dataplanelabs

TECHNICAL BRIEF
V1.0 · 2026
DATAPLANELABS.COM

AGENTIC AI SYSTEMS FOR DATA TEAMS

The secure runtime that puts data-team agents into production.

DataPlaneLabs is a product company. We build AI agents — and the governed runtime they run on — for the people who own pipelines, warehouses, analytics, and governance. Every agent ships on your own infrastructure and acts under your controls, with each action governed and observable. We do not build foundation models; you bring the models, and we put them to work in production.

Runtime architecture

CONTROL	Policy, identity, and routing — the decision layer for every tool call.
DATA	Execution, tool calls, and retrieval — where agents do the work.
STORAGE	Audit, state, and knowledge — a complete, reviewable trail.

Request path: `agent → gateway → policy decision (identity + RBAC) → tools / warehouse → audit log`

What we build

- **Pipeline & ELT agents** — build, fix, and maintain ingestion and transformation.
- **Data-quality & observability agents** — watch freshness, schema, anomalies; act on breaks.
- **Analytics & insight agents** — answer questions over the warehouse, surface what changed.
- **Governed tool-execution runtime** — policy, identity, and audit on every tool call.
- **Self-hosted agent control** — deploy, observe, and govern a fleet inside your perimeter.

Security posture

- **Self-hosted** on your own Kubernetes cluster — no vendor cloud, no shared tenancy.
- **Zero-trust at tool invocation** — every call requires an explicit policy decision.
- **Encrypted** in transit and at rest within your environment.
- **RBAC** with least-privilege defaults for agents and operators.
- **Full audit log** per tool call — who, what, when, and the policy decision.
- **No egress** — models, data, prompts, and logs stay on your infrastructure.

What we do not yet claim
Formal certifications (SOC 2, ISO 27001) are not yet in place. We will not display badges we have not earned. For specific compliance needs, contact us to walk through our controls.

Works with your stack

LLM providers — hosted or self-hosted, route to what you use.

Vector stores — ground retrieval in your embeddings store.

Data warehouses — read/write under your access controls.

Existing tools — orchestration, identity, observability wired in.

Category-level by design — we connect to what you already run, not a fixed vendor list.

How we work

01	02	03
Assess	Deploy	Operate
Week 1	Weeks 2–4	Ongoing

Typical time to a first production workflow is roughly four weeks. Scope and stack complexity shift the range.