FINANCIAL CRIME MANAGEMENT VENDOR SECURES CLOUD CUSTOMER DATA WITH BAFFLE AND AWS

This technology vendor is an industry pioneer in anti-financial crime management solutions, with a mission to create the world's most effective crime-fighting network. The vendor services a global ecosystem of Tier-1 and Tier-2 banks, as well as regulatory authorities and consortium initiatives.

Data Encryption to Improve Top Line Revenue and Customer Retention

The vendor's cutting-edge fraud prevention solutions are delivered as SaaS offerings hosted in Amazon Web Services (AWS). Hence sensitive customer data is flowing to the cloud.

Their customers, which include large banks, must meet strict global privacy and compliance requirements. As such, they require the vendor to encrypt their sensitive data end-to-end, at rest and when in use. The vendor sought a solution that would provide them with a **competitive edge** and improve their customer experience directly impacting their **top line revenue**.

Their team evaluated several options to meet this critical data protection requirement, including options to either build in-house or purchase an established data protection solution. They ended up choosing the joint solution delivered by Baffle and AWS for seamless data protection that was easy to implement and could scale to their needs.

Customer Control for AWS Hosted Databases

The vendor hosts more than 3,000 customer database instances in **Amazon Relational Database Service (RDS) for PostgreSQL**. Each customer's data is accessed from a virtual database dedicated to that customer.

Ultimately, the vendor chose Baffle Data Protection to encrypt data on-the-fly as it is created or moved into the RDS instances. With **Bring Your Own Key (BYOK)** capabilities, they provide each customer control over their own data, ensuring data isolation between multiple tenants. Customers also gain the ability to digitally shred their data should they ever need to do so.

Baffle allows this solution provider to centrally define policies for encrypting sensitive data at a granular level using **Column Level Encryption (CLE)**. It also offers a variety of data anonymization options including Format Preserving Encryption **(FPE)** which does not alter the structure of the original data.

A key reason for selecting the **joint Baffle + AWS solution** was that its unique proxy based approach does not require any code changes to existing applications. All regulated data is encrypted in real-time as it is produced or transferred. The data passes from the application through the Baffle proxy and lands in the target AWS database in encrypted format.

AWS RDS Database   Applications

Baffle Shield

When applications need to consume the data for analysis, **role-based policies** dictate which data is visible to whom and in what format. This significantly reduces the attack surface for data breaches and meets global privacy compliance regulations. Baffle automatically transforms the data as per the defined policy and passes it on to the application.

To the application, Baffle appears as the underlying database with the same schema and data structure. Only the connection string to the database needs to be updated in the application. This can also be done by changing DNS records, hence requiring no changes whatsoever.

The vendor also uses **AWS Key Management Service (AWS KMS)** to securely manage the encryption keys, and **AWS Data Migration Services (DMS)** to move data through Baffle.

High Performance and Rapid Time To Market

The vendor also required a highly performant solution that can scale and meet the needs of its sophisticated customers. They conducted extensive application performance testing and found that Baffle passed all their requirements with flying colors.
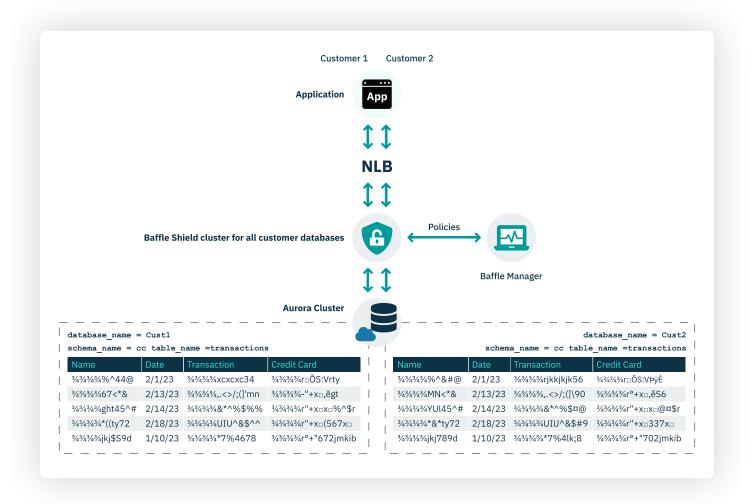
In addition, Baffle integrates seamlessly with AWS multi-region access making it easy to scale and deploy globally.

The simplicity, scalability, and flexibility of the Baffle architecture enabled this industry leader to have their test environment setup in less than a week. They completed all testing and received internal stakeholder approval within 30 days.

Baffle Advantages

1. **No-code Application Integration:** Does not require changes to application code, simplifying implementation and deployment.

2. **High Performance:** Achieves high scalability with negligible impact on the end user experience.

3. **Granular Control:** Allows for more fine-grained control over which specific data elements within the application's data should be encrypted, reducing the risk of exposing unnecessary sensitive information.

4. **Reduced Exposure:** With Baffle Data Protection, data remains encrypted in the database, even when accessed by authorized users or applications. In contrast, TDE automatically decrypts data when accessed, which exposes the sensitive data in clear text within the database.

5. **Secure Data Transfer:** When using Baffle Data Protection, data is encrypted before transmission to the database. This provides an additional layer of security during data transfer, protecting against potential eavesdropping or data interception.

6. **AWS Marketplace:** Procurement was simplified and more cost effective via the leading cloud software store.

image: vecstock on Freepik.com

About Baffle and AWS

Baffle and AWS have collaborated closely to create the leading data protection solution for cloud data stores. As the leading provider of no-code data protection solutions, Baffle is a proud member of the Amazon Partner Network ISV Accelerate program. The Baffle solution is also available on the AWS Marketplace.