

Vectra Managed Detection and Response (MDR) Services

The combination of today's ever-expanding hybrid cloud landscape and cyber attackers' advanced tactics, create a multitude of unknown threats for security teams to address. Additionally, many teams are already overwhelmed with alert noise, resource constraints and limitations presented by an ongoing challenge to retain and recruit talent.

This reality can't be fixed by adding more tools and data sets to analyze. That will only lead to more analyst fatigue, burnout and eventually — turnover. Meanwhile, security, risk and compliance leaders can no longer depend on detection and response methodologies that rely on signatures, anomalies and rules to see and stop cyber attackers from infiltrating an organization. The traditional approach is broken, and in order to defend against today's threats — 24/7/365 threat detection and response is required.

83% of security leaders think traditional approaches do not work for modern threats. – Global Research Study, Fit for Purpose or Behind the Curve

Key challenges addressed:

- Skills shortage and analyst burnout
- Securing ever-evolving cloud environments
- Vectra TDR platform optimization
- Hunting and investigation expertise
- 24/7/365 threat detection and response
- Tool proliferation and management

Vectra MDR erases unknown threats with 24/7/365 trusted expertise

Vectra Managed Detection and Response delivers the cybersecurity skills you need to detect, investigate and respond to threats 24/7/365. Vectra analysts and your security team work together in the Vectra Threat Detection and Response platform for complete visibility, collaboration and faster resolution times leveraging our **shared responsibility model**. Our platform empowers your organization to keep control by interacting as much (or as little) as you want with our Vectra analyst team on investigations and response actions allowing for 'real time' collaboration. Your security operations team gains:

Coverage

Vectra MDR is your 24/7/365 eyes-on-glass service that proactively investigates and stops attacks across your public cloud services, SaaS applications, identity systems and network infrastructure.

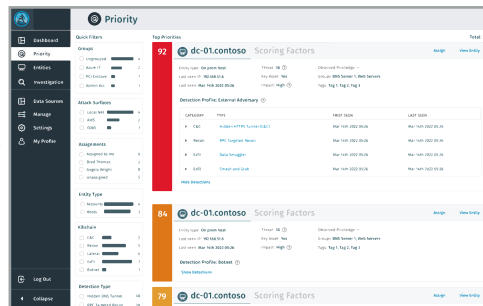
Clarity

Vectra MDR is an extension of your security team with expert analysts available for 24/7/365 investigations and alert prioritization.

Control

Going beyond typical MDR services, your security analysts work in the same platform as Vectra analysts for complete visibility, control, and collaboration investigating and resolving threats.

Vectra MDR



Your Team



Cyber defense reinforcements at the ready

Human intelligence that does not sleep

Vectra Attack Signal Intelligence enables AI-detection, triage and prioritization of modern, evasive and sophisticated attacks. Vectra MDR analysts deliver 24/7/365 investigative, response and platform optimization expertise. By adding human intelligence from our analyst team to the power of the Vectra platform, we respond faster, delivering unmatched outcomes for customers.

Extension of your security team

Vectra MDR is an extension of your security team that deploys experienced security analysts to help you fully utilize the Vectra platform. This includes recurring meetings with security experts to discuss customer specific and global trends, security posture and events in your network. You gain:

- Expertise and threat analysis
- 24/7/365 monitoring and proactive investigations
- Proactive Vectra deployment customization
- Live in-app MDR team/customer communication

Optimize the Vectra platform

Vectra security analysts work alongside your Vectra platform with knowledge and experience to efficiently investigate and resolve incidents. Ensuring you get the most out of Vectra by providing:

- Investigation expertise
- Configuration optimization
- Global threat and attack insight
- Platform investigations, context and visibility

Turn the tables on attackers with human intelligence and AI-driven operations

Arm security leaders, architects and analysts to get ahead and stay ahead of modern cyberattacks.

Early threat detection and context

Vectra MDR services will investigate and respond to threats with the expert lens of a Vectra security analyst. Threats are automatically detected and prioritized.

AI-driven triage and platform tuning

Vectra MDR security analysts have amassed extraordinary knowledge from observing countless threat behaviors in hundreds of Vectra deployments. Security teams get support in creating custom filters to approve authorized behaviors and get individualized suggestions for an effective triage process.

Vectra Security AI-driven Attack Signal Intelligence™ empowers analysts to:

- **Think like an attacker** AI-driven detections expose the complete narrative of an attack.
- **Know what is malicious** AI-driven triage exposes malicious true positives.
- **Focus on the urgent** AI-driven prioritization is 85% more effective at prioritizing critical threats.

Given the number of security tools in use across organizations, it can be challenging for everyone to be an expert on any one platform or solution. At the same time, it's increasingly important to make sure security controls are being optimized 24/7/365 in order to stay ahead of attackers. Unlike other approaches, Vectra MDR services enables your organization to keep the control in a shared responsibility model — whether you leverage the service to augment your current team alongside the Vectra platform or to outsource security operations completely. When you extend your SOC team with Vectra MDR analysts — your organization is empowered to erase the unknown and turn the tables on attackers.

[Learn more about Vectra's Managed Detection and Response](#)

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.