— TECHNOLOGY PRESENTATION

CYSEC

Data security at scale

CYSEC is a European data security company providing a software solution in Confidential Computing, which enables companies to secure business logic (workloads) on distributed infrastructures (from the core to the cloud and to the edge).
CYSEC's flagship solution, called «ARCA Trusted OS» is a hardened Linux-based operating system combined with a secure Kubernetes orchestrator providing a trusted runtime platform for containers. ARCA provides cryptographic functions, in order to protect keys, code and data, be it at rest, in transit and in use.

ABOUT US

- Founded in 2018
- A team of +30
- Based in Switzerland and Europe
- Active in the following industries


Healthcare


Industrial Automation


Smart Infrastructure


Energy


Space


Automotive


Financial services

Member of CONFIDENTIAL COMPUTING CONSORTIUM

www.cysec.com

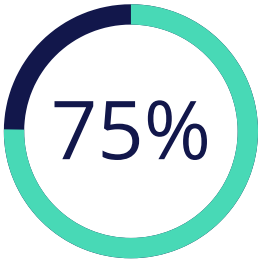
Our business

CYSEC is a pionner in Confidential Computing for several verticales
The company provides a Trusted Execution Environment (TEE) for containers.
We help companies to enforce data security on distributed architectures (from the core, to the cloud, to the edge).

OUR MISSION

Our mission is to protect business sensitive data on distributed architecture enterprises don't own or control.
We believe organizations should be able to benefit from state-of-the art security in a straightforward, transparent and cost-efficient way.

MARKET TRENDS



By 2025, 75% of enterprise-generated data will be created and processed in the cloud and at the edge, outside of a traditional data center.

*References: Gartner Gartner: By 2025 half of enterprise IT spending will be for cloud | Network World

5X increase in Data Volume (2020 - 2025)

The adoption of cloud computing and edge computing is extremely fast to process and access those sensitive data to create business value out of it.

MAIN PROBLEMS

Data-in-use had become the primary risk for IT hybrid and distributed infrastructures.

Challenges

- Extending infrastructures footprint to the cloud & the edge provides a new surface for attackers
- Lack of trust in infrastructure enterprises don't own and/or control
- Data protection regulations

Confidential Computing solution

INTRODUCING THE TECHNOLOGY

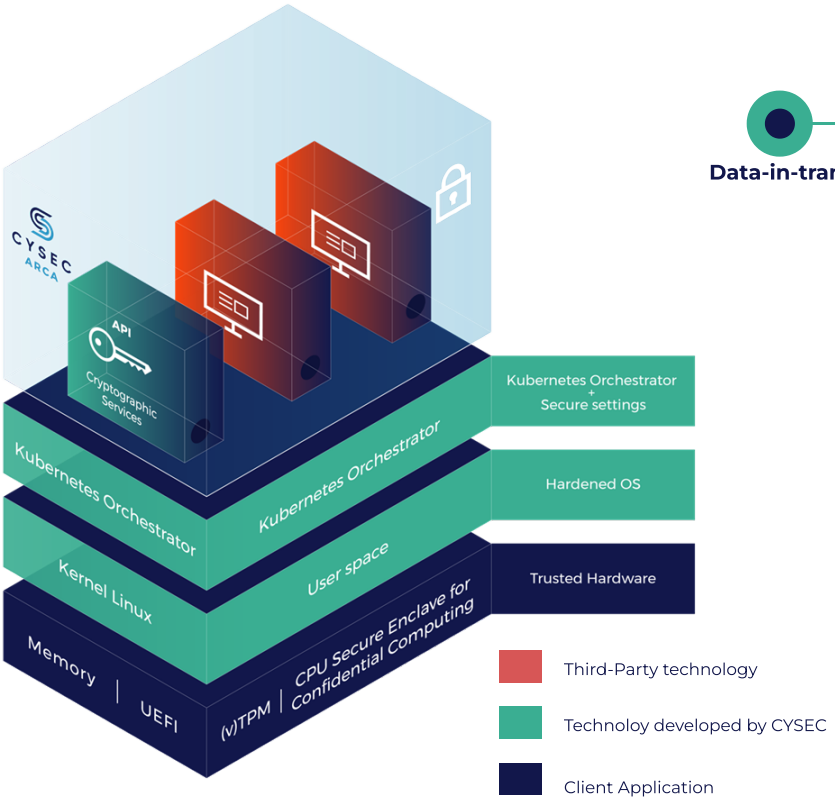
Confidential Computing prevents unauthorized access and modification of data & code while being executed. Computation is performed in an isolated hardware-based enclave to protect data in memory during computation. It provides full data confidentiality and integrity, as well as code integrity. Confidential computing provides businesses with more trust that their data in the cloud and in the edge is secure and private.

WHAT WE PROVIDE

We help to protect and isolate sensitive data and code on hybrid architecture from Data Center, to the Cloud, to the Edge, with ARCA Trusted OS, a Trusted Execution Environment (TEE) for containers

ARCA TRUSTED OS

Arca Trusted OS is a hardened Linux-based operating system combined with a secure Kubernetes orchestrator to provide a trusted runtime platform for containers.
ARCA eases the adoption of **Confidential Computing** and provides cryptographic functions to protect **keys, data & code.**



We help enterprise in the adoption of **Confidential Computing** and protection of data-in-use, in transit and at rest.

Securing sensitive data

REGARDING THE CONTEXT OF DATA, WE SECURE

Sensitive data migration on the Cloud
Homogeneous security on multiple cloud/hybrid cloud strategy

Blockchain node and digital assets
We protect the node that runs Custody, Vault micro services, transaction signatures

Data processed at the Edge
Protect hyper service personalization in branches (AI Robbot to face customers)
Real-time fraud detection at ATM and Branches (Facial Recognition)

Multi-party computing
Share sensitive data with third parties for better result such AML & Fraud prevention
Multi-Party analytics using AI/ML

OUR VALUE PROPOSITIONS

Protection of containers without code modification
It speeds up case deployment

Deployment of the same TEE on a distributed architecture
It enforces homogeneous security level across core / cloud/ edge

Confidential Computing protects data-in-use
It enables to deploy data & applications on infrastructures enterprises don't own and/or control

Securisation of distributed key management system
Multi-clouds and hardware agnostic

GET IN TOUCH

CYSEC

EPFL Innovation Park - Building D
CH 1015 Lausanne
Switzerland

Website

www.cysec.com

Email

patrick.trinkler@cysec.com

CYSEC