PolicyCortex

PLATFORM ARCHITECTURE

Sovereign Cloud Governance and the Three Proofs

Collect cloud configuration state inside your boundary and export authorization packages your assessor verifies offline.

Authorizing officials and independent assessors no longer accept static screenshots assembled weeks before a review. Government agencies and regulated cloud operators need continuous, attributable records showing what was configured on the review date, who approved every change, and what automated workflows were permitted to touch.

Why Point-in-Time Compliance Breaks Under Review

Traditional compliance tools pull broad telemetry into a vendor cloud, map findings against generic checklists, and leave engineering teams rebuilding Word and Excel artifacts by hand before every audit. When an assessor asks how a control stayed in place across quarters, teams face missing history and unverifiable claims.

Verifiable Evidence Inside Your Own Cloud Boundary

PolicyCortex runs inside a customer-operated cloud installation with zero telemetry or evidence sent to PolicyCortex servers, or as a hosted service in PolicyCortex's US Azure tenant. Default onboarding uses read-only cloud permissions agreed up front with your security team.

Every exported package pairs human-readable SSP, SAR, and POA&M documents with machine-readable OSCAL 1.1.2 JSON and a SHA3-256 hash-chained evidence stream. Assessors run the included Python verifier offline without logging into PolicyCortex.

ARCHITECTURAL PILLARS

Proof of State

39 cloud collectors across Azure and AWS record timestamped configuration posture mapped to NIST, FedRAMP 20x, and CMMC controls.

Proof of Change

Every configuration delta, exception, and remediation step links to the named approver, ticket context, and before-and-after state.

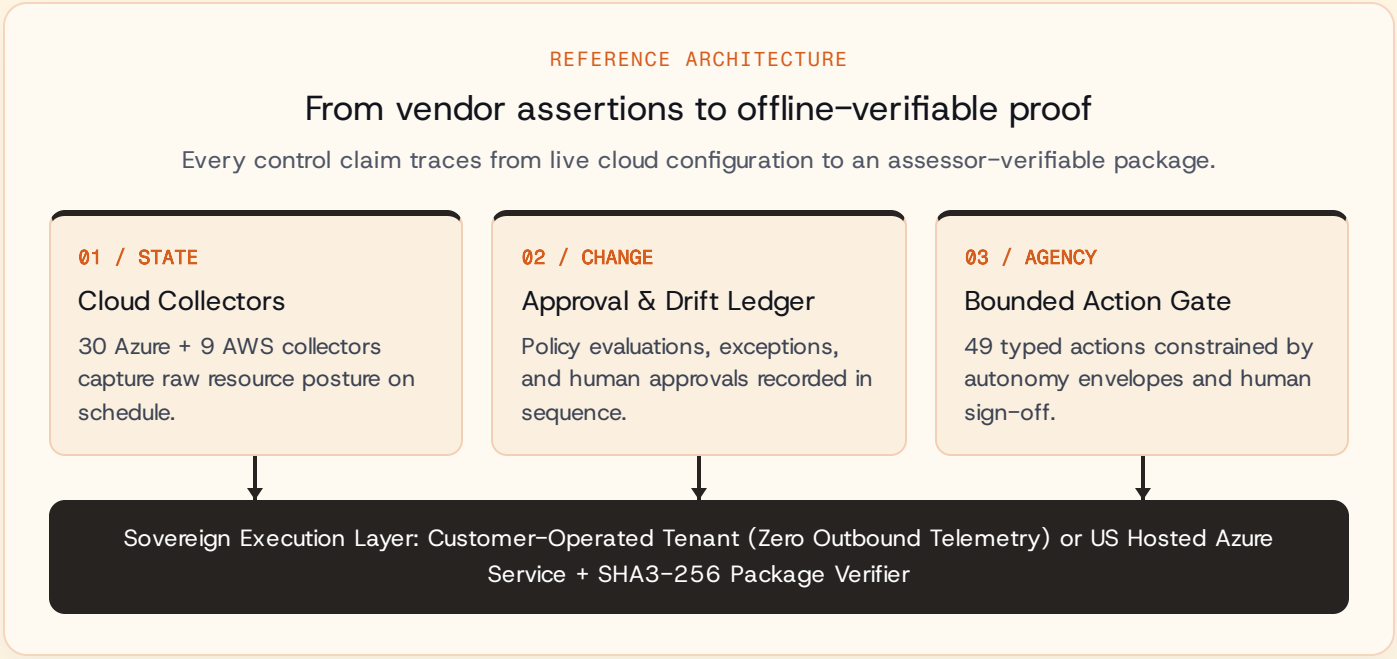
Proof of Agency

49 typed cloud actions enforce explicit autonomy envelopes, approval gates, and a 0.9 confidence floor before any write path runs.

Solution overview

PolicyCortex unifies cloud posture collection, framework mapping, gated remediation, and assessor-ready package generation in one operational record:

- **Read-only collection first:** Start with 30 Azure collectors and 9 AWS collectors, plus Google Cloud posture ingestion, using read-only credentials so evaluation never alters production resources.
- **Single implementation record across baselines:** Map live cloud evidence once across 1,196 NIST SP 800-53 Rev. 5 controls and enhancements, all 110 NIST SP 800-171 Rev. 2 requirements, and FedRAMP 20x KSI mappings.
- **Declared gaps instead of silent omissions:** When a collector is unreachable or a credential expires, the evidence stream records a declared observation gap rather than extrapolating green status.
- **Eight export formats from the same snapshot:** Generate Word SSP and SAR drafts, eMASS-compatible POA&M spreadsheets, OSCAL 1.1.2 SSP, SAR, and POA&M JSON, PDF summaries, and the offline verifier archive.



Solution components

Core modules, delivery options, and machine-readable handoff artifacts included in the platform:

Evidence & Control Engine

- **Cloud Collector Fleet:** 30 Azure resource collectors, 9 AWS service collectors, and GCP Security Command Center ingestion.
- **Unified Control Catalog:** 1,196 NIST SP 800-53 Rev. 5 controls and enhancements plus 110 NIST SP 800-171 Rev. 2 requirements.
- **As-Of Replay Queries:** Inspect control posture and linked evidence rows for any historical review date.

Package & Export Formats

- **OSCAL 1.1.2 Native JSON:** Schema-checked System Security Plan, Assessment Results, and POA&M JSON bundles.
- **Assessor Office Documents:** Editable Word SSP and SAR narratives paired with eMASS-ready POA&M workbooks.
- **Offline Python Verifier:** Standalone verify_ledger.py script validates SHA3-256 chain continuity without vendor access.

Governance & Action Gating

- **49 Typed Actions:** Pre-defined remediation operations with scoped blast-radius limits and rollback definitions.
- **Confidence & Approval Gates:** 0.9 confidence floor and mandatory human approval before privileged changes execute.

Deployment & Operations

- **Customer-Operated Boundary:** Deploys inside your own Azure or AWS subscription so raw evidence stays in-tenant.
- **US Hosted Option:** Managed deployment in PolicyCortex's US Azure environment for rapid onboarding.

39	1,196	8	SHA3-256
Cloud Collectors (30 Azure, 9 AWS)	NIST 800-53 Controls & Enhancements	Assessor & OSCAL Export Formats	Offline Hash-Chained Package Check

Evaluation and onboarding

Start with read-only permissions and verify exported packages before granting any write scope:

Step 01

Agree Read-Only Scope

Define target subscriptions, accounts, and baseline controls with your security team before connecting read-only collectors.

Step 02

Capture Baseline Evidence

Populate control implementation rows, open POA&M items, and declared gaps directly from live cloud configuration state.

Step 03

Export & Verify Offline

Hand your assessor or authorizing official a complete ZIP bundle and run verify_ledger.py on any air-separated workstation.

Additional resources

Download the unedited Sample Assessor Package and offline verifier	policycortex.com/sample-package
Inspect the in-tenant component boundary and verification guide	policycortex.com/architecture
Explore Proof of State, Proof of Change, and Proof of Agency	policycortex.com/platform
Review federal contracting and SAM registration details	policycortex.com/procurement

Explore the PolicyCortex Platform →

policycortex.com

gov@policycortex.com

© 2026 PolicyCortex, Inc. All rights reserved. SAM Registered Federal Contractor (CAGE 19CQ3). Specifications reflect audited product capabilities as of November 2026. Document ID: PCX-SB-2026-01.