Moltiplicare le forze con proattività e intelligenza (artificiale)

Luca De Fassi, Sales Engineer

AI & CYBERSECURITY: THE CONSTANT EVOLUTION

TREND MICRO™

Over 70 years ago, AI was conceived. Since its inception, this technology has continued to transform, learn, and develop, becoming embedded in businesses, communities, and everyday life. AI is here to stay... but what impact has it had on the cyber threat landscape, and how will it shape its future?

1950 THE TURING TEST

Alan Turing publishes "Computing Machinery and Intelligence", proposing the Turing Test to evaluate machine intelligence, forming the conceptual foundation for AI.

1972 PROLOG

A programming language for AI and computational linguistics, Prolog enhances the development of AI applications.

1993 NEURAL NETWORKS

Advancements in neural network research promotes interest in AI pattern recognition and anomaly detection in cybersecurity.

1997 IBM'S DEEP BLUE

Chess-playing computer Deep Blue defeats world chess champion Garry Kasparov, demonstrating AI's capabilities in strategic thinking.

2004 DARPA GRAND CHALLENGE

Autonomous vehicles navigate a challenging course, promoting consideration of AI in automated threat response.

2009 IMAGENET

The launch of ImageNet, a large-scale visual database, boosts progress in deep learning and computer vision.

2010 STUXNET DISCOVERY

The detection of the Stuxnet worm—the first known use of AI in cyber warfare—emphasizes the need for AI-enhanced security measures.

2015 OPEN AI

Establishment of OpenAI accelerates research with a focus on safety and ethics, contributing to secure AI applications in cybersecurity.

2017 DEEPFAKES

Creation and widespread recognition of deepfake technology raises concerns for misinformation, fraud, and social engineering attacks.

2019 AUDIO DEEPFAKE CRIME

AI-generated audio deepfake used to impersonate a UK CEO and trick the executive into transferring over €220,000.

2020 GPT-3 RELEASE

OpenAI releases GPT-3, a state-of-the-art language model, highlighting AI's capabilities in generating human-like text, while raising ethical and security concerns.

2022 CHATGPT

ChatGPT goes viral with one million users just five days after launching. ChatGPT marks an acceleration in the AI boom, making AI more accessible to the general public.

2023 LLaMA LEAK

Meta's AI language model, LLaMA, created to help researchers, was leaked on 4chan one week after it was announced. Cyber experts raise concerns around distributing technology too freely through the open sourcing of these models.

2024 MULTIMODAL GENERATIVE AI

Generative AI becoming increasingly advanced, moving beyond text only to produce and understand richer and more coherent outputs, including image, audio and video.

2024 & BEYOND

PREDICTION 1: Transformation in AI-driven security

AI will fundamentally change key industries like healthcare, education, finance, social networking and cybersecurity. Automation, predictive analytics, custom detection modelling, reporting, and cyber-aware assistants will **BOOST PRODUCTIVITY AND EFFICIENCY**. AI is already being used to combat cybercrime, with 34% of organizations implementing AI cybersecurity tools.

PREDICTION 2: Heightened focus on AI governance

Global collaboration on AI governance and ethical frameworks will be a vital measure to balance innovation with security and ethical considerations. Rapid advancements in autonomous systems, such as vehicles and robotics, will significantly impact industry and society, necessitating robust security measures. With the 2023 EU AI Act Proposal laying out a framework for governing AI development and deployment, we predict the US will follow suit with a **FORMALIZED LEGISLATION** surrounding the safe and responsible use of AI.

PREDICTION 3: Increased role of AI in cybercrime

Spear phishing, harpoon whaling, and virtual kidnapping are just the tip of the iceberg when it comes to AI's potential role in cybercriminal schemes. We predict **VOICE CLONING**—already a powerful tool for identity theft and social engineering—will take center stage in targeted scams.

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

Proactive security starts here

Visibility • Prioritization • Mitigation

TREND MICRO™ Vision One

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.

Powering Proactive

TREND MICRO™

Trend Vision One AI Solution Strategy

AI for Security

enhance your cybersecurity efforts and transform security operations with AI

Security for AI

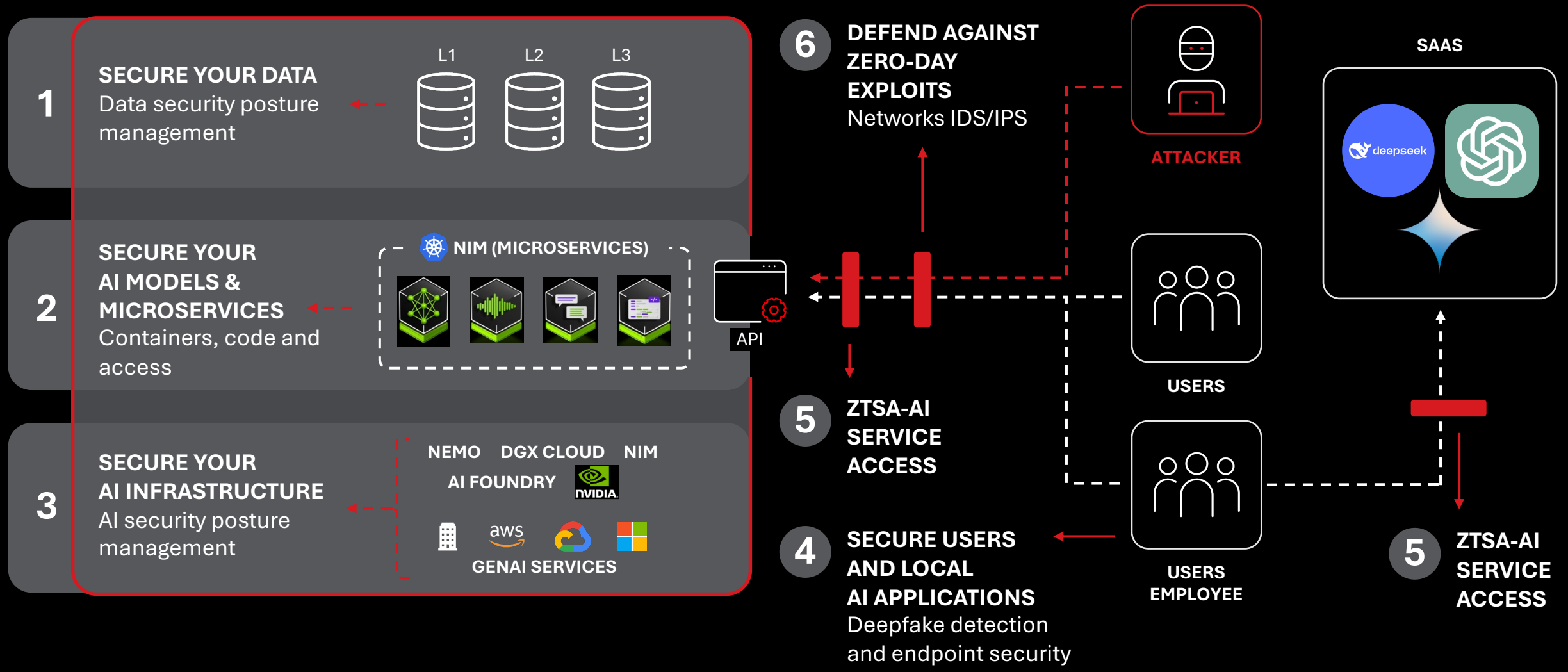
secure your AI journey and defend against AI-related threats and attacks

AI Ecosystem

Threat and Attack Intelligence

Responsible AI

Security for AI



AGENTIC AI

Intentional

Proactive

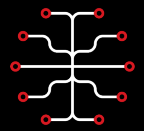
Autonomous

Decisive

Built to Act.

Traditional AI vs. Agentic AI

User Experience



Traditional AI

Ensemble of problem-specific tools, panes and windows

Narrow experts capable of prediction based on similar patterns in specific features

Pulling data from chatbots tied to backend information retrieval systems

Agentic AI

Goal-driven solution assistant, capable of cross-domain problem solving

Custom automations from user goals and environment, pushing any required approvals

Proactive planning for continuous improvement

Threat Defense

Traditional AI

Anomaly Detection

Malware, Script and Content Classification

Templatized mitigations and reporting

Vendor inter-inoperability

Agentic AI

Explanatory analytics

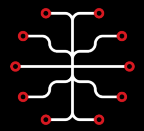
Automated detection patterns

Environment-specific playbook generation

User directed multimodal reporting

Schema-free telemetry ingestion

Risk Mitigation



Traditional AI

Asset and identity behavioral anomalies

Event chain (un)likelihood

Formulaic impact assessment

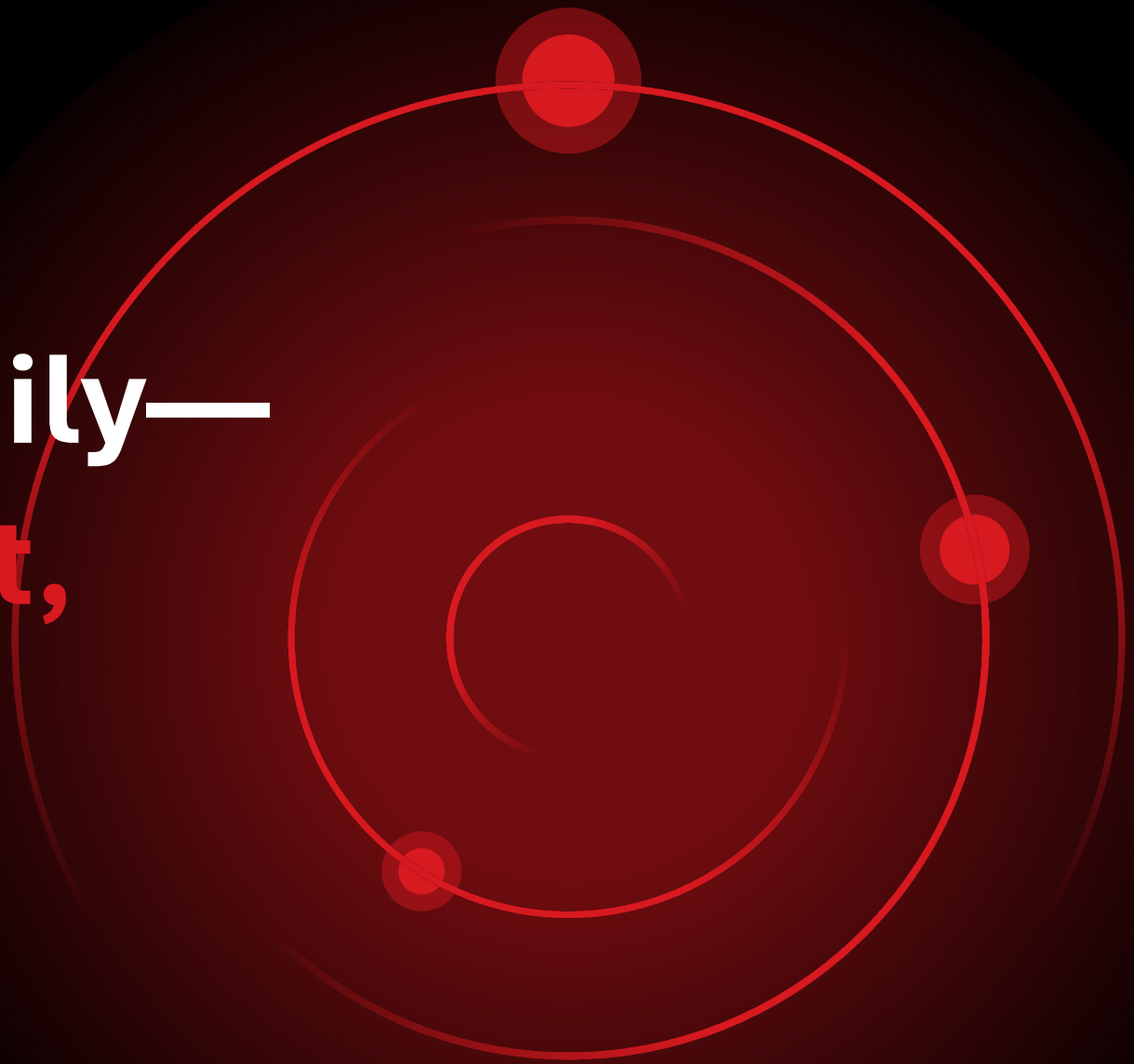
Agentic AI

Continuous attack surface assessment and attack planning

Reasoning about novel telemetry

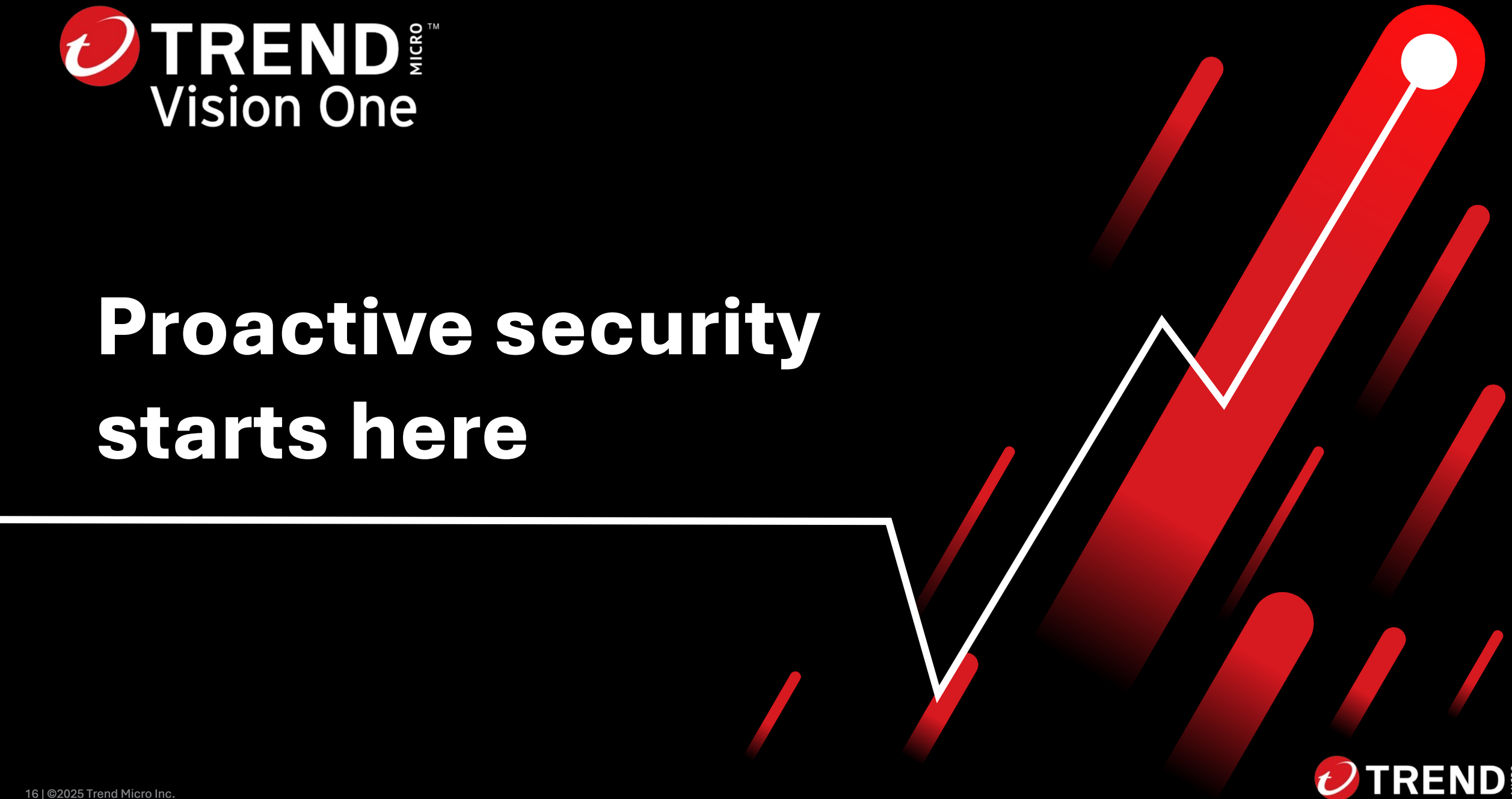
Cost benefit analysis for mitigation prioritization

Threats evolve daily—
leaders don’t wait, they anticipate, adapt, and act



TREND MICRO™ Vision One

Proactive security starts here



TREND MICRO™