
USE CASE

Let AI assistants call Aribot through one governed gateway

Point any MCP client at the Aribot server, and its calls pass through the same gateway and permission checks as every other agent action, with write calls metered.

THE PROBLEM

Connecting an AI assistant to internal systems usually means a new integration with its own permissions that nobody reviews.

Security asks what the assistant could do on a bad day, and we can't answer. The cost shows up at month end with nothing to say where it came from.

WHY IT MATTERS NOW

56%

of US IT executives at \$1B+ companies name IT security as their top concern about agentic AI, ahead of cost at 37%

Source: UiPath Agentic AI Report 2025

HOW ARIBOT HANDLES IT

1 **Add the server**

Enter the MCP server URL in your AI client.

2 **List capabilities**

The client sees each capability with its kind: read, write or govern.

3 **Call a capability**

Calls such as generating a threat model or running a code scan are served, and write calls are metered.

4 **Route changes to approval**

A govern-kind call, such as applying a remediation, is sent for approval and changes nothing.

WHAT YOU GET

- AI assistants and coding agents that call threat modeling, code review and compliance scans directly
- The same licence, permission and tenant checks as the app on every call
- Govern-kind calls held for approval
- Write calls metered as they happen

SEE IT IN THE DEMO

- A capability list that includes generating a threat model, running a code security scan, planning a remediation as a dry run and applying a remediation under governance
- Call results labelled SERVED, SERVED · METERED and AWAITING APPROVAL
- Counters for capabilities exposed, read-only, needs approval and calls this session
- A message stream between sample security agents

See it for yourself

ayurak.com/demos/mcp

Same per-action prices as the app; reads free