Data Security & Compliance for Snowflake Cortex Apps

Overview

Trust3 allows AI platform owners and security teams to enforce centralized, customizable fine grained content moderation and access controls to bring **enterprise grade thoroughness and flexibility to any** AI systems built using Snowflake Cortex platform. This includes:

- **Enhanced Content Moderation:** Automatically detect and manage PII, toxic content, intellectual property, and any other custom content within AI applications, allowing for immediate redaction, approval, or denial based on centralized policies.
- **Unified Access Management:** Consolidate and enforce fine-grained access policies across both structured and unstructured data, ensuring consistent control over who can access AI applications.
- **Data Security & Compliance:** Maintain and enforce permissions on unstructured content when utilizing Cortex Search, strengthening data security and supporting compliance efforts for AI deployments. Trust3 offers centralized and detailed access logs, enabling easy viewing and compliance through comprehensive audit reports.

In this quickstart guide, we'll demonstrate how to **safeguard and monitor conversations** in LLM-powered applications using **Trust3**. As an example, we'll build a simple **Intelligent Sales Assistant** using **Snowflake's Cortex Agents** and **Streamlit**. This assistant will help simulate realistic LLM interactions, allowing us to showcase how Trust3 can enforce guardrails, monitor usage, and ensure secure, responsible AI behavior.

What You'll Learn

- Installing and configuring the **AI Trust Layer for Cortex** from the Snowflake Marketplace
- Integrating **Trust3** with your Streamlit app to enforce **guardrails**, **monitor interactions**, and **ensure responsible AI usage**

What You'll Build

- Interact with sales data through semantic search, metrics analysis, and LLM-powered Q&A
- Safeguard and monitor all assistant conversations using **Trust3** to enforce security, compliance, and responsible AI use

What You'll Need

- **Snowflake Account**: With permissions to create databases, tables, upload files, create external access integration, install applications from snowflake marketplace. (Snowflake setup)
- **Access to Snowflake Cortex Services**: Including Cortex Agents, Cortex Search, and Cortex Analyst

- **AI Trust Layer for Cortex**: Available via the Snowflake Marketplace, required to safeguard and monitor assistant conversations.

Setup Workspace

Step 1. In Snowsight, create a SQL Worksheet and open setup.sql to execute all statements in order from top to bottom.

This script will:

Note:- The script contains placeholders like <YOUR_USER> and <YOUR_PRIMARY_ROLE>, please update those with your snowflake username and role according to your setup.

- Create roles
- Create the database, schema, and warehouse
- Create tables for sales conversations and metrics
- Load sample sales data
- Enable change tracking for real-time updates
- Configure Cortex Search service
- Create a stage for semantic models and python packages

Step 2. Upload the semantic model:

- Download sales_metrics_model.yaml (NOTE: Do NOT right-click to download.)
- Navigate to Data » Databases » SALES_INTELLIGENCE » DATA » Stages » MODELS
- Click "+ Files" in the top right
- Browse and select sales_metrics_model.yaml file
- Click "Upload"

Step 3. Install **AI Trust Layer for Cortex** from Snowflake Marketplace:

- **Log in** to your Snowflake account and navigate to **Data Products** → **Marketplace**.
- **Search for "AI Trust Layer for Cortex".**
- Click on the application result, then click **Get** to install it into your Snowflake account.
- **Grant the required privileges** and launch the application.
- Follow the on-screen instructions to **create the external access integration** and verify it.
- Click **Check Service Status** to ensure the service is running. Once it's active, click **Get Service URL** to retrieve the endpoint.
- Make a note of this endpoint as it will be needed later in the configuration process.
- Open the URL in a new tab. After authenticating with Snowflake, you'll access the **Trust3 Portal**.
- Use the following credentials to log in:
    - **Username**: `admin`
    - **Password**: `welcome1`

Create Trust3 Application

Step 1. Create Vector DB for Snowflake Cortex Search

- Login to Trust3 Portal
- On the left hand navigation, click on **Vector DB** under **Navigator**
- Click on **CREATE VECTOR DB**
- Select the type as **Snowflake Cortex** and enter the name for your vector database
- Click on **Create**
- You will now see the vector db configuration page, navigate to the **Permissions** tab
- Click on edit icon and enable the toggle of **User/Group Access-Limited Retrieval** and click **Save**

Step 2. Create Trust3 Application for Snowflake Streamlit Application

- On the left hand navigation, click on **AI Applications** under **Navigator**
- Click on **CREATE APPLICATION**
- Enter the name for your application and select the vector database we have created from the dropdown
- Click on **Create**

Create Streamlit Application

Step 1. Generate Trust3 Application API Key

- On the Trust3 Portal, click on **AI Applications** under **Navigator**
- Navigate to the application you have created
- Click on the **API Keys** tab and click on the **Generate API Key**
- Put the API key name and validity as per your requirements and click **Generate**
- Make a note of this API Key as it will be needed later in the configuration process.

Step 2. Create Snowflake PAT Token using the instructions provided in the link below

- https://docs.snowflake.com/en/user-guide/programmatic-access-tokens#generating-a-programmatic-access-token
- Make a note of this PAT Token as it will be needed later in the configuration process.

Step 3. Upload the Trust3 Packages

- Download trust3_common.zip and trust3_client.zip (NOTE: Do NOT right-click to download.)
- Navigate to Data » Databases » SALES_INTELLIGENCE » DATA » Stages » PYTHON_PACKAGES
- Click "+ Files" in the top right
- Browse and select trust3_common.zip and trust3_client.zip file
- Click "Upload"

Step 4. In your Snowflake account:

- On the left hand navigation menu, click on **Streamlit** under **Projects**
- On the top right click the **Streamlit App** button
- In the Create Streamlit App dialog, select **sales_intelligence** for your database and **data** as your schema
- Select your Warehouse
- Click on Create button

Note:- Make sure your database and schema match the ones created in the setup step.

Step 5.

- Copy and Paste contents from the streamlit.py into your new Streamlit App
- In the streamlit app, you will find the below placeholders, where you need to update the values according to your configurations
  - <your-trust3-server-base-url> - Trust3 Native Application Endpoint (url should include https://, For eg. https://abcde-gk76548-demo.snowflakecomputing.app)

    - <your-snowflake-pat-token> - The snowflake PAT token generated in above steps.
    - <your-trust3-ai-app-api-key> - Trust3 AI Application key generated in above steps.
- Click on the 3 dots icon on the top right corner and click on **App Settings,** click on the **External Networks** tab and select enable toggle for **ALLOW_SNOWFLAKE_NATIVE_APPS_EAI**
- Then Run the streamlit application

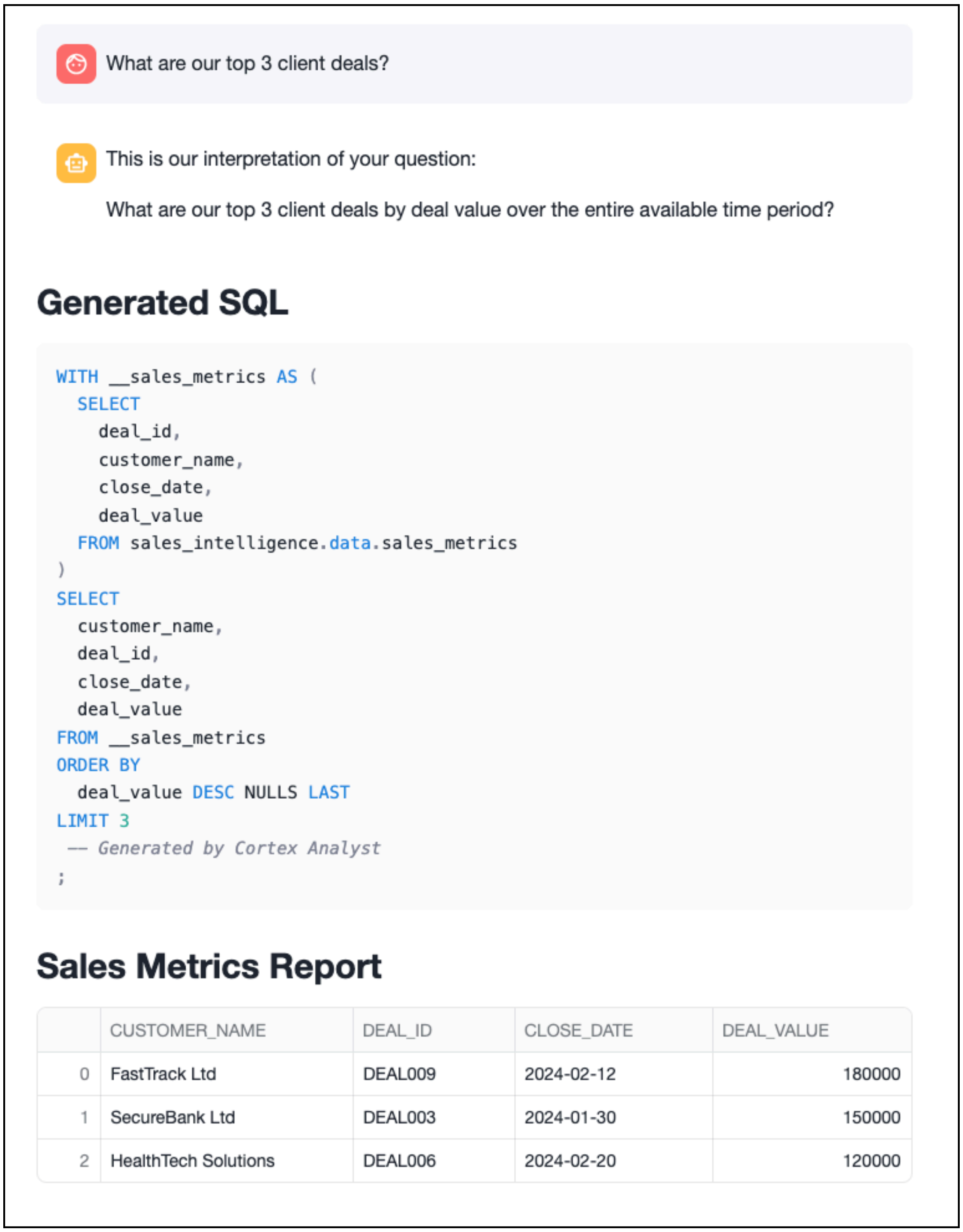
Safeguarding Cortex with Trust3

Use Case 1: Auditing conversations with Cortex Analyst using Trust3

- Ask below question in your streamlit application

  What are our top 3 client deals?

- You will get the reply from the streamlit application as shown in below screenshot



What are our top 3 client deals?

This is our interpretation of your question:

What are our top 3 client deals by deal value over the entire available time period?

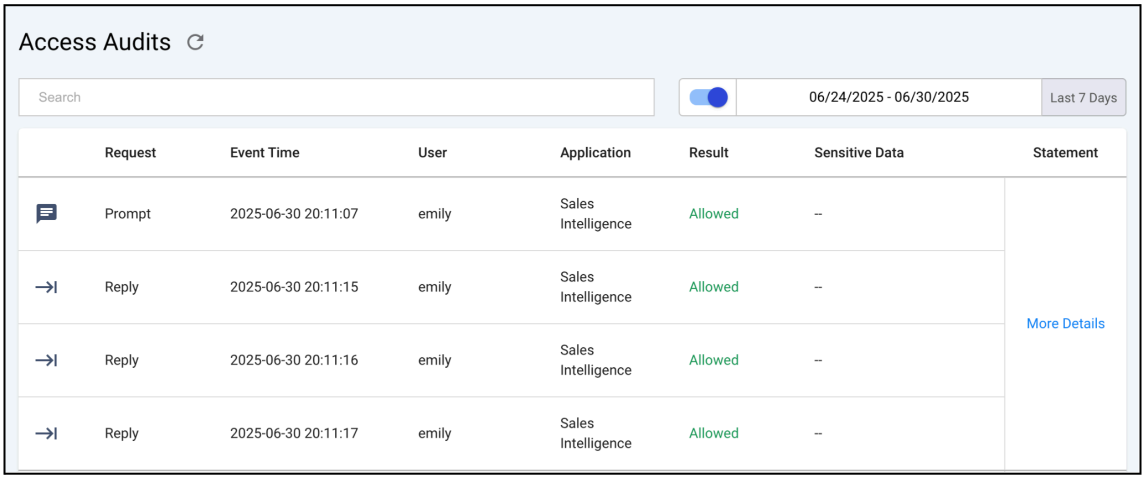
Generated SQL

```
WITH __sales_metrics AS (
  SELECT
    deal_id,
    customer_name,
    close_date,
    deal_value
  FROM sales_intelligence.data.sales_metrics
)
SELECT
  customer_name,
  deal_id,
  close_date,
  deal_value
FROM __sales_metrics
ORDER BY
  deal_value DESC NULLS LAST
LIMIT 3
 -- Generated by Cortex Analyst
;
```

Sales Metrics Report

	CUSTOMER_NAME	DEAL_ID	CLOSE_DATE	DEAL_VALUE
0	FastTrack Ltd	DEAL009	2024-02-12	180000
1	SecureBank Ltd	DEAL003	2024-01-30	150000
2	HealthTech Solutions	DEAL006	2024-02-20	120000

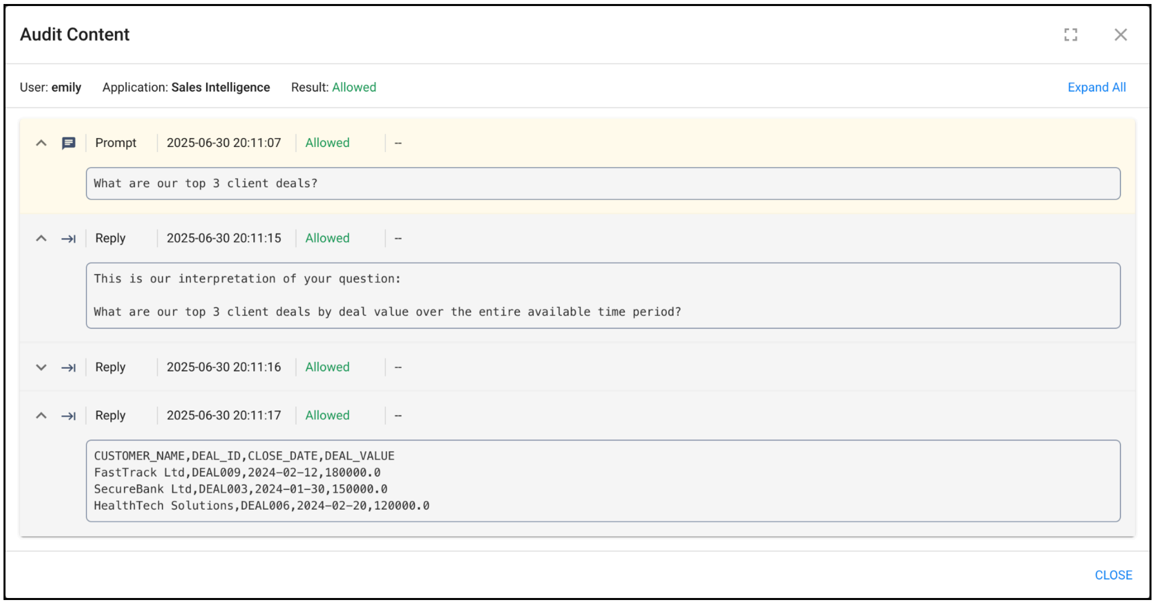
- To check the audits for this conversation, you can navigate to the **Access Audits** within **Observability** on **Trust3 Portal**
- You will be able to see the top most entry for our recent conversation



Access Audits

	Request	Event Time	User	Application	Result	Sensitive Data	Statement
	Prompt	2025-06-30 20:11:07	emily	Sales Intelligence	Allowed	--	More Details
→I	Reply	2025-06-30 20:11:15	emily	Sales Intelligence	Allowed	--	
→I	Reply	2025-06-30 20:11:16	emily	Sales Intelligence	Allowed	--	
→I	Reply	2025-06-30 20:11:17	emily	Sales Intelligence	Allowed	--	

- Further, you can click on the More Details to see prompt and responses related to that conversation thread, you can expand each section as shown in below screenshot to get more details



Audit Content

User: emily Application: Sales Intelligence Result: Allowed

Prompt | 2025-06-30 20:11:07 | Allowed | --

```
What are our top 3 client deals?
```

Reply | 2025-06-30 20:11:15 | Allowed | --

```
This is our interpretation of your question:

What are our top 3 client deals by deal value over the entire available time period?
```

Reply | 2025-06-30 20:11:16 | Allowed | --

Reply | 2025-06-30 20:11:17 | Allowed | --

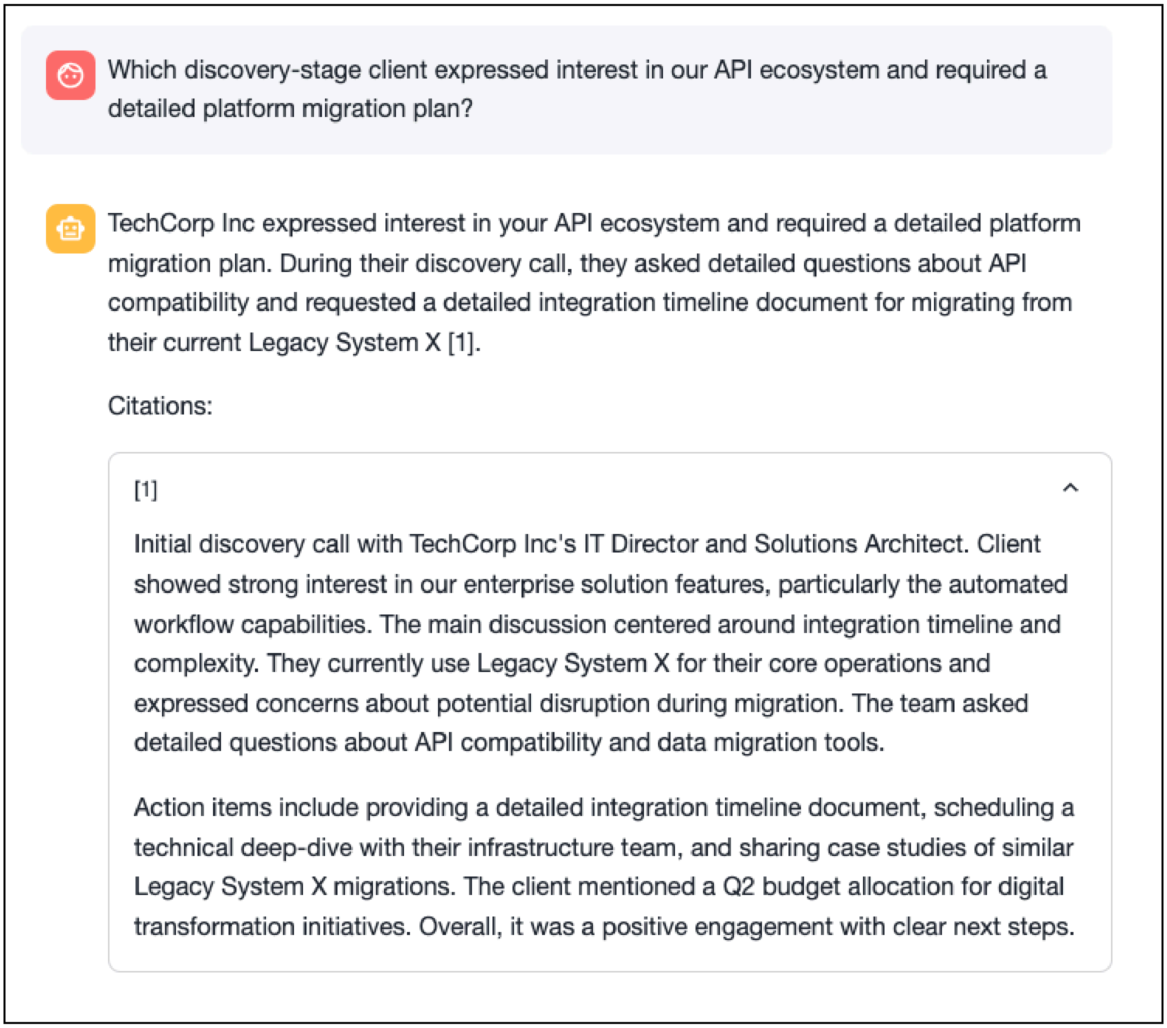
```
CUSTOMER_NAME,DEAL_ID,CLOSE_DATE,DEAL_VALUE
FastTrack Ltd,DEAL009,2024-02-12,180000.0
SecureBank Ltd,DEAL003,2024-01-30,150000.0
HealthTech Solutions,DEAL006,2024-02-20,120000.0
```

Use Case 2: Safeguarding conversations with Cortex Search using Trust3

- Switch the role in snowsight to **account_executive** role
- Start the streamlit application and ask the below question

  Which discovery-stage client expressed interest in our API ecosystem and required a detailed platform migration plan?

- You will get the reply from the streamlit application as shown in below screenshot



Which discovery-stage client expressed interest in our API ecosystem and required a detailed platform migration plan?

TechCorp Inc expressed interest in your API ecosystem and required a detailed platform migration plan. During their discovery call, they asked detailed questions about API compatibility and requested a detailed integration timeline document for migrating from their current Legacy System X [1].

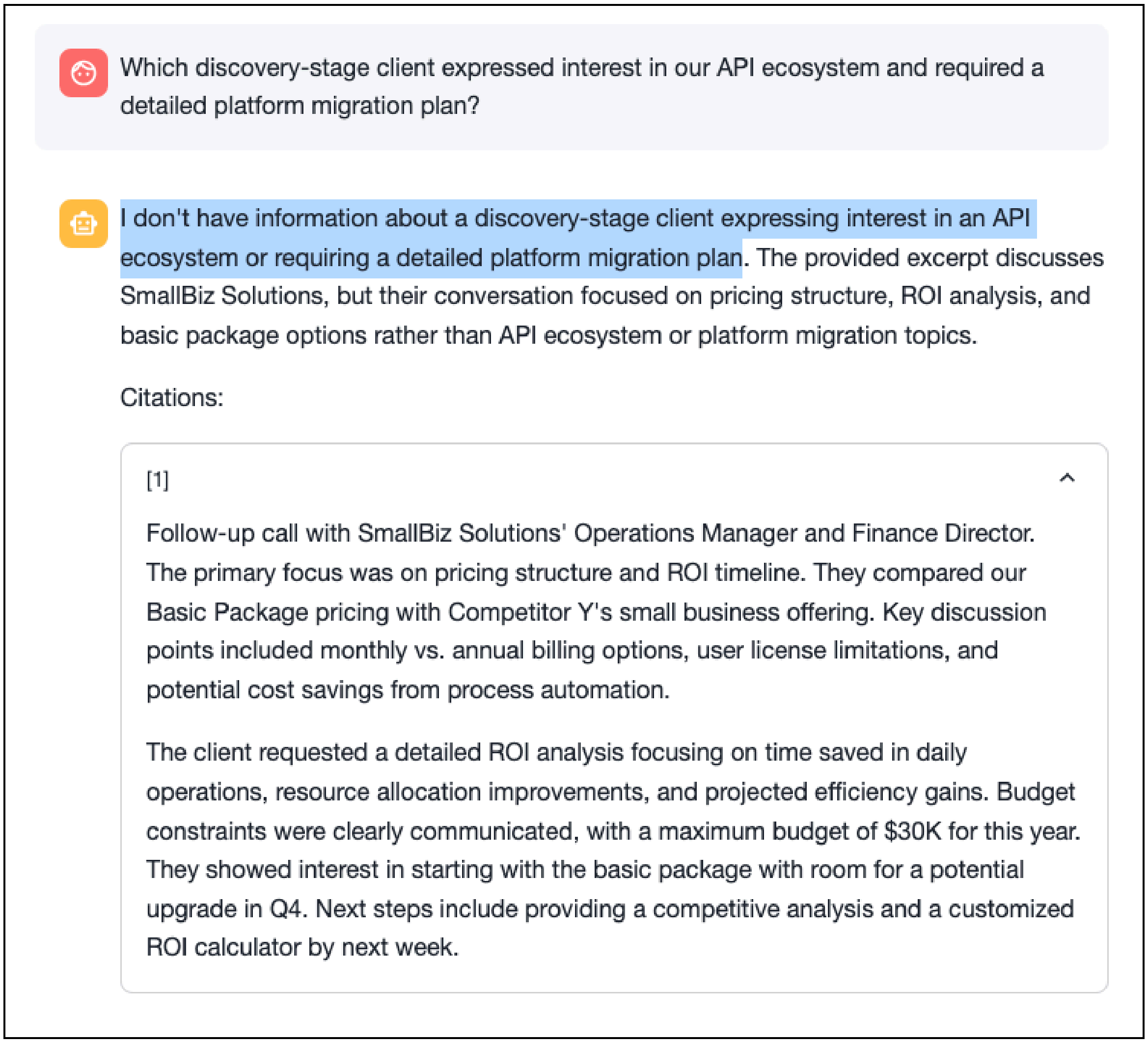
Citations:

[1]

Initial discovery call with TechCorp Inc's IT Director and Solutions Architect. Client showed strong interest in our enterprise solution features, particularly the automated workflow capabilities. The main discussion centered around integration timeline and complexity. They currently use Legacy System X for their core operations and expressed concerns about potential disruption during migration. The team asked detailed questions about API compatibility and data migration tools.

Action items include providing a detailed integration timeline document, scheduling a technical deep-dive with their infrastructure team, and sharing case studies of similar Legacy System X migrations. The client mentioned a Q2 budget allocation for digital transformation initiatives. Overall, it was a positive engagement with clear next steps.

- We have got the expected answer and again we can check the audits for the same on **Trust3 Portal** under **Observability** => **Access Audits**
- Now lets switch the snowsight role to **sales_manager** role and again ask the same question to streamlit application.
- You will now get the reply from the streamlit app as shown below



Which discovery-stage client expressed interest in our API ecosystem and required a detailed platform migration plan?

I don't have information about a discovery-stage client expressing interest in an API ecosystem or requiring a detailed platform migration plan. The provided excerpt discusses SmallBiz Solutions, but their conversation focused on pricing structure, ROI analysis, and basic package options rather than API ecosystem or platform migration topics.

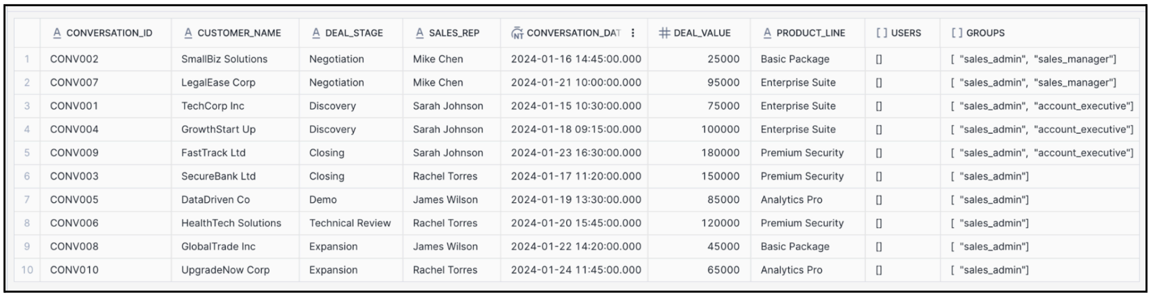
Citations:

[1]

Follow-up call with SmallBiz Solutions' Operations Manager and Finance Director. The primary focus was on pricing structure and ROI timeline. They compared our Basic Package pricing with Competitor Y's small business offering. Key discussion points included monthly vs. annual billing options, user license limitations, and potential cost savings from process automation.

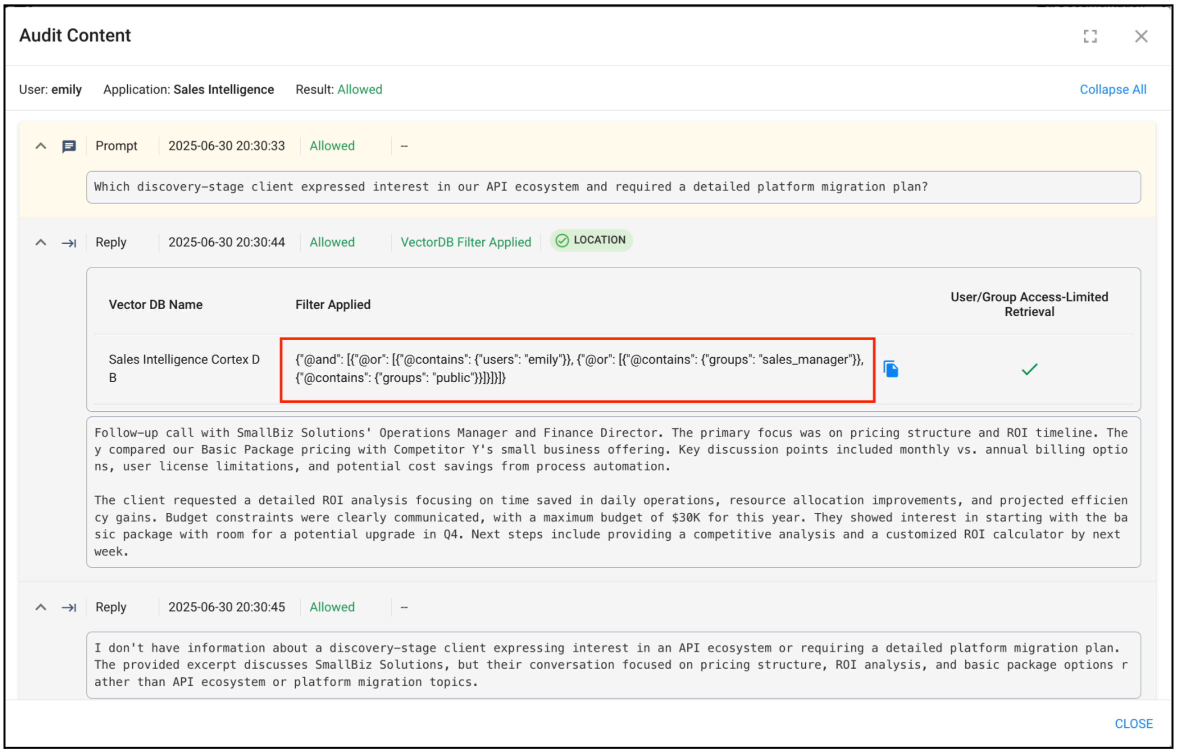
The client requested a detailed ROI analysis focusing on time saved in daily operations, resource allocation improvements, and projected efficiency gains. Budget constraints were clearly communicated, with a maximum budget of $30K for this year. They showed interest in starting with the basic package with room for a potential upgrade in Q4. Next steps include providing a competitive analysis and a customized ROI calculator by next week.

- Notice that now we have not got the same response which we got while running the streamlit application as **account_executive** role, this is because of the Trust3 Dynamic Filtering Capability.
- If you look at the base table which cortex search is querying to get the context documents in order to answer the questions, that has the column as groups, which contains the role names who should have access to the particular record from the table.



	CONVERSATION_ID	CUSTOMER_NAME	DEAL_STAGE	SALES_REP	CONVERSATION_DAT	DEAL_VALUE	PRODUCT_LINE	USERS	GROUPS
1	CONV002	SmallBiz Solutions	Negotiation	Mike Chen	2024-01-16 14:45:00.000	25000	Basic Package	[]	["sales_admin", "sales_manager"]
2	CONV007	LegalEase Corp	Negotiation	Mike Chen	2024-01-21 10:00:00.000	95000	Enterprise Suite	[]	["sales_admin", "sales_manager"]
3	CONV001	TechCorp Inc	Discovery	Sarah Johnson	2024-01-15 10:30:00.000	75000	Enterprise Suite	[]	["sales_admin", "account_executive"]
4	CONV004	GrowthStart Up	Discovery	Sarah Johnson	2024-01-18 09:15:00.000	100000	Enterprise Suite	[]	["sales_admin", "account_executive"]
5	CONV009	FastTrack Ltd	Closing	Sarah Johnson	2024-01-23 16:30:00.000	180000	Premium Security	[]	["sales_admin", "account_executive"]
6	CONV003	SecureBank Ltd	Closing	Rachel Torres	2024-01-17 11:20:00.000	150000	Premium Security	[]	["sales_admin"]
7	CONV005	DataDriven Co	Demo	James Wilson	2024-01-19 13:30:00.000	85000	Analytics Pro	[]	["sales_admin"]
8	CONV006	HealthTech Solutions	Technical Review	Rachel Torres	2024-01-20 15:45:00.000	120000	Premium Security	[]	["sales_admin"]
9	CONV008	GlobalTrade Inc	Expansion	James Wilson	2024-01-22 14:20:00.000	45000	Basic Package	[]	["sales_admin"]
10	CONV010	UpgradeNow Corp	Expansion	Rachel Torres	2024-01-24 11:45:00.000	65000	Analytics Pro	[]	["sales_admin"]

- The **account_executive** role has access to the record we're querying. Trust3 dynamically sends filters to Cortex based on the user's current role, allowing only the **account_executive** to retrieve the related context documents and see the correct answer. In contrast, the **sales_manager** role doesn't have access to that record and therefore couldn't retrieve the correct response.
- You can also view the filter sent to the cortex in the Access Audits details in the Trust3 Portal as below



Audit Content

User: emily Application: Sales Intelligence Result: Allowed

Prompt 2025-06-30 20:30:33 Allowed --

```
Which discovery-stage client expressed interest in our API ecosystem and required a detailed platform migration plan?
```

Reply 2025-06-30 20:30:44 Allowed VectorDB Filter Applied LOCATION

Vector DB Name	Filter Applied	User/Group Access-Limited Retrieval
Sales Intelligence Cortex DB	{"@and": [{"@or": [{"@contains": {"users": "emily"}}, {"@or": [{"@contains": {"groups": "sales_manager"}}, {"@contains": {"groups": "public"}}]}]}]}	✓

Follow-up call with SmallBiz Solutions' Operations Manager and Finance Director. The primary focus was on pricing structure and ROI timeline. They compared our Basic Package pricing with Competitor Y's small business offering. Key discussion points included monthly vs. annual billing options, user license limitations, and potential cost savings from process automation.

The client requested a detailed ROI analysis focusing on time saved in daily operations, resource allocation improvements, and projected efficiency gains. Budget constraints were clearly communicated, with a maximum budget of $30K for this year. They showed interest in starting with the basic package with room for a potential upgrade in Q4. Next steps include providing a competitive analysis and a customized ROI calculator by next week.

Reply 2025-06-30 20:30:45 Allowed --

I don't have information about a discovery-stage client expressing interest in an API ecosystem or requiring a detailed platform migration plan. The provided excerpt discusses SmallBiz Solutions, but their conversation focused on pricing structure, ROI analysis, and basic package options rather than API ecosystem or platform migration topics.

Conclusion and Resources

Congratulations! You’ve successfully built a secure, AI-powered Sales Assistant that not only leverages the analytical and semantic capabilities of Snowflake Cortex, but also integrates Trust3 to ensure enterprise-grade safety, compliance, and control.

This quickstart demonstrated how to:

- Enforce fine-grained access policies and content moderation within LLM interactions
- Monitor and log assistant conversations for auditing and compliance
- Securely analyze structured and unstructured data using Cortex Search and Analyst

By integrating Trust3 with Cortex, you've taken a key step toward building responsible AI applications that meet security, compliance, and governance requirements from day one.

Resources

- AI Trust Layer for Cortex – Snowflake Marketplace
- Trust3 Documentation