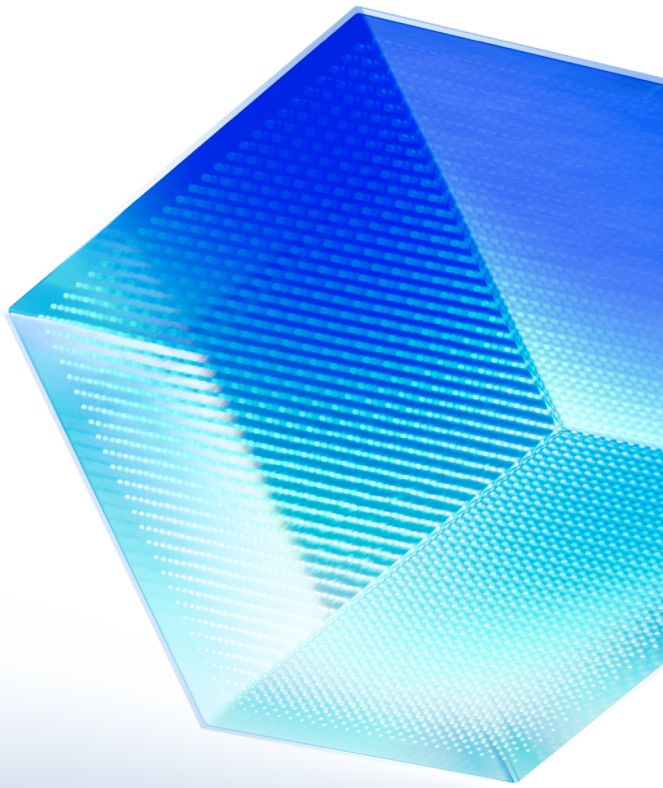
AI Detection and Response



Gain visibility and control over AI and reduce the risks of rogue and shadow AI

AI is transforming how organizations operate, but security and governance are struggling to keep pace. As employees rapidly adopt AI tools across the organization, many security teams are losing visibility into how AI is being used, what data it can access, and the risk it introduces to the environment.

Traditional cybersecurity solutions were not built for AI-driven activity, leaving organizations exposed to new challenges including:

- **Data exposure and compliance concerns**
- **Over-permissioned AI tools and integrations**
- **Expanded attack surfaces and blast radius of successful attacks**
- **AI manipulation through malicious prompts and hidden instructions**
- **Lack of visibility into rogue AI activity and behavior**
- **Shadow AI usage outside IT oversight**

CAPABILITIES

Protecting the new AI attack surface

Field Effect AI Detection and Response (AIDR) helps organizations securely adopt AI by providing visibility into AI usage, enforce control, and support stronger AI governance across the environment.

01 — DISCOVER

Uncover shadow AI

Shining a light on AI tools being used across the organization — including unsanctioned or unknown applications — to reduce blind spots and bring shadow AI activity into view.

02 — GOVERN

Mature and enforce AI Governance & Policy Control

Visibility into AI tools gives organizations the insight needed to govern AI with confidence. By understanding which tools are being used and by whom, organizations can establish and enforce guardrails to reduce risk, eliminate shadow AI, and maintain control over AI adoption.

03 — ADOPT SAFELY

Ensure safe AI adoption

Monitor employee adoption of new AI tools, giving security teams the visibility needed to support secure, responsible AI adoption and maintain oversight across the organization.

> **"Field Effect AIDR gives us real visibility into how AI is being adopted across the environment, so we can make sure innovation stays aligned with our governance and security standards."**
>
> Rob Schenk — Chief Strategy Officer, Intelligent Technical Solutions

AT A GLANCE

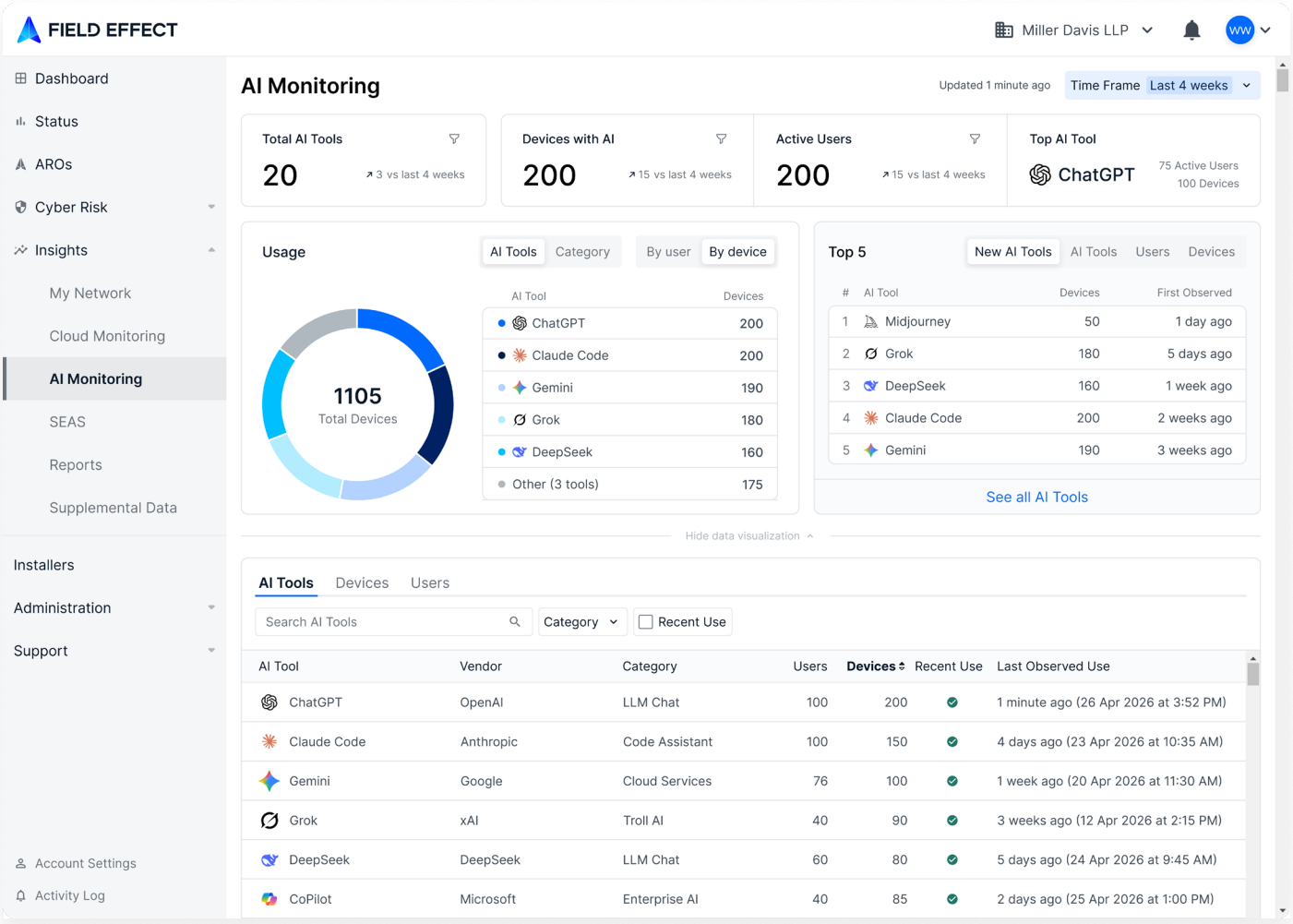
Field Effect's AI Detection and Response at a glance

Field Effect's AI Detection and Response (AIDR) provides organizations with visibility into AI tools and activity across their environment, helping security teams:

Uncover where AI is being used and who's using it

Understand where AI is creating risk across your environment

Enforce guardrails and take back control



ROADMAP

The future of AIDR

1

AI Awareness AVAILABLE NOW

Discover AI tools in use, who is using them, and what tools they're connecting to, and understand the holistic AI activity across the environment.

2

AI Usage Control AVAILABLE NOW

Establish governance by controlling which AI applications and services can be used across the organization.

3

AI Impact Visibility

Understand what AI tools are actually doing and how they're impacting the environment to spot malicious and potentially rogue AI use.

4

AI impact Control

Apply zero-trust principles to AI-driven activity with deeper enforcement and control over what AI tools can do.

See AIDR in your environment

Premium protection should not require a bigger team.
Get a guided walkthrough of AI Detection and Response.

Get a demo →