USE CASE

Find the AI already running, then govern it

Aribot finds the AI already running in your code and cloud, then puts every agent under least-privilege access with a record your auditors can check.

THE PROBLEM

Dozens of teams are building on language models.

The new AI governance board has a policy but no inventory: nobody knows which models the code calls, which agents hold credentials, or what they did.

WHY IT MATTERS NOW

82%

of organisations discovered shadow AI agents in the past year; 65% had an AI-agent-caused security incident in 12 months

Source: CSA & Token Security, Apr 2026

HOW ARIBOT HANDLES IT

1 **Discover Shadow AI**

Read the code for AI SDK calls and the endpoints they reach.

2 **Inventory the agents**

List every agent that holds a credential, registered or not.

3 **Right-size access**

Compare granted scopes with used scopes and remove what is never used.

4 **Report in currency**

Show the board AI exposure and AI cost from the same data.

WHAT YOU GET

- An inventory of AI call sites and agents
- Least-privilege access with refusals recorded
- AI cost visible by feature and caller
- Mapping to the EU AI Act and ISO/IEC 42001

SEE IT IN THE DEMO

- Agent Assurance: the agent inventory
- Authority That Matches Use: held versus used
- Economic Intelligence: AI spend guards

See it for yourself

ayurak.com/demos/agent-assurance

€40 per Shadow AI scan · licence for agent governance