Vectra AI Platform

Integrated signal for extended detection and response (XDR)

The Vectra AI Platform provides hybrid attack surface visibility across identity, public cloud, SaaS, data center networks and endpoints via EDR integration. With patented AI-driven Attack Signal Intelligence™ the Vectra AI Platform prioritizes real attacks in real-time with integrated, automated and co-managed response that moves at the speed and scale of hybrid attackers.

The Problem

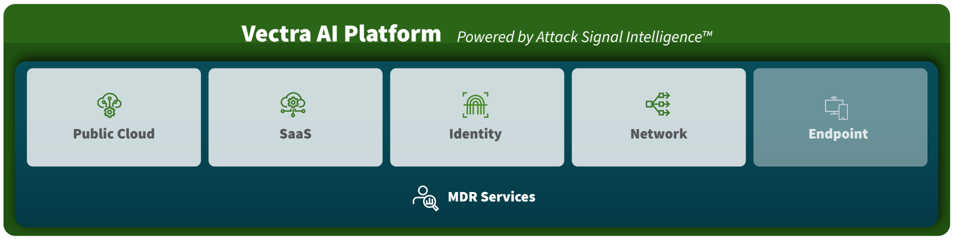
As enterprises shift to hybrid and multi-cloud environments, embrace digital identities, digital supply chains, and ecosystems, SOC teams are forced to deal with a vicious spiral of more. More attack surface to cover. More alerts to manage. More analyst workload, burnout and turnover. Breaking the spiral of more requires a modernized SOC for hybrid attack resilience.

SOC Modernization Use Cases

- **Signature + AI-driven detection:** Integrate signatures, threat intel and AI-driven behavior-based models in a single platform.
- **SIEM / SOAR optimization:** Lower cost and complexity by reducing detection engineering time.
- **IDS replacement:** Ingest Suricata signatures to retire legacy IDS tools — reducing complexity and containing cost.
- **PCAP displacement:** Eliminate the cost and complexity of managing terabytes of network data.
- **EDR extension:** Extend beyond endpoint to cover data center networks, identities, SaaS and public clouds.
- **Hybrid SOC:** Supplement in-house SOC talent and resources with MDR services providing global 24x7x365 coverage.
- **Cloud Control Plane protection:** Monitor, detect and prioritize when cloud infrastructure are compromised.
- **Cloud identity protection:** Map attack progression with contextualized cloud identity threat activity.
- **Critical infrastructure risk:** Reduce exposure to hybrid cloud infrastructure and supply chain.
- **OT environment risk:** Future-proof your defenses as your IT and OT attack surface expands.
- **Remote workforce risk:** Monitor, detect and stop known and unknown attacks to your remote and hybrid workforce.

How the Vectra AI Platform helps modernize the SOC

- Consolidates public cloud, identity, SaaS and data center network visibility, eliminating 90% of blind spots.
- Tracks attack progression and lateral movement to and from public cloud, identity, SaaS and data center network domains.
- Keeps pace with advanced hybrid attacks with AI-driven Attack Signal Intelligence.
- Reduces latency in the detection, investigation and response process by focusing on entities, not events.
- Leverages 150+ pre-built AI detection models by domain to reduce detection engineering time from months to days.
- Reduces alert noise by 80% by automating alert triage, boosting SOC analyst productivity more than 2x.
- Accelerates mean time to investigate and respond with pre-built pathways and customizable metadata queries.
- Integrates with 40+ tools across EDR, SIEM, SOAR and ITSM technologies.
- Delivers a shared-responsibility hybrid SOC model where customer and Vectra MDR analysts collaborate in real-time.
- Reinforces cyber resilience through harnessing attack insights derived from thousands of customers.



Vectra AI Platform *Powered by Attack Signal Intelligence™*

Public Cloud | SaaS | Identity | Network | Endpoint

MDR Services

Why the Vectra AI Platform? *We find attacks others can't.*

Coverage: Integrated attack visibility and context across the entire hybrid attack surface: identity, public cloud, SaaS and data center networks.

- Covers >90% of MITRE ATT&CK techniques, eliminating blind spots.
- Most MITRE D3FEND references for defensive countermeasures.
- Seamless integration for attack context, investigation workflow and response.

Clarity: Integrated AI-driven Attack Signal Intelligence thinks like an attacker, knows what's malicious and focuses on what's urgent to prioritize attacks in real-time.

- Sees through encryption removing the burden of decryption for detection.
- Focuses on accounts most useful to attackers with patented Privileged Access Analytics (PAA).
- Zeros in on attacker behavior, analyzing in many dimensions to see real attacks in a sea of different.

Control: Integrated, automated, co-managed investigation and response actions that arm SOC teams to move at the speed and scale of hybrid attackers.

- Puts 360-degrees of attack context at analysts' fingertips to investigate attacks in real-time.
- Enables automated or manual response actions that isolate and contain attacks in minutes.
- Communicate and collaborate with Vectra MDR analysts in real-time to build hybrid attack skills and expertise.

Vectra AI Platform capabilities:

The Vectra AI Platform's modular design provides SOC teams with the flexibility to add coverage, clarity and control as the organization's on-premises, hybrid and multi-cloud infrastructure evolves including:

- Network Detection and Response for on-premises and cloud networks
- Identity Detection and Response for Microsoft Active Directory and Azure AD (now known as Microsoft Entra ID)
- Cloud Detection and Response for Microsoft 365
- Cloud Detection and Response for AWS
- Managed Detection and Response services

Vectra AI Platform features:

- **AI-driven Prioritization**: security automation that correlates, scores and ranks incidents by urgency level.
- **AI-driven Triage**: security automation that learns customers' unique environment, distinguishing between malicious and benign events.
- **AI-driven Detection**: security automation that monitors for attacker behavior post-compromise.
- **Instant Investigation**: arms analysts of all skill levels with lighted pathways that serve as a quick start guide for investigations.
- **Advanced Investigation**: enables analysts to query Azure AD (now known as Microsoft Entra ID), M365, or AWS Control Plane logs directly in the platform UI.
- **Targeted Response**: analyst-driven enforcement triggered automatically or manually to lockdown an account, isolate an endpoint or execute a playbook.

Vectra AI Platform ecosystem:

- **EDR:** Microsoft Defender, CrowdStrike, SentinelOne, Carbon Black, Cybereason
- **SIEM:** Microsoft Sentinel, Splunk, IBM QRadar, Google Chronical
- **SOAR:** Palo Alto CORTEX, Splunk, IBM QRadar, Google Siemplify, Swimlane
- **SASE / SSE:** Zscaler, Netskope
- **ITSM:** ServiceNow, Atlassian Jira
- **Firewalls:** Palo Alto, Juniper, Fortinet, Check Point
- **Traffic Optimization:** Keysight Technologies, Gigamon, cPacket networks

Watch a demo of the Vectra AI Platform

Take a tour of the Respond UX interface

Schedule a personal demonstration

About Vectra AI

Vectra AI is the leader in AI-driven threat detection and response for hybrid and multi-cloud enterprises. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single platform. The Vectra AI Platform with patented Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks in their hybrid environment. Vectra AI has 35 patents in AI-driven threat detection and is the most referenced vendor by MITRE D3FEND. Organizations worldwide rely on the Vectra AI Platform and MDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

For more information please contact us:

Email: info@vectra.ai | vectra.ai