Data Cloud Protection

Baffle® Data Protection Service for Snowflake protects data at the field-level in data clouds. As data is ingested from on-premise databases to object stores like AWS S3 on to data clouds like Snowflake, Baffle protects sensitive data. Consumption of that data continues without any disruption including reporting and operations while the data owner holds/brings their own keys (HYOK/BYOK).

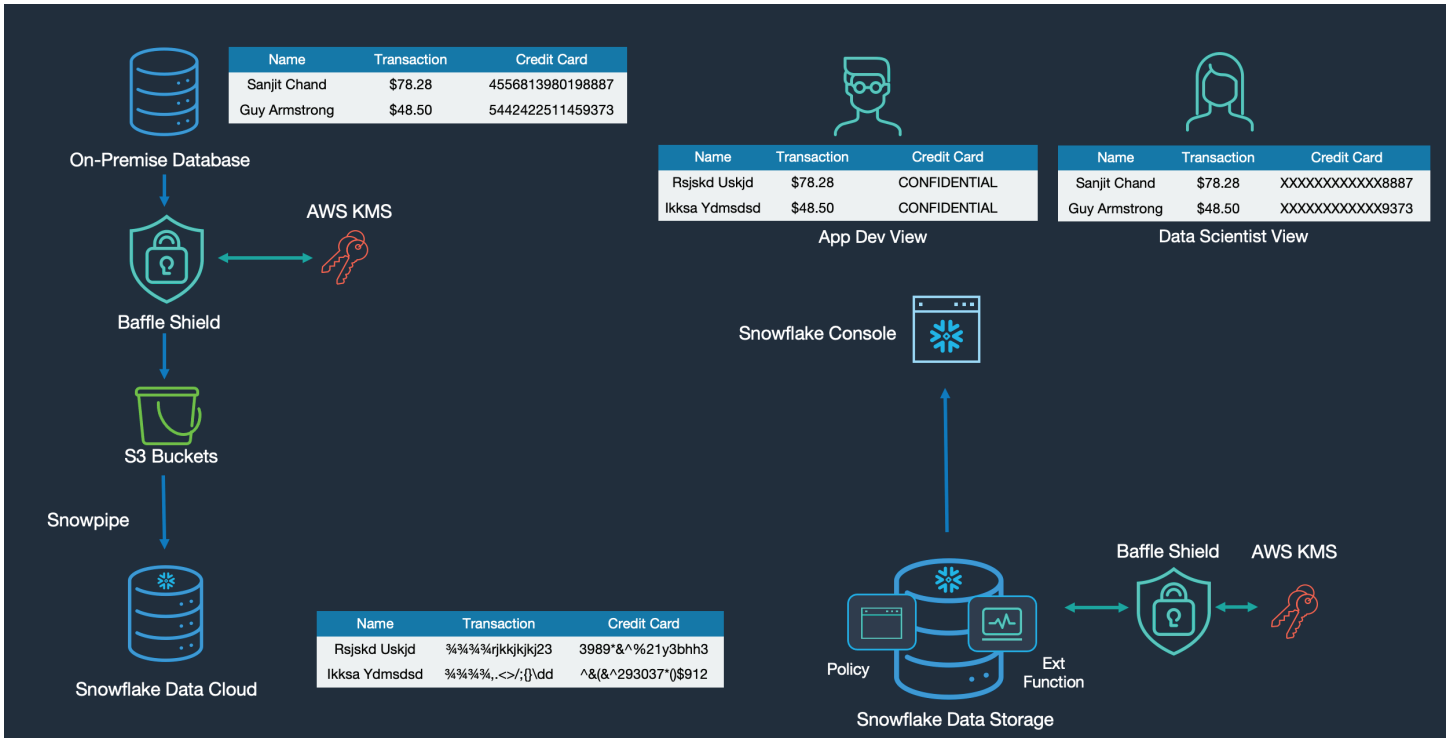
Key Benefits

- BYOK / HYOK capability for control of sensitive data in the cloudPolicy-based field-level control
- Reporting and operations on protected data is preserved
- Policy-based field-level control to allow for views based on personas
- Transparent integration with Snowflake using the built-in external tokenization support feature

Solution Overview

Enterprises are consolidating their data footprint in cloud at a rapid rate exposing sensitive contents in the process. Privacy regulations require them to maintain control of their data at all times. Baffle's solution utilizes the Snowflake native external function capability to tokenize sensitive data at a field-level granularity allowing policy-based application access without disruption

Baffle Data Protection Service for Snowflake allows enterprises to maintain control of their sensitive data in the Snowflake data cloud environment. Utilizing the ability of Snowflake to call external functions, Baffle uses Format-Preserving Encryption (FPE) to tokenize sensitive data with encryption keys that are never visible to Snowflake administrators.



Visit **https://baffle.io/snowflake/** for more information.

Baffle Data Protection Service for Snowflake

DPS integrates with Baffle's Key Virtualization Layer to leverage existing enterprise key management stores, cloud key stores, HSMs, or secrets managers. This allows customers to use their own keys as data is protected during the data consolidation process beginning with migration through ingestion in S3 and transfer to Snowflake.

Baffle DPS continues to allow the Snowflake console to query and process tokenized data. It also integrates with the Snowflake policy engine that enables customized views to be generated based on access rights. Reporting functions such as aggregation and min/max calculations continues to function even while accessing sesntive data.

Key Capabilities

Advanced Data Protection

Data is encrypted using Format Preserving Encryption (FPE) techniques that utilize the AES encryption algorithm. This renders the data useless unless the key is available to decrypt the data

Support for Customer Owned Keys

Customers always own the keys that are never visible to Snowflake administrators eliminating a significant cause of data breaches

Policy Support

Using the Snowflake Policy Engine, it is possible to restrict access to specific fields within the data table and create persona-based views

Flexible Architecture

The deployment model supports direct source to Snowflake ingestion through object storage such as S3 without any application code changes or performance impact

About Baffle

Baffle Data Protection Services (DPS) provides a transparent "no code" data security layer for distributed data and hybrid cloud environments. Baffle DPS secures data from any source to any destination to ensure data privacy and minimize the risk of data breaches.

Only Baffle supports on-the-fly data de-identification with support for masking, tokenization, field and row level encryption, BYOK/HYOK and privacy preserving analytics for secure data sharing and computation.

info@baffle.io
https://baffle.io
2811 Mission College Blvd., 7th Floor, Santa Clara, CA 95054