Vectra CDR for M365 | AI-Driven Cloud Detection and Response

See and stop threats aimed at Microsoft 365 applications and data

Microsoft 365 (M365) is the go-to productivity suite that hundreds of millions of business users rely on for teams to connect, collaborate and get work done every day. Yet with an abounding number of users on board, the platform is also a prime target of cyber attackers to steal credentials, take over accounts, access critical systems or launch malicious campaigns. Without visibility, proper insight and broad coverage across M365, it remains difficult to discern a compromise in a fast and effective manner. As you connect more employees, security should be a primary concern as native controls can leave apps exposed to attackers who can execute end-to-end attacks without any outside tools. Vectra can help.

Key Challenges Addressed

- Limited SOC visibility across M365
- Account compromise and unnoticed user/entity activity
- Unified visibility for M365
- Clear understanding of attacks

Know when your Microsoft 365 environment is compromised

Vectra Cloud Detection and Response (CDR) for M365 is the industry's most advanced AI-driven attack defense for identifying and stopping threats and attacks across your M365 environment. Vectra CDR for M365 harnesses Security AI-driven Attack Signal Intelligence™ to go beyond simple anomaly detection to analyze and understand attacker behavior. This ensures early detection with clarity, precision and context to erase unknowns and surface threats, attacks and malicious activities across a full chain of suspicious events. With Vectra, organizations see, understand and effectively respond to threats and attacks other solutions miss so security teams spend less time tuning, hunting and investigating — and can respond to attacks sooner.

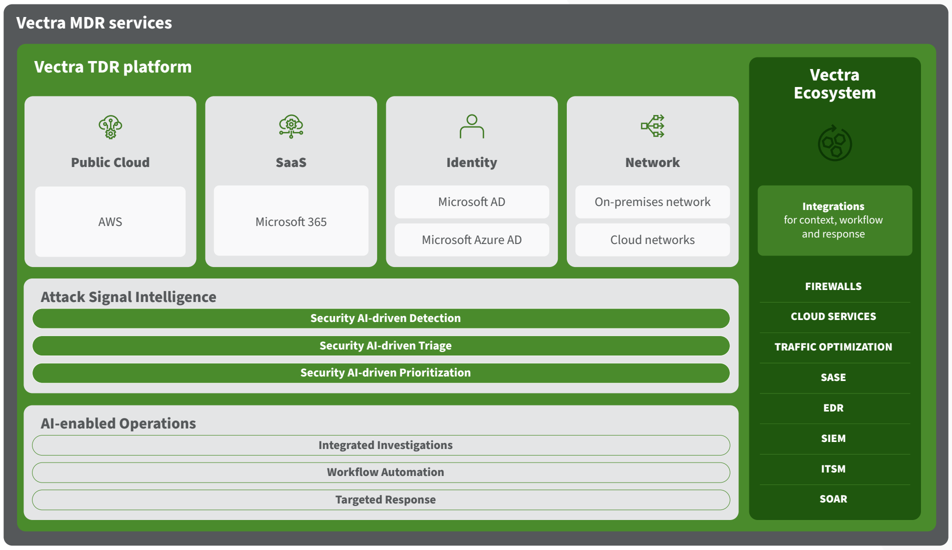
Key Product Capabilities

- **AI-driven Detection**
  Harnessing Security AI-driven Attack Signal Intelligence, Vectra goes beyond signatures and simple anomaly detection to expose the complete narrative of attacks facing M365 applications. Pre-built detection models accurately detect and correlate attacker activity, automating the complex analysis of M365 data to reveal over 90% of malicious techniques in the MITRE ATT&CK framework.
- **AI-Driven Triage**
  Harnessing Security AI-driven Attack Signal Intelligence, Vectra understands previously prioritized threats and suspicious M365 activity. Vectra continuously analyzes M365 incidents and distinguishes malicious events from benign incidents and automates manual tasks with the perspective of an expert analyst, so associated risk scores, context and commonalities are triaged as 'true' detections.
- **AI-driven Prioritization**
  Harnessing Security AI-driven Attack Signal Intelligence, Vectra automatically correlates, scores and ranks multiple and concurrent detections when events unfold. AI analytics automatically assess incidents against extant events to the degree of a highly experienced security analyst — instantly revealing levels of risk exposure and related prioritization so SecOps can devote more time to driving action plans.
- **Advanced Investigation**
  Vectra simplifies deep investigation and puts answers at analysts' fingertips, reducing the effort and time it takes to run complex queries and interpret findings. For M365, Vectra CDR uniquely curates large volumes of sourced data behind each detection then leverages AI to derive more meaning and to surface insights in minutes. Investigators quickly understand the "who," "what," "when" and "how" details behind threats along with the far-reaching effects they will have on M365 apps and data.
- **Automated Workflows**
  Eliminate time-consuming tasks required to aptly monitor and assess cloud logs, investigate detections, initiate threat response and arrive at attribution with threats. Vectra does the work in minutes, so analysts can see compromised accounts, offending apps and how users are accessing tenants.
- **Targeted Response**
  With deeper threat context than native Microsoft tools, security teams gain rich capabilities to respond, contain, investigate, communicate and address compromised systems in less time. Resilient analyst-driven enforcement puts humans in control of response with a flexible approach allowing automated workflows or through in-UI analyst triggered actions. Out of the box response controls include tools and playbooks already in place — all together instilling confidence throughout the team, reducing burnout and minimizing cost.

Explore the Vectra platform

The Vectra Threat Detection and Response (TDR) platform combines complete attack surface coverage across public cloud, SaaS, identity and network. Harnessing Security AI-driven Attack Signal Intelligence™, get unmatched signal clarity that puts you in control while defending against modern, evasive and advanced cyber attackers.

- **Attack Coverage** – Erase unknown threats across 4 of your 5 attack surfaces — cloud, SaaS, identity and networks.
- **Signal Clarity** – Harness Attack Signal Intelligence to automatically detect, triage and prioritize unknown threats.
- **Intelligent Control** – Arm human intelligence to hunt, investigate and respond to unknown threats.



Why enterprises choose Vectra for M365

- **Attack Signal Intelligence** provides rich signal that analysts can use to automate manual tasks related to threat detection, triage and prioritization.
- **Agentless coverage that deploys in minutes** and activates detection without signatures, virtual taps or static policy.
- **Detect threats across MITRE tactics** that other solutions can't see.
- **Built in investigation and response** that speeds threat detections and expands coverage to significantly reduce mean time to response (MTTR).
- **Eliminates mountains of false positives** to give analysts more time for proactive and strategic research.
- **Single view of activity that links detections** originating in M365, on-premises, AWS and AzureAD.

About Vectra

Only Vectra optimizes Security AI to understand attacker behaviors across public cloud, identity, SaaS applications, and data centers. Harnessing Security AI, Vectra is committed to empowering security teams to go on offense and stop cyberattacks from becoming breaches. Vectra provides the threat coverage, clarity, and controls security operations teams need to build more effective, efficient, and resilient security strategies. Organizations worldwide rely on the Vectra Platform and managed services for greater resilience to ransomware, supply chain, account compromise, and insider threats. Learn more at www.vectra.ai.

For more information please contact us:
Email: info@vectra.ai | vectra.ai