OUR SERVICES

MDR for AI

Extending MDR across the full AI attack surface

The challenge

AI has closed the gap between exposure and impact. Attackers use it to move faster while your own employees are using AI tools everyday without oversight, creating exposure most programs can't see. And the AI systems your teams build and run carry blind spots conventional tools were never built to reach. This problem is new enough that most teams aren't sure how to tackle it—or even know whose job it is. Security, the AI builders, the data teams: everyone can see the risk, no one owns the response. The defense crawls, while attackers keep compressing the time to breach.

How we help

Expel is now extending the MDR you already trust backed by 10+ years of SOC production data and the operators who've run it to the full AI attack surface. We've taken a multi-pronged approach to protecting against AI-shaped attacks by bolstering detection coverage and creating new hunt techniques that target AI-augmented attack patterns and AI exposure.

We aren't just building AI-specific detections in a silo; we've mapped our detection coverage to MITRE ATLAS and look at AI risk through the entire attack life cycle. MDR for AI runs across 160+ integrations — endpoint, identity, cloud, SaaS, network, and more. AI detection applies across all of it, regardless of which vendor surfaced the signal. Our visibility extends to:

AI-ASSISTED ATTACKS

The threats attackers launch using AI: Think AI-enhanced phishing, AI-assisted lateral movement, and accelerated exploit development

EMPLOYEE AI ADOPTION

The risks employees introduce through AI use: Issues like shadow AI, unapproved tool usage, and sensitive data in AI systems

CUSTOMER AI SYSTEMS

The attacks targeting the AI systems you build: For attacks using things like prompt injection, agent manipulation, and non-human identity sprawl

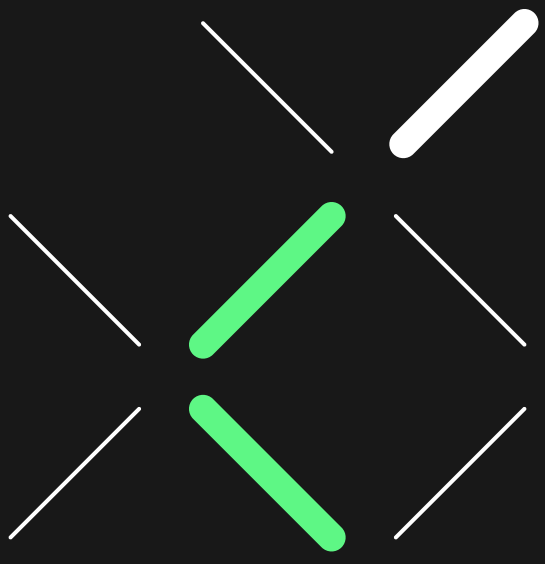
MDR FOR AI COVERAGE

Coverage across the full attack surface—from external threats to internal system exposure

Claude integration provides telemetry on usage activity, prompt content, and tool use

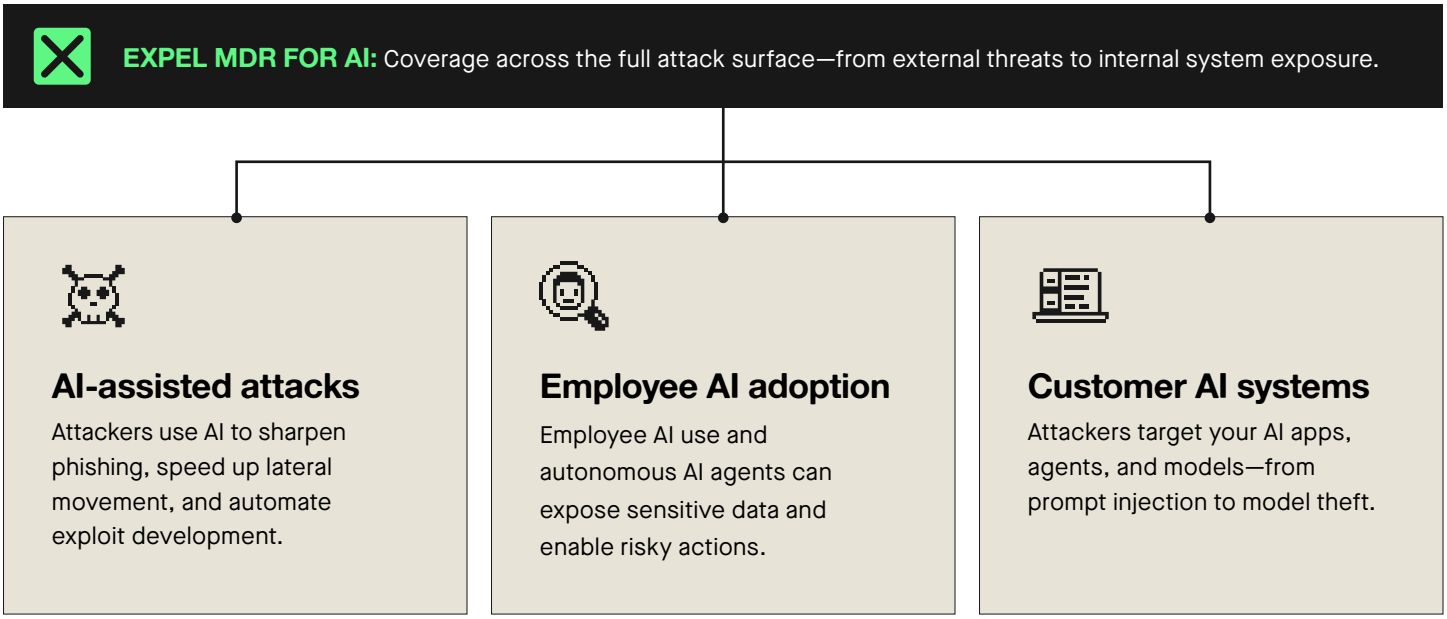
AI detections labeled and mapped to MITRE ATLAS

New AI-focused hunt techniques targeting AI-augmented attack patterns and exposure



How MDR for AI works

MDR for AI covers three dimensions of AI risk: attacker use, employee misuse of AI, and attacks on your own AI systems.



- **Claude integration.** Our first AI-native integration pulls Claude Enterprise compliance signals—usage activity, prompt content, and tool use—into our investigative pipeline. Our detections are built on the prompts themselves, so operators see intent and model responses, not just activity.
- **Detection coverage labeled and mapped.** Expel's detection library is labeled where AI is a factor, mapped to MITRE ATLAS, and is available to customers. Coverage today includes 13 of the 16 tactics.
- **AI-focused hunt techniques.** A library of structured behavioral hypothesis-based hunts built by Expel experts to target AI-augmented attack patterns and AI exposure, crafted and run by our threat hunters.
- **Expanded AI-native partner integrations, including:** coverage for prompt injection and agentic telemetry across a growing set of AI platforms, with integrations spanning model providers and AI-specific EDR and endpoint protection.
- **Ongoing detection and hunt expansion,** built to stay ahead of AI threats as they evolve, not just cover what's known today.

Why Expel

Human-led, not autonomous

Our operators investigate every signal—it's not just autonomous agents guessing at intent.

Coverage across your whole stack

AI detection runs across 160+ integrations, not just one vendor's telemetry.

Built on 10+ years of SOC data and expertise

The same production data and operators behind your MDR today, now applied to the AI attack surface.