Data Protection Services

baffle

The Fastest, Easiest, and Most Secure Cloud Data Protection Platform

Baffle Data Protection Services (DPS) protects data in the cloud via a “no code” and “low code” data security mesh. The solution provides universal data protection by de-identifying sensitive data and restricting access to the information. In a Zero Trust world where one must assume they are already breached, companies can easily control who can see what data with this security layer.

Key Benefits

- Mitigate insider threat and data theft risk
- Encrypt data without breaking application functionality
- Simplify encryption deployment and reduce development costs
- Ensure highly performant applications
- Never allow clear data to touch the cloud
- Meet compliance with data privacy regulations

Use Cases We Solve For

Data De-Identification in the Cloud

Simplified on-the-fly encryption, tokenization, data masking, and file level encryption as you move data to the cloud or cloud-to-cloud. Baffle moves data more easily and faster than any other solution.

Database Encryption

No-code field or row level encryption in Postgres, MySQL, Snowflake, Amazon Redshift, Microsoft SQL Server, Kafka and more

Privacy-Enhanced Computation and Analytics

Run AI and ML algorithms against encrypted data without ever decrypting the underlying values. Baffle DPS supports any mathematical operation on encrypted data in memory and in process.

Data Masking

Simplified dynamic data masking plus role-based access control with no code or application changes to control who can see what data. Employ irreversible static masking to devalue data for test/dev environments or production clones.

Secure Data Sharing

Multi-party data sharing without compromising privacy. Allow multiple parties to submit data with a HYOK model and allow aggregate analytics to execute on co-mingled data stores.

Governance and Compliance

Efficiently meet privacy requirements for GDPR, CCPA, HIPAA and modern day data privacy regulations. Ensure Safe Harbor for your business in the event of data breaches.

The Baffle Difference

Simple

No application code modification required

Fast

Virtually no performance impact

Seamless

Integrates easily into your infrastructure

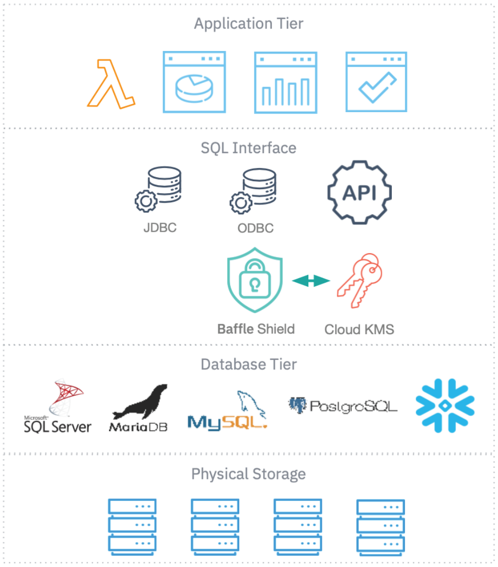
Secure

AES encryption in memory, in use, and at-rest

How It Works

Baffle DPS comes in three form factors: a database SQL Proxy, a Data Proxy and Connectors for any HTTP or REST API, and a packaged REST API for any application or data store coverage

SQL Proxy

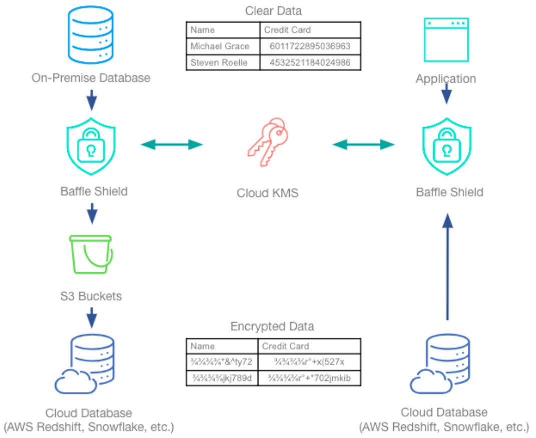


Baffle's SQL Proxy offers a transparent "no code" approach to enable field or row level encryption of data. The solution appears to applications and clients as the original database and always presents the original data schema to the application. It functions by creating a key mapping to data fields and performing encrypt and decrypt operations on-the-fly for any application query.

Applications or entire app tiers are redirected to the SQL proxy via a simple connection string change. This can also be implemented by a DNS hostname change. Application connections are proxied to the database on a one-to-one basis and the solution is deployed inline with several Fortune 100 organizations at scale.

Baffle DPS provides a key virtualization layer (KVL) to allow for integration with virtually any key management solution.The KVL enables orchestration of key generation, key rotation and mapping to application fields without embedding SDKs or figuring out key exchange and storage protocols. Baffle supports a two tier key management hierarchy with a master key (e.g. CMK, KEK) and a data encryption key (DEK). The DEKs are encrypted with the master key for protection and simplified key rotation. *At no time are any keys or data persisted by the Baffle solution.*

Data Proxy



Clear Data

Name	Credit Card
Michael Grace	6011722895036963
Steven Roelle	4532521184024986

Encrypted Data

Name	Credit Card
¾¾¾¾*&^ty72	¾¾¾¾r°+x(527x
¾¾¾¾jkj789d	¾¾¾¾r°+*702jmkib

Baffle's Data Proxy offers a transparent "no code" approach to enable field or row level encryption of data for data pipelines, ETL, file and object storage and modern data stores that rely on HTTP protocols or REST APIs.

The solution appears to applications and clients as the original data store and can transparently intermediate between the application and data structure. Baffle Data Proxy allows for simplified de-identification of data inside flat files, CSV and other formats to easily de-identify data on-the-fly as it is migrated to the cloud.

These methods support continuous change data capture (CDC) modes and event-based publishing methods to reduce the amount of data pipeline engineering work that your teams need to perform in order to stage data for cloud analytics.

REST API Service

Baffle's REST API service can be easily deployed by organizations to provide their own tokenization and data protection service for virtually any application or data store. The solution offers encryption, format preserving encryption (FPE), and tokenization to easily transform data via flexible policies and support application development teams and custom applications or data environments.

All of Baffle's solutions support high availability operational models via load balancing and auto-scaling or deployment in kubernetes pods. The solution supports SSL/TLS connections, mutual certificate-based authentication, IP whitelist support, and role-based access controls to restrict unauthorized access to data.

Key Capabilities

The Baffle Data Protection Service provides a transparent data-centric security layer that offers several data protection modes. The solution supports tokenization, format preserving encryption (FPE), database and file AES-256 encryption, privacy preserving analytics and access control. As a transparent solution, cloud native services are easily supported with almost no performance or functionality impact.

Data Pipeline De-Identification

Protect data on-the-fly as it moves from a source data store to a cloud database or object storage, ensuring safe consumption of sensitive data by downstream applications

Learn More

Tokenization / FPE

De-identify and tokenize data using Format Preserving Encryption (FPE) or deterministic encryption modes

Learn More

Field & Record Level Encryption

Data-centric protection at the field or record level in data stores secures the actual data values

Learn More

Dynamic & Static Data Masking

Simplified dynamic data masking plus role-based access control to control who can see what data. Irreversible static masking to devalue data for test/dev environments or production clones

Learn More

Database Encryption

No-code field or row level encryption in Postgres, MySQL, Snowflake, Amazon Redshift, Microsoft SQL Server, Kafka and more

Learn More

File and Object Encryption

Encrypt files and de-identify data in cloud data lakes to enable AI and privacy preserving analytics

Learn More

BYOK for SaaS

Provides an off-the-shelf BYOK service for SaaS vendors to support multiple customer-owned keys in multi-tenant environments

Learn More

REST API Data Protection Services

Easily deploy tokenization and data protection service for virtually any application or data store

Role-Based Access Control

Define which systems, users or groups can access data stores and dynamically entitle who can see what data

Learn More

Privacy-Enhanced Computation and Analytics

Run AI and ML algorithms against encrypted data without ever decrypting the underlying values. Baffle DPS supports any mathematical operation on encrypted data in memory and in process

Learn More

Secure Data Sharing

Multi-party data sharing without compromising privacy. Allow multiple parties to submit data with a HYOK model and allow aggregate analytics to execute on co-mingled data stores

Learn More

Governance and Compliance

Enable secure sharing of data across multiple parties without revealing private values to other participants

Learn More

WATCH PRODUCT VIDEOS

REQUEST A DEMO

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

Key Integrations

Platforms

- aws
- Azure
- IBM Cloud
- Google Cloud Platform
- NUTANIX
- IBM Cloud for Financial Services

Databases / Data Warehouses

- PostgreSQL
- snowflake
- MySQL
- Microsoft SQL Server
- Amazon Redshift
- Amazon Aurora
- Amazon Relational Database Service (Amazon RDS)
- Google Cloud SQL
- MariaDB

Data Stores

- Amazon Simple Storage Service (Amazon S3)
- Microsoft Azure Blob Storage
- IBM Cloud Object Storage
- kafka

Encryption Key Management

- HashiCorp Vault
- Gemalto SafeNet KeySecure™
- Azure Key Vault
- AWS CloudHSM
- AWS Key Management Service (AWS KMS)
- Key Management Interoperability Protocol (KMIP)
- PKCS#11 Library
- IBM Key Protect
- Thales Key Secure

Database Migration Services

- HVR
- Azure Database Migration Service
- ATTUNITY
- AWS Database Migration Service (AWS DMS)