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

See, understand and stop cyber threats targeting AWS applications and data

AWS makes moving to the cloud faster, easier and more cost effective to capture new growth opportunities. And while many organizations are jumping on board, so too are cyber attackers who continue to evolve and improve tactics that enable them to target applications and data living in the cloud. This dynamic has SOC teams struggling to address unknown threats that prevention security and native cloud controls won't catch —leaving blind spots for attackers to access your most critical systems.

Key Challenges Addressed

- Account compromise and unnoticed user/entity activity
- Mean Time to Respond (MTTR)
- Limited SOC visibility in the cloud
- Research and investigation
- Heightened attack understanding
- Broad coverage across workloads and applications deployed regionally

Know when your AWS applications and data are compromised

Vectra Cloud Detection and Response (CDR) for AWS is the industry's most advanced AI-driven attack defense for identifying and stopping threats and attacks across your AWS services and storage. Vectra CDR for AWS 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 while responding to attacks sooner.

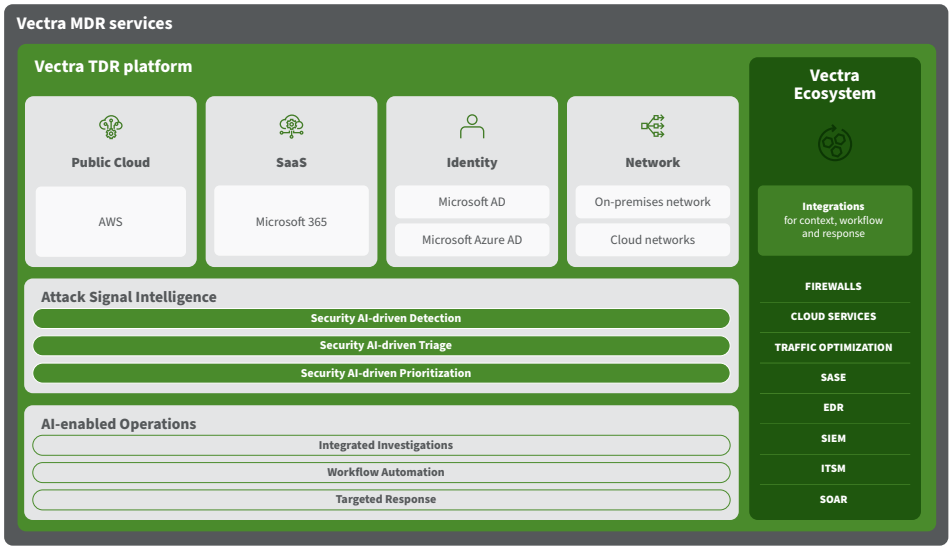
Key Capabilities

- **AI-Driven Detection**
  Harnessing Security AI-driven Attack Signal Intelligence™ Vectra CDR automates threat detection tasks and exposes the complete narrative of active attack methods targeting data in AWS. Just like an expert analyst, it accurately discerns incidents and distinguishes the veracity of weak indicators from billions of data points derived from various logs and sources while covering over 90% of tactics recognized by MITRE ATT&CK.
- **AI-Driven Triage**
  Harnessing Security AI-driven Attack Signal Intelligence Vectra CDR uses machine learning (ML) to generate security analysts' intuition and automate alert triage, reducing alert noise by over 80%. With the logic of an expert analyst, previously prioritized threats and attacks are further assessed against associated risk scores, context and commonalities to triage detections.
- **AI-Driven Prioritization**
  Harnessing Security AI-driven Attack Signal Intelligence Vectra CDR minimizes the time and effort needed to correlate, score and rank multiple and concurrent detections as events unfold. AI analytics assess each detection against extant events automatically to the degree of a highly experienced security analyst. You instantly see levels of risk exposure and related prioritization without manual research and analysis so SecOps can devote more time to driving action plans.
- **Advanced Investigation**
  Vectra simplifies the approach to deep investigation with AI, reducing the effort and time it takes to run complex queries and interpret findings from vast amounts of data sourced from AWS logs, other properties and third-party tools. AI surfaces signals with contextual details in milliseconds so security analysts become more informed and drive response action at the right time. You can examine data across hosts, users and entities to bring clear attack signals into view across the full enterprise to easily see relationships, characterize intent for a full understanding of the overall business impact.
- **Chaos Dashboard**
  Gain immediate visibility across the AWS surface, revealing all accounts, services, users and roles active in every AWS region, so you know what and whom you are monitoring.
- **Control Plane Security**
  Stop threats in the control plane by analyzing activity associated with users and assumed roles. Vectra reveals masked attacks that compromise trusted identity and escape detection to threaten AWS compute, network, storage services and data.
- **Targeted Response**
  Native capabilities or out of the box integrations with SIEM, SOAR, EDR and ITSM solutions allow teams to respond effectively and easily contain, investigate, communicate and address compromised systems in a fluid manner that instills confidence throughout the team and reduces burnout.

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, 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 CDR for AWS

- **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.
- **Compliment Guard Duty** and CWPP/CSPM solutions to reduce noise and reveal threat signals with more context of the effects on the control plane and network.
- **Detects threats across MITRE tactics** that speed up threat detections, expands coverage, reduces and significantly lowers 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 AWS, on-premises, M365 and AzureAD.

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