

# PlainID & Data Virtuality

## Dynamic Authorizations for Data

### About PlainID

PlainID is the Authorization company providing advanced IAM solutions that focus on dynamic, fine-grained access controls.

### About Data Virtuality

Data Virtuality provides data integration solutions that help companies to easily connect and manage data from multiple data sources such as APIs, databases and flat files.

## PlainID has partnered with Data Virtuality to provide advanced solutions for dynamically controlled access to data.

### Controlled access to data

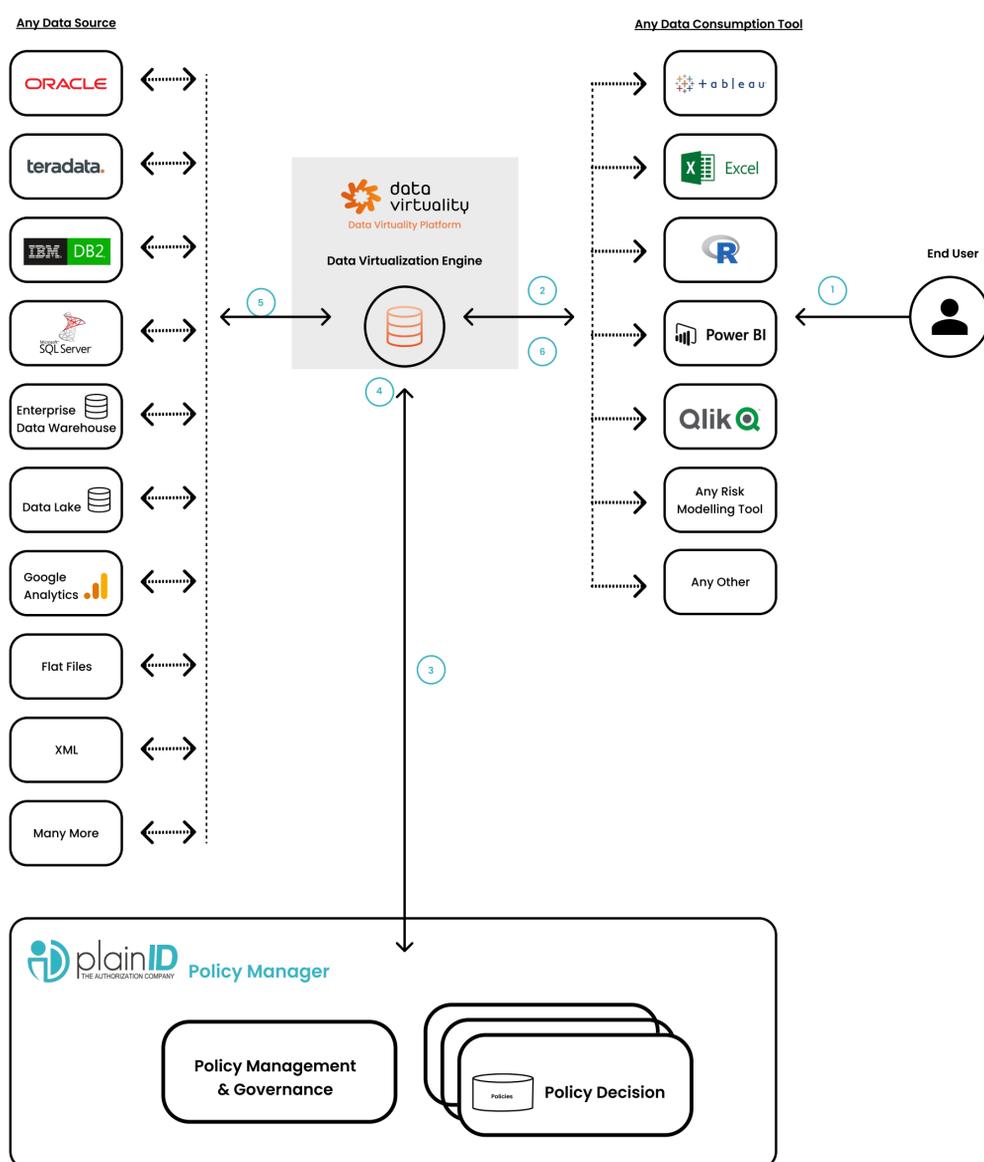
Consistently protecting the same data assets across different databases is a challenge that many data owners struggle with. Often there is a lack of transparency around the authorizations that are enabled due to the different layers of permissions that can surround a database. In addition, most repositories do not support built-in fine-grained access controls.

### Policy Manager provides the policies to dynamically control fine-grained access to data, and Data Virtuality provides the enforcement layer

PlainID Policy Manager together with Data Virtuality Platform, offers unique support for database adaptive access. The integration is designed to add/modify the SQL query the application/user is trying to perform so that only authorized data is processed. The main benefits of this solution are:

- **Dynamic authorizations for data** – Address security and risk management requirements with dynamic authorization for just in time access decisions, considering who the user is, what they are trying to access and any relevant environmental conditions.
- **Fine-grained access solution** – Use an access solution that supports fine-grained access controls, both on row and column level.
- **Unified access management** – Manage access to data objects using a unified interface, that provides consistent access decisions.
- **Central enforcement layer** – Implement a central, unified enforcement layer for your data across your digital landscape.
- **Databases and connectors** – More than 200 ready to use connectors, providing wide coverage for consistent data access enforcement.

### Solution high-level architecture



### Architecture flow:

1. Authenticated users access the application/service.
2. Applications and services use the Data Virtuality Platform to access the data.
3. Data Virtuality Platform sends a "policy resolution" request and receives a decision from the Policy Manager PDP at the time of access.
4. The response is translated to a data filtering clause and a list of authorized data elements, this is used to modify the original data query.
5. The data request continues to the relevant repository with the modified query.
6. Required data, with the filtering based on the access controls, is sent back to the application.

### Solution main benefits

#### Dynamic access controls

Access is determined based on user attributes and context of access, at the time of access.

#### Fine-grained controls

Fine-grained controls are enforced on both column and row levels. Addition of dynamic filters to the query, reduces the need to create views to control access, thus providing the missing flexibility and reducing the management overhead.

#### Investigate access

The policy administration UI enables investigation of access on both user and data asset perspectives.

#### Consistent access decisions

Access is controlled on both the data level and application level, providing consistency in decisions across the digital landscape.

#### Unified view of access controls

The policy administration UI provides unified view and understanding of access on the different levels of access control.

#### Controlled management and deployment

Managing and changing access controls is done in a sandbox environment where it can be tested before deployed to production. Deployment can be controlled by a workflow process of approvals.