

# Data Warehouse

## Protecting Data Anywhere

### All The Time

#### Challenge

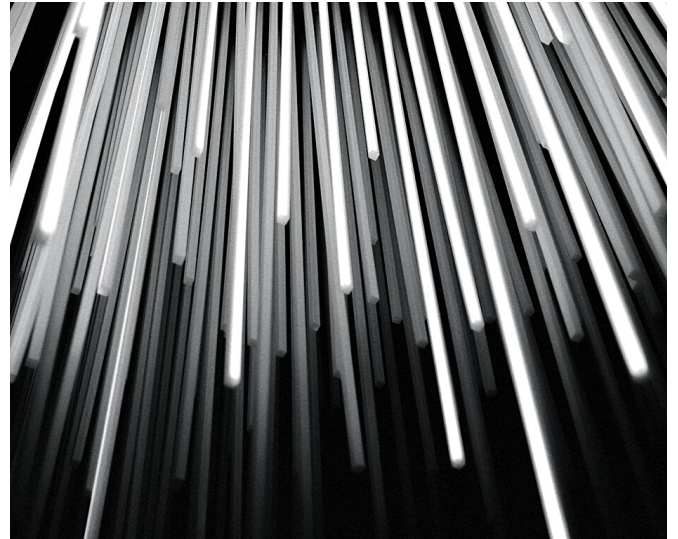
- Data warehouse incorporates vast volumes of structured data, often with availability to numerous parties, including machine personas
- Identifying sensitive information and restricting access to it is crucial for maintaining governance
- Lack of audit trail for modifications to the data collection

#### Solution

- Sotero is used to selectively de-identify and encrypt data in the warehouse to protect customer data, making it available to different users.
- Role-based access controls allow for different data controls on data to be placed on different groups. This facilitates multiple groups having access with different visibility levels.

#### Benefits

- Users can access the entire warehouse while data is protected with fine-grained access controls using RBAC to simplify management.
- In-depth data modification tracking helps maintain compliance with the strictest regulatory standards, ensuring a fully attributable access trail.
- Sensitive data remains encrypted throughout its lifecycle, in transit, storage, and use.
- Data warehouse collection can be controlled by both user role and the data sensitivity allowing flexible security management of the entire volume.
- Encryption, access restrictions, and active threat monitoring prevent data leaks from both external and internal threats.



#### About Sotero

The Sotero Data Security Platform provides a centralized way to encrypt and protect data through its entire lifecycle – at rest, in transit, and in use. With real-time detection and automated quarantine of malicious access, Sotero also prevents active threats, giving you 360-degree data security without disrupting the user experience. With our lightning-fast encryption and our point and click set-up, Sotero's solution is easy to deploy and manage, ensuring you are protected in a matter of days, not weeks or months.

