

USE CASE

An audit trail the auditor can verify

Every live remediation is written to an append-only ledger, hash-chained and signed, and anyone with access can verify the chain on demand.

THE PROBLEM

Logs can be edited, and 'immutable' is usually a claim nobody can test. After an incident we need to know exactly what changed and when, and whether the record itself can be trusted. A false tamper alarm on a routine dry run would wreck confidence in every alarm after it.

HOW ARIBOT HANDLES IT

- 1 Seal each change**
Each approved, applied change appends an entry sealed to the one before it.
- 2 Grow the chain**
Each further change adds another sealed entry.
- 3 Verify on demand**
A reviewer checks the full ledger for linkage, content integrity and signature.
- 4 Read the result plainly**
The result names how many entries carry a seal, and an entry that never claimed one is labelled that way.

WHAT YOU SEE IN THE DEMO

- A heal ledger with entries labelled SEALED or NO SEAL CLAIMED
- A verification panel showing whether the chain verified and whether tampering was detected
- A ledger that starts empty and grows as fixes are applied
- A plain statement that the ledger is tamper-evident, a property you can check

WHO IT IS FOR

Internal Audit IT Manager

Head of GRC

CISO

WHAT YOU GET

- A tamper-evident record of every live remediation
- Verification you can run yourself, whenever you need it
- Labels that tell an unsealed entry apart from tampering
- Evidence that feeds audit readiness in Ayurak Trust

DORA (EU financial sector) · 17 Jan 2025
Incident reporting and ICT risk management call for a change record you can stand behind.

See it: ayurak.com/demos/ledger-integrity

€75 per compliance scan · €120 per vendor assessment · Trust licence