Vectra ITDR for Microsoft Azure AD | AI-Driven Identity Threat Detection

See, understand and stop attacks targeting critical SaaS identity services

With the increasing use of SaaS services and the rising volume of remote users, security teams must do more to ensure the identity of users and entities interacting and accessing data across cloud domains. Zero Trust remains far-reaching as organizations struggle with configuration complexities and expert support for identity and access management; leaving threat actors shifting targets to IAM services including Microsoft Azure Active Directory (AD). In the face of ever-increasing attacks, security teams need a new and easier way of identifying threat actors leveraging human and machine-privileged accounts. Vectra can help.

Key Challenges Addressed

- Limited SOC visibility in Azure AD
- Understanding of risks across federated apps
- Account compromise and unnoticed user activity
- Deep attack understanding

Know when your Azure AD Accounts are Compromised

Vectra Identity Threat Detection and Response (ITDR) for Azure AD is the industry's most advanced AI-driven attack defense for closing the door on cyber attackers accessing Azure AD. Vectra ITDR for Azure AD harnesses Security AI-driven Attack Signal Intelligence™ to uncover and counter account compromises and close the door on cyber attackers accessing federated applications and services including: Azure AD M365, Salesforce, AWS and VPNs.

Integrated with the Vectra platform, Vectra ITDR enriches CDR capabilities with user perspective on activities in federated and SaaS apps, where Security AI makes sense of unauthorized sign-ins, scripting engine access, trusted application abuse, domain federation changes and general cloud privilege abuse. AI is applied to learn from data, identify patterns, and to make decisions with no human intervention, ensuring visibility across changing patterns, users and admins — even when MFA fails or authentication is made with stolen cookies.

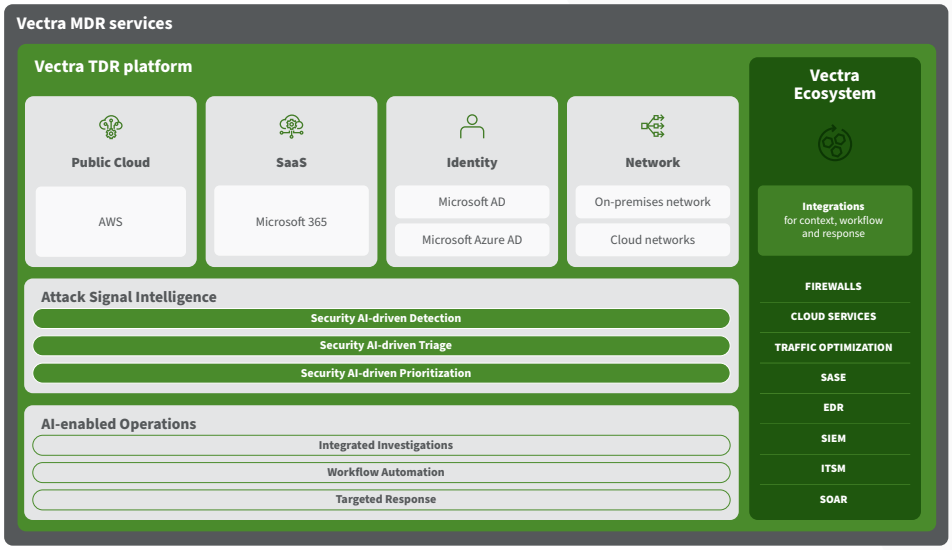
Key Product Capabilities

- **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. With comprehensive analysis of Azure AD account data that's enriched with organizational and consortium insights, Vectra ITDR uncovers malicious use of compromised accounts and credentials. Vectra reveals deeper threat context on a per-account basis to drive attribution and detect over 90% of malicious MITRE ATT&CK techniques.
- **AI-driven Triage**
  Harnessing Security AI-driven Attack Signal Intelligence, Vectra understands previously prioritized threats and suspicious Azure AD activity. By continuously analyzing events, Vectra distinguishes malicious events from those that are benign based on context and commonalities. Benign detections are then triaged automatically with the perspective of an expert analyst.
- **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, interpret findings and proactively surface signals to stop progressing threats. Findings from vast amounts of data are automatically interpreted with up-to-date details, so security analysts become more informed and can drive response action at the right time.
- **Chaos Dashboard**
  Clearly see the impact and any gaps in your Azure AD configurations. Active posture shows the activity that normal users are performing and where it could be leaving your organization open to future attacks, so that you know which risks to mitigate.
- **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 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 Azure AD

- **Attack Signal Intelligence** provides rich signal that analysts can use to automate manual tasks related to threat detection, triage and prioritization.
- **Easy 10-minute setup process** without any hardware.
- **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 Azure AD, M365, on-premises and AWS.

About Vectra

Vectra® is the leader in cyber threat detection and response for hybrid cloud. Vectra's patented Attack Signal Intelligence™ detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra's Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enables security operations teams to prioritize, investigate and respond to cyber-attacks in progress sooner and faster. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyber-attacks. Visit www.vectra.ai

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