Keep control of code, credentials, and execution.

A procurement-ready overview of ThriveOnDev deployment boundaries, execution isolation, authentication, and auditability.

Two deployment paths, one operating model

Use managed cloud for fast pilot activation, or install the whole platform in your Kubernetes environment when policy requires an in-perimeter control plane.

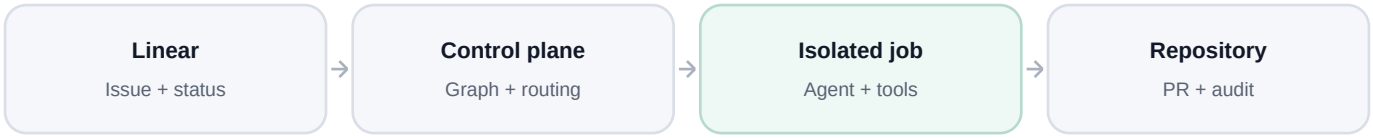
Managed cloud

Tenant-scoped Kubernetes jobs and credentials, HMAC-signed callbacks, and a connected audit trail for every run.

Self-hosted via Helm

Control plane and agent execution run in your cluster, with offline license validation, SSO/OIDC, and an air-gapped path.

Execution and data boundary



Self-hosted: control plane, code, credentials, and jobs remain inside the customer boundary

Controls described for pilot review

- Tenant-scoped job and credential boundaries
- Repository and tool scope defined per run
- Retries, timeouts, cleanup, and failure handling
- Connected trace: issue, graph, events, and outcome
- Per-user subscription auth - no shared accounts
- Customer-owned API keys as a first-class path
- Rate-limit-aware scheduling
- Offline license and air-gapped self-host path

AUTHENTICATION AND BILLING

Agents can run on each engineer's existing subscription auth or on customer-owned API keys. ThriveOnDev charges for the pipeline, not inference tokens; API-billed inference remains attributable in the run receipt.

What the trust-pack conversation should confirm

Data handling

Deployment-specific flows, retention, deletion, and underlying provider choices.

Identity and access

SSO/OIDC scope, user-to-credential mapping, repositories, tools, and approval gates.

Assurance status

Current policies, contracts, test evidence, and roadmap - stated without implied certification.

Next step: scope the trust pack during a 25-minute pilot intro

info@thriveondev.com | thriveondev.com