



BAFFLE DATA SECURITY FOR AMAZON S3

The Easy Way to Secure Your Data in S3

Baffle Data Security for Amazon S3 offers a simple no-code solution to protect your sensitive data stored in Amazon Simple Storage Service (S3) buckets. By encrypting data at the field level before it enters S3, Baffle eliminates the risk of data exposure due to human errors, such as misconfigurations or unauthorized access.

Key Benefits

- **Secure:** Sensitive data is always anonymized before it lands in S3
- **Easy:** No code changes required to any applications
- **Control:** Even cloud admins can't see your data in S3
- **Flexible:** Encrypt at the field-level in CSV, JSON, Parquet, and XML files

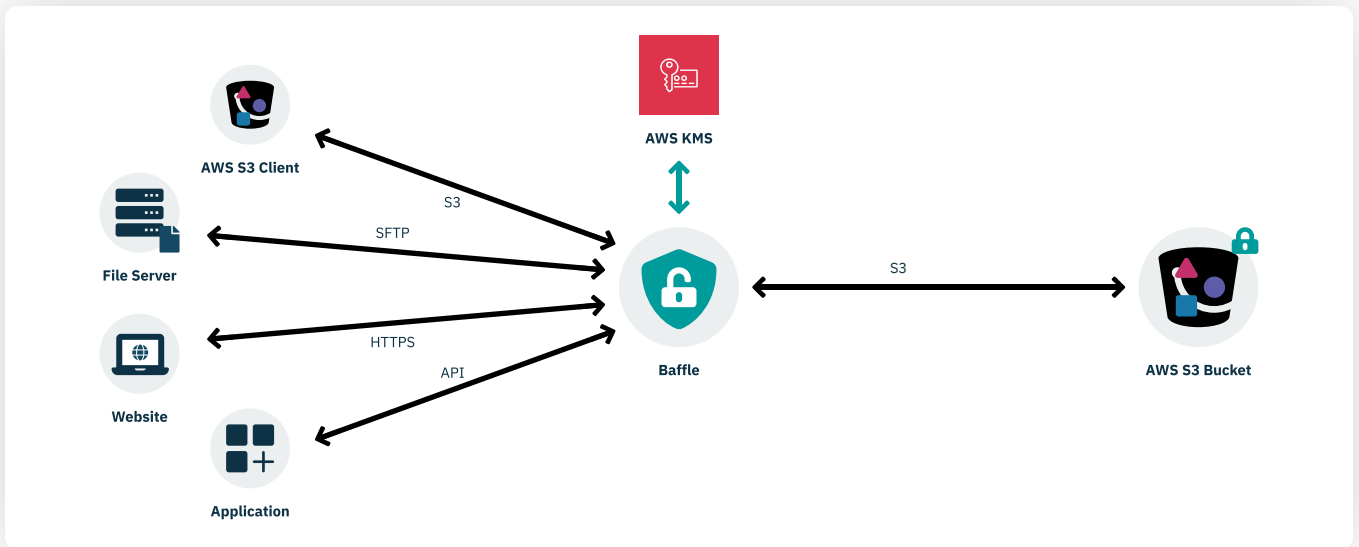
Key Capabilities

Client-side encryption

Encrypt data before it lands in an S3 bucket

Prevent unauthorized access even from cloud administrators

Apply quantum-resistant AES-256 encryption to any file type

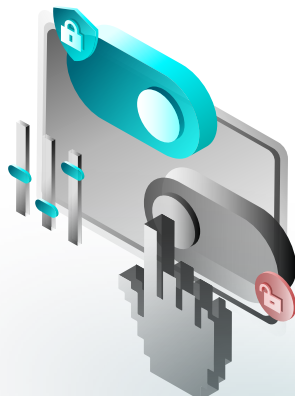


No-code Architecture

Deploy easily without having to modify any applications

Proxy-based architecture provides transparent data encryption

Supports the most popular S3 ingestion protocols



Field-level anonymization

Encrypt data at the field level for unstructured or semi-structured data

Easily protect CSV, JSON, Parquet, and XML files

Centrally manage data protection policies and encryption keys

Name	Status	Phone	Credit Card #
Jill	Active	123-456-7890	7102-3411-1234-5678
Anu	Inactive	416-123-4567	2200-1200-9988-7766



Name	Status	Phone	Credit Card #
Jill	Active	XXX-XXX-7890	9100-1999-8887-8273
Anu	Inactive	XXX-XXX-4567	3222-9283-6837-8844

Role-Based Access Control

Restrict use of data based on fine-grained policies at the field level

Combine permissions at field-level with access type ((clear text, partially masked, fully encrypted, etc.)

Integrate with existing IAM systems for easier administration of access control policies



Data isolation for multi-tenancy BYOK

Isolate individual objects in a bucket by tenant

Provide each tenant their own encryption key

Allow tenants to retain control and even digitally shred their own data

