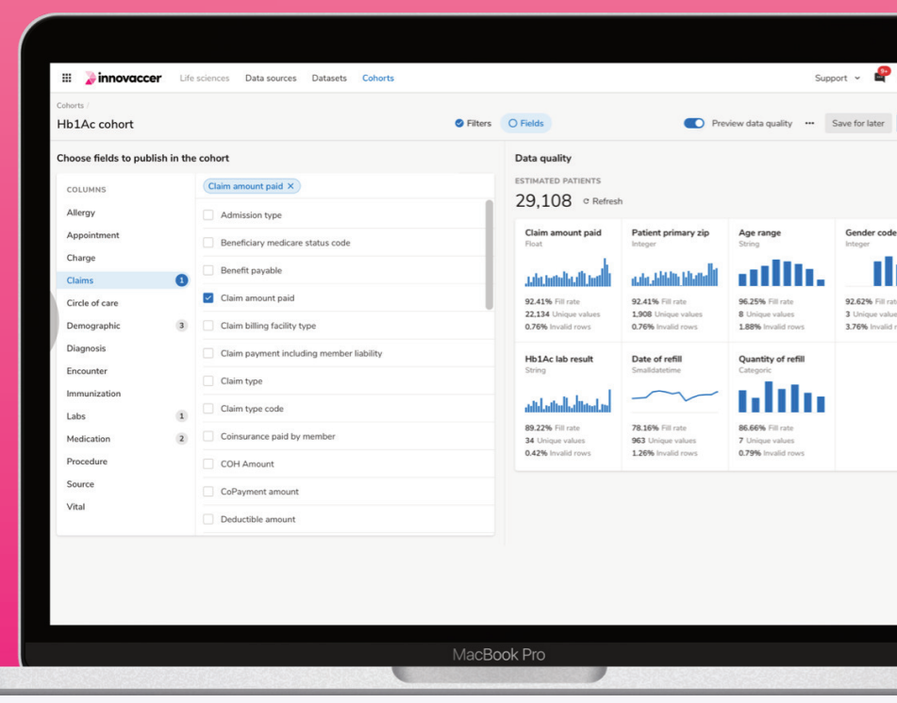
innovaccer

Innovaccer secures sensitive protected health information (PHI), while powering hyper-growth

Protecting sensitive data in Amazon Redshift, Snowflake, Azure SQL and Postgres in AWS and Azure Cloud



About Innovaccer

Innovaccer Inc., the Health Cloud company, is dedicated to accelerating innovation in healthcare. The Innovaccer® Health Cloud unifies patient data across systems and care settings, and empowers healthcare organizations to develop scalable, modern applications that improve clinical, financial, and operational outcomes. Innovaccer's solutions have been deployed across more than 1,600 care settings in the U.S., enabling more than 96,000 providers to transform care delivery and work collaboratively with payers and life sciences companies. Innovaccer has helped its customers unify health records for more than 39 million people and generated over $1B in cumulative cost savings. Innovaccer is the #1 rated Data and Analytics Platform by KLAS, and the #1 rated population health technology platform by Black Book.

Size:
1000 - 1500 Employees

Location:
San Francisco, California

Industry:
Healthcare Technology

Business Need

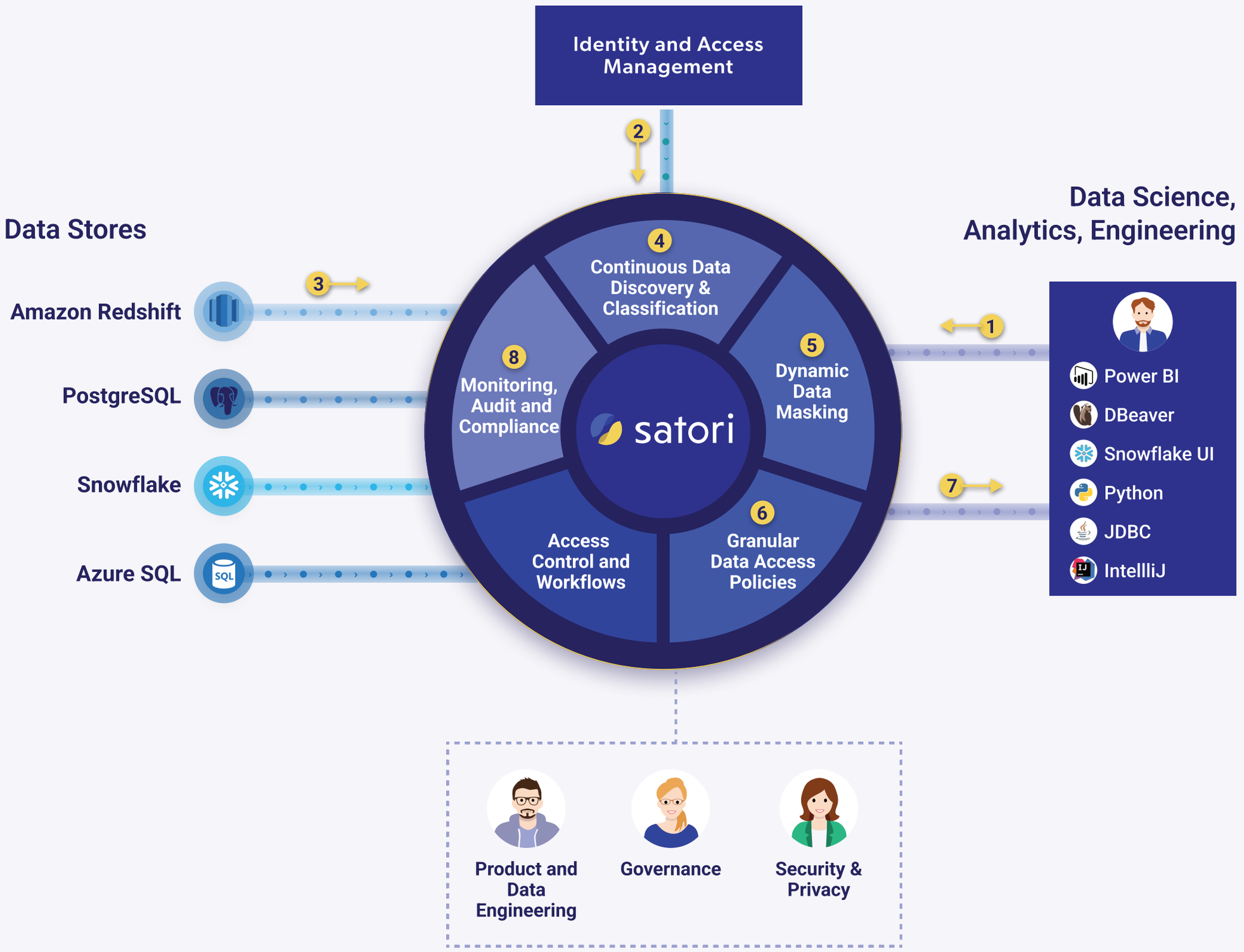
Innovaccer's health cloud integrates dispersed clinical and payer data from multiple practices, hospitals, and systems. Advanced data analytics delivers insights with population stratification displayed through customizable dashboards. Customers such as Banner Health, Adventists Health and Children's Health Alliance now have a unified view of patient data across e-Health record systems.

Innovaccer's innovative healthcare approach relies on its analysts' ability to work quickly with sensitive protected health information (PHI) while also ensuring that access is monitored and controlled. Given the large variety of data technologies, cloud providers and use-cases, the application of security policies to protect PHI data has to be done without compromising business growth or security.

Innovaccer's product engineering and information security leadership realized that they needed a data security platform that can connect multiple data platforms containing patient data, identify and tag sensitive data and obfuscate the relevant fields based on the user's access privileges. Innovaccer required a security platform that applies data masking policies without requiring access to the data.

Securing Sensitive Data at Innovaccer with Satori

1. Engineers, analysts and data scientists query Amazon Redshift, Snowflake, Azure SQL and Postgres through Satori via multiple BI and other tools including **Microsoft Power BI, DBeaver, Snowflake UI, Python, JDBC and IntelliJ.**
2. **Satori** gets the user context from **Innovaccer's identity and Access Management (IAM)** platform.
3. **Satori** applies access policies and sends the queries to the data stores.
4. **Satori** inspects and classifies the result dataset.
5. **Satori** applies security policies such as data masking to PII and PHI data to protect it as per the user's access privileges.
6. **Satori** applies granular access control policies such as ABAC to the result dataset as per the user's access privileges and attributes.
7. The user gets the anonymized query result in their BI tool or other tools.
8. Data privacy, security, and compliance teams monitor access to sensitive PII and PHI data with out-of-box reports.



Result

Innovaccer deployed Satori as their data security platform solution in just 90 days across four data store technologies including Amazon Redshift, Snowflake, Azure SQL and Postgres. Satori's data security platform delivers secure access to sensitive data in over 120 data stores with 10 active Data Access Controllers (DACs), supporting millions of queries per month.

Security engineers configure and maintain security policies in a simple, timely way. Hundreds of users from analytics and engineering teams use multiple BI and analytics platforms including Microsoft Power BI, DBeaver, Snowflake UI and Python, JDBC and IntelliJ clients and query the data stores containing patient data via Satori. Satori integrates with the identity and access management platform for retrieving users' roles and attributes. The pre-defined roles and attributes determine whether or not to grant the user access to data and the applicable security policies.

Satori's data security platform delivers the following business functionality for Innovaccer:

1. **Identify PII and PHI data in real-time, as the data is being retrieved for queries. Satori ensures that Innovaccer has a continuously updated data inventory, and security policies are also applied on newly discovered sensitive data.**
2. **Enforce dynamic data masking following Innovaccer's sensitive data security access policies based on the user's identity and attributes.**
3. **Apply data filtering using Innovaccer's security policy for the row, role, and attribute-based access control based on the user's identity, department, function, and data type.**

Additionally, the privacy, security, and compliance teams utilize pre-built reports for monitoring access to sensitive PII and PHI data.

"Satori's service is a real game changer, providing both control and visibility over data compliance and security issues across multiple data stores. We were able to deploy Satori quickly because it does not require making any changes in existing data flows."

innovaccer

Arun K. Buduri, VP Engineering, IT & CISO, Innovaccer

Benefits of Satori's Platform

No changes to schema or configuration for the data stores.

Seamless integration with user identity based on IAM integration.

Data classification, masking and filtering for PII and PHI data in Amazon Redshift, Snowflake, Azure SQL and Postgres with security policies.

Pre-built comprehensive audit trail and reporting for privacy, security and compliance.

Non-intrusive deployment for end-users allowing them to continue working with their preferred BI and analytics platform or client without any additional training, query changes, or driver installations.