

AIRMDR

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



AirMDR Agentic 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

Black Box MDR You Can't Verify

Traditional MDRs are costly black boxes – teams receive tickets and verdicts, but can't verify whether alerts were thoroughly investigated or conclusions were sound. Meanwhile, alert volumes keep growing: more tools, more noise, coverage gaps outside business hours, and SLAs that slip. The result is a service you're paying for but can't inspect.



THE SOLUTION

Agentic MDR

The AirMDR 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

Agentic AI investigates 100% of alerts, completing 95% of investigations in under five minutes – so every alert is 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 documents what happened, what evidence was reviewed, what was concluded, and what action should follow – ready for audits, escalations, 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
Higher Efficiency	Agentic AI investigates 100% of alerts, completing 95% in under five minutes – freeing your team to focus on confirmed threats and high-impact initiatives.
Faster Response	Investigations complete in under 5 minutes, slashing MTI and MTTR.
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

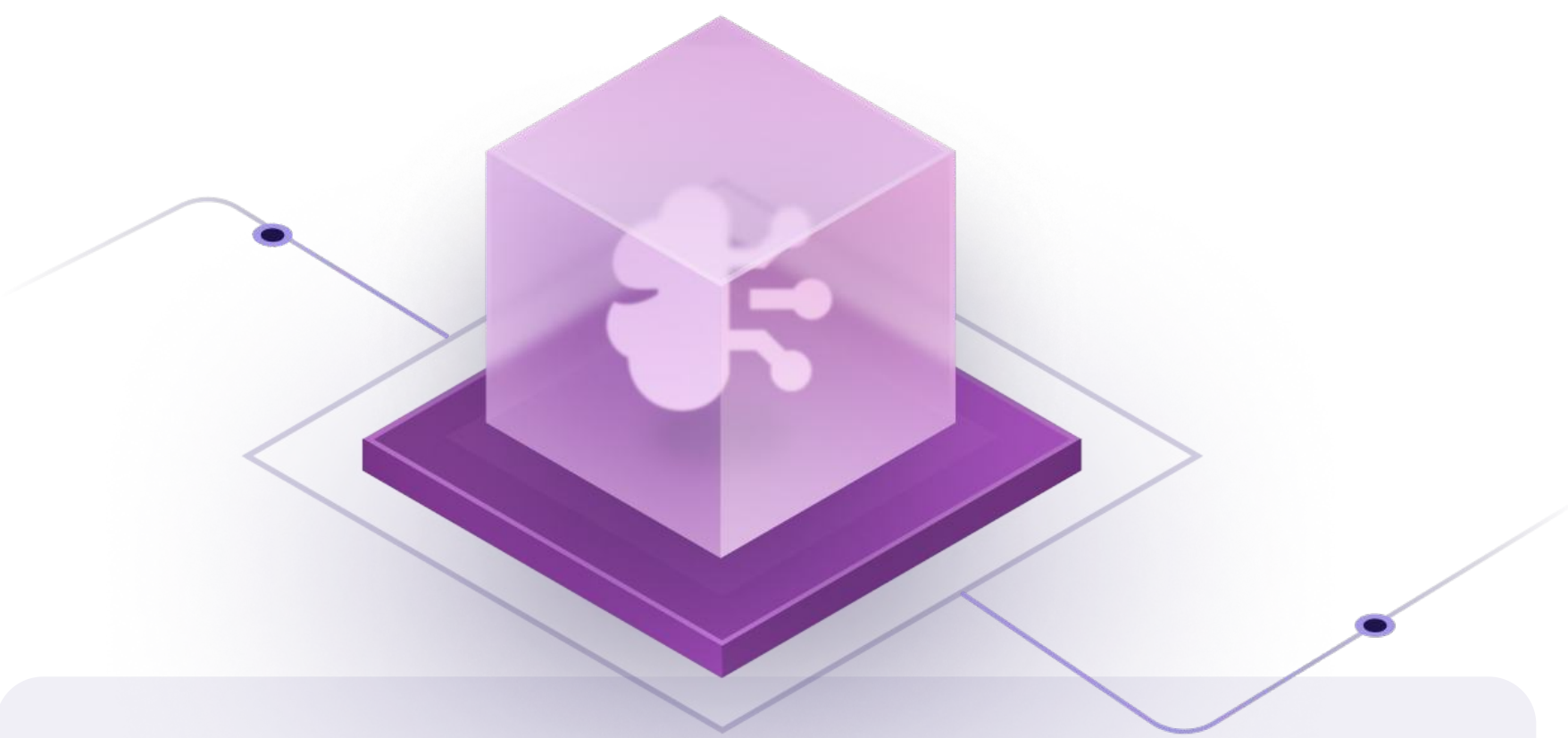
Tracks SaaS and public cloud environments for suspicious activity and risky misconfigurations.

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.



Get Started

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

Ingest & Detect

Connect sources via 200+ prebuilt integrations; identify likely threats across your stack

AI Triage & Investigation

Agentic AI enriches, investigates, risk-ranks, and documents every alert – escalating threats and low-confidence cases

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