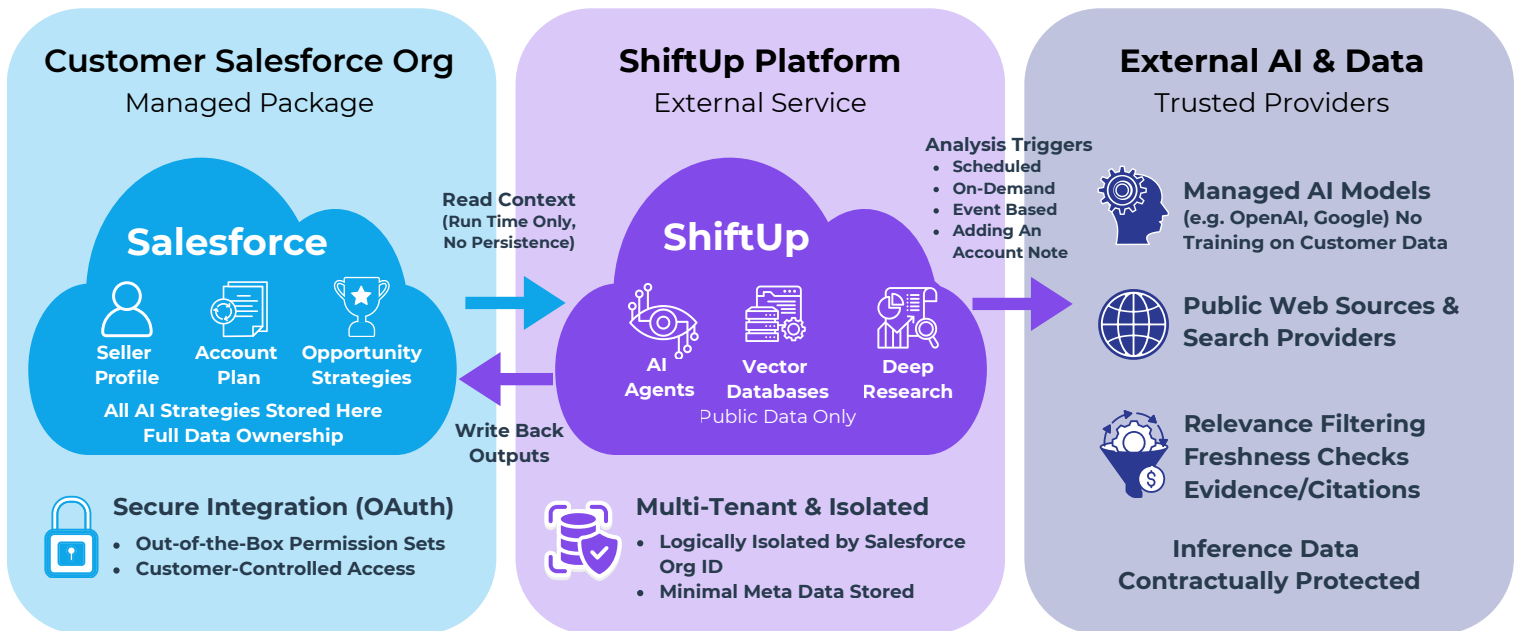


ShiftUp Customer Security Overview



Purpose

This document provides a concise, customer-facing overview of how ShiftUp handles data security, access, and AI processing when deployed in a Salesforce environment.

Product Architecture

ShiftUp is a SaaS solution that helps companies build high-quality sales pipeline and advance deals faster using AI agents that perform deep, sales-focused research and generates:

- Account Plans
- Opportunity Strategies
- Relevant Stakeholders & Contact Details
- Conversational Roadmaps
- Personalized Outreach Messaging & Cadences

Data is never shared across customers

ShiftUp Consists of Two Components:

- **Salesforce Managed Package:** A Salesforce-approved managed package installed directly in the customer's Salesforce org.
- **ShiftUp AI Platform:** An external AI service leveraged by the managed package to execute agentic workflows and maintain vector databases for external research data.

Data Location

- ShiftUp creates managed Custom Objects for Seller Profiles, Account Plans, Opportunity Strategies, and integration events.
- All AI-generated outputs are written back and stored exclusively in the customer's Salesforce org within ShiftUp managed objects.



Data Ownership

- Customers retain full ownership of all data stored in their Salesforce org.
- If a customer stops using ShiftUp, all data remains in Salesforce unless the managed package is explicitly uninstalled.

What Triggers an Analysis

- An Account is added to a Seller Profile.
- A scheduled refresh (daily or weekly, configured by the customer).
- A user initiates an on-demand refresh or update request.
- An Account Note is added to the Account.

Integration Access & Permissions

- The ShiftUp Platform connects to Salesforce via an External Client Application included in the managed package.
- Authentication uses OAuth client credentials and runs as a customer-defined integration user.
- The permissions of this integration are strictly limited to those granted to that user.

ShiftUp Provides an Out-of-the-Box Integration Permission Set Covering:

- ShiftUp managed Objects
- Required Apex classes
- Flows

Customers Explicitly Controls Any Additional Permissions for:

- Standard Salesforce Objects
- API access
- Apex REST service
- Never shared across customers

Existing ShiftUp Data

Previously generated Account Plans and strategies are read to determine what requires updating.

Data Storage Outside Salesforce

- ShiftUp does **not** persist CRM record content outside Salesforce.
- Only minimal operational metadata (e.g., org ID, account plan IDs, API key hashes) is stored to operate workflows.
- All final analysis outputs are written back to Salesforce.

Multi-Tenancy & Data Segregation

- The ShiftUp AI Platform is multi-tenant. Each request is authenticated using an API key and Salesforce org ID.
- Internal workflows are logically isolated and keyed by org ID to prevent cross-org access.

Vector Data & External Research

- ShiftUp stores vector embeddings derived from publicly available external data gathered during research.
- No customer CRM content is embedded or stored in vector databases.



AI Model Training

- ShiftUp does not build, fine-tune, or train AI models using customer data.
- The platform uses managed AI models from trusted providers; contractually guaranteed inference data is not used for training.
- Example providers include OpenAI, Google, Anthropic, Voyage AI, and Mistral AI.

Salesforce Sharing Model & User Access

- ShiftUp supports private sharing models.
- Account Plans and Seller Profiles can be configured as private objects.
- Account Plan ownership can be synchronized with the related Account Owner.
- Only users assigned ShiftUp permission sets can access ShiftUp's functionality.

API Usage

- ShiftUp uses bulkified and composite REST APIs to minimize Salesforce API consumption.
- Typical usage is approximately 10 inbound calls per analyzed account.
- Customers are encouraged to configure Salesforce API usage alerts.

External Data Sources & Trust

- ShiftUp research is public web sources via search providers and custom web scrapers.
- Stakeholder enrichment may include LinkedIn and other third-party data providers.

All External Content is Treated as Untrusted & Processed With:

- Relevance filtering
- Freshness checks
- Evidence requirements with citations and multiple sources, where possible.