Dynamic Authorization for Data Lakes

Leading data cloud platform, Snowflake, enables enterprises to gain valuable insight from disparate data sources and types. With the rapid growth of data, there is growing pressure on enterprises and their security and data teams to ensure data is not exposed to unauthorized users.

Authorization has traditionally been built into individual, homegrown applications. However, this method is not scalable nor secure. Data that was protected by the application's authorization has moved to the data lake or data warehouse. Rules that were built for original databases must be rebuilt for Snowflake in order to secure data access across all applications.

PlainID eliminates these challenges by externalizing authorization and centralizing its management via The PlainID Authorization Platform. Enforcement is then distributed to the **PlainID Authorizer for Snowflake** which sits at the data layer and addresses data security at scale and dynamically for all users who access Snowflake for business intelligence and data projects.

For example, when a user attempts to access data, the Authorizer intercepts data requests made to Snowflake and checks whether they meet the prescribed conditions (e.g. location, risk score, etc.). Stricter conditions can be set for sensitive data down to the row, column, and even cell-level.

Ultimately, PlainID strengthens data security for Snowflake by ensuring users are only able to see certain data based on who they are, and where they're accessing the data from.

Benefits

Unified Policy Management
Manage access to Snowflake data objects with PlainID's graphical UI to provide consistent access decisions across enterprise applications.

Coarse & Fine-grained Authorization
Enforce fine-grained controls at a granular level by determining what rows/columns/cell data are exposed to the authorized user.
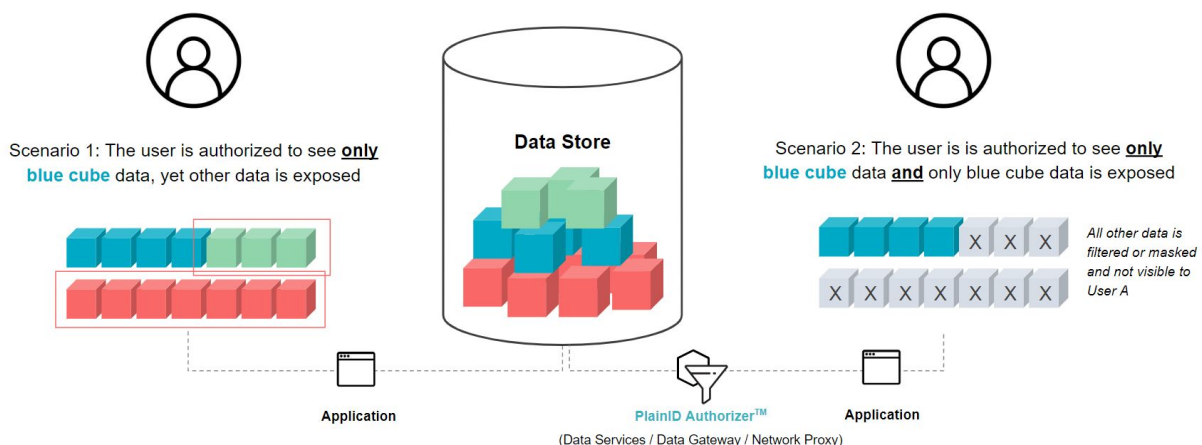
Full Visibility of Data Access
Gain bi-directional view of the relationship between users and data assets and investigate the attack surface of sensitive data.

Consistently Control Data
Deliver control over data across any layer in the stack by externalizing authorization with the PlainID Authorization Platform.

Improving Data Security & Application Performance

Scenario 1: The user is authorized to see **only blue cube** data, yet other data is exposed

Data Store

Scenario 2: The user is is authorized to see **only blue cube** data **and** only blue cube data is exposed

All other data is filtered or masked and not visible to User A

Application

PlainID Authorizer™
(Data Services / Data Gateway / Network Proxy)

Application

Authorization for Snowflake
Securely connecting identities to digital assets,
Powered by Policy Based Access Control (PBAC)

plainID
THE AUTHORIZATION COMPANY
+
snowflake

Dynamic Authorization at Query Runtime

Data is traditionally accessed without authorization of the user in mind. It's often fetched using a service account, with too many permissions. Applications will typically retrieve all data and mask information at the middleware or service mesh layer, which creates vulnerabilities for sensitive data.

The PlainID Authorizer for Snowflake dynamically modifies the query at runtime to return only data the user is authorized to see. A simple example from this:

```
select * from sales_table;
```

Whereas, PlainID's Policy-based Access Control (PBAC) restricts the query to return data only in the user's assigned region:

```
select name, company, amount from sales_table where sales_table.region = {user.region};
```

Solution Architecture
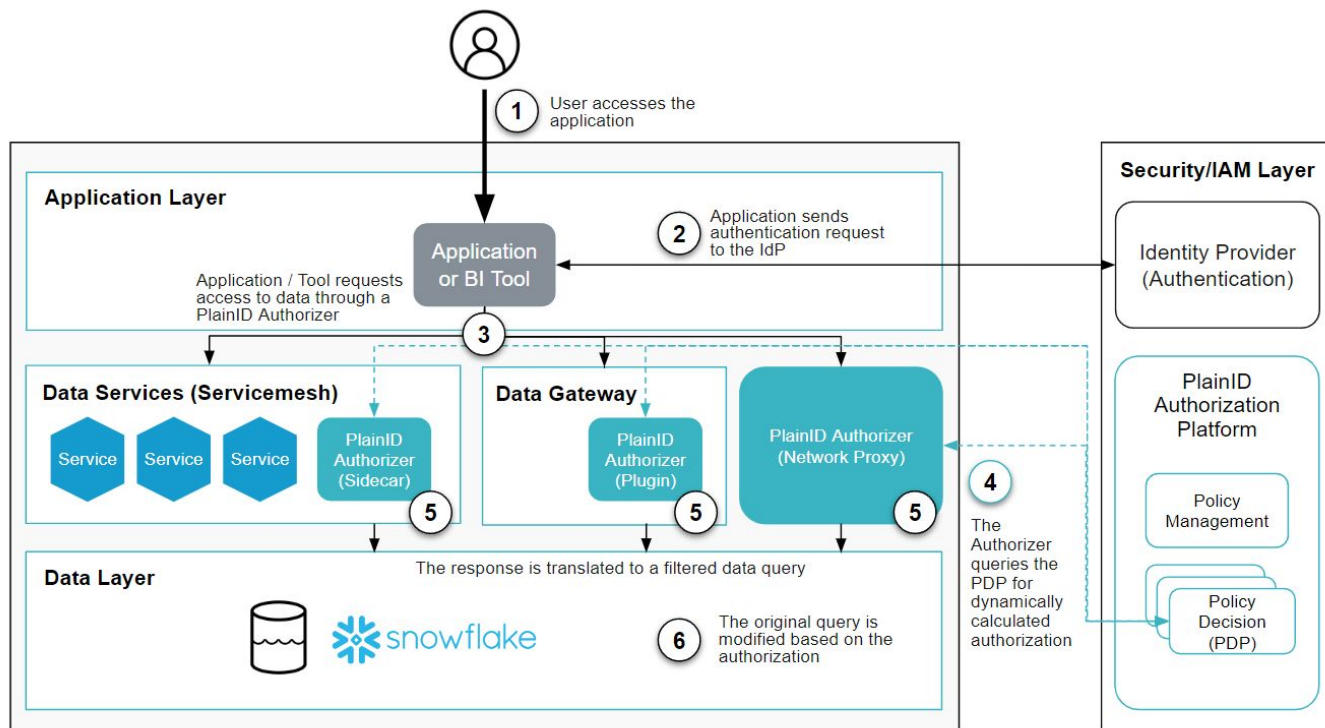
About PlainID

PlainID, the Authorization Company, simplifies the complexity businesses face when securely connecting identities to digital assets. Powered by PBAC, PlainID provides a SaaS-based, centralized policy management platform with decentralized enforcement to manage who can access what across the enterprise technology stack; including applications, data, API, microservices and more.

Visit Us