Une vue holistique et collaborative de la Cybersécurité par Trend Micro.

Bechtle-IT Forum | 13.06.2023| SwissTech Convention Center Lausanne

Claudio Guerrieri, Partner/Entreprise Account Manager, Trend Micro

Trend Micro – Cyber Security for 35 Years

Claudio Guerrieri
Partner & Enterprise Account Manager

Trend Micro At a Glance

35 Years

Founded 1988

Headquatered in Japan

CEO Eva Chen

Co-Founder

96 Consecutive Profitable Quarters

Every quarter since going public

424,000+ SaaS Commercial Customers

500,000+ commercial customers, 175+ countries

62M+

SaaS-Protected Assets

#1 Cloud Security

Based on global market share*

Leader in **XDR**

Based on offering strength and strategy*

Leader in **EPP**

Based on offering strength and strategy*

#1 Next-Gen IPS

Based on global market share*

#1 in Public Vulnerability Disclosure*
+ Over 140 Billion threats blocked in 2022

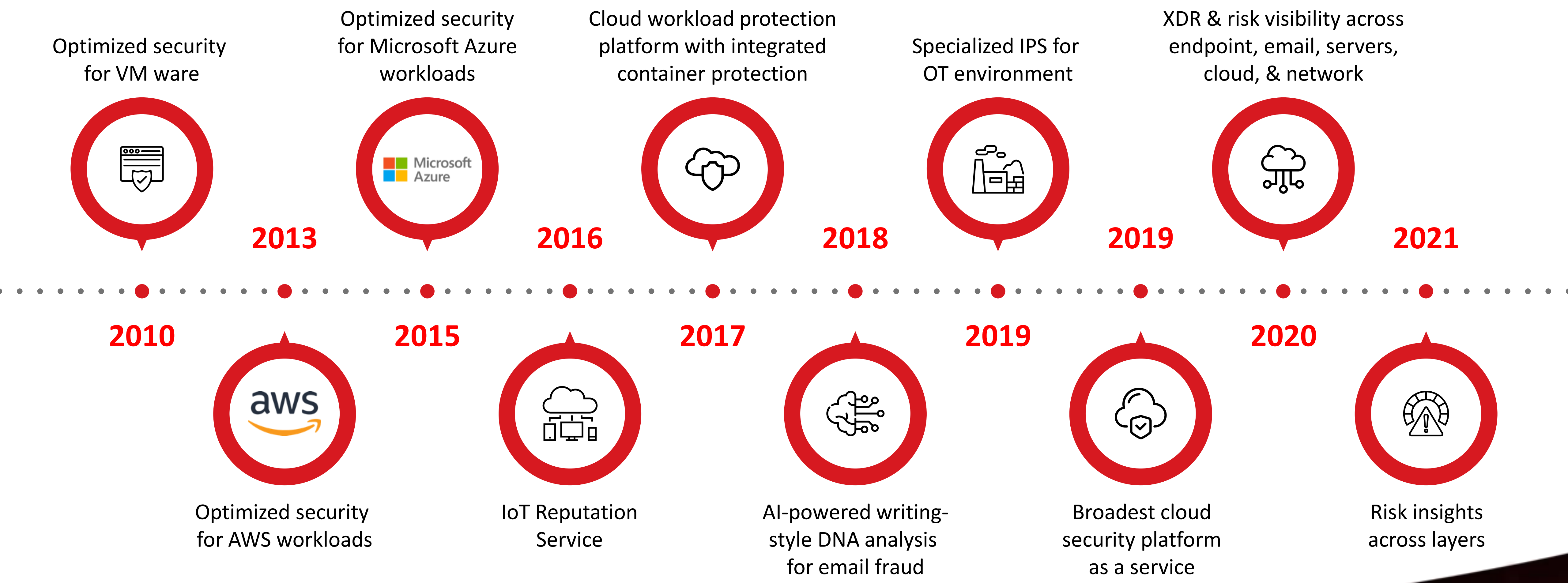
7500+ Employees in **73 Countries**

$1.93 Billion

2021 Net Sales

*IDC Worldwide Cloud Workload Security 2021 Share Snapshot, July 2022
*Forrester Wave, Extended Detection and Response (XDR), Q4, 2021
*Gartner Magic Quadrant for Endpoint Protection Platforms, May 2021
*Gartner Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 3Q22
*Quantifying the Public Vulnerability Market, Omdia, May 2022

Industry firsts: Always Anticipating, Adapting



2010
Optimized security for VM ware

2013
Optimized security for AWS workloads

2015
Optimized security for Microsoft Azure workloads

2016
IoT Reputation Service

2017
Cloud workload protection platform with integrated container protection

2018
AI-powered writing-style DNA analysis for email fraud

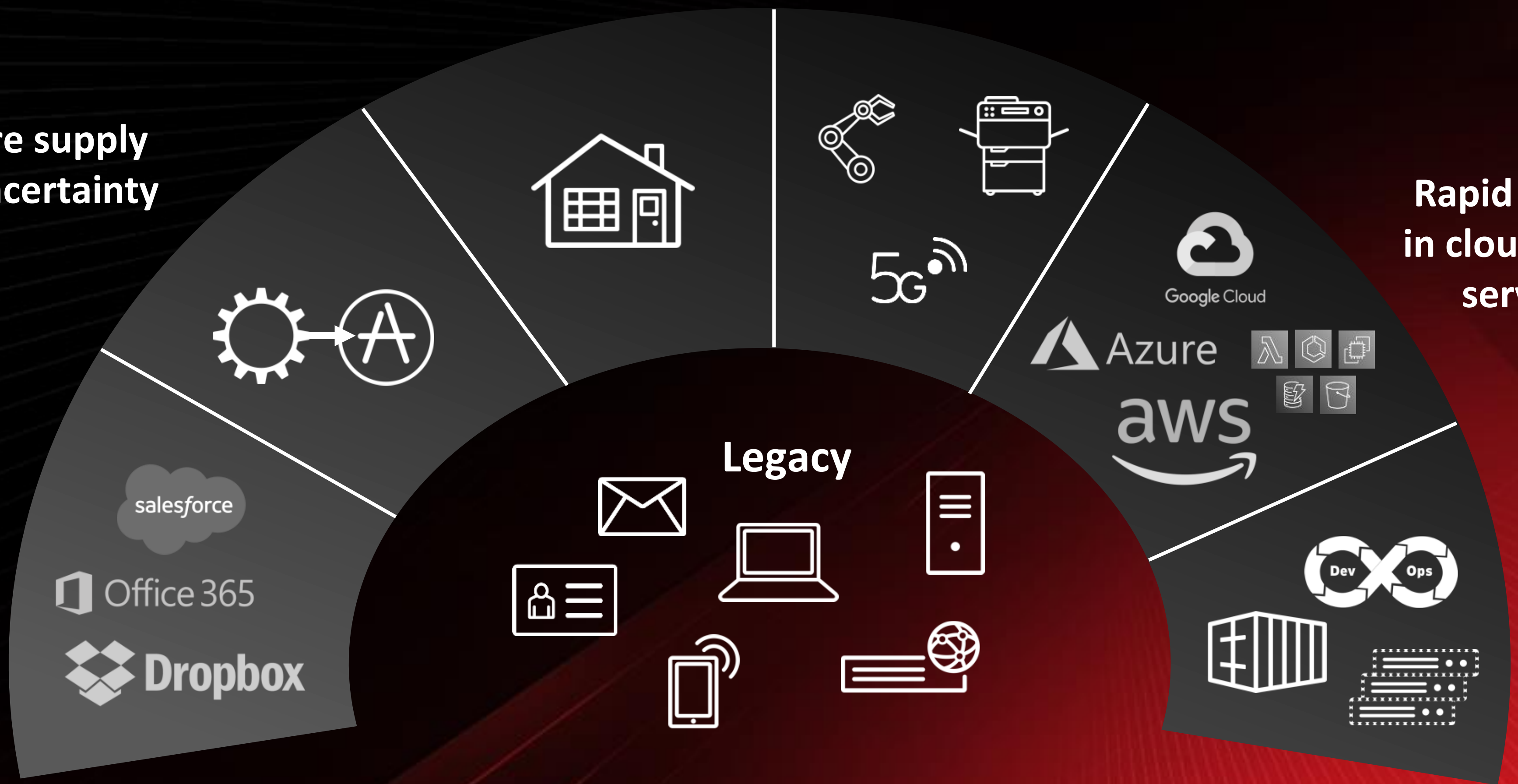
2019
Specialized IPS for OT environment

2019
Broadest cloud security platform as a service

2020
XDR & risk visibility across endpoint, email, servers, cloud, & network

2021
Risk insights across layers

Increasing complexity & attack surface



Work-from-home

IT / OT convergence & 5G

Software supply chain uncertainty

Rapid growth in cloud native services

Massive growth in SaaS applications

Legacy

Cloud native applications

Overwhelmed security teams

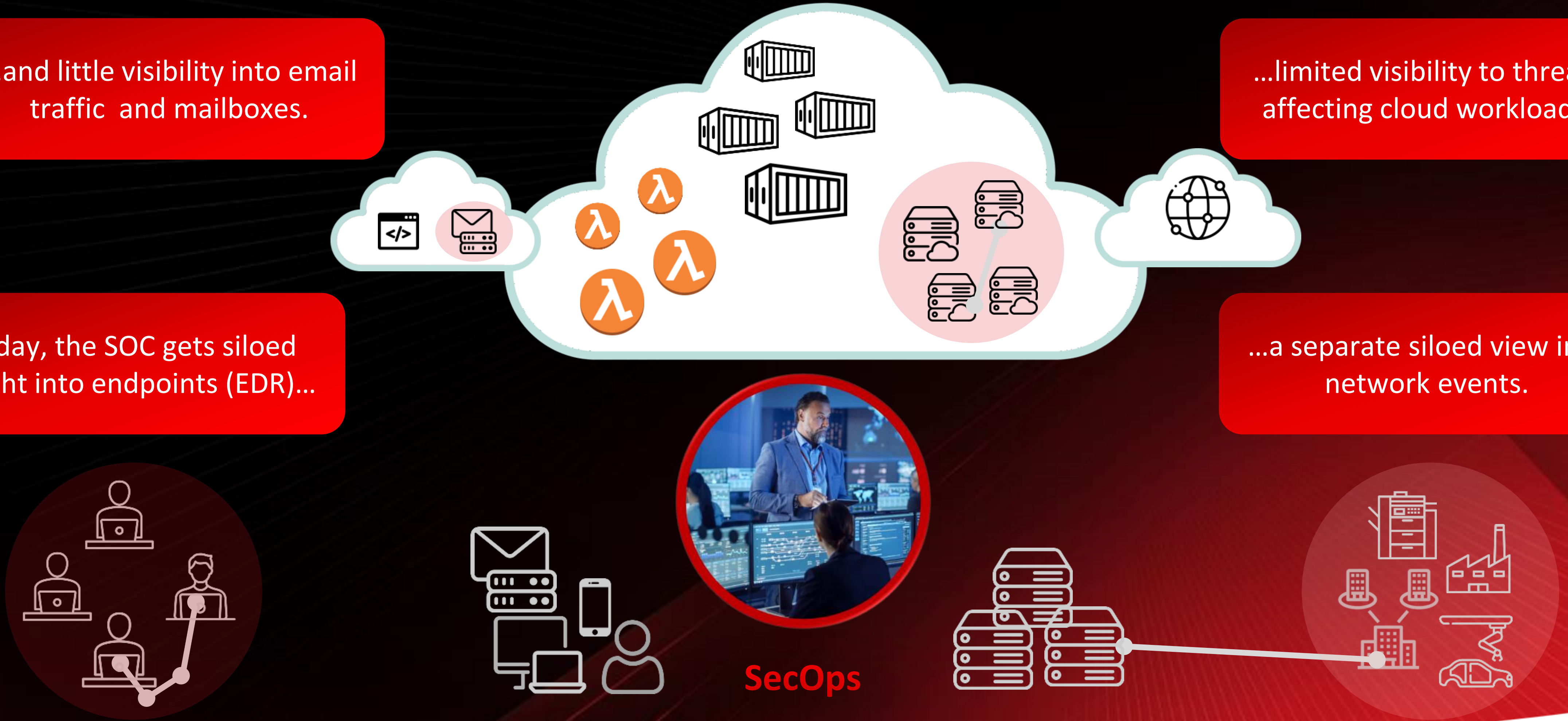
Too many alerts

Where to **focus?**

What to **prioritize?**

Skills shortage

Siloed Telemetry



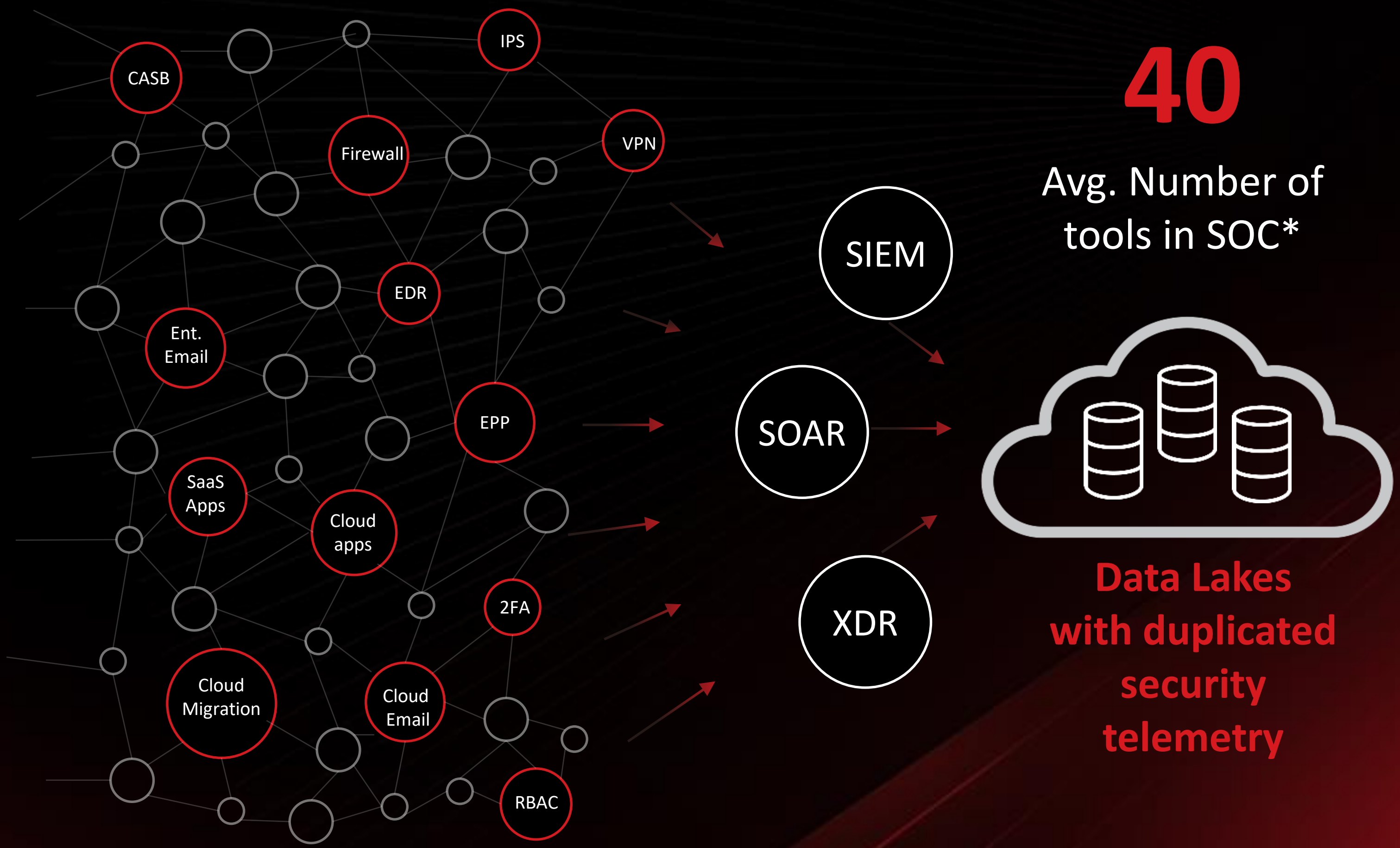
Today, the SOC gets siloed insight into endpoints (EDR)…

…and little visibility into email traffic and mailboxes.

…a separate siloed view into network events.

…limited visibility to threats affecting cloud workloads.

Too Much Security Solutions



40

Avg. Number of tools in SOC*

Data Lakes with duplicated security telemetry

Overlapping solutions

Data lake & cost proliferation

Poorly integrated

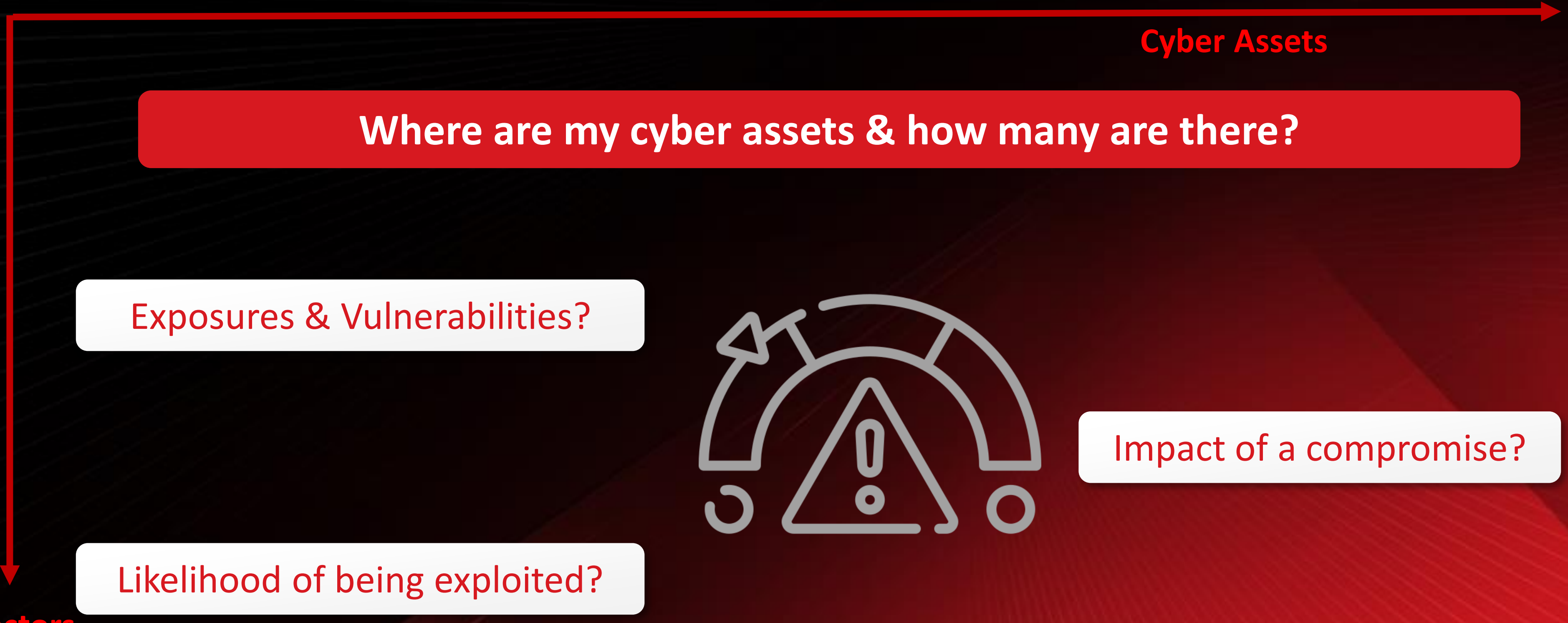
People costs rising

Challenging to measure effectiveness

*SAPIO Research –commissioned by Trend Micro, 2021

Take Charge of Your Risks
with Attack Surface Risk Management

Lack of safety precautions



User Accounts | Endpoints | Storage | Servers | Containers | Domain, Subdomains | Active Directory | Cloud Workloads | Routers, Switches | VPN Gateway | IoT | 5G Private Network | …

Cyber Assets

- Compromised Credentials
- Weak Credentials
- Ransomware
- Phishing
- Social Engineering
- Software Vulnerabilities
- Denial-of-Service
- Unpatched Vulnerability
- Misconfiguration
- …

Attack Vectors

Where are my cyber assets & how many are there?

Exposures & Vulnerabilities?

Likelihood of being exploited?

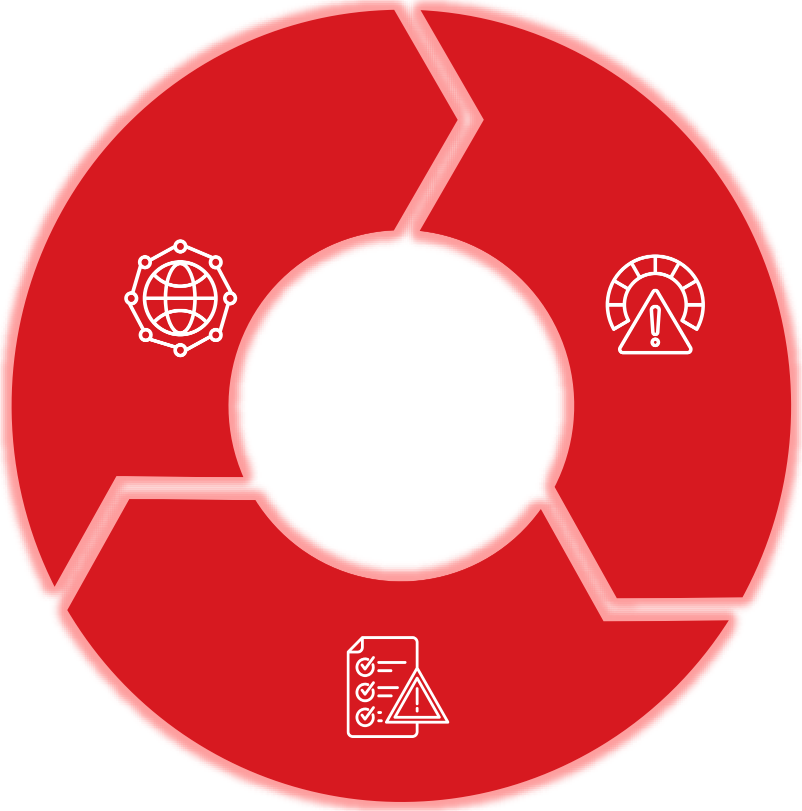
Impact of a compromise?

You Can’t Defend What You Don’t Know About

69% of organizations have experienced some type of cyberattack in which the attack itself started through the exploit of an unknown, unmanaged, or poorly managed internet-facing asset

* Source: Jon Oltsik, ESG Research, *Attack surface management to go mainstream in 2022*, Feb 2022,

Pivot to Proactive - Attack Surface Risk Management



Discover Attack Surface

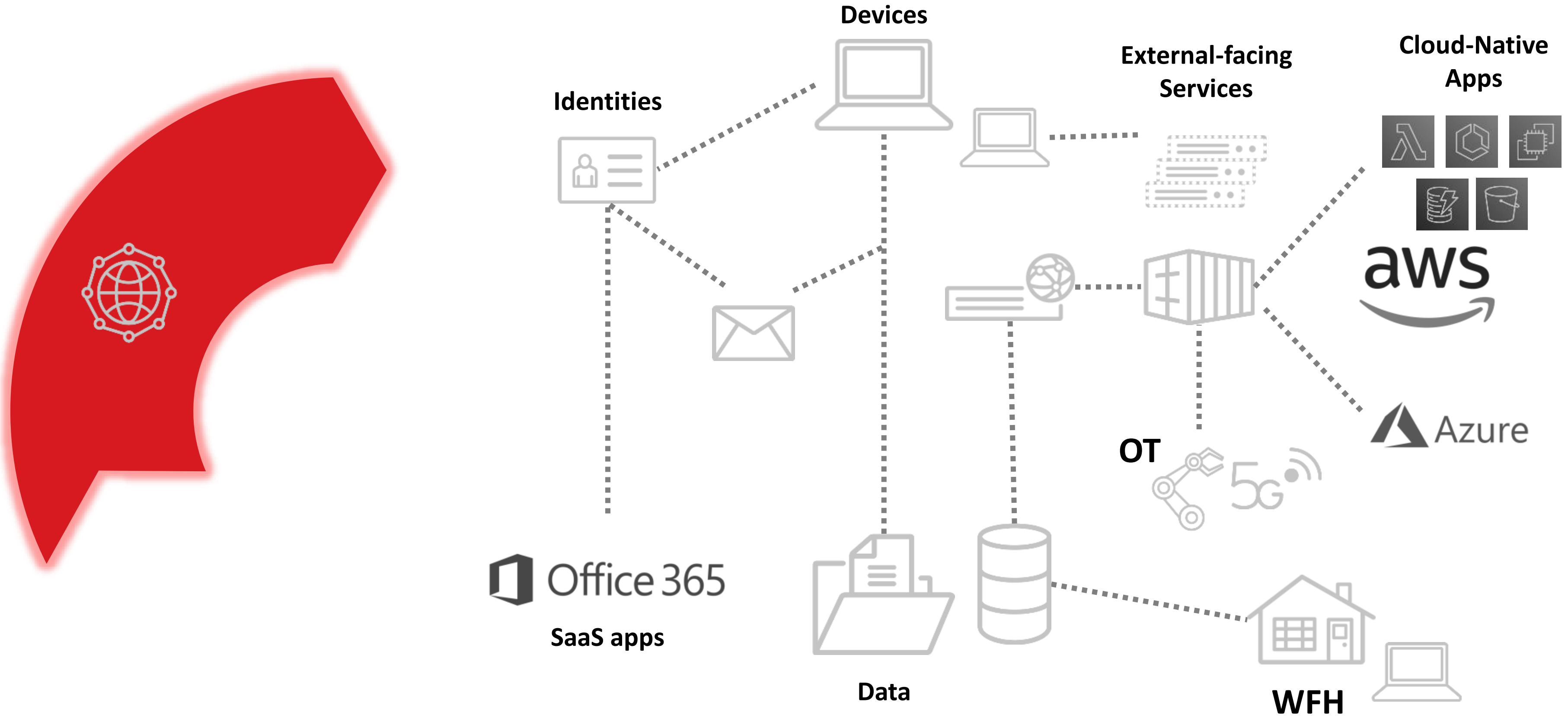
Assess & Prioritize Risk

Mitigate Risk

Eliminate Blind Spots

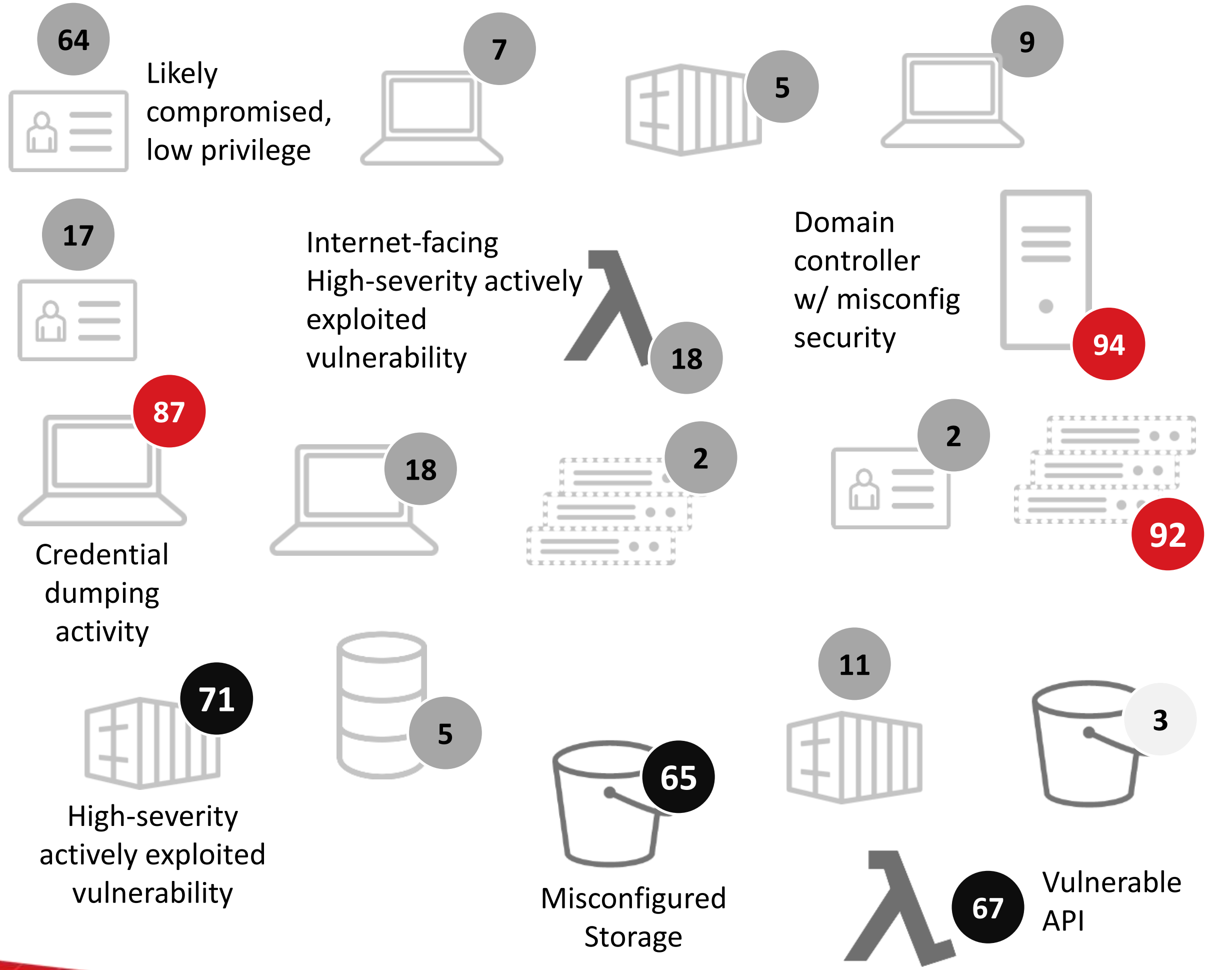
with continuous discovery of known, unknown, internal, & internet-facing (external) assets

Discover Attack Surface



Understand Risk and Exposure

Calculate overall enterprise risk and individual asset risk using Risk Score

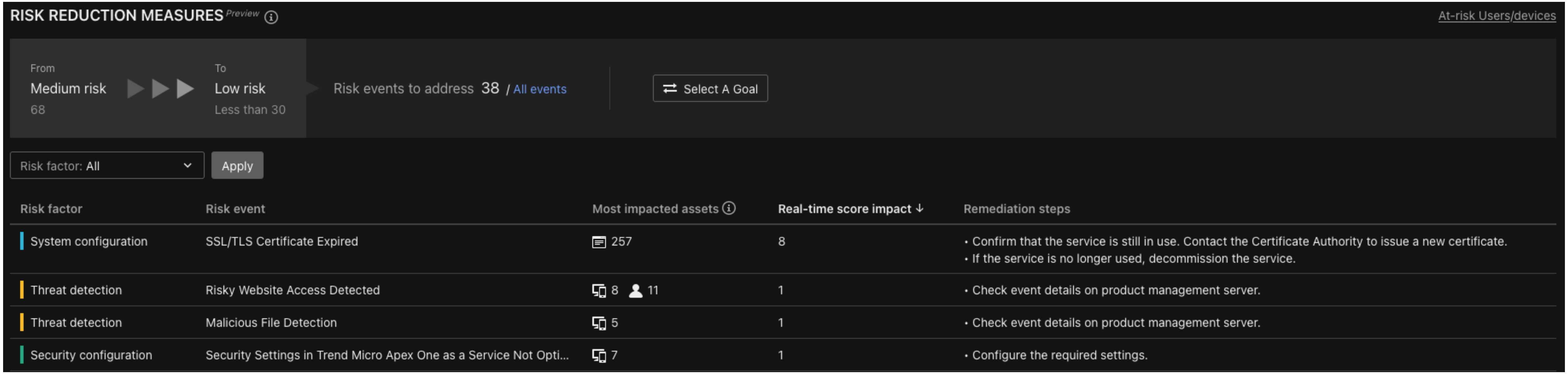


64
Likely compromised, low privilege
7
5
9
17
Internet-facing High-severity actively exploited vulnerability
18
Domain controller w/ misconfig security
94
87
Credential dumping activity
18
2
2
92
71
High-severity actively exploited vulnerability
5
65
Misconfigured Storage
11
3
67
Vulnerable API

Assess & Prioritize Risk

Reduce Risks

Get clear next steps with custom, prioritized recommendations based on your environment



RISK REDUCTION MEASURES *Preview* ⓘ

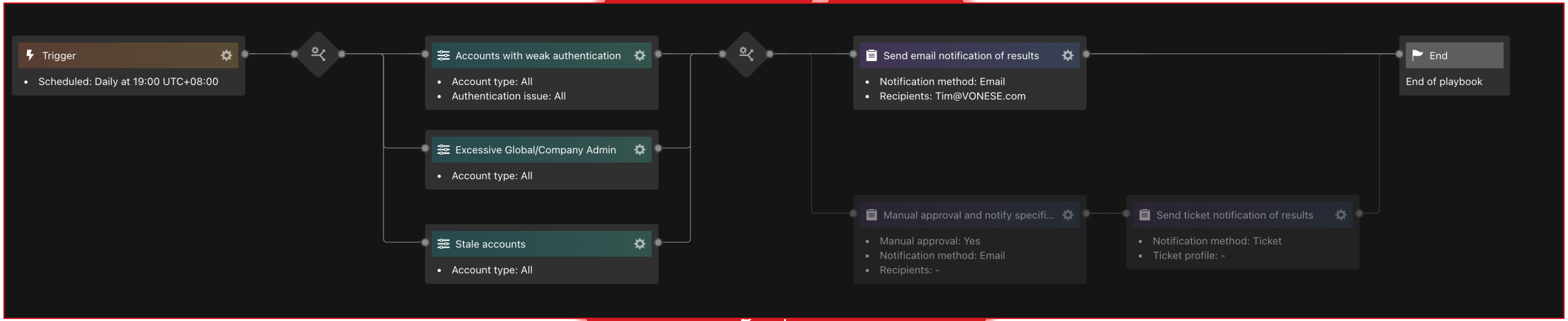
At-risk Users/devices

From Medium risk 68 ▶▶▶ To Low risk Less than 30

Risk events to address 38 / All events

Risk factor	Risk event	Most impacted assets ⓘ	Real-time score impact ↓	Remediation steps
System configuration	SSL/TLS Certificate Expired	257	8	• Confirm that the service is still in use. Contact the Certificate Authority to issue a new certificate. • If the service is no longer used, decommission the service.
Threat detection	Risky Website Access Detected	8 11	1	• Check event details on product management server.
Threat detection	Malicious File Detection	5	1	• Check event details on product management server.
Security configuration	Security Settings in Trend Micro Apex One as a Service Not Opti...	7	1	• Configure the required settings.

Mitigate risk and action recommendations to reduce the likelihood of breach, with playbooks and workflows that integrate with your ecosystem.



Trigger
- Scheduled: Daily at 19:00 UTC+08:00

Accounts with weak authentication
- Account type: All
- Authentication issue: All

Excessive Global/Company Admin
- Account type: All

Stale accounts
- Account type: All

Send email notification of results
- Notification method: Email
- Recipients: Tim@VONESE.com

Manual approval and notify specifi...
- Manual approval: Yes
- Notification method: Email
- Recipients: -

Send ticket notification of results
- Notification method: Ticket
- Ticket profile: -

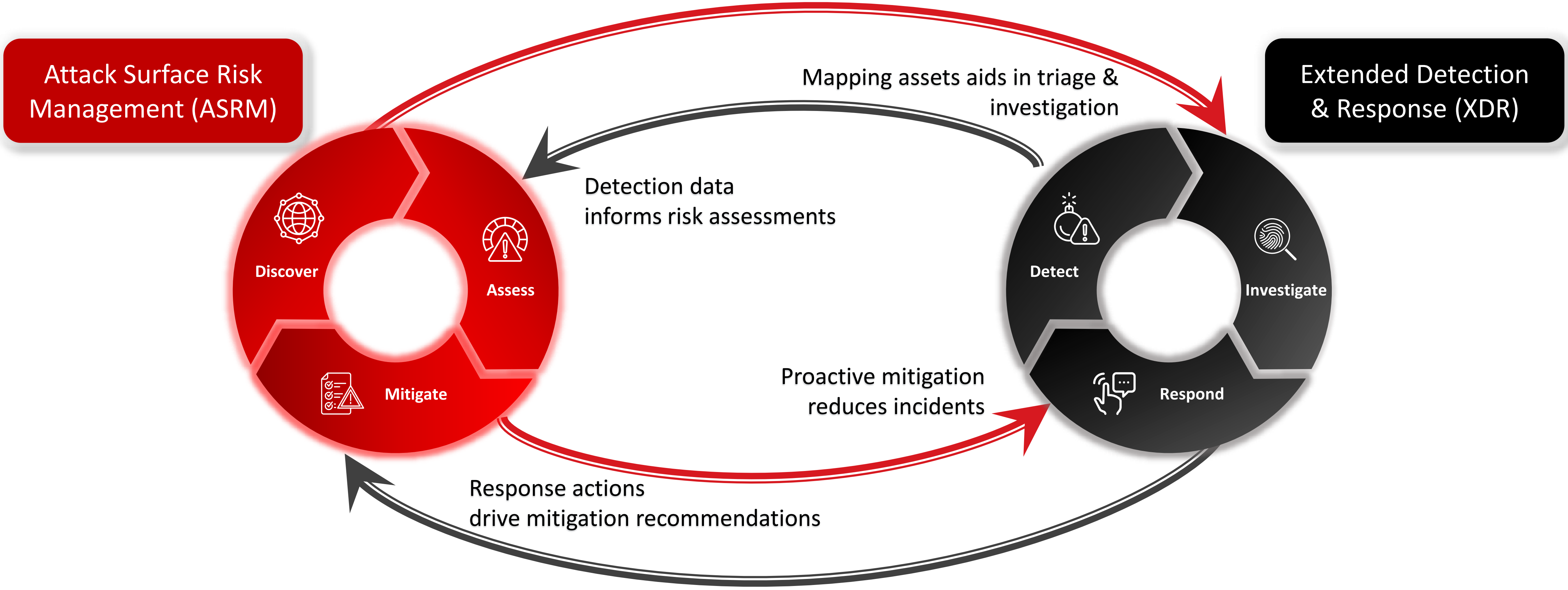
End

End of playbook

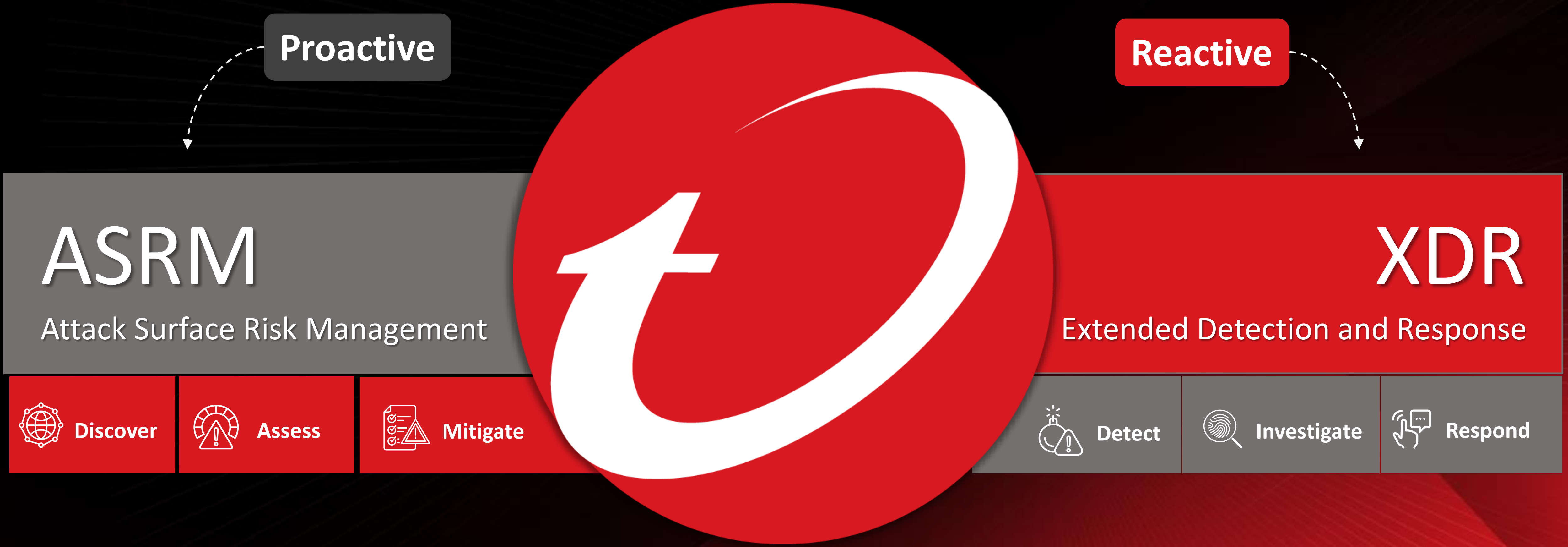
Mitigate Risk

Integrate with XDR

Bridge responsive threat detection and response with proactive attack surface risk management


Attack Surface Risk Management (ASRM)
Extended Detection & Response (XDR)
Mapping assets aids in triage & investigation
Detection data informs risk assessments
Discover
Assess
Mitigate
Detect
Investigate
Respond
Proactive mitigation reduces incidents
Response actions drive mitigation recommendations

Trend Vision One
Solution Overview



Proactive

ASRM

Attack Surface Risk Management

- Discover
- Assess
- Mitigate

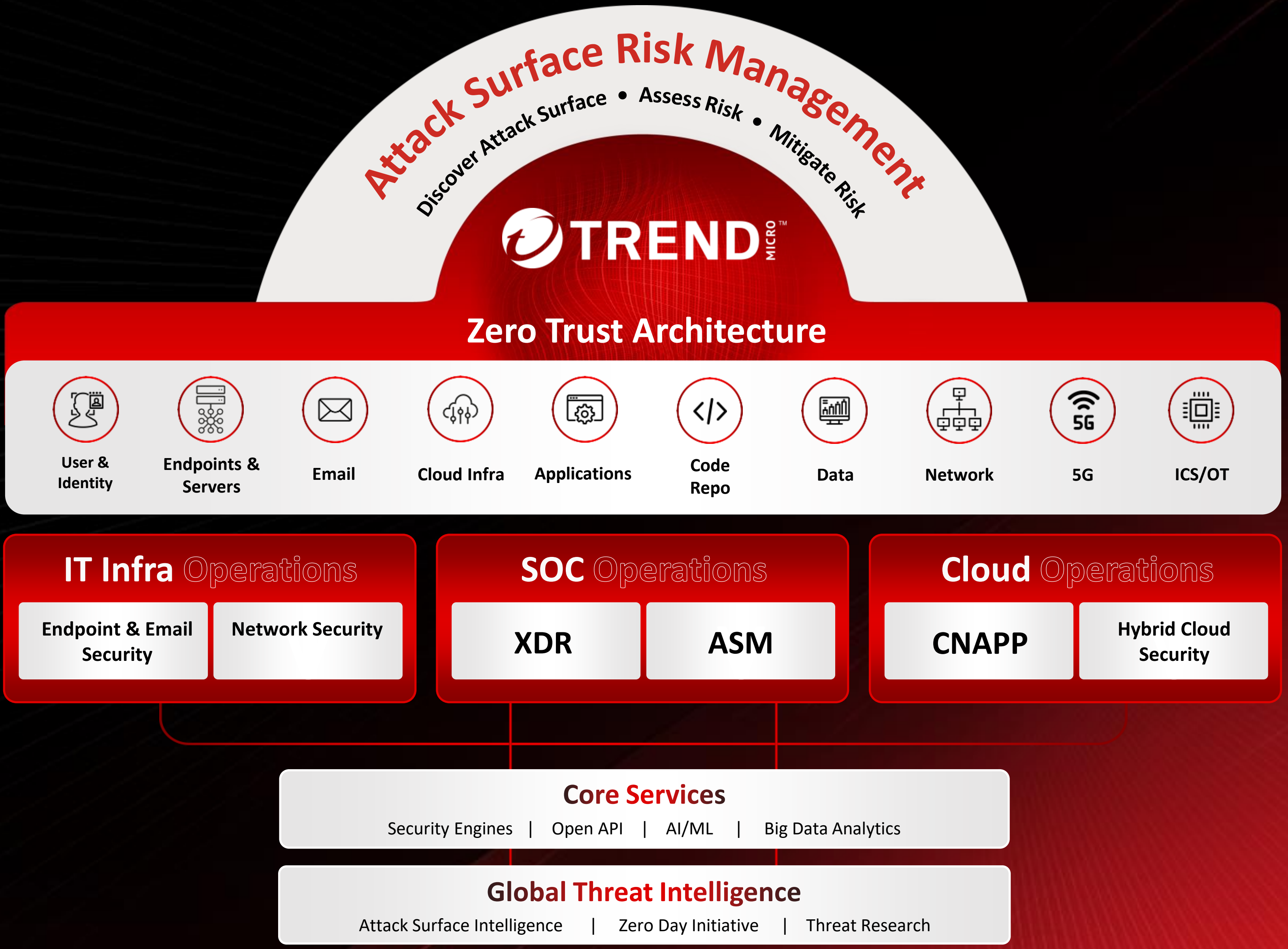
Reactive

XDR

Extended Detection and Response

- Detect
- Investigate
- Respond

Managed Services



Attack Surface Risk Management

Discover Attack Surface • Assess Risk • Mitigate Risk

TREND MICRO

Zero Trust Architecture

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

IT Infra Operations
- Endpoint & Email Security
- Network Security

SOC Operations
- XDR
- ASM

Cloud Operations
- CNAPP
- Hybrid Cloud Security

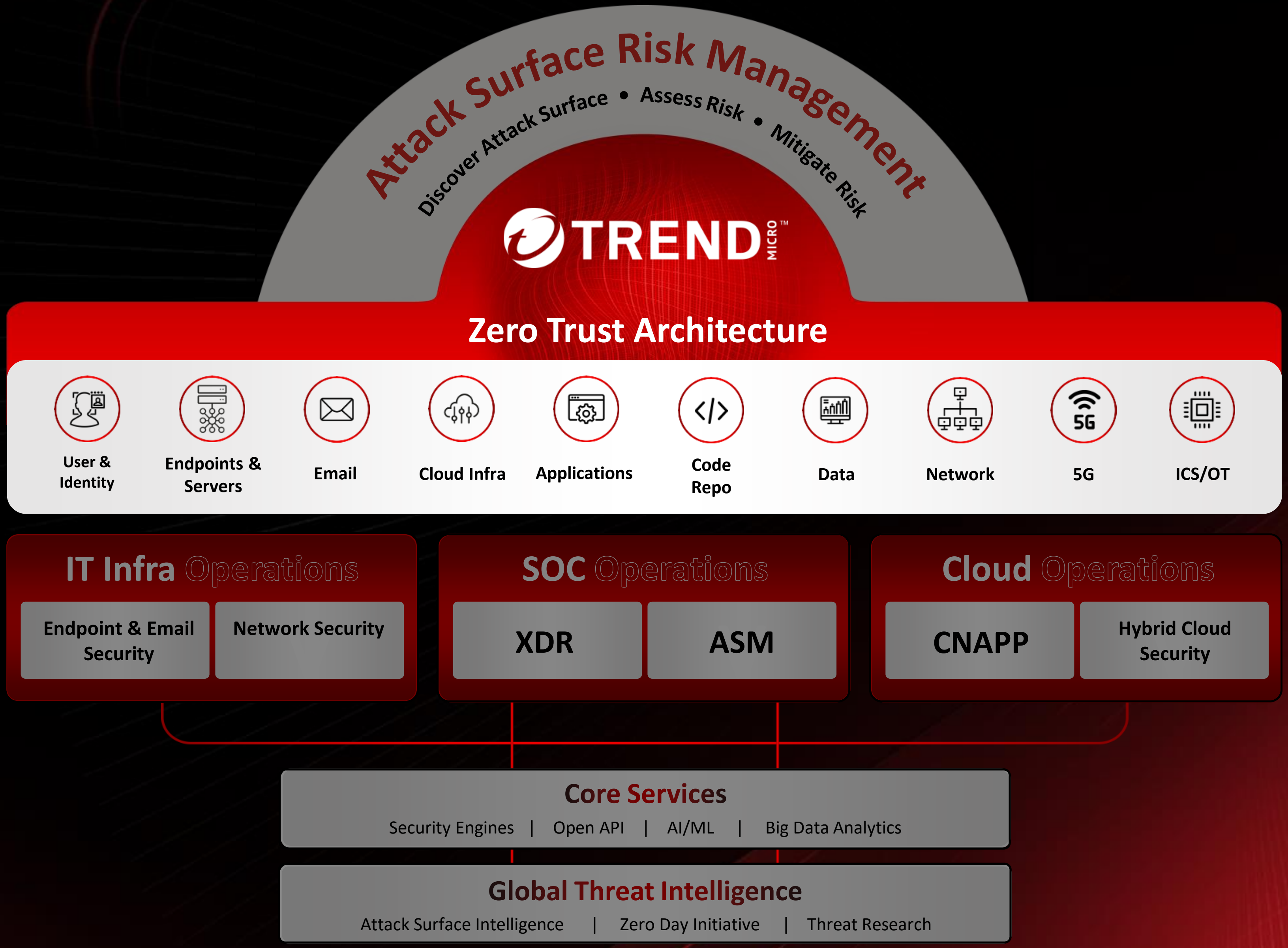
Core Services

Security Engines | Open API | AI/ML | Big Data Analytics

Global Threat Intelligence

Attack Surface Intelligence | Zero Day Initiative | Threat Research

Ecosystem Integration



Attack Surface Risk Management

Discover Attack Surface • Assess Risk • Mitigate Risk

Zero Trust Architecture

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

IT Infra Operations: Endpoint & Email Security | Network Security

SOC Operations: XDR | ASM

Cloud Operations: CNAPP | Hybrid Cloud Security

Core Services

Security Engines | Open API | AI/ML | Big Data Analytics

Global Threat Intelligence

Attack Surface Intelligence | Zero Day Initiative | Threat Research

Visibility and protection across all Zero Trust pillars

Continuous risk assessment

Automated security measures

Access control using in-the-moment risk analysis

Differentiators

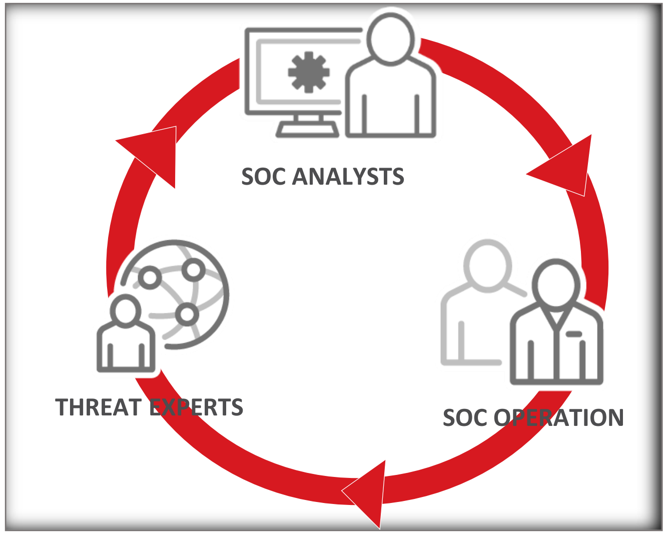
Integrated Attack Surface Risk Management and XDR platform

Helping security teams operationalize Zero Trust architectures to move security forward

Bridging technology gaps, streamlining consolidation, and delivering a clear solution path to the future

Why Trend Micro?

Industry-leading detection technologies managed and correlated by expert threat investigators



Threat Expertise and Intelligence

- Managed XDR operations team are Trend Micro employees (no outsourcing) with various expertise and rich experience within areas such as Trend Micro threat research, threat response, and technical support.
- Service leverages the Trend Micro™ Smart Protection Network™, EDR, XDR, and threat researchers across 15 global threat research centers, with a deep collective knowledge of threat techniques and actors.

Did you Know?

Managed XDR analysts have access to additional threat intelligence which is not shared outside of Trend Micro.

Trend Vision One

Security Operations
SOC and SecOps | CISO and CIO | IT Ops

Industry-leading XDR and EDR

- **Broadest** native XDR sensor coverage
- **Purpose-built** to ingest, analyze and act across multiple vectors

Attack Surface Risk Management

- Rapid attack surface discovery
- **Continuous risk assessment** and prioritization
- Proactive **risk and threat remediation**

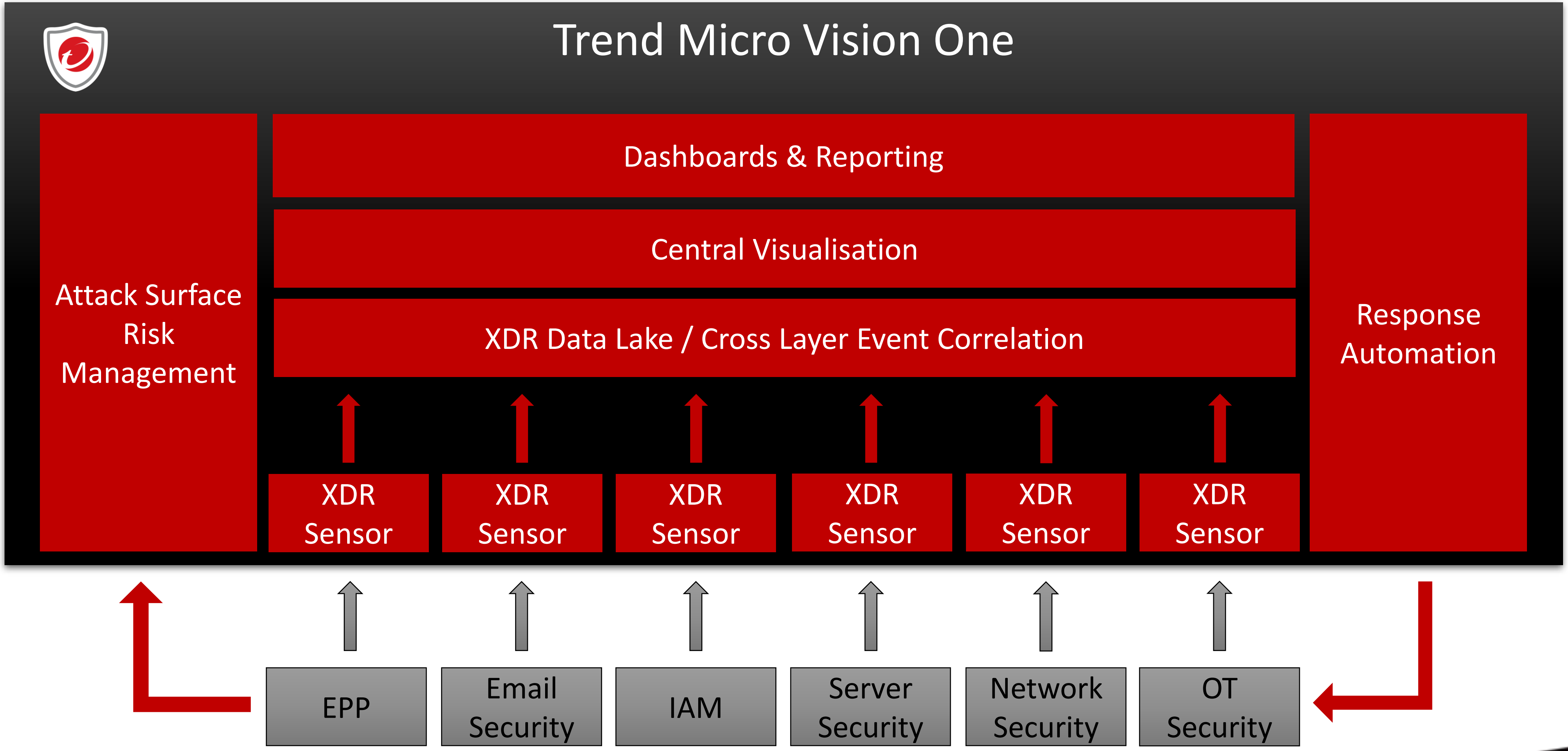
Zero Trust Secure Access

- Secure access for internet and private access
- Continuous **user and identity** assessment
- SSE/SASE with ZTNA, SWG, CASB

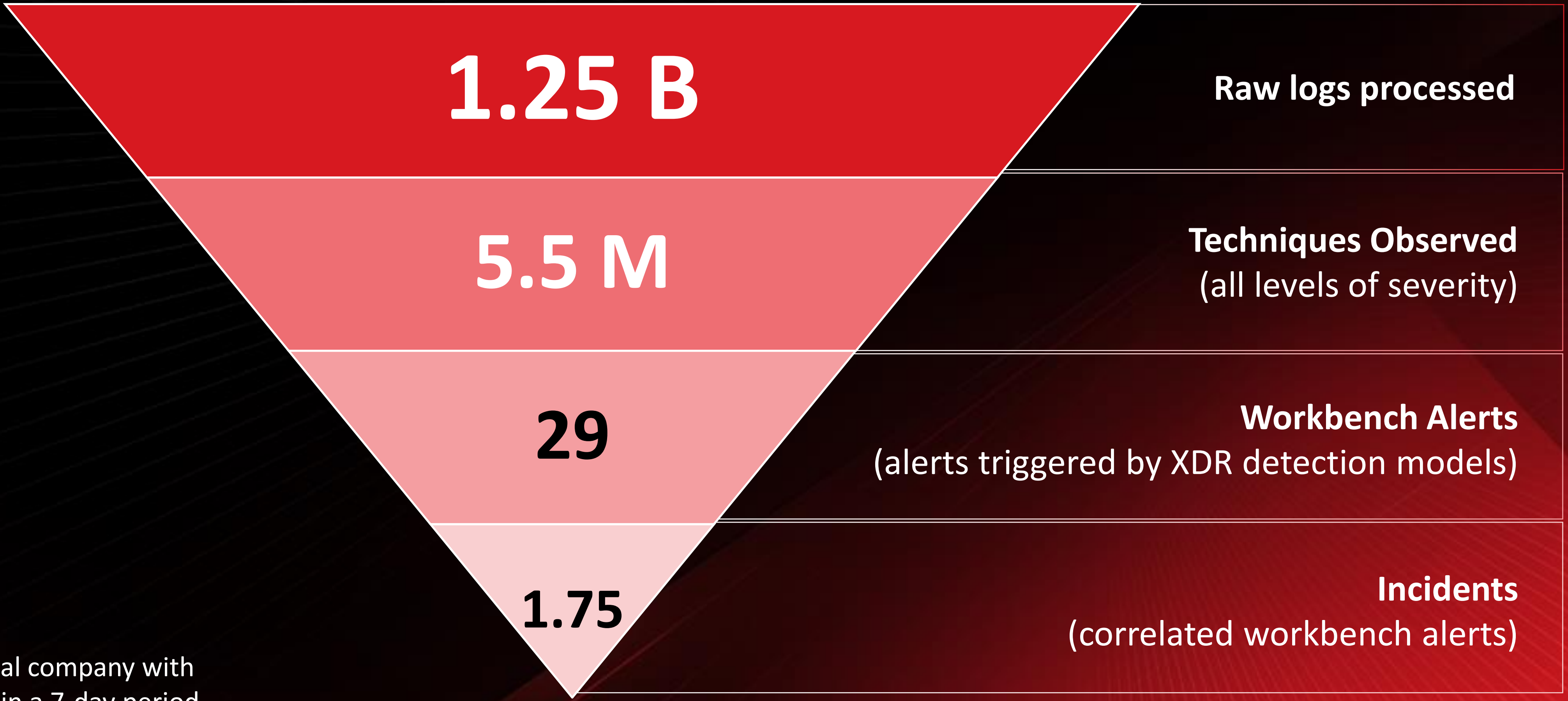
Central Visibility across Trend and third-party products

- Risk, Attack, Exposure **Indices**
- API-friendly platform with broad and growing integration ecosystem

Simplified Approach for SOC Light with TM Vision One



High Confidence Detections without Alert Overload



1.25 B — **Raw logs processed**

5.5 M — **Techniques Observed**
(all levels of severity)

29 — **Workbench Alerts**
(alerts triggered by XDR detection models)

1.75 — **Incidents**
(correlated workbench alerts)

Based on a real company with
1000 devices in a 7-day period

Bringing Simplicity to SOC Operations

TREND MICRO | research

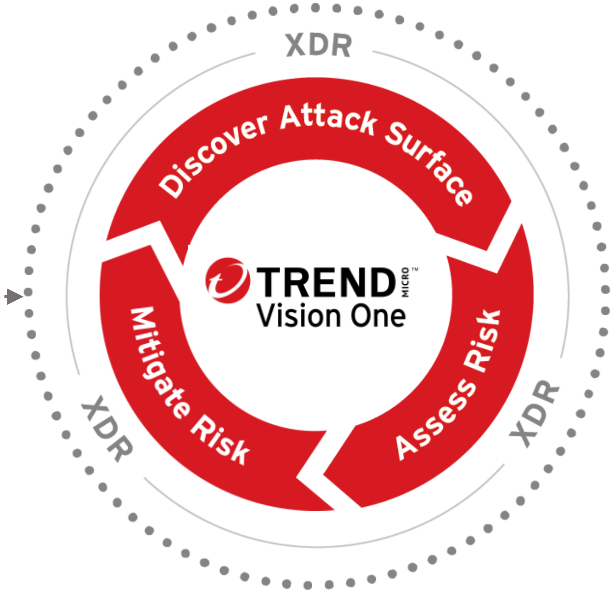
TREND MICRO SMART Protection Network™

ZERO DAY INITIATIVE

IOCs shared by:

Government Agencies
Security information sharing organizations
Independent Security Researchers
Third-Party Detections sourced from your SIEM
Corporate Security Teams
Other Security Vendors
Third-party TAXII/MISP

XDR Sensor Data (endpoint, email, network, etc.)



Centralized Risk Assessment
Centralized Investigation
Centralized Response
Centralized Cross-Vendor Block Lists

Automated or Manual Response

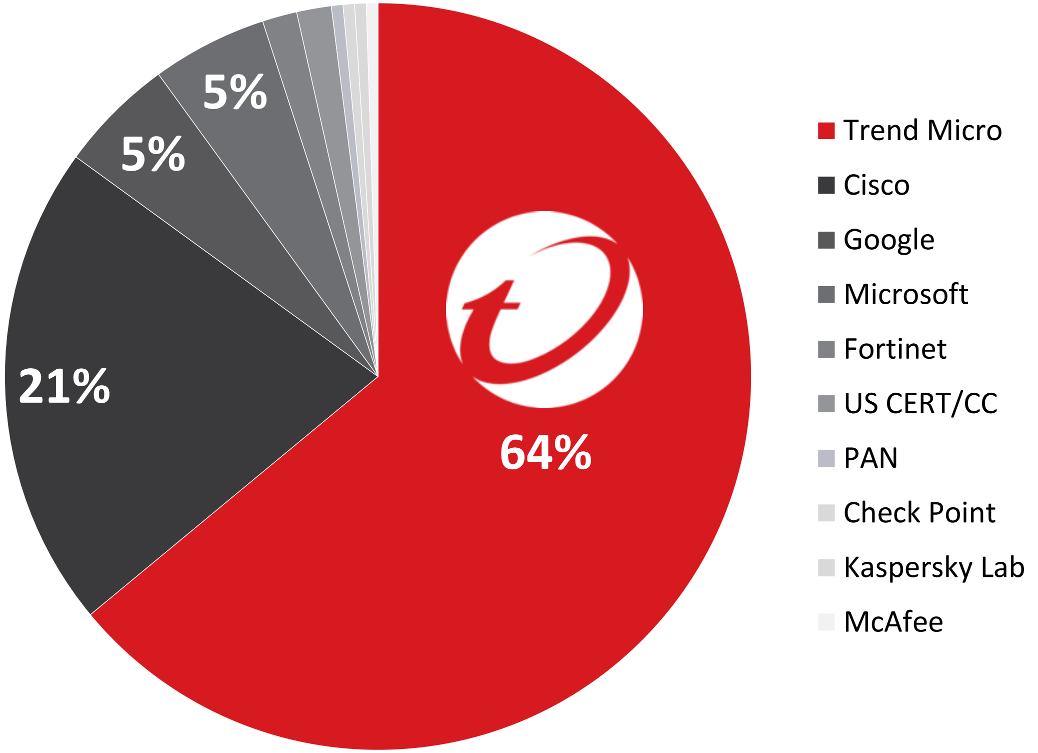
- Quarantine or Delete Emails
- User Password Reset or Disable Account
- Endpoint Isolation
- URL Blocking
- Network Firewall Rules
- Cloud Sandboxing

OMDIA – Market Leader in Vulnerability Disclosure

ZERO DAY INITIATIVE

- **10,000+** independent vulnerability researchers
- Market leader in the public disclosure market for past 14 years, discovering & reporting **64% of the vulnerabilities** in 2021
- **Most** disclosed high impact vulnerabilities (critical + high severity)

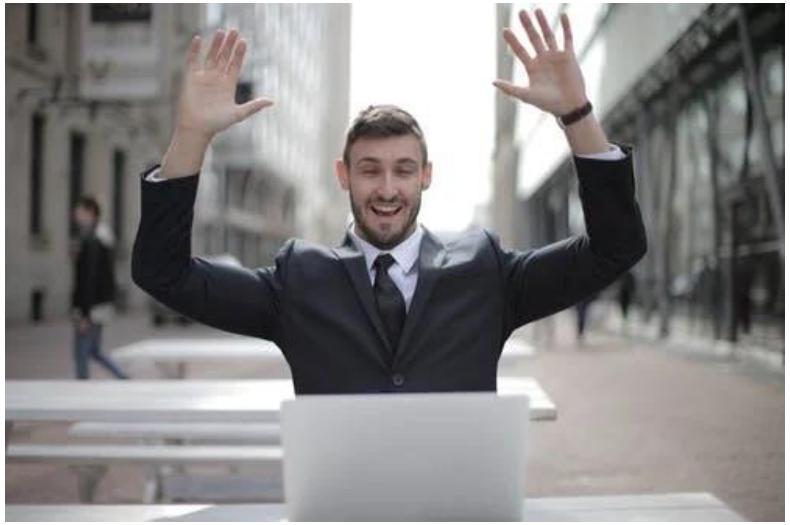
Source: Quantifying the Public Vulnerability Market, Omdia, May 2022



Virtual Patching

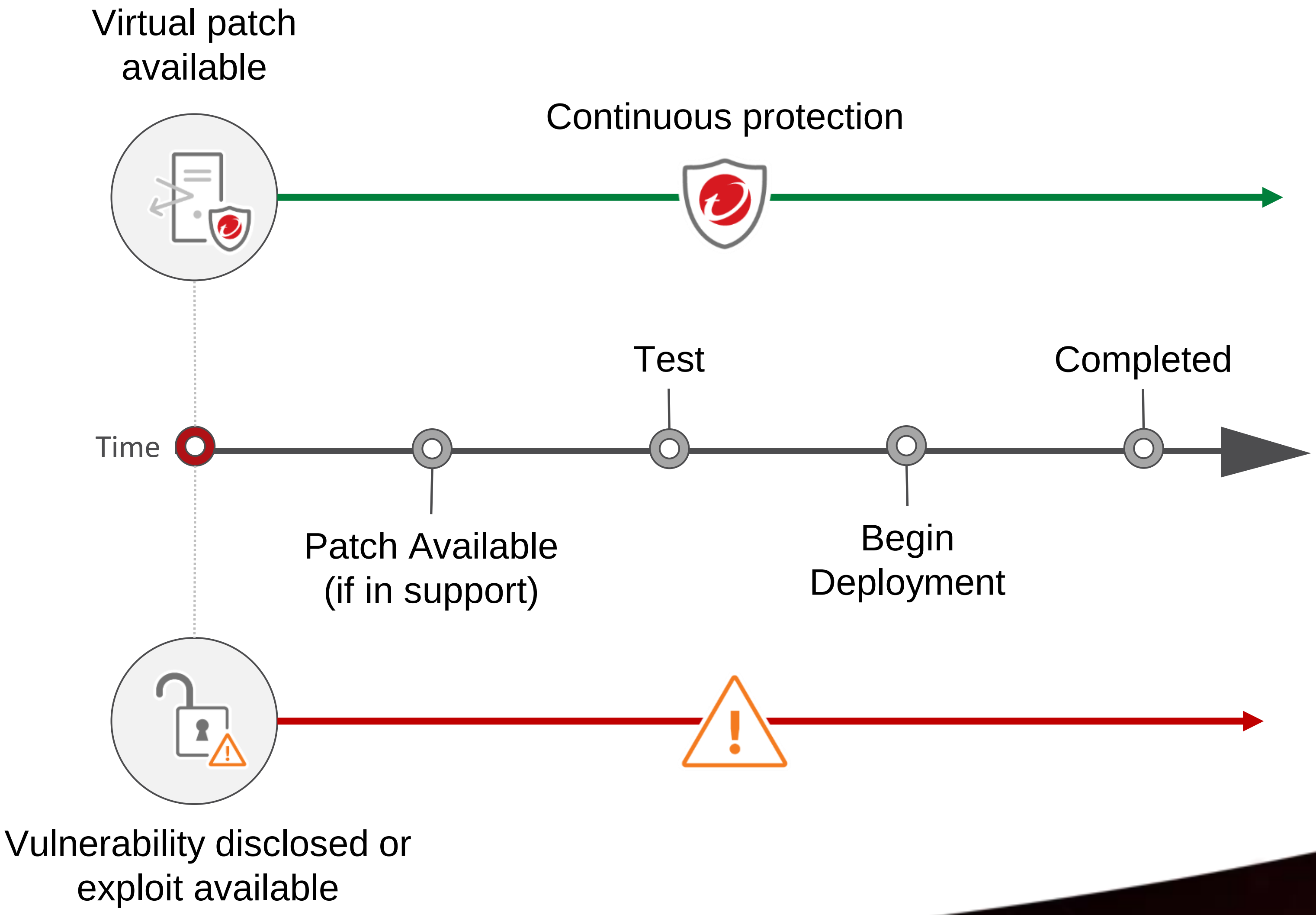
Solution for relaxing patch management

- Apex One / Worry-Free
  - This solution offers with virtual patching a protection for a multitude of endpoints
- Deep Security / Cloud One
  - Offers virtual patches to protect Cloud Workloads, Server, Container against networks based threats in criticals application and operating systems.
- Tipping Point
  - Provides virtual patches which protects Cloud Workloads, Server against network-exploitable vulnerabilities
- TXone
  - Vulnerability protection with virtual patching for productions environments, Health Care, Smart Factories etc.



Virtual Patching / Reduce operational impacts

- Reduce operational costs of emergency & ongoing patching.
- Protect systems where no patches will be provided.
- Secure server and application-level vulnerabilities.



TREND MICRO™

BECHTLE

Trend Micro Solution Overview

[redacted]

Trend Micro One

A unified cybersecurity platform

BECHTLE

Discover Attack Surface → Assess Risk → Mitigate Risk

Managed Services

Trend Micro Service One

- Managed XDR
- Incident response
- Targeted attack detection
- Onboarding and health monitoring
- 24*7 global support

Security Operations

Trend Micro Vision One

XDR – Extended Detection and Response

- Hunt, detect, investigate and respond
- Native sensors plus 3rd party integrations

Central visibility

- Single, unified threat defense console
- Correlated activity view across security layers

Attack Surface Risk insights

- Cyber risk indices and trending
- Attack surface visibility

Threat assessment

- Threat intelligence and assessment tools
- MITRE ATT&CK mapping

Reporting

- Security posture dashboards
- Executive reporting views

Endpoint and Email Security

Trend Micro Workforce One

- Ransomware prevention and rollback
- Data loss prevention
- Vulnerability protection
- Phishing protection for Microsoft 365

Endpoints · Email · SaaS Applications · Mobile

Cloud Security

Trend Micro Cloud One

- Cloud misconfiguration and compliance
- Open source repository analysis
- Virtual patching
- Ransomware protection

Cloud Accounts · Workloads & VMs · Cloud Native Applications · File/Object Storage · Cloud Network

Network Security

Trend Micro Network One

- Network vulnerability protection
- Unmanaged device visibility
- Advanced network analysis
- Zero trust access

Enterprise Network · ICS / OT · Secure Access Service Edge

Common Services

Security Engines

- Machine learning, behavioral analysis, virtual patching, app control, anti-malware, integrity monitoring, etc.
- Cloud sandbox

Big Data Analytics

- Data architecture
- Data lake
- Analytics and reporting

SaaS Architecture

- Multi-geo infrastructure
- Role-based access control (RBAC)
- Multi-factor authentication

Global Threat Intelligence

Attack Surface Intelligence

- Native sensors across cloud, endpoint, email, network and IoT
- Expert human intelligence with advanced machine automation

Threat Research

- Vulnerability analysis and public disclosure (Zero Day Initiative)
- Future threat research

Cybercriminals

- Underground research
- Investigation and law enforcement support

APIs

Ecosystem Integration

SIEM / SOAR

splunk> · paloalto · IBM QRadar · FORTINET

Cloud Service Providers

aws · Microsoft Azure · Google Cloud

Vulnerability Assessment

QUALYS · RAPID7 · tenable

External Attack Surface Management

BIT DISCOVERY

Identity and Access Management

okta · Active Directory · Azure Active Directory

Environments and Apps

Microsoft 365 · Google · box · Windows · android · docker · kubernetes · vmware · servicenow

Make the world safe for exchanging digital information

Simplify and secure your connected World

Fueled by decades of security expertise, global threat research, and continuous innovation

People

We have 7,000 security experts, fiercely focused and passionate about security

Values

With core values focused on innovation, we are securing an ever-evolving IT and threat landscape

Merci!

Des questions? Contactez-nous: it-forum.ch@bechtle.com

Plus d‘informations :
bechtle.com