Keep control of code, credentials, and execution.

The agent-neutral delivery pipeline for Linear — isolated execution, explicit deployment boundaries, and a connected record of every run.

Two deployment paths, one operating model

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

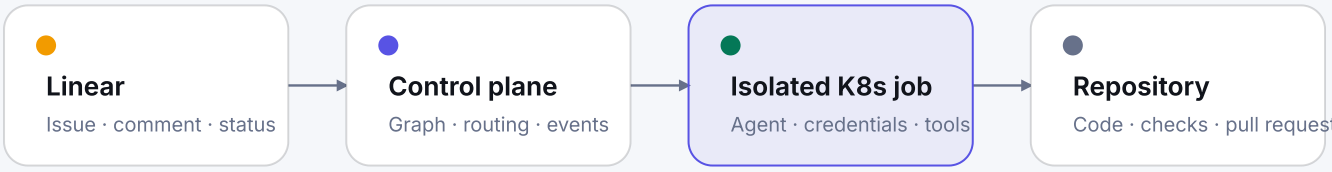
Managed cloud

Tenant-scoped Kubernetes jobs and credentials, HMAC-signed callbacks, and a connected issue, graph, event, and outcome trail for each run.

Self-hosted via Helm

Control plane, planning, execution, and data stay in your cluster, with offline license validation, Keycloak SSO/OIDC, and an air-gapped installation path.

Execution and data boundary



job filesystem is ephemeral · control plane retains run records, not a repository copy

Self-hosted — platform data stores, code, credentials, and jobs remain inside the customer boundary; model calls follow customer-configured routing.

Controls

- ✓ 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 provider credentials — 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	Runs bill to customer-owned API keys at provider rates. Policy-aware routing applies each provider's terms automatically; sanctioned subscription auth is per-user and per-tenant, with no shared accounts.

Data handling, access, and assurance.

Data handling

DATA CATEGORY	WHAT WE ACCESS	WHERE IT LIVES — MANAGED CLOUD	RETENTION
Repository code	Cloned and accessed inside the isolated job for the requested run.	Ephemeral job filesystem. The control plane does not persist a repository copy.	Removed with job cleanup; finished jobs have a 30-second TTL.
Linear issue and comment metadata	Issue, comment, status, workspace, user, and session identifiers needed to route and report work.	Linear and tenant-scoped control-plane records on DigitalOcean.	Service term; return or deletion within 30 days after termination under an executed DPA.
User identifiers	Name, email, organization/workspace ID, and account identifiers used for auth, billing, and audit.	Keycloak and tenant-scoped control-plane records.	Service term; return or deletion within 30 days after termination under an executed DPA.
Run telemetry	Outcome, provider/model, duration, cost estimates, CI result, and failure reason.	Tenant-scoped PostgreSQL and Temporal; diagnostic errors may be sent to Sentry.	Temporal history: 7 days. Event partitions: 3 months. Other tenant records follow the service term and DPA termination window.
Agent session logs	Prompts, output, tool events, elicitation, artifacts, and lifecycle events associated with a run.	Tenant-scoped session/event records; pod logs exist for the life of the job.	Pod logs: job lifetime. Session records follow the service term and DPA termination window.

Managed-cloud offboarding: the draft DPA provides return or deletion within 30 days after termination and certification on request; this becomes contractual when signed. Deleted PostgreSQL data may remain beyond use in DigitalOcean's daily backups for up to 7 days before expiry. **Self-hosted:** retention remains under customer control unless support access is explicitly granted.

Sub-processors — managed cloud

PROVIDER	PURPOSE	LOCATION OR HANDLING NOTE
DigitalOcean	Kubernetes compute, hosting, and managed data infrastructure.	LON1 — London, United Kingdom.
Linear	Issue/session command surface and API used to receive work and report progress.	Customer's Linear workspace; processed under Linear's service terms.
Sentry	Error monitoring and diagnostics.	Configured to exclude personally identifiable information by default; no session replay.

AI model providers are customer-directed. Anthropic, OpenAI, GitHub, and Google are engaged through the customer's own API keys or sanctioned per-user subscription auth and remain governed by the customer's agreements with those providers.

Identity and access

SSO/OIDC: Keycloak provides the identity layer; Kong validates JWTs at the API boundary.

Per-user credential mapping: provider credentials are mapped to each engineer and tenant; shared accounts are not the operating model.

Run scope: tenant job secrets contain only approved repository, provider, Linear, and tool credentials for that job.

Callbacks: agent callbacks use HMAC-SHA256 signatures with constant-time verification.

Audit trail: issue/session IDs, graph and node execution, events, outcomes, and failure reasons are connected for each run.

Assurance status

Mutual NDA + DPA: DPA draft available for legal review; mutual NDA in preparation.

Penetration test: Not yet conducted.

SOC 2 Type I: Not certified; no audit is in progress.

No certification, independent attestation, completed penetration test, or active SOC 2 audit is claimed.

ThriveOnDev Ltd
Company no. 14781768 · Registered in England and Wales