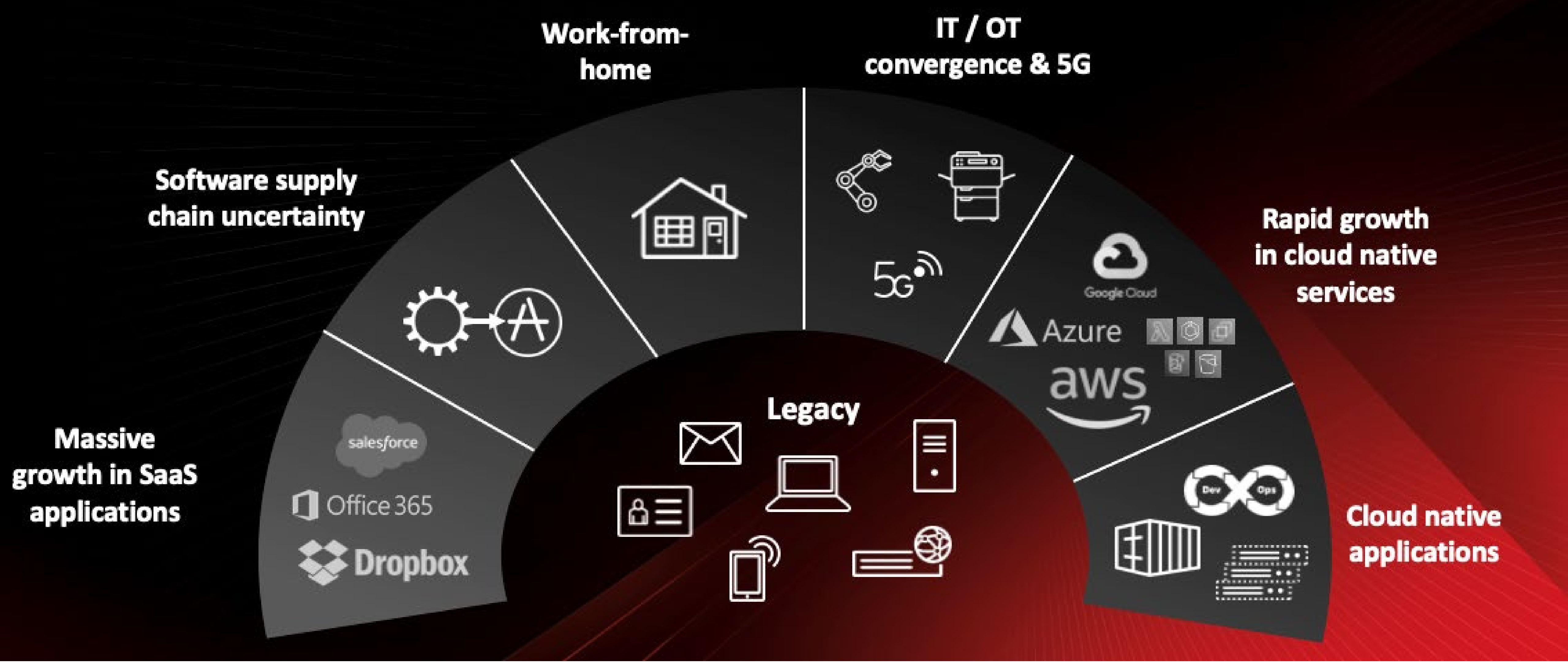
Contrôlez vos risques grâce à une bonne maîtrise de votre Surface d’attaque.

Bechtle IT Forum | 11.06.2024 | SwissTech Convention Center

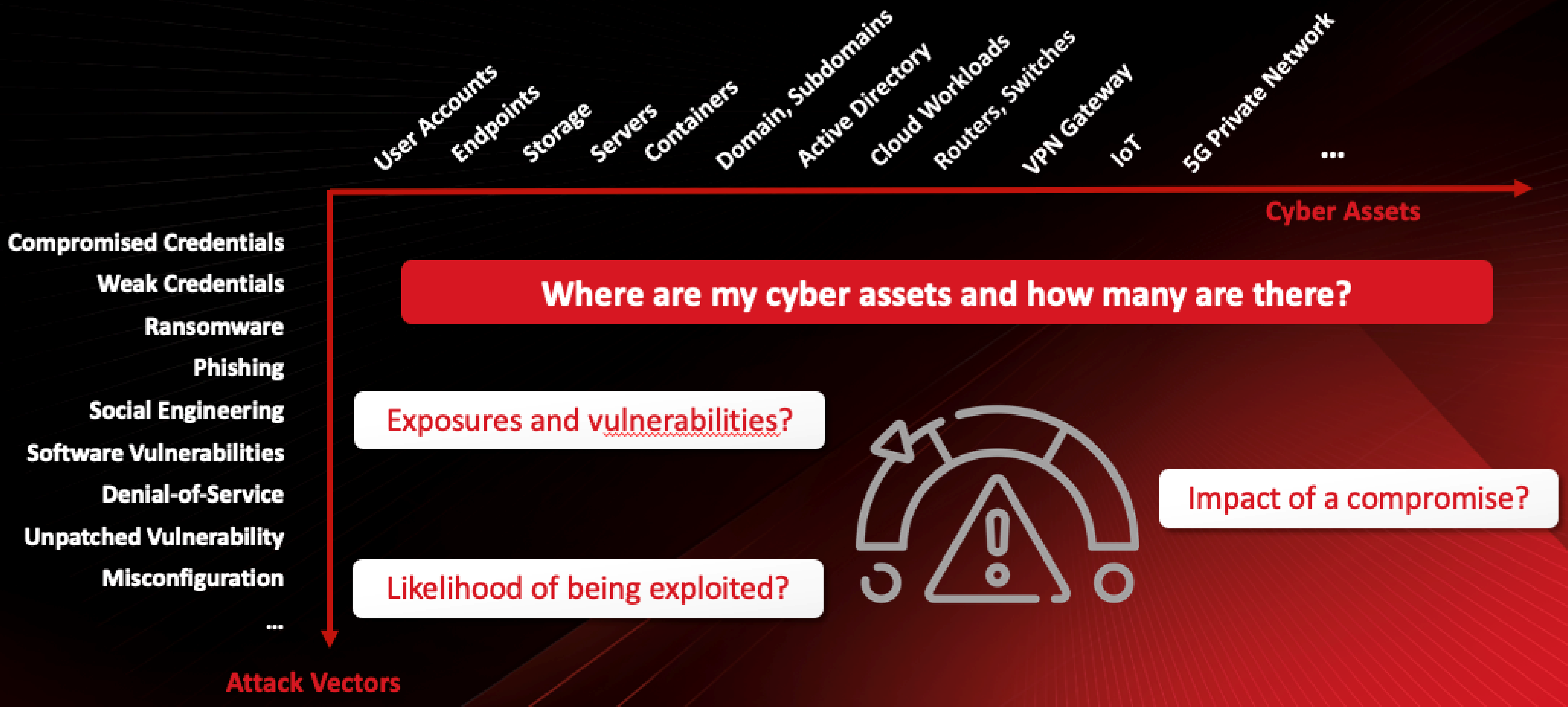
Cyrille Larrieu, Senior Sales Engineer, Trend Micro
Claudio Guerrieri, Business Development Manager Network & Security, Bechtle Suisse

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
5G
Google Cloud
Azure
aws
salesforce
Office 365
Dropbox
Dev
Ops

Lack of Security Posture Across Cyber Assets



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

...

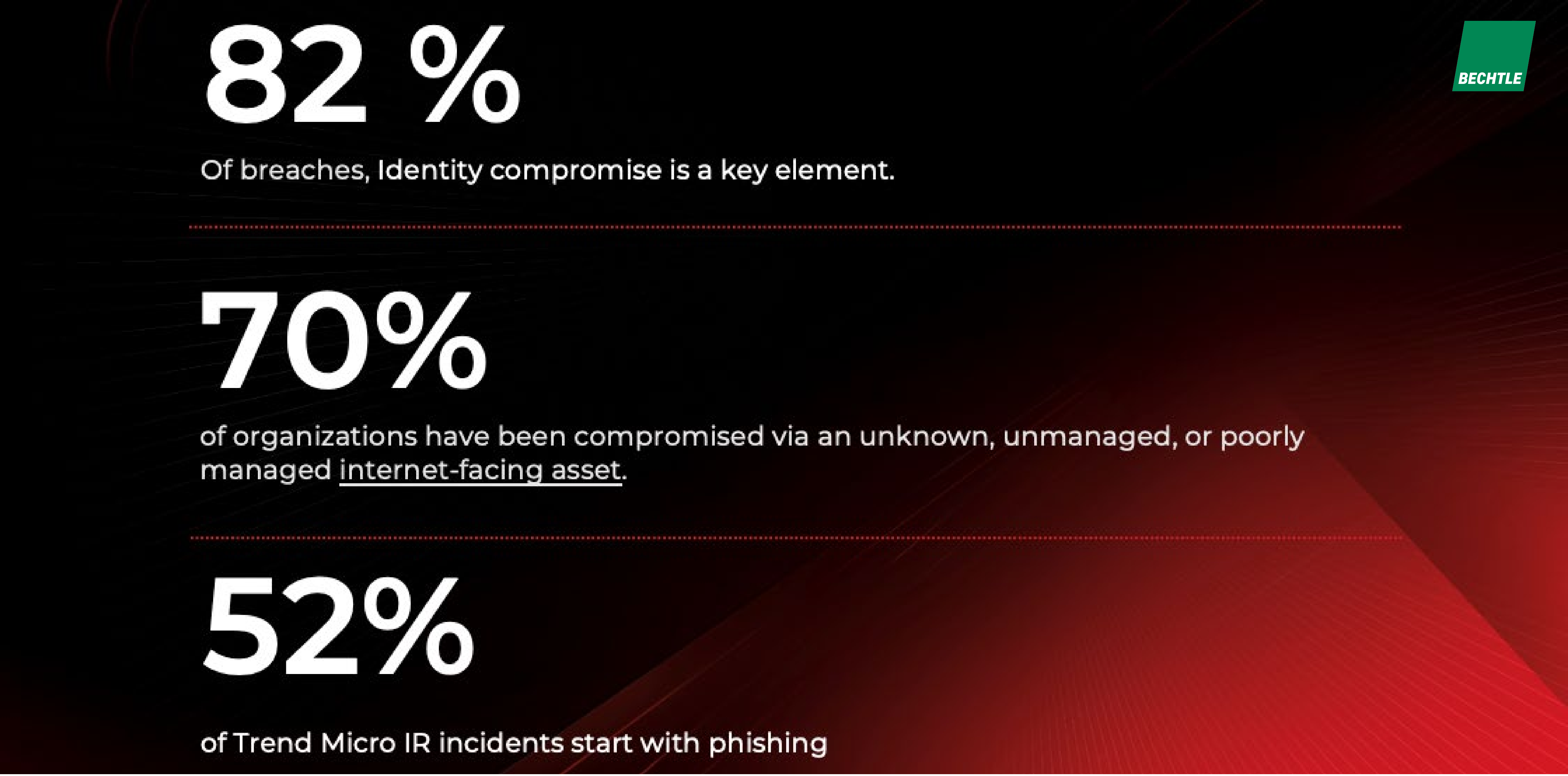
Attack Vectors

Where are my cyber assets and how many are there?

Exposures and vulnerabilities?

Likelihood of being exploited?

Impact of a compromise?



82 %

Of breaches, Identity compromise is a key element.

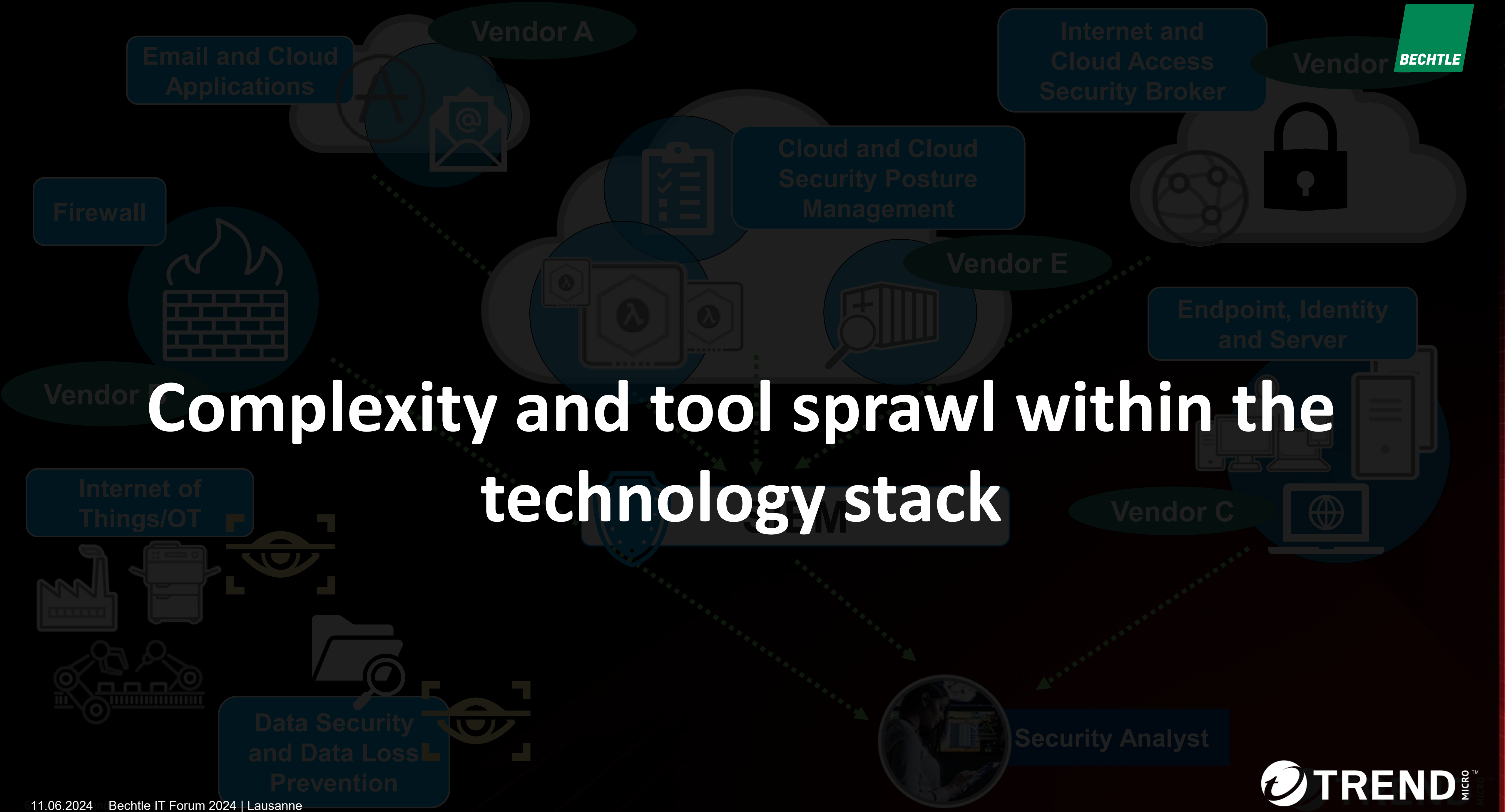
70%

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

52%

of Trend Micro IR incidents start with phishing

Complexity and tool sprawl within the technology stack


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

Challenges

- Are we safe? Do we know our security situation?
- How high is my risk?
- Do I need to actively intervene today?
- Are the investments in cyber security appropriate or do they need to be readjusted?
- Are we insurable?
- Do we comply with regulatory requirements?

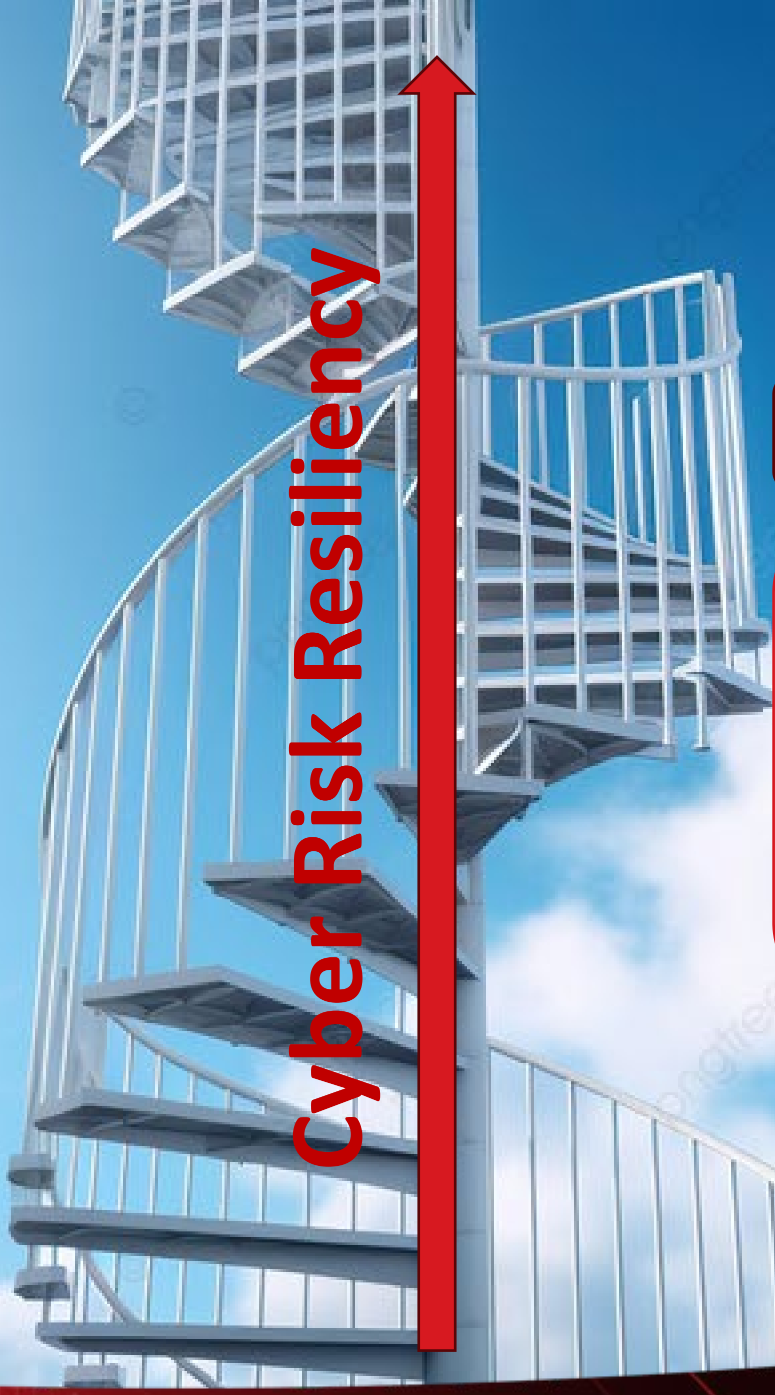
What can be achieved with Trend Micro?

Proactive Cyber Security

- Continuous Attack Surface Monitoring with proactive evaluation and mitigation of risks
- Technologies in place like ASM, ASRM, VAS etc.

Passive Cyber Security

- Focus on protective measures
- Traditional technologies in place like Firewalls, IPS, EPP, CWPP etc.



Reactive Cyber Security

- Established SOC or MDR-Service
- Capabilities to detect anomalies and suspicious events
- Prepared to defend attacks quickly
- Technologies in place like EDR / XDR, NDR, SIEM, SOAR etc.

Slow Down Attackers

Attack Surface Management

Assess risk and mitigate proactively, reducing the attack surface

Cloud-Native Application Protection Platform (CNAPP)

Integrate security into the development process, making apps secure before go-live

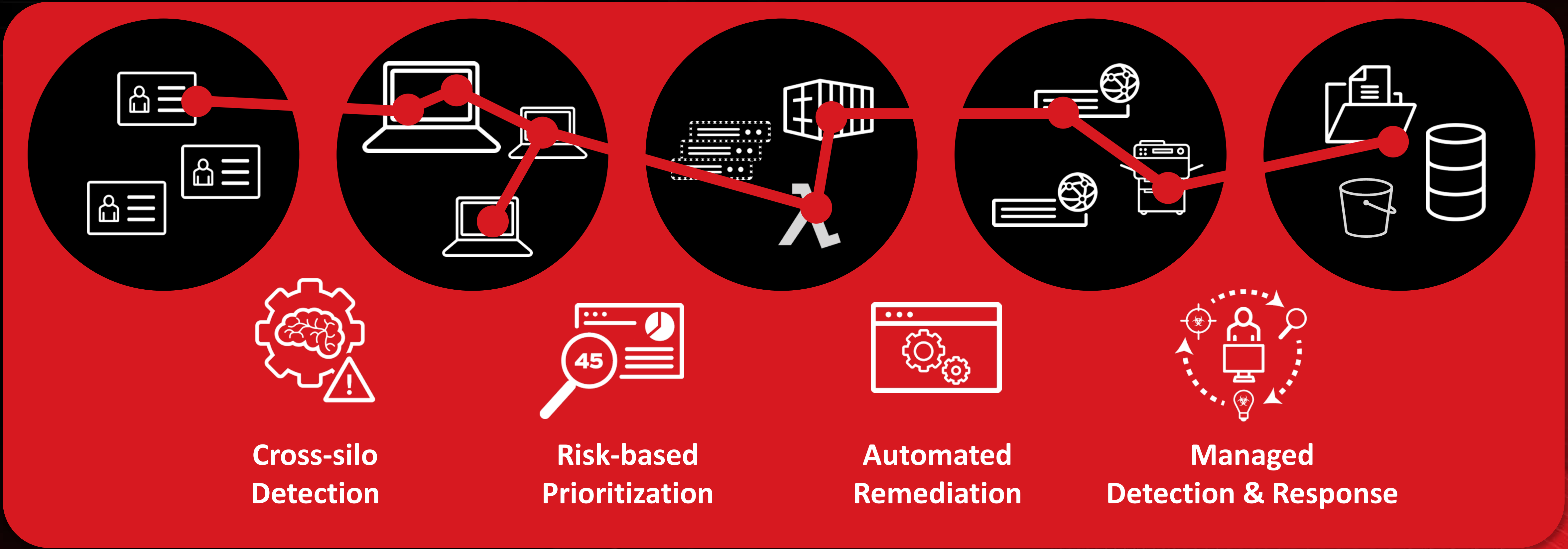
Zero Trust Strategy

"Never Trust, Always Verify"

Add more hurdles for attackers, and make them visible to detection

Detect and respond faster

TO: Extended Detection and Response (XDR) to focus on what's most important.



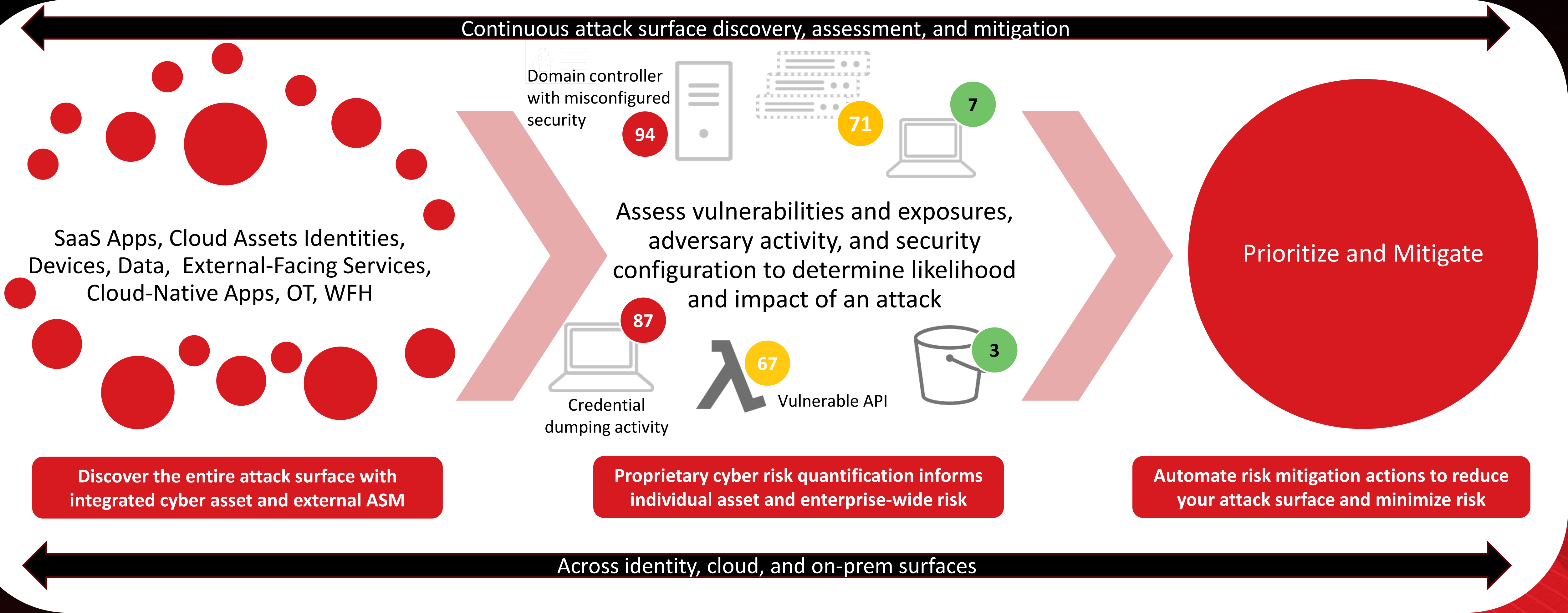
Cross-silo Detection

Risk-based Prioritization

Automated Remediation

Managed Detection & Response

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
94
71
7
Assess vulnerabilities and exposures, adversary activity, and security configuration to determine likelihood and impact of an attack
87
Credential dumping activity
67
Vulnerable API
3
Prioritize and Mitigate
Across identity, cloud, and on-prem surfaces

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

A platform approach

BECHTLE

Vendor Consolidation

Consolidate the number of security tools and vendors to simplify security operations and purchasing

Reduce Cost & Complexity

Leverage security platforms with multiple capabilities vs. point solutions

Stay Compliant

Data sovereignty and privacy requirements are increasing – security tools need to align with your evolving needs

TREND MICRO™

Driving Better Business Outcomes

Strengthen Security Posture

Integrated platform approach ensures all cyber assets are identified and monitored across the digital environment

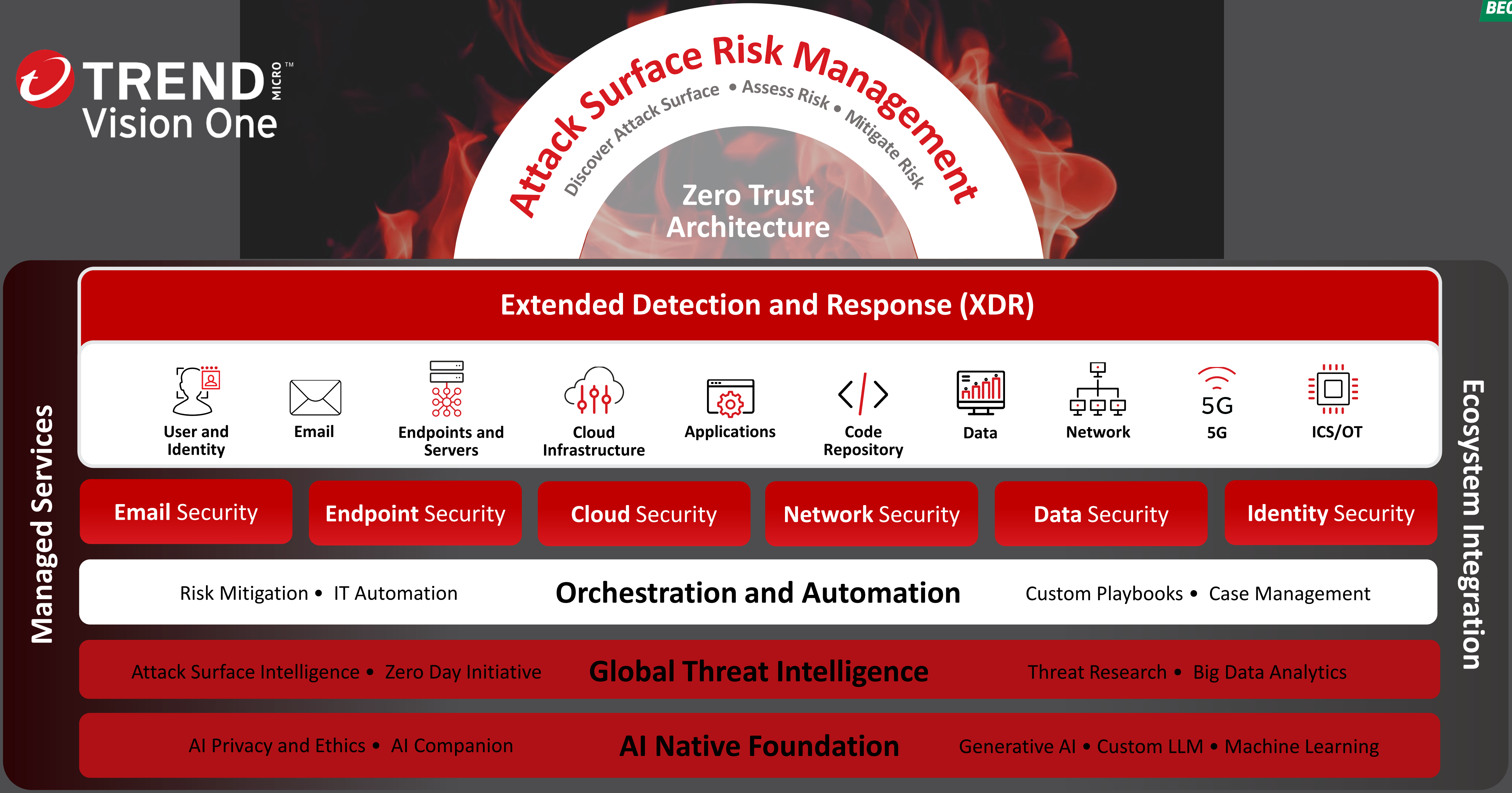
Improve Agility

Automated threat response and risk remediation gives teams more time to focus on value creation

Elevate Cybersecurity

Risk quantification helps communicate and align cyber risk management practices with business operations and goals

TREND MICRO Vision One



Attack Surface Risk Management

Discover Attack Surface • Assess Risk • Mitigate Risk

Zero Trust Architecture

Extended Detection and Response (XDR)

Email Security | Endpoint Security | Cloud Security | Network Security | Data Security | Identity Security

Risk Mitigation • IT Automation **Orchestration and Automation** Custom Playbooks • Case Management

Attack Surface Intelligence • Zero Day Initiative **Global Threat Intelligence** Threat Research • Big Data Analytics

AI Privacy and Ethics • AI Companion **AI Native Foundation** Generative AI • Custom LLM • Machine Learning

Merci!

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