CROWDSTRIKE

VECTRA

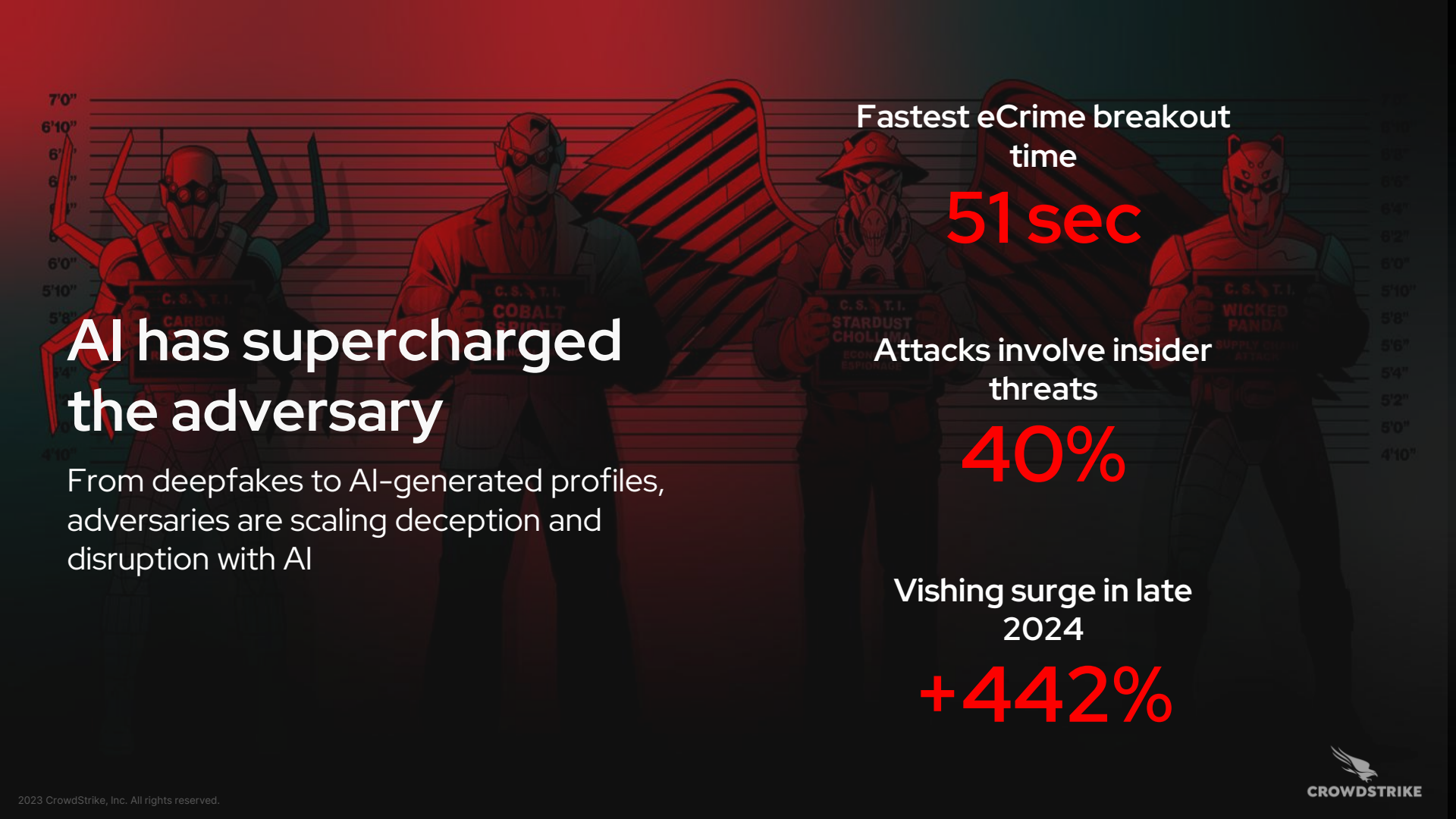
Entspannt digitalisieren: So macht KI Ihre Ämter widerstandsfähig

CrowdStrike Charlotte AI +
Vectra.AI Attack Signal Intelligence

We Stop Breaches

Protection that powers you.

CROWDSTRIKE



AI has supercharged the adversary

From deepfakes to AI-generated profiles, adversaries are scaling deception and disruption with AI

Fastest eCrime breakout time

51 sec

Attacks involve insider threats

40%

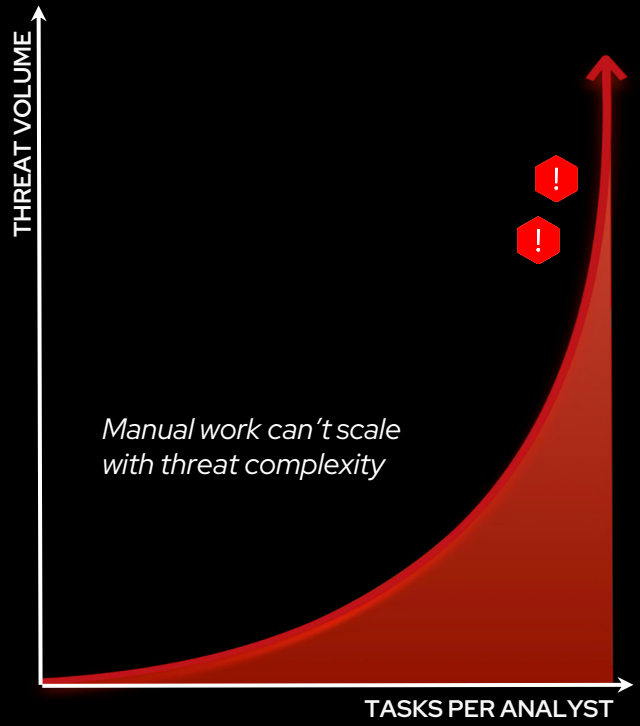
Vishing surge in late 2024

+442%

CROWDSTRIKE

The Defender's Tipping Point: Unrelenting Labor Pains

The labor curve is breaking — and so is defender capacity. A new approach is needed to regain control.



OVERWHELMING COMPLEXITY
Attack surfaces are expanding faster than human teams can handle

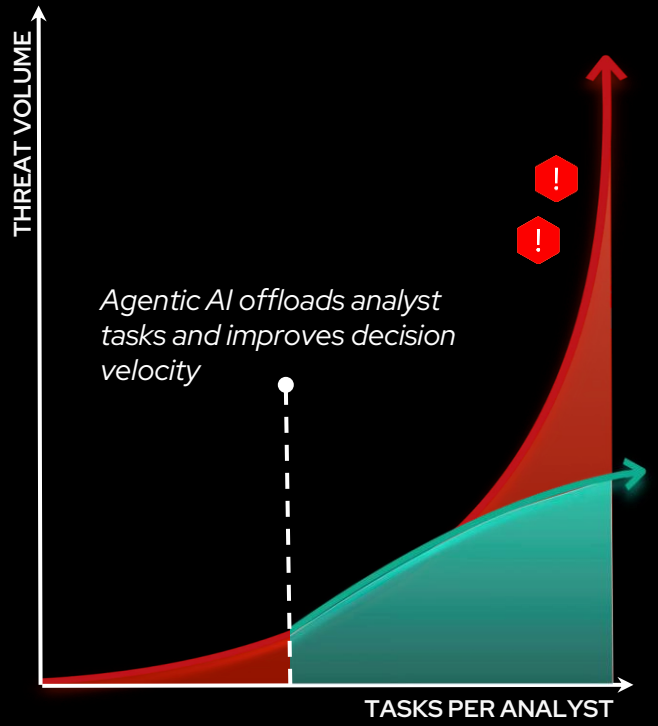
ESCALATING BURNOUT
Repetitive investigations, alert triage, and manual handoffs lead to overload and errors

UNRESOLVED GAPS
Too many tools, too much noise, not enough time- vulnerabilities fester and threats slip through

CROWDSTRIKE

A New Foundation: Agentic AI bends the labor curve

Agentic AI transforms operations — cutting complexity, scaling analyst output, and driving real-time response



REDUCE NOISE
Triage alerts in real time, suppress false positives, and surface only what matters

OFFLOAD OPERATIONAL DRAG
Alleviate analyst backlogs — from routine to complex tasks— and redirect cognitive load to high-impact work

ACCELERATE RESPONSE
Execute at machine speed — with analyst-guided or fully autonomous agents

CROWDSTRIKE

What defenders need- and CrowdStrike delivers

CrowdStrike surveyed 1,000+ security leaders on their AI priorities

Platform-delivered AI. Not another point solution.

Domain-specific Intelligence. Not one-size-fits-all LLMs.

Analyst augmentation. Not replacement.

Built-in value. No hidden costs.

Security by design. Not bolt-on safety.

CROWDSTRIKE

CrowdStrike

Charlotte AI

Accelerate security workflows with a purpose-built AI security analyst

CROWDSTRIKE

Charlotte AI

ACCELERATE RESPONSE

Respond in seconds, not cycles. Use state-of-the-art AI - from agentic AI to embedded assistance - to streamline high-friction tasks and accelerate response.

BUILT ON THE INDUSTRY-LEADING PLATFORM

Purpose-built for the modern SOC, Charlotte AI is powered by the industry's richest telemetry and frontline intelligence, driving informed action to stop breaches

ELEVATE EVERYONE

Empowers users across security workflows with superior signal, expert investigation guidance and surfaced insight from Falcon modules.

OPERATE WITH PEACE OF MIND

Automate confidently and stay in control with customer-defined guardrails for autonomy, oversight, role-based access, and auditability.

CROWDSTRIKE

Charlotte AI: The Rise of the Agentic SOC

With mission-ready agents, operate at adversary speed,with autonomy, precision, and 24/7 operational scale

EXPERT-GRADE PRECISION

>98%

Accuracy in autonomous triage

COMPOUNDING TIME SAVINGS

40+ hours

Avg. analyst hours reclaimed weekly

AUTONOMOUS ACTION

24/7

Drive outcomes around the clock

CHARLOTTE AI

DETECTION TRIAGE

Autonomous, cross-domain triage

- →Consistently triage with expert-level precision
- → Offload manual triage and surface only what matters

CHARLOTTE AI

AGENTIC RESPONSE

AI-guided investigations

- →Apply the frontline expertise to every investigation
- → Accelerate analyst decisions with faster, richer context

CHARLOTTE AI

AGENTIC WORKFLOWS

LLM-powered SOAR

- →Adapt seamlessly to edge cases and unknowns
- → Tailor outputs to fit any team, audience or mission

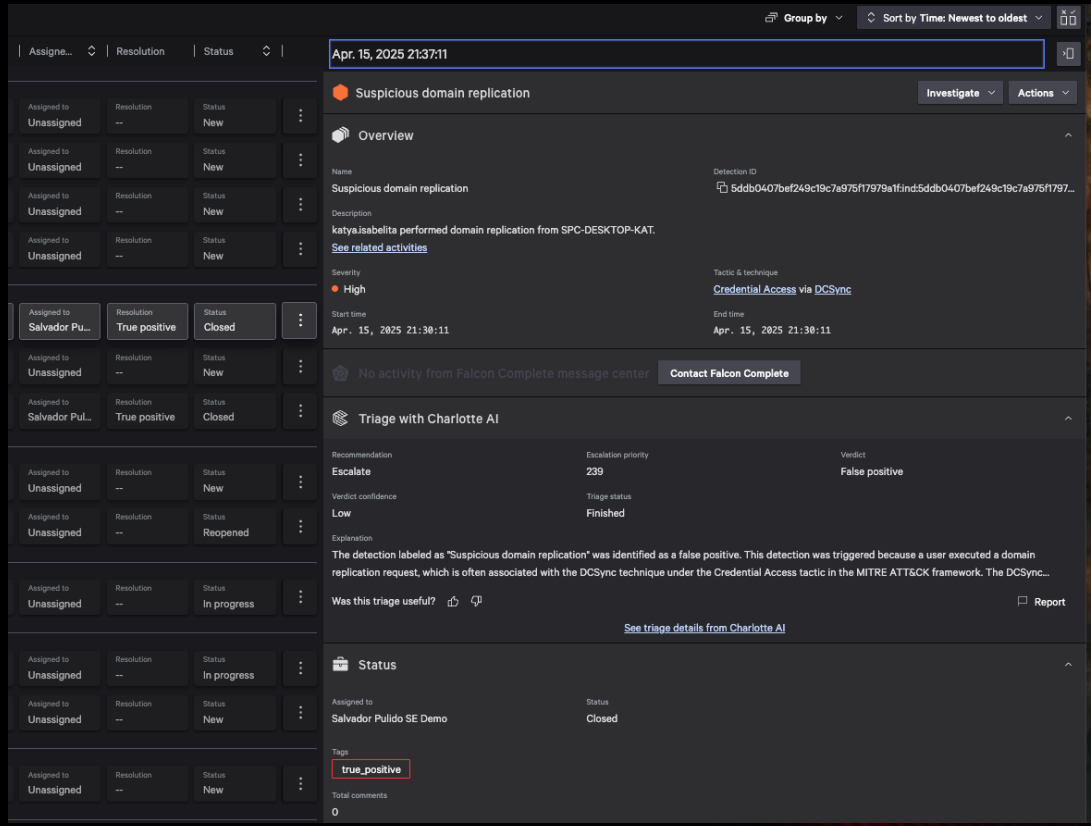
CROWDSTRIKE

CHARLOTTE AI

DETECTION TRIAGE

Autonomous, cross-domain triage

- Expert-level triage across endpoint & identity detections
- Superior, prioritized signal across domains
- Accelerates investigations and MTTR

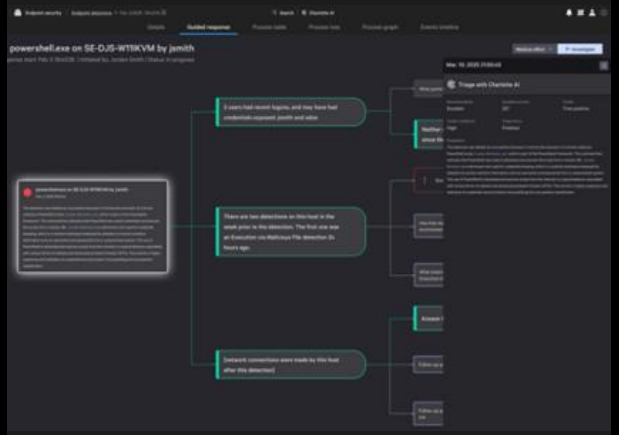


CROWDSTRIKE

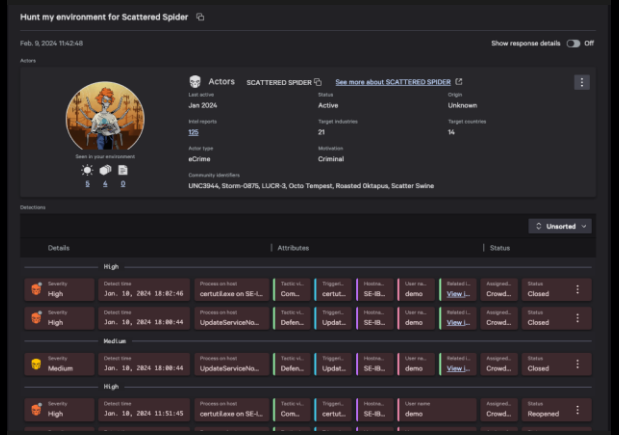
From Mission-Ready Operator to Hands-on Assistant

Powered by state-of-the-art foundational models, Charlotte AI turns hours of work into seconds — from mission-critical investigations to fully autonomous operations

Automate complex tasks
WITH AGENTIC AI



Get fast answers to plain questions
WITH CONVERSATIONAL AI



Streamline hands-on investigations
WITH EMBEDDED GENAI

CROWDSTRIKE

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

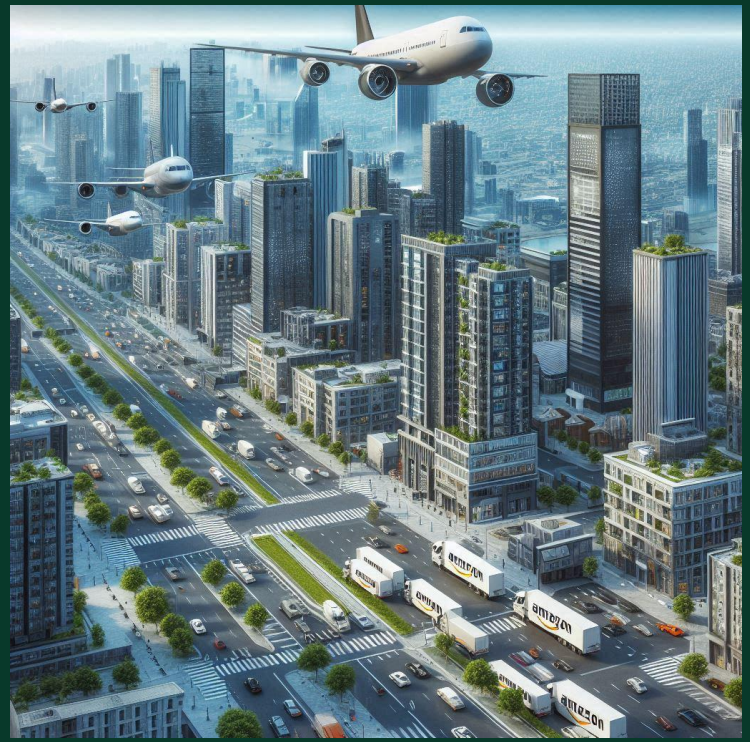
GARTNER MAGIC QUADRANT FOR NDR 2025

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

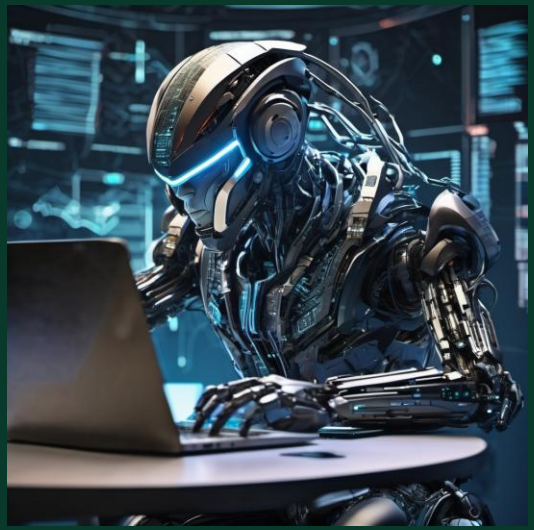
„Organizations rely on NDR to detect and contain postbreach activity such as ransomware, insider threats and lateral movements. NDR complements other technologies that primarily trigger alerts based on rules and signatures by building heuristic models of normal network behavior and detecting anomalies"

„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).“

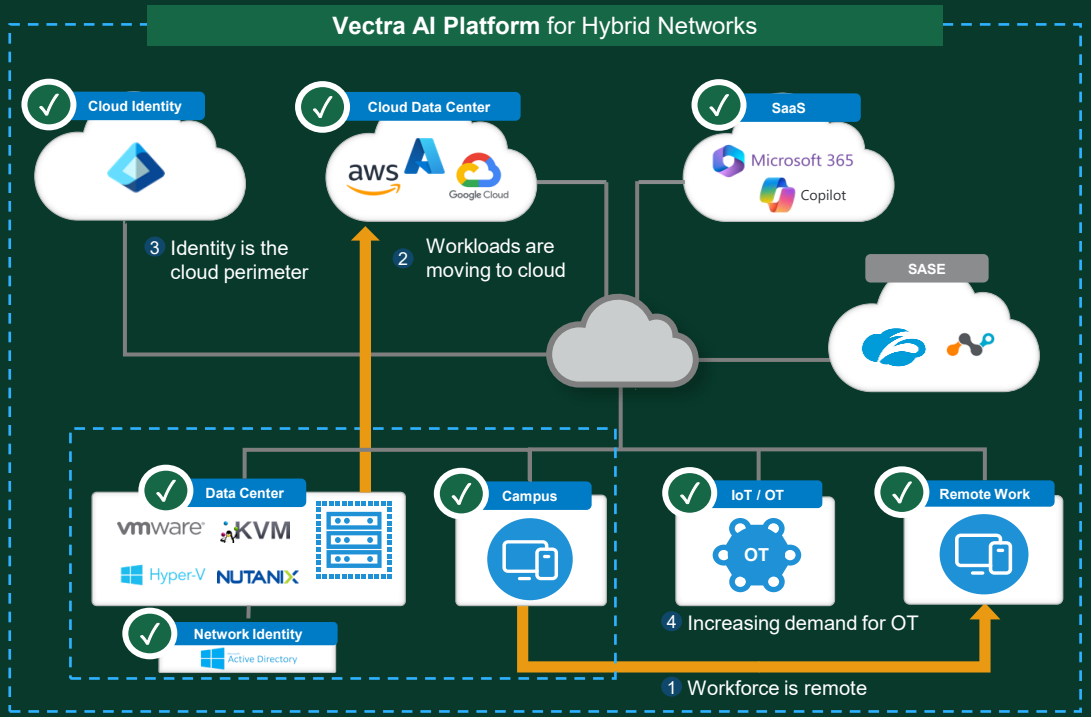
EVOLUTION TOWARDS MODERN NETWORKS



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