
USE CASE

Cut machine access down to what is used

Aribot shows what each agent or machine identity holds beside what it has used, so access reviews rest on evidence and unused access can be removed.

THE PROBLEM

Service accounts and agents get broad access to start a task, and the grant outlives the task.

In the access review nobody can tell whether a permission is still needed, so the safe answer is always to keep it. Nothing ever gets removed.

WHY IT MATTERS NOW

97%

of organisations that reported an AI-related breach
lacked proper AI access controls

Source: IBM Cost of a Data Breach 2025

HOW ARIBOT HANDLES IT

1 **Point at your identities**

Tell Aribot where access is held, and it builds an inventory.

2 **See held against used**

Each identity shows its granted access beside the access it has exercised, with unused scopes named.

3 **Rehearse a reduction**

Test proposed limits against recent activity to see what would break before you apply them.

4 **Evidence the review**

Export a record of who decided what, and when.

WHAT YOU GET

- A named list of unused scopes for each identity
- A rehearsal of every reduction before it is enforced
- Access reviews that can run all year
- A record of who approved each change

SEE IT IN THE DEMO

- A page marked Research Preview that covers the problem and the outcome
- A flow from identity inventory to a list of reducible access
- A rehearsal step showing which actions a proposed limit would refuse
- An Authority that matches use card describing the observable result

See it for yourself

ayurak.com/demos/innovation/authority-in-use

€40 per Shadow AI scan · licence for agent governance