

Securing a Modern Data Mesh in the Snowflake Data Cloud

A leading provider of tax and immigration services—with over 3,000 multinational clients and 5,700 professionals helping enterprises manage complex cross-border workforce challenges—decided to modernize their data platform.

Modernization Goals

- Handle the needs of a growing number of employees and customers with petabytes of data being generated.
- Ensure sensitive and regulated data management with right access to the right team members seamlessly
- Eliminate manual operations to better serve internal and external customers

The Need for a Modern Data Platform

The main goals were to unify customer data, enable self-service analytics, and enhance security and governance. Some of the key challenges facing the team included:

- Customer data was spread across multiple data platforms, which created a technical challenge for providing a unified suite of mobility products.
- Managing sensitive and regulated data posed significant challenges. Their legacy platform demanded extensive time and effort to comply with regulatory requirements from their customers, who were spread over 40 countries and had 500+ analysts. Accommodating individual client rights necessitated the development and maintenance of intricate workflows. This complex process diverted resources from strategic initiatives, hindering agility when responding to client needs.
- IT teams manually provisioned consistent access controls for internal employees across multiple data platforms.
- A need to provide external customers access to reports, analytics & insights from their datasets.
- The old, on-premise architecture slowed down addressing complex real-time data analytics use cases.

Business Impact



Improved Operational Efficiency in Terms of User Onboarding



Faster Access to Data from Days to Hours



Removed risk by uncovering numerous access violations



One Policy to Manage 1000's of Users

Access & Compliance Requirements for Building the Platform

- A framework that can consistently enforce policy-based access controls regardless of where the data is consumed
- A platform that can support access controls based on dynamic business rules for a large pool of data workers, that include internal employees, external clients, service accounts, and bots
- Empower data stewards and data owners to manage access controls, data access requests and define/manage metadata for their responsible data sets.
- Enable data consumers to self-serve data access requests - discover the data products in internal marketplace and request access.
- Balance decentralized data ownership with centralized visibility and control
- Provide a seamless, secure data consumption experience across channels
- A centralized platform to provide evidence of compliance and audit requests
 - Easily identify any data misuse or overly assigned permissions
 - Ensure the visibility to governance team what data is moving

Solution

To address these challenges, a modern data mesh on Snowflake was built. Snowflake provides near-infinite scalability and enables a single source of governed data.

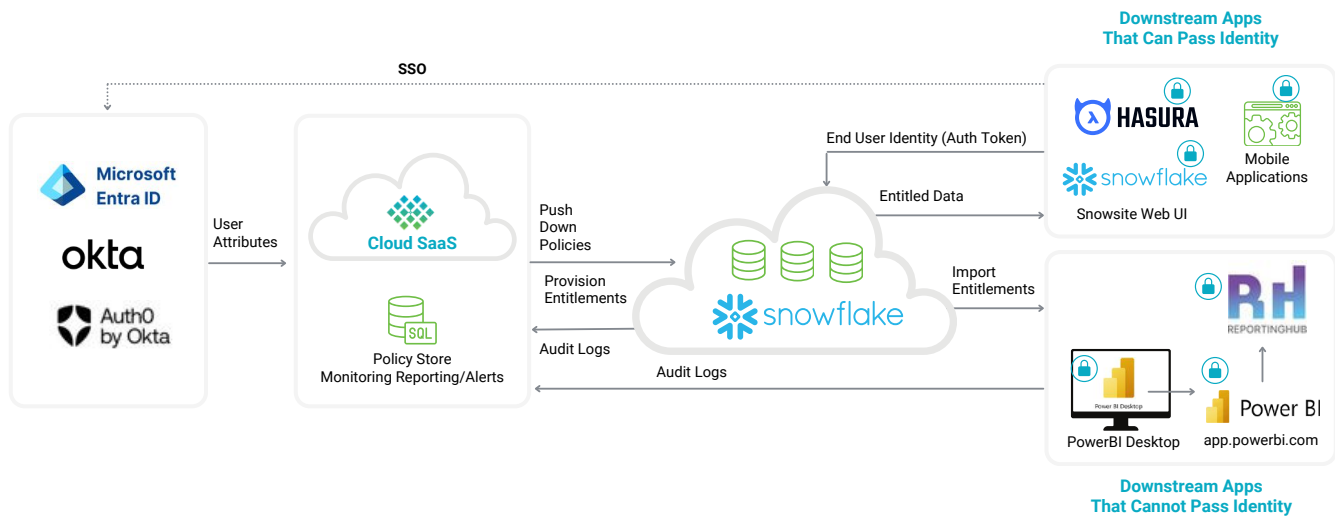
Securing the Data Mesh with TrustLogix

- TrustLogix policy-based access controls and entitlements integrate with Snowflake to ensure fine-grained data protection across the data products for data workers. Leveraging Role-based access control (RBAC) and Attribute-based access control (ABAC), TrustLogix enables policy automation based on user attributes and classification meta-data.
- Data products are organized within Snowflake using a tagging taxonomy defined in TrustLogix.
- Domain stewards manage access policies to their data products using TrustLogix Entitlements framework, while global policies ensure baseline protections.

“

Our data products with petabytes of extremely sensitive PII information and 500+ data analysts over 40 different countries necessitate us to comply with 100+ local regulations. Snowflake multi-tenancy architecture helped us to build the sophisticated data products, **only TrustLogix was able to build out the granular access controls that our CISO endorses while also meeting the lightning-fast data access that our biggest stakeholders require.** The combined approach has become a major competitive advantage for us.

”



Solving Complex Use Cases

Multi-channel Data Consumption

User Entitlements defined in TrustLogix policies ensure that PowerBI dashboards, GraphQL APIs like Hasura, and mobile apps receive filtered and masked data.

Example: a data engineer wants to connect the data and perform some development activity for a specific domain. The TrustLogix user entitlement and policy definition enable the data engineer to consume the same data via multiple interfaces.

Proactive Security & Visibility of Data Sprawl

TrustLogix provides the Data Governance team with real-time visibility into data movement, alerts on sensitive data sharing between accounts, and enables remediation actions to mitigate security risks promptly.

Entitlement & Activity Reports

TrustLogix offers compliance features including change tracking, access history, data lineage, role management, and permission management, allowing the Data Governance team to generate centralized audit reports for SOX, SOC2, and GDPR compliance.

Customer Isolation

Customers can only access their own data within the data mesh based on TrustLogix ABAC Policies and Entitlement entries. Strict tenant isolation is ensured without sacrificing analytics performance.

Example: customer data access can be confined to data product(s) via entitlement entries in TrustLogix.

Least Privilege Access

Contributors are provisioned access to specific data projects. Sensitive immigration and tax data is masked per policy.

Automated Access Requests

The Governance team leveraged TrustLogix APIs to implement a custom data access request workflow to manage user entitlements, allowing data owners to deliver discoverable data products and enabling self-service for data consumers, reducing time to access insights and reports.

Benefits Realized



Seamless, secure data access

Business teams gain easy access to permissioned data in their tools or channels of choice.



Scalable policy management

ABAC streamlines policy creation and maintenance across hundreds of customers.



Unified governance

Security and compliance teams can now centrally manage and audit all data access.



Faster access to data and reduced manual process

Through self-service access requests, the governance team has enabled both internal and external data consumer access to newer data products easily and faster.

Summary

By combining Snowflake's scalable platform features with TrustLogix Data Security Platform, the Global Mobility vendor streamlined secure data access and auto-enforced governance, while empowering users with seamless self-service analytics across channels.