Simplifying Application Encryption with Baffle Data Centric Protection and SafeNet KeySecure

Easy-to-deploy "no-code' application-level encryption backed by enterprise grade encryption key management

Encrypting data at the application level offers the greatest security for securing sensitive data at rest. But, it can present clear, insurmountable drawbacks.Often application-level encryption requires organizations to make code changes that are either resource intensive or may be impossible to make. And, encryption can make data unsearchable in structured data stores. While the desire is there for security professionals, the means for application-level encryption may not always be available.

Fortunately, Baffle and Thales are working together to address these challenges.

Key Benefits

- Application level encryption with no code modifications:
  - Field & record level encryption
  - Most applications incl. off-the-shelf apps
  - API data access models
  - Support for microservices and serverless
- Eliminates developer costs associated with modifying applications, and accelerates build and release cycles
- Ensures compliance with data privacy regulations
- FIPS 140-2 Level 1 to FIPS 140-2 Level 3 validated roots of trust to address compliance requirements
- Homomorphic-like functionality to allow mathematical operations, sorting, and searching on encrypted data

Baffle's Data Centric Protection

Baffle's Data Centric Protection provides a "no code"method for application level encryption that can be configured in four ways:

1. Standard Encryption: Baffle functions as an application level encryption (ALE) equivalent that encrypts data on a field-level basis.

2. Record Level Encryption: Baffle encrypts at the record-level with for support for multiple keys within a single column that are mapped to respective data owners or entities. This mode is suited for multi-tenant or shared data environments where segmenting data is difficult.

3. Data Masking: Baffle simply masks data to prevent unauthorized data decryption from configuration errors or deleted keys. Data masking minimizes data exposure in test/dev environments and controls data exfiltration to external parties.

4. Advanced Encryption: Baffle lets organizations operate on encrypted data with "homomophic-like" operations for optimal application functionality and minimal breakage to business processes.

Thales SafeNet KeySecure

SafeNet KeySecure by Thales is an encryption and key management appliance that securely stores Baffle encryption keys.

Organizations use SafeNet KeySecure – the industry leading enterprise key management platform – to centrally manage their encryption keys and ultimately own their data. Regardless of its location, be it stored in a database, file server, application, traditional or virtualized data center, SafeNet KeySecure keeps sensitive data secure from compromise. SafeNet KeySecure's management tools and capabilities such as key versioning streamline time-consuming tasks, including key rotation. Organizations

can select from flexible options spanning FIPS 140-2 Level 3 or 1 validated hardware appliances and hardened virtual appliances. Supporting a broad encryption ecosystem— encompassing both Gemalto and a diverse range of third-party products — SafeNet KeySecure supports a hardware root of trust using SafeNet Network Hardware Security Modules (HSM) or the Amazon CloudHSM and Microsoft Azure HSM services.
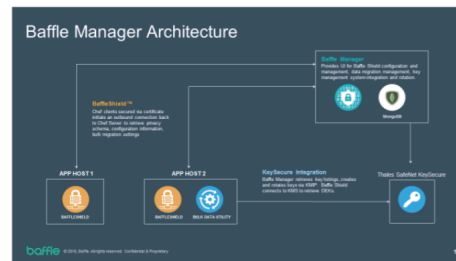
Features

Policy Management and Separation of Duties

With SafeNet KeySecure, administrators can set authentication and authorization policies that dictate which data can be accessed in the clear by a particular user or set of users. These controls provide administrators with tighter governance of sensitive data. Policy-driven security using granular access controls provides a vital layer of protection tohelp organizations comply with the separation of duties between IT and security administrators that isrequired in many security mandates.

Logging, Auditing, and Reporting

SafeNet KeySecure records all key state changes incentralized logs, simplifying auditing and reporting access to data and encryption keys. By tracking this information from one platform, organizations increase security around their data and can readily demonstrate their compliance with industry mandates and government regulations

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing amount of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments

About Baffle

Baffle™ is a modern data-centric encryption solution designed for distributed data and cloud-native environments.

Baffle dramatically simplifies the complexity of encryption for data-centric protection strategies to mitigate the risks of data theft and breaches and ensure compliance with modern day privacy regulations.

info@baffle.io
https://baffle.io
2811 Mission College Blvd., 7th Floor, Santa Clara, CA 95054