CROWDSTRIKE

VECTRA

Threat Hunting Reloaded: Sichtbarkeit + Kontext = Proaktive Verteidigung

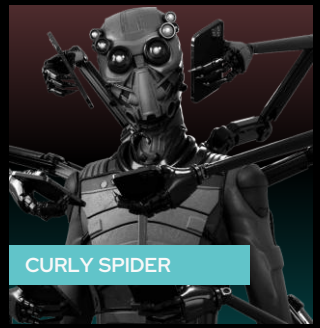
CrowdStrike Charlotte AI +
Vectra.AI Attack Signal Intelligence

We stop breaches.

Protection that powers you

AI-enabled adversaries are accelerating...

Traditional Defenses Are Obsolete

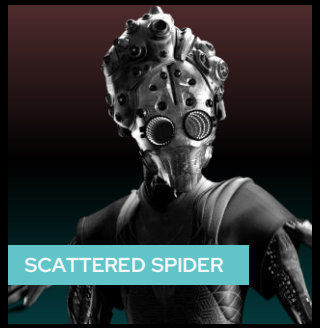


35% increase in "interactive intrusion" techniques

AI Has Weaponized Deception at Scale

220% increase in AI accelerated human manipulation

Speed Has Become the Ultimate Offense



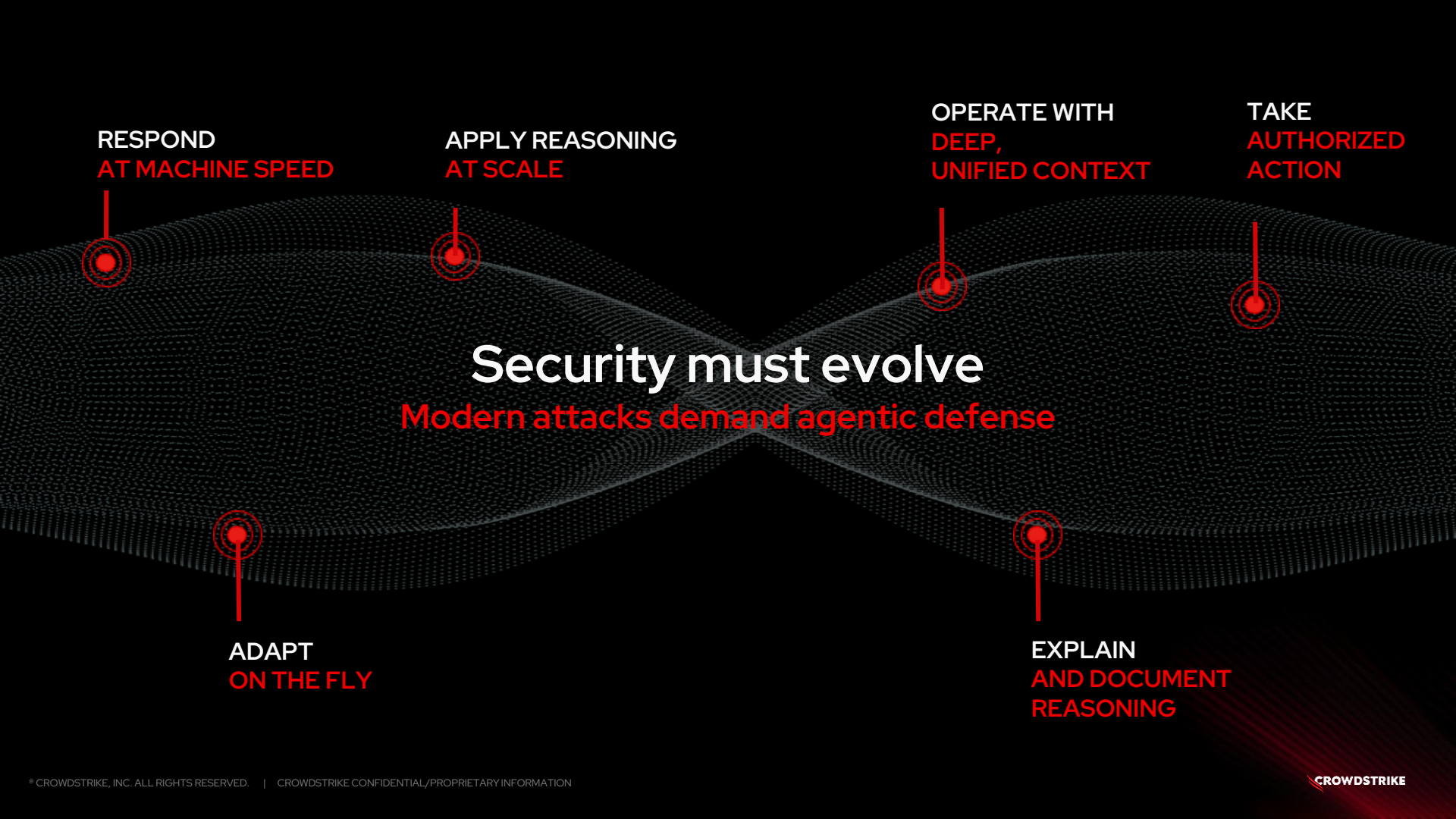
Less than 24 hours: account takeover to ransomware

Fragmentation Gives Adversaries the Advantage

Cross-domain attack are the norm: siloed tools cannot detect

CROWDSTRIKE

...intensifying the gaps between security teams and adversaries



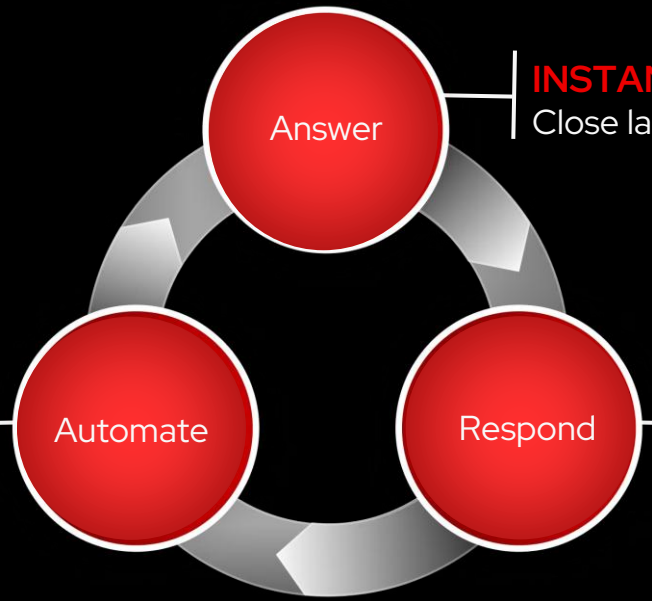
CROWDSTRIKE

Charlotte AI

The brain of the agentic SOC

Charlotte AI helps teams close the gaps.

Automate repetitive tasks, accelerate outcomes and free analysts to focus on high-impact work

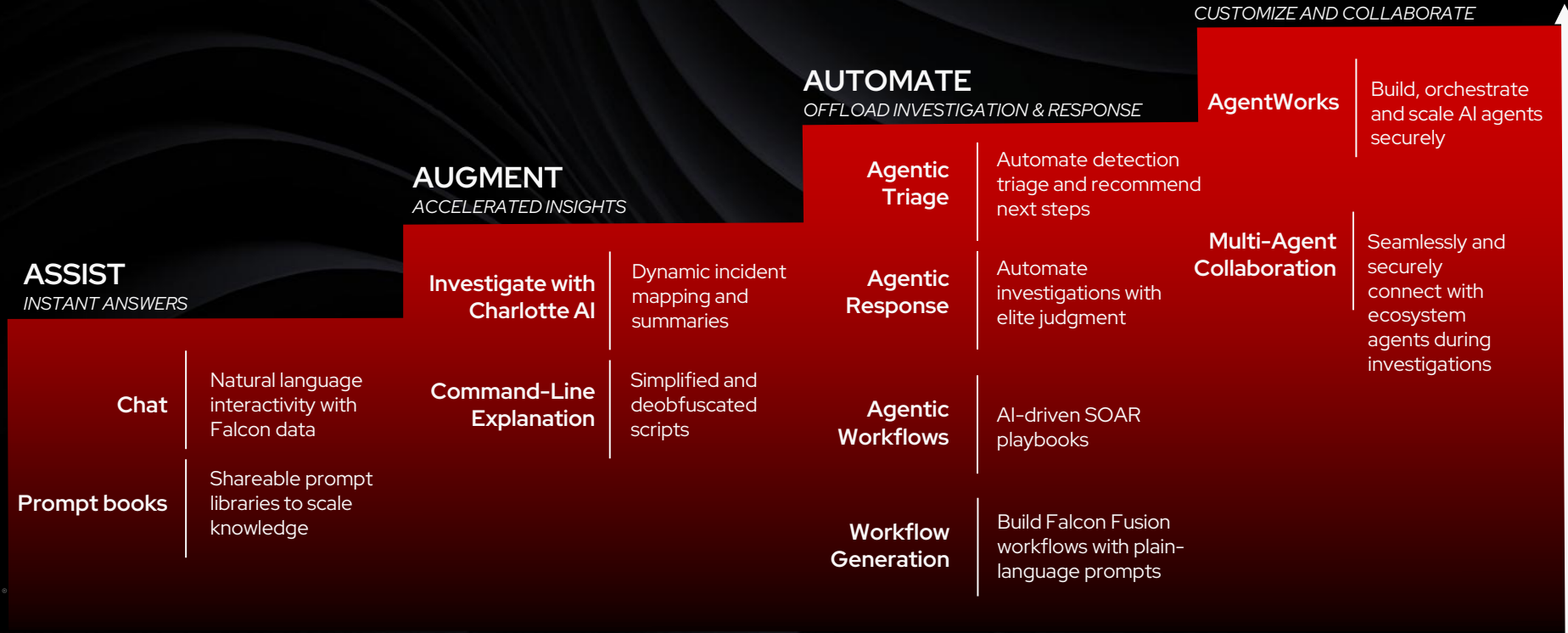


INSTANT ANSWERS
Close labor gaps with instant clarity

AGENTIC WORKFLOWS
Close speed gaps by activating AI reasoning and action in automated playbooks

AGENTIC TRIAGE & RESPONSE
Close skill gaps with expert-level reasoning

Accelerate Outcomes and automate high-value work with Charlotte AI



Charlotte AI

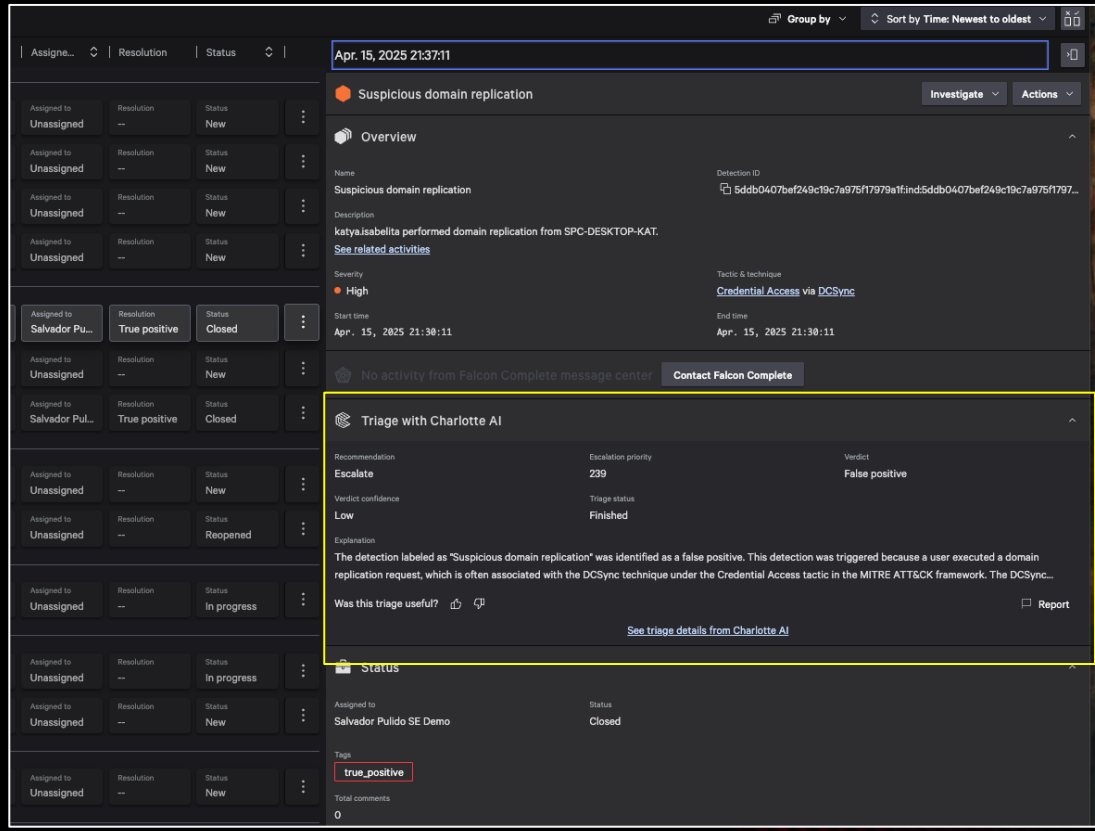
Agentic Detection Triage

Automatically analyze new detections, obtaining:

- ➔ Triage verdict + confidence level
- ➔ Clear explanation
- ➔ Next-step recommendation

Why it matters:

- Save 5+ minutes per detection
- Apply the expertise of Falcon Complete
- Prioritize real threats
- Triage analysis does not consume Charlotte AI credits



Time savings represents the amount of time an analyst would have spent triaging detections but can now use that time for other skilled work while Charlotte triages the detections. Individual results may vary based on factors such as total alert volume.

CROWDSTRIKE

Charlotte AI

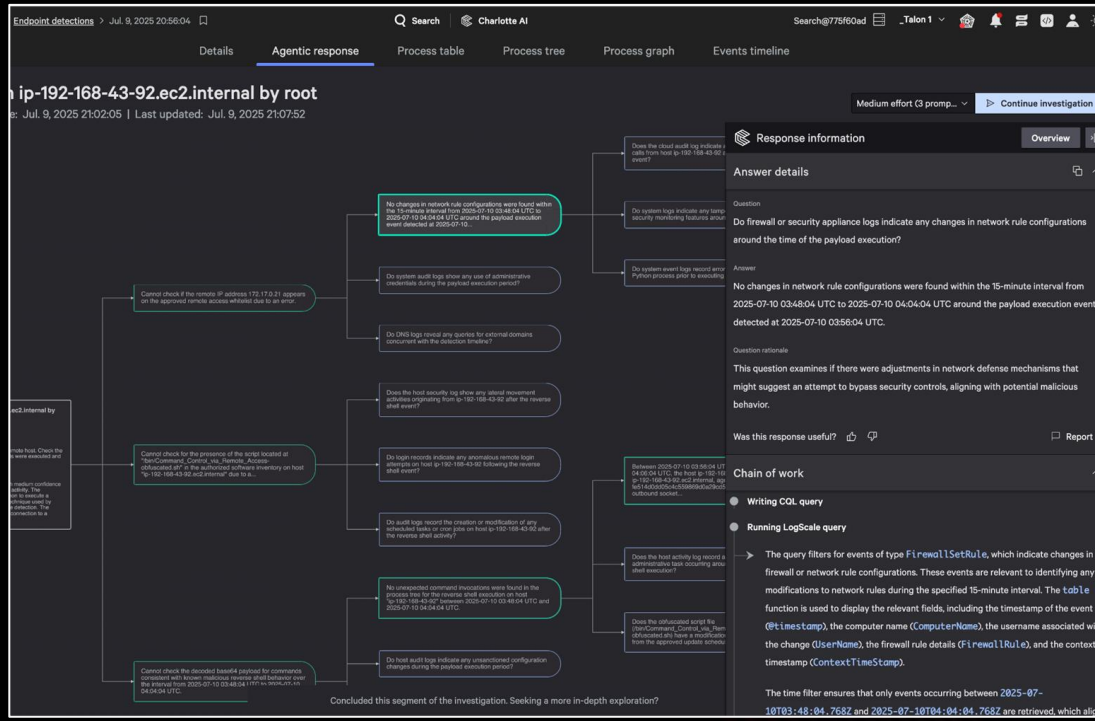
Agentic Response

Autonomously investigate detections:

- ➔ Generates analysis questions and answers them
- ➔ Explains rationale for each question
- ➔ User-activated through the Detection Details view (manual) or via Falcon Fusion SOAR workflows (automated)

Why it matters:

- Save 10+ minutes per credit spent
- Apply the latest insights from Falcon Complete Next-Gen MDR at scale with consistency



The time savings of more than 10 minutes per investigation is an estimate based on Agentic Response's ability to automate tasks that would otherwise require more than 10 minutes of manual effort by a human analyst. This should not be interpreted as a guarantee that this will lead to a 10 minute reduction in the total investigation time or mean time to respond (MTTR)

CROWDSTRIKE

Charlotte AI

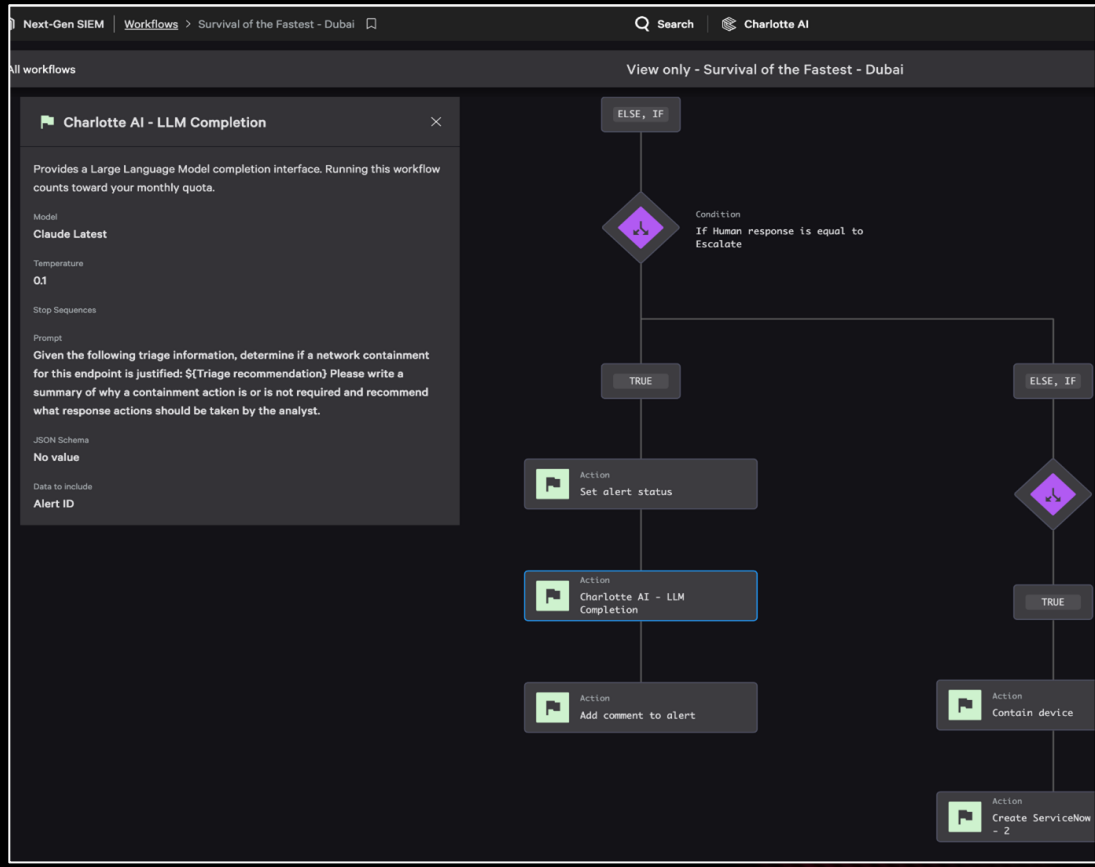
Agentic Workflows

Customize AI-powered playbooks:

- ➔ Bring AI models into Falcon Fusion SOAR workflows to analyze 1st/3rd party data
- ➔ Use natural language to direct model analysis
- ➔ Configure automated actions based on AI reasoning

Why it matters:

- Create adaptable, automated response
- Generate audience-ready outputs
- Use cutting-edge models — no extra infrastructure or agreements



VECTRA®

HOW TO PROTECT MODERN NETWORKS

INTRODUCTION TO VECTRA AI / TEAM ALPINE

Customer First, Partner Centric

+ Founded 2011, Privately held
+ Headquartered in San Jose, CA
+ 580+ employees
+ 113 countries
+ 3 Global SOCs
+ >1800 customers

AI Driven

+ Research + Data Science + Engineering
+ 150+ AI-driven attacker behavior models
+ 35 patents in AI-driven threat detection
+ Most referenced vendor in MITRE D3FEND (11)
+ Cover >90% of MITRE ATT&CK techniques

Kim Rehage
Team Alpine

Michael Buchner
Team Alpine

Jo Wegener
Team Alpine

David Solar
Team Alpine

Aurélien Hess
Team Alpine

VECTRA AI NAMED TO Forbes AI 50 LIST

Gartner Peer Insights Customers' Choice 2024

4.7 ★★★★★

SC 2022 awards EUROPE

THE CHANNEL CO. CRN SECURITY 100 2023

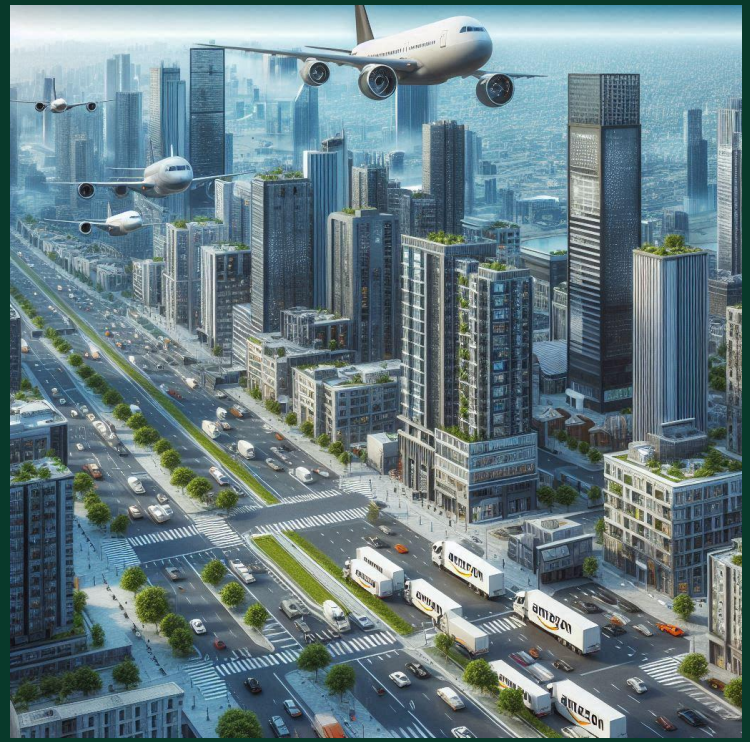
GARTNER MAGIC QUADRANT FOR NDR 2025

„Network detection and response platforms continuously monitor traffic for anomalies, suspicious patterns and threat indicators, and they complement other threat detection solutions“

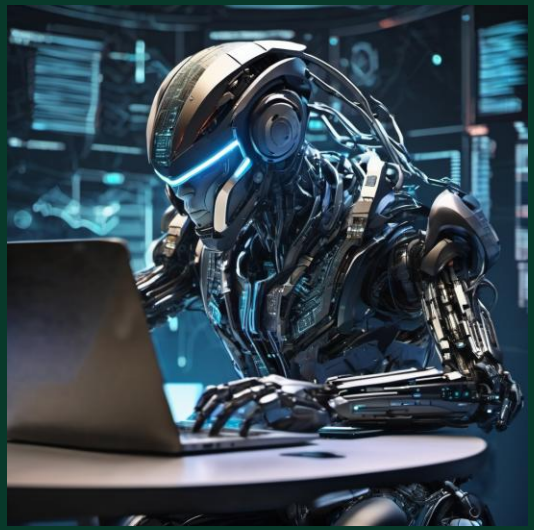
„Organizations rely on NDR to detect and contain postbreach activity such as ransomware, insider threats and lateral movements. NDR complements other technologies that primarily trigger alerts based on rules and signatures by building heuristic models of normal network behavior and detecting anomalies"

„NDR is commonly used as a complementary detection and response technology as part of a broader arsenal of security operation center (SOC) tools. These include security orchestration, automation and response (SOAR), security information and event management (SIEM), endpoint detection and response (EDR), and other detection technologies, but also services such as managed detection and response (MDR).“

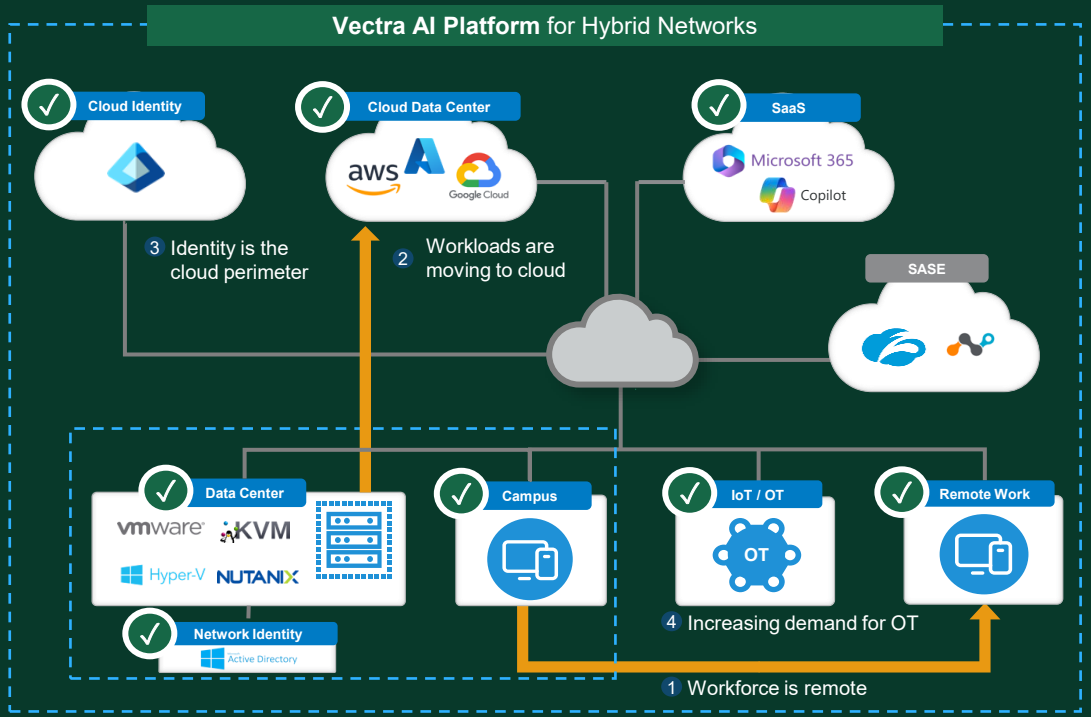
EVOLUTION TOWARDS MODERN NETWORKS



EVOLUTION TOWARDS MODERN ATTACKS



VECTRA AI COVERAGE FOR MODERN NETWORKS



VECTRA

- Agentless
- Native coverage
- Real-time detections
- Enterprise scale
- Intuitive SaaS UX
- Modular design
- Ecosystem-friendly
- 24x7x365 MDR

WHAT VECTRA BRINGS TO THE TABLE

Unified visibility

Correlation of detected attacker behaviour

Accelerated threat detection and response

Vielen Dank