DATA SHEET

TROVATA

Security & Trust · AI

Modern treasury AI, built with enterprise-grade security at the core.

Trovata AI is built for high-trust treasury environments where confidentiality, auditability, and control are non-negotiable — so teams can adopt AI with confidence.

HOW WE KEEP YOUR ENVIRONMENT & DATA SECURE

Airgapped by design

Fully airgapped within Trovata's AWS architecture — no public internet access, no external AI routing.

Governed access to data and workflows

A controlled execution layer governs exactly which treasury data and workflows the model can access.

Role-based permissions remain in place

Trovata AI enforces role-based TMS controls — users access only what their permissions allow.

Data stays protected

Encrypted in transit and at rest within Trovata's AWS — used to generate answers, never to train a shared model.

Agents are constrained and auditable

Agents are scoped to defined tasks and actions, with run history, logs, and full traceability for review and oversight.

Tenant isolation is built in

Customer data and AI workflows stay separated within defined tenant boundaries under the same platform isolation model.

COMMON QUESTIONS

Will Trovata AI be trained on my company's data?
No. Customer data generates answers inside your environment — never to train a shared model or benefit another customer.

Does my data leave Trovata's cloud environment?
No. Trovata AI runs entirely within Trovata's airgapped AWS architecture — no public internet accessibility.

Does Trovata AI override our existing user permissions?
No. Trovata AI enforces the same TMS role-based controls — users only see accounts and records they're authorized to access.

Can we audit what AI agents have done?
Yes. Every agent run is logged with full traceability so teams can review and validate every automated workflow.

SECURITY AT A GLANCE

- **Airgapped AWS environment**
  No public internet access, ever
- **Controlled execution layer**
  Governed access to treasury data and workflows
- **RBAC enforced throughout**
  AI respects all existing TMS permissions
- **Encryption in transit & at rest**
  Within Trovata's AWS environment
- **No model training on customer data**
  Data generates answers, not shared models
- **Agent run history & audit logs**
  Full traceability for every workflow
- **Enterprise tenant isolation**
  Customer environments fully separated

AI INFRASTRUCTURE

Powered by Anthropic's Claude Sonnet 4.6 via Amazon Bedrock — no third-party routing, no open internet exposure.

DATA USE POLICY

Customer data is never used to train models for other customers. Your data generates answers inside your environment — and nothing else.

Book a Demo →