baffle

image: Freepik.com

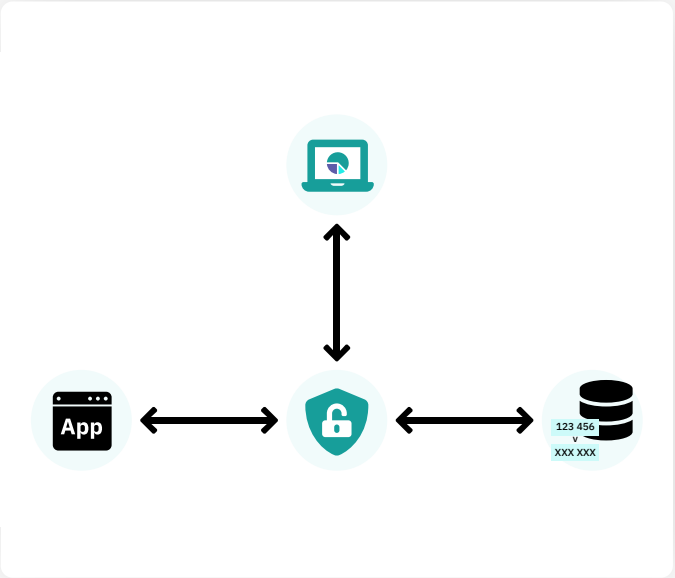
BAFFLE DATA PROTECTION FOR ANALYTICS

The easiest and fastest way to data-centric protection

Baffle's no-code column-level protection implements controls on regulated data to meet compliance. Get secure analytics without high deployment costs or management overhead.

Key Benefits

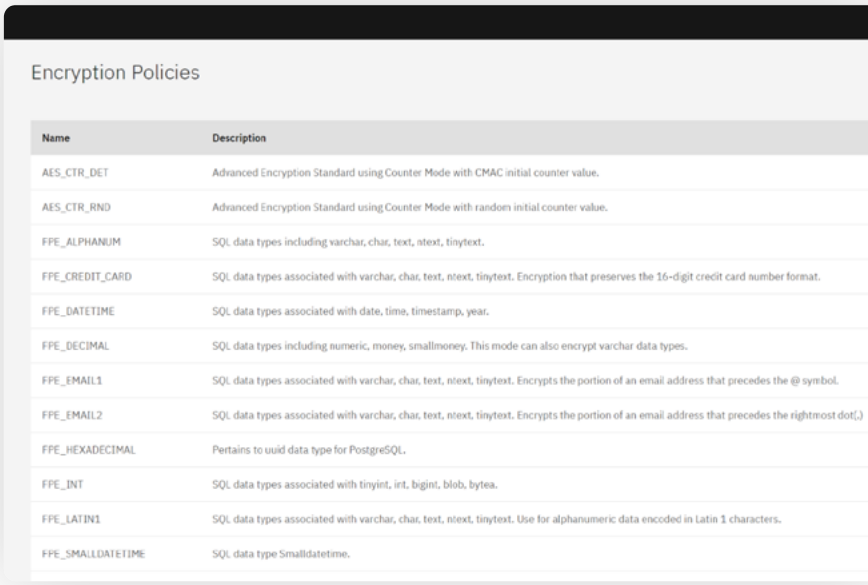
- **Secure:** Regulated Data is anonymized on ingest and is protected in analytics projects
- **Easy:** The data is protected everywhere it flows, without changes to analytics
- **Performant:** There is no perceived impact on analytics or data science performance
- **Compliant:** Ensure compliance with privacy regulations and data protection standards

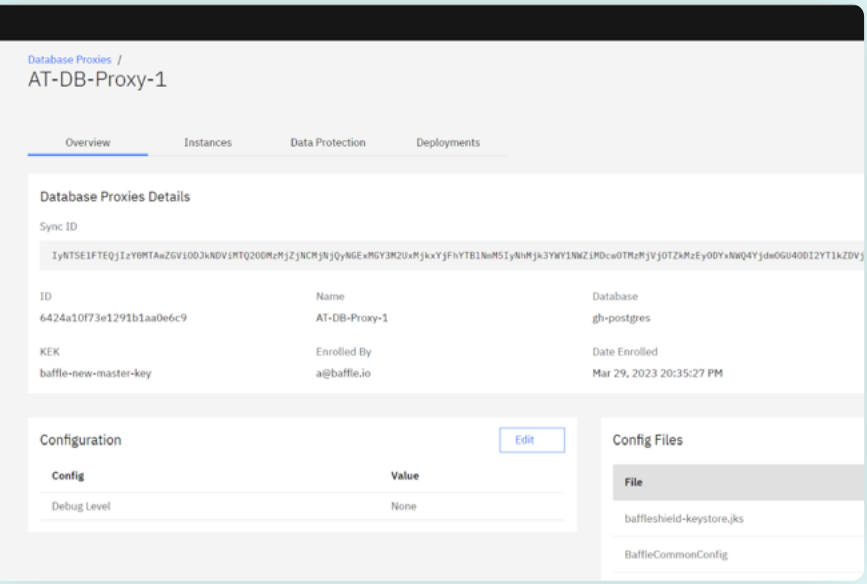


Key Capabilities

Cryptographically-enforced Protection

- Baffle's fine-grained access control ensures no unauthorized users, including cloud or database administrators, can access sensitive data in clear text
- The data is kept in a "fail safe" security posture, minimizing the risk of data breaches
- Data is protected even when it is loaded into another database or data warehouse
- Additional capabilities for completing analytic operations on encrypted data



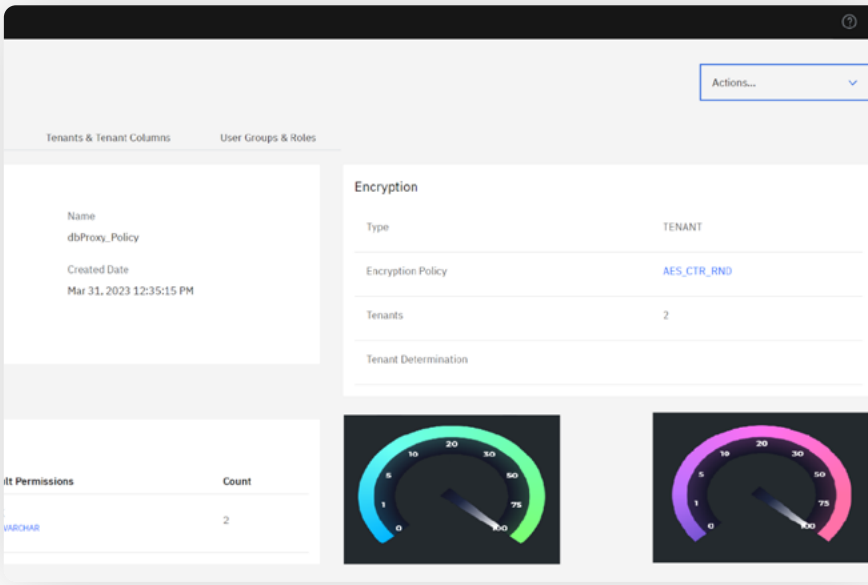


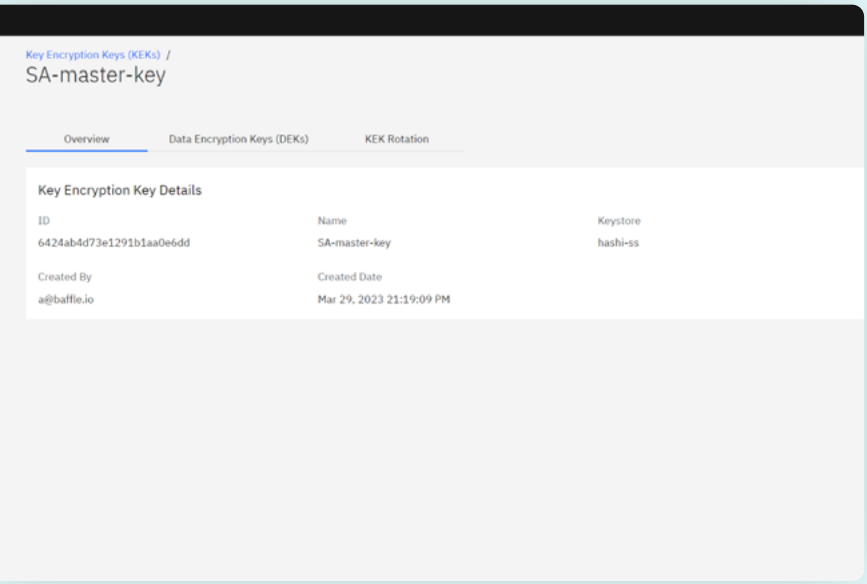
No Code Implementation

- Baffle is easily deployed and configured, without any modifications to applications
- No ongoing maintenance impact to applications
- Changes in data protection policies don't impact application

High-Performance Architecture

- Baffle has been designed for performance and scalability, minimizing impact on application and database performance
- Architecture enables horizontal scaling, so application continues to meet SLAs
- Non-sensitive data is passed through with minimal overhead



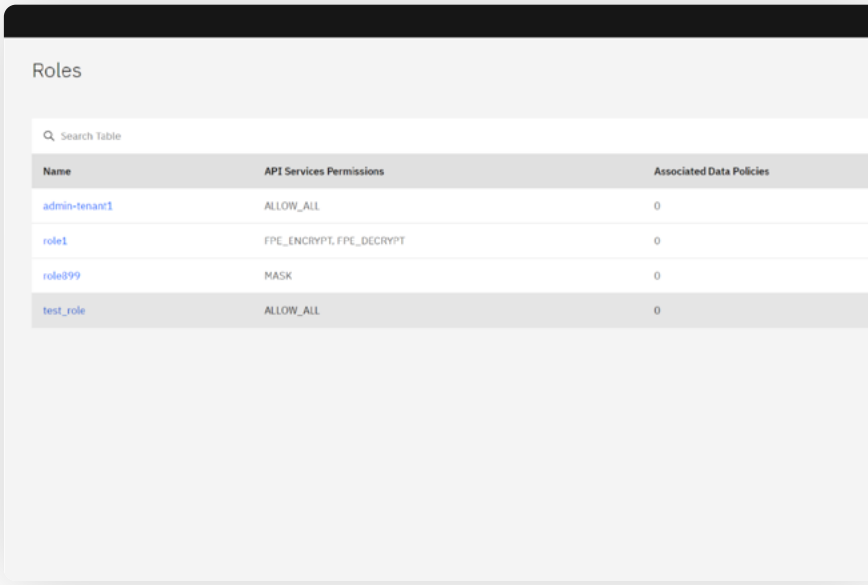


Comprehensive Key Management

- Baffle handles all aspects of key management from creation, use, rotation and retirement of keys used for encryption
- BYOK / KYOK ensures companies control their own keys, which in turn gives them full control over their data, even in cloud data stores
- Destroying the key “shreds” the data making it inoperable no matter where it is located (eg BC/DR/partners)

Role-Based Access Control

- Baffle's policy based controls specify which authorized users can access specific fields and columns in a database
- Granular policies determine how much of the data authorized users can see in clear text (their level of anonymization)
- Policies are declarative and auditable



Compatibility

Cloud Service Providers:

aws Microsoft Azure

Databases:

amazon REDSHIFT snowflake® SQL

Key Management / HSM:

AWS CloudHSM AWS KMS Azure Key Vault HashiCorp Gemalto SafeNet KeySecure™

info@baffle.io
https://baffle.io
3979 Freedom Circle, Suite 970
Santa Clara, CA 95054