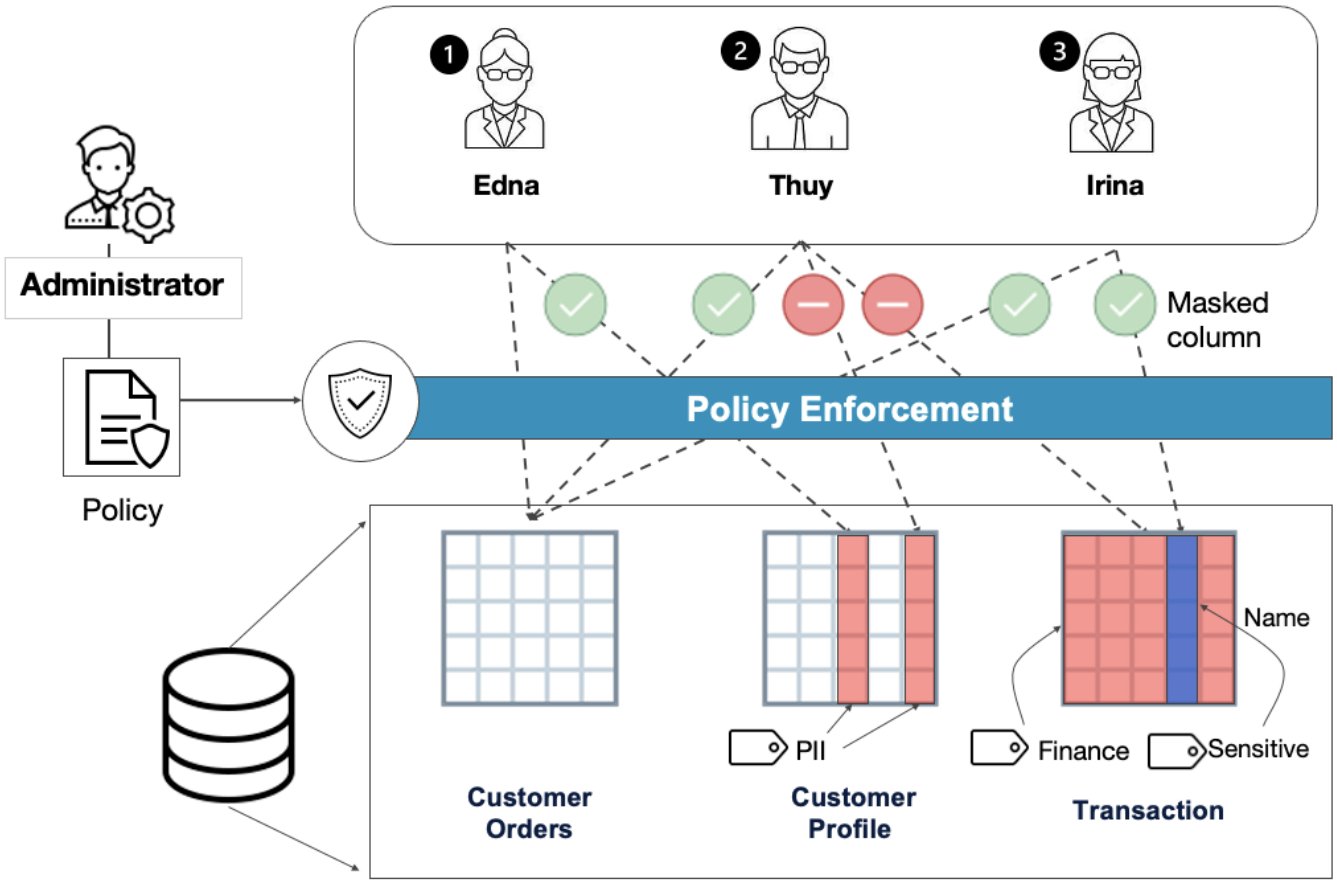
About Column-level Access Control

Column-level Access Control is Beta.

A challenge in managing database access is the complexity of data types and users accessing data in the same database. Treasure Data addresses this challenge with column-level access control, allowing administrators and database owners to tag column data, define policies, and then assign those policies to users.

You must enable the column-level access control feature to access these security protections.

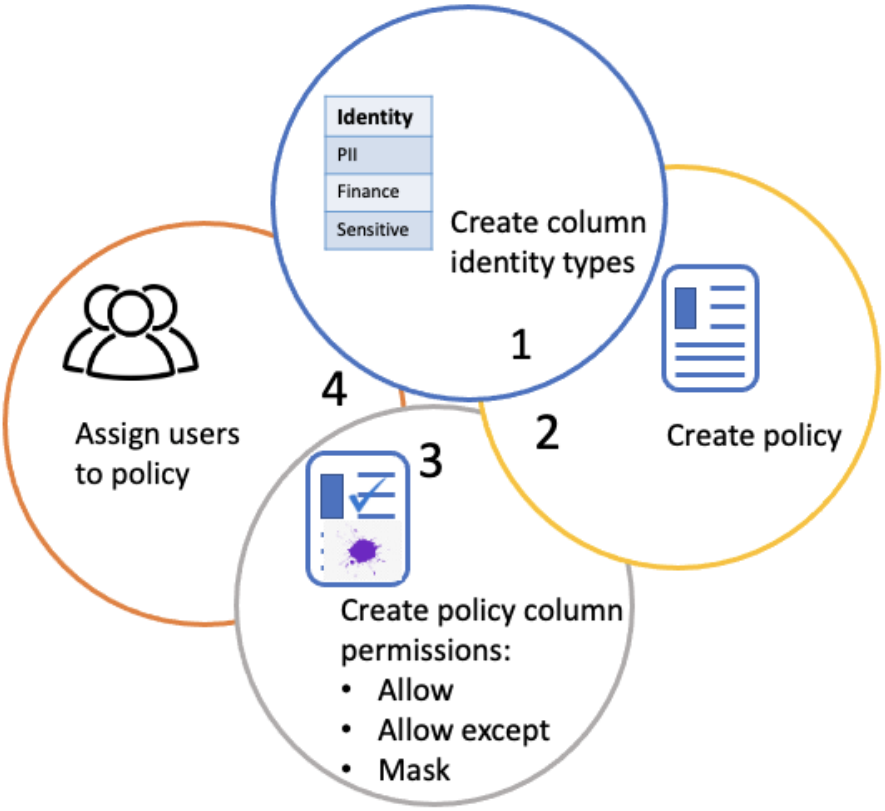


In the previous diagram, you can see that one database contains numerous tables that need to be accessed by different users:

1. Edna needs access to the Customer Orders table and restricted access to personnel identifiable information (PII) in the Customer Profile table.
2. Thuy needs access to the Customer Orders table but is restricted from accessing two data types: PII in the Customer Profile table and Finance information in the Transaction table.
3. Irina needs access to the Customer Orders table. She also needs access to restricted finance data In the Transaction table. While she has access to the column labeled "Sensitive," the data is masked and is unreadable.

How it Works

Granular access control provides the capability to grant different access levels to a particular resource to particular users. Column-level access control allows administrators to create customized column tags and then create policies that provide user access. The following image represents a high-level overview of the steps to implement column-level access control.



For a detailed workflow, review Implementing Column-Level Access Control.

Security Consistency

Treasure Data actively ensures that all features that might interact with each other protect your data from unauthorized access.

Treasure Data automatically ensures security consistency when column-level access control is enabled:

- Restrict user access to query results created by other people.
- Remove other database entry points when column-level access control is enabled to prevent access and exportation of database data.

Administrators can achieve security consistency through the following measures:

- Avoid excessive data access with systematic checks when both database access and granular access policies are applied.
- Restrict downloading query results locally to prevent data exfiltration risks.