# Vectra platform overview

**The adoption of hybrid cloud has led to an increased attack surface, making it easier for attackers to bypass prevention controls, infiltrate, compromise credentials, gain privileged access, move laterally and exfiltrate sensitive corporate data while largely going undetected. In fact, Vectra research found that 72% of security leaders think they may have been breached but don't know it. Put another way, "*we don't know where we are compromised - right now.*"**

**We call this the unknown.**

We argue the unknown threat is the biggest risk to organizations today, and it is being fueled by the massive shift to hybrid cloud over the past two years. The challenge for security teams defending against the unknown comes down to three things:

- How to cover more attack surface without adding more complexity?
- How to detect more evasive attackers without creating more alert noise?
- How to ensure SOC analysts keep pace without burning them out?

### Key challenges:

- Increasing analyst workloads
- Growing cloud complexity, vulnerabilities and exploits
- Difficulty identifying and prioritizing real attacks
- More devices accessing cloud and on-premises networks
- Difficulty keeping pace with cloud-based attacks

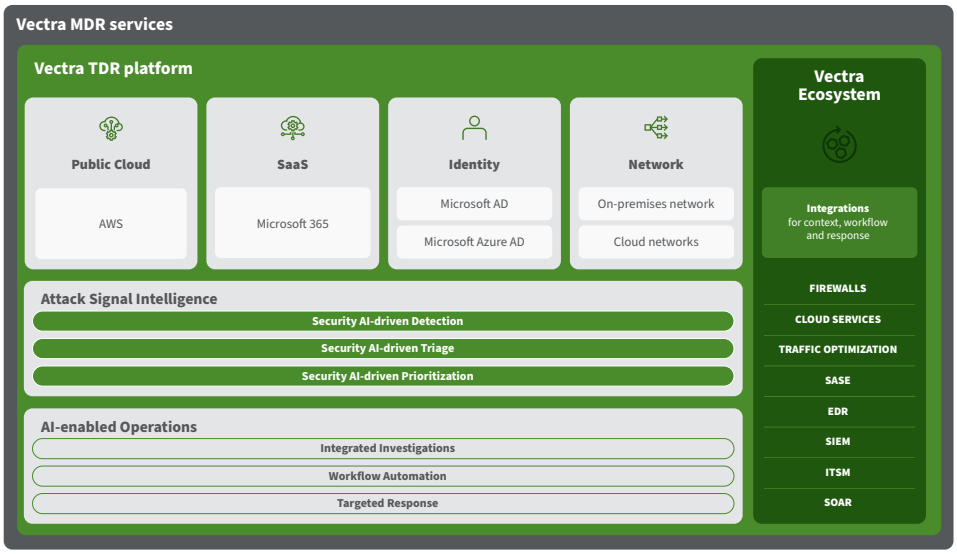
## Vectra Hybrid Cloud Threat Detection and Response platform and services

Our approach is simple. Defending against modern cyber attackers comes down to arming defenders with the right **coverage, clarity,** and **control**.

**Attack surface coverage across four of the five attack surfaces:** network (both on-premises and cloud-based), public cloud, SaaS, identity and endpoint detection and response (EDR) integrations for context, workflow and response.

Vectra provides the hybrid cloud building blocks to future proof your cyber defense as your attack surface expands:

- Vectra Network Detection and Response (NDR)
- Vectra Cloud Detection and Response (CDR) for AWS
- Vectra Cloud Detection and Response (CDR) for M365
- Vectra Identity Detection and Response (IDR) for Azure AD
- Vectra Recall to query, investigate, hunt for threats
- Vectra Stream for security-enriched metadata lake
- Vectra Managed Detection and Response (MDR)




**Signal Clarity with Vectra's Security AI-driven Attack Signal Intelligence™:** automate threat detection, triage and prioritization across the cyber kill chain from execution, persistence and reconnaissance to command and control, evasion, access, escalation, lateral movement and exfiltration.

**Intelligent Control with AI-enabled operations:** an intuitive user interface that puts answers at analysts' fingertips. Including automated workflows that reduce complexity and cost by automating manual tasks, while targeted response puts analysts in control with flexible response actions triggered automatically or manually.

## Prioritize real threats and turn the tables on attackers

The Vectra Hybrid Cloud Threat Detection and response platform harnesses Attack Signal Intelligence, empowering analysts with:

**AI-Driven Detections that think like an attacker**

- Behavior-based models accurately detect attacker TTPs.
- Correlated detections of attacker TTPs across domains.
- Comprehensive visibility of the complete attack narrative.

**AI-Driven Triage so you know what is malicious**

- Continuous analysis of all active detections for commonalities.
- Intuitive by design to distinguish malicious vs. benign activity.
- Automated to expose the malicious and log the benign.

**AI-Driven Prioritization so you know what is urgent**

- Real-time threat analysis for severity and impact.
- Unified view of prioritized threats by severity and impact.
- Contextual alerting accelerates investigation and response.

### Resiliency across your SOC

**Advanced Investigation**

Streamline research of M365 and AWS Control Plane logs to understand the attacks facing you in minutes.

**Ecosystem Integrations**

Integrate existing tech for correlation and context and to automate analyst workflows and response controls.

**Managed Services**

Managed detection, response, and training services to provide the skills and 24/7/365 reinforcements defenders need.

## What it means for security teams

With the Vectra Hybrid Cloud Threat Detection and Response platform, your organization is more resilient to attacks:

- Up and running with actionable detections in days if not hours.
- Future-proof your cyber defense as your attack surface expands.
- Reinforcements at the ready with Vectra MDR services.

Your processes and workflows are more efficient:

- Reduce SIEM costs, detection rule creation and maintenance.
- Automate analysts' manual tasks and time to investigate and respond.
- Optimize existing investments in EDR, SOAR and ITSM.

Your security analysts are more effective:

- Reduce analyst burnout with accurate detection of malicious true positives.
- Increase analyst throughput by accelerating investigation and response.
- Builds analyst expertise and skills hunting and defending against advanced attacks.

The Vectra Hybrid Cloud Threat Detection and Response platform and services provide the intelligent signal that empowers security analysts to take intelligent action. The result: empower SOC teams to get ahead and stay ahead of modern, evasive and sophisticated attackers.

**Resources to Learn More**

## 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 enable 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.

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