cosmian

Ubiquitous Encryption: higher security & performance.
No more excuses. Move to data/s.

▸ www.cosmian.com

Cloudproof Encryption

Access & search encryption for your data in the cloud

In complex, scalable infrastructures, encryption must abstract physical implementations and must provide a way to securely and quickly find and extract discrete data across the entire encrypted repository. You need application-level encryption with encrypted search.

Cloudproof Encryption brings improved security, high performance at the application level.

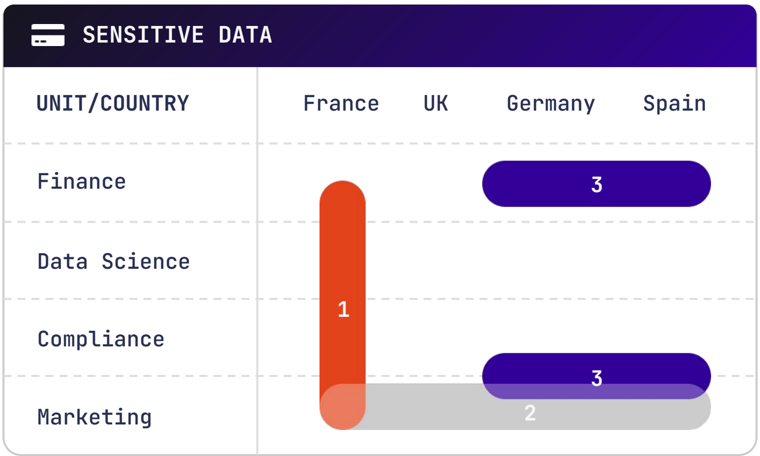
And it’s open source.

Adapts to your business

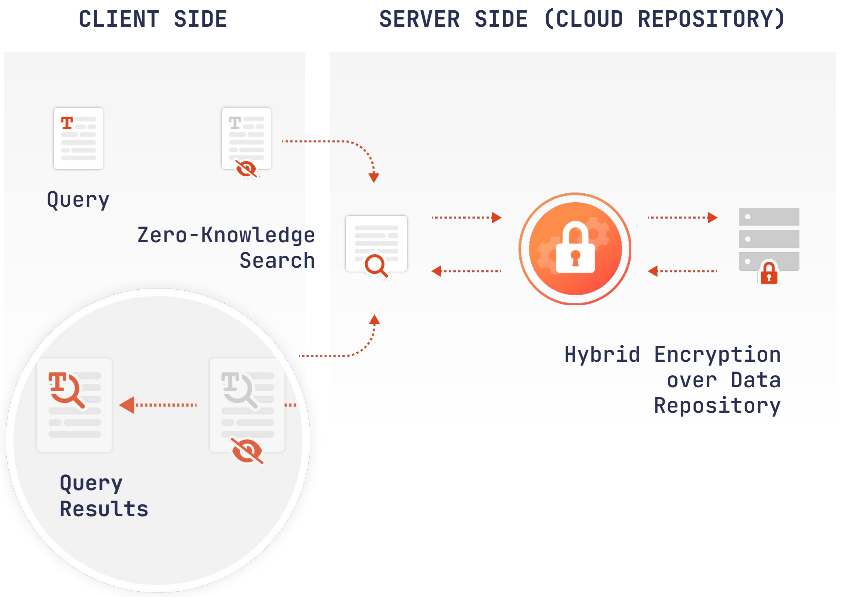
Application level encryption with freely defined attributes along multiple axes and user decryption keys embedding access policies, simply defined as boolean expressions over the attributes.

The cloud learns nothing

Everything is encrypted: the data, the indexes, the search queries, and their response. Data is kept encrypted at all times and only decrypted on the end user's device.



- (Unit::*) && Country::France
- (Unit::Marketing && Country::*)
- (Unit::Marketing || Unit::Compliance) && (Country::Spain || Country::Germany)


CLIENT SIDE
SERVER SIDE (CLOUD REPOSITORY)
Query
Zero-Knowledge Search
Query Results
Hybrid Encryption over Data Repository

Designed for big data repositories

Encrypted data partitioning facilitates feeding data from multiple sources, the management of ciphertext rotations, and defining policies for extractions. Encrypted search provides a secure mechanism to quickly find encrypted data across the partitions.

cosmian

Ubiquitous Encryption: higher security & performance.
No more excuses. Move to data/s.

▸ www.cosmian.com

Cloudproof Encryption

Performance

200µs

Encryption/Decryption: about 200µs (0,0002s) for a ciphertext for one partition.

10 to 20%

Ciphertext Expansion: 10% to 20% compared to cleartext size.

Cryptographic Technology

Cloudproof encryption is based on 2 open source cryptographic stacks: **CoverCrypt** and **Findex**. They respectively provide a fast version of access control encryption and searchable encryption.

These stacks are actively designed by Cosmian cryptographers in collaboration with the ENS/CNRS/INRIA cryptographic lab headed by Pr. David Pointcheval.

The reference implementation of the stacks is developed in Rust according to the ANSSI guidelines and is submitted for their review.

Packaging

Cloudproof Encryption is packaged in open-source libraries, and directly available on [GitHub] in multiple languages, including Java, Javascript, Python, and Rust. They expose APIs meant for developers who are not cryptographers.

Libraries run on all operating systems, including Android and IOS, as well as inside browsers (using Javascript and Web Assembly).

Plugins are available for Spark and Denodo, with examples in Java for Kafka and the Hadoop ecosystem.

Flutter python Linux
hadoop APACHE Spark JS 5
mac OS iOS android Java

Pricing

Annual license based on the number of encrypting servers.

Improved security model

Using application level encryption limits the attack surface. Ciphertext partitioning limits the consequences of key leakage.

Post-quantum

Hybridization with post quantum cryptography provides security against future threats (following ANSSI recommendation).

Easier to deploy

Encrypting systems do not need to be secured since they only use the public key. Decryption keys are only created when needed.

Scalable

Everything but private keys is in the cloud. Everything in the cloud is encrypted.

cosmian

About Cosmian

Cosmian is the leading platform for securing sensitive applications and data through the use of advanced cryptographic technologies.Data is encrypted everywhere and at all times: this is Ubiquitous Encryption.