

**Improve data protection and fraud prevention  
with advanced cryptography.**

**OSSIR - 9 November 2021**

# **Cosmian helps you to operate in secure, Zero Trust environments.**

**“I have a SaaS offering but my clients don’t want anymore to send their data to my platform in clear text”**

**“I have a secret algorithm that I want to run on my client’s remote data sets”**

**“I want to send sensitive data via email to my customer and I want to make sure that he is the only one who can access it”**

**“I want to make sure my sensitive files are only accessed & retrieved by the authorized people”**

# Yes, there are risks.



## **GDPR Risk**

Will necessary  
processes be  
followed?



## **Cloud Act Risk**

Can the cloud be trusted ?



## **Cyber Risk**

Can my data leak ?

# This is how we address these critical use cases with advanced cryptography.

**“I have a SaaS offering but my clients don’t want to send their data to my platform in clear text”**

- Data anonymization
- Sensitive data stay encrypted / protected during computation

✓ Confidential Micro-Services

**“I have a secret algorithm that I want to run on client’s remote data sets”**

- Encryption of algorithms / parameters
- Run the encrypted algo in the cloud over customer (encrypted) data

✓ Confidential Micro-Services

**“I want to send sensitive data via email to my customer and I want to make sure that he is the only one who can access it”**

**“I want to make sure my sensitive files are only accessed & retrieved by the authorized people”**

- Direct encryption at the edge with advanced cryptography (> actual end-to-end encryption)
- Authorization Policy embedded in encrypted data
- Key Management for many keys

✓ Encryption/decryption at the edge

✓ KMS

**Cosmian in action.**





***Move your data &  
applications in the cloud  
with the same level of  
security.***

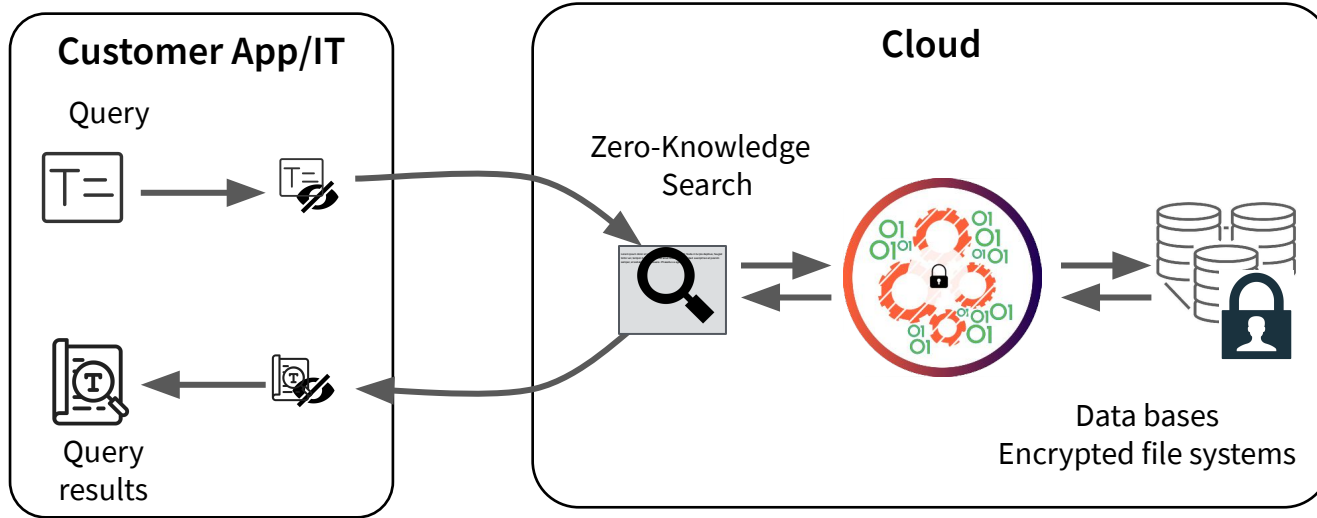
Queries directly processed over **encrypted databases.**

The cloud can't **learn anything from the computation.**

**No key in the cloud.**



## Encryption of files directories & databases in the cloud. Encrypted queries over encrypted data. No key in the cloud.



- **Exploit cloud storage and computation without losing control of confidential assets (data, applications...)**
- **The cloud can't learn anything from the computation: data + indexes + queries + result queries are encrypted.**
- **No key in the cloud. Individual user key.**



***Harden data access of your existing IT systems.***

Advanced cryptography helps you to:

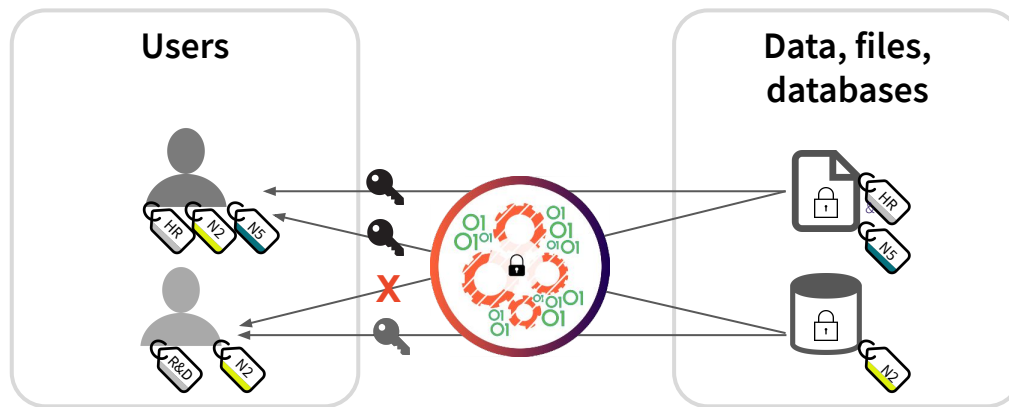
Harden the **security of your legacy applications**

Encrypt & manage your sensitive files, data and queries with **powerful, precise access right management.**





**Increase security of data access policies when data stored in the cloud.  
Data are encrypted with authorization attributes.**



- Users & Data are provided with attributes - based on team, confidentiality level...
- To retrieve a data in clear text, you need to have the right attribute(s)
- Access control attributes are embedded in the data when encrypted in the cipher text itself - a far more secure protection against cyber attacks vs. centralized access solutions.



***How to run your models in the cloud on your clients' sensitive data while protecting your IP.***

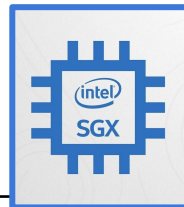
**Fintech :** IP protection of machine learning models in use over banks' sensitive data.

**Medtech/Biotech :** IP protection of statistical, models in use over sensitive data in hospitals, pharmaceutical laboratories, medical sensors.

**Financial Services - Cyber :** Protection of confidential fraud detection algorithms in use over sensitive data in subsidiaries.



# Confidential Computing with Secure Enclave: Confidential algorithm protected at runtime.



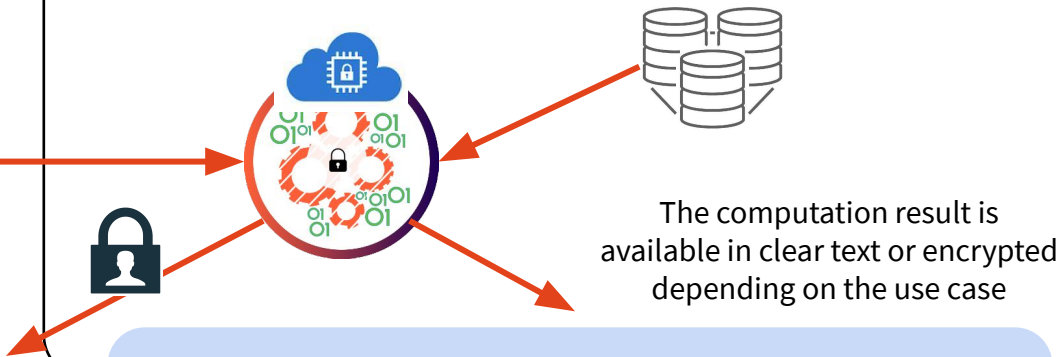
## Third Party/Partner with Proprietary Algorithm

Encrypted  
Algorithm before  
deployment in the  
Secure Enclave



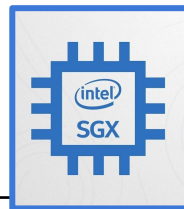
Cosmian patented the special key ceremony needed to encrypt the algorithm with Secure Enclave specific secret.

## Data Owner's Premises



- **Proprietary Algorithm decrypted in the Secure Enclave at runtime**
- **Secure Enclave prevents any system admin to have access to the algorithm during the computation**

# Confidential Computing with Secure Enclave: Protection of sensitive data and proprietary algorithm at runtime in the cloud => Confidential Micro Services



## Third Party/Partner with Proprietary Algorithm

Encrypted  
Algorithm before  
deployment in the  
Secure Enclave



## Secure Enclave in the Cloud



## Data Owner's Cloud



Data is encrypted  
before upload into  
the Secure  
Enclave

Cosmian patented the special key ceremony  
needed to encrypt the algorithm with Secure  
Enclave specific secret.

- **Proprietary Algorithm & Data only decrypted in the Secure Enclave at runtime**
- **Secure Enclave prevents any system admin to have access to the algorithm and data during the computation**

***Improve the confidentiality  
of your fraud & cyber  
detection systems.***

**Financial Services :** Protection of confidential fraud detection algorithms in use over sensitive data in subsidiaries.

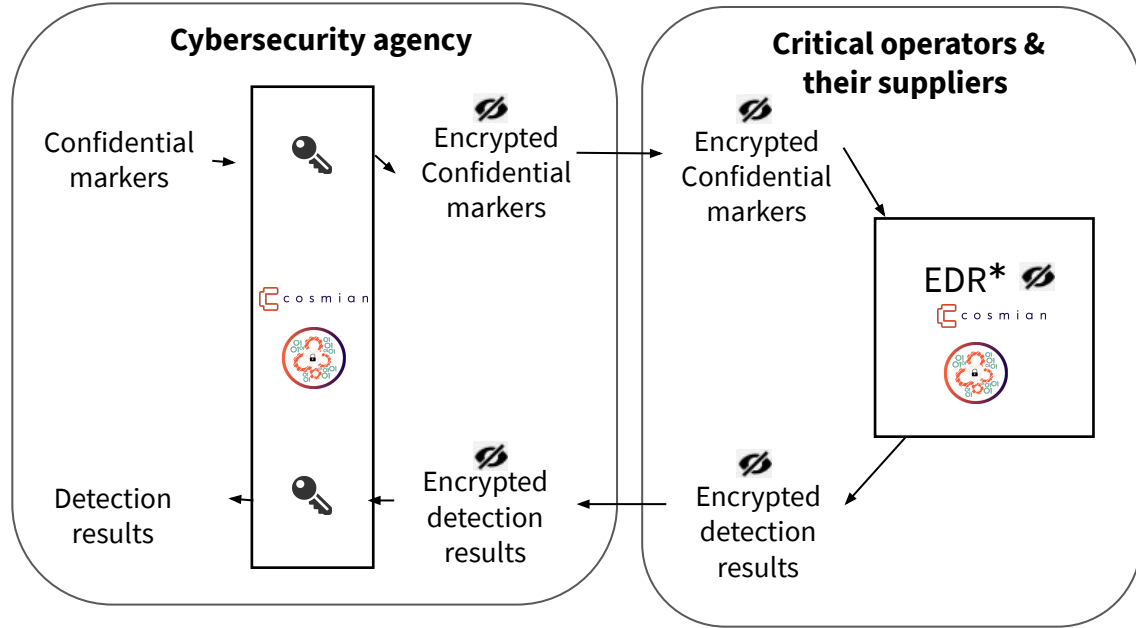
**Financial Services :** Confidential compute and analyze of KPIs over suspicious IBANs.

**Cybersecurity :** Confidential mining & analyzing of cyber intel data between SOC/CERTs.

**Cybersecurity :** How to process & analyze confidential, sensitive markers in detection systems.

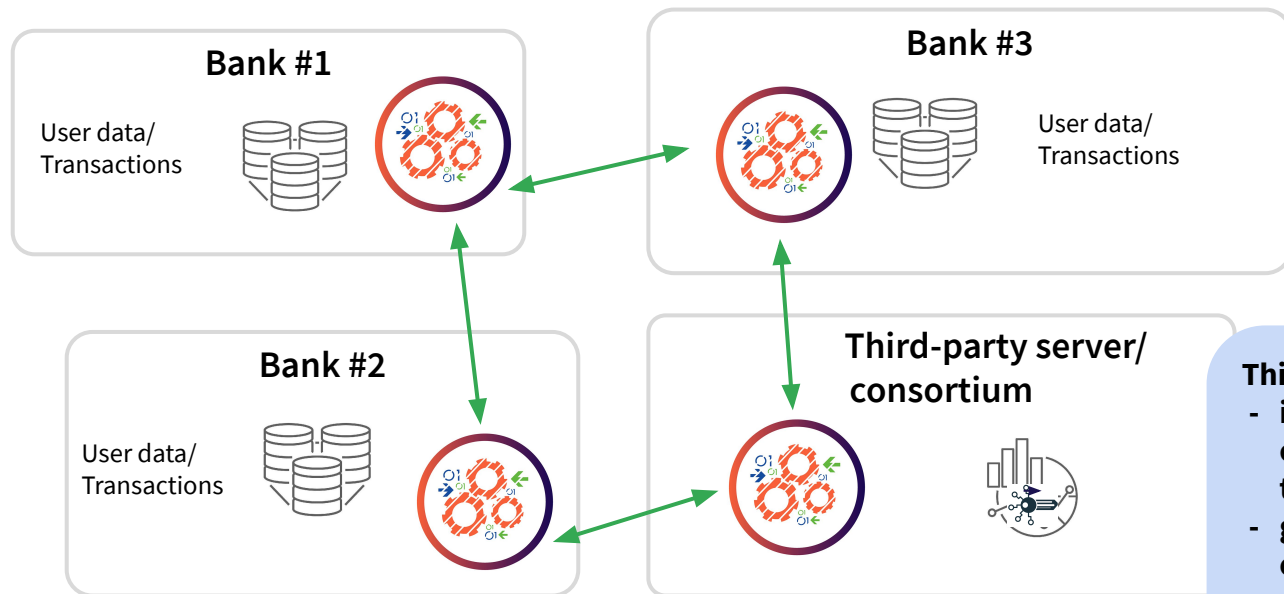
## How to process & analyze confidential, sensitive markers in detection systems.

Deploy super sensitive markers into critical operators' detection systems without compromising the markers.



\*EDR : Endpoint Detection & Response

## Financial Services : Fraud detection / Confidential compute and analyze of KPIs over suspicious IBANs.

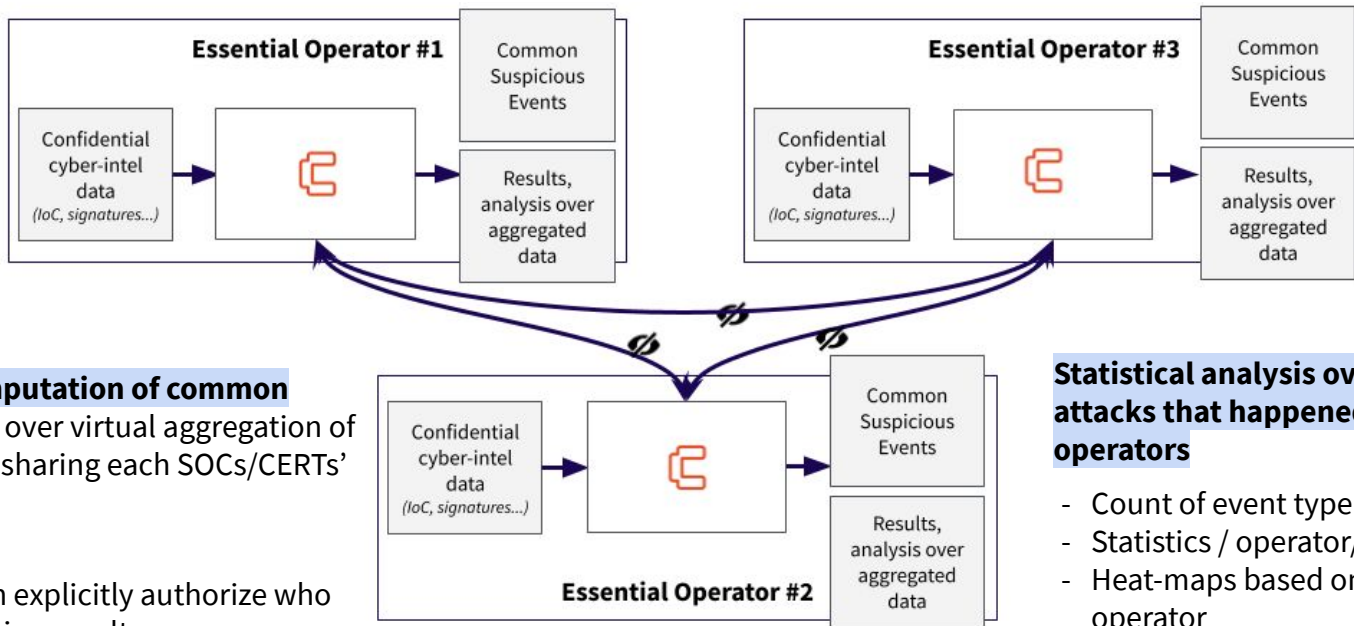


**Third-party server/consortium :**

- implements collaborative computations as approved by the consortium banks.
- guarantees the engagement of each participant in the computation.

**Results of analysis  
KPIs**

# #1 - How to increase SOC/CERTs collaboration: detection of common suspicious events, statistical analysis over confidential cyber-intel data.



**Intersection Computation of common events** processed over virtual aggregation of IoCs without ever sharing each SOC/CERTs' IoCs

Each Operator can explicitly authorize who will use the detection results.

**Statistical analysis over events or attacks that happened in several operators**

- Count of event type
- Statistics / operator/region
- Heat-maps based on event type / operator
- Customized algorithms

2020 I-nov Cybersecurity Award BPI/ANSSI)



***Increase learning across entities' data silos while guaranteeing compliance.***

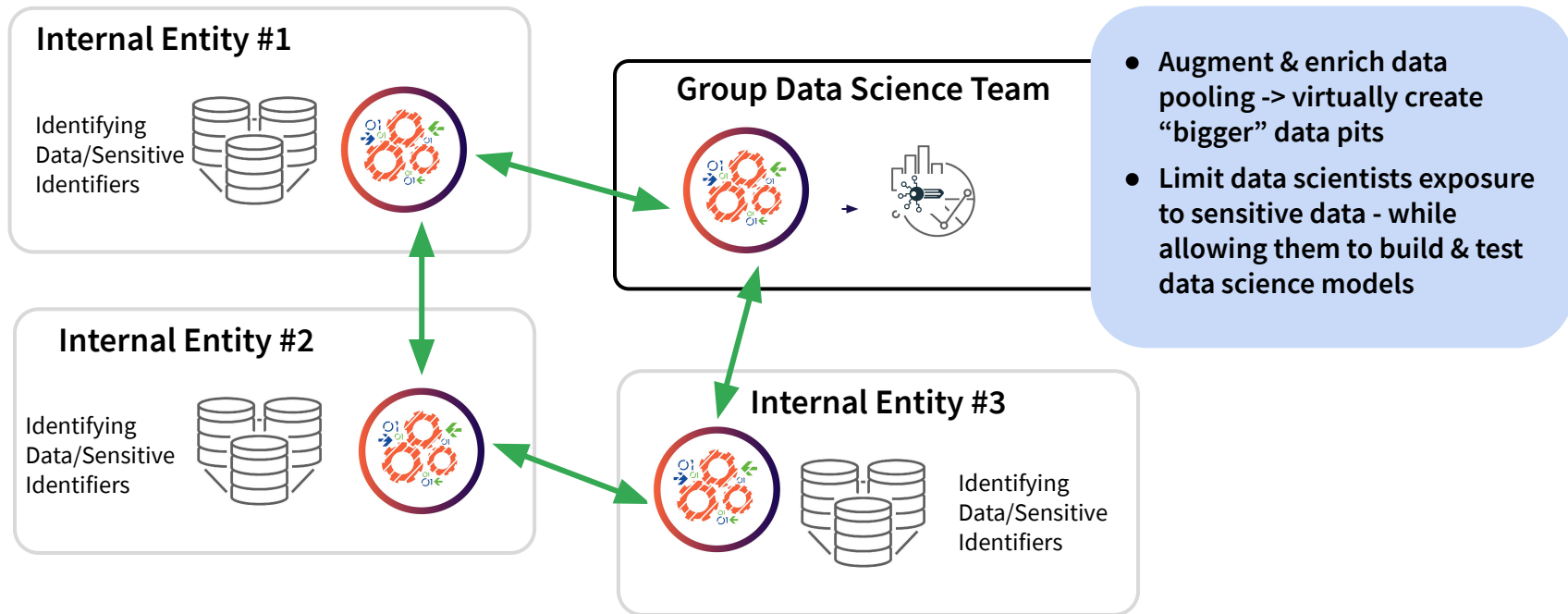
**Multi-party analysis of confidential satellite trajectories** between satellite operator competitors.

**Pathology scoring** over combined health data.

**Data Science Modeling** on encrypted sensitive identifiers from different internal data sources.

How to dashboard KPIs **without ever revealing the participants' KPIs.**

## Financial Services: Data Science Modeling on encrypted sensitive identifiers from different internal data sources.



**About Cosmian:  
a few words from customers & partners.**





“

Cosmian develops a platform to empower key players to pool data , without any of the players to access other parties' sensitive data. It is very obvious to understand the potential of this platform: you need to share data but you need to protect private data. It's critical!

Michel Paulin  
CEO OVHcloud - OVHcloud Summit 2019

Source : [Keynote - #OVHcloudSummit 2019 FR](#)



“

We work with Cosmian, they proposed us a cloud encryption solution. It is extremely useful. It's a matter of sovereignty.

Laure Belluzzo  
CEO Technologies & Services, Crédit Agricole Bank

Source : [Netexplo](#)



“

Cosmian is both a pioneer and a leader in very advanced cryptographic technologies - they allow us to meet our customers' confidentiality requirements . There is a whole range of customers we could not have reached without Cosmian.

Julien Cantegreil  
Founder and CEO, Spaceable

Source : [BSmart TV](#).

# Solving the Data Paradox: How to use sensitive data without compromising data security nor data privacy.

Cosmian established key partnerships with **world-renowned academic teams** to leverage the most advanced cryptographic techniques.

ENS Ulm/CNRS/INRIA Computer Sciences Laboratory headed by M. David Pointcheval  
COSIC//Computer Security & Industrial Cryptography Group, KU Leuven, headed by M. Nigel Smart.



KU LEUVEN



COSIC

We also partnered with industrials at the forefront of Secure Enclave hardware solutions..



Cosmian is a proud member of





Virginie Anne  
Pre-Sales Engineer  
[virginie.anne@cosmian.com](mailto:virginie.anne@cosmian.com)

Bruno Grieder  
CTO, co-founder  
[bruno.grieder@cosmian.com](mailto:bruno.grieder@cosmian.com)

Sandrine Murcia  
CEO, co-founder  
[sandrine@cosmian.com](mailto:sandrine@cosmian.com)