Poligovern

Open-source library for AI governance infrastructure.

The Problem.

Enterprises are adopting AI at scale. Governance is the bottleneck.

- No audit trail — who used what model, with what data?
- No cost control — per-team budgets, anomaly detection, attribution
- PII/PHI sent to external LLMs with no redaction
- Prompts in plaintext in Git — no encryption or access control
- No alternative to public LLMs — shadow usage, no visibility

Current SaaS tools: data leaves your VPC, vendor lock-in, closed source, per-token markup, long procurement.

Gap: Security wants auditable code. Engineering wants flexibility. Finance wants cost clarity. No solution gives all three.

The Solution.

Poligovern - Open-source AI governance library. An infrastructure and not a service.

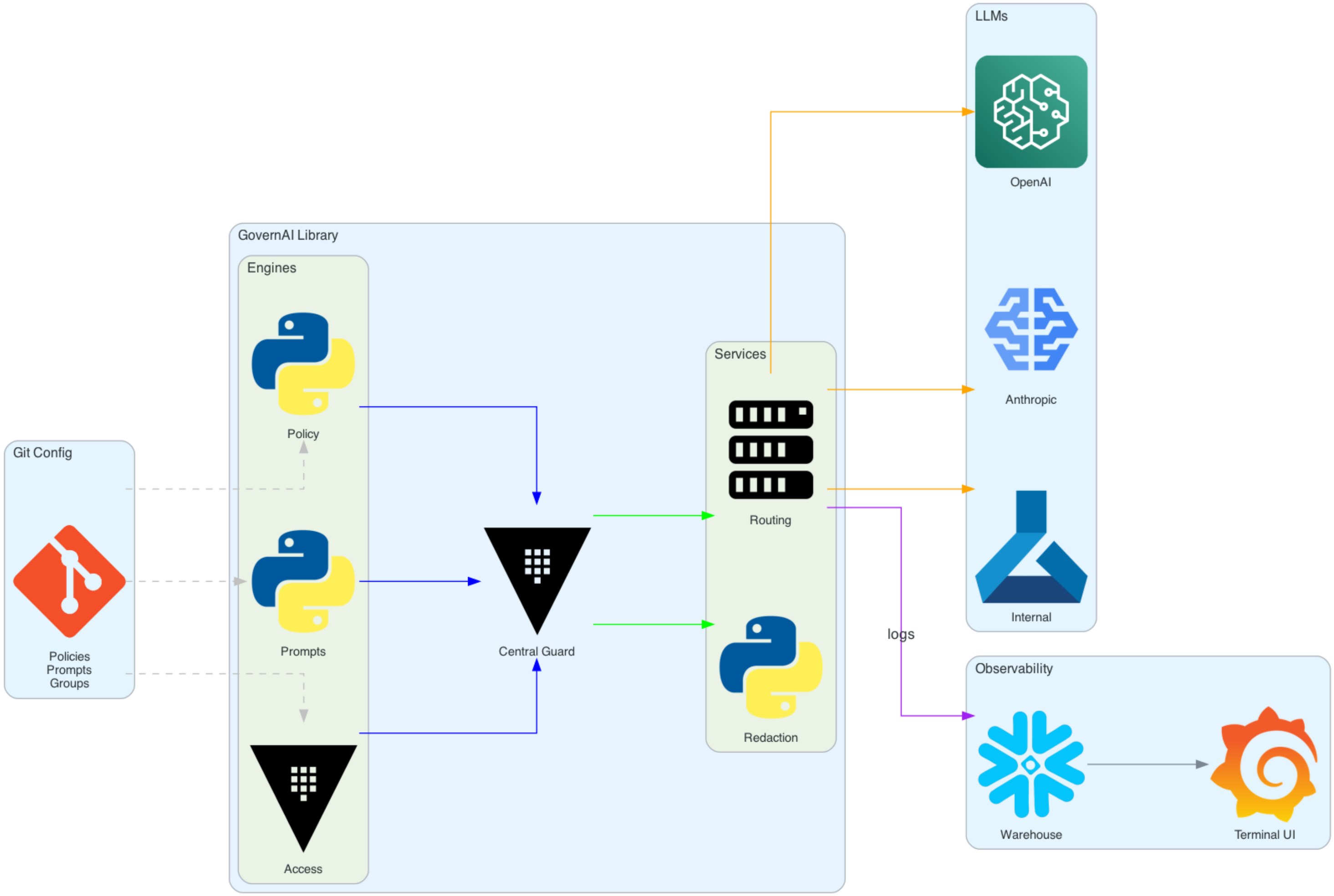
- Policy as code — Git-controlled rules, budgets, model access
- PII/PHI redaction — tokenize before LLM, reconstruct on response
- Centralized audit — all requests logged to your warehouse
- Cost control — per user/team/agent token tracking and limits
- Prompt library — encrypted, versioned, access-controlled

Like dbt, but for AI governance. Infrastructure, not a service.

How it works?

Request flow: Authenticate → Policy check → Redact PII → Route to LLM → Reconstruct → Log to warehouse → Return to user.

- Library — pip install poligovern
- Keys in your secrets manager, injected at runtime
- Policies as YAML in Git (environments, enforcement modes)
- Logs in your warehouse (Snowflake/BigQuery) with RLS


LLMs
OpenAI
Anthropic
Internal
GovernAI Library
Engines
Policy
Prompts
Access
Central Guard
Services
Routing
Redaction
Git Config
Policies
Prompts
Groups
logs
Observability
Warehouse
Terminal UI

Why now?

- Every large enterprise has AI initiatives; governance lags
- EU AI Act, GDPR, HIPAA push for audit trails and data protection
- First-gen SaaS gateways: closed source, data leaves VPC, lock-in

Pattern: Terraform, dbt, Kong — infrastructure moved from SaaS to open source.

AI governance is next.

Market.

- TAM: Enterprises adopting LLMs (Fortune 500, mid-market)
- Target: Platform teams, security/compliance, engineering at scale
- No dominant open-source governance solution yet

Comparison.

	SaaS	Poligovern
Deployment	Vendor proxy	Library in your infra
Data	Leaves VPC	Stays in your VPC
Code	Closed	Open source
Integration	Vendor onboarding	pip install
Pricing	Per-token markup	No markup
Audit logs	Vendor DB	Your warehouse
Lock-in	High	None

Business Model.

	Free	Paid ($50K/year)
Core	Library, policy, redaction, routing	Multi-tenant
Features	Warehouse logging	Advanced redaction, SSO/SAML
Support	Community	Priority support, SLAs
Compliance	—	Reporting (SOC2, HIPAA, GDPR)

Go-to-Market

Phase	Focus	Target
1 (0–6 mo)	Open-source launch, docs, integrations	Git Hub1,000 stars, 50 companies evaluating
2 (6–12 mo)	Design partners, case studies, enterprise tier	10 paying customers
3 (Year 2)	Managed option, marketplace, partners	100+ enterprises

The Ask - $1.5M Pre-seed

Engineering 70%

- Build in phases: policy + secrets → redaction + routing → RBAC + quotas → portal + SSO.
- Ship v1.0 in 12 months.

GTM 20% - Integrations, docs, community

Ops 10% - Legal, infra, hiring

12-month milestone

- v0.5 (6 mo): Redaction, prompts, warehouse logging
- v1.0 (12 mo): Full library + UI
- 20+ pilots, $100K ARR

Thanks!

Kiran Kannan | Agash Uthayasuriyan | Dharun Karthick Ramaraj

Contact: startupadk@gmail.com