



Acra

ЄДИНЕ РІШЕННЯ ДЛЯ
ЗАХИСТУ ЖИТТЄВОГО
ЦИКЛУ ДАНИХ

ЗУСТРІЧАЙТЕ АСРА



Асра – це інструментарій для захисту даних: набір засобів безпеки даних, створених для захисту даних протягом усього їхнього життєвого циклу в сучасних розподілених системах.

Асра надає низку засобів безпеки даних та механізмів шифрування, які дозволяють забезпечити багатoshаровий захист чутливих даних у комплексних системах.

ТИПОВІ ВИПАДКИ ВИКОРИСТАННЯ

Наші клієнти використовують
Asra для вирішення ряду завдань:



Запровадження контролю доступу до конфіденційних даних та шифрування на рівні застосунків без внесення значних змін у архітектуру систем.



Запобігання витоку даних з боку внутрішніх та зовнішніх атакуючих.



Дотримання норм безпеки та конфіденційності даних, та підсилення фактичного рівня кібербезпеки.



Захист даних у широкомасштабних розподілених системах обробки та передачі інформації.

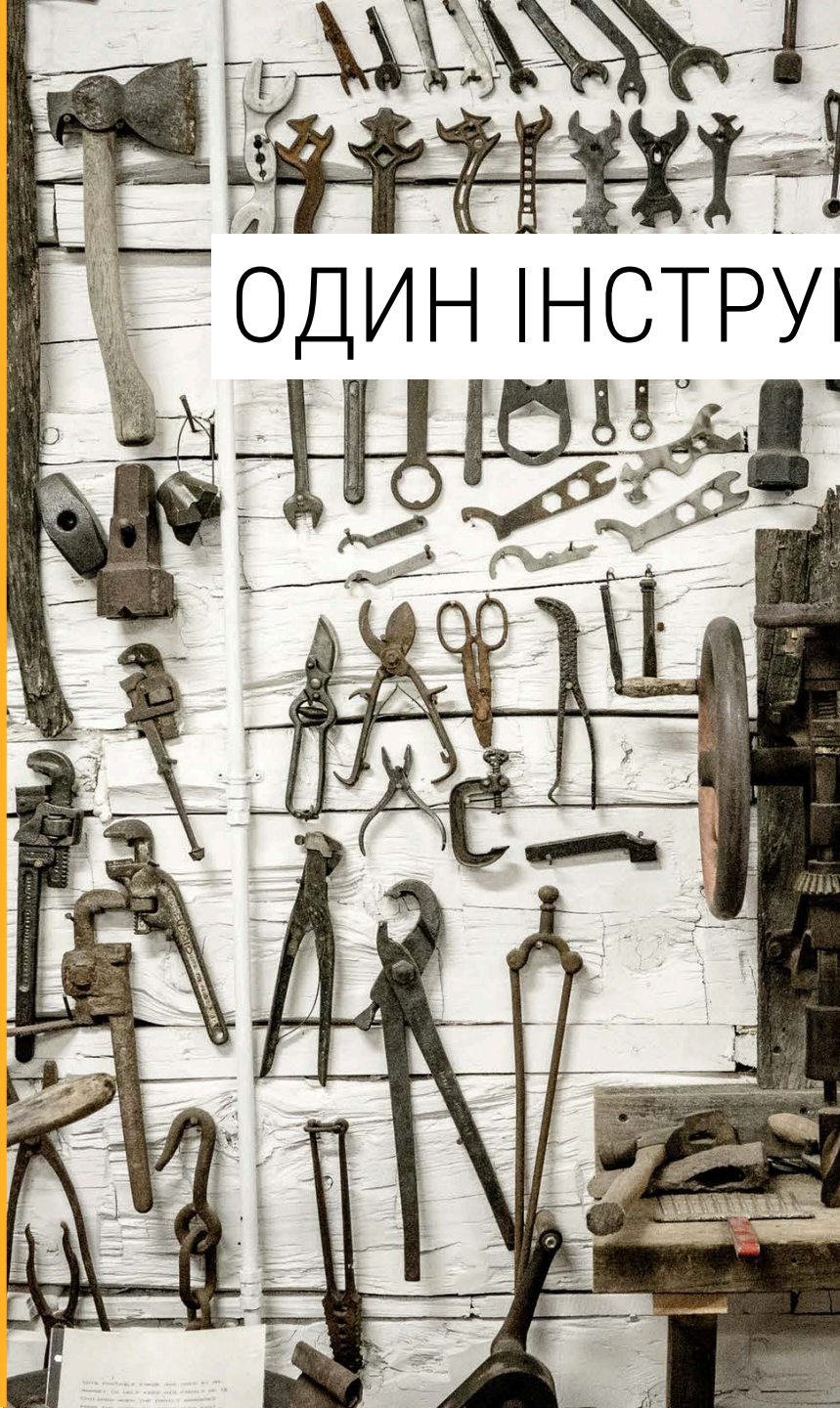
АСРА КОРИСНА ДЛЯ:



Систем, які потребують **багатoshарових та пов'язаних між собою засобів безпеки** для конфіденційних даних.

Систем, які потребують **підпорядкування новітнім регуляціям з безпеки та приватності даних**, без значної перебудови.

Великих багатокомпонентних систем, які потребують **уніфікованого набору засобів безпеки** для чутливих даних.

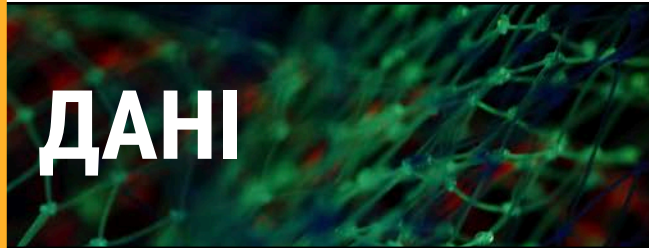


ОДИН ІНСТРУМЕНТ, 9 ЗАСОБІВ БЕЗПЕКИ

1. шифрування даних (у спокої та у русі),
2. шифрування з можливістю пошуку,
3. маскування даних,
4. токенизація даних,
5. автентифікація,
6. фаєрвол баз даних,
7. система виявлення витоку даних,
8. логування та журнал аудиту,
9. автоматизація подій безпеки.

ОДИН ІНСТРУМЕНТ, 9 ЗАСОБІВ БЕЗПЕКИ

- Менше коду, менше помилок.
- Швидко розгортати, просто конфігурувати, ефективно керувати.
- Короткий середній час виявлення та реагування (MTTD, MTTR).
- Економічно виправданий, фундаментальний вплив на безпеку.
- Підтримуйте, контролюйте та автоматизуйте один інструмент замість дев'яти.
- Аска зростає разом із вашим продуктом: масштабуйте та активуйте модулі зі зростанням вашого бізнесу.



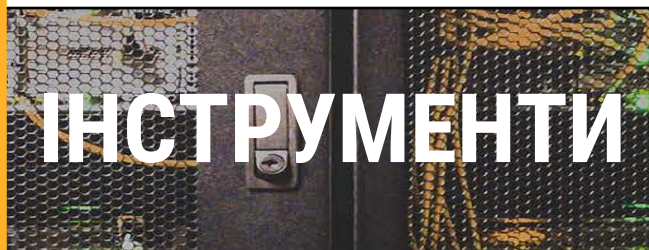
Маскування даних та токенизація:

Анонімізуйте, маскуйте або токенизуйте важливі дані. Зберігайте формат даних, додаючи шифрування та токенизацію.



Вибіркове шифрування та пошук:

Шифруйте дані будь-де, зберігайте їх зашифрованими протягом всього життєвого циклу, розшифруйте тільки коли потрібно, та шукайте в зашифрованих даних.



Контроль доступу та захист:

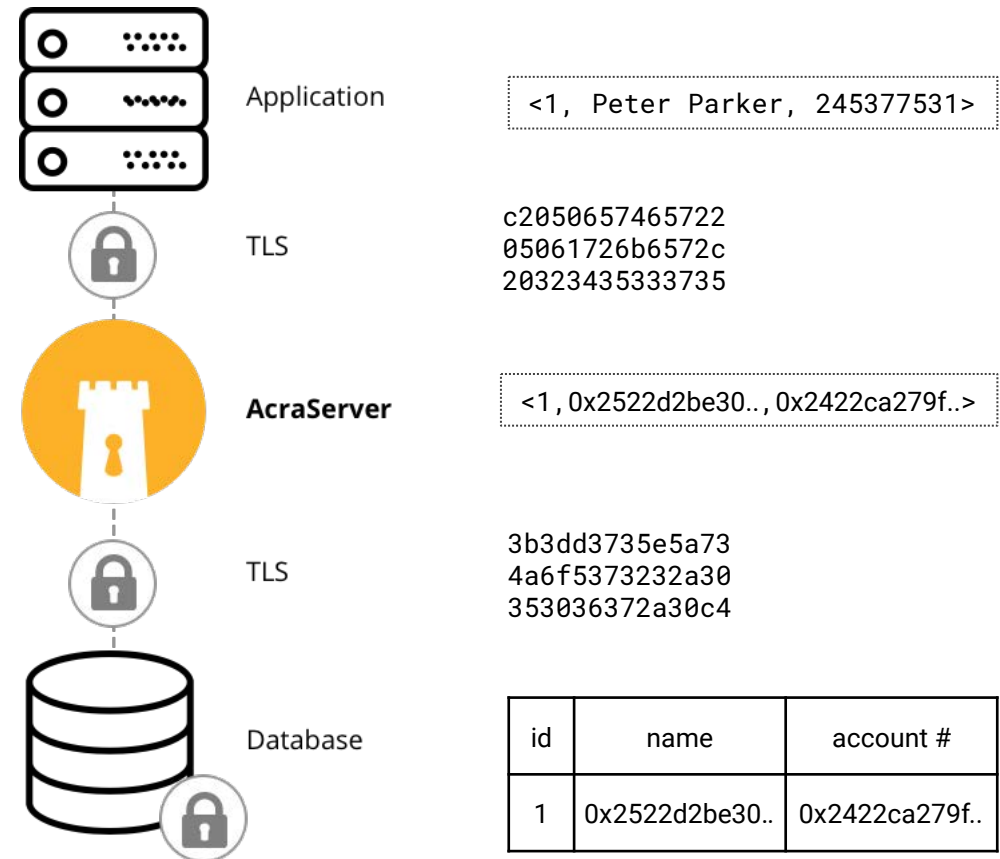
Обмежте запити до бази даних, виявляйте та запобігайте витоку даних, створюйте захищені від підробки журнали аудиту.

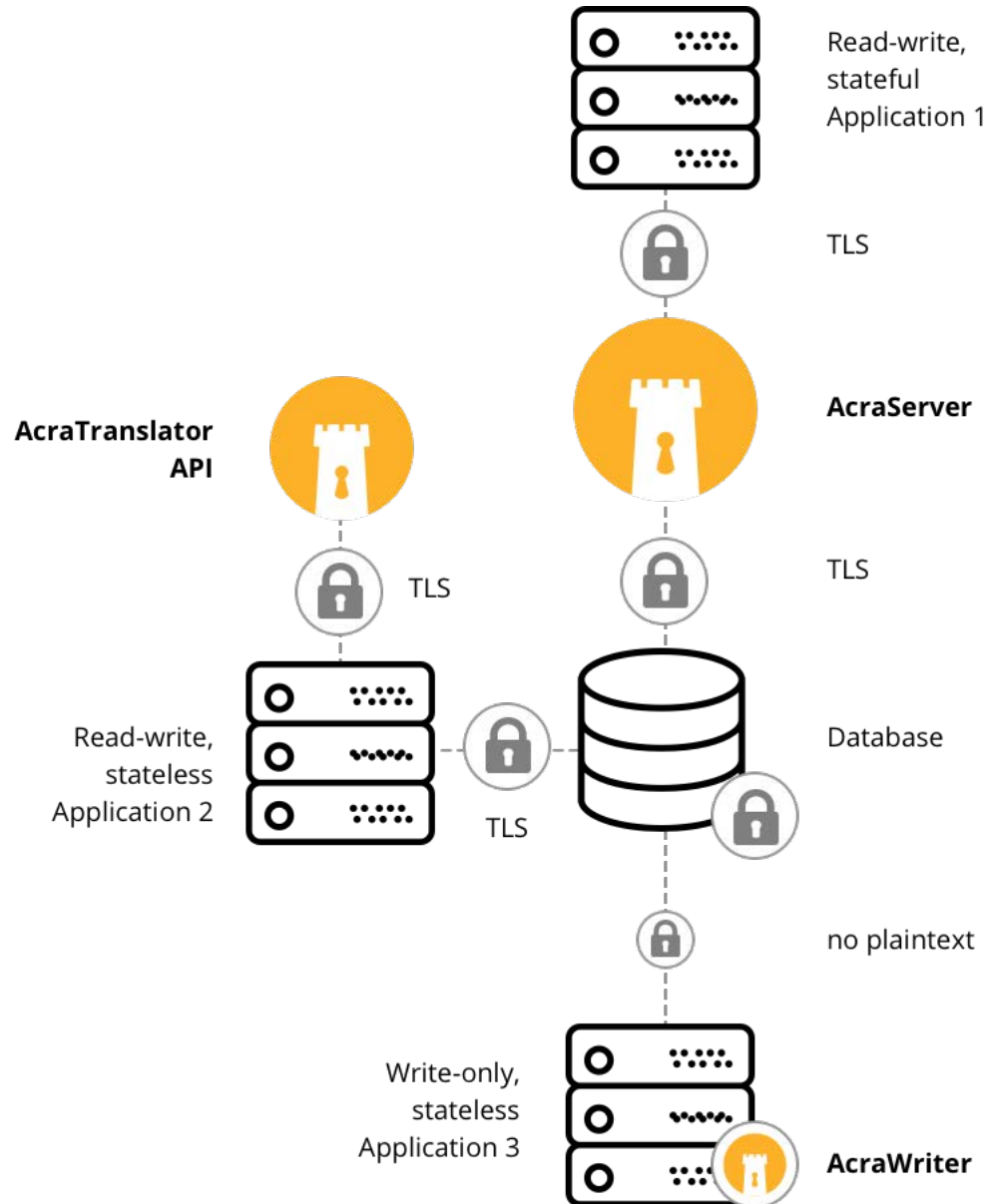
ШИФРУВАННЯ

Найпростіший спосіб інтегрувати шифрування у ваш застосунок без істотних змін в архітектурі.

Розгортайте Асра прозоро: Асра може знаходитись між застосунком та базою даних як проксі, прозоро шифруючи та розшифровуючи обрані поля.

Шифруйте лише обрану підмножину більшої структури даних для досягнення оптимального балансу швидкодії та безпеки.





ШИФРУВАННЯ

Шифруйте в будь-якому місці життєвого циклу даних за допомогою проксі-сервера бази даних, сервера API, або самостійного SDK в застосунку.

Шифруйте з write-only ключами будь-де в інфраструктурі, не ризикуючи ключами для розшифровки; розшифруйте на сервері Acra безпечним способом.

Розшифруйте лише на надійному проксі / API сервері, де криптографічні ключі захищені та під суворим наглядом.

РЕЖИМИ ШИФРУВАННЯ

ACRASTRUCT: Гнучко та безпечно

ECDH + AES 256 GCM

Шифруйте на стороні застосунку, не ризикуючи ключами розшифровки, розшифруйте лише за допомогою проксі-сервера Acra або API сервера.

ACRABLOCK: Блискавично швидко

AES 256 GCM

Шифруйте/розшифруйте лише на стороні проксі або API сервері. Менше CPU навантаження у застосунку, швидша криптографія. Збільшення довіри до keystore.

CUSTOM PRIMITIVES:

Використовуйте власні крипто-примітиви.

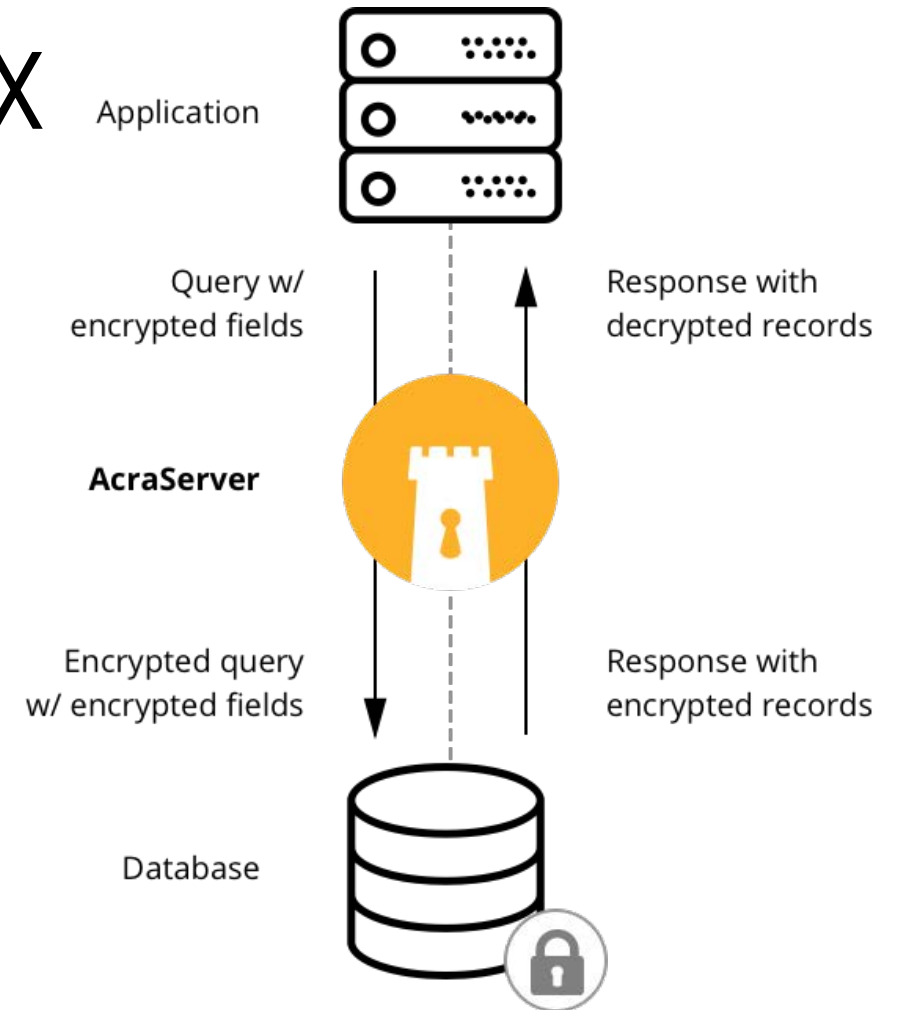
Acra дозволяє використовувати зовнішні крипто-примітиви, щоб відповідати місцевим крипто-регуляціям або використовувати HSM.

ПОШУК ПО ЗАШИФРОВАНИХ ДАНИХ

Зберігайте дані зашифрованими в базі даних, але з можливістю запускати прості запити по зашифрованих полях, не розшифровуючи їх.

Зашифрований пошук базується на підході **blind index з probabilistic bloom filters** [1], побудованими навколо AES GCM та HMAC.

Будуйте **складені зашифровані індекси** для захищених даних, щоб зробити можливими навіть складні запити по зашифрованим даним.



ПОШУК ПО ЗАШИФРОВАНИХ ДАНИХ: ЗАПИС

Запит у відкритому вигляді

```
INSERT INTO customers (id, name, email) VALUES (1, "Peter Parker", "peter@acme.corp")
```



Запит у зашифрованому вигляді

```
INSERT INTO customers (id, name_searchindex, name, email) VALUES (1, "0x13bf11de", "0xc395f2de3058847e3d50", "0x584967203916748203")
```



Database:

id	Name_SearchIndex	Name	Email
1	0x13bf11de	0x22222222e30...847e3d50	0x584967203916748203

проіндексований
зашифрований стовпчик

зашифрований стовпчик

зашифрований стовпчик

ПОШУК ПО ЗАШИФРОВАНИХ ДАНИХ: ЧИТАННЯ

Запит у відкритому вигляді

```
SELECT id, email FROM customers
WHERE name="Peter Parker"
```



Запит у зашифрованому вигляді

```
SELECT id, email FROM customers
WHERE searchindex="0x13bf11de"
```



Database:

id	Name_SearchIndex	Name	Email
1	0x13bf11de	0x22222222e30....847e3d50	0x584967203916748203



Розшифрована відповідь

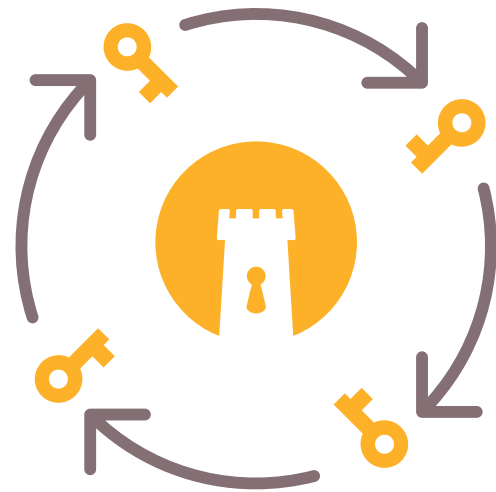
```
<1, "peter@acme.corp">
```



Зашифрована відповідь

```
<1, 0x584967203916748203>
```

УПРАВЛІННЯ КЛЮЧАМИ



Ми зробили управління ключами в Asca простим у впроваджені, простим у автоматизації та складним для зловживання, щоб управління ключами відбувалося так само просто, як і шифрування.



Генерація та реєстрація ключів, ротація та розгортання, анулювання, закінчення терміну дії, резервне копіювання, відкат даних та міграція.



Інструменти управління ключами та сховище для їхнього зберігання, в автономному пакеті з CLI, файлами конфігурації та під контролем API.

МАСКУВАННЯ ДАНИХ

Токенізація: замініть конфіденційні дані на токени і використовуйте оригінали лише за потреби. Для забезпечення додаткового захисту, зберігайте дані у зашифрованому вигляді та розшифруйте їх лише тоді, коли відбувається запит до токена.

<“Anna Jones”, 4929062148292857, \$50>

↓
tokenize

<“fce59a04b2”, 5892760396739214, \$50>

↓
de-tokenize

<“Anna Jones”, 4929062148292857, \$50>

Анонімізація/Маскування:

використовуйте повне або часткове маскування для видалення або приховування конфіденційних даних, для анонімізації даних для звітування або для обміну даними з недовіреними сторонніми особами.

<“Anna Jones”, 4929062148292857, \$50>

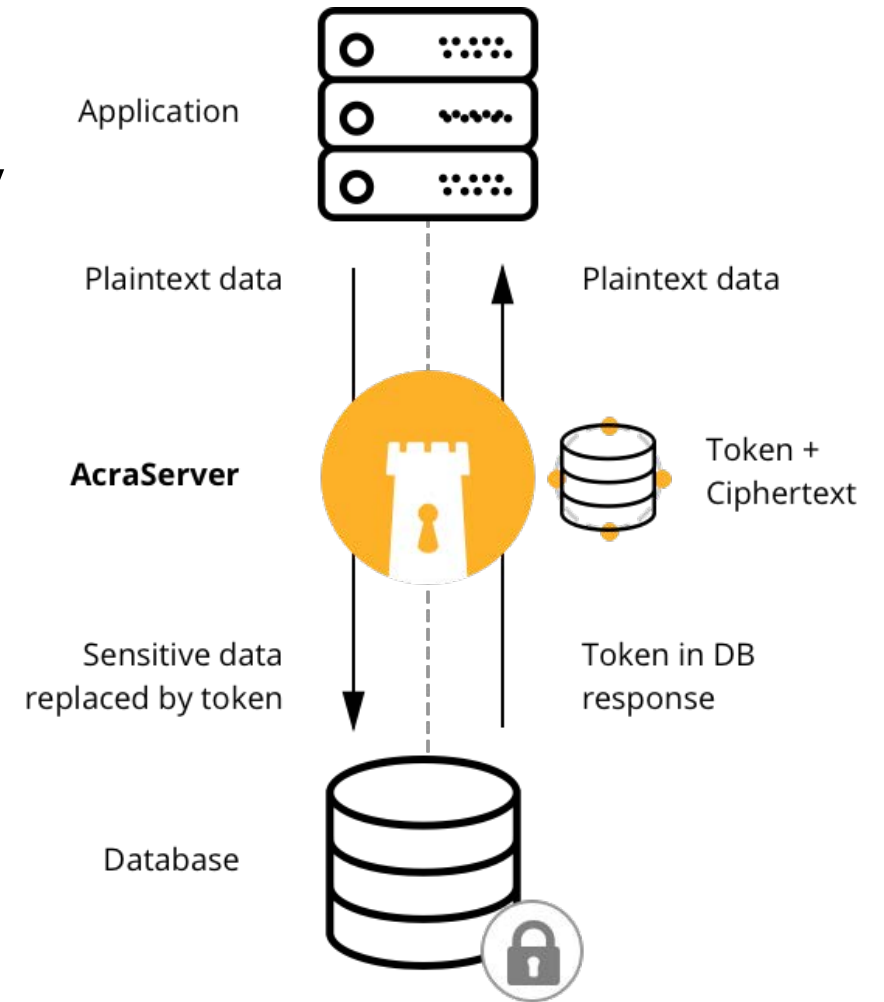
↓
mask

<“ [REDACTED]”, 4929xxxxxxxxx2857, \$50>

ШИФРУВАННЯ ЗІ ЗБЕРЕЖЕННЯМ ФОРМАТУ

Зберігайте формат даних, при цьому захищаючи їх за допомогою поєднання шифрування та токенизації.

В цьому режимі Асра виробляє токени згідно з форматом стовпчиків таблиці, і замінює на них чутливі дані. Відповідні дані шифруються та зберігаються зашифрованими за межами таблиць з обмеженим форматом.



ФАЄРВОЛ БАЗИ ДАНИХ

Acra's Request Firewall дозволяє перевірити всі запити до бази даних щодо набору правил та реакцій.

Правила фаєрволу включають семантичні патерни та атрибути таблиць/стовпчиків.

Після спрацьовування, правила призводять до множини реакцій – від вимкнення Acra або відхилення запиту до надання підроблених даних замість фактичної відповіді від бази даних.

```
# deny suspicious queries and log all queries
to user table

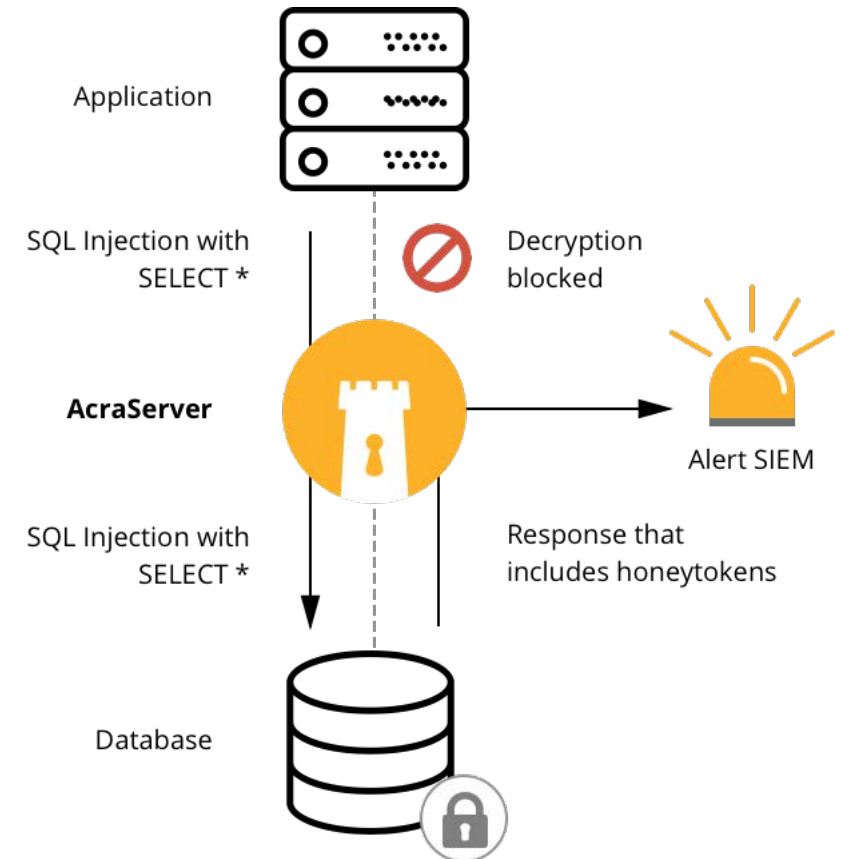
handler: deny
queries: select data_raw from plaintext_table
tables: users
patterns:
"SELECT password"
"SELECT * from users"

handler: query_capture
tables: users
filepath: users_accesslog.log
```

ЗАПОБІГАННЯ ВИТОКУ ДАНИХ

Компонент виявлення вторгнення Acra сканує потік даних за допомогою декількох методів:

- **Poison records / Honeytokens.** Acra розміщує спеціальні маркери у таблицях баз даних, які схожі на звичайні зашифровані записи. В разі виявлення маркера, Acra сповіщає про тривогу і зупиняє розшифровку.
- **Довільні патерни.** Acra можна використовувати як звичайний DLP для бази даних, щоб контролювати, що обрані шаблони або блоки даних ніколи не проходять Acra без сигналу тривоги.



ПЕРЕДОВЕ ЛОГУВАННЯ ПОДІЙ БЕЗПЕКИ

```

{
  "code":538,
  "error":"security-auth",
  "integrity": "2e2678880688b..7d369ba310a19ec88f9051f596e",
  "level":"error",
  "msg":"Can't wrap connection from acra-connector",
  "product":"acra-server-ee",
  "timestamp":"2018-04-10T20:06:31+03:00",
  "unixTime":"1583457792.225",
  "version":"0.85.0"}

```

Логи подій безпеки Асра спеціально попередньо налаштовані так, щоб допомагати операторам SIEM/SOC з аналізом та автоматизацією подій безпеки.

Щоб забезпечити захист логів від фальсифікації, Асра використовує **криптографічний захист та перевірку експортованих логів.**

Аудит логи Асра охоплюють доступ, події безпеки, зв'язують сесії з користувачами та розширюють логи застосунків надійними доказами.

SCADA & ICS SECURITY KIT

Асра надає набір додаткових функцій та модулів корисних для безпечної агрегації даних у масштабних системах ICS/IIoT/SCADA та забезпечує шлюзи між сховищами даних SCADA та зовнішніми ІТ-системами.

Збирайте: автономний SDK для збору даних з віддалених пристроїв з обмеженою можливістю шифрування та кешування даних.

Аналізуйте: інструменти для аналізу сигналів з/до популярних форматів ICS, SCADA та IIoT для забезпечення безперебійної інтеграції.

Зберігайте: оптимізоване шифрування та зберігання для ефективного захисту величезної кількості крихтих блоків даних (телесигналів) та підтримки TS-сховищ даних.

Використовуйте Асра як зовнішнє захищене сховище для історичних даних або передавач даних між SCADA та системами ІТ-аналітики, застосовуючи весь арсенал Асра для безпеки даних.

ДОСТУПНО ДЛЯ ВАШОГО ТЕХНІЧНОГО СТЕКУ.
СПРОЕКТОВАНО ДЛЯ ВАШОЇ АРХІТЕКТУРИ.

3 ШЛЯХИ ВИКОРИСТАННЯ

Acra Writer

Вбудована бібліотека/SDK тільки для шифрування даних (без можливості розшифровки), для збереження їх зашифрованими та передачі до Acra або бази даних.

Acra Server

Проксі-сервер бази даних, який аналізує дані між застосунком та базою даних, та застосовує функції безпеки Acra там, де вони доречні.

Acra Translator

API сервер, який надає доступ до функціональності Acra за REST/gRPC протоколами, з клієнтськими бібліотеками та захистом трафіку.

3 ШЛЯХИ ВИКОРИСТАННЯ: ФУНКЦІЇ

Acra Writer

Шифрування для зберігання даних локально та в базах, генерування токенів та пошукових індексів, безпечна передача даних до надійного середовища.

Acra Server

Шифрування/розшифрування, пошук по зашифрованих даних, маскування та токенізація, фаєрвол бази даних, логування подій, захист від витоку даних, автентифікація.

Acra Translator

Шифрування/розшифрування, пошук по зашифрованих даних, маскування та токенізація, логування подій, захист від витоку даних, автентифікація.

3 ШЛЯХИ ВИКОРИСТАННЯ: ПЕРЕВАГИ

Acra Writer

Найкраще підходить для збору чутливих даних за межами контрольованого периметра та подальшої їхньої передачі в систему. Допомагає ефективно керувати навантаженням та складністю системи.

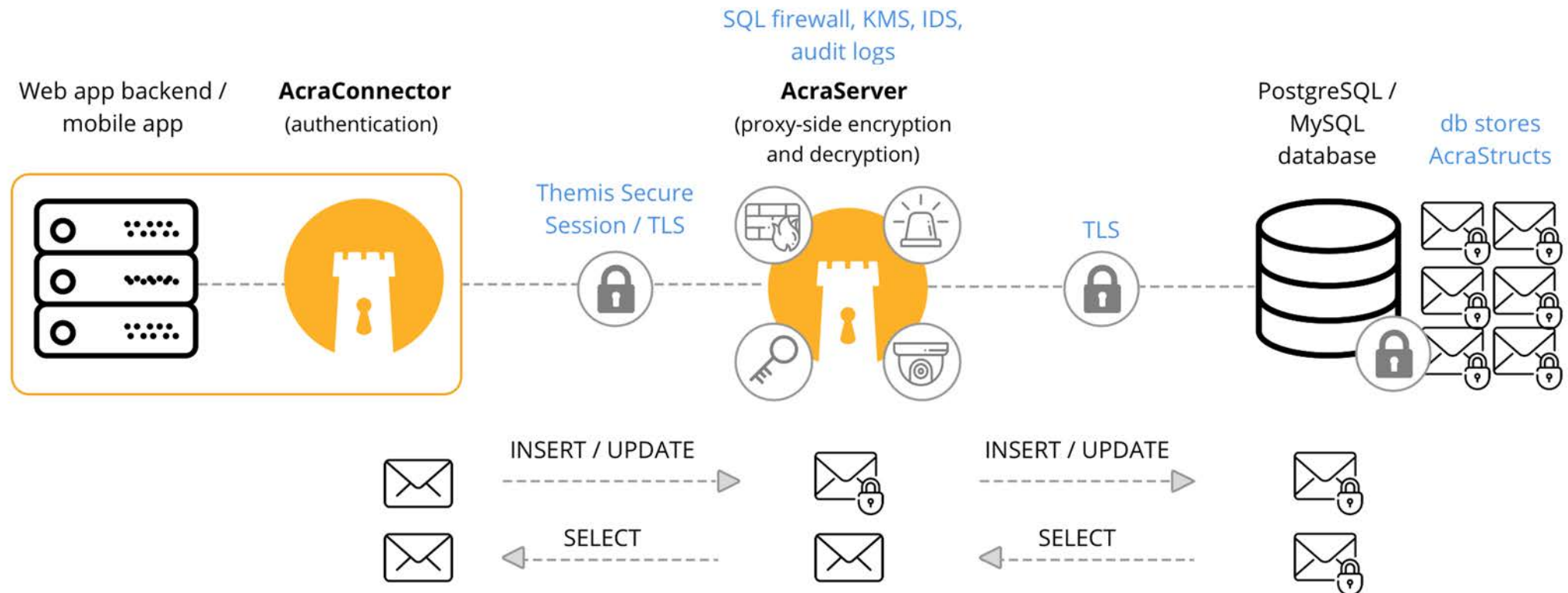
Acra Server

Найкраще підходить для інтеграції всіх функцій безпеки Acra в систему у найпростіший спосіб. Потребує певних архітектурних рішень для ефективного масштабування.

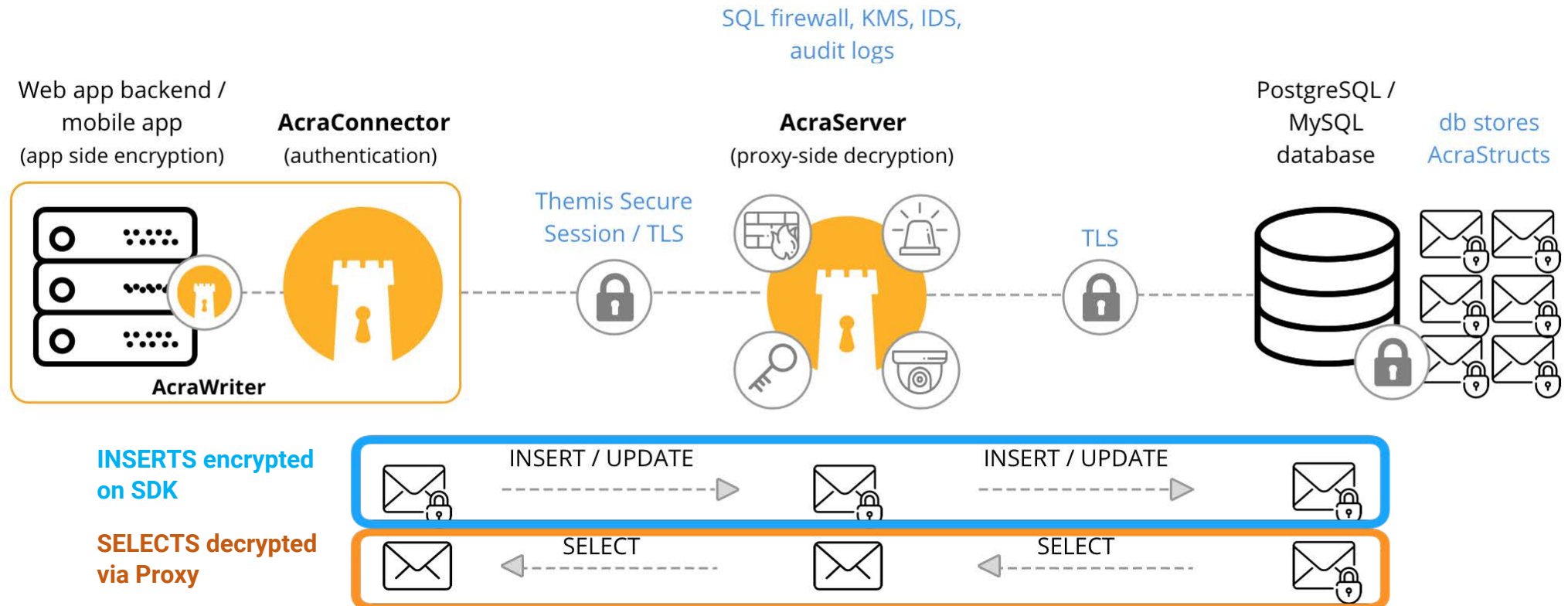
Acra Translator

Найкраще підходить для шифрування/розшифрування даних в масштабних stateless архітектурах. Потребує простої модифікації застосунків.

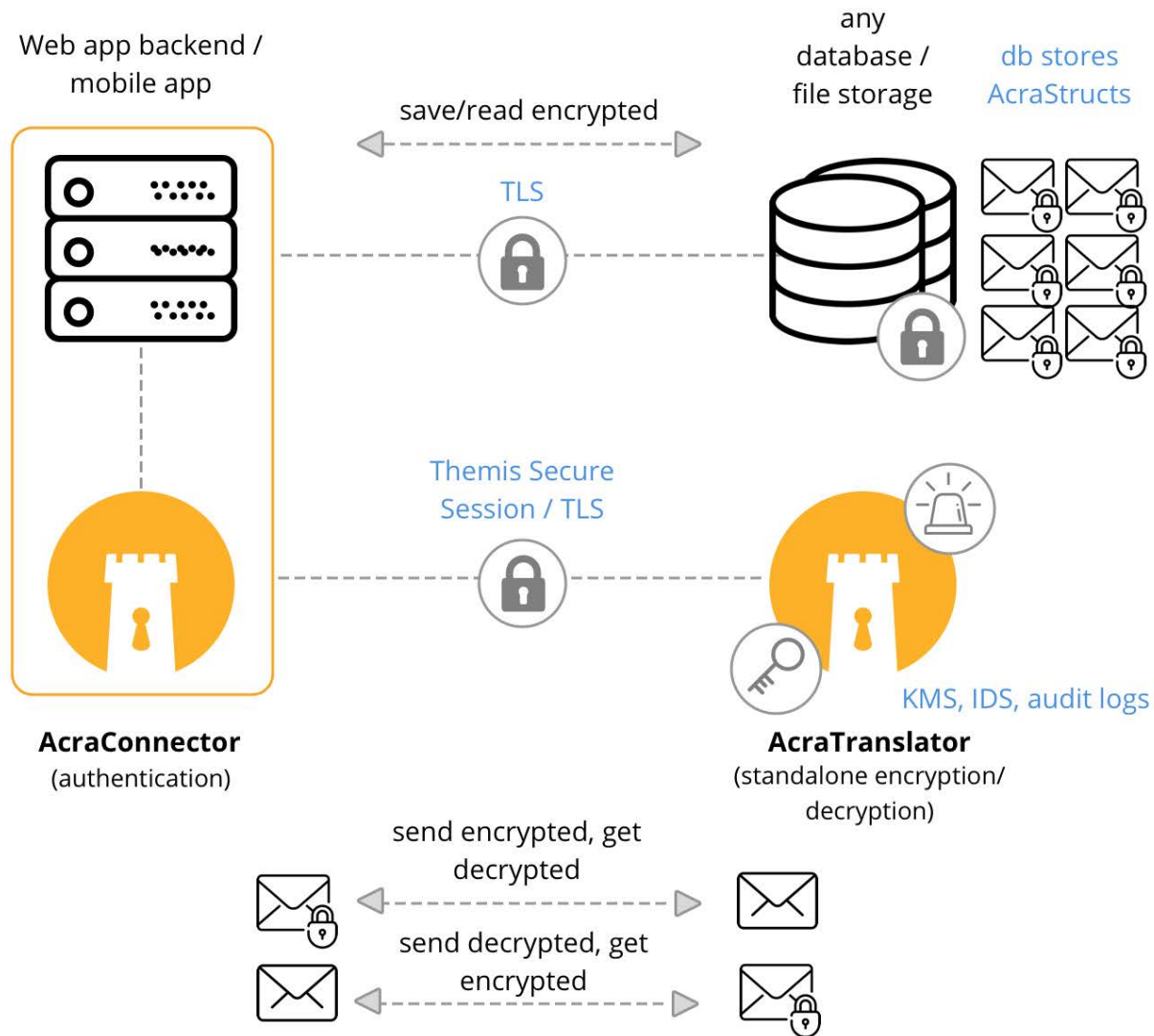
АРХІТЕКТУРА 3 ПРОКСІ-СЕРВЕРОМ



АРХІТЕКТУРА 3 ПРОКСІ-СЕРВЕРОМ ТА SDK



АРХИТЕКТУРА 3 API-СЕРВЕРОМ



ЛІЦЕНЗУВАННЯ



Community Edition

Ліцензія Apache 2, всі основні функції безпеки.
Обмежена підтримка платформ, мов програмування та баз даних.
Відсутність управління балансом безпеки/швидкодії.



Pro

Комерційна підтримка Community Edition версії,
додаткові пакети з розширеною функціональністю.



Enterprise Edition

Пошук по зашифрованим даним, пакети інтеграції, різні режими шифрування, інструменти управління ключами, інструменти для інфраструктури, допомога в інтеграції з вашою системою, декілька рівней технічної підтримки.

СУМІСНІСТЬ

Client side:	Browser: WASM/JavaScript Mobile: Swift/ObjC, Java/Kotlin IoT/embedded: C++, Rust, C Regular applications: Go, Python, Ruby, Java, C++, PHP, Node.js
Server-side:	Proxy/API server can run on CentOS, Red Hat, Debian, Ubuntu
SQL Databases:	MySQL 5.7+, PostgreSQL 9.4+, MariaDB 10.3+, Google Cloud SQL, Amazon RDS, TiDB, CockroachDB, Timescale DB
NoSQL databases:	Any datastore or database with REST API, filesystems, Amazon S3, Google Cloud DataStore
Containers:	Pure Docker, Swarm, Compose, Kubernetes

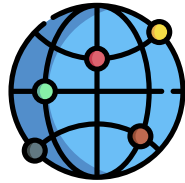
COSSACK LABS: ПРО КОМПАНІЮ

Компанія Cossack Labs була заснована у 2014 році командою експертів із захисту даних та криптографії для того, щоб допомогти сучасним технологічним підприємствам зменшити ризики, пов'язані з безпекою даних, не порушуючи зручність та гнучкість їхніх систем.

Cossack Labs створює сучасні рішення безпеки, які запобігають витоку чутливих даних, захищають дані клієнтів та дають змогу бізнесу дотримуватися регуляцій з безпеки даних.

Ми вихідці з індустрій, де безпека критично-важлива: промислові системи, фінансові послуги, державні служби та системи охорони здоров'я. Ми привносимо десятиліття власного досвіду створення зручних та надійних систем безпеки, та інтегруємо цей досвід у кожен рядок нашого коду.

GET IN TOUCH



Загальні питання: info@cossacklabs.com
Продажі: sales@cossacklabs.com
Технічні питання: dev@cossacklabs.com



Cossack Labs Limited
Suite 329, 19-21 Crawford Street
London W1H 1PJ, United Kingdom



Intelligent IT Distribution
iitd.com.ua
Юрій Гатупов, info@iitd.com.ua