Acra

Data leakage prevention for your apps with centralised data storage.

COSSACK LABS

Essential benefits for:

- **Your clients:** secure storing and processing of their data.
- **Your developers:** security tooling that is simple to operate and convenient to integrate.
- **Your product:** 20 additional lines of code that make it 200 times more secure.

Key features:

- Selective **encryption** with easy integration API.
- Decryption as **database proxy service.**
- **SQL firewall** that filters requests and detects attacks.
- **Intrusion/leakage detection** via poison records (honey tokens).

Compatibility:

SQL databases: MySQL, PostgreSQL, Google Cloud SQL, Amazon RDS.

Object stores: filesystems, KV databases, Amazon S3, Google Cloud DataStore.

Languages/frameworks: Ruby, Python, PHP, Go, Java, NodeJS, Objective-C/Swift.

Server OS: CentOS, Debian, Ubuntu.
Application OS: Linux (x86/ARM, Android, iOS).

Overview

Cryptographic protection of sensitive and personal data is mandated by regulations (GDPR, HIPAA, PCI DSS) and industry best practices. However, building encryption into a modern application is a tedious task, which has limited security impact and plenty of architectural trade-offs.

Encryption and secure data lifecycle is a cornerstone of security in any application. Acra was built to mitigate data leakage risks while providing **affordable and convenient security** across the whole data lifespan within the application. Acra is **easy to integrate**, does not require significant modifications in existing product code, and provides **reliable encryption** and data leakage prevention to any kinds of applications that use databases to store data.

Acra was specifically designed for web apps and mobile apps with centralised data storage, including distributed, microservice-rich applications.

Typical use cases

- Personally-identifiable information (PII) protection under GDPR demands (articles 25, 32, 33, and 34).
- General sensitive data protection for web and mobile apps, including financial, medical, e-commerce industries.
- Secure data aggregation and centralised access control for industrial sensors and other high throughput systems.
- Custom security toolkit for distributed applications.

Form-factor and licensing

- **Acra Open-source:** Apache 2 licensed bare-bones version with core features.
- **Acra Pro:** improved performance, easy scaling, management tools, dedicated support.
- **Acra-as-a-Service:** managed Acra with secure SQL backend of your choice, pre-configured and integrated.

Acra

Data leakage prevention for your apps with centralised data storage.

COSSACK LABS

Architecture and features

Encryption & key model

Acra integration library encrypts the data so that only the server-side components of Acra can decrypt it. Inside Acra holds all the **necessary key management tools** to support the process: key distribution, rotation, compartmentalization.

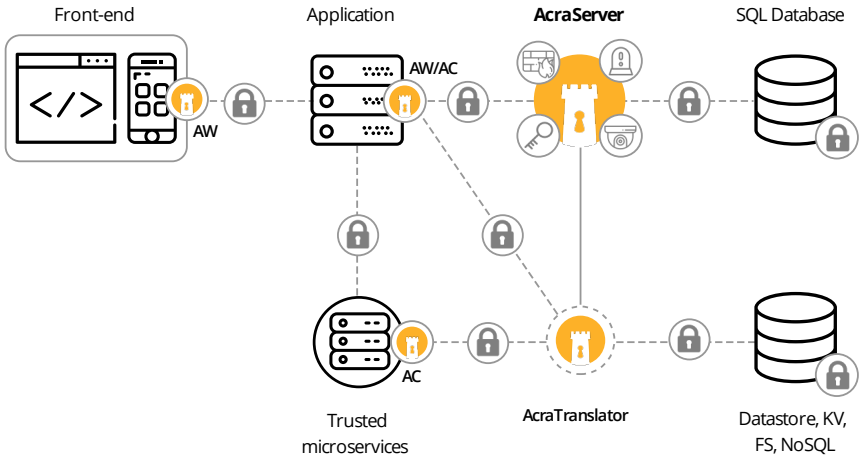
Realistic security model

Acra operates on the assumption that datastore and application components can be compromised by attackers, yet data is protected.
Acra **minimises** the leakage scope, **detects** unauthorised behavior, and **prevents** the leakage, informing operators of the incident underway.

Narrow attack surface

Acra's encryption model is built around the requirement that no credentials stored in application components are sufficient for decryption of the data stored in the backends.

As Acra becomes the only gateway to access plaintext version of the sensitive data, it can perform various checks to detect anomalous/unauthorised behavior, and log access to sensitive data.



Acra easily integrates into modern application of any complexity, protecting every step of the sensitive data lifecycle in your application**.**

Core components:

AcraWriter (AW): in-app integration library that encrypts data.
AcraConnector (AC): secure connector that protects transport and provides API interface to AcraServer.
AcraServer: main database proxy that provides decryption, SQL firewall, and intrusion-detection.
AcraTranslator: companion service for data decryption data from non-SQL datastores.

Acra protects only data that needs protection, which is specified within your app code. Call Acra encryption on the records you need, request them back through Acra — and receive your data.

Acra decrypts everything in a compartmented server/VM/container, making the keys to the encrypted assets unavailable to an attacker.

Try Acra now!

Request Acra Live Demo — interactive simulator that demonstrates the basic workflow of Acra.
Visit Acra Open-Source GitHub to see code and examples.