
You do not send us your data.

Most of a security questionnaire asks how a vendor protects data you send them. RotaGrant is deployed in your cloud account, your data centre, or fully airgapped. This document is the shorter, harder version: what runs where, what can leave, what we hold, and what we do not have.

Deployment

MODEL	Single tenant, in your environment. Not a namespace in a shared cluster with a residency label attached.
RUNS ON	Your VPC, your data centre, or an airgapped network with no route out.
COMPONENTS	API, console, Postgres, Cedar policy evaluator, identity through your OIDC provider.
OUR ACCESS	None by default. We hold no standing credential into a customer deployment.

Data handling

PAYLOAD EGRESS	None. No prompt, no completion, no record and no identifier leaves the deployment on any path.
OUTBOUND CONNECTIONS	Enumerable and probed rather than described. The deployment reports its own egress posture, and a setting selecting a service outside your network is visible on that screen.
AIRGAPPED MODE	Refuses to start if any setting selects a service outside your network. Checked at startup, not at first use. It also refuses external anchoring, and the platform states which property that costs you rather than pretending it is free.
THE ONE OPTIONAL PATH	External anchoring publishes a Merkle root — a hash of a hash. Off unless switched on.

TELEMETRY	None. No licence check, no update check, no crash reporter, no analytics. A test fails the build if any appears, and a second fails it if a module opens a network connection absent from the egress inventory.
MODELS	No model is called on any path — not for a summary, a digest or a classification. Asserted by a test that fails the build if a model provider appears in the dependency graph.

Tenancy, identity and keys

TENANCY	Row-level security in PostgreSQL rather than in application code. A query that forgets its workspace filter returns nothing rather than everything.
IDENTITY	OIDC. Identity, groups and multi-factor policy stay with your provider; RotaGrant maps them to what they grant here and stores no credentials.
ROLES	admin, governance-officer, reviewer, auditor. Read-only is a role that cannot write because it is absent from the write set, not because a flag says so.
KEY CUSTODY	deployment, KMS, HSM, or external — where the platform cannot sign without you. Every artefact records which custody signed it, because a signature is worth what the custody is worth.
PRIVATE KEYS	Never uploaded, pasted, downloaded or exported. The capability is absent from the interface rather than present and forbidden.

Evidence integrity

SEALING	Records are sequenced and sealed into Merkle batches with per-record inclusion proofs.
VERIFICATION	A signed artefact verifies in any browser against a key you obtained out of band. Verifying against the key inside a document proves it is unaltered; it does not prove who signed it, and the verifier says which of the two questions it answered.

FAILURE MODES	Capture fails open, enforcement fails closed. A recording problem must not cause an outage; an unreachable control plane must not silently permit an ungoverned action.
ADVERSARIAL TESTING	We attack our own identifier detector and publish the grid, including the cells it fails, classified as defect or residual.

What we do not have

CERTIFICATIONS	No SOC 2 or ISO 27001 today. Deferred until a customer requires one, and the scope is small when we do it — we would be audited on how we build and support, not on a platform holding your data, because we do not hold it.
HEALTH CLAIMS	Not a medical device. No HIPAA or FDA claim.
SUBPROCESSORS	For the platform in your environment: none. Our own website uses Cloudflare and Resend, both listed at rotascale.com/trust/ .

Reporting a vulnerability

security@rotascale.com. The disclosure policy is at rotascale.com/security/. A completed security questionnaire, the egress inventory and the architecture are kept ready rather than assembled per deal — ask and they arrive the same day.

This document describes the software. It is not a warranty about your deployment, your configuration or your regulator's view of either. Rotascale governs the action; it does not warrant the outcome.