Vectra IDR | Microsoft Active Directory and Azure AD

Intelligent identity threat detection and response

Privileged credentials arm malicious insiders and cyber attackers with the most effective means to move about, manipulate services, execute ransomware and steal your data. With Vectra IDR, security operations can easily defend credentials where the IAM infrastructure leaves off — detecting and stopping active credential misuse and privilege abuse by malicious insiders and cybercriminals.

Key Challenges Addressed

- Attackers bypassing access controls and MFA
- Account compromise attacks
- Misuse of over-privileged access
- Pathways between AD and Azure AD
- Increasing threats on AD and Azure AD
- Understanding and defense of identity-based IOCs

See and take action when trusted accounts are compromised

Vectra IDR provides intelligent identity threat detection and response that surfaces and stops active AD and Azure AD identity misuse and account takeover in real-time. As a component of the Vectra platform, Vectra IDR leverages AI-driven Attack Signal Intelligence™ to signal active and covert identity behaviors like stealthy admins, misused service accounts and malicious sign-ins across multiple attack surfaces. With full context into incidents and knowledge of acceptable behavior, it ensures a 365-degree view of identity-based attacks with 90% less noise than other ITDR tools. Vectra delivers unmatched signal clarity, coverage and control, enabling organizations to immediately see, make sense of, and shut down unauthorized sign-ins, scripting engine access, trusted application abuse, domain federation changes and widespread cloud privilege abuse before the onset of ransomware and data breaches.

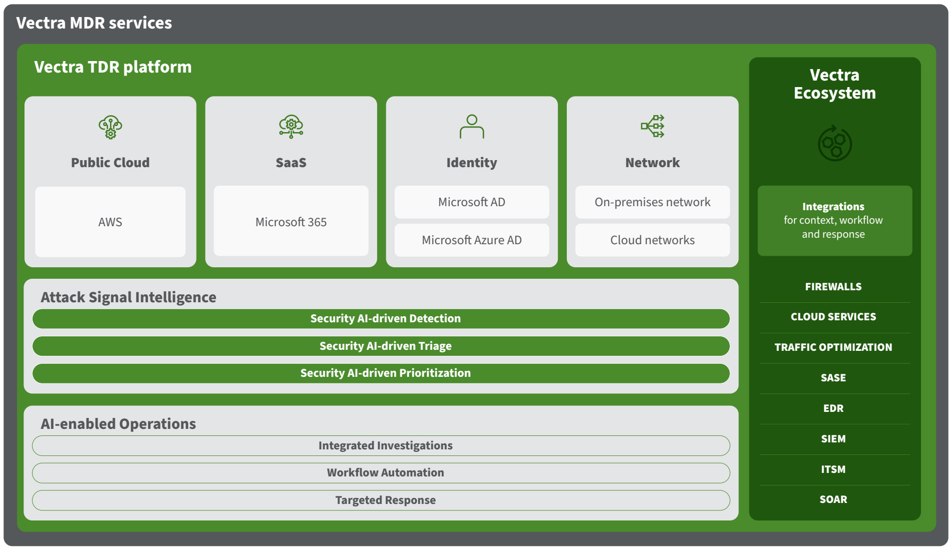
Key Capabilities

- **AI-Driven Detection with an Identity Focus**
  Vectra IDR automatically identifies active insider threats and cyber attackers abusing privileges and compromising accounts with comprehensive machine learning and identity-focused behavior analytics. Attack Signal Intelligence ensures granular insight into Azure AD and Active Directory data distinguishing benign anomalies from nefarious, uncommon user activity. Vectra reveals credential misuse, privilege elevation, entitlement abuse, elusive replication streams and other identity-based threat tactics with meaningful detail and without long delays and guesswork.
- **AI-Driven Prioritization and Triage**
  Vectra IDR continually correlates manifolds of identity-related events into actual threat activities indicative of account compromise and abuse. It then scores, ranks and triages active threat detections as suspicious human, system and cloud service access activity unfolds. The AI-driven analytics shift the human element out of efforts needed to understand where to focus resources instantly revealing AD and Azure AD risk exposure level, threat priority and urgency — bringing focus to what matters most.
- **Instant Insights and Advanced Investigation**
  Accelerate analyst research efforts across the growing pool of AD and Azure AD accounts/users. With one click, SOC analysts can explore the indicators of compromised identities in detail — what was exposed, functions, services, files, and accounts manipulated with the alert trigger. When deep investigation is needed, it automatically coalesces vast amounts of identity data to bring visibility to weaker signals more efficiently and give more meaning to IOCs with the evidence and insight needed.
- **Continuous Monitoring and Visual Control**
  Maintain a comprehensive view of active account abuse from our cloud UI or a consolidated UI on the NDR appliance. Experience rich dashboards that zero in on identity-based attacks highlighting what's most important — see threats in specific regions and apps, observe risk levels on nefarious authentication activity and access abuse of all accounts and endpoints (managed and unmanaged), and know where you need to strengthen defenses to protect data on-premises and in the cloud.
- **Targeted Response in Minutes**
  Activate identity enforcement playbooks and lock down compromised accounts and privilege misuse immediately. Vectra IDR overcomes delays in addressing comprised accounts with high-fidelity threat detection and controls that ensure the SOC can move swiftly. Out-of-the-box controls drive near real-time response automation and support analyst-triggered actions to quickly suspend or reset user/application access, double validate a threat, initiate action through ticketing and reporting workflows — using cloud-native tools and solutions like Microsoft Sentinel, Defender and Splunk.
- **Activate in Minutes**
  Vectra's powerful ITDR solutions activate from a SaaS UI without the need for sensors, appliances or software deployment. SOC teams can easily augment threat detection and response strategies and get up and running fast, with a few simple steps and without complex integrations.

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 your SOC in control with the most effective defense against modern, evasive and advanced cyber attackers.

- **Attack Coverage** – Erase unknown threats across 4 of your 5 attack surfaces – cloud, SaaS, identity, 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 Leverage Vectra IDR

- **Employs AI-driven Attack Signal Intelligence™** to detect, prioritize, and triage identity-based attacks other solutions cannot see.
- **Defends when attackers obtain unauthorized access** to critical assets, domain servers, service accounts, local credentials and network and cloud data.
- **Simplifies investigation with AI and automation** that reduces efforts to query and interpret findings.
- **Activates in 10 minutes** and delivers a single view of identity activity in AWS, Azure and M365 without hardware, signatures, virtual taps or static policy.
- **Unmatched threat context** that ensures understanding of network and risky cloud user behaviors to stop future attacks.

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 cyberattacks. Visit www.vectra.ai.

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