AIRMDR

MDR That Moves Fast, Integrates Completely, and Shows Its Work

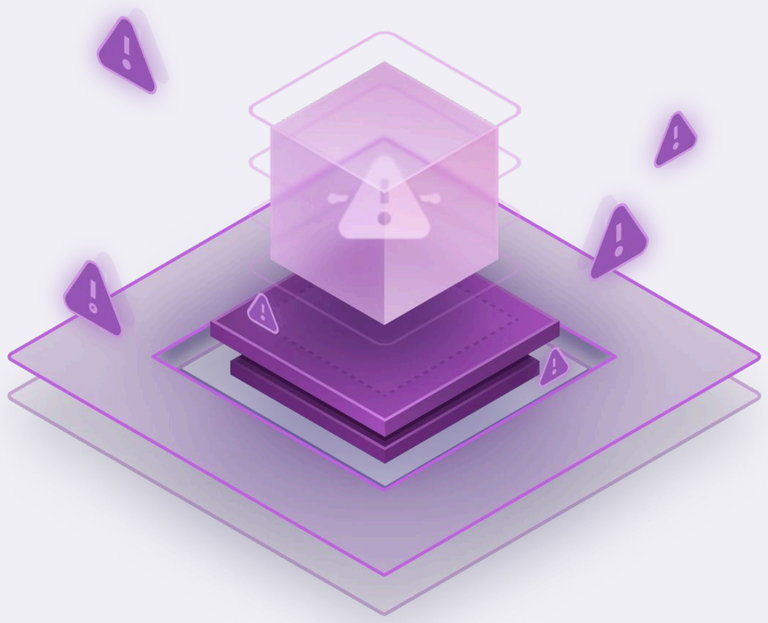
October 2025

AirMDR Managed Detection & Response (MDR) delivers full alert coverage with expert-backed, AI-led investigations. Built for lean teams, it is a cost-effective solution that delivers enterprise-grade security operations.

THE CHALLENGE

Drowning in Alerts

Lean security teams face more alerts than they can triage, coverage gaps outside business hours, and SLAs that slip. The result: stressed analysts, audit exposures, and delayed investigations when speed matters most. Traditional MDRs are costly black boxes, leaving teams waiting for answers while threats move fast.



THE SOLUTION

AI Powered MDR

Our MDR combines agentic AI speed with expert oversight to investigate every alert, fast.
This hybrid model automates triage and investigation so your team can stay focused on high-impact initiatives – with full transparency and control.

AI-Driven Triage

Virtual analyst triages 90%+ of alerts in under 5 minutes – so every alert gets examined and critical threats are identified immediately.

Expert Oversight

Human analysts provide 24x7 monitoring and oversight, validating critical threats and acting when needed.

Full Visibility

Every case includes rich context, conclusions, and next steps – ready for audits and compliance.

Comprehensive Coverage

200+ prebuilt integrations cover Endpoint, Email, Identity, Cloud, SaaS, and more.

Always Learning

The platform adapts with every case and customer feedback, getting smarter over time.

Key Outcomes

Always-on coverage
24x7 investigations with analyst review before escalation

Faster Response
Investigations complete in under 5 minutes, slashing MTTI and MTTR.

Higher Efficiency
Automate 80–90% of routine tasks so your team can focus on threat hunting and strategy.

Audit-Ready Compliance
Continuous monitoring and documented cases simplify audits and reporting.

Key Use Cases

AirMDR defends against the most common threats, while integrating seamlessly with your existing tools.

Phishing
Works with secure email gateways and platforms to detect and respond to phishing attempts in real time.

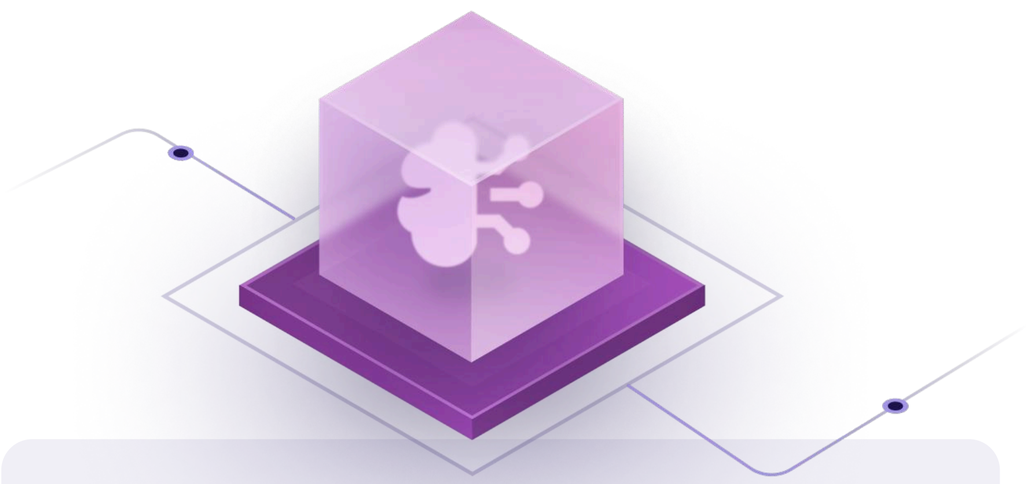
Identity
Monitors identity providers to catch credential theft, brute-force attacks, and unauthorized access.

Cloud
Tracks SaaS and public cloud environments for suspicious activity and risky misconfigurations.

Endpoint & Network
Covers alerts from EDR, XDR, NDR, and SIEM tools to deliver full-spectrum detection and response.

How it Works

AirMDR delivers the power of a world-class SOC – without the overhead. Our fully managed service combines AI-driven investigations with expert escalation and response.



Ingest & Detect — Connect sources via 200+ prebuilt integrations; identify likely threats across your stack

AI Triage & Investigation — AI Virtual Analyst enriches, investigates, risk-ranks, and writes up every case

Human Review & Escalation — Our analysts review critical cases and escalate with clear, actionable recommendations

Learn & Improve — Refines investigations using your natural-language feedback

Take Action — Remediate directly with one-click actions – or respond with full context and confidence

Get Started

Contact AirMDR now to see a demo and discuss how it fits into your environment.