

USE CASE

A posture score that shows which accounts it covers

Scan results across connected accounts, where the headline score states how many accounts it was computed over and unscanned accounts stay on the list.

THE PROBLEM

Our posture score is one number for the whole estate, and everyone assumes the whole estate was read. An account that refused access contributes nothing and drops out of the report. When the score moves, we can't tell whether posture changed or coverage did.

HOW ARIBOT HANDLES IT

- 1 **Start the scan**
Choose the connected accounts to put in scope.
- 2 **Read each account**
Live resources are checked against security standards, account by account.
- 3 **Flag what was refused**
An account that could not be read is marked NOT SCANNED and kept on the list.
- 4 **Score with coverage**
The score is computed only from what was read and shown beside an account-coverage figure.

WHAT YOU SEE IN THE DEMO

- Account rows marked SCANNED or NOT SCANNED
- Counters for accounts scanned, resources read, checks passed and checks failed
- An overall posture panel with checks passing beside account coverage
- A live activity list of findings such as a public endpoint exposed without authentication

WHO IT IS FOR

Head of Cloud Security

Cloud Security Engineer

CISO

WHAT YOU GET

- A score that states its basis
- Unscanned accounts kept in view
- Coverage reported as its own figure, so month-on-month changes can be explained
- Checks passed and failed for each account and each provider

PCI DSS 4.0.1 · 31 Mar 2025

Requirements that became mandatory include authenticated internal scanning, so you need to show which accounts a scan actually read.

See it: ayurak.com/demos/scan-results

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