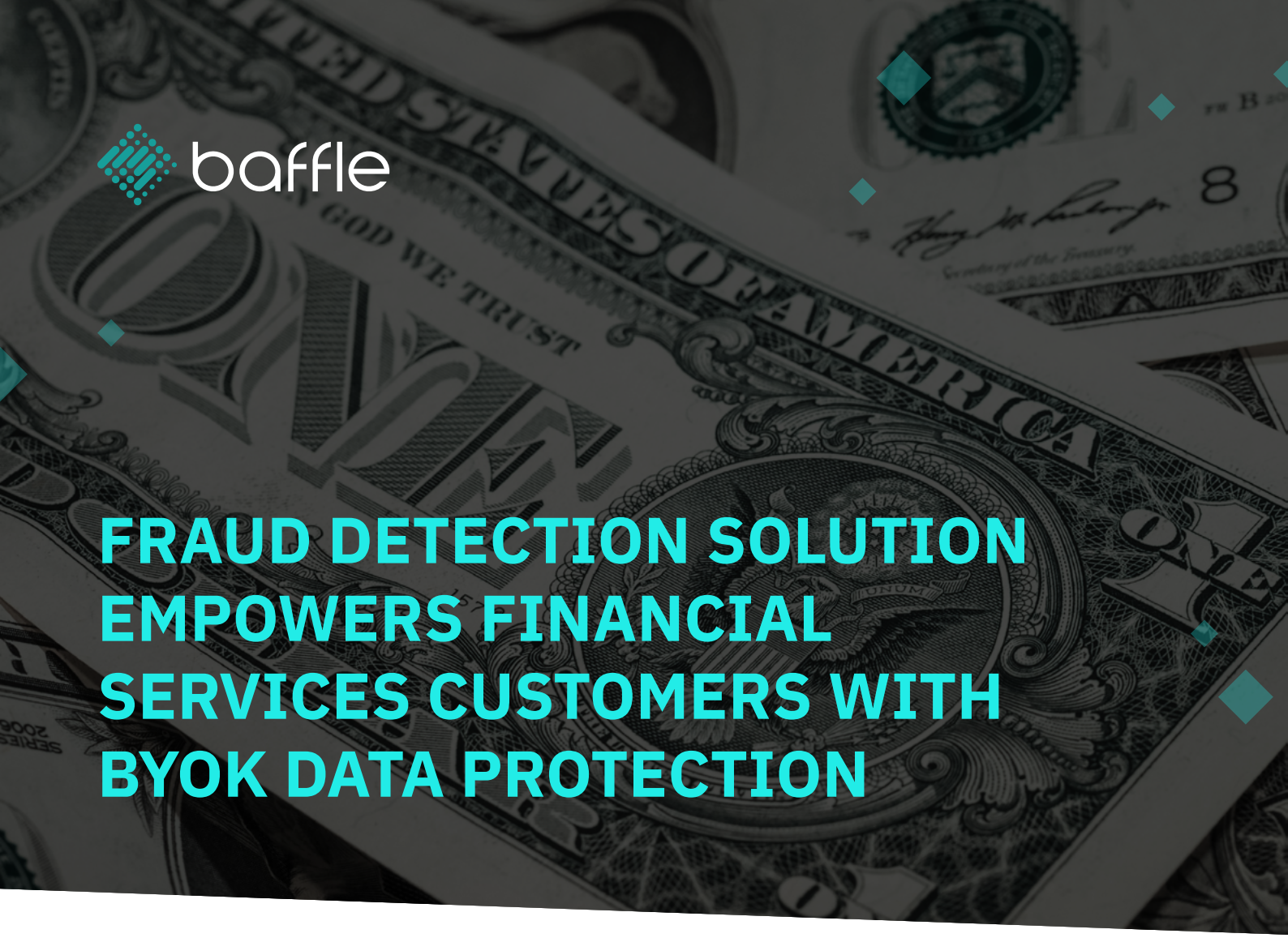


FRAUD DETECTION SOLUTION EMPOWERS FINANCIAL SERVICES CUSTOMERS WITH BYOK DATA PROTECTION

This organization is a leading provider of fraud and risk management solutions for financial institutions and fintechs. Their customers include 7 of the top 15 banks, 6 of the top 10 credit unions, and 30+ fintech unicorns. Customers use their forward-thinking solutions to stop identity fraud at the point of application.

Top Banks Demand Bring Your Own Key (BYOK)

As an integrated fraud prevention solution, this vendor taps into their customers data to perform fraud analysis. Customer data is brought into the vendor's infrastructure which can include sensitive information pertaining to privacy and confidentiality of customers and their end users.

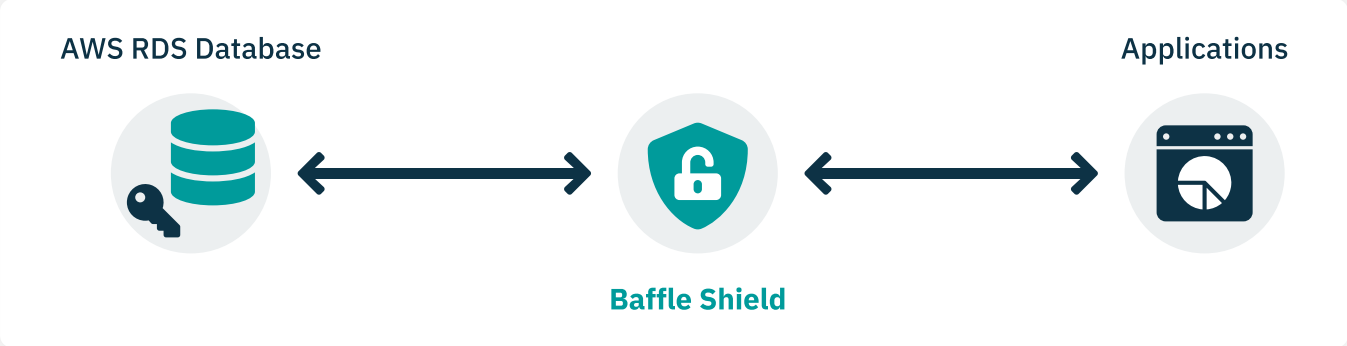
Large banks must meet strict global privacy and compliance requirements, and as such require the vendor to encrypt their sensitive data. Furthermore, these banks require the data be encrypted with their own encryption keys so that they alone can control revocation of access, or to put it another way the banks require the "right to be forgotten."

The vendor sought a solution that would allow it to easily implement Bring Your Own Key (BYOK) for its customers, without arduous changes to its applications and systems.

No-Code Data Encryption for Cloud Hosted Databases

The vendor leverages **Amazon Web Services (AWS)** to host its sensitive customer databases in **Amazon Relational Database Service (RDS)**. Each customer's data is accessed from a virtual database where a separate table is used per customer.

Baffle Data Protection encrypts data on-the-fly as it moves from customers' applications into the vendor's RDS instances. Baffle allows them to centrally define policies for encrypting sensitive data, and offers a variety of data anonymization options including **Format Preserving Encryption (FPE)** which does not alter the structure of the original data. It also supports Tokenization, Standard AES Encryption, Data Masking, etc. 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 database in encrypted format. **No application code needs to be changed** because of this innovative model.



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.

Customers Gain Control with BYOK

The ability to seamlessly encrypt and decrypt data on the fly is a huge benefit for the vendor. However, the ability to provide clients BYOK capabilities helped them land some of the largest financial services institutions as customers.

With out of the box BYOK support, Baffle streamlined the process by which the vendor was able to offer this to their customers. Baffle also supports many third party key management systems. The vendor uses **AWS Key Management Service (AWS KMS)** to empower their customers to control their own cryptographic keys. This allows their customers to feel assured that their data is adequately protected, while also giving them the ability to digitally shred their data if necessary.

Baffle Advantages

1. **Granular Control:** Baffle Data Protection allows for more fine-grained control over which specific data elements within the application's data should be encrypted. It means that sensitive data can be protected at a more granular level, reducing the risk of exposing unnecessary sensitive information.

2. **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.

3. **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.

4. **Application-Specific Key Management:** Baffle Data Protection allows for better control over encryption keys, as the application manages and controls the encryption and decryption process. This minimizes the risk of unauthorized access to keys and enhances overall security.

5. **Limitation of Database Access:** Baffle Data Protection can help limit database access to only authorized applications or users, reducing the attack surface and the potential for unauthorized access.

6. **Complementing Other Security Measures:** Baffle Data Protection can be used in combination with other security measures, such as access controls, and role-based permissions, to provide a comprehensive security strategy.

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.

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