Strataflows

Security & Trust Overview

Prepared by: Luke Viering, Founder | luke@strataflows.io | strataflows.io

Strataflows turns your team's sales calls and CRM data into honest, actionable deal intelligence. That means connecting to systems that hold your most sensitive data — so here is exactly how we protect it.

How we connect to Salesforce

We connect through Salesforce's standard **OAuth 2.0 Authorization Code flow with PKCE (S256)**, requesting only least-privilege scopes (api refresh_token offline_access id). **Access is read-only** — Strataflows never writes to, modifies, or deletes anything in your Salesforce org (the only outbound call is an OAuth token revoke when you disconnect). **Nothing is installed into your Salesforce** — there is no managed package. You can disconnect at any time, from either side.

Encryption

Your OAuth tokens are encrypted at rest with **AES-256-GCM** at the application layer, with the encryption key held **outside the database** — so a database compromise alone cannot expose them — on top of infrastructure-level storage encryption. All data in transit is protected with **TLS 1.3**.

Tenant isolation

Every customer's data is walled off by organization and enforced in **three independent layers**: database row-level security, an application-level access gate on every request, and an automated build-time check that fails the release if any query is not correctly org-scoped. One customer's data can never be read by another.

Your data and who processes it

We are upfront about where your data flows. To generate intelligence, content *derived from* your CRM and call data is sent over TLS to **OpenAI** (our LLM provider) for inference; OpenAI returns generated text, and Strataflows retains no prompts or completions — only usage metadata. Our full subprocessor list:

Subprocessor	Purpose	Data received
OpenAI	LLM inference	Prompt content derived from CRM & call data; no prompts/completions retained by Strataflows
Supabase	Database	Application data at rest (US region); SOC 2 Type II / ISO 27001
Vercel	Hosting / compute	Data in transit; runtime metadata
Stripe	Billing	Billing identifiers only — no CRM data
Resend	Transactional email	Email address; alert subject (account name only)
Sentry	Error monitoring	Masked error metadata (PII collection off)

Built on trusted infrastructure

Strataflows runs on **SOC 2 Type II / ISO 27001-certified infrastructure** (Supabase / AWS). Our OAuth integration meets Salesforce's current Connected App security controls (PKCE, refresh-token rotation, least-privilege scopes), and our AppExchange Security Review is in progress.

You are always in control

Disconnect any integration instantly from Settings, revoke access on the Salesforce side, export your data, or request deletion at any time.

Security documentation

Available on request or from our Trust Center (strataflows.io/security): API callout reference, false-positive analysis, and DAST scan results (OWASP ZAP; CASA Tier 2 by TAC Security, score 9.7/10). Full penetration-scan reports available on request.
