Your data stays in your systems. People make the call.

What runs where, what can leave your environment, how people stay in control, and what we can show your security team today.

Where it runs

- **Your cloud tenancy**, in your account and region, under your keys.
- **Hybrid**: sensitive workloads and data on your servers, the rest in your cloud.
- **Your data centre**, on your hardware, behind your firewall.
- **Air-gapped**, with self-hosted models only.

Built-in controls

- Role- and attribute-based access with deny-overrides, and isolated projects per team, environment and business line.
- Every model call authenticated, logged, metered and routed by your rules at a gateway.
- Guardrails on inputs and outputs, and evaluation gates before any model is promoted.
- Each company runs as its own organisation, with its own people, knowledge and model credentials.

What stays, and what can leave

What	Where it lives	Can it leave your environment?
Business records (ERP, CRM, core systems)	Your systems, read at query time	No. Records are not copied into the platform.
Documents and knowledge	Governed collections in your environment	No, except a retrieved passage sent with an allowed request.
A model request and its retrieved context	Created in your environment	Only if your routing rules send it to an external provider. You can switch this off.
Models, weights and fine-tunes built for you	Your environment	No. They are yours.
Decision history, approvals, audit trail, gateway logs	Your environment	No.

Evidence on every decision

- Reason codes and cited source passages with each output.
- A signed evidence trail linking each output to its inputs and sources.
- Each agent's rules written down in plain language; limits held as settings a manager can change.
- Who approved what, when and why, recorded with the decision.

People stay in charge

- Agents stop for a named approver where their rules say so; the approver can approve, edit or send back.
- Payroll, accounts payable, refunds and returns, contract preparation and CV screening always need their owner's sign-off.
- When a record is missing, the agent says so and asks for it.

Our security status, plainly

- We do not yet hold SOC 2 or ISO/IEC 27001 certification. Because the platform runs in your environment, your own controls apply to it.
- Send us your questionnaire: we answer it in writing before a pilot.
- You may test a deployment in your environment, with your own tools or testers.
- If you allow external model providers, you choose which, and your contract terms with them apply.

Before a pilot starts

1. **Agree the data flows**, retention and access in writing with your security team.
2. **Read access first.** Nothing is written back.
3. **Approval on every action**, each recorded with its evidence.
4. **Write access where earned**, within limits you set.

Report a vulnerability: hello@wersel.io, subject "Security". We acknowledge within three working days.