PolicyCortex — Value Proposition

Generated automatically from current understanding of the application's capabilities.

Core value proposition

A single, AI-driven control plane that unifies cloud cost, security access (RBAC/IAM), compliance, and operations into one actionable workflow layer. It doesn't just visualize risk and spend; it correlates, prioritizes, and turns findings into guided fixes (JIT, SoD, de-provision, policy remediations) with measurable savings and risk reduction.

Why companies care

- **Cost:** Cut cloud spend 8–15% via anomaly detection and optimization guidance.
- **Risk:** Reduce breach and audit exposure with least-privilege, SoD checks, and continuous controls.
- **Speed:** Shorter MTTR and faster approvals through AI triage, correlations, and predictive insights.
- **Audit/compliance:** Fewer hours and lower fees with drill-downs, evidence capture, and report-ready posture.

What makes it different

- **AI-native remediation (not just dashboards):** Predictive and correlation views drive "what to fix next" and "why" (`app/ai/predictive/page.tsx`, `app/ai/correlations/page.tsx`); in-product assistant for triage/actions (`app/ai/chat/page.tsx`).
- **End-to-end, not siloed:** Cost anomalies, compliance violations, IAM/RBAC over-entitlements, and ops health live in one place:
  - Cost: `components/cost/CostAnomalyDeepDrill.tsx`
  - Compliance: `components/compliance/ComplianceDeepDrill.tsx`
  - Access governance: `components/rbac/DeepDrillDashboard.tsx`, `app/security/rbac/page.tsx`, `app/security/iam/page.tsx`
  - Ops/monitoring: `app/operations/monitoring/page.tsx`, `app/operations/resources/page.tsx`
- **Actionability built in:** JIT access, SoD conflict workflows, and permission removal flows are first-class UI actions, not FYIs.

- **Production readiness focus:** Guardrails and reliability scaffolding (e2e click sweeps, button verifiers, scripted audits) reduce UI regressions (`scripts/verify-clickables.js`, `frontend/tests/clicks.spec.ts`). Security-first headers/CSP/middleware patterns.

Who buys and why (primary ICPs)

- **FinOps + Platform Engineering:** unify spend visibility with fix-paths.
- **Security/IAM:** least-privilege at scale, SoD and JIT automation.
- **Compliance/GRC:** continuous evidence and faster audits.
- **SRE/Operations:** faster incident triage and remediation guidance.

Competitive angle

- **Versus point tools:** correlates across cost, access, compliance, and ops to compress handoffs (find → decide → fix).
- **Versus generic BI:** ships domain-specific actions and guardrails, not just charts.
- **Versus "AI overlays":** AI drives grounded, workflow-safe actions tied to real RBAC/compliance objects, not chat summaries.

Proof in code (feature → module map)

- Cost anomalies deep-drill: `components/cost/CostAnomalyDeepDrill.tsx`
- Compliance deep-drill and evidence: `components/compliance/ComplianceDeepDrill.tsx`
- RBAC/IAM deep-drill, JIT/SoD actions: `components/rbac/DeepDrillDashboard.tsx`, `app/security/rbac/page.tsx`, `app/security/iam/page.tsx`
- Predictive/correlation analytics: `app/ai/predictive/page.tsx`, `app/ai/correlations/page.tsx`
- AI assistant for triage: `app/ai/chat/page.tsx`
- Ops monitoring/resources: `app/operations/monitoring/page.tsx`, `app/operations/resources/page.tsx`
- Reliability/security scaffolding: `scripts/verify-clickables.js`, `frontend/tests/clicks.spec.ts`

Tagline

> *Turn cloud risk and spend into guided, auditable fixes—one AI control plane for FinOps, SecOps, and Compliance.*