TREND MICRO™

Secure Innovation, Not Slower Innovation

Andrew Philp
Field CISO, ANZ
Trend Micro

Digital Transformation is Everywhere

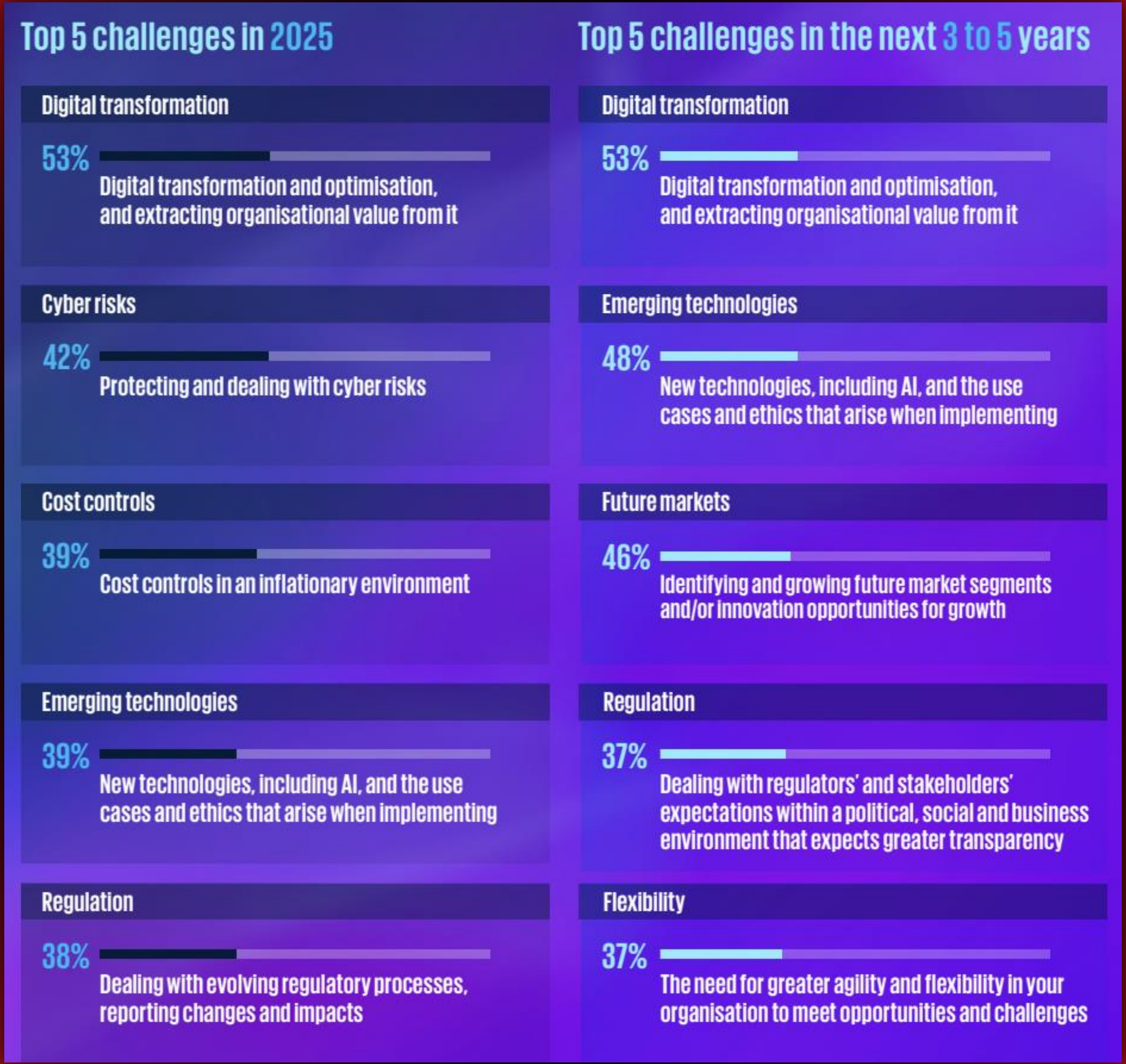
But it’s Keeping People Up at Night

KPMG

Keeping us up at night

The big issues facing business leaders in 2025

Sources
https://assets.kpmg.com/content/dam/kpmg/au/pdf/2025/keeping-us-up-at-night-2025.pdf



Top 5 challenges in 2025

Digital transformation

53% Digital transformation and optimisation, and extracting organisational value from it

Cyber risks

42% Protecting and dealing with cyber risks

Cost controls

39% Cost controls in an inflationary environment

Emerging technologies

39% New technologies, including AI, and the use cases and ethics that arise when implementing

Regulation

38% Dealing with evolving regulatory processes, reporting changes and impacts

Top 5 challenges in the next 3 to 5 years

Digital transformation

53% Digital transformation and optimisation, and extracting organisational value from it

Emerging technologies

48% New technologies, including AI, and the use cases and ethics that arise when implementing

Future markets

46% Identifying and growing future market segments and/or innovation opportunities for growth

Regulation

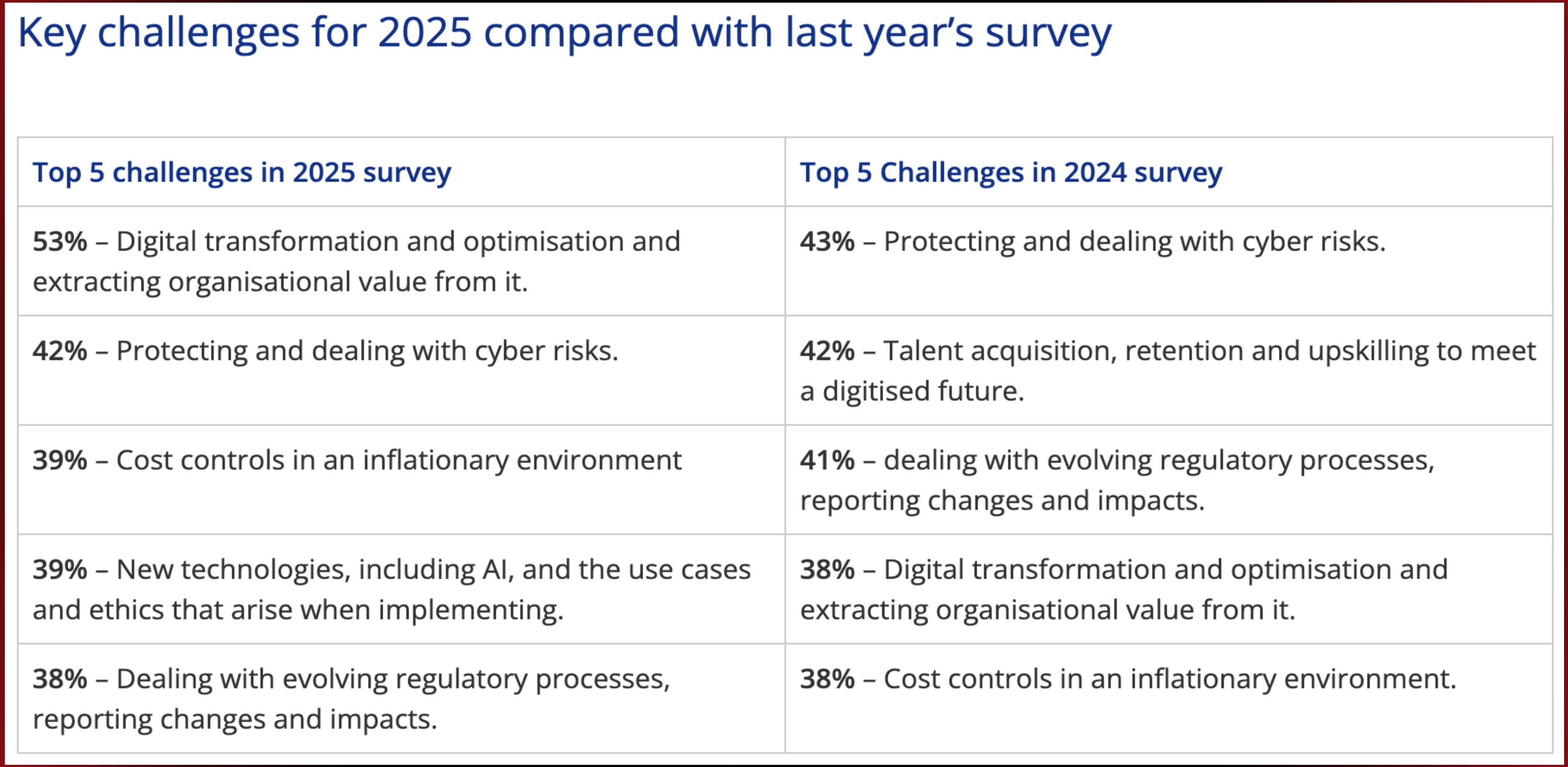
37% Dealing with regulators' and stakeholders' expectations within a political, social and business environment that expects greater transparency

Flexibility

37% The need for greater agility and flexibility in your organisation to meet opportunities and challenges

Sources
https://assets.kpmg.com/content/dam/kpmg/au/pdf/2025/keeping-us-up-at-night-2025.pdf

Which are Getting More Focus

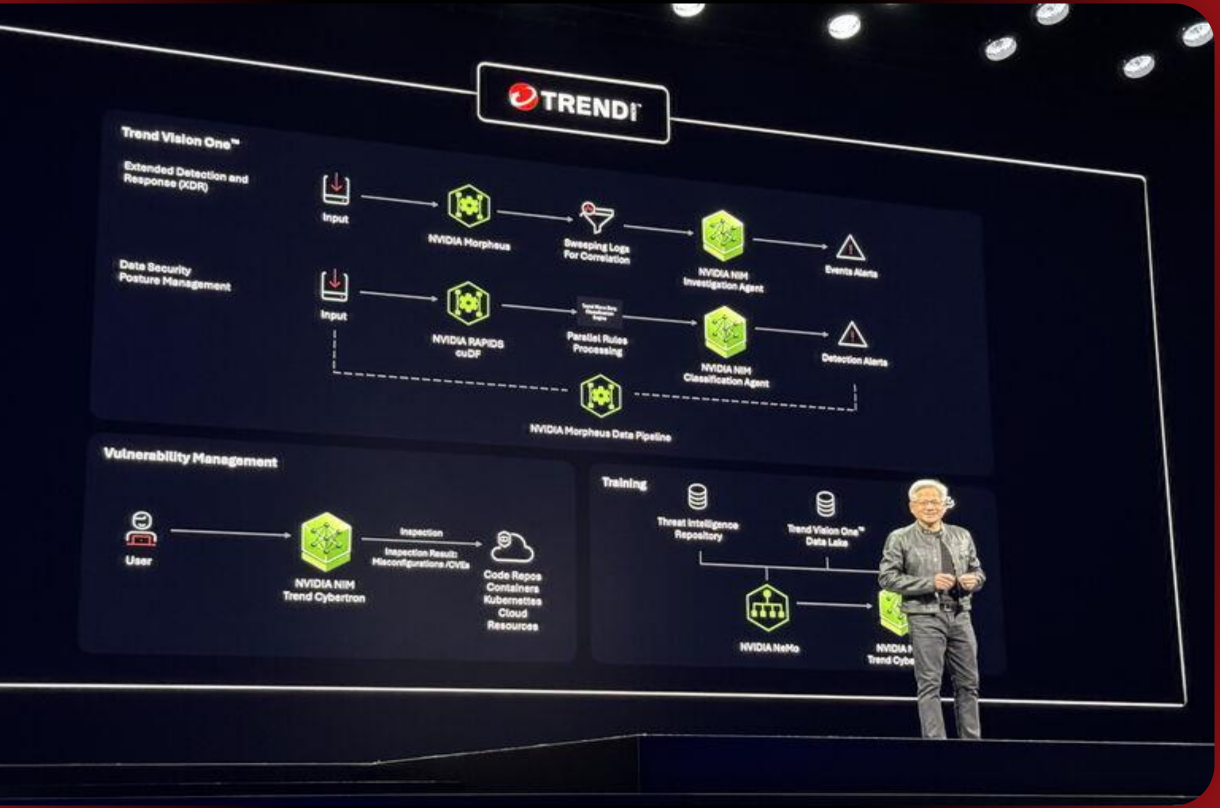


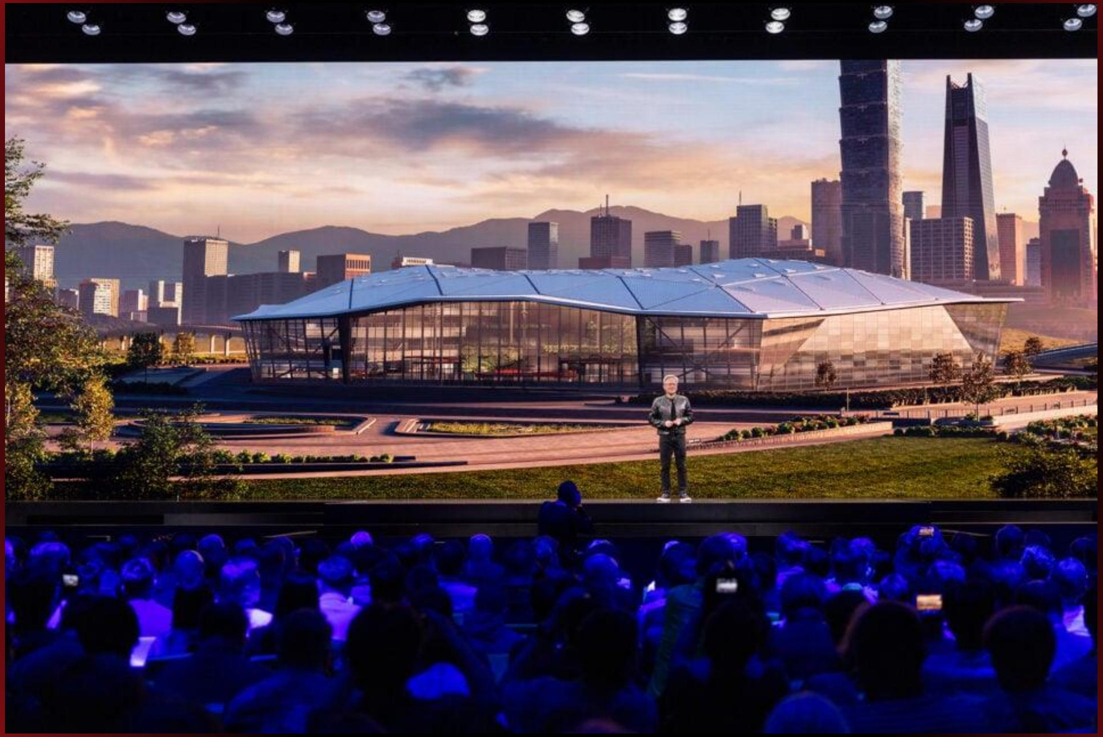
Key challenges for 2025 compared with last year's survey

Top 5 challenges in 2025 survey	Top 5 Challenges in 2024 survey
53% – Digital transformation and optimisation and extracting organisational value from it.	**43%** – Protecting and dealing with cyber risks.
42% – Protecting and dealing with cyber risks.	**42%** – Talent acquisition, retention and upskilling to meet a digitised future.
39% – Cost controls in an inflationary environment	**41%** – dealing with evolving regulatory processes, reporting changes and impacts.
39% – New technologies, including AI, and the use cases and ethics that arise when implementing.	**38%** – Digital transformation and optimisation and extracting organisational value from it.
38% – Dealing with evolving regulatory processes, reporting changes and impacts.	**38%** – Cost controls in an inflationary environment.

Sources
https://kpmg.com/au/en/home/media/press-releases/2025/01/2025-business-game-changers-ai-costs-housing.html

AI Transformation


TRENDi
Trend Vision One™
Extended Detection and Response (XDR)
Input
NVIDIA Morpheus
Sweeping Logs For Correlation
NVIDIA NIM Investigation Agent
Events Alerts
Data Security Posture Management
Input
NVIDIA RAPIDS cuDF
Parallel Rules Processing
NVIDIA NIM Classification Agent
Detection Alerts
NVIDIA Morpheus Data Pipeline
Vulnerability Management
User
NVIDIA NIM Trend Cybertron
Inspection
Inspection Result: Misconfigurations /CVEs
Code Repos Containers Kubernettes Cloud Resources
Training
Threat Intelligence Repository
Trend Vision One™ Data Lake
NVIDIA NeMo
NVIDIA N
Trend Cybe



Computex 2025

How is this possible | GTC 2025

”Huangs Law” GPU 25x faster in last 5 years compared to 10x for CPU (Moore’s Law)

Single rack - Grace Blackwell, **1,800kg**, **120KW**, *36 CPU’s* and **72 GPUS** connected with **5,000 cables** (NVlink) to operate as one, **13.5TB memory**

NVlink throughput **88x peak** total internet throughput (130TB/s)

1,000 times computation increase in 8 years

xAI’s Data Centre

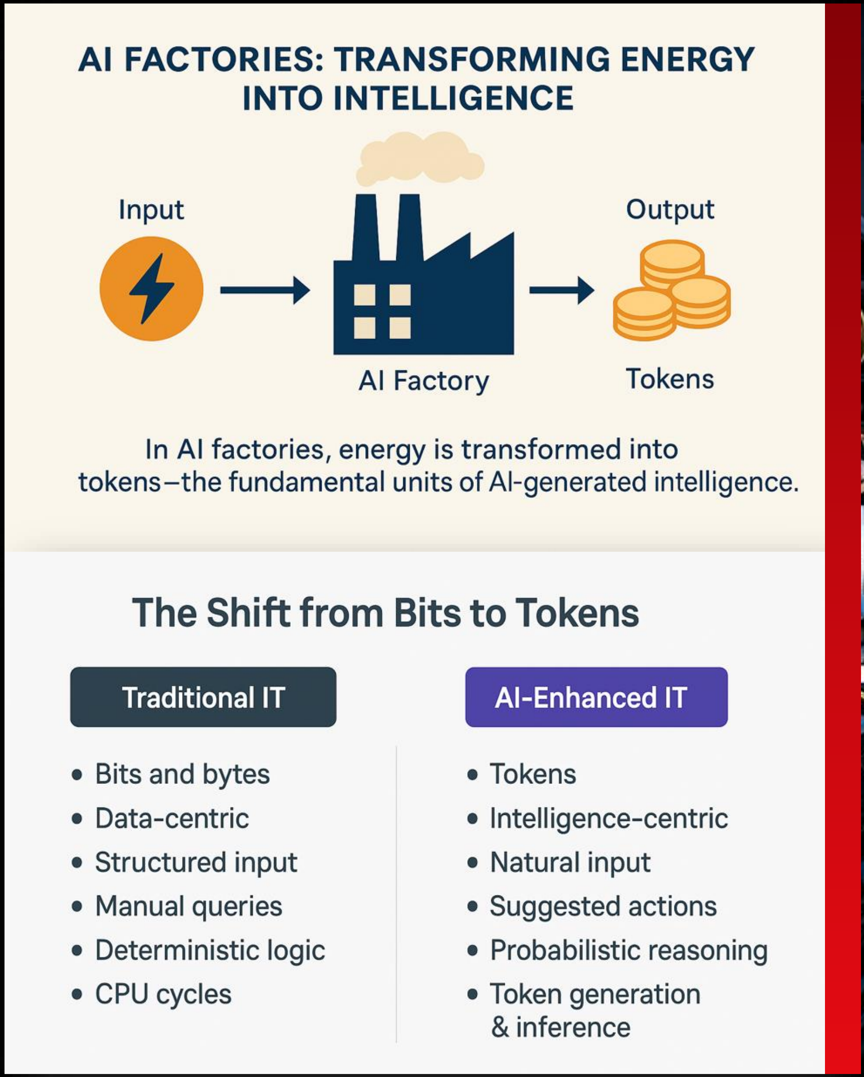
'Colossus’, from empty old Electrolux factory (73k sqm) to 100,000 GPU AI Factory

With approx 12.5k servers and 1.5k Racks – all in 4 months (late 2024)

‘Training’ power load approx. 100MW

Grown to approx. 200k GPU max power load around 300-400MW (equivalent to ~ Hamilton’s power load)

AI Factories



AI FACTORIES: TRANSFORMING ENERGY INTO INTELLIGENCE

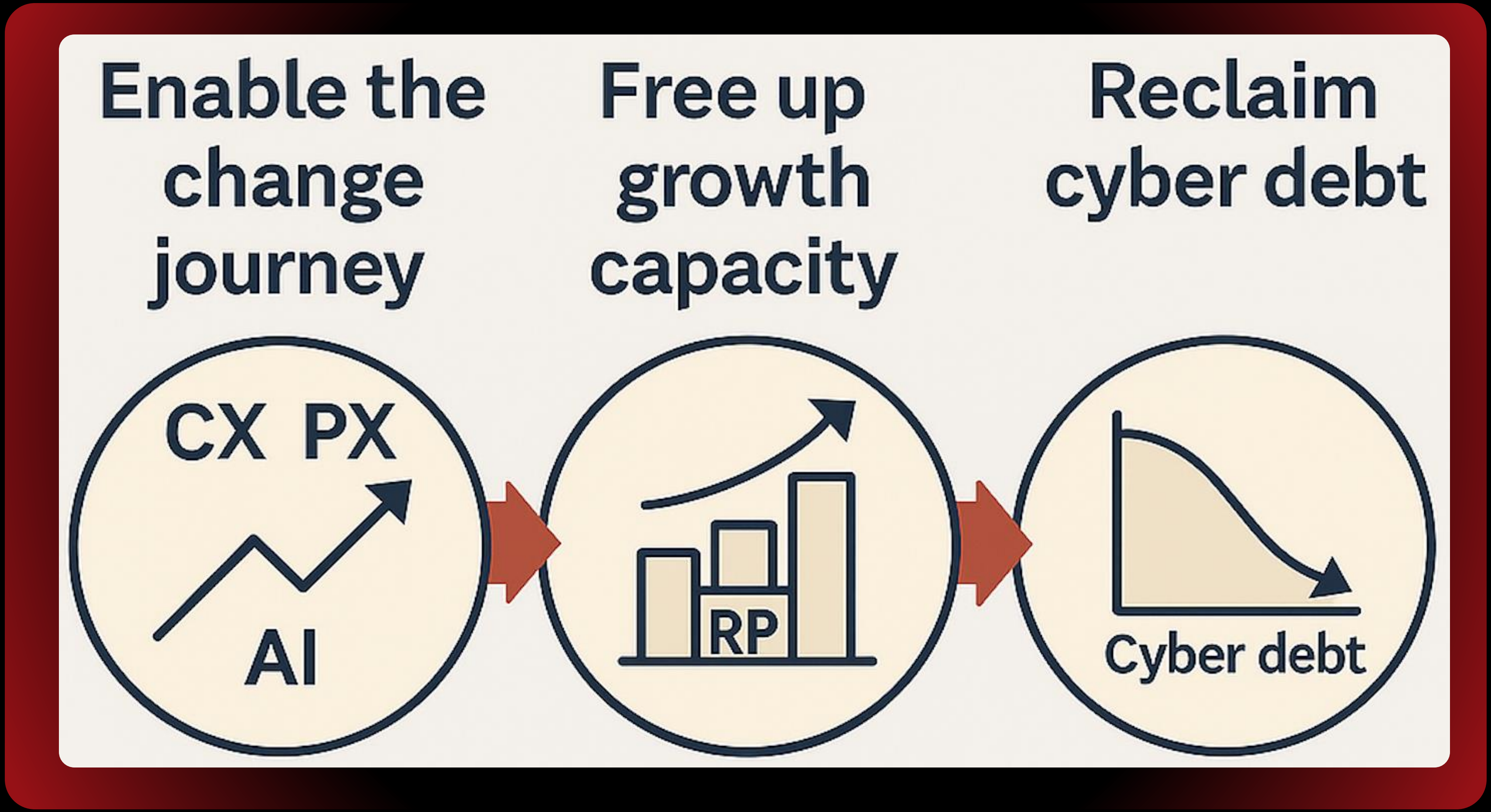
In AI factories, energy is transformed into tokens—the fundamental units of AI-generated intelligence.

The Shift from Bits to Tokens

Traditional IT	AI-Enhanced IT
Bits and bytes	Tokens
Data-centric	Intelligence-centric
Structured input	Natural input
Manual queries	Suggested actions
Deterministic logic	Probabilistic reasoning
CPU cycles	Token generation & inference

Change | Capacity | Budget

Sources;
Daniel Gregory, Principal Security Strategist, Trend Micro



Key transformative areas;
CX: Cloud and DC Exit
PX: Process Digitalisation
AI: Artificial Intelligence

Re-purpose risk provisions

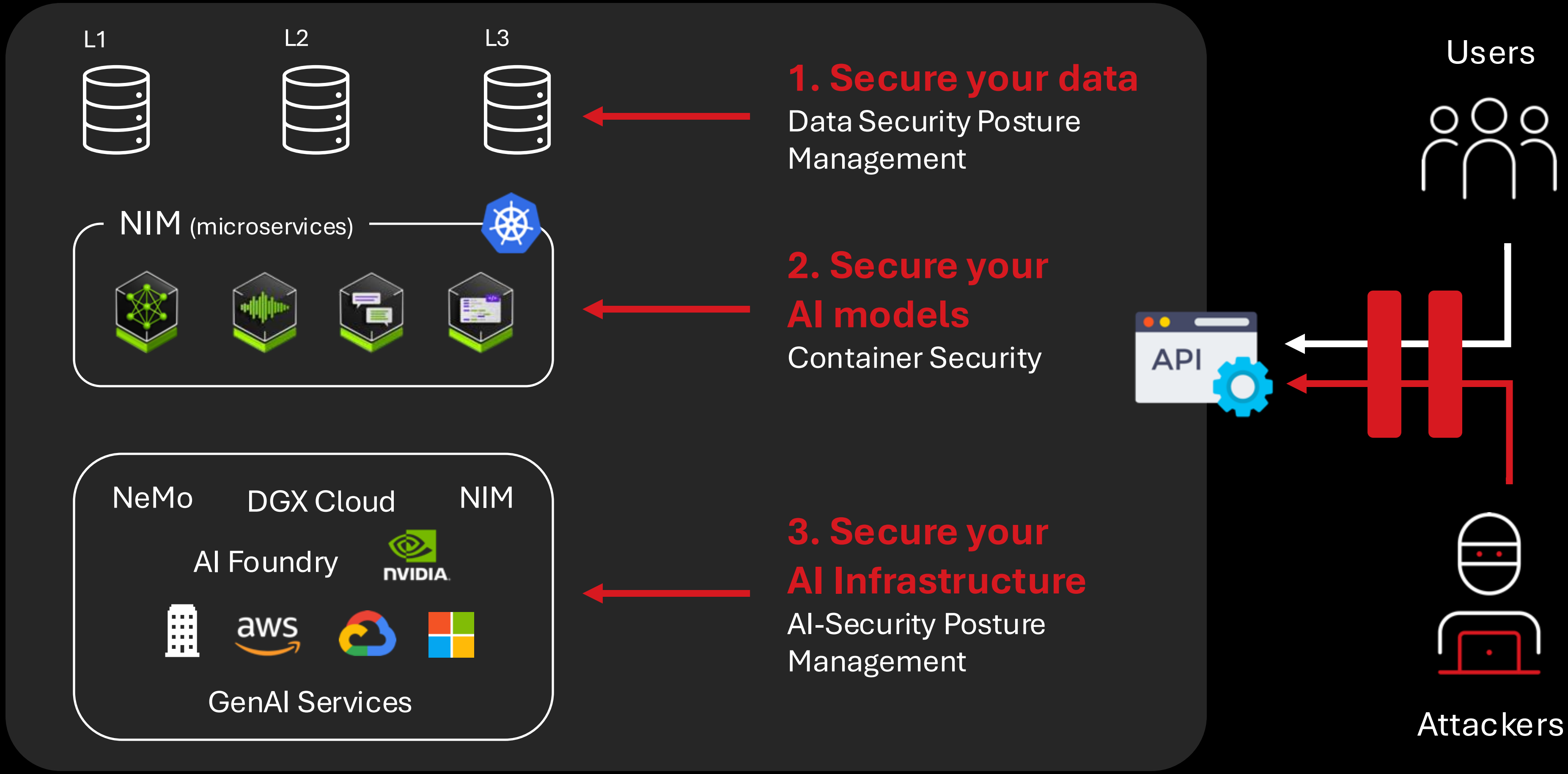
Retire wasteful mitigations

The need for Proactive Security and Cyber Risk Management

“While we are seemingly on the cusp of unimaginable benefits associated with the adoption of AI, we should remember that from a business leadership perspective, having responsibility creates pressure”

Sources
https://assets.kpmg.com/content/dam/kpmg/au/pdf/2025/keeping-us-up-at-night-2025.pdf

Customer Use Case - Securing your AI Stack



1. Secure your data
Data Security Posture Management

2. Secure your AI models
Container Security

3. Secure your AI Infrastructure
AI-Security Posture Management

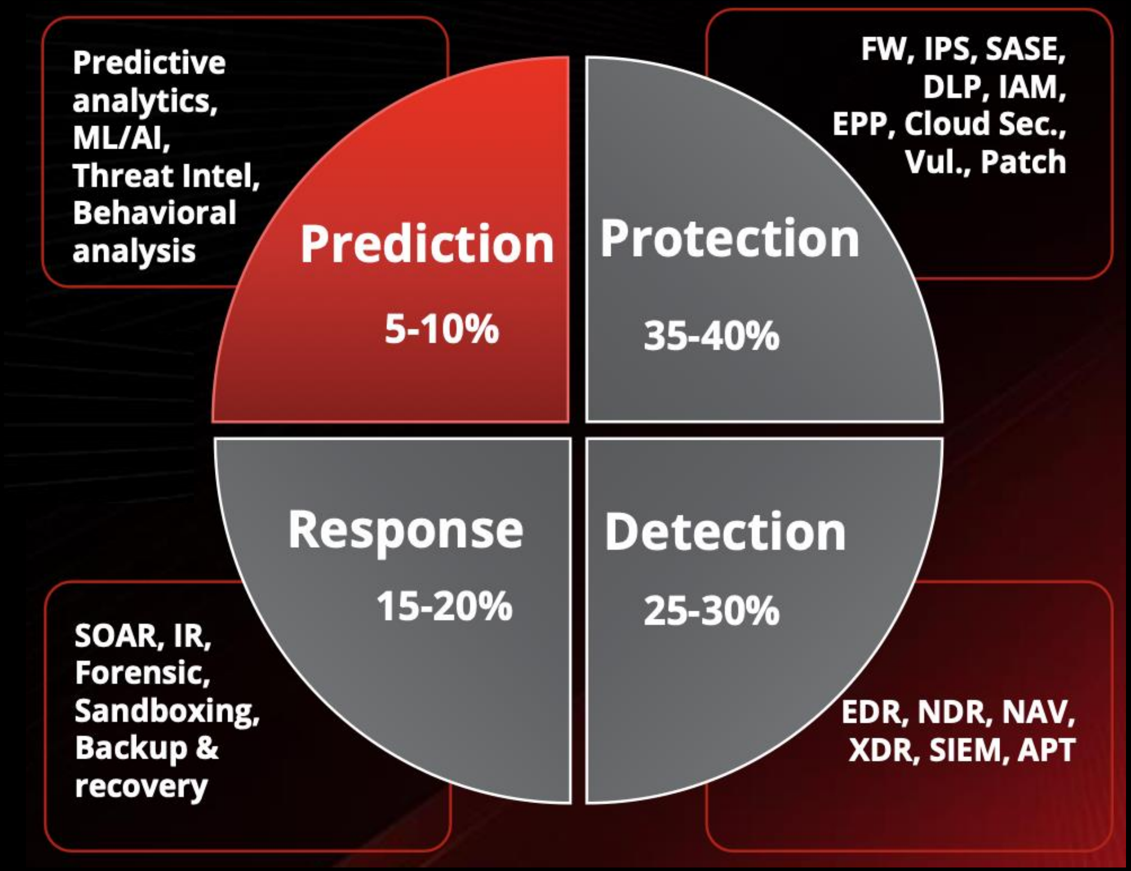
4. Secure your users & local AI apps
Deepfake Detection & Endpoint Security

5. Secure access to AI services
AI Services Access

6. Defend against Zero-Day exploits
Network IDS/IPS

NIM: a set of accelerated inference microservices to run AI models
NeMo: an end-to-end platform for developing custom generative AI

Achieving Proactive Security



Predictive analytics, ML/AI, Threat Intel, Behavioral analysis
Prediction
5-10%
FW, IPS, SASE, DLP, IAM, EPP, Cloud Sec., Vul., Patch
Protection
35-40%
Response
15-20%
SOAR, IR, Forensic, Sandboxing, Backup & recovery
Detection
25-30%
EDR, NDR, NAV, XDR, SIEM, APT

65%

CONDUCT VULNERABILITY ASSESSMENTS **MONTHLY OR FURTHER** APART

60%

EXPERIENCE SECURITY INCIDENTS DUE TO **LACK OF VISIBILITY**

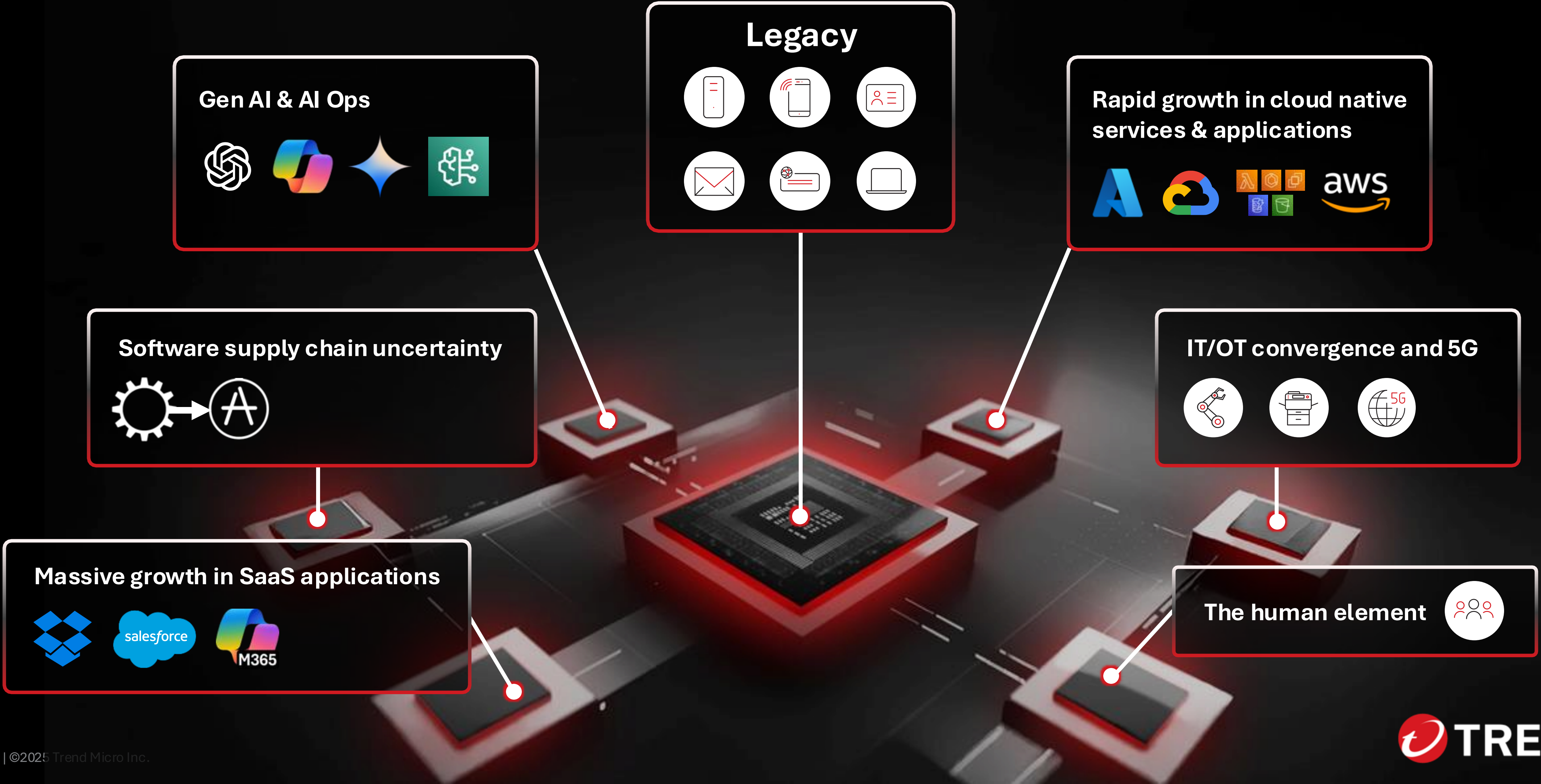
Source: Trend Cyber Risk & AI Study, 2025

81%

CAN DETECT & RESPOND TO MISCONFIGURATIONS & EXPOSED VULNERABILITIES **WITHIN A FEW HOURS**

Source: Trend Cyber Risk & AI Study, 2025

Complexity & Scale of Attack Surface



Legacy

Gen AI & AI Ops

Rapid growth in cloud native services & applications

Software supply chain uncertainty

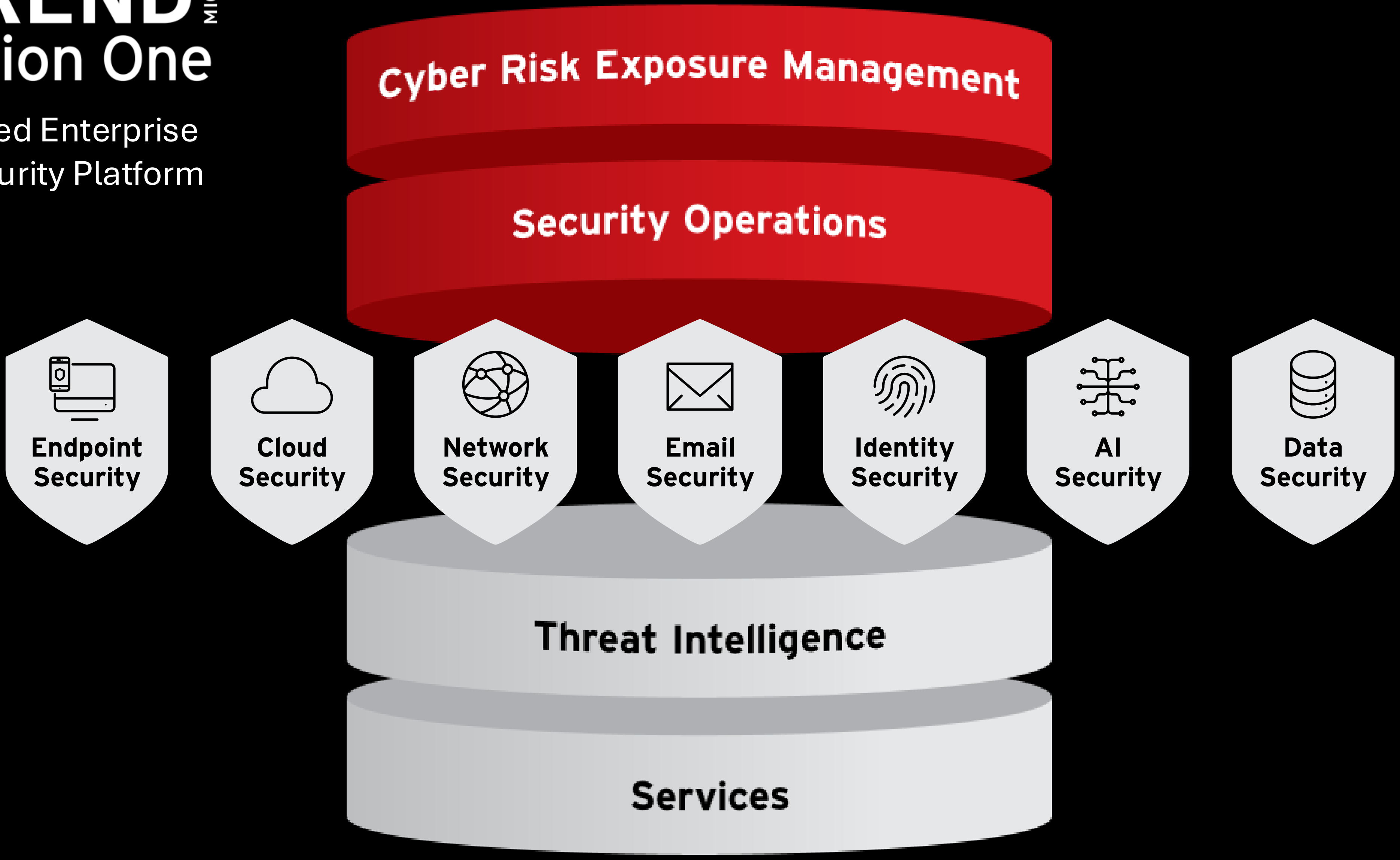
IT/OT convergence and 5G

Massive growth in SaaS applications

The human element

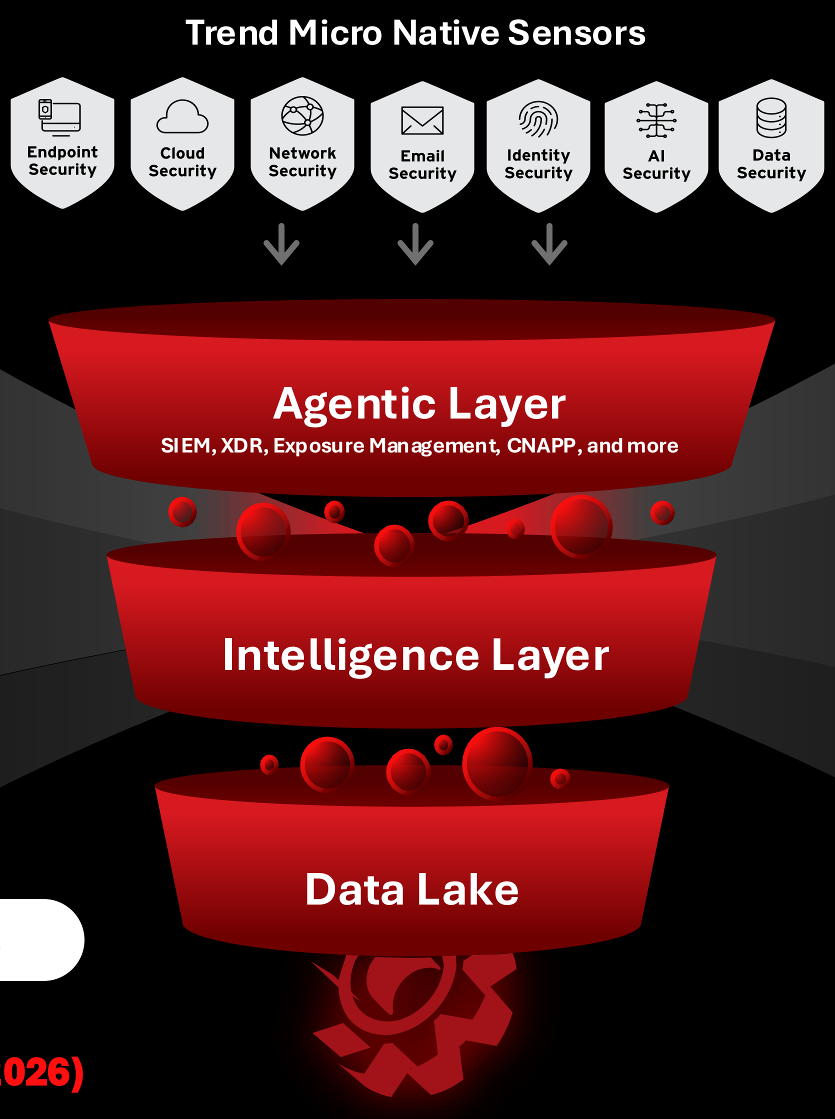
TREND MICRO™ Vision One

AI-Powered Enterprise Cybersecurity Platform



SaaS On-premises GovCloud Private cloud For service providers

Trend Vision One™ Ecosystem



Trend Micro Native Sensors

Endpoint Security

Cloud Security

Network Security

Email Security

Identity Security

AI Security

Data Security

Agentic Layer

SIEM, XDR, Exposure Management, CNAPP, and more

Intelligence Layer

Data Lake

Third-Party

SONICWALL

aws

f5

netskope

Barracuda

cisco

CHECK POINT

paloalto NETWORKS

FORTINET

CROWDSTRIKE

Forcepoint

okta

Azure

zscaler

Google Cloud

Microsoft

Third-Party

NOZOMI NETWORKS

servicenow

Microsoft

RAPID7

sumo logic

CYBERARK

Greenbone

tenable

Qualys

exabeam

RELIAQUEST

Google

Microsoft Sentinel

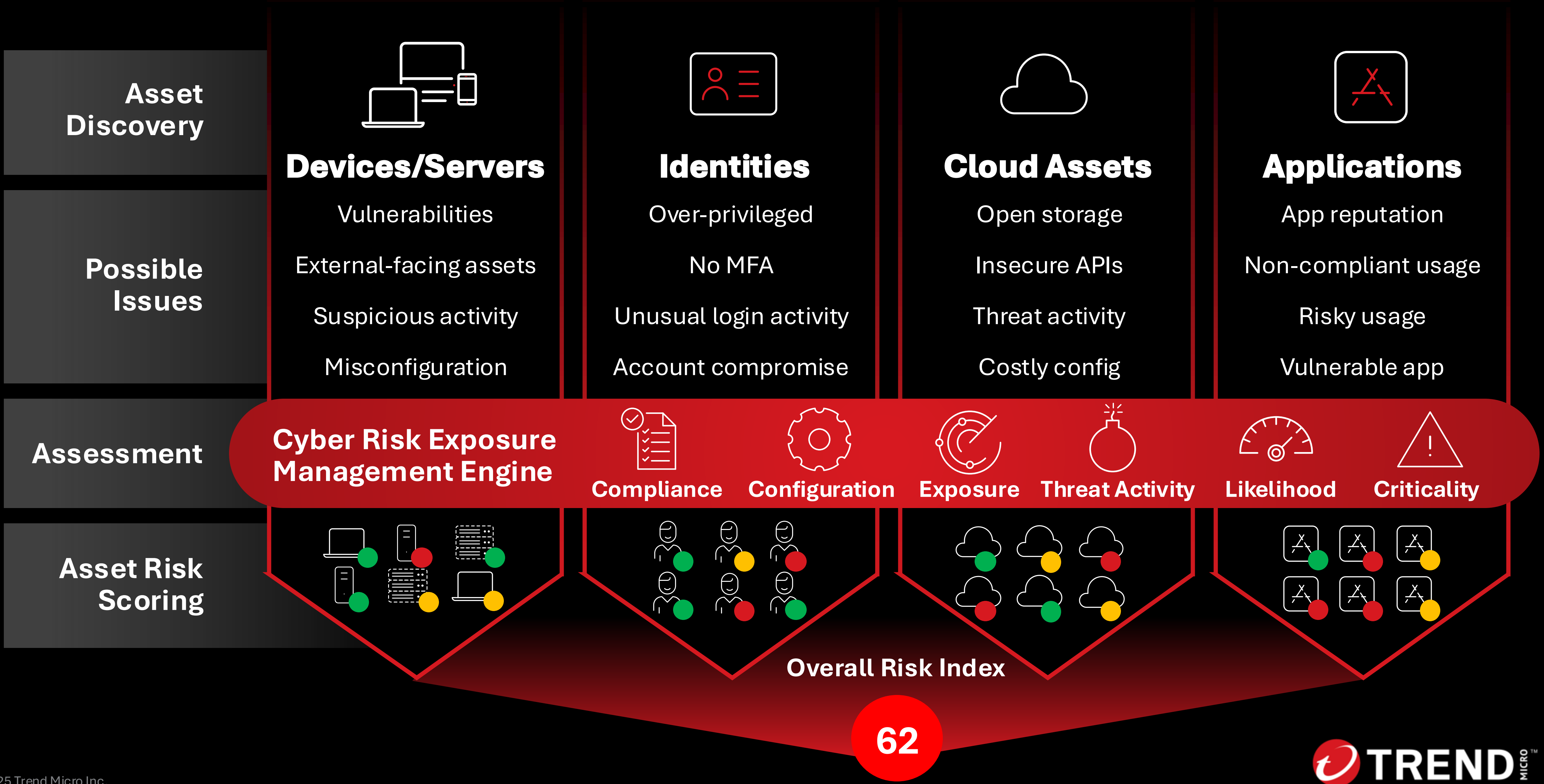
ATLASSIAN

... and more

900+ Third-Party Data Sources

Supporting Any Logs in 3 days (2025) **in 3 hours (2026)**

How Cyber Risk Exposure Management works



	Devices/Servers	Identities	Cloud Assets	Applications
Asset Discovery	Devices/Servers	Identities	Cloud Assets	Applications
Possible Issues	Vulnerabilities External-facing assets Suspicious activity Misconfiguration	Over-privileged No MFA Unusual login activity Account compromise	Open storage Insecure APIs Threat activity Costly config	App reputation Non-compliant usage Risky usage Vulnerable app

Assessment

Cyber Risk Exposure Management Engine

Compliance

Configuration

Exposure

Threat Activity

Likelihood

Criticality

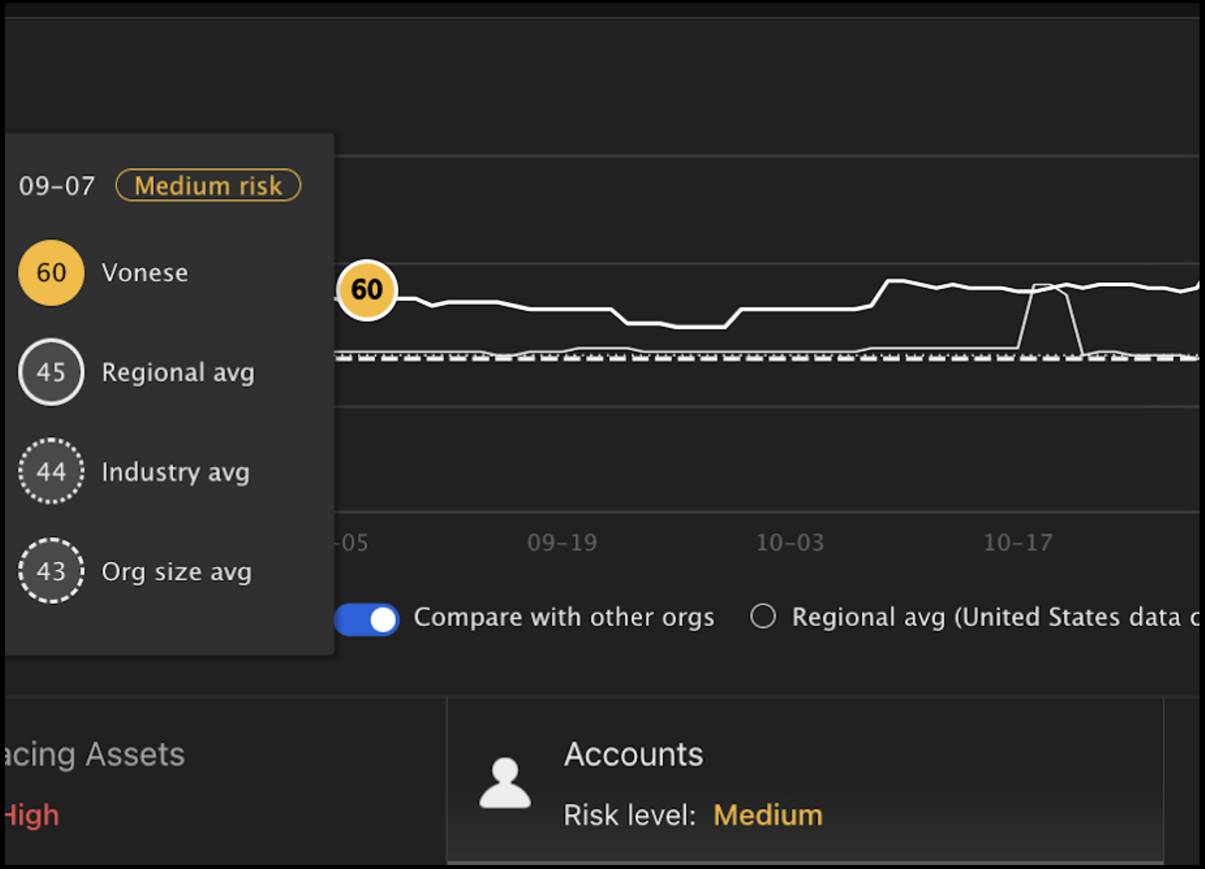
Asset Risk Scoring

Overall Risk Index

62

“One Score. Shared Understanding”

- Holistic, outcome-driven view across identities, cloud, devices, applications.
- Translates technical controls into **business-aligned risk metrics**.
- Builds **confidence and clarity** for teams, leaders, and boards.



09-07 Medium risk

60 Vonese

45 Regional avg

44 Industry avg

43 Org size avg

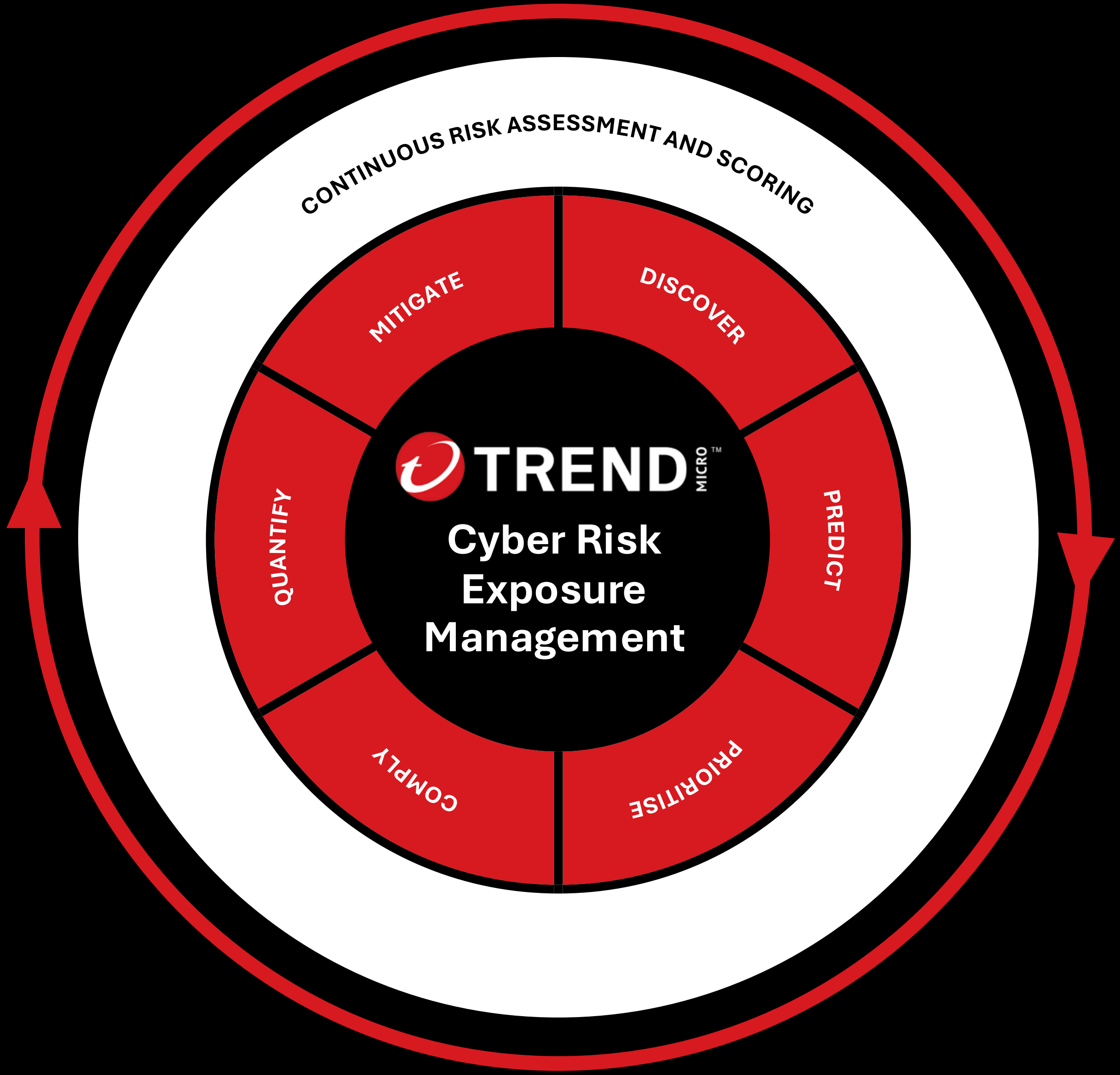
Compare with other orgs ○ Regional avg (United States data c

acing Assets

High

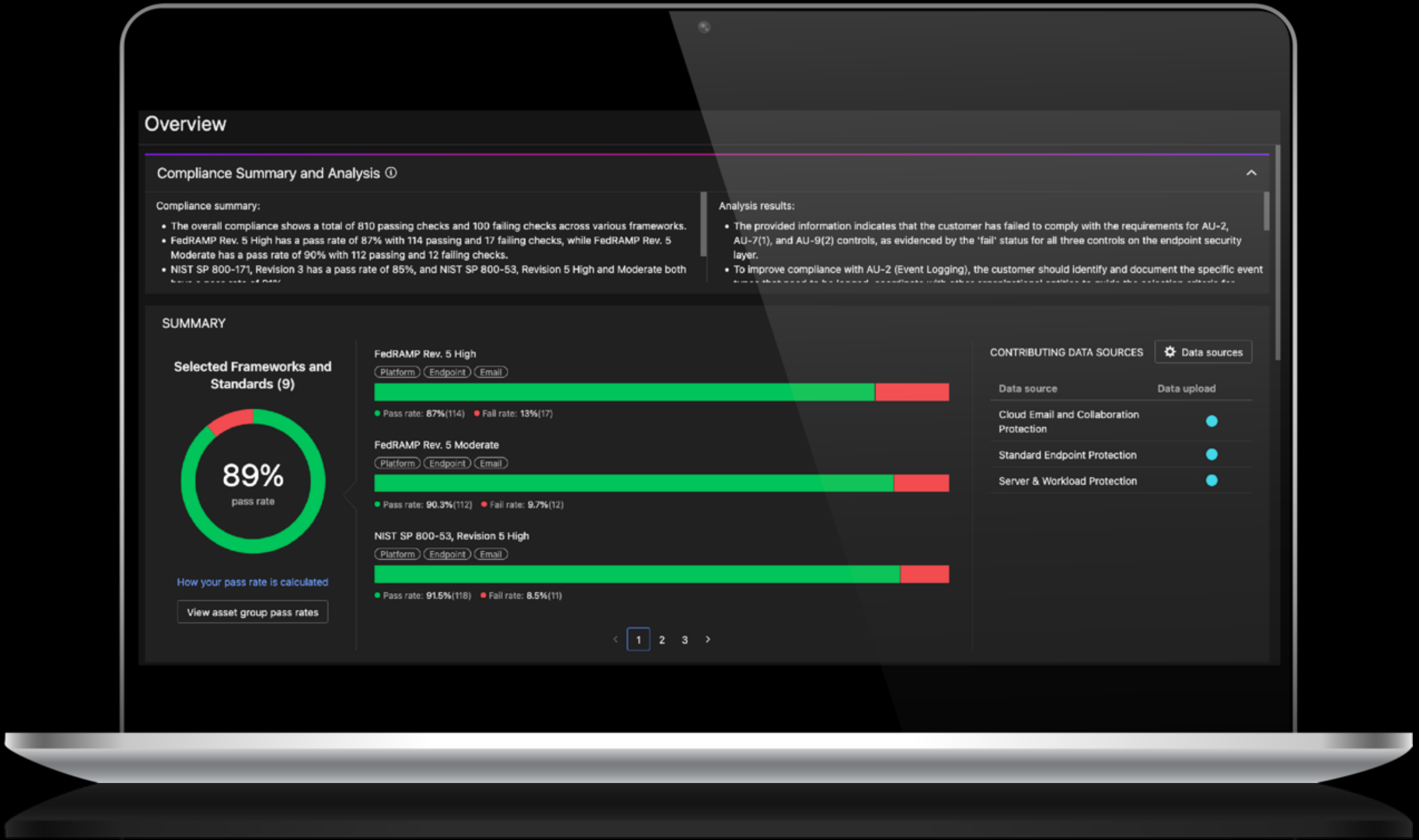
Accounts

Risk level: Medium


CONTINUOUS RISK ASSESSMENT AND SCORING
DISCOVER
PREDICT
PRIORITISE
COMPLY
QUANTIFY
MITIGATE
TREND MICRO
Cyber Risk Exposure Management

Let's get proactive.

Comply



Overview

Compliance Summary and Analysis ⓘ

Compliance summary:

- The overall compliance shows a total of 810 passing checks and 100 failing checks across various frameworks.
- FedRAMP Rev. 5 High has a pass rate of 87% with 114 passing and 17 failing checks, while FedRAMP Rev. 5 Moderate has a pass rate of 90% with 112 passing and 12 failing checks.
- NIST SP 800-171, Revision 3 has a pass rate of 85%, and NIST SP 800-53, Revision 5 High and Moderate both

Analysis results:

- The provided information indicates that the customer has failed to comply with the requirements for AU-2, AU-7(1), and AU-9(2) controls, as evidenced by the 'fail' status for all three controls on the endpoint security layer.
- To improve compliance with AU-2 (Event Logging), the customer should identify and document the specific event

SUMMARY

Selected Frameworks and Standards (9)

89%
pass rate

How your pass rate is calculated

View asset group pass rates

FedRAMP Rev. 5 High
Platform Endpoint Email
● Pass rate: 87%(114) ● Fail rate: 13%(17)

FedRAMP Rev. 5 Moderate
Platform Endpoint Email
● Pass rate: 90.3%(112) ● Fail rate: 9.7%(12)

NIST SP 800-53, Revision 5 High
Platform Endpoint Email
● Pass rate: 91.5%(118) ● Fail rate: 8.5%(11)

‹ 1 2 3 ›

CONTRIBUTING DATA SOURCES

⚙ Data sources

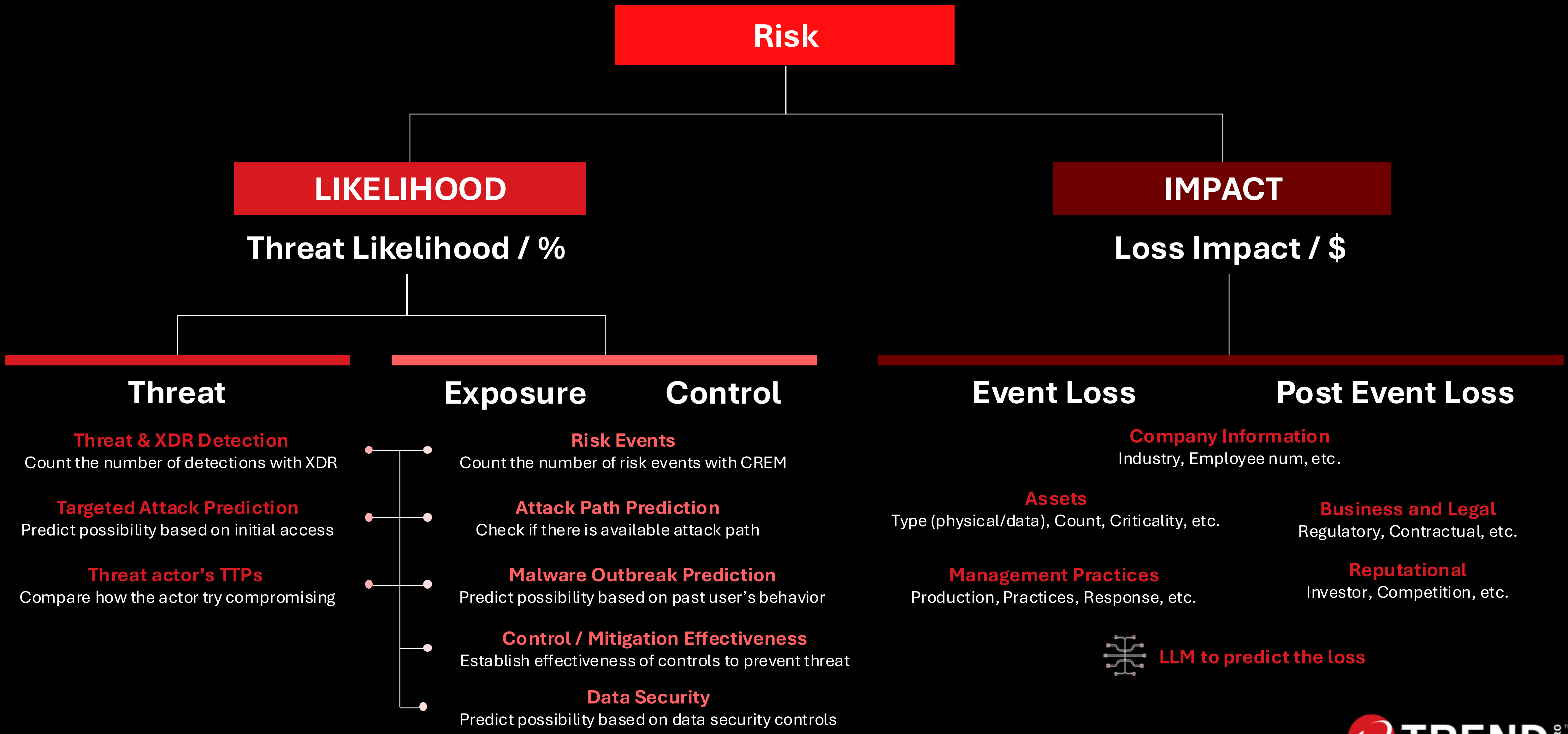
Data source	Data upload
Cloud Email and Collaboration Protection	●
Standard Endpoint Protection	●
Server & Workload Protection	●

What is Risk?

Risk is the likelihood that an undesirable event will occur and lead to severe consequences

$$\text{RISK} = \underbrace{\text{Likelihood}}_{\text{f (vulnerabilities, threats, exposure, security controls)}} \times \overbrace{\text{Impact}}^{\text{g (business criticality)}}$$

Quantifying risk in Vision One?



Risk

LIKELIHOOD

Threat Likelihood / %

IMPACT

Loss Impact / $

Threat

Threat & XDR Detection
Count the number of detections with XDR

Targeted Attack Prediction
Predict possibility based on initial access

Threat actor's TTPs
Compare how the actor try compromising

Exposure

Control

Risk Events
Count the number of risk events with CREM

Attack Path Prediction
Check if there is available attack path

Malware Outbreak Prediction
Predict possibility based on past user's behavior

Control / Mitigation Effectiveness
Establish effectiveness of controls to prevent threat

Data Security
Predict possibility based on data security controls

Event Loss

Post Event Loss

Company Information
Industry, Employee num, etc.

Assets
Type (physical/data), Count, Criticality, etc.

Management Practices
Production, Practices, Response, etc.

Business and Legal
Regulatory, Contractual, etc.

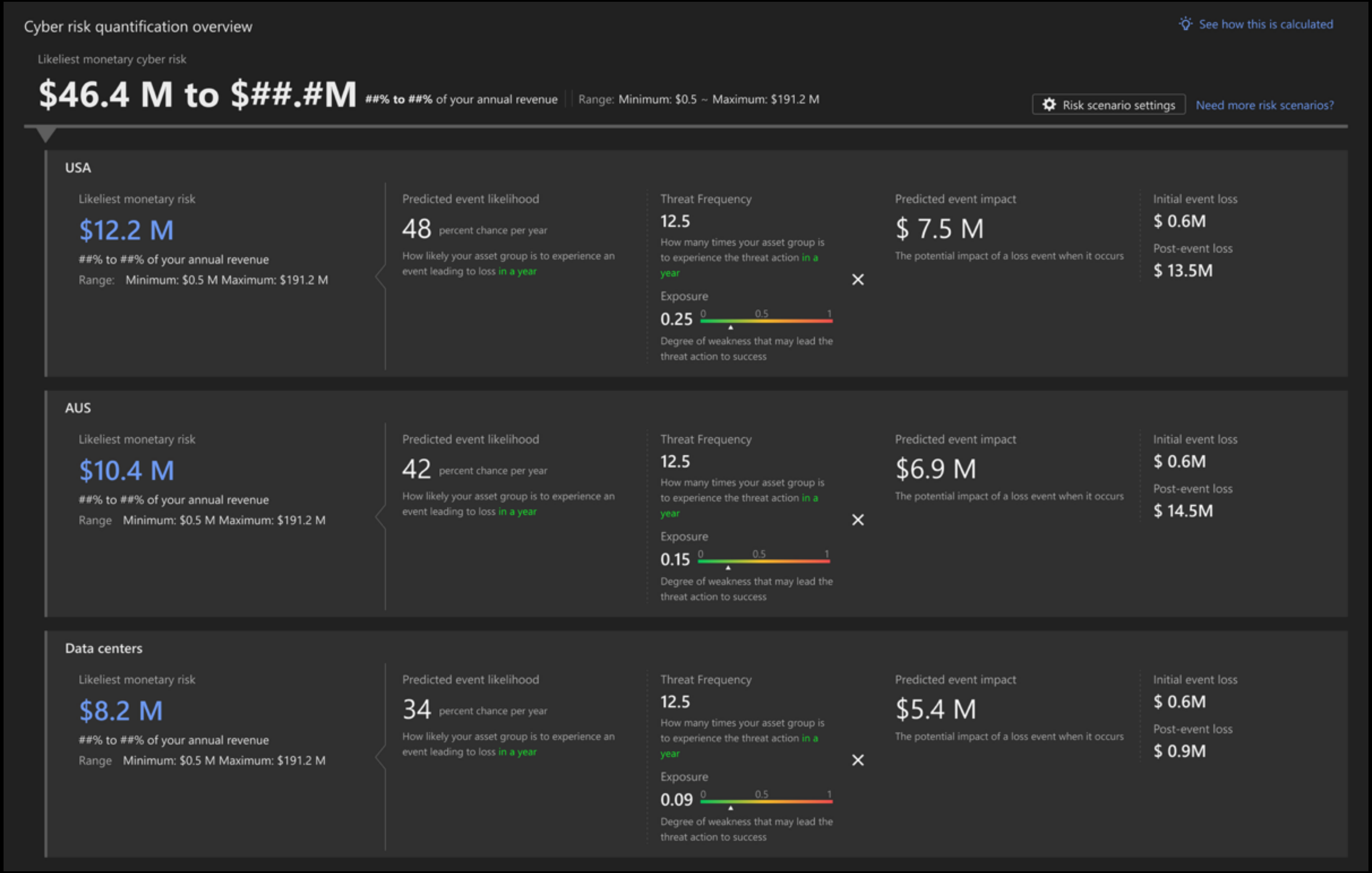
Reputational
Investor, Competition, etc.

LLM to predict the loss

Proactively Forecast Risk and Reward

We group risks based on related assets or business functions – not just alerts or CVEs – so you have visibility into risks the way your organizations operates.

- **See top risks scenarios** by asset group
- **Spot high-risk areas** at a glance
- **Track risk reduction** overtime



Cyber risk quantification overview

Likeliest monetary cyber risk

$46.4 M to $##.#M ##% to ##% of your annual revenue | Range: Minimum: $0.5 ~ Maximum: $191.2 M

USA

Likeliest monetary risk
$12.2 M
##% to ##% of your annual revenue
Range: Minimum: $0.5 M Maximum: $191.2 M

Predicted event likelihood
48 percent chance per year
How likely your asset group is to experience an event leading to loss in a year

Threat Frequency
12.5
How many times your asset group is to experience the threat action in a year

Exposure
0.25
Degree of weakness that may lead the threat action to success

×

Predicted event impact
$ 7.5 M
The potential impact of a loss event when it occurs

Initial event loss
$ 0.6M
Post-event loss
$ 13.5M

AUS

Likeliest monetary risk
$10.4 M
##% to ##% of your annual revenue
Range Minimum: $0.5 M Maximum: $191.2 M

Predicted event likelihood
42 percent chance per year
How likely your asset group is to experience an event leading to loss in a year

Threat Frequency
12.5
How many times your asset group is to experience the threat action in a year

Exposure
0.15
Degree of weakness that may lead the threat action to success

×

Predicted event impact
$6.9 M
The potential impact of a loss event when it occurs

Initial event loss
$ 0.6M
Post-event loss
$ 14.5M

Data centers

Likeliest monetary risk
$8.2 M
##% to ##% of your annual revenue
Range Minimum: $0.5 M Maximum: $191.2 M

Predicted event likelihood
34 percent chance per year
How likely your asset group is to experience an event leading to loss in a year

Threat Frequency
12.5
How many times your asset group is to experience the threat action in a year

Exposure
0.09
Degree of weakness that may lead the threat action to success

×

Predicted event impact
$5.4 M
The potential impact of a loss event when it occurs

Initial event loss
$ 0.6M
Post-event loss
$ 0.9M

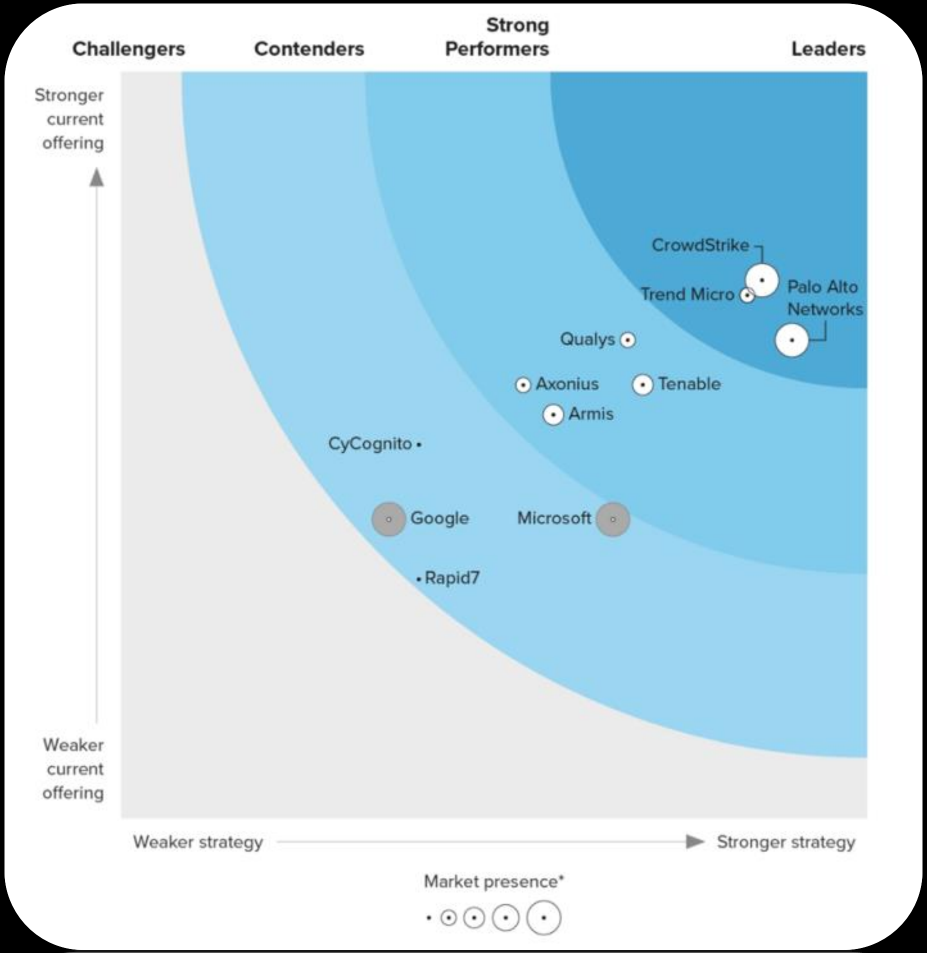
Recognised in the industry as a leader

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.

Proven Impact: How CREM Pays for Itself

Government Department:

- *Gained full visibility over legacy systems and modern assets, enabling measurable risk beyond only E8 compliance — reducing audit preparation time and overheads by over* ***30%****.*

Private Healthcare Provider:

- *Nearly* ***70%*** *improvement in mean time to respond, resulting in multi-million dollar FTE reallocation and faster decision-making across the security function.*

Local Council:

- *After a competitive market evaluation, found that recreating CREM's coverage through multiple vendors and integrations was* ***cost-prohibitive by 1–2x*** *— reinforcing the business case for consolidation.*

Finance Industry:

- *Transformed qualitative risks into real-time, board-ready metrics — accelerating reporting cycles by* ***50%*** *and enabling earlier risk remediation decisions that reduced exposure windows.*

How Would CREM Pay for Itself in Your Organisation?

Most breach costs stem from issues CREM is designed to catch early.

By remediating exposures before attackers exploit them, organisations reduce their risk and avoid downstream costs.

But even without a breach, the hard ROI is clear:

- What's the estimated cost of a data breach in your sector?
  - Could identifying exposure paths earlier reduce that risk by **40–70%**?
- How much time does your team spend chasing alerts or reconciling reports across siloed tools?
- What's the annual spend across point solutions CREM could replace?
- What would 30–50% faster audit prep or board reporting save your risk/compliance function?

How can Trend Vision One help you?

65% Reduction in dwell time

99.6% Fewer alerts

$1.3M Avg savings from risk reduction

- Analysing the Economic Benefits of Trend Vision One, January 2024

TREND MICRO™

A Trusted Security Partner

Global Leader in Cybersecurity

$2.1B 2024 Gross Sales & Profitable

†Constant currency

7000 Employees in **73** countries

Cybersecurity Platform Protecting

500,000+ Enterprise customers in 175+ countries

87M+ Protected enterprise assets

Innovator & Cybersecurity Expert

Market leader across **XDR, Cloud, EPP, Email, Network** with over 700 global patents

#1 in Public Vulnerability Disclosure‡

147B+ threats blocked in 2024

‡ Quantifying the Public Vulnerability Market: 2023 Edition

The CISO’s Playbook for Enabling Transformation

1. Start With the Business: Define Innovation Goals & Desired Outcomes
2. Establish Baseline Risk & Exposure
3. Assess Capacity to Absorb Innovation Risk
4. Translate Risk Appetite Into Decision Guardrails
5. Prioritise Work Packages that unlock innovation safely
6. Embed Continuous Measurement
7. Govern Innovation as a Partnership

TREND MICRO™ | Proactive Security Starts Here

Contact

Andrew Philp

https://www.linkedin.com/in/philpy/