Vectra NDR | AI-Driven Network Detection and Response

Detect, investigate and respond to attacks across your network

Your network is the foundation of your enterprise infrastructure and warrants a highly effective cyber defense strategy. Without the right level of network visibility and the tools to quickly contextualize an abundance of security data, external attackers and malicious insiders will maintain an advantage and cost you millions.

Key Challenges Addressed

- Lateral movement
- Unusual network activity
- Mean Time to Respond (MTTR)
- Overburdened hunting and investigation
- Real-time intrusion detection
- Heightened attack understanding

Detect the unknown, stop the breach

Vectra Network Detection and Response (NDR) is the industry's most advanced AI-driven attack defense for identifying and stopping malicious tactics in your network without noise or the need for decryption. Vectra NDR harnesses Security AI-driven Attack Signal Intelligence™ to ensure early visibility 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 more time enabling business growth.

Key Capabilities

- **Network Visibility**
  See, analyze and store all network activity and reveal hidden malicious behavior without prior knowledge or pattern detection. Automatically track attacker activity including privileged credential abuse, lateral movement, command & control and remote execution across your network and distributed host system environments on-premises and in the cloud.

- **AI-Driven Detection**
  Vectra NDR automates threat detection with advanced analytics, deep learning, complex behavior analysis and insights into attacker methods to effectively discern incidents from billions of data points just like an expert analyst. Teams can pinpoint threats and attributions around attacks and malicious transactions on the network including duplicate or asymmetric traffic and encapsulations to automatically distinguish the veracity of weak indicators, evasive and unknown patterns and detect up to 90% of attacker tactics and techniques listed in MITRE ATT&CK.

- **AI-Driven Triage**
  Prioritization is taken to the next level with an ML/AI approach that further analyzes active detections, the context of each, commonalities between events and scores to assess the urgency of each true positive detection without any human involvement. Analysts are able to spend more time on urgent incidents while reducing the pool of detections that need reviewing by 80%.

- **AI-Driven Prioritization**
  Vectra NDR automates prioritization that escalates the most urgent threats by scoring and ranking thousands of events as they unfold and to the degree of a highly experienced security analyst — putting relevant details at your fingertips in milliseconds rather than minutes and hours.

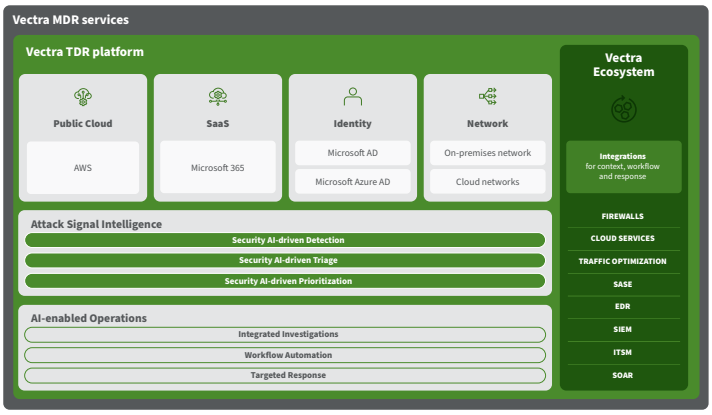
- **Advanced Investigation**
  Constantly derives knowledge from your ever-changing network infrastructure and presents the insights you seek most:
  - Looks for anomalous outbound flows of data, even in encrypted channels.
  - Correlates detections across host entities, learns the archetype and identifies each object to present information in various ways that allow you to easily see relationships, characterize intent and understand business impact.

- **Built-in Response Actions**
  Designed to ensure patented MITRE D3FEND countermeasures for powerful response action to contain, investigate and remediate compromised systems. Your teams are more focused, more efficient and effective and as a result — you reduce analyst burnout and turnover.

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.
- **Control** – Arm human intelligence to hunt, investigate and respond to unknown threats.



Enhance your Vectra NDR Solution with the following:

- **Vectra Match** brings intrusion detection signature context to Vectra NDR by coupling exploit detection powered by Suricata and AI-driven detection to contextualize attacker behaviors.
- **Vectra Recall** enables your SecOps team to perform retrospective threat hunting using enriched network metadata organized by both host name and IP address. Store and search through your network metadata for as long as it is needed with cloud-powered limitless scale.
- **Vectra Stream** enables your security-enriched cloud and network metadata with security insights to be streamed directly to SIEMs and data lakes for your own custom models.

Why enterprises choose Vectra for NDR

- **Attack Signal Intelligence** provides rich signal that analysts can use to automate manual tasks related to threat detection, triage and prioritization.
- **Ensures that you know if and when your network** has been compromised and that you are equipped to manage the best outcome.
- **Speeds up threat detections** by expanding coverage, reducing investigation time and significantly lowers mean time to response (MTTR).
- **Automates the manual tasks associated with tier-1 and tier-2 analysis** to reduce the overall security operations workload.
- **Stops ongoing attacks** and gives security analysts more time to proactively hunt and research.
- **Eliminates mountains of false positives** and the associated tasks of hunting and investigating, which can impose more risk.
- **Deploy everywhere** across physical, virtual or cloud environments.
- **Integrate seamlessly** with cloud network, firewall, XDR security and SIEM/SOAR.

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