BEACON

Verifiable AI Governance for the Agent Era

v2.5 · Small edition · Apache 2.0 · No SaaS lock-in

YES-Ship AI · YES-Steady AI · YES-Recover AI

github.com/bobrapp/aigovops-beacon aigovopsfoundation.org live demo

Your company runs on AI.
So does your risk.

Shadow models — Teams ship LLM features your governance team has never seen.

Unlogged prompts — Inputs vanish. Outputs go unverified. Receipts do not exist.

Frameworks proliferate — NIST AI RMF, EU AI Act, ISO 42001, HIPAA — 23 and counting.

Auditors arrive — Questions you cannot answer. Evidence you cannot reproduce.

Trust is not a feature you bolt on.

Trust is the substrate.

Every decision an agent makes should be signed, replayable, and verifiable — by anyone, forever.

Meet Beacon.

An open-source MCP server that turns every AI decision into a signed, verifiable receipt.

SIGNED

Ed25519

Every decision sealed cryptographically. Tamper-evident. Replayable forever.

SCORED

23 Frameworks

NIST AI RMF, EU AI Act, ISO 42001, HIPAA — auto-mapped from receipts.

SHIPPABLE

Apache 2.0

Three deployment shapes. One repo. No SaaS lock-in. No vendor capture.

Six tools. One protocol.

Beacon ships as a Model Context Protocol server. Any MCP-capable agent gets governance for free.

`record_decision`

Sign a decision. Returns a receipt.

`verify_receipt`

Re-validate any receipt against its signature.

`query_inventory`

Search every model, decision, and dataset on file.

`score_framework`

Score posture against NIST, EU AI Act, ISO 42001, HIPAA.

`bundle_for_auditor`

Sealed evidence pack. Hand it to anyone. They verify it themselves.

`replay_case`

Reconstruct any decision end to end, with full provenance.

Browse the MCP server code: github.com/bobrapp/aigovops-beacon/tree/main/mcp-public

Three shapes. One repo.

Pick the deployment that fits your trust model. Switch when it changes.

1

Local desktop client

Runs on a workstation. Owned data, owned keys.

Trust: Your team only

View code →

2

Hosted MCP server

Render-deployable. Share across an enterprise.

Trust: Authenticated callers

View code →

3

Restricted public agent

Cloudflare Worker. BYO key. Read-only safe ops.

Trust: Anyone with a key

View code →

Use it in the real world.

Concrete patterns Beacon was built to handle.

Internal copilots

Sign every prompt and response. Replay any conversation when legal asks for it.

Customer-facing agents

Bundle receipts per session. Hand them to regulators on demand, without delay.

Multi-agent workflows

Log routing decisions across agents. Detect drift between runs, before users do.

High-stakes automation

Lending, healthcare, hiring — every decision auditable, verifiable, replayable.

Model inventory

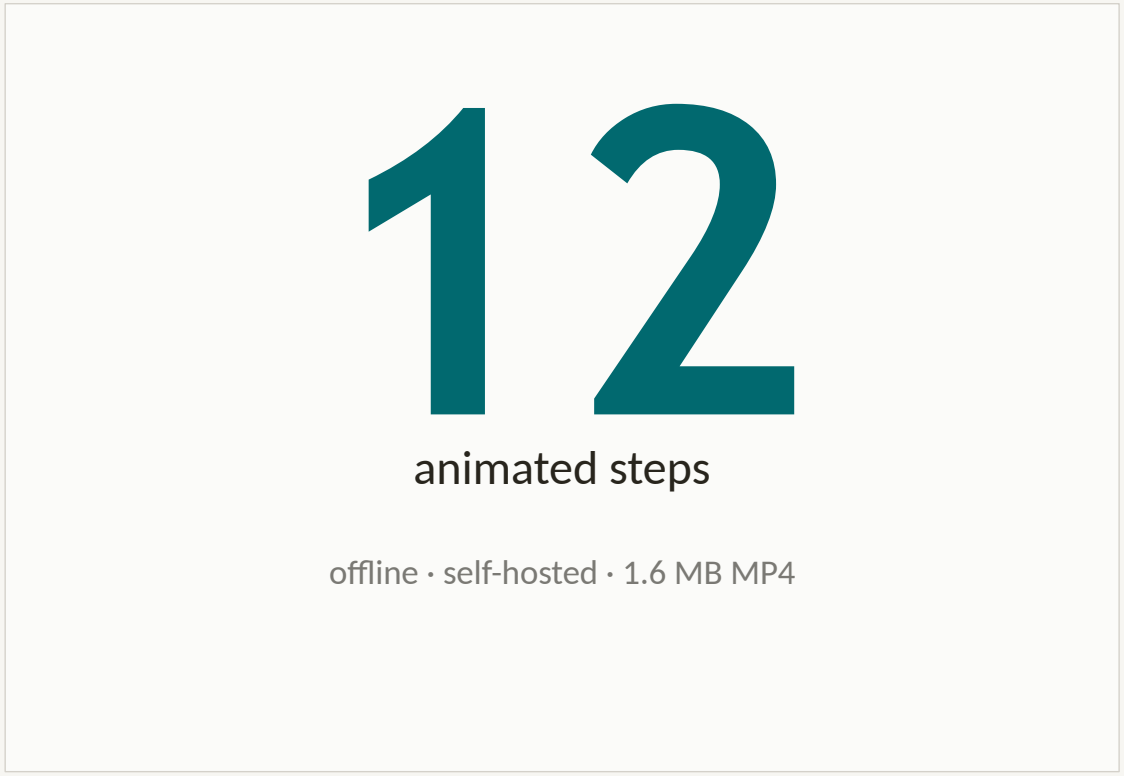
Track every model in production, with provenance, owners, and a live risk class.

Audit prep

Hand the auditor a bundle they can verify themselves. No portal logins required.

See the whole loop in 70 seconds.

Twelve animated steps. Decisions in. Receipts out. Auditor bundle, sealed and signed.



01 Agent emits a decision
02 Beacon receives the payload
03 Ed25519 signature applied
04 Receipt stored, indexed, replayable
05 Framework mapping auto-scored
06 Inventory updated, owners notified
07 Verification on demand by anyone
08 Bundle prepared for the auditor
09 Bundle handed off, sealed
10 Auditor verifies it themselves
11 Case replayable end to end
12 Trust, on the substrate

See it live: bobrapp.github.io/aigovops-beacon/walkthrough/

Hosted MCP + restricted public agent.

Two new deployment paths shipped in v2.3. Both verified live.

HOSTED MCP

mcp-public/

Deploy to Render in one click. Shareable across your enterprise. All six tools, signed receipts, auditor bundles — over HTTPS.

- Apache 2.0
- Render-ready manifests
- Auth-gated MCP endpoints
- Same six tools as the local client

RESTRICTED PUBLIC AGENT

agent/

Cloudflare Worker. BYO key. Restricted to safe, read-only operations. Run a public-facing Beacon agent at your own edge — no surprises.

- Cloudflare Worker template
- Bring-your-own API key
- Allow-listed tool surface
- Verifiable receipts, public traffic

The layer that lets a $1M super-agent actually ship.

Big budgets buy capability.

Beacon supplies the trust they cannot ship without.

Read the brief: **SUPERAGENT.md**

23 frameworks built in. Yours plugs right in.

Run score_framework. Get a posture report per framework, with the receipts that backed every claim.

NIST AI RMF	EU AI Act	ISO/IEC 42001	ISO/IEC 23894	HIPAA	GDPR Art. 22/35
SOC 2 TSC	AIDA (Canada)	OECD AI Principles	IEEE 7000-2021	Brazil PL 2338	Korea AI Basic Act
NYC LL 144	Colorado SB24-205	California SB-53	Texas TRAIGA	UK AI WP	UN GA A/78/L.49
Singapore GenAI	Australia VAISS	China Interim	India DPDP	US AI Bill of Rights	**+ your own (YAML)**

Browse all 23: github.com/bobrapp/aigovops-beacon/tree/main/frameworks

Run it today.

Three commands. One repo. Apache 2.0.

```
$  git clone https://github.com/bobrapp/aigovops-beacon
$  cd aigovops-beacon
$  ./demo.sh                                  # local desktop, port 8801

$  cd mcp-public && ./deploy-render.sh        # hosted MCP server
$  cd agent && wrangler deploy                # restricted public agent
```

DEMOS.md	Three deployment shapes, end to end, in under five minutes.
SUPERAGENT.md	How Beacon lets a $1M super-agent actually ship.
walkthrough/	Twelve animated steps. Decisions in. Receipts out.

Code is on GitHub. Community is at the Foundation.

Both are open. Both are waiting.

THE CODE

aigovops-beacon

Apache 2.0. Six MCP tools. Three deployment shapes. Walkthrough included.

github.com/bobrapp/aigovops-beacon

Star · Fork · Run · Contribute

THE COMMUNITY

AI GovOps Foundation

Where practitioners share frameworks, case studies, and reference implementations — open governance, open practice.

aigovopsfoundation.org

Join · Contribute · Lead a working group

Hand the auditor a bundle.

Let the tokens flow.

Beacon. Verifiable AI governance. Available now.

→ **github.com/bobrapp/aigovops-beacon**

→ **aigovopsfoundation.org**

→ **aigovops-fact-check.md** — every claim in the repo, classified and sourced.