SecuriX

Enterprise AI gateway

AI governance, made auditable.

How SecuriX turns NIST AI RMF and ISO/IEC 42001 from policy documents into controls you can enforce and evidence.

Catalyst Ops Private Limited
Incubated at IIT Madras Incubation Cell

securix.app

Why SecuriX

AI adoption is already happening. Governance is not.

01

Policy on paper

AI policies exist, but nothing stops a prompt with customer data or an agent with excess access.

02

Usage is invisible

Shadow AI, embedded copilots and agents spread across teams with no single inventory.

03

Evidence is manual

Audit and risk teams assemble screenshots and spreadsheets to show controls actually work.

Enterprises need to adopt AI without giving up security, compliance, budget or operational control.

The control layer

Four pillars. One gateway.

01 Data security and compliance

Protect sensitive information before it reaches AI providers. Redact PII and keep an auditable trail.

02 Agentic data governance

Govern agents and MCP-connected tools with granular policies on what they can see, fetch and execute.

03 Budget and cost control

Centralize AI access, move to transparent consumption and set hard limits by team or department.

04 Operational governance

SSO, model allowlists and observability give IT a single governance layer.

Architecture

One control layer between people, agents and AI.

Employees and applications

Chat · copilots · developer tools · business applications

SecuriX AI gateway

Identity · DLP · policy · routing · budget · audit · MCP governance

AI and enterprise systems

LLMs · AI providers · MCP servers · enterprise data and tools

Nothing is ripped out. Employees keep their familiar tools.

Pillars 01 and 02

Stop data leaks. Govern every agent action.

01

Data security and compliance

- PII shield redacts sensitive data before it reaches models
- Zero-trust policies enforced at the gateway
- Controls on outbound prompts and inbound responses
- Traceable records for internal and external reviews

02

Agentic data governance

- Native MCP connectivity for enterprise agent workflows
- Granular limits on what an agent can see, fetch and execute
- Tool invocation and data access controlled at the action layer
- Activity attributed to users, agents, models and tools

Pillars 03 and 04

Cap spend. Standardize access.

03

Budget and cost control

- Consumption-based visibility instead of fragmented seat costs
- Hard budget caps at team or department level
- One dashboard for AI usage and budget use
- Protection against runaway usage

04

Operational governance

- SSO for verified employee access
- Model allowlists based on corporate security standards
- Centralized observability across AI activity
- A familiar employee experience with governed access

NIST AI RMF

Supporting all four functions of the AI RMF.

Govern

Policy and accountability

Central policy engine, SSO and role-based access define who may use which AI, and for what.

Map

Context and risk

Surfaces agents and MCP tools; inventories users, models and data flows.

Measure

Assess and track

Logs prompts, tool calls and policy hits; tracks PII/PHI detections, usage and spend.

Manage

Prioritize and respond

Redacts or blocks risky data, limits agent actions, caps spend, and keeps incident-ready records.

SecuriX provides the runtime controls and evidence; your risk team owns the assessments and decisions.

ISO/IEC 42001

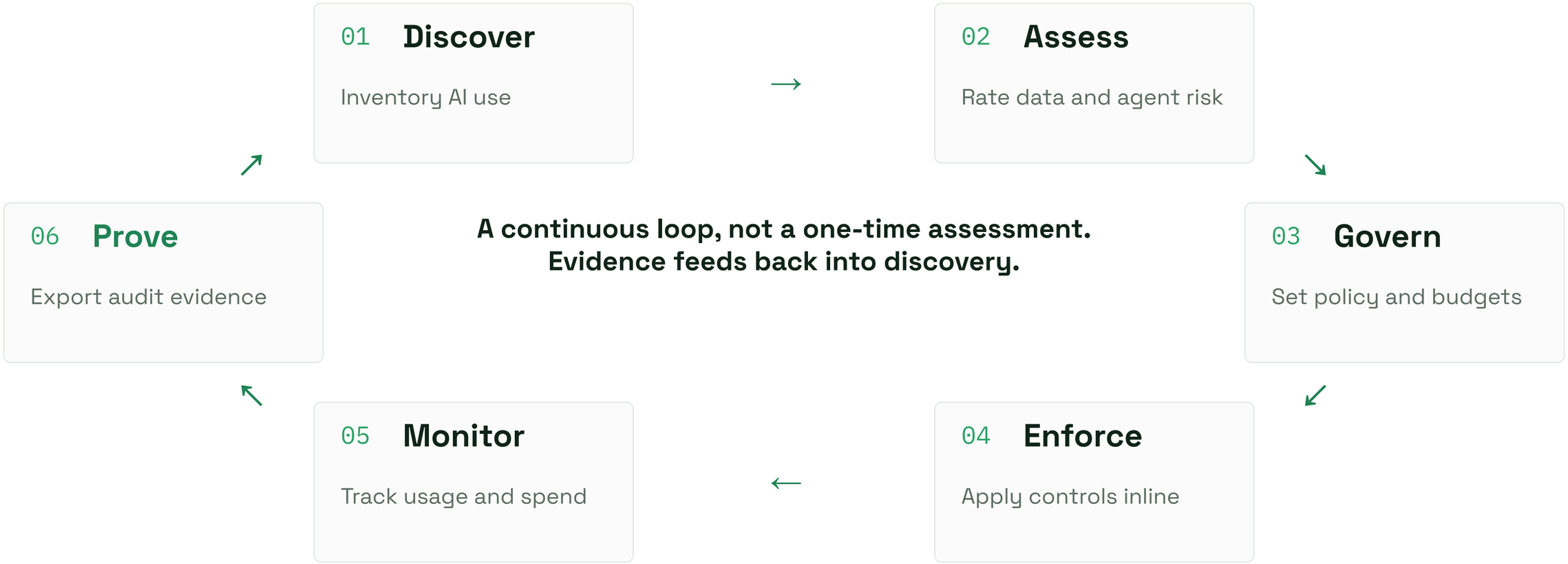
Evidence for the AI management system, built in.

Clause 5 · Leadership and policy	Enforceable AI usage policy applied at the gateway, not only written down.
Clause 6 · Risk and impact	Inputs for your risk register: PII/PHI exposure, agent permissions, provider risk.
Clause 8 · Operational controls	Runtime guardrails: allowlists, redaction, tool-call permissions and spend caps.
Annex A · Data and third parties	Data shielded before it leaves; per-provider routing, visibility and control.
Clauses 9-10 · Monitoring and improvement	Central logs and dashboards, with exportable evidence for internal audit and reviews.

SecuriX supports alignment and audit evidence. Certification is issued by accredited auditors.

Operating model

Govern AI from request to outcome.



Enterprise use cases

Designed for regulated, data-intensive organizations.

BFSI / NBFC

Protect financial and customer data; govern underwriting, collections and service agents.

Insurance

Govern claims, underwriting and service AI handling sensitive policyholder records.

Healthcare

Control access to patient and clinical information across AI assistants and agents.

BPO / shared services

Govern employee AI use, prevent data leakage and control spend by team.

Manufacturing

Secure operational data and govern agents connected to enterprise tools.

Enterprise IT

One policy and audit layer across providers, applications and developer agents.

GDPR | HIPAA | ABDM | CDSCO | RBI | DPDPA

Deployment

Fits the environment you already run.

01

For employees

Familiar AI experiences, with nothing ripped out.

02

For IT

One policy, audit and budget layer across every provider.

03

For leadership

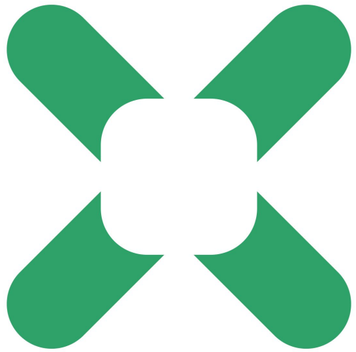
Evidence on demand and spend under control.

Security, policy and cost enforcement run in the background, so adoption does not slow down.

SecuriX

Next steps

Ready to govern AI responsibly?



Start with a focused pilot and expand the control layer across enterprise AI.

01

Framework gap workshop

02

Scoped pilot on one AI workflow

03

Evidence pack for your controls