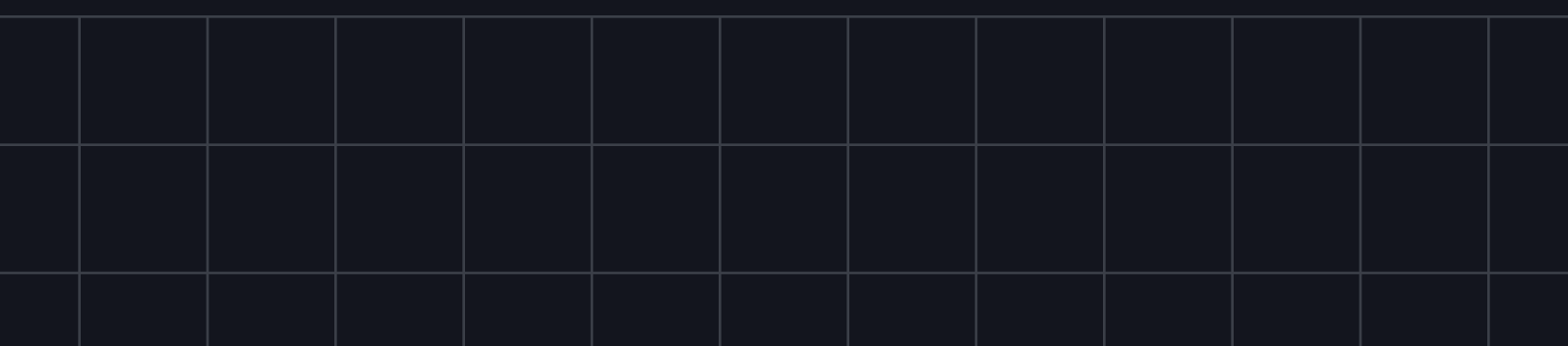




CASE STUDY

Australian Insurance Provider Strengthens Data Security to Better Serve 1.75M Customers






top insurance co.

ARCHITECTURE


 IMMUTA

 snowflake

 Buildkite

sumo logic

 dbt

 + a b | e a u

 okta

INDUSTRY

Financial Services

Key Takeaways

- A top Australian insurance provider's existing on-prem data stack was siloed, resource-constrained, and cumbersome to manage. The company migrated its data to Snowflake and Immuta to secure personally identifiable information in full compliance with privacy regulations.
- Greater transparency and collaboration between data, security, and governance teams improves operational efficiency throughout the enterprise.
- Deeper analytics empowers customers to improve health outcomes through greater accessibility to affordable health services and information.

One of Australia's leading insurance companies provides health coverage to more than 1.75 million residents of Australia and New Zealand. In addition to being a premier health insurer in New Zealand, they rank among Australia's largest travel insurers and are a global distributor of travel insurance, providing financial protection and assurance to travelers wherever they are in the world.

This insurance provider recognized the need to modernize their IT infrastructure to better serve their customers. Their existing data stack was siloed, resource-constrained, and cumbersome to manage. The company thus embarked on a technology-led business transformation, migrating their data to Snowflake and securing it with Immuta.

Challenge

Given that the insurance provider operates in a highly regulated industry subject to a wide range of legal requirements from agencies like the Australian Prudential Regulation Authority, they needed a best-in-class data security platform to protect sensitive data as it was migrated to Snowflake. The company's homegrown, role-based access control solution posed several challenges, including scope creep, undocumented features prone to failure, and mounting data creation and usage. To remedy this, the company built its new data infrastructure with Snowflake's viewless integration while using dbt to programmatically manage data.

The company also wanted to both get a better handle on the personally identifiable information (PII) in their system—such as name, age, and medical conditions—and to automate access for their different business groups, including customer service, finance, and human resources. The goal was to create a new, automated system secured with access controls while simultaneously increasing data accessibility across the enterprise.

The insurance provider's philosophy was to enable broad access with more strict masking policies on PII data. "You need to have a culture of automation, an understanding of how all the bits hold together, and how you're going to govern that," said a senior engineering manager at the company. "You need to have tools like Immuta in place."

"You need to have a culture of automation, an understanding of how all the bits hold together, and how you're going to govern that. You need to have tools like Immuta in place."

Solution

“Snowflake on the output side allows us to securely talk to external organizations with PII data,” the engineering manager said.

“We use Immuta on the inside for who can access what; who are you and should you be looking at this?” The company started with two main use cases for Immuta:

Use Case 1: Simplify Data Access Control

- **Problem:** The insurance provider’s existing data access control model was brittle and often granted users exceptions from standard access. They wanted a system to automate access and control user access sprawl.
- **Solution:** Subscription policies based on business unit and data user job seniority are mapped to tags placed on tables according schema, enabling data protection that is comprehensive yet simple and scalable.

Use Case 2: Enhance Sensitive Data Discovery

- **Problem:** The insurance company lacked a complete picture of where their sensitive data resided and were concerned about the security risks of this data potentially being overlooked and exposed. As data sets were repeatedly copied and shared, they lost insight into who has what data and how it’s being used.
- **Solution:** Immuta’s sensitive data discovery (SDD) automatically detects and classifies sensitive data. This enables the insurance provider to create high-level policies that can apply masking policies as soon as new data is ingested into Immuta without time-consuming, error-prone processes. For example, when a new insurance claim is submitted, protected health information is tagged so that the claims department can see this data while the finance department cannot.

“The exciting part of ABAC is being able to talk to our cybersecurity people and our governance people with a system that resembles the regulations.”

The insurance provider's new attribute-based access controls (ABAC) enabled several beneficial capabilities and process efficiencies: policies aligned to regulations; data categories clearly linked to access; integration with data product development; and time-limited access. "The exciting part of ABAC is being able to talk to our cybersecurity people and our governance people with a system that resembles the regulations," the engineering manager said. Immuta's intuitive policy builder enables data stakeholders to build rules in plain language consistently across any data. Because rules are driven by metadata that anyone can understand, it becomes possible for teams to build proactive consensus on how to protect data instead of refactoring models after the latest policy initiative.

Top-level tags are managed in real time with dbt while Immuta enforces policies and applies column-level tags to tables for more granular detail. The way that data assets are tagged in internal dbt projects determines the extent to which a user will have access to it. "ABAC simplifies managing the data sets that you're building up," the engineering manager said. "It means we don't have to proliferate our dbt projects and models quite so much, and it can be a lot more flexible over time."

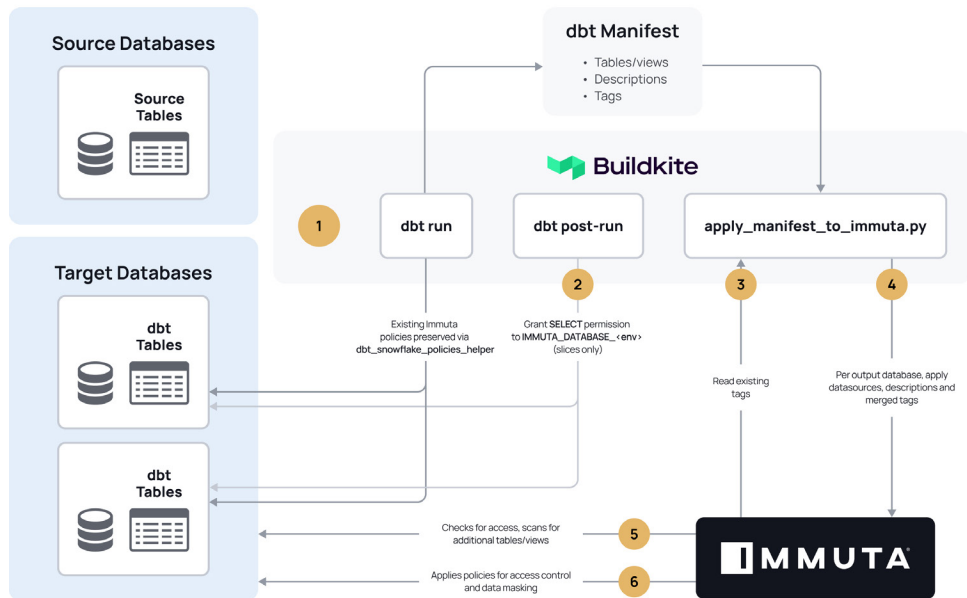
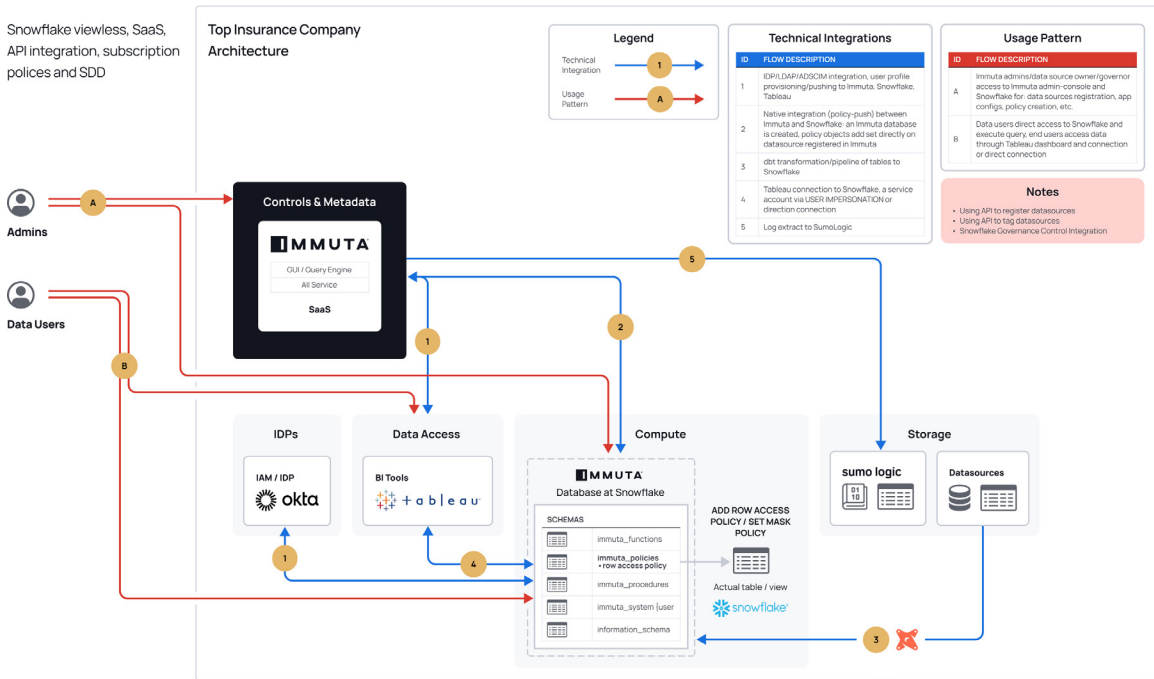
Outcome

The insurance company's Immuta implementation has resulted in several business and process improvements. Policies were applied to data just weeks after the data were loaded into Immuta. The company now has thousands of data sources in Immuta with more than 400 users accessing data from more than 17,000 sources via nine global subscription policies.

"ABAC simplifies managing the data sets that you're building up. It means we don't have to proliferate our dbt projects and models quite so much, and it can be a lot more flexible over time."

With Immuta's Data Security Platform, the insurance provider has fortified their data security and access control to better protect sensitive PII. "We want to help people live healthier lives," the engineering manager said. "That's why we want to understand more about who they are and their specific health needs." The company's data stack is now more robust than ever and drives their technology-led business transformation in compliance with industry regulations. At the same time, deeper analytics empower customers to improve health outcomes through greater accessibility to affordable health services and information.

Architecture



About Immuta

Immuta is the leader in Data Security, providing data teams one universal platform to control access to analytical data sets in the cloud. Only Immuta can automate access to data by discovering, protecting, and monitoring data. Data-driven organizations around the world trust Immuta to speed time to data, safely share more data with more users, and mitigate the risk of data leaks and breaches. Founded in 2015, Immuta is headquartered in Boston, MA.

