baffle

GLOBAL FINTECH SOFTWARE-AS-A-SERVICE PROVIDER PROTECTS SENSITIVE DATA IN MULTI-TENANT CLOUD

image: Sketchpedia on Freepik.com

A leading cloud-based enterprise software-as-a-service (SaaS) platform enables their customers to manage and file financial documents with regulatory agencies. The content they host for their customers is extremely sensitive and hence requires the highest level of protection, especially in a multi-tenant environment.

SaaS Data in Public Cloud

The organization uses **Amazon Aurora (RDS) to host MySQL databases** to store their customer information. The data is structured in a multi-tenant architecture that enables high efficiency and flexibility.

To provide the highest levels of security assurance, the team wanted to ensure their customers have options and flexibility on how their data is encrypted. Some customers wanted completed control of the encryption keys, and to be able to rotate and revoke the keys on their own schedule.

Moving to a Modern Microservices Architecture

As a technology innovator, the company was an early adopter of modern systems and had decided to move from a monolithic backend to a microservices based architecture.

As such, they needed a data protection solution that would work well with their new infrastructure. It also needed to support customer-owned Bring Your Own Key (BYOK) with the ability to rotate and revoke encryption keys.

The solution also needed to be easy to deploy, provide a set of common encryption services for all their developers, and be highly performant and scalable.

Row-Level Encryption with BYOK

After evaluating several data encryption solutions including some open source options, the company chose to implement Baffle Data Protection for SaaS.

With Baffle, they applied row-level encryption to logically segment customer data. Each customer gets their own key and each row in the database associated with that customer is encrypted using their specific key.

Customer data is ingested via multiple different paths which include customers creating data directly in the company’s platform, integrations with external connectors, through 3rd party application integrations, manual imports, or the company’s public APIs. In all cases, the customer data is encrypted before it is ever written to the company’s Aurora databases.

Customers can manage their own dedicated Key Encryption Keys (KEK) which is then used to encrypt Data Encryption Keys (DEKs). This provides customers of the SaaS platform with full control over their data. They can disable their KEKs any time thus effectively digitally shredding data stored in the SaaS database.

Customers are also able to manage and rotate keys based on their own policies and terms, adding an additional layer of protection and risk mitigation. A BYOK administration portal allows customers to easily upload their key materials, or generate a unique key for themselves, or even upload a wrapped key.

The company manages its encryption keys through **AWS Key Management Service (AWS KMS)**.

Billions of Records Protected

Successfully deployed in production for a few years, the Baffle solution has helped the company protect terabytes of customer data. They were able to meet all of their existing customers’ needs as well as win over new customers due to this high level of security assurance.

Boasting very high customer satisfaction, the company is ideally positioned as a strong leader in its space. As it looks to the future, they plan to advance their architecture with Hold Your Own Key (HYOK), a data storage agnostic platform, and more.