Acra

DATA PROTECTION AND LEAKAGE PREVENTION FOR YOUR APPS AND DATABASES

Encryption of sensitive and personal data **is mandated by regulations** (GDPR, HIPAA, CCPA, PCI DSS) and industry best practices. However, building cryptography into distributed application is often a tedious task, which has a **limited security impact** and plenty of architectural trade-offs.

Acra is here to change it. Acra is one tool that covers 9 data security controls.

Acra is built to mitigate data leakage risks while providing **defense in depth** across the whole data lifespan within the application. Acra is **easy to integrate**, doesn't require significant modifications in the existing code, provides **reliable data security**, reduces MTTD and MTTR.

KEY BENEFITS

Data breaches don’t matter

Datastore and apps can be compromised, yet the data is protected.

Modern data security

Protection, detection, reaction security controls in one package.

Low-footprint security upgrade

Fast cryptography, easy deployment, quick configuration.

Security that fits

Designed to fit your architecture and grow with your solution.

Compliance by design

Acra-based solutions meet regulatory and compliance requirements.

Get to market quickly

Comparing to other tools, Acra users deploy their secure solutions faster.

TYPICAL USE CASES

Secure data vault: protect a crucial database with Acra so that high-risk data has separate protection infrastructure built around it. Encrypt, anonymize, mask or tokenize data.

Quick and transparent integration of encryption: quickly integrate Acra into your existing applications with a minimum amount of re-engineering efforts – days instead of months. Acra will encrypt/decrypt data fields “on the fly”, while your application and database don’t know that the data is encrypted.

Secure data lifecycle: protect sensitive data’s journey in your solution, from the database to the microservices, backups and logs. Operate on encrypted data. Build end-to-end encrypted dataflows.

Gain visibility and transparency: with cryptographically signed audit logging in Acra, you have proofs of who-when-how has accessed the data or tried to tamper the logs.

Detect and prevent incidents: automate Acra’s reactions to detect potential leakage and protect sensitive data and keys during security incidents.

Achieve compliance in data security and privacy while actually increasing practical security posture. Best of two words.

WHY PEOPLE LOVE ACRA

Cryptography hidden under the hood: Acra doesn’t require any cryptographic expertise for proper usage.

Strong encryption to protect sensitive data preventing unauthorized parties from accessing it (including insiders and APT).

Hardened key lifecycle – follow NIST SP 800-57 key management flow.

Centralised security – deploy and manage one tool instead of integrating solutions from multiple vendors.

Quick and automation-friendly integration with minimal changes in the application code and architecture.

Hard to misuse: secure-by-default configurations, ready-to-use examples, validation of configuration files, alerting on suspicious activity, etc.

Full operational control: logs, events, metrics and 360 degree operational and security overview into Acra’s inside processes.

No vendor lock – Acra’s cryptographic core is open source and Acra provides rollback utilities to decrypt the database back into plaintext.

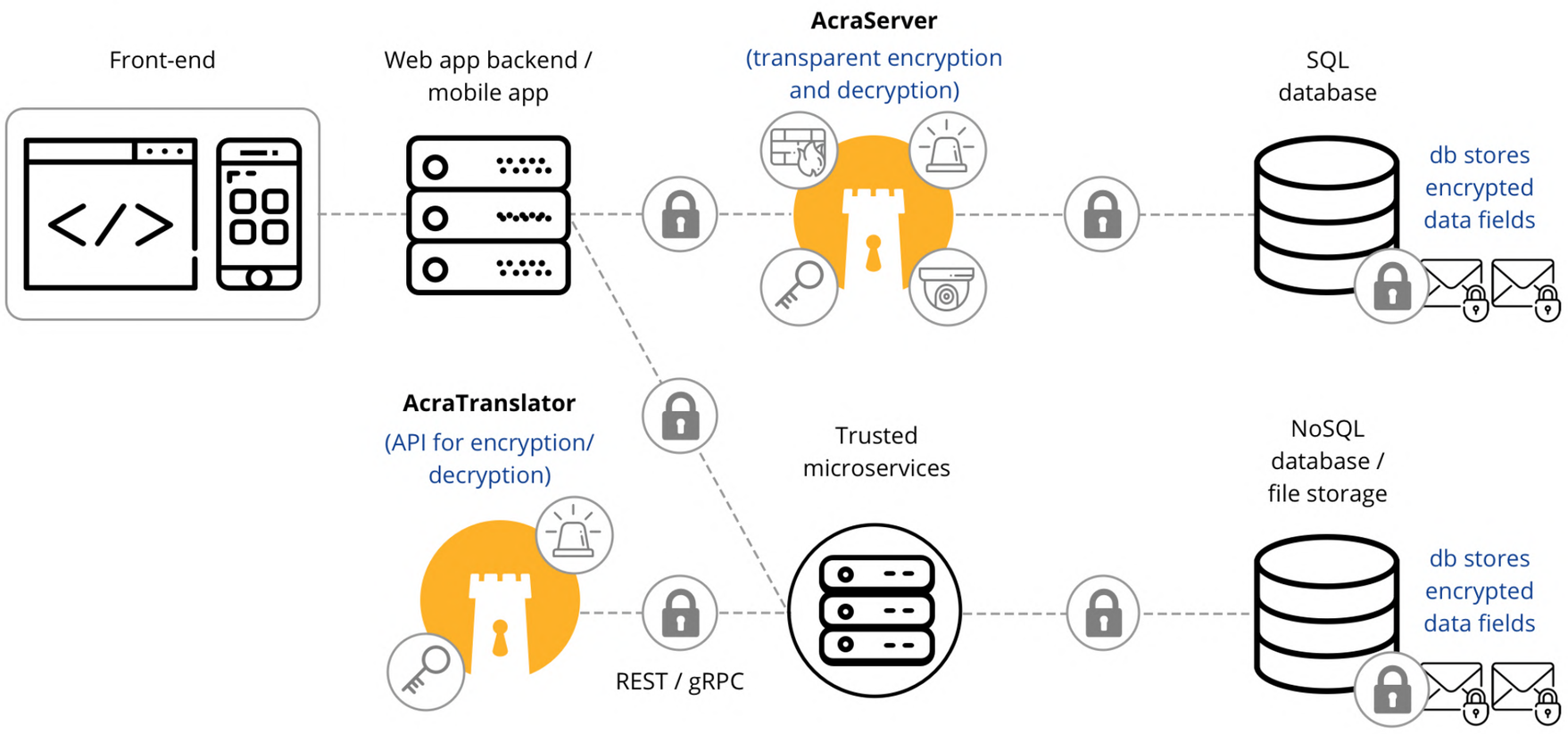
Demos, examples, documentation – numerous pre-configured example projects available (docker-compose: database, Acra, client-side app).

COMPATIBILITY TABLE

Cloud platforms	DigitalOcean, AWS, GCP, Heroku, Azure, any cloud.
RDBMS	MySQL 5.7+, PostgreSQL 9.4+, MariaDB 10.3, TiDB, CockroachDB, Google Cloud SQL, Amazon RDS, TimescaleDB.
NoSQL, KV datastores	MongoDB, Redis, Cassandra, Amazon S3, Google Cloud DataStore. Any datastore or database with REST API, filesystems.
KMS	AWS KMS, GCP KMS, HashiCorp Vault, Keywhiz
Server-side platforms to run Acra	Ubuntu, Debian, CentOS, RHEL. Docker, Swarm, Compose, Kubernetes.
Load balancing	HAProxy, cloud balancers.
Logging, SIEMs	ELK stack, Datadog, Graylog, Prometheus, Grafana, Jaeger.
Acra's client-side SDKs are available for	python, Go, Node.js, ruby, PHP, C++, iOS (Swift, ObjC), Android (Java, Kotlin).
You apps can run on	Languages: any language :) Platforms: web, server, desktop, mobile, embedded (ARM). Linux servers, Windows servers.

ARCHITECTURE AND FEATURES

Acra consists of several services and utilities, allowing you to construct infinitely sophisticated data flows that are perfectly suited to your exact infrastructure. Depending on your architecture and use case, you might need to deploy only basic services or all of them.



AcraServer: transparent SQL database proxy that parses SQL traffic between an app and a database and applies security functions where appropriate.

AcraTranslator: Encryption-as-a-Service API that exposes most of Acra's features as HTTP and gRPC API.

AnyProxy: API server that works as a gateway to the encryption layer for several applications and databases. Available in the Acra Enterprise Edition only.

Client-side SDKs make developers' life easier by encrypting/decrypting data on the application side and providing SKDs for AcraTranslator and AnyProxy. Available in the Acra Enterprise Edition only.

Key storage: use Redis for storing encrypted intermediate keys, connect Acra to KMS for storing Master keys.

Additional services and utils: key management utils, data migration scripts, transport security service, policy management tools. Any of them are optional.

KEY FEATURES

Cryptographic security: every selected data field is encrypted before storage using field-level encryption, and transferred via protected channels with encryption and mutual authentication.

Searchable encryption – search through encrypted data without decryption. Designed for exact queries, based on AES-GCM and blind index.

Data masking and **tokenization:** anonymise or pseudonymise the data preserving its original format.

Key management tooling: flexible management of key rolling, rotation, revocation, export, backup – to suit your load needs and data architecture.

SQL request firewall: prevent SQL injections, stop unauthorized and suspicious queries.

Intrusion detection system: detect data leakage using poison records and warn about suspicious behaviour.

Logging, monitoring and security events: always have an operational and security overview on what's happening with your data.

Cryptographically protected audit log – Acra provides cryptographic protection and validation of logs to prevent unnoticed tampering.

Policies: expressive policy language that allows to configure Acra's behavior in large infrastructures.

FORM-FACTOR AND LICENSING

ACRA COMMUNITY EDITION

Apache 2 licensed open source version with all core security features. Best for prototyping and small-scale projects.

ACRA COMMUNITY EDITION + SERVICES

Acra Community Edition plus assistance with integration and configuration. Best for small businesses without an Ops team.

ACRA ENTERPRISE EDITION

Provides more value for enterprise teams: refined key management and policy management, support of multiple KMS and SIEMs, advanced services and utilities (client-side SDKs and AnyProxy) for building security layers fitted to your architecture.

Best for products with high security requirements, large-scale cloud solutions with multiple databases or B2B SaaS.

ACRA ENTERPRISE OPTION KITS

Custom extensions for particular use cases: ICS/SCADA, TimeSeries/ Monitoring, deep mobile integration, services for the end-to-end encrypted dataflow.

ACRA-AS-A-SERVICE

Managed Acra with backend of your choice, pre-configured and integrated.

HOW TO EVALUATE AND GET STARTED

START WITH ACRA COMMUNITY EDITION AND EXAMPLES

Check out **Acra Community Edition on GitHub** and **Acra engineering examples** – a collection of ready-to-try projects with Acra, database, web application and monitoring tools. Learn how easy it is to integrate Acra into your existing application.

FREE PLAYGROUNDS TAILORED FOR YOUR USE CASE

Sign NDA and get access to a free playground that runs **Acra Enterprise Edition**, a database of your choice and a client application. After evaluating the playground, your team knows more about Acra functionality and security benefits it brings into your project.

PAID PILOT / POC, HIGHLY CUSTOMIZED FOR YOUR USE CASE

Sign NDA, Acra Evaluation license and consulting agreement. We allocate engineering time to build your use cases, configure Acra, tune data model and queries. After evaluating PoC, your team is confident that you can attain your security objectives with Acra prior to buy-in.

CONTACT US

Would you like to learn more and evaluate Acra Enterprise Edition?

Drop us a line at:
sales@cossacklabs.com

WWW.COSSACKLABS.COM