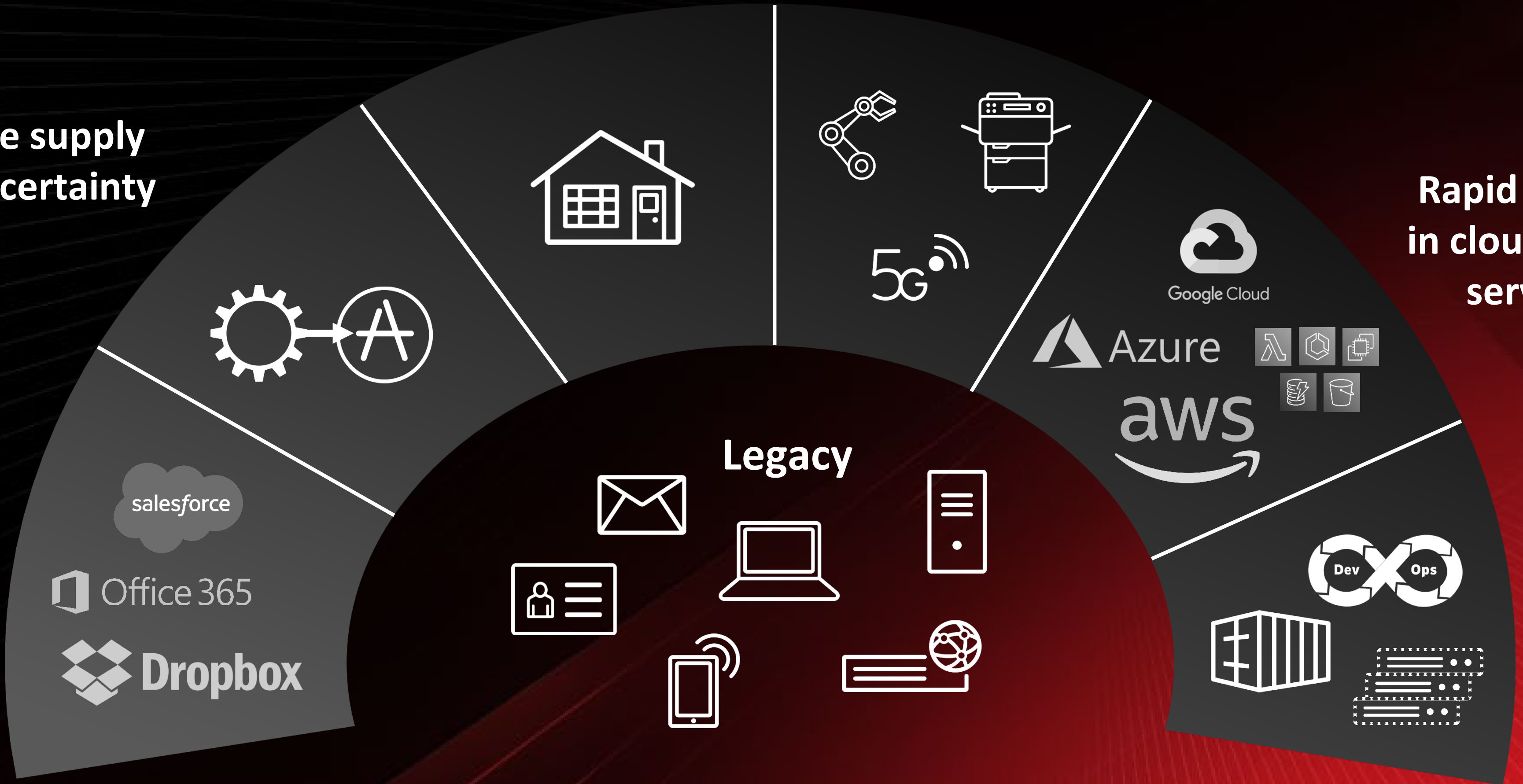
Journey Towards Discovery and Visibility with XDR

Noramiza Ayu Bt Bahrom

Snr Pre-Sales Consultant

Why are breaches still occurring and increasing at an accelerated rate?

A complex growing attack surface



Work-from-home

IT / OT convergence & 5G

Software supply chain uncertainty

Rapid growth in cloud native services

Massive growth in SaaS applications

Cloud native applications

Legacy

82 %

Of breaches, Identity compromise is a key element.

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

Threat actor evolution

Cyber Criminals

Extortion and BEC growing

Economic headwinds driving more crime

Increased specialization, targeting, customization

Nation State Actors

Disruption, destruction, IP theft

Tolerating and harboring criminals

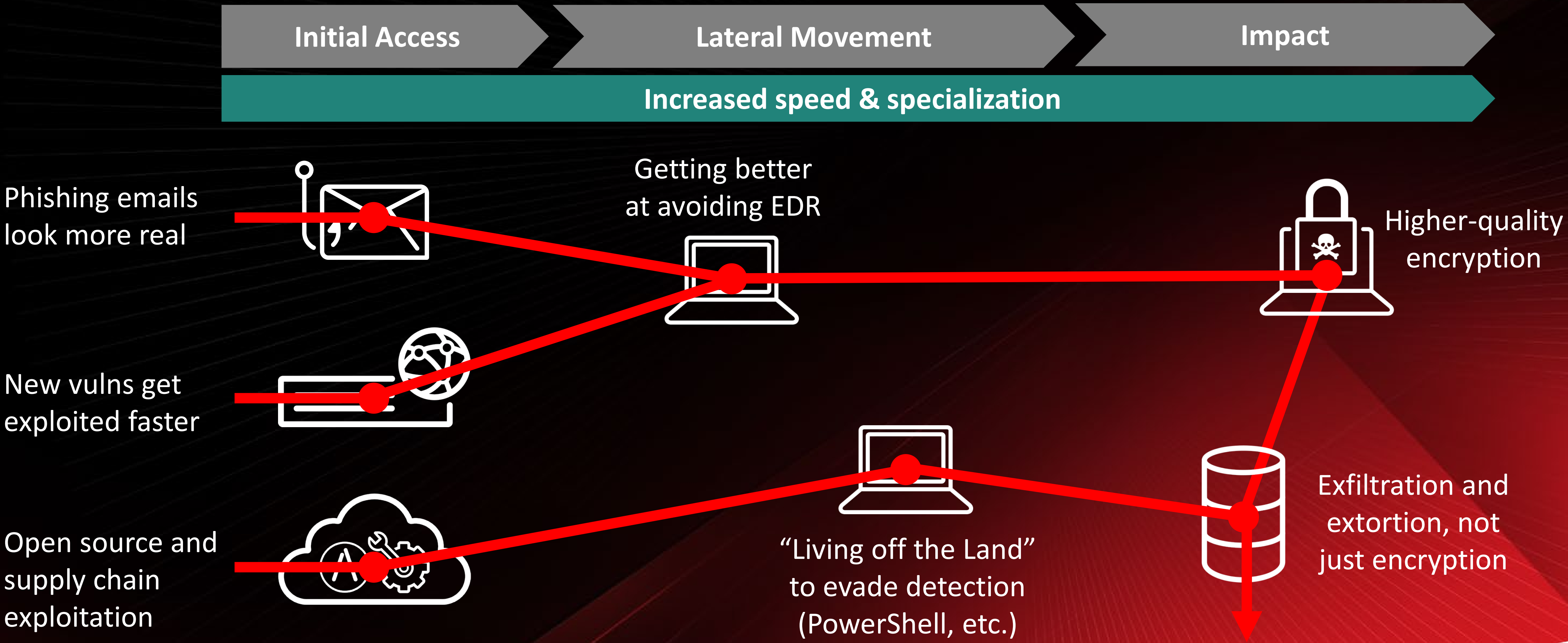
Some “federal” regimes profit-driven e.g., North Korea

Insiders

Economic pain will drive increased misbehavior

Cyber-criminals paying insiders for access

Threat activity evolution



Initial Access

Lateral Movement

Impact

Increased speed & specialization

Phishing emails look more real

New vulns get exploited faster

Open source and supply chain exploitation

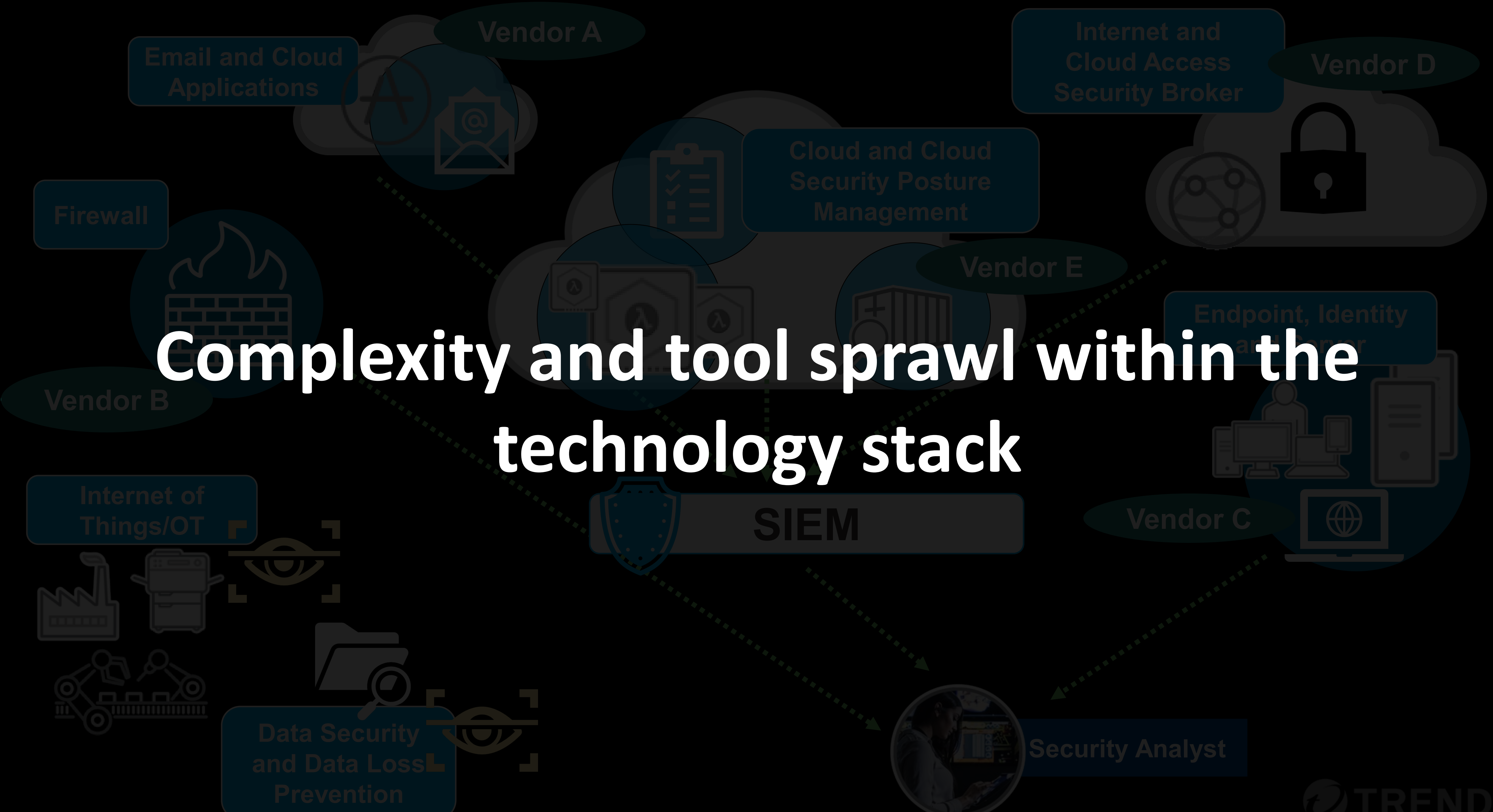
Getting better at avoiding EDR

“Living off the Land” to evade detection (PowerShell, etc.)

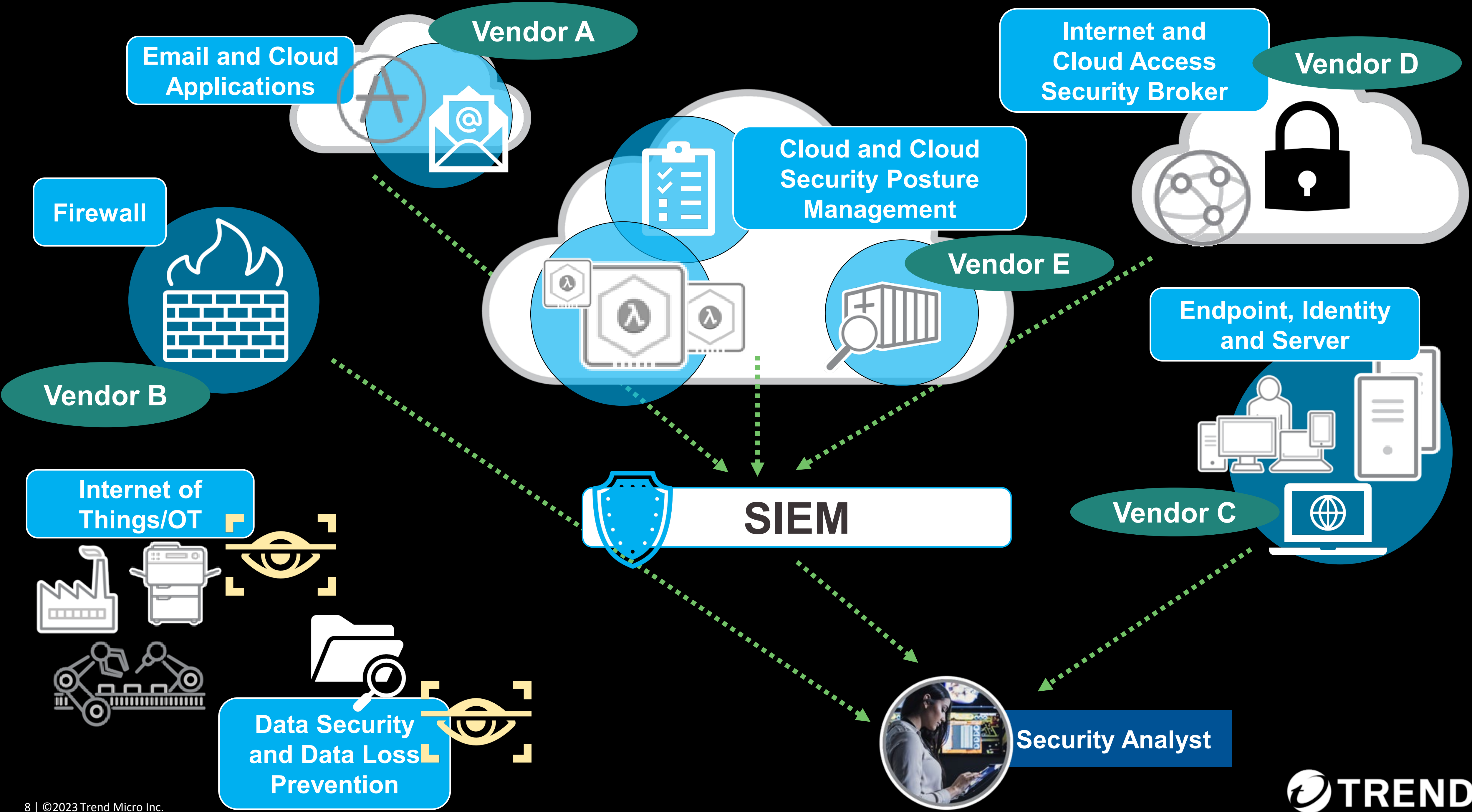
Higher-quality encryption

Exfiltration and extortion, not just encryption

Complexity and tool sprawl within the technology stack



Vendor A
Email and Cloud Applications
Internet and Cloud Access Security Broker
Vendor D
Cloud and Cloud Security Posture Management
Firewall
Vendor E
Endpoint, Identity and Server
Vendor B
Internet of Things/OT
SIEM
Vendor C
Data Security and Data Loss Prevention
Security Analyst



Email and Cloud Applications

Vendor A

Internet and Cloud Access Security Broker

Vendor D

Cloud and Cloud Security Posture Management

Vendor E

Firewall

Vendor B

Endpoint, Identity and Server

Vendor C

SIEM

Internet of Things/OT

Data Security and Data Loss Prevention

Security Analyst

Tool sprawl enables attackers

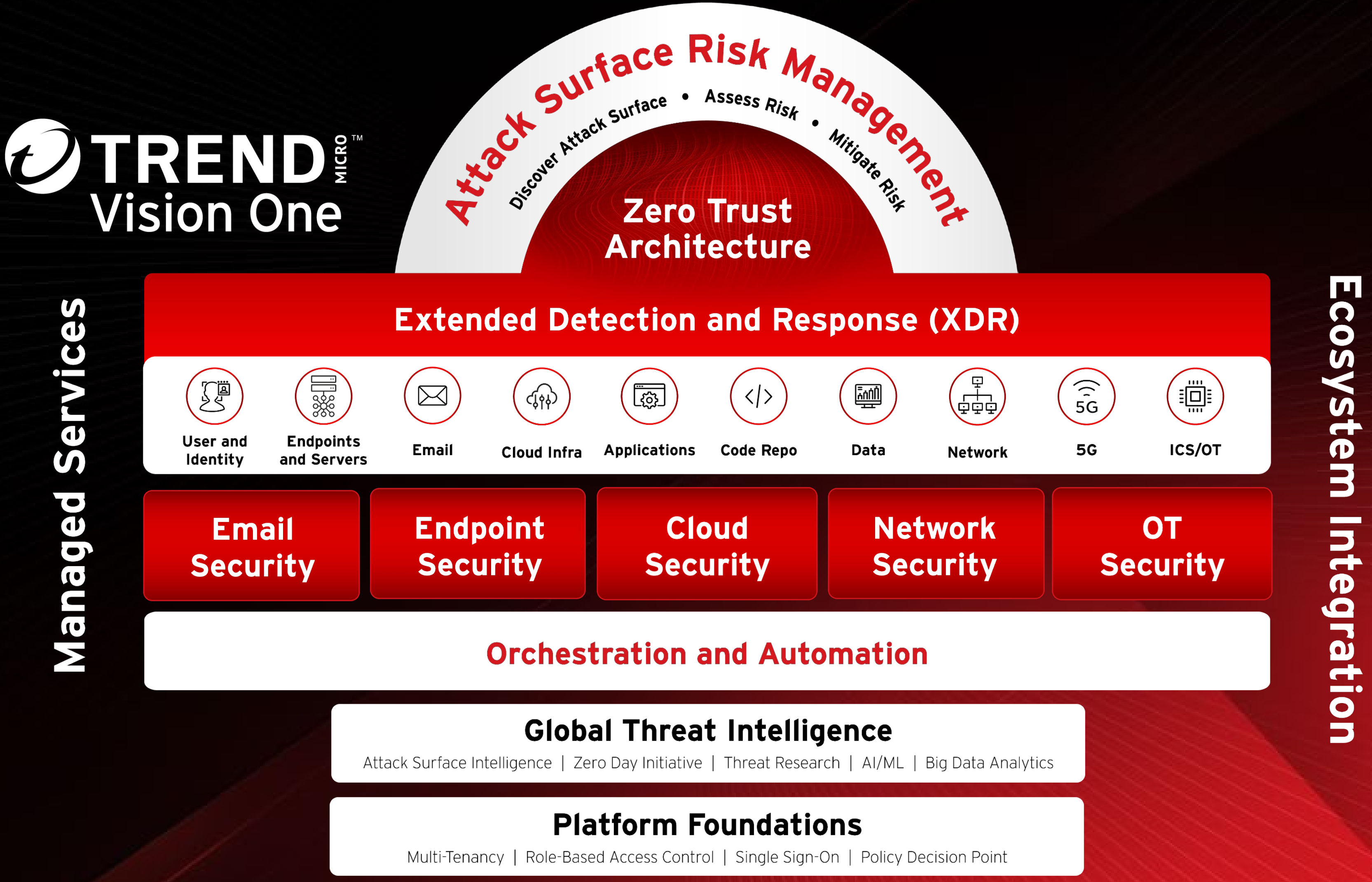
Proliferating silos from point solution sprawl

Missing visibility across security layers

Inadequate hybrid IT environment compatibility

Trend Vision One Approach

Shift from Security Tools to a Cybersecurity Platform



TREND MICRO Vision One

Managed Services

Attack Surface Risk Management

Discover Attack Surface • Assess Risk • Mitigate Risk

Zero Trust Architecture

Extended Detection and Response (XDR)

User and Identity | Endpoints and Servers | Email | Cloud Infra | Applications | Code Repo | Data | Network | 5G | ICS/OT

Email Security | Endpoint Security | Cloud Security | Network Security | OT Security

Orchestration and Automation

Global Threat Intelligence

Attack Surface Intelligence | Zero Day Initiative | Threat Research | AI/ML | Big Data Analytics

Platform Foundations

Multi-Tenancy | Role-Based Access Control | Single Sign-On | Policy Decision Point

Ecosystem Integration

User and Identity

Endpoints and Servers

Email

Cloud Infra

Applications

Code Repo

Data

Network

5G

ICS/OT

Email Security

Endpoint Security

Cloud Security

User and Identity | Endpoints and Servers | Email | Cloud Infra | Applications | Code Repo | Data | Network | 5G | ICS/OT

Email Security

Endpoin Security

Cloud Security

Network Security

OT Security

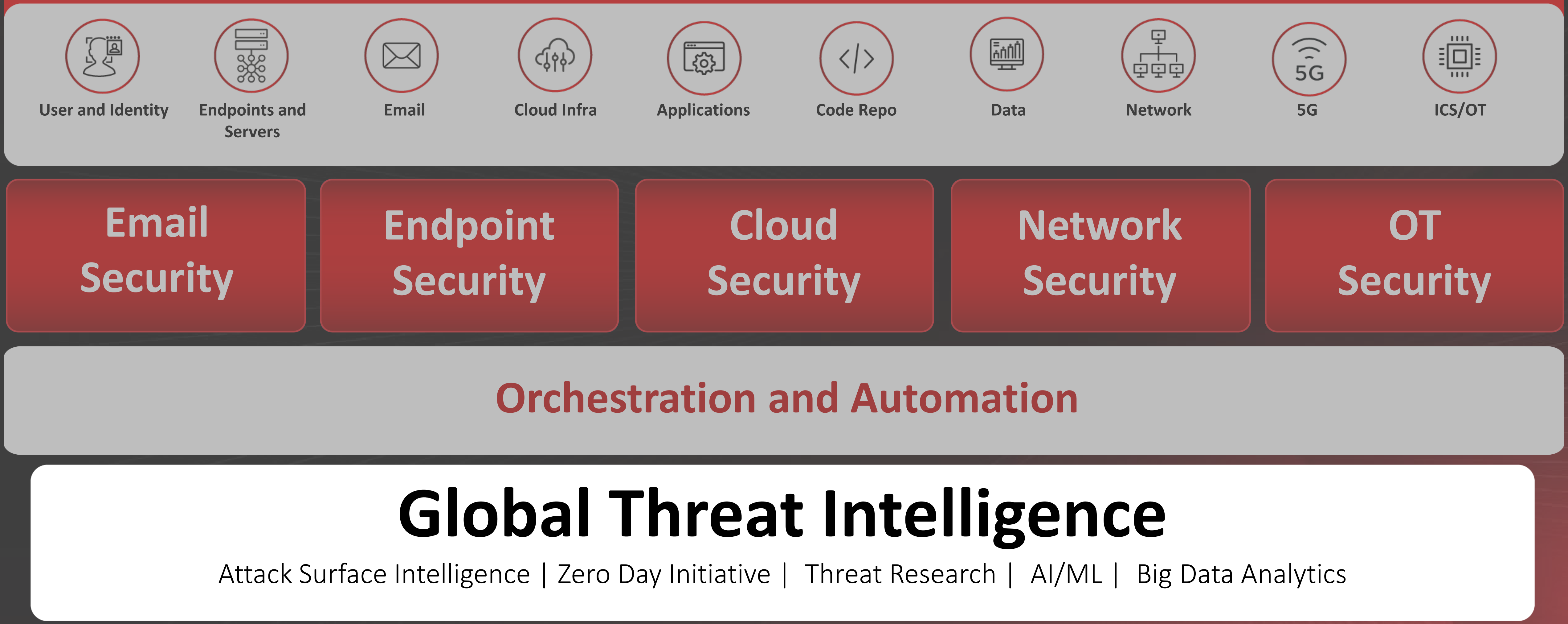
TREND MICRO

User and Identity | Endpoints and Servers | Email | Cloud Infra | Applications | Code Repo | Data | Network | 5G | ICS/OT

Cloud Security

Network Security

OT Security



User and Identity | Endpoints and Servers | Email | Cloud Infra | Applications | Code Repo | Data | Network | 5G | ICS/OT

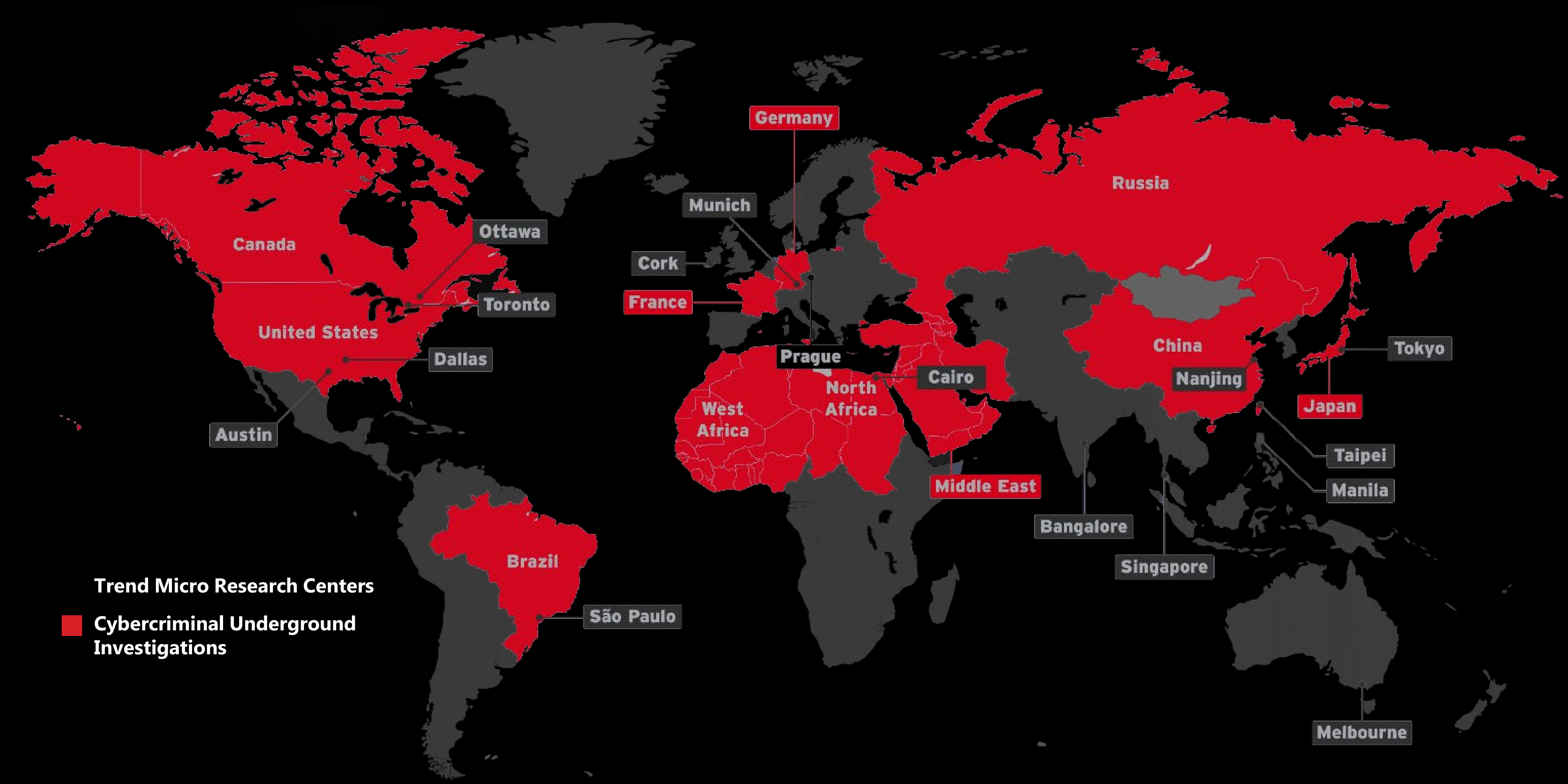
Email Security | Endpoint Security | Cloud Security | Network Security | OT Security

Orchestration and Automation

Global Threat Intelligence

Attack Surface Intelligence | Zero Day Initiative | Threat Research | AI/ML | Big Data Analytics

Threat Intel powered by Global Research



Trend Micro Research Centers

🟥 Cybercriminal Underground Investigations

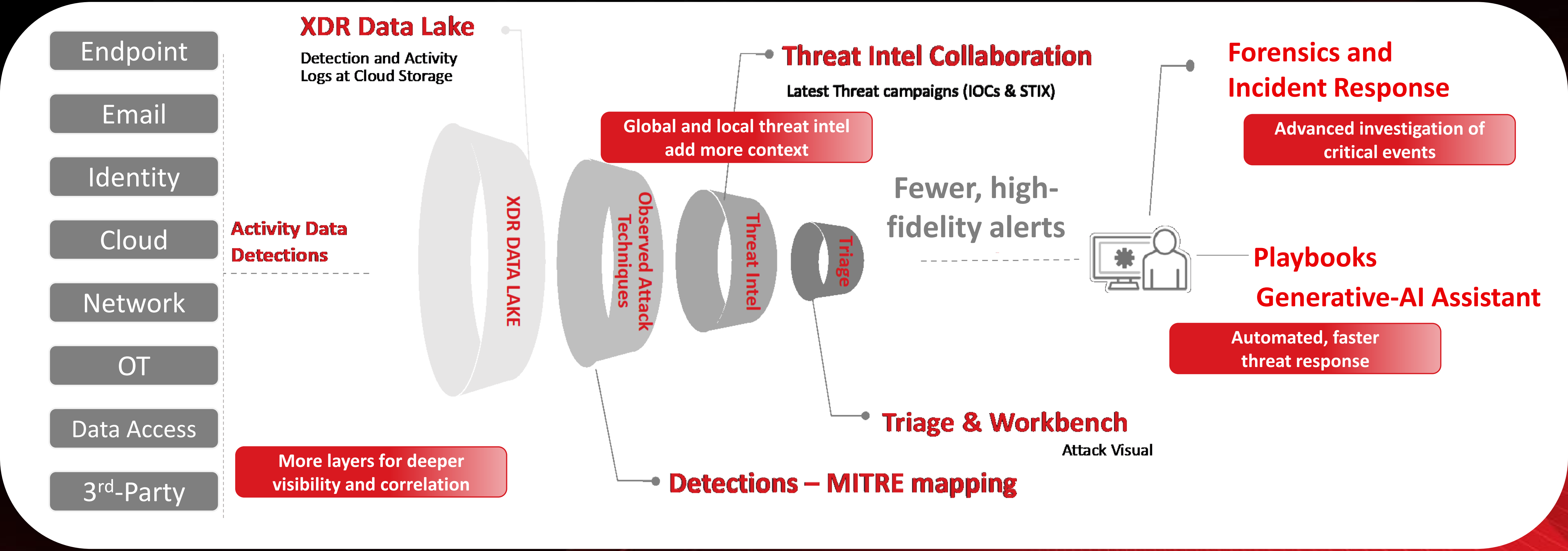
Global Threat Intel fueled by AI/ML and ***world leading 250 million sensors deployed***

TREND MICRO™

Stop Adversaries Faster

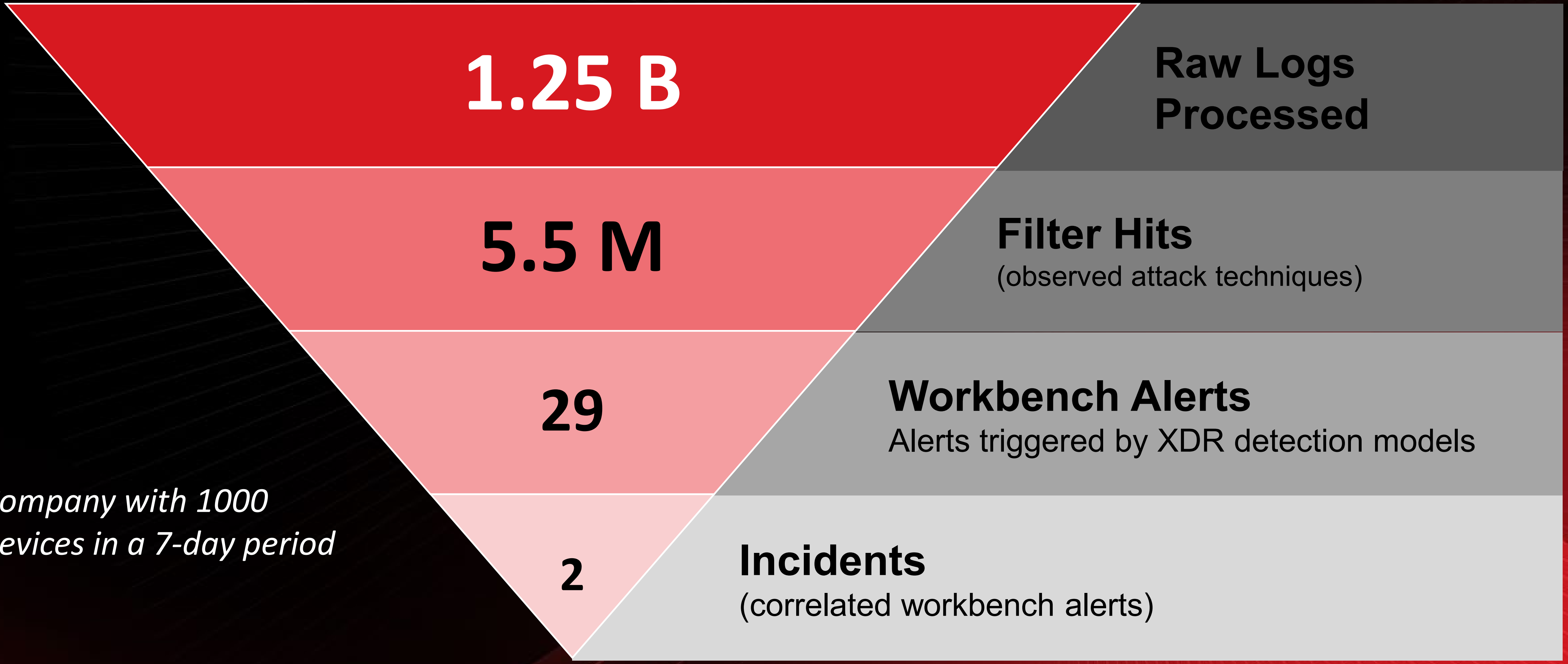
XDR

Cross-Layer XDR with Hybrid IT Environment Support



Endpoint
Email
Identity
Cloud
Network
OT
Data Access
3rd-Party
XDR Data Lake
Detection and Activity Logs at Cloud Storage
Activity Data
Detections
More layers for deeper visibility and correlation
XDR DATA LAKE
Observed Attack Techniques
Threat Intel
Triage
Threat Intel Collaboration
Latest Threat campaigns (IOCs & STIX)
Global and local threat intel add more context
Fewer, high-fidelity alerts
Forensics and Incident Response
Advanced investigation of critical events
Playbooks
Generative-AI Assistant
Automated, faster threat response
Triage & Workbench
Attack Visual
Detections – MITRE mapping

Minimize alert fatigue with **high confidence detections**



1.25 B	**Raw Logs Processed**
5.5 M	**Filter Hits** (observed attack techniques)
29	**Workbench Alerts** Alerts triggered by XDR detection models
2	**Incidents** (correlated workbench alerts)

Company with 1000 devices in a 7-day period

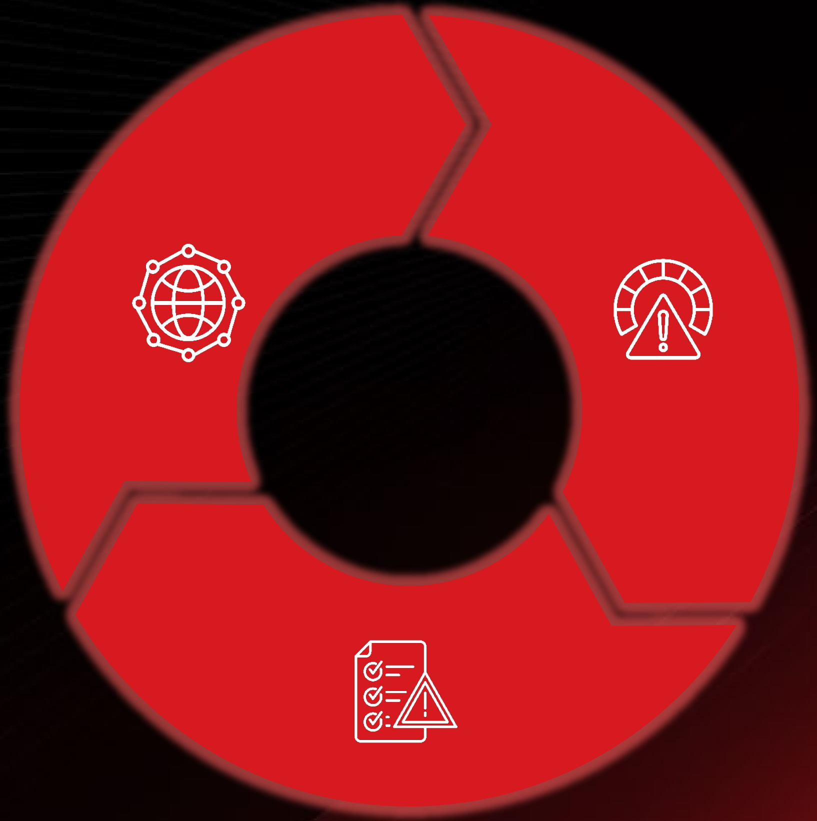
Trend Micro Security Analytics Engine (SAE), 2022

TREND MICRO™

Take Charge of Cyber Risk

Attack Surface Risk Management

Proactive Security | Attack Surface Risk Management

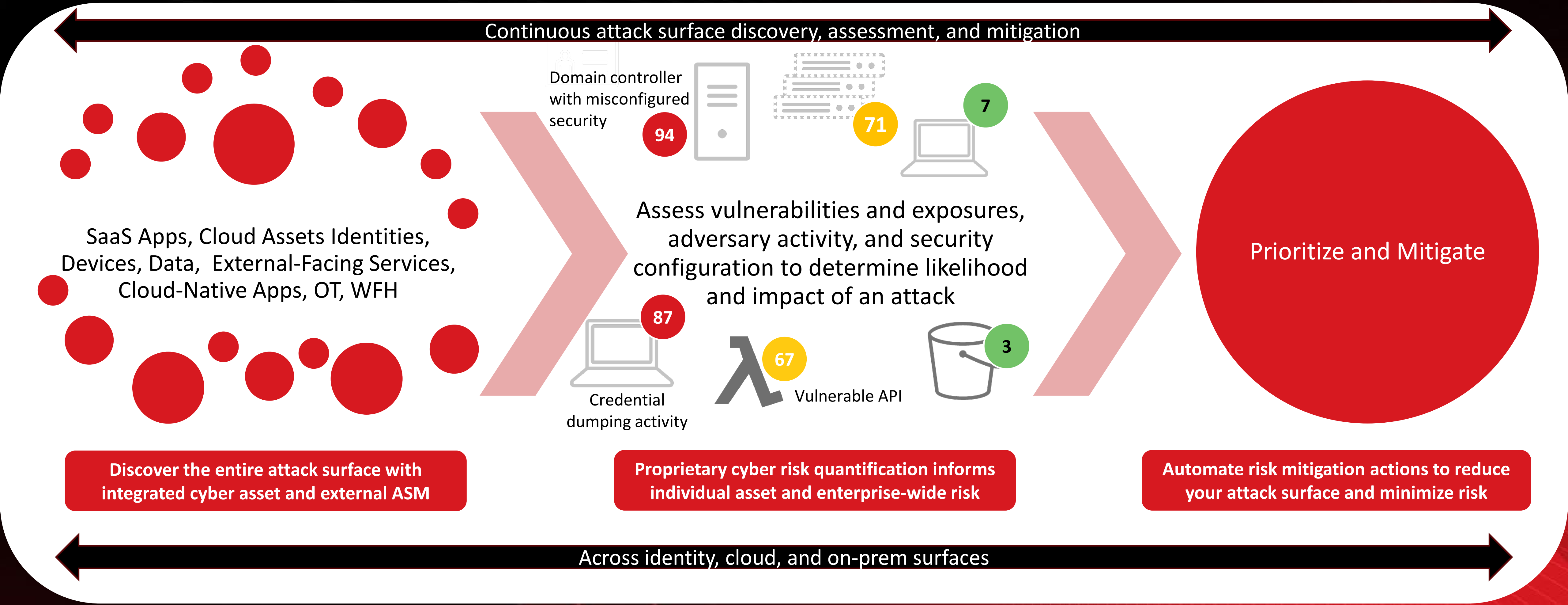


Discover Attack Surface

Assess & Prioritize Risk

Mitigate Risk

Proactive Security | Attack Surface Risk Management



Continuous attack surface discovery, assessment, and mitigation

SaaS Apps, Cloud Assets Identities, Devices, Data, External-Facing Services, Cloud-Native Apps, OT, WFH

Domain controller with misconfigured security

Assess vulnerabilities and exposures, adversary activity, and security configuration to determine likelihood and impact of an attack

Credential dumping activity

Vulnerable API

Prioritize and Mitigate

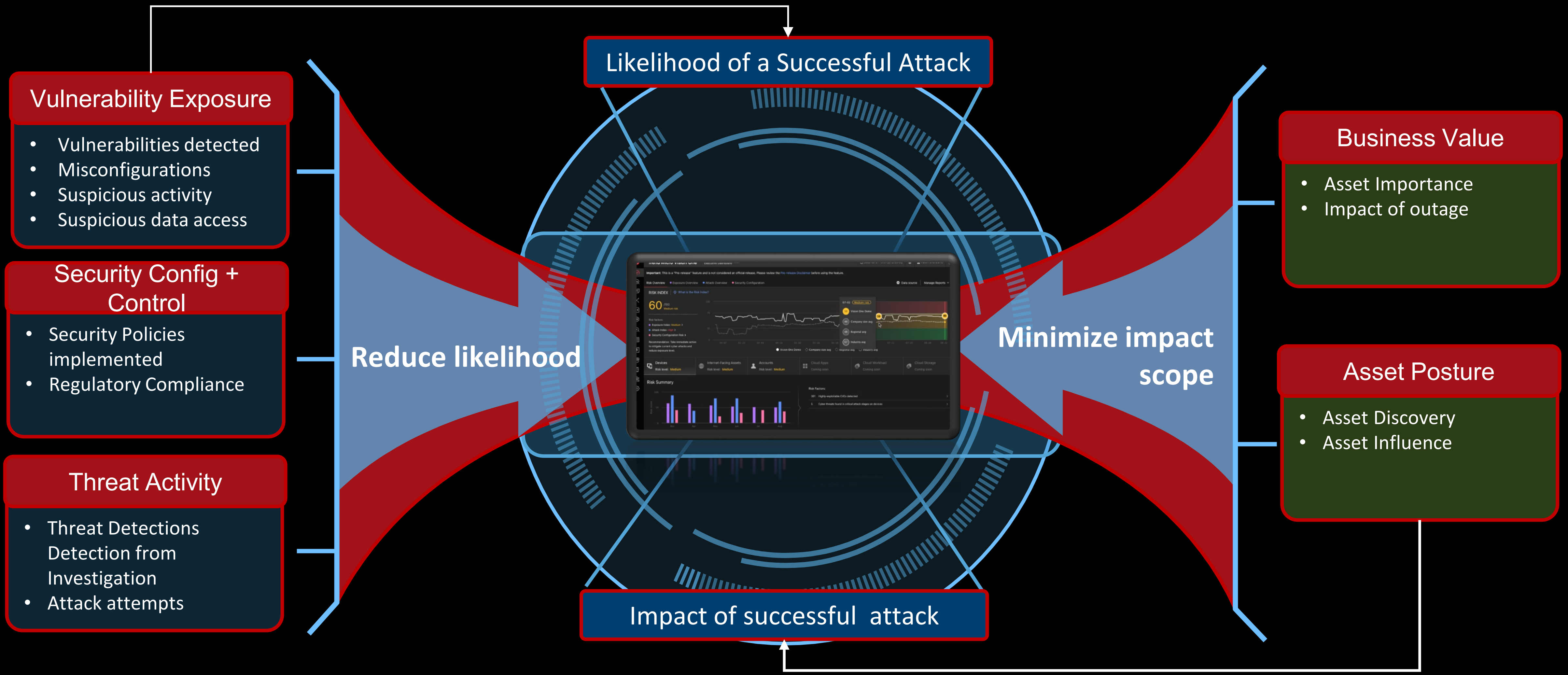
Discover the entire attack surface with integrated cyber asset and external ASM

Proprietary cyber risk quantification informs individual asset and enterprise-wide risk

Automate risk mitigation actions to reduce your attack surface and minimize risk

Across identity, cloud, and on-prem surfaces

Continuously Assess Risk | Attack Surface Risk Management



Vulnerability Exposure

- Vulnerabilities detected
- Misconfigurations
- Suspicious activity
- Suspicious data access

Security Config + Control

- Security Policies implemented
- Regulatory Compliance

Threat Activity

- Threat Detections Detection from Investigation
- Attack attempts

Reduce likelihood

Likelihood of a Successful Attack

Impact of successful attack

Minimize impact scope

Business Value

- Asset Importance
- Impact of outage

Asset Posture

- Asset Discovery
- Asset Influence

Important: This is a "Pre-release" feature and is not considered an official release. Please review the Pre-release Disclaimer before using the feature.

Risk Overview · Exposure Overview · Attack Overview · Security Configuration · Data source · Manage Reports

RISK INDEX · What is the Risk Index?

60 /100 Medium risk

Risk factors:
- Exposure Index: Medium
- Attack Index: High
- Security Configuration Risk

Recommendation: Take immediate action to mitigate current cyber attacks and reduce exposure level.

07-02 Medium risk: 59 Vision One Demo · 48 Company size avg · 48 Regional avg · 57 Industry avg

Devices – Risk level: Medium · Internet-Facing Assets – Risk level: Medium · Accounts – Risk level: Medium · Cloud Apps – Coming soon · Cloud Workload – Coming soon · Cloud Storage – Coming soon

Risk Summary

Risk Factors:
- 381 Highly-exploitable CVEs detected
- 5 Cyber threats found in critical attack stages on devices

Security Automation and Orchestration

Swiftly address unpatched vulnerabilities, exposed accounts, & misconfigurations

Deploy response actions across multiple security layers when a threat alert is triggered

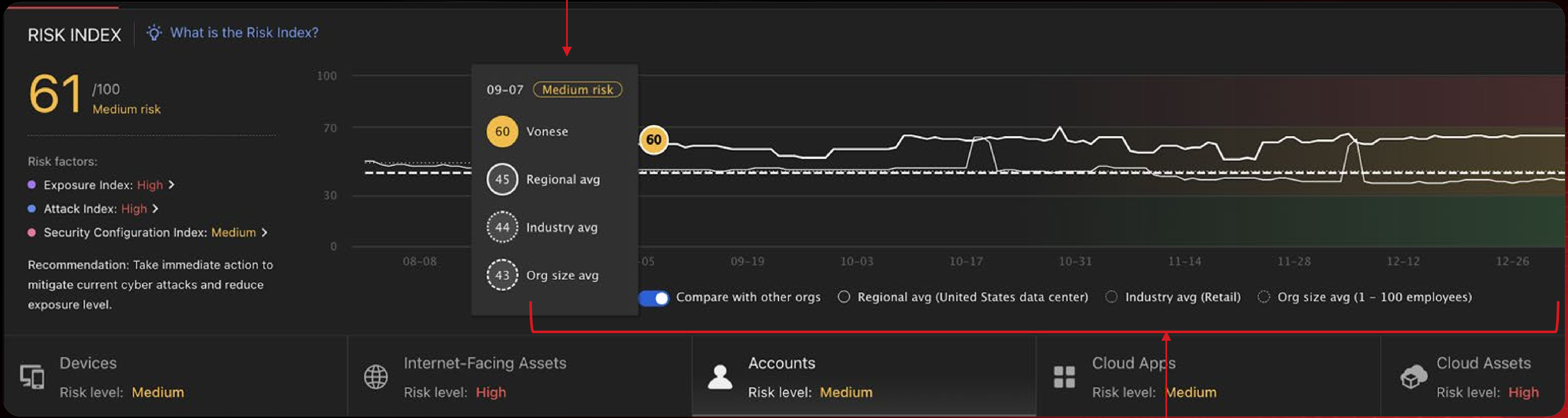
Improve mean-time-to-detect, respond, remediate, and contain

Automate dynamic remote access control

Collect forensic evidence immediately

Centralized Reporting and Benchmarking

Benchmark Comparisons



RISK INDEX | What is the Risk Index?

61 /100
Medium risk

Risk factors:

- Exposure Index: High >
- Attack Index: High >
- Security Configuration Index: Medium >

Recommendation: Take immediate action to mitigate current cyber attacks and reduce exposure level.

09-07 Medium risk

60	Vonese
45	Regional avg
44	Industry avg
43	Org size avg

Compare with other orgs ○ Regional avg (United States data center) ○ Industry avg (Retail) ○ Org size avg (1 – 100 employees)

Devices	Risk level: Medium
Internet-Facing Assets	Risk level: High
Accounts	Risk level: Medium
Cloud Apps	Risk level: Medium
Cloud Assets	Risk level: High

Risk Levels Over Time

Purpose Built Dashboards for All User Types

*"I want to **quickly verify** if an event is an incident and gauge its **severity** on my monitoring console."*

[Active Monitoring]
SOC Analyst I

*"I want to quickly get an **overview of the incident**, including its **scope, timeline, and impact**."*

[Forensic Analysis]
Incident Responder

*"What is our **Cybersecurity Risk Exposure**? What have we done to limit the exposure?*

Chief Information
Security Officer

Job Duty and Security Knowledge Level

Triages security alerts, monitor health of security sensors, collect data & context necessary to initiate response.

100% Monitor

Security Knowledge Level:
Medium

Primary tasks are **policy definition** and **incident investigation, performing dive-dive incident analysis** by correlating data from various resources.

50% Monitor

Security Knowledge Level:
Expert

Leads cybersecurity strategy, ensures it's **aligned with business strategy & objectives**; helps communicates strategy & progress across the board and key leaders.

30% Monitor

Security Knowledge Level:
High

Tools Used

System and Network Management Consoles, XDR Workbench, Operations Dashboard, Security Configuration and Control Dashboard

XDR Workbench, Search App, Threat Intelligence, Forensic App, Security Playbooks, Operations Dashboard, Attack Overview

Executive Dashboard (Risk Index, Security Posture Status), Automated Risk and Compliance Reports, Attack Surface Exposure Overview

Greater Peace of Mind with Expert Services

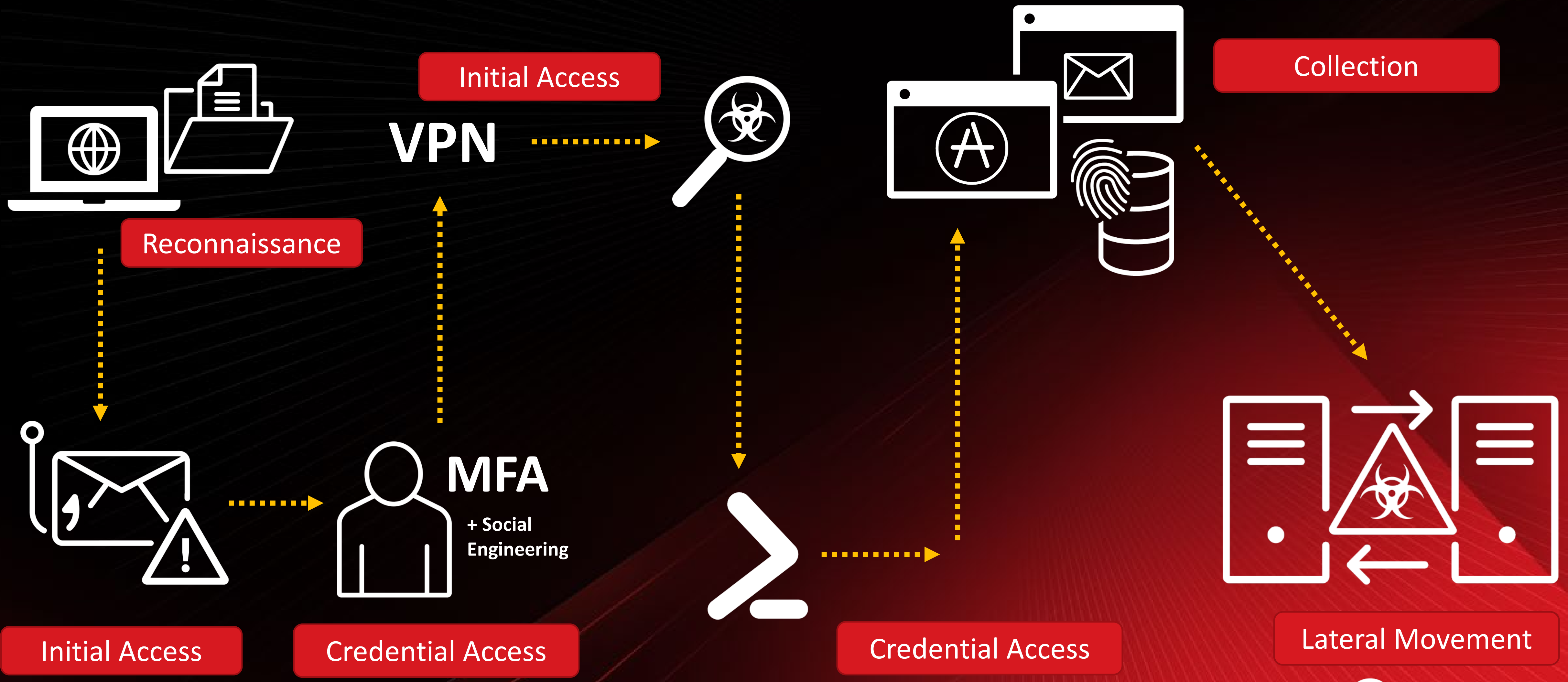
Address skills shortage and augment security operations with 24/7 Managed EDR and XDR

Build resilient strategies with Red Teaming and Incident Response (IR) services

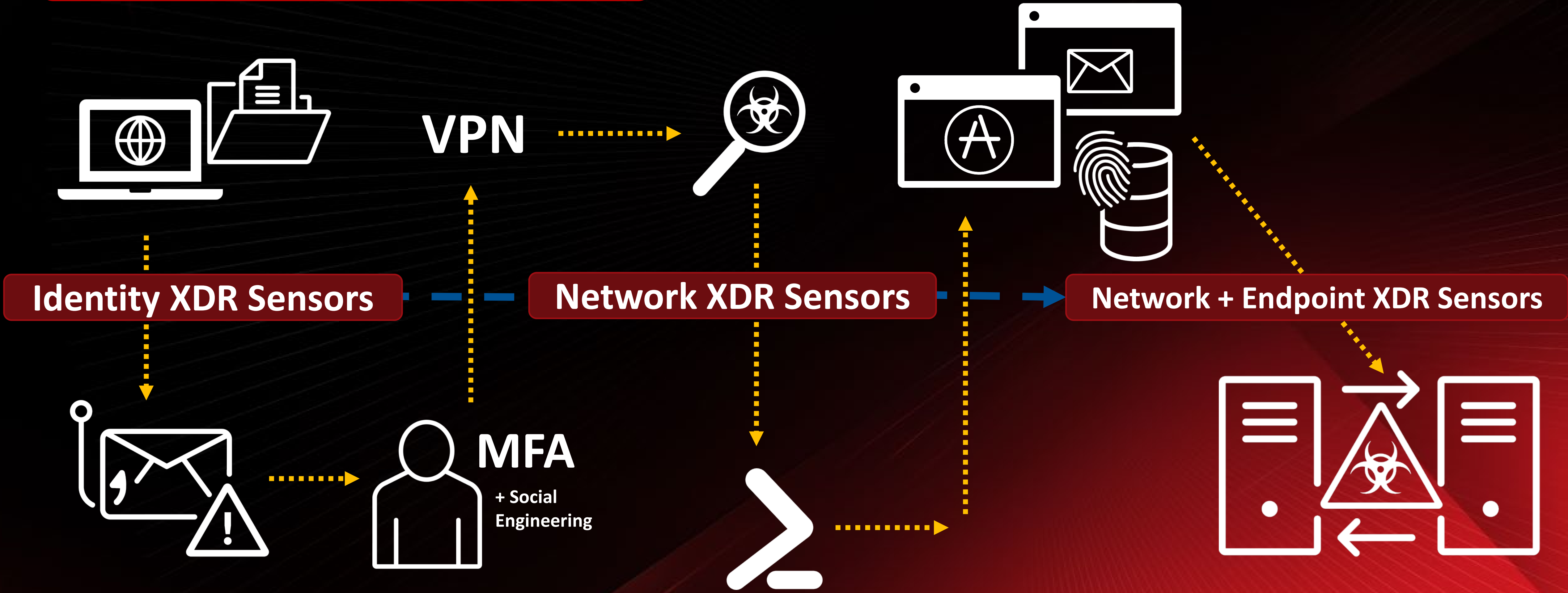
Optimize onboarding and your technology investment to best protect cyber assets

Breach Scenario

UBER BREACH: STORY OF THE ATTACK

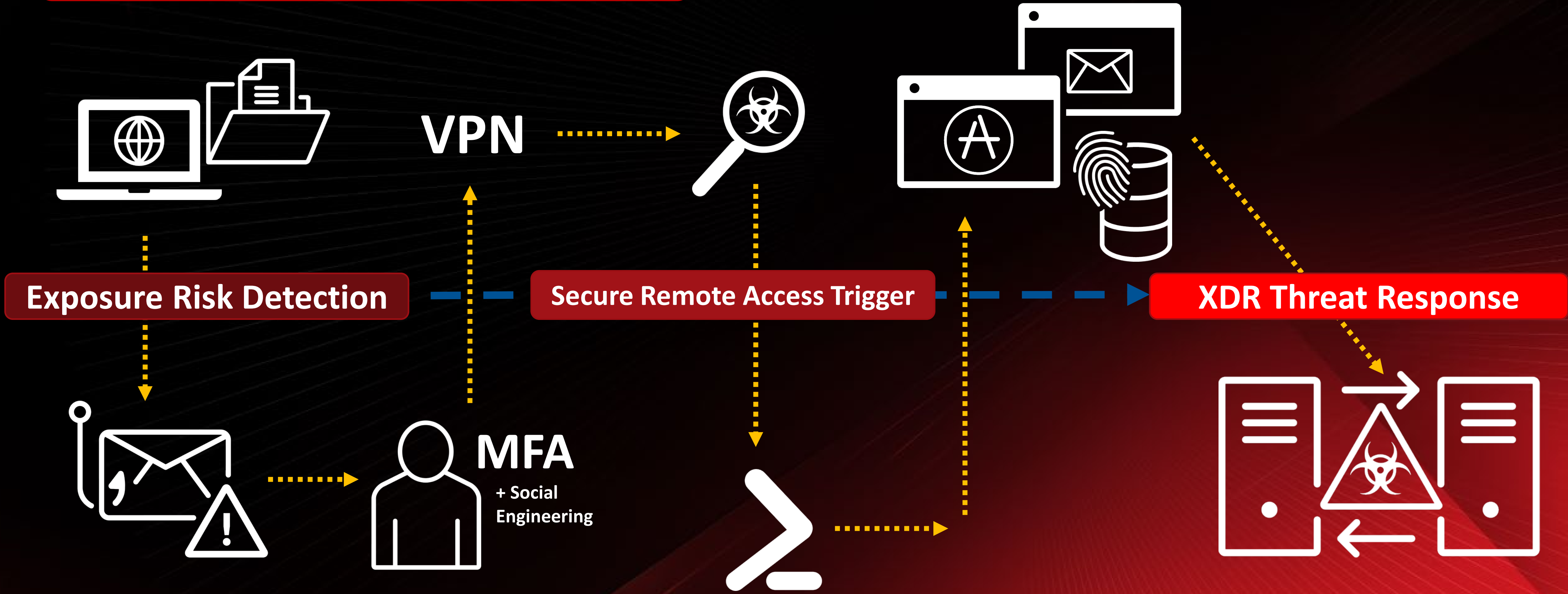


UBER BREACH: RESPONSIVE



Detect, investigate, and respond to suspicious activity across security vectors

UBER BREACH: PRE-EMPTIVE



VPN

Exposure Risk Detection

Secure Remote Access Trigger

XDR Threat Response

MFA

+ Social Engineering

Accelerate SOC capabilities with ASRM + Zero Trust + XDR from Security Platform Approach

Security and Business Benefits

Cybersecurity Outcomes | What can we accomplish?

CONSOLIDATION | Pivot from a siloed cybersecurity approach to a unified cybersecurity platform — *without losing quality*

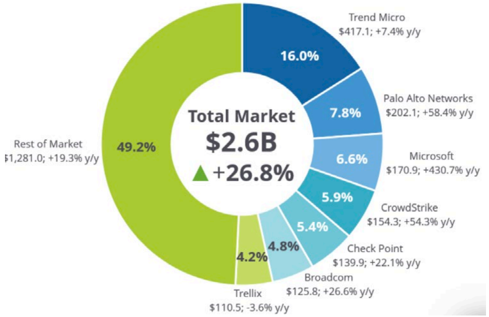
VISIBILITY | Transform from limited visibility to broad visibility into security and risk exposure, across all assets with Attack Surface Risk Management — *for proactive defense*

AUTOMATION | Shift from manual response to automated workflows and AI-supported response with integrated security playbooks — *achieve real time protection, assessment, detection and response, and improve mean time to contain*

Consolidation without Compromise

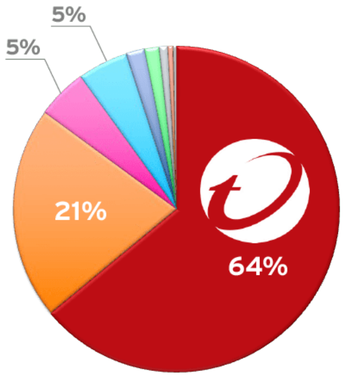
IDC Worldwide Cloud Workload Security Market Shares

May 2023



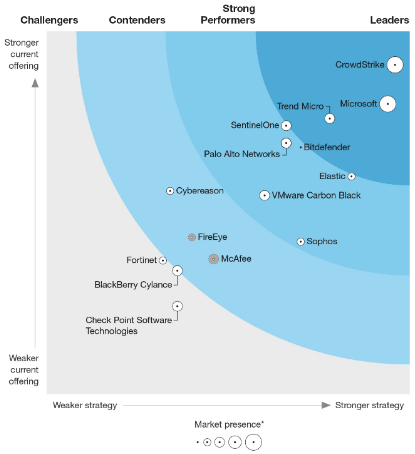
Omdia Global Vulnerability Research and Discovery

2022 Edition



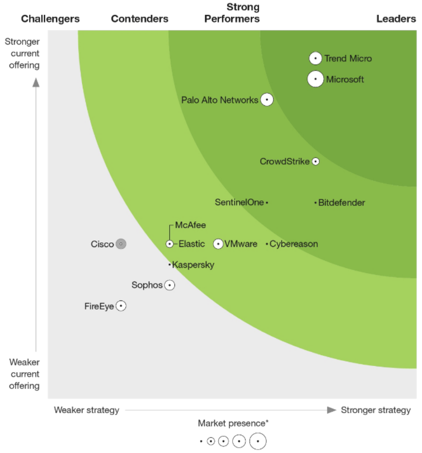
Forrester Wave™: Endpoint Detection and Response

Q2, 2022



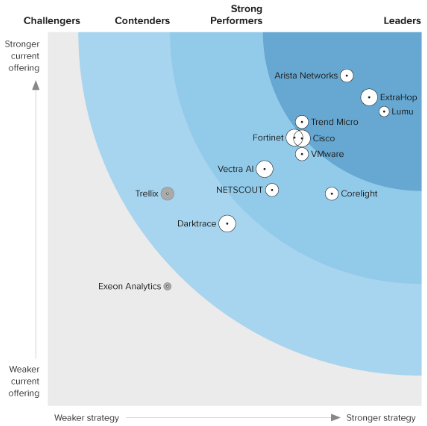
Forrester New Wave™: Extended Detection and Response (XDR)

Q4, 2021



Forrester Wave™: Network Analysis and Visibility

Q2, 2023

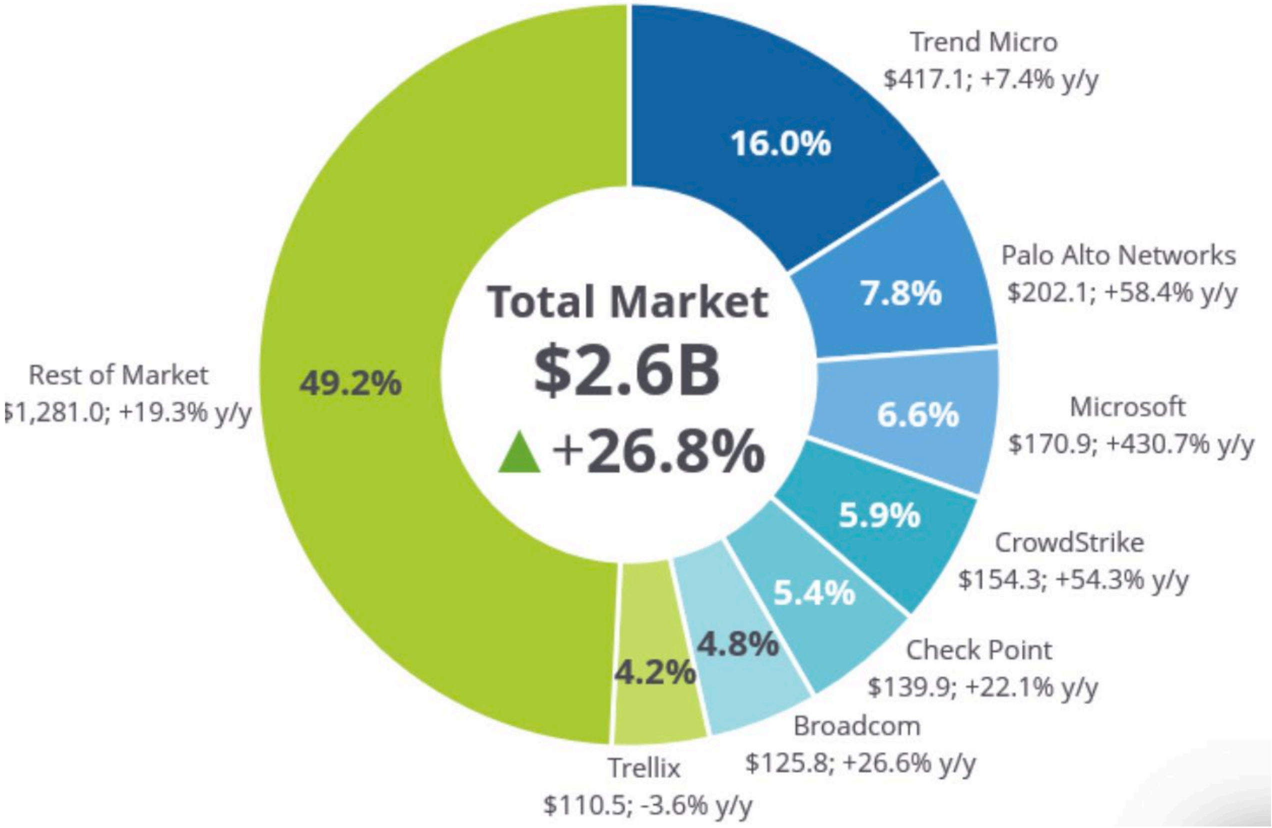


The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments.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

Consolidation without Compromise

IDC Worldwide Cloud Workload Security Market Shares

May 2023



Omdia

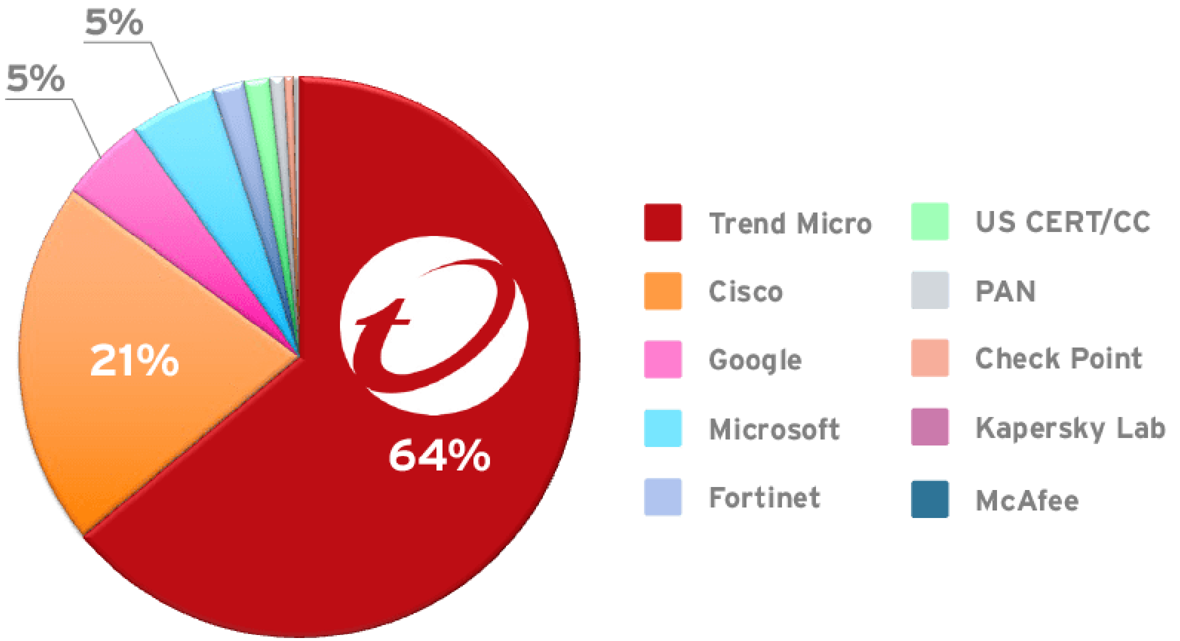
The Forrester Wave^{TM} is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and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

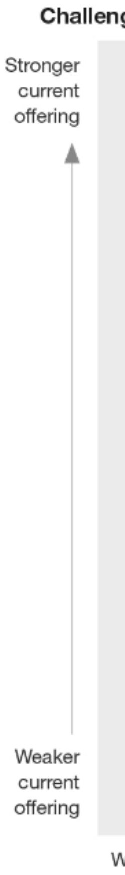
Consolidation without Compromise

Quantifying the Public Vulnerability Market

2022 Edition

Omdia Research: Quantifying the Public Vulnerability Market: 2022 Edition



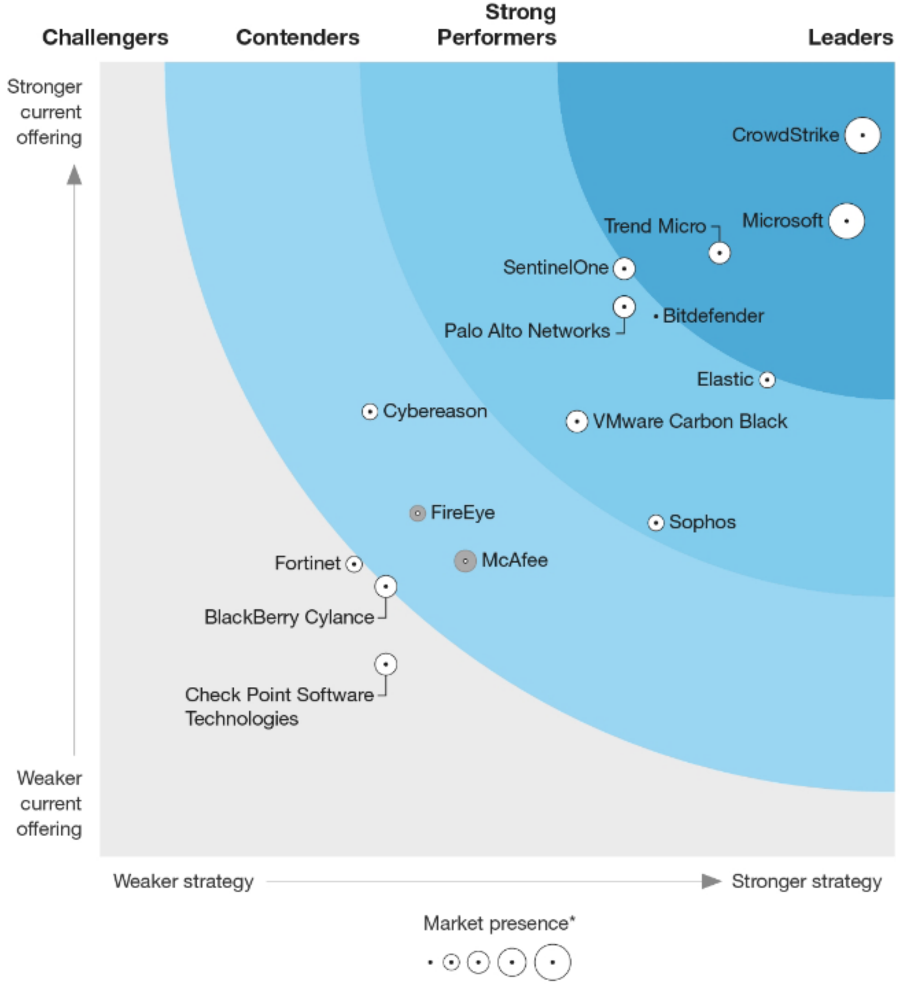


The Forrester Wave™ *is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments.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

Consolidation without Compromise

Forrester Wave$^{\text{TM}}$: Endpoint Detection and Response

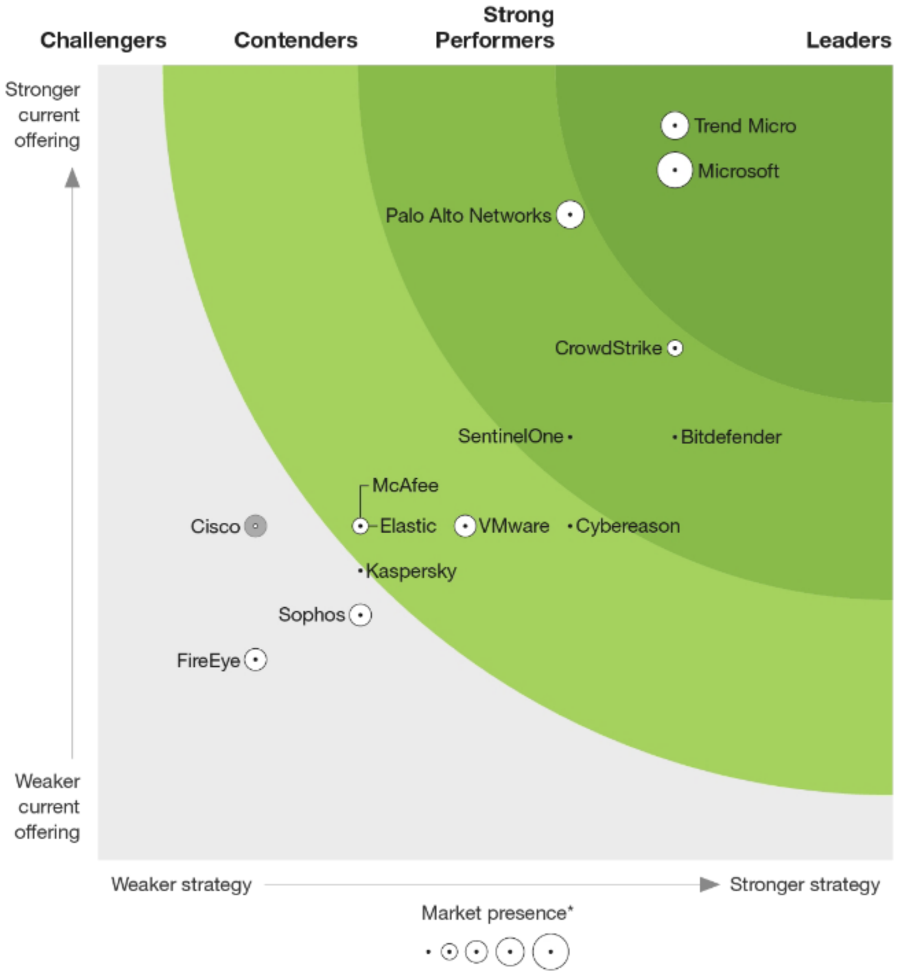
Q2, 2022

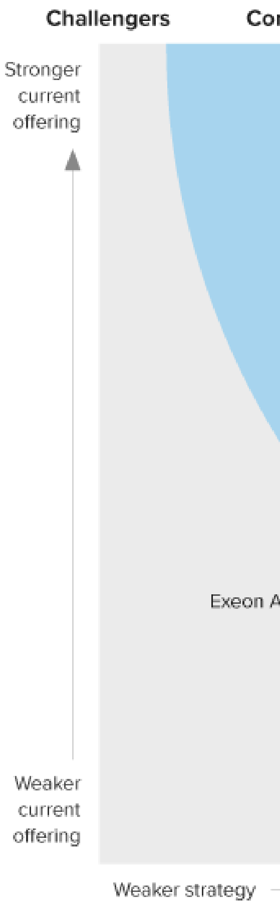


Consolidation without Compromise

Forrester New Wave™: Extended Detection and Response (XDR)

Q4, 2021



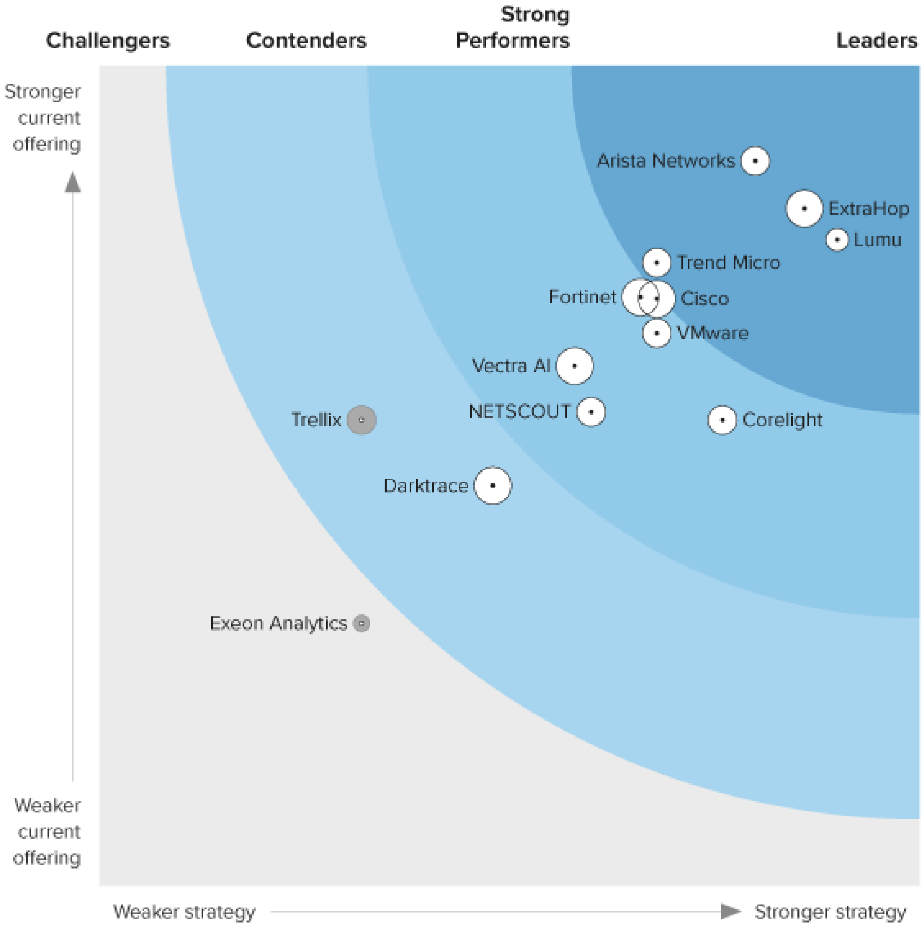


The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments.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

Consolidation without Compromise

Forrester Wave^{TM}: Network Analysis and Visibility

Q2, 2023

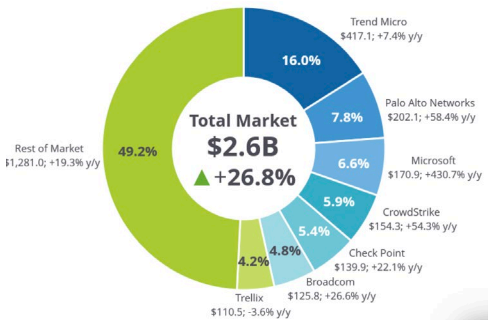


The Forrester Wave^{TM} is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and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

Consolidation without Compromise

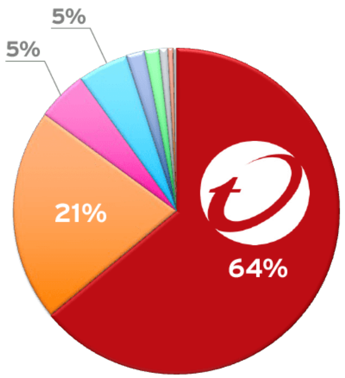
IDC Worldwide Cloud Workload Security Market Shares

May 2023



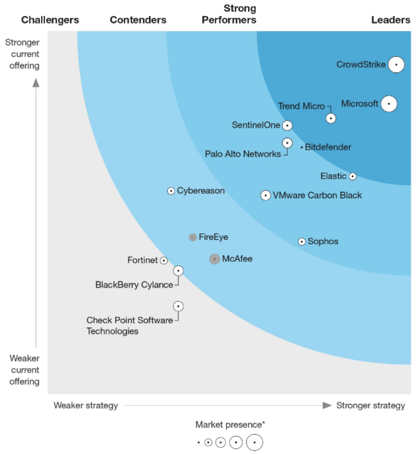
Omdia Global Vulnerability Research and Discovery

2022 Edition



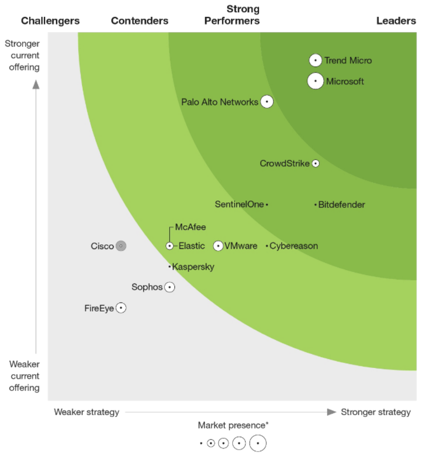
Forrester Wave^{TM}: Endpoint Detection and Response

Q2, 2022



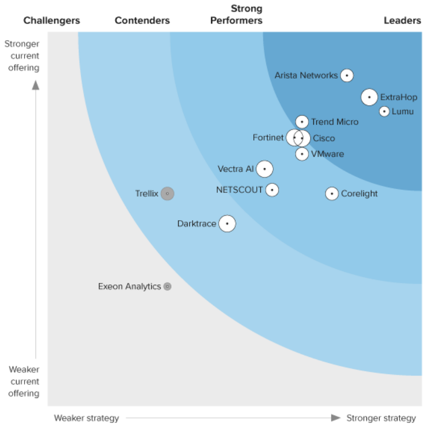
Forrester New Wave^{TM}: Extended Detection and Response (XDR)

Q4, 2021



Forrester Wave^{TM}: Network Analysis and Visibility

Q2, 2023

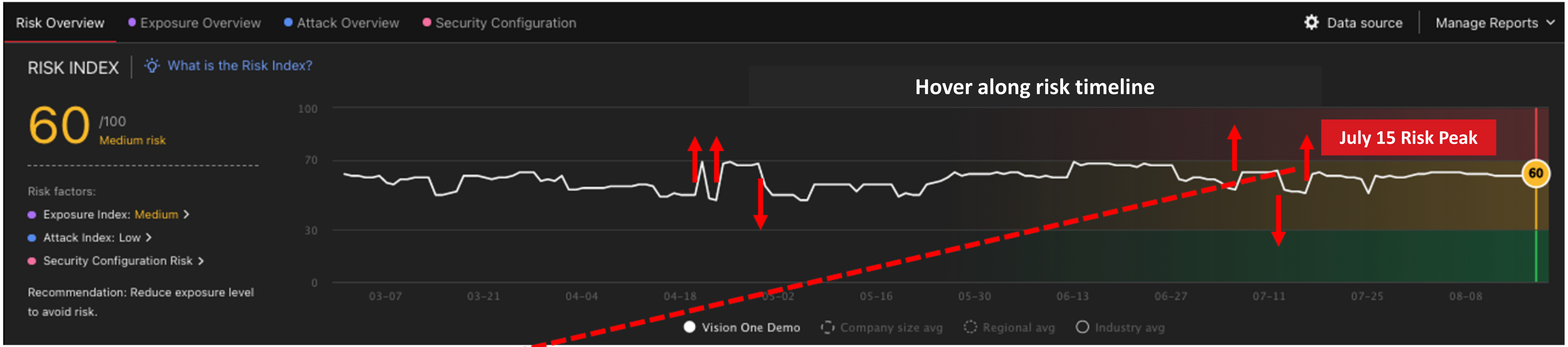


***The Forrester Wave^{TM}** is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings,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

What is missing from my strategy and what can I consider?

Cyber Risk as a Communication Tool

Cyber Risk Quantification for the SOC



60 /100 Medium risk

Risk factors:

- Exposure Index: Medium
- Attack Index: Low
- Security Configuration Risk

Recommendation: Reduce exposure level to avoid risk.

Hover along risk timeline

July 15 Risk Peak

July 15 Peak Caused By:

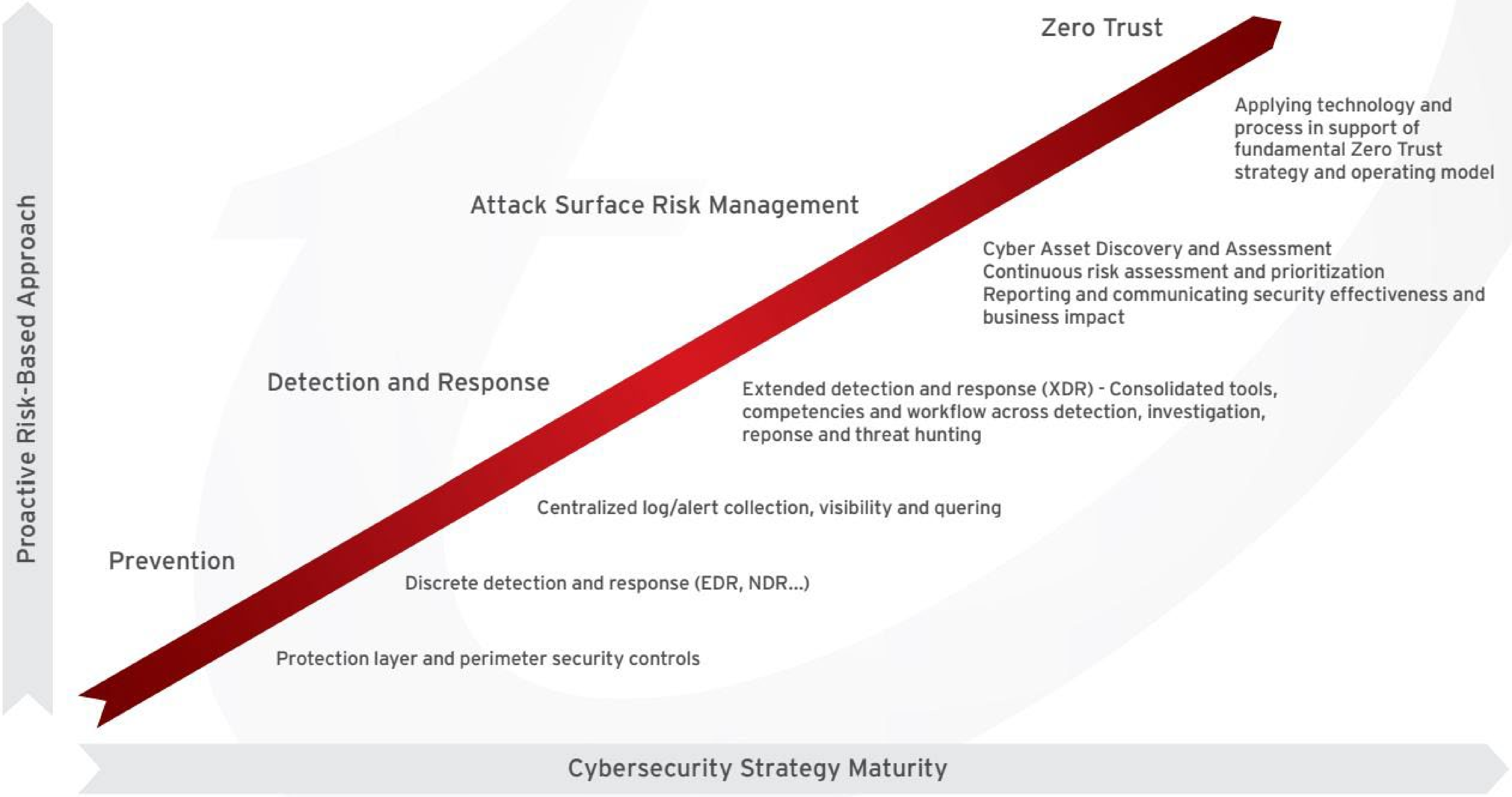
- 1 user risk level elevated too high
- 1 device risk score increased from low to medium risk level

User Alice risk score changes from 53 to 72:

- Risk Factor: Account Compromise -> User info leaked from breach domain detected
- Risk Factor: System configuration -> Risk Event: Account with Weak Sign-in policy
- Risk Factor: Cloud app activity -> Risk Event: Risky Cloud App Access risk

Device mike-pc1 risk score changes from 31 to 68:

- Risk Factor: Vulnerability-> OS vulnerability identified
- Risk Factor: Security configuration -> Risk Event: Behavior monitoring didn't enabled
- Risk Factor: XDR detection-> Risk Event: Anomalous Auto-start Registry



Proactive Risk-Based Approach

Zero Trust

Applying technology and
process in support of
fundamental Zero Trust
strategy and operating model

Attack Surface Risk Management

Cyber Asset Discovery and Assessment
Continuous risk assessment and prioritization
Reporting and communicating security effectiveness and business impact

Detection and Response

Extended detection and response (XDR) - Consolidated tools, competencies and workflow across detection, investigation, reponse and threat hunting

Centralized log/alert collection, visibility and quering

Prevention

Discrete detection and response (EDR, NDR...)

Protection layer and perimeter security controls

Cybersecurity Strategy Maturity

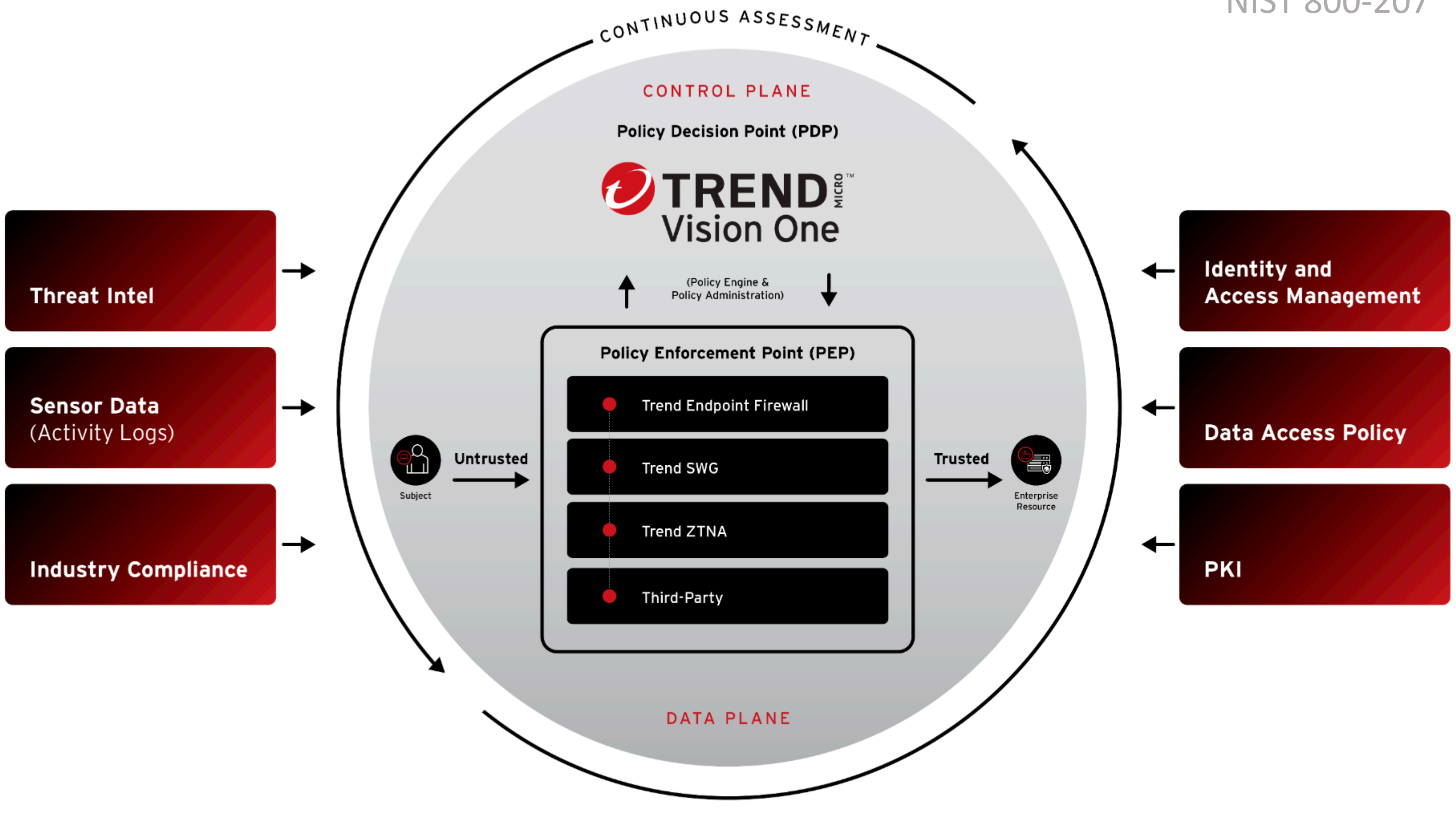
OUR VISION

Assist customers operationalize Zero Trust with the most accurate analysis of risks and threats in their environment.

Through continuous risk assessment, we empower customers to see more and respond faster with automation and guidance.

NIST 800-207

Operationalizing Zero Trust



CONTINUOUS ASSESSMENT

CONTROL PLANE

Policy Decision Point (PDP)

TREND MICRO Vision One

(Policy Engine & Policy Administration)

Policy Enforcement Point (PEP)

- Trend Endpoint Firewall
- Trend SWG
- Trend ZTNA
- Third-Party

Subject

Untrusted

Trusted

Enterprise Resource

DATA PLANE

Threat Intel

Sensor Data (Activity Logs)

Industry Compliance

Identity and Access Management

Data Access Policy

PKI

Feeds

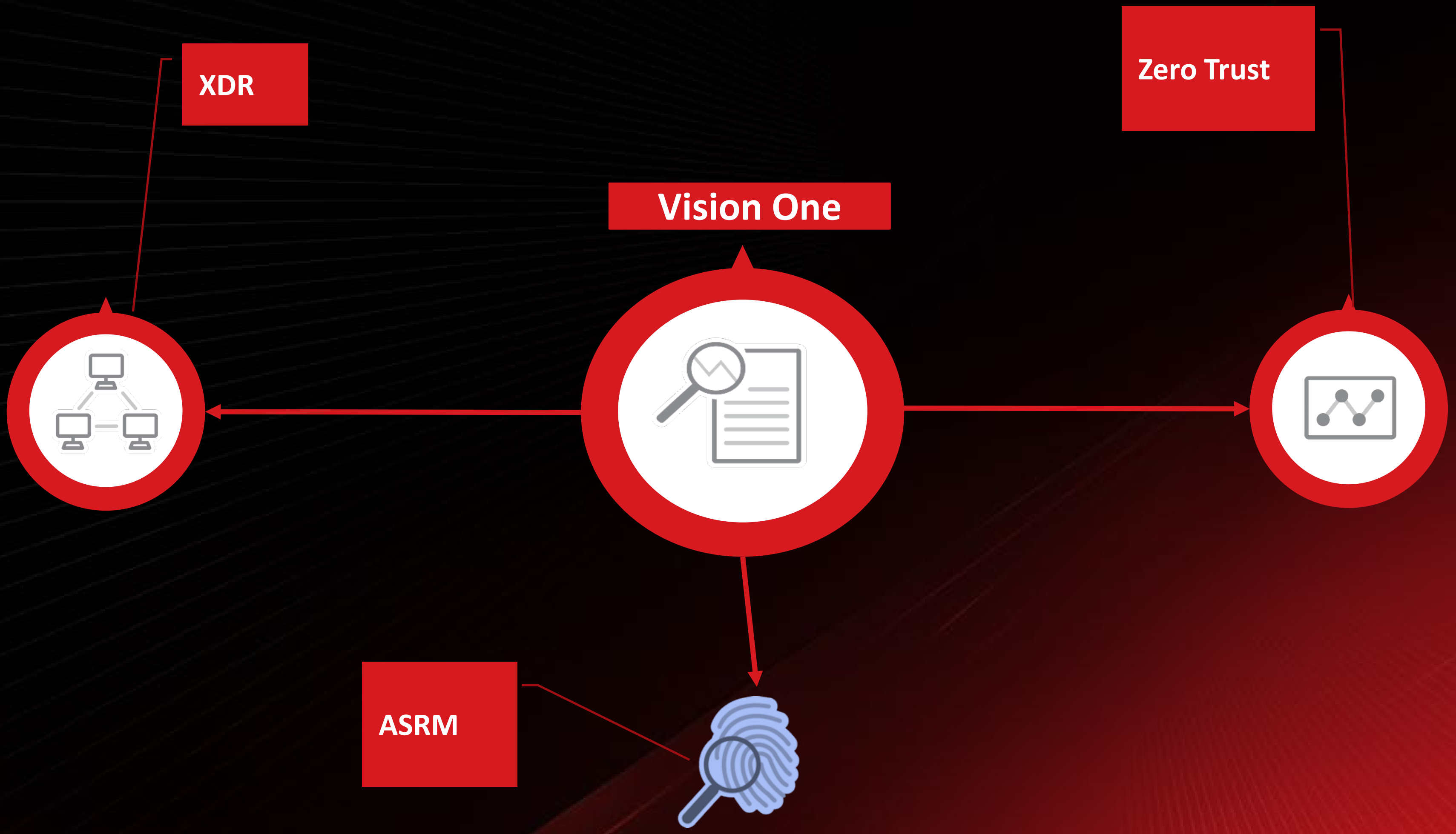
Third Party

Response

splunk>
Microsoft
paloalto
FORTINET
CYBERARK
okta
IBM Security
Microsoft Azure
Azure Active Directory
Google
Qualys
nessus Professional
netskope
CHECK POINT
tenable
Siemplify

Sample integration partners. Full list here:
https://www.trendmicro.com/en_us/partners/alliance-partners/explore-alliance-partners.html

The Vision One



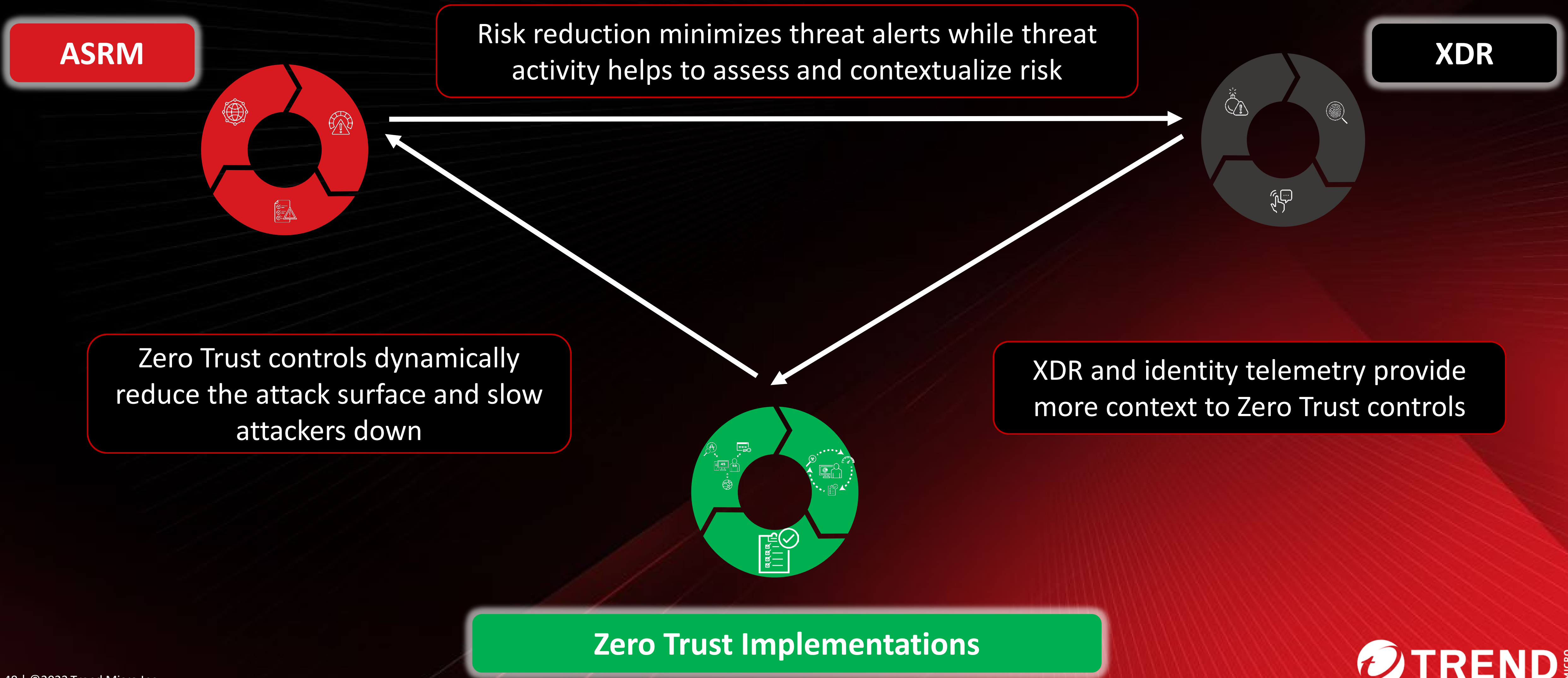
Vision One

XDR

Zero Trust

ASRM

Leverage Existing Investments | Zero Trust



ASRM

Risk reduction minimizes threat alerts while threat activity helps to assess and contextualize risk

XDR

Zero Trust controls dynamically reduce the attack surface and slow attackers down

XDR and identity telemetry provide more context to Zero Trust controls

Zero Trust Implementations

Leverage Existing Investments | Zero Trust

Enable flexibility and mobility within the workforce

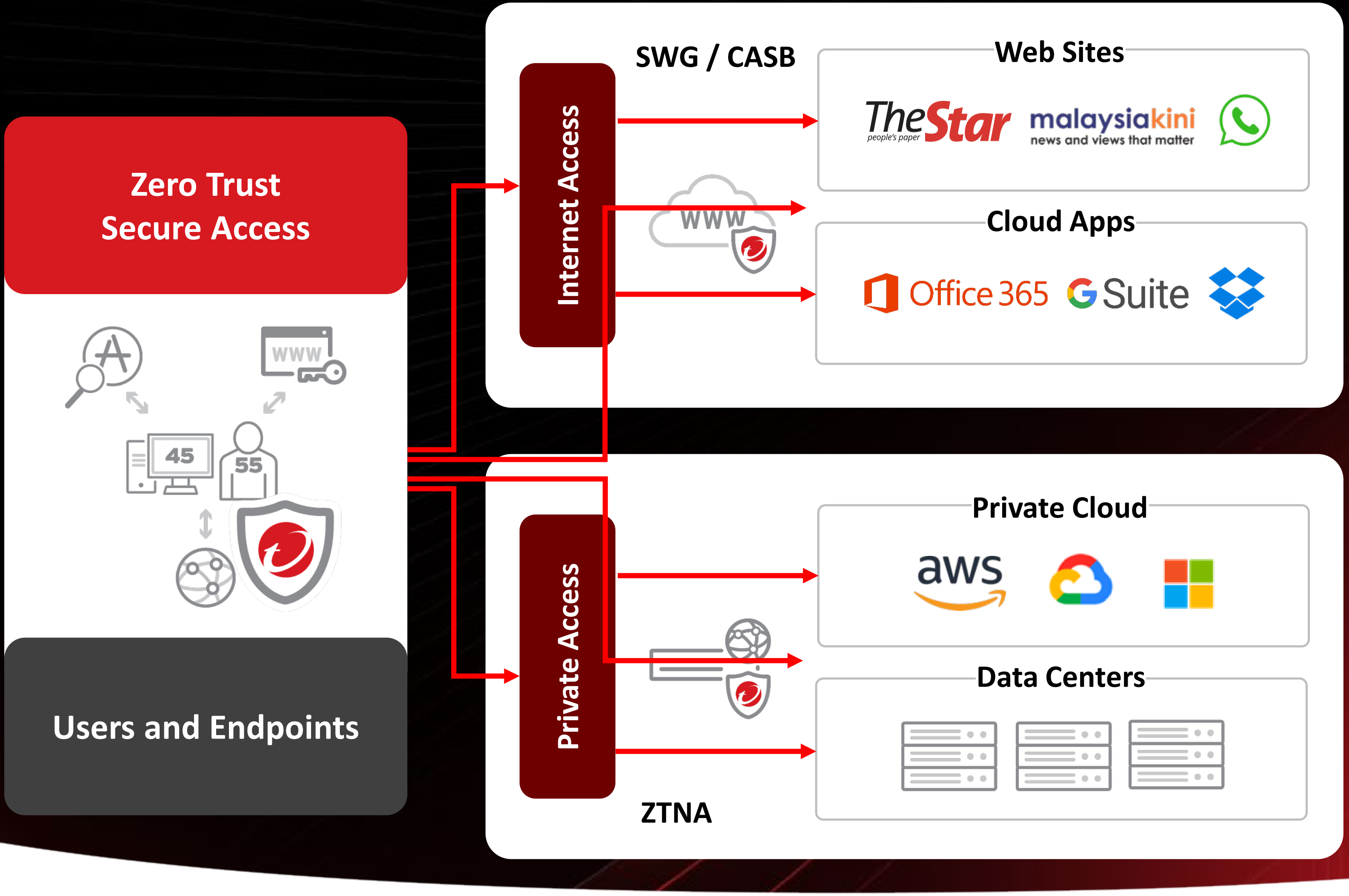
Decrease cyber attack-related downtime and improve overall security posture

Minimize reliance on outdated VPN technology

Integrate Zero Trust Network Access, Secure Web Gateway, & Cloud Access Security Broker

Meet regulatory requirements and align to Zero Trust principles by default

Zero-trust Capabilities with Vision One



Zero Trust Secure Access

Users and Endpoints

Internet Access

SWG / CASB

Web Sites

Cloud Apps

Private Access

ZTNA

Private Cloud

Data Centers

1. Secure Access to the Internet

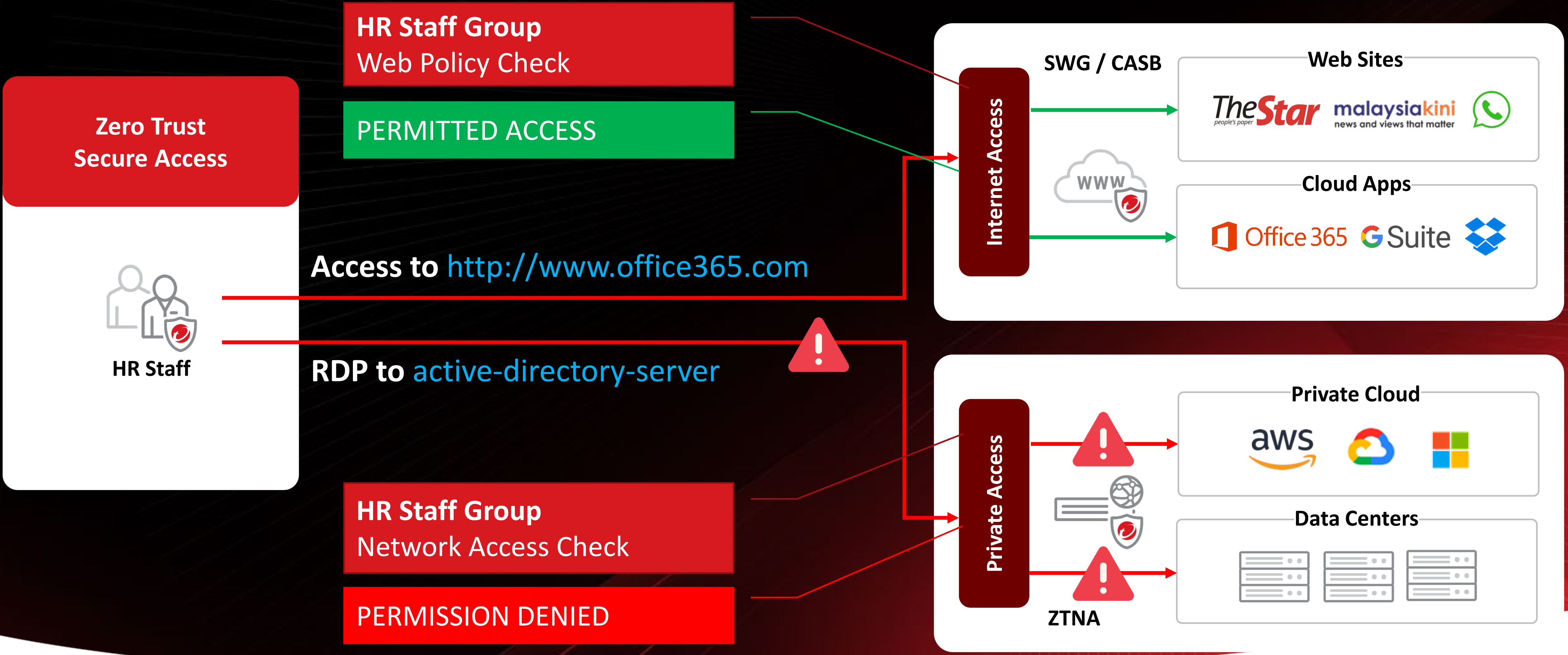
2. Deliver fast and secure access to cloud apps

Previous state

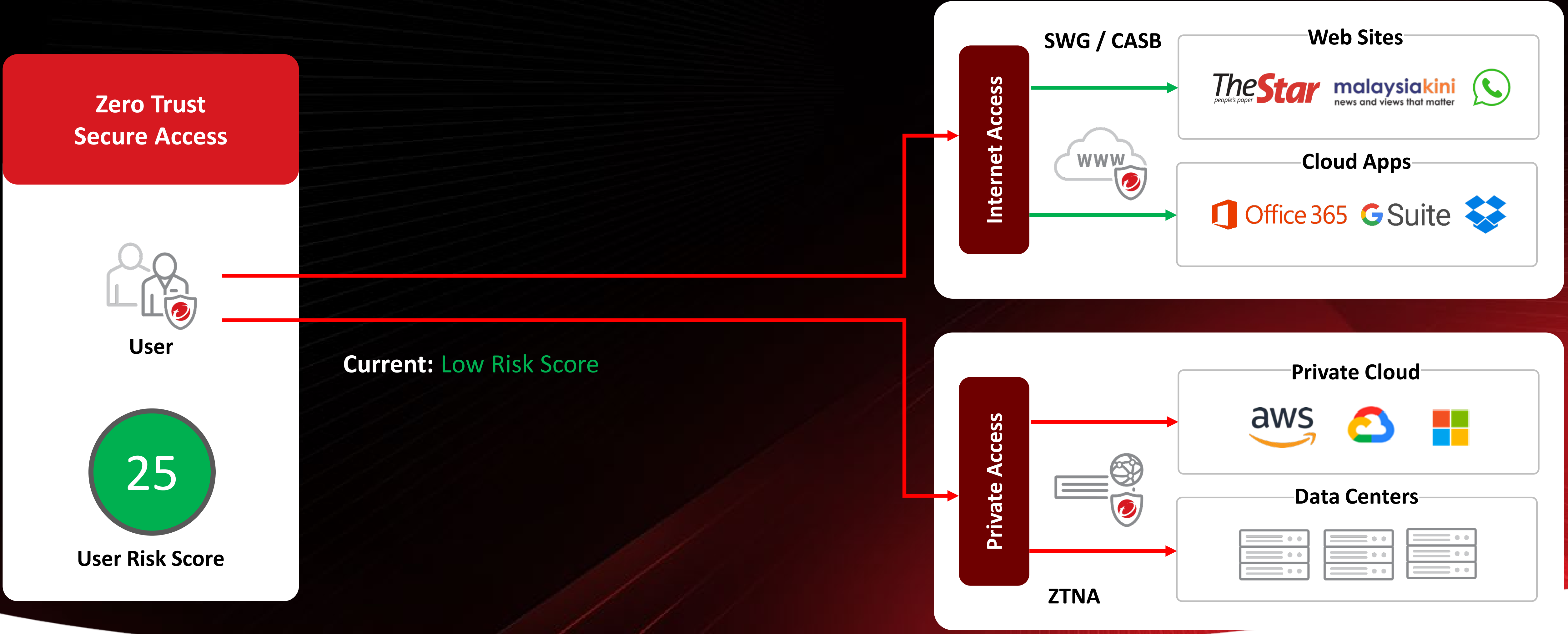
- Users and endpoints are automatically allowed network and Internet access.

3. Transform your remote access solution

Used Case 1: Zero-trust Policy Based Access

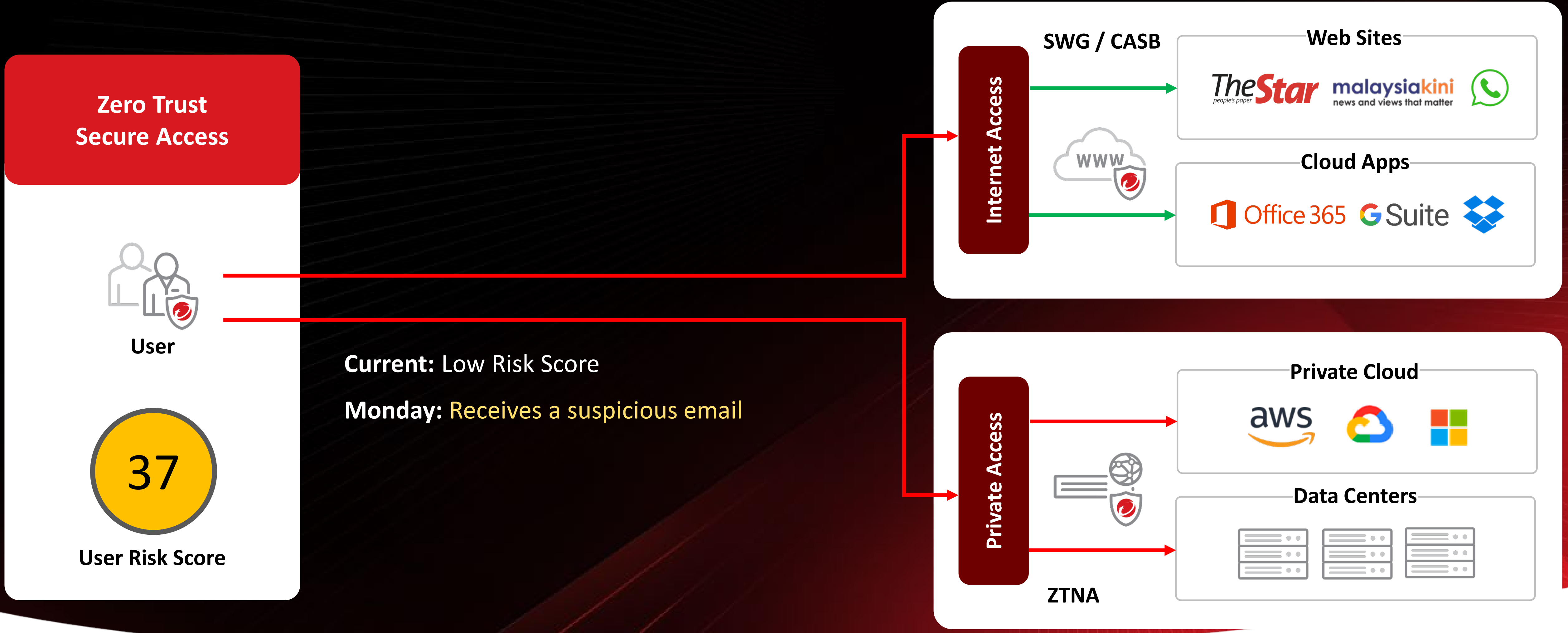


Used Case 2: User Risk Based Defense



TREND MICRO™

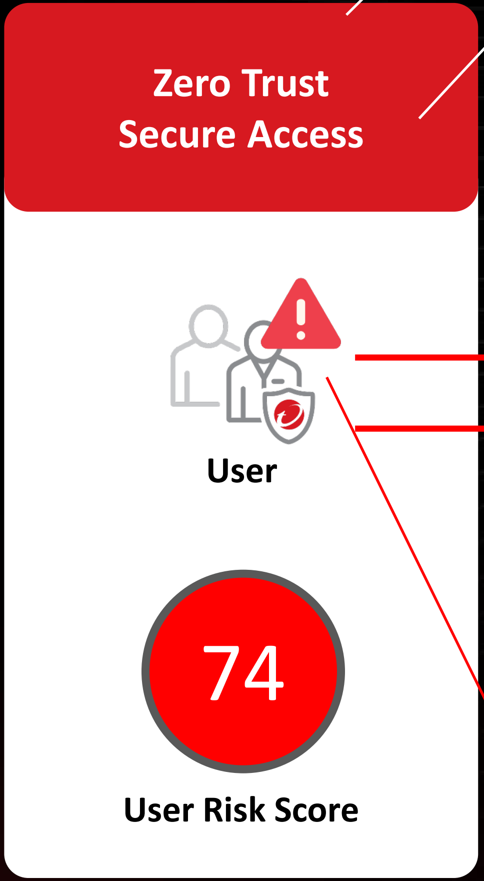
Used Case 2: User Risk Based Defense



Current: Low Risk Score

Monday: Receives a suspicious email

Used Case 2: User Risk Based Defense



High-risk Zero-Trust Policy Trigger

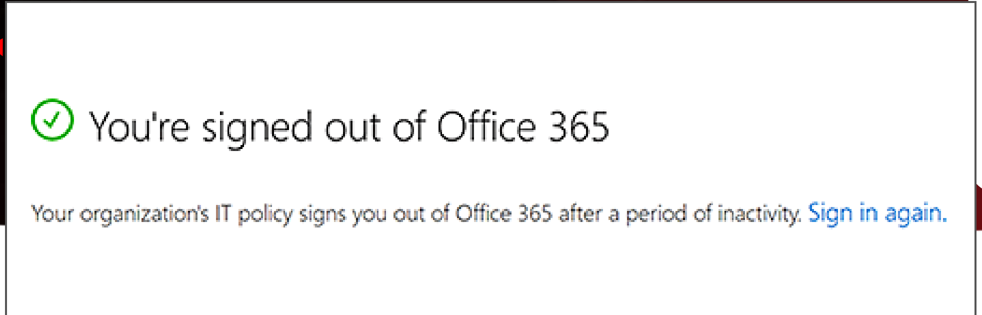
Actions:

x Force Sign-out
x Blocks Access to Internet
x Blocks Access to Internal Apps

Current: Low Risk Score

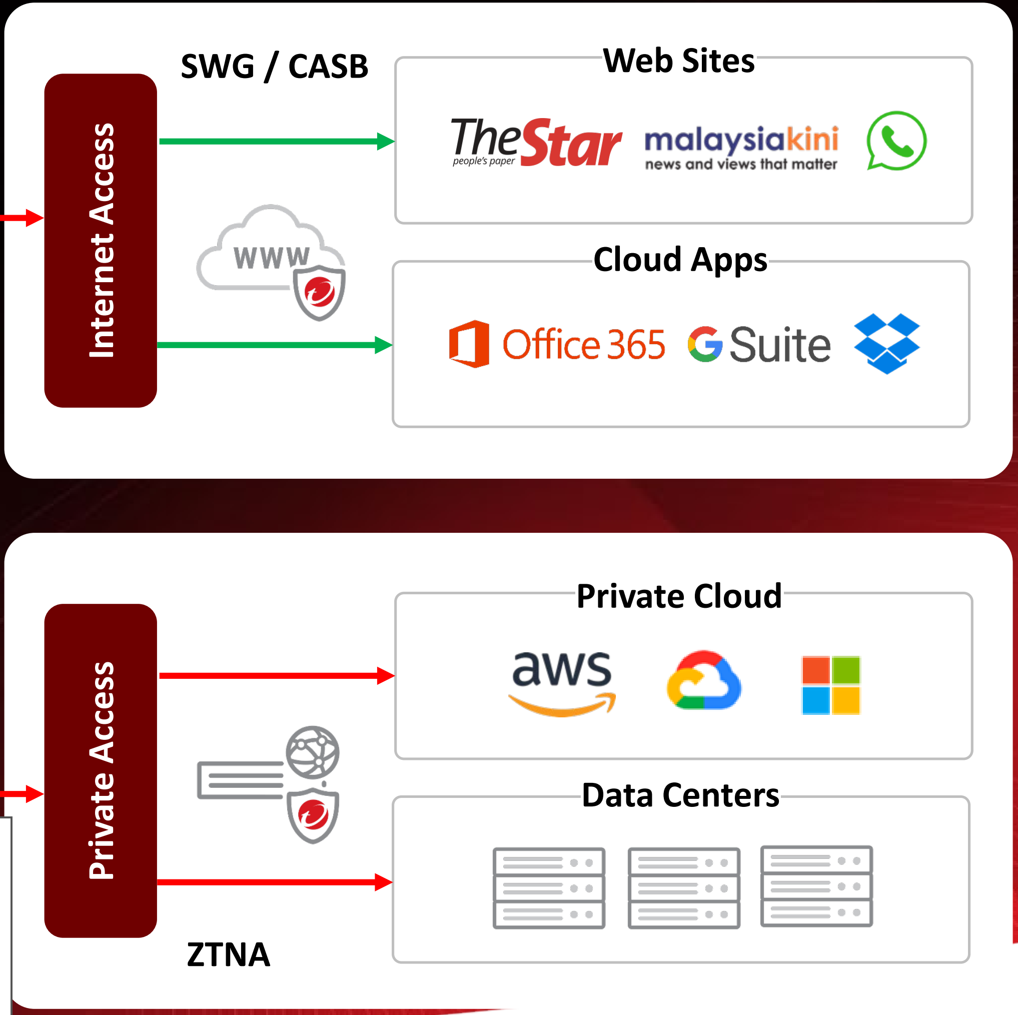
Monday: Receives a suspicious email

Tuesday: Detected with a suspicious traffic and behavior

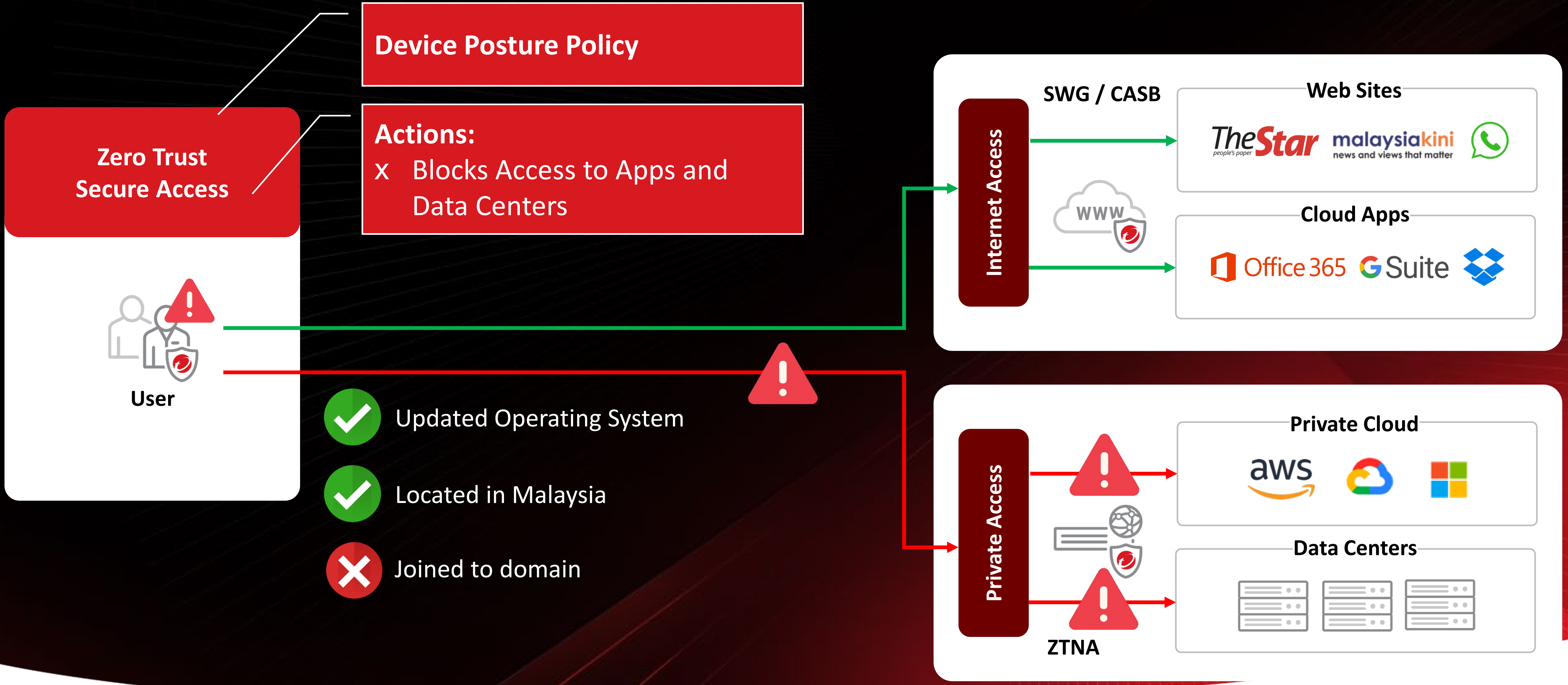


✓ You're signed out of Office 365

Your organization's IT policy signs you out of Office 365 after a period of inactivity. Sign in again.



Used Case 3: Device Posture Policy



Device Posture Policy

Actions:

x Blocks Access to Apps and Data Centers

Zero Trust Secure Access

User

- ✓ Updated Operating System
- ✓ Located in Malaysia
- ✗ Joined to domain

Internet Access

SWG / CASB

Web Sites

TheStar people's paper

malaysiakini news and views that matter

Cloud Apps

Office 365

G Suite

Private Access

ZTNA

Private Cloud

aws

Data Centers

Key Takeaways….

- Simplify Security Complexity and Reduce Operation Costs with Trend Micro Unified Cyber Security Platform (Vision One)
- Handle the XDR resource demand with Trend Micro MXDR services
- Accelerate and Transform your Cybersecurity outcomes with Trend Micro as your Trusted Cybersecurity & Cloud Partner

Thank you!