







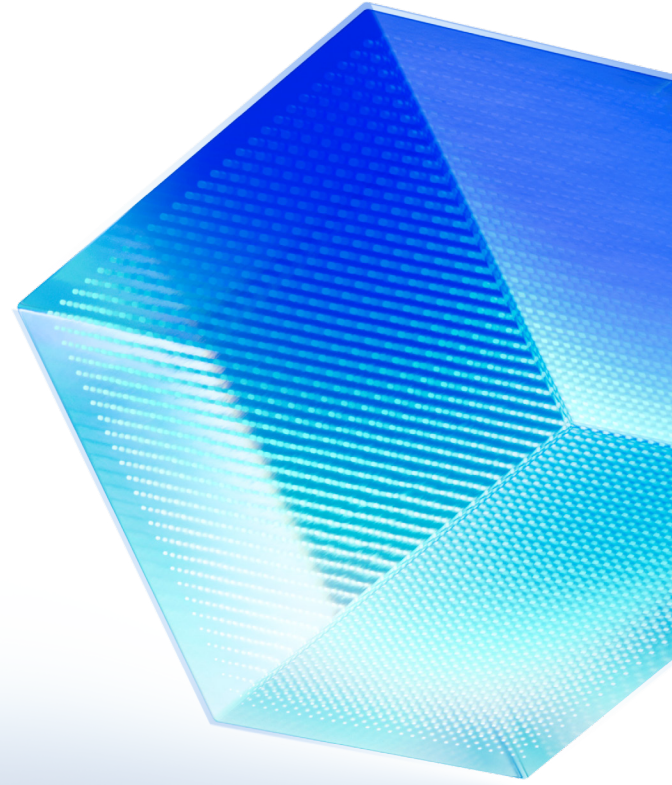
AI Detection and Response

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

FIELD EFFECT
Miller Davis LLP
ww

- Dashboard
- Status
- AROs
- Cyber Risk
- Insights
- My Network
- Cloud Monitoring
- AI Monitoring
- SEAS
- Reports
- Supplemental Data
- Installers
- Administration
- Support
- Account Settings
- Activity Log

AI Monitoring

Updated 1 minute ago Time Frame Last 4 weeks

Total AI Tools

20

▲ 3 vs last 4 weeks

Devices with AI

200

▲ 15 vs last 4 weeks

Active Users

200

▲ 15 vs last 4 weeks

Top AI Tool

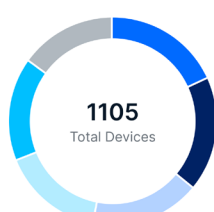
ChatGPT

75 Active Users
100 Devices

Usage

1105

Total Devices



AI Tools Category By user By device

AI Tool	Devices
ChatGPT	200
Claude Code	200
Gemini	190
Grok	180
DeepSeek	160
Other (3 tools)	175

Top 5

#	AI Tool	Devices	First Observed
1	Midjourney	50	1 day ago
2	Grok	180	5 days ago
3	DeepSeek	160	1 week ago
4	Claude Code	200	2 weeks ago
5	Gemini	190	3 weeks ago

[See all AI Tools](#)

Hide data visualization

AI Tools
Devices
Users

Category
 Recent Use

AI Tool	Vendor	Category	Users	Devices	Recent Use	Last Observed Use
ChatGPT	OpenAI	LLM Chat	100	200	✓	1 minute ago (26 Apr 2026 at 3:52 PM)
Claude Code	Anthropic	Code Assistant	100	150	✓	4 days ago (23 Apr 2026 at 10:35 AM)
Gemini	Google	Cloud Services	76	100	✓	1 week ago (20 Apr 2026 at 11:30 AM)
Grok	xAI	Troll AI	40	90	✓	3 weeks ago (12 Apr 2026 at 2:15 PM)
DeepSeek	DeepSeek	LLM Chat	60	80	✓	5 days ago (24 Apr 2026 at 9:45 AM)
CoPilot	Microsoft	Enterprise AI	40	85	✓	2 days ago (25 Apr 2026 at 1:00 PM)

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 →](#)