

USE CASE

Fix cloud findings in bulk behind an approval gate

Aribot turns routine cloud fixes into dry runs behind policy gates, and a finding closes only when the cloud confirms the change.

THE PROBLEM

We have a backlog of cloud findings with obvious fixes, and nobody has time to write each change. The one time we automated it, the tool reported success on dispatch and a failed fix looked the same as a real one. No one will give a system write access to production without an approval step and a way back.

HOW ARIBOT HANDLES IT

- 1 **Group findings by fix**
Findings that share a remediation are grouped, so one review covers many resources.
- 2 **Generate a dry run**
The exact change is shown with the resources and parameters it touches, and nothing is applied.
- 3 **Let the gates rule**
Policy, scope and change-window gates evaluate the proposal, and a gate that cannot run holds the change.
- 4 **Approve and apply**
A rollback checkpoint is taken first, then the change is applied to the named resources only.
- 5 **Verify, then close**
The resource is re-read from the cloud, and only a confirmed match closes the finding.

WHAT YOU SEE IN THE DEMO

- A proposed change shown as a diff on storage public-access settings
- A Safety gates panel that includes a change-window gate
- Gate results labelled PASS, BLOCKED · SAVE, PENDING and SKIPPED
- A ledger entry marked CONFIRMED after the re-check

WHO IT IS FOR

- Head of Cloud Security
- Cloud Security Engineer
- SRE / Platform Lead
- Head of Platform Engineering

WHAT YOU GET

- A dry run you can review for every fix before anything changes
- Gate refusals recorded with their reason and counted as saves
- A rollback point taken before each change
- Findings closed on a re-read of the resource

95%

of security teams report a skills gap;
59% call it critical or significant

Source: ISC2 Workforce Study 2025

See it: ayurak.com/demos/self-healing

€30 per scan · €30 per applied fix (dry runs free)