TECHNICAL WHITEPAPER WP-03 · REFERENCE DEPLOYMENT TOPOLOGIES, RELEASE GATING & VERIFICATION BLUEPRINT

Production API-to-Agent Verification & Deployment Reference: Workstation, Kubernetes Topologies, PostgreSQL 15-18 RLS & Policy Gate Specification

The complete architect and CISO reference for Arcverin: 5-stage CLI/CI pipeline, air-gapped vs. multi-provider LLM modes, Personal/Team/Enterprise Kubernetes topologies, and the release sign-off checklist.

5 Stages	Ed25519	Postgres 15-18	1 Worker
1:1 STUDIO & CLI PARITY	**DSSE EVIDENCE PACKS**	**ROW-LEVEL SECURITY (RLS)**	**50+ GOVERNED TOOLS**
Deterministic artifacts from OpenAPI intake to governed vMCP runtime.	Offline-verifiable SHA-256 manifests, JUnit/SARIF & policy journals.	Multi-tenant Kubernetes isolation with OIDC SSO (Auth Code + PKCE), SCIM 2.0 & SoD.	Each Active Worker serves an entire API or multi-tool catalog.

1. Unified 5-Stage Studio & Headless CI/CD Pipeline Architecture

Arcverin pairs interactive browser authoring (Guided & Workbench modes at http://127.0.0.1:3002) with deterministic headless CLI execution for GitHub Actions, GitLab CI, and Azure DevOps:

Stage	Deterministic CLI Command Surface	Cryptographically Bound Output Artifacts
1. Find Gaps	arcverin-qualify <spec> --out <dir> arcverin mcp-economy <spec>	arcverin-qualification-report.html, arcverin-qualification-summary.json, BPE token report
2. Fix Contract	arcverin capability new --spec <spec> --outcome <goal> arcverin decisions answer <cap> | arcverin capability compile <cap>	capability.yaml (arcverin.capability/v1), OpenAPI 1.2.0 Overlays, workflow.arazzo.json, mcp-tool.json, compiled runtime plan (worker.ir.json)
3. Prove Safety	arcverin validate --capability <cap> --spec <spec> --target mock|staging arcverin validate --capability <cap> --spec <spec> --export <dir> | --suite <dir> --import <res>	23-scenario stateful mock & 12-mode fault receipts, digest-bound portable test suite receipts
4. Ship	arcverin gate <target> --policy gate.yaml --junit junit.xml --sarif gate.sarif arcverin pack build --source <spec> | capability export <cap> --format all	DSSE Evidence Pack (manifest.json, scorecard.json), JUnit/SARIF, Arazzo 1.1, OPA/Cedar/Temporal (projects & Sagas)/Gateway bundles
5. Operate	arcverin-commissioning submit | approve arcverin-runtime serve | arcverin-runner serve --mode progressive	Host-locked .dwpack, .arcverinvault bindings, policy-journal.jsonl, OTel/SIEM streams, MCP configs

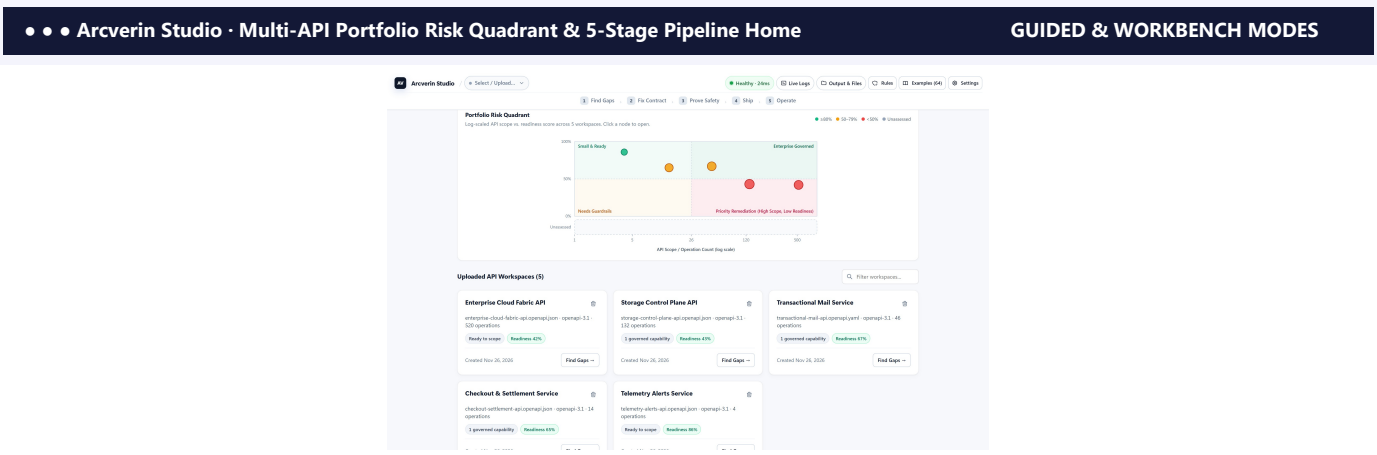


Figure 1: Arcverin Studio Home displaying the Multi-API Portfolio Risk Quadrant across assessed OpenAPI workspaces alongside the 5-stage guided pipeline (1. Find Gaps through 5. Operate).

2. 102 Deterministic Rules & Air-Gapped / Multi-Provider LLM Architecture

Every edition includes all 102 built-in rules and decision-graph projections. Studio runs 100% Offline Deterministic by default with zero network calls, or connects to 11 cloud and local LLM modes (OpenAI, Claude, Gemini, Azure OpenAI, Bedrock, OpenRouter, Groq, Mistral, DeepSeek, Ollama/vLLM, and Custom BYOK) while keeping deterministic rules authoritative.

Architectural Layer	Personal Edition (Workstation)	Team Edition (Shared Docker/K8s)	Enterprise Edition (Multi-Replica K8s & vMCP)
Compute & Storage	Windows x64 (.zip) & Linux Ubuntu 26.04 x64 (.tar.gz) on 127.0.0.1 + SQLite	Linux x86_64 Docker/Kubernetes + PostgreSQL 15-18	Linux Kubernetes (HA Control Plane & Runner HPA, 1 Runtime pod), Air-Gapped + PostgreSQL 15-18 RLS
Identity & Quotas	Single local user ($99 1-Month Pass / $49/mo billed annually · $588/yr · 3 projects / 2 workers / 1 seat)	Multi-User Portal & 5-Role RBAC (10 projects / 5 workers / 5 seats; expandable via Capacity Packs)	OIDC SSO & SCIM 2.0, PATs, SoD (Standard: 25 projects / 15 workers / 25 seats · Unlimited)
Rules & Compliance	102 Built-In Rules + Overlays + Arazzo 1.1 / OPA / Cedar / Temporal skeleton exports	102 Built-In Rules + Overlays + peer-reviewed waivers + CI Gate + runnable Temporal TS/Py projects	Custom Visual JDM Studio, Drift Baselines, 6-Framework DSSE, Gateway Bundles + vMCP Temporal Sagas
Runtime & Telemetry	Local Pilot Runtime + local Ed25519 signing + Live Logs	Shared MCP Runner + OpenTelemetry (OTel / OTLP) HTTP/JSON audit log export	Multi-Provider vMCP + OTel HTTP/JSON & token-auth Splunk HEC + Software CMK Ed25519 + Rust Data-Plane Source

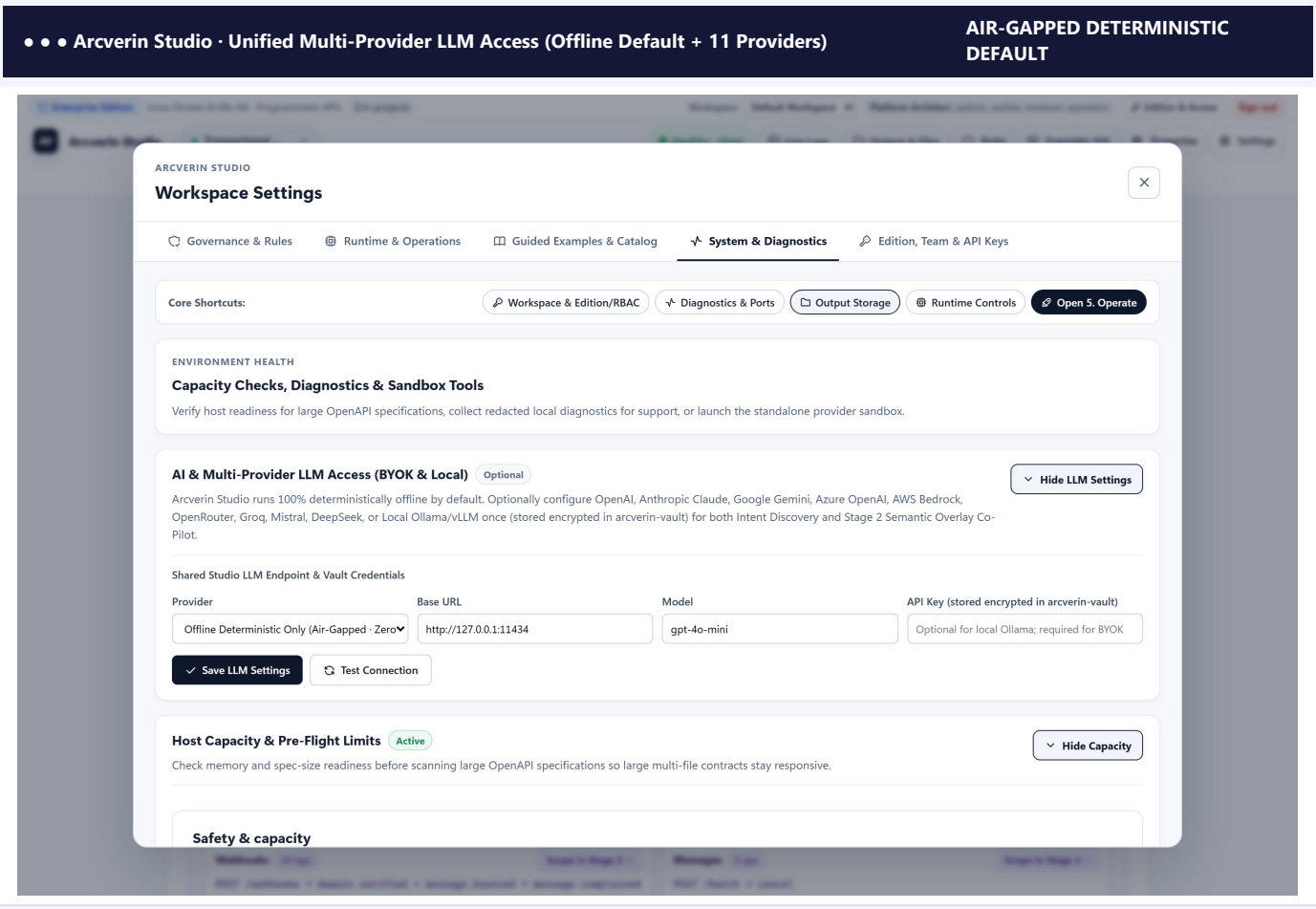
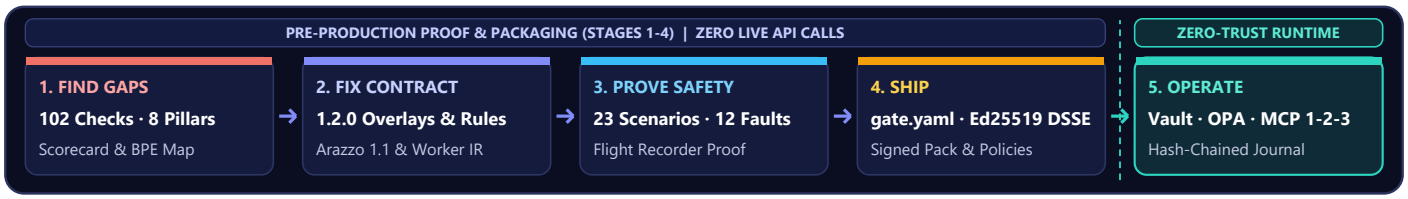


Figure 2: Multi-Provider LLM settings supporting air-gapped Offline Deterministic execution alongside 11 cloud and local LLM providers with encrypted Vault storage.

3. Production Release Gate & CISO Sign-Off Checklist

Complete this five-stage checklist before promoting an API capability into production:



- [ ] [Stage 1 - 8-Pillar Qualification & Token Budget] Verify zero syntax blockers and confirm exact o200k_base BPE compaction via arcverin mcp-economy <spec>.
- [ ] [Stage 2 - Overlays, Owner Decisions & Visual JDM] Resolve all AR0 (Blocked) unknowns via OpenAPI 1.2.0 Overlays or signed Owner Decisions, and pass all Visual JDM tests.
- [ ] [Stage 3 - 23-Scenario Fault Simulation] Confirm passing receipts across all 12 fault modes (504 retry idempotency, async 202 polling, and cross-tenant 403 denials).
- [ ] [Stage 4 - Fail-Closed Gate & DSSE Pack] Verify arcverin gate <target> --policy gate.yaml exits 0 and run arcverin pack verify <pack-dir> --trusted-signers trusted-signers.json.
- [ ] [Stage 5 - Vault, Dual-Control & Policy Journal] Bind secrets in .arcverinvault, complete Operator + Reviewer sign-off, and verify policy-journal.jsonl via arcverin-runner verify-journal.

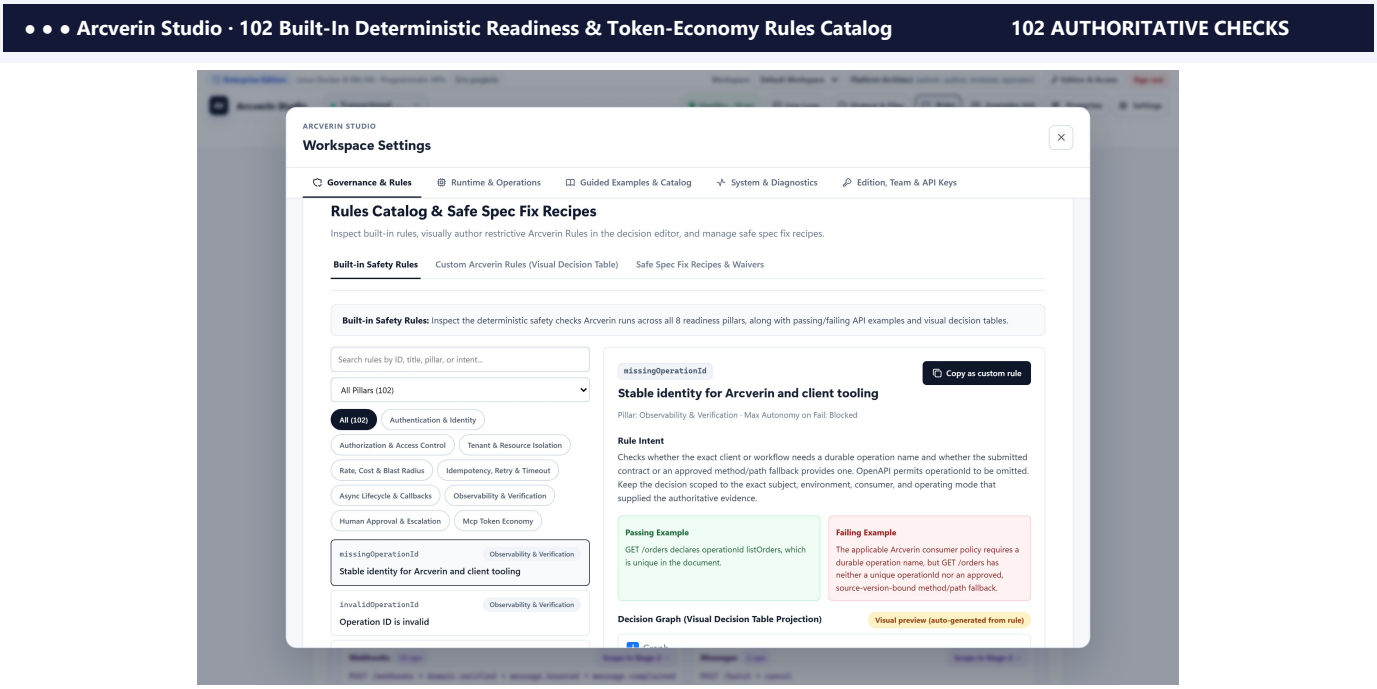


Figure 3: Built-in Rules Catalog showing rule intent, passing and failing OpenAPI examples, and pillar filters across all 8 readiness pillars.

Explore the Arcverin Technical Documentation & CLI Reference at https://www.arcverin.com/docs/ →

https://www.arcverin.com/docs/

Retain the signed DSSE Evidence Pack (manifest.json, scorecard.json, report.html) and policy-journal.jsonl alongside the exact OpenAPI specification revision evaluated.