

Conversational Analytics: Empowering Admins with Intelligent Insights

Transmit Security simplifies and enhances data analysis by bringing the power of generative AI to customer identity security.

Conversational Analytics is a cutting-edge solution that provides administrators with a powerful ally in their data-driven decision-making journey by allowing them to ask freeform questions about their data, facilitating a more natural interaction with the analytics engine.

This technical brief will explain how admin questions are transformed into SQL queries, then delivered and returned as natural language or rich visualizations while ensuring the best possible security, precision and user experience.

How It Works

1. An admin enters a text question into the admin portal.
2. The question is sanitized and transformed into a prompt using prompt engineering.
3. The AI vendor processes the prompt and generates an SQL query.
4. The SQL query is executed on the secure data warehouse containing the telemetry and recommendation data.
5. The data warehouse results are validated and transformed into the proper format.
6. The formatted data is presented as a text or visual response in the admin portal.
7. Developers conduct frequent assessments by evaluating responses against human-generated and expert-reviewed outputs and use the results to continually retrain the model.

Model Governance

Access

Authentication and authorization is governed by your predefined access controls.

Accuracy

Metadata from each request is used to enrich the query with additional context that helps to generate more accurate results.

Reliability

The system checks the validity of the results against predefined criteria to ensure its reliability.

Data Privacy

Customer data is private and remains in your control. It is never shared to OpenAI or used to train foundation models.

Data Security

Data is protected through OpenAI's highest security standards and our platform's continuous risk and trust assessment.

Example Queries

In the last 24 hours,
what is my denial rate?

How many users were
challenged in the last 30
days?

What are the top 10 IP
addresses associated with
fraudulent activity?

What is the number of
devices that login outside
of the US?

What are the most active
countries outside of the US?

What was the most commonly
reported fraud reason in the
past day?

AI Vendor

We chose OpenAI as our vendor because of their natural language processing expertise and effective handling of freeform queries. By leveraging OpenAI's capabilities, we can ensure that our tool provides accurate and insightful responses to various analytical questions.

Transmit Security uses OpenAI Enterprise API with the highest possible security & privacy standards offered by OpenAI. Read more about their enterprise privacy and security here:

- [Ensuring data privacy](#)
- [Securing customer data](#)

Deep Dive

Data Validation

Validation is a crucial step to ensure the accuracy and reliability of the information presented. The system checks the validity of the results to confirm that the data returned aligns with the intended interpretation of the user's query and that it adheres to the expected data quality standards. Validation processes may include checking for outliers, ensuring consistency with historical data and confirming that the response meets the criteria defined for the specific query type.

Data Transformation

Once the SQL query is executed on the user's data, the raw output is structured as a set of database records, statistical values or other format. This raw output is then transformed into a user-friendly and comprehensible response by mapping the technical results into a human-readable format that is easily understandable by administrators. For instance, numerical results might be formatted into graphs, charts, or simple text explanations, depending on the nature of the query.

Feedback Mechanism

Human reviewers continually assess the model to ensure responses are relevant, logically structured, and demonstrate an understanding of the prompt's context by comparing the model's outputs against benchmark datasets and human-generated responses. These results are used to continually retrain the model and optimize its performance.

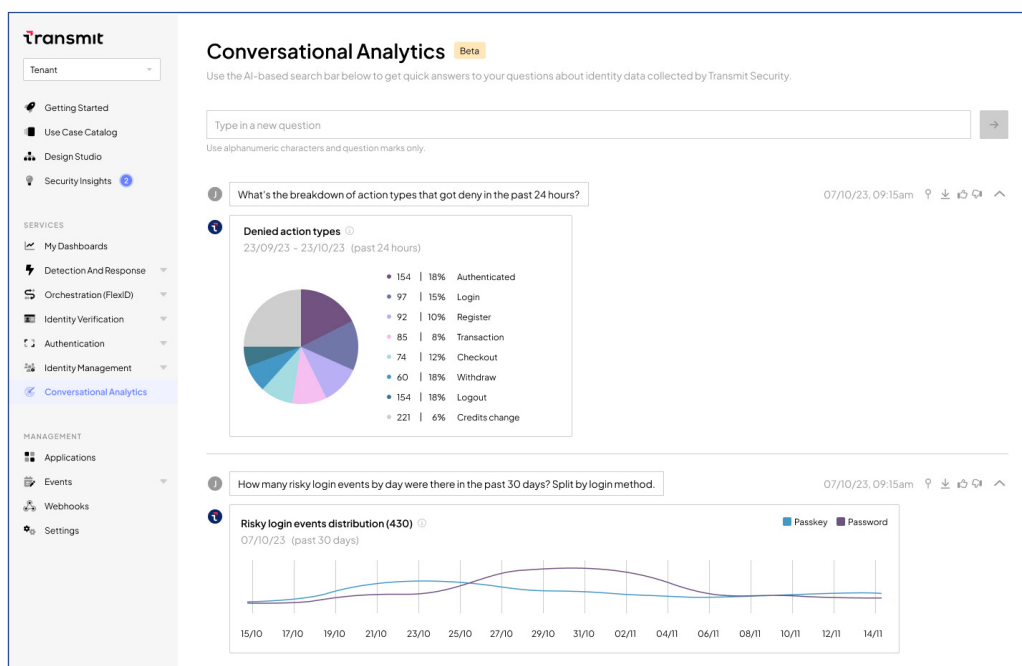
Data Privacy & Security

Our commitment to customer privacy is paramount. Customer data is never shared with OpenAI; only the anonymized prompt is transmitted. Sensitive information such as personally identifiable information (PII) and IPs are masked from the prompt to protect user privacy and ensure our users can confidently engage with the tool without compromising their data security.

To further minimize risk and ensure privacy, security and compliance, each interaction with Conversational Analytics is underpinned by the same authentication, authorization and continuous risk assessment protocols that are used across our entire platform and trusted by some of the largest and most demanding enterprises in the world.

A Closer Look

The Conversational Analytics UI is designed to deliver a user-friendly experience that is integrated with our complete customer identity security platform, enabling admins to query a broad range of user events relating to risk and trust, authentication, identity verification and more. Visualizations and images can be exported directly within the UI to be shared with stakeholders, and the service includes a self-service feedback mechanism to continuously improve responses over time.



Conclusion

Conversational Analytics takes a responsible approach to AI model governance with rigorous controls that ensure data privacy and security, and includes safeguards such as prompt engineering, data validation and self-service feedback to continuously improve the accuracy and usefulness of its results. To read more about how this innovative solution simplifies and enhances data analysis, [click this link](#).