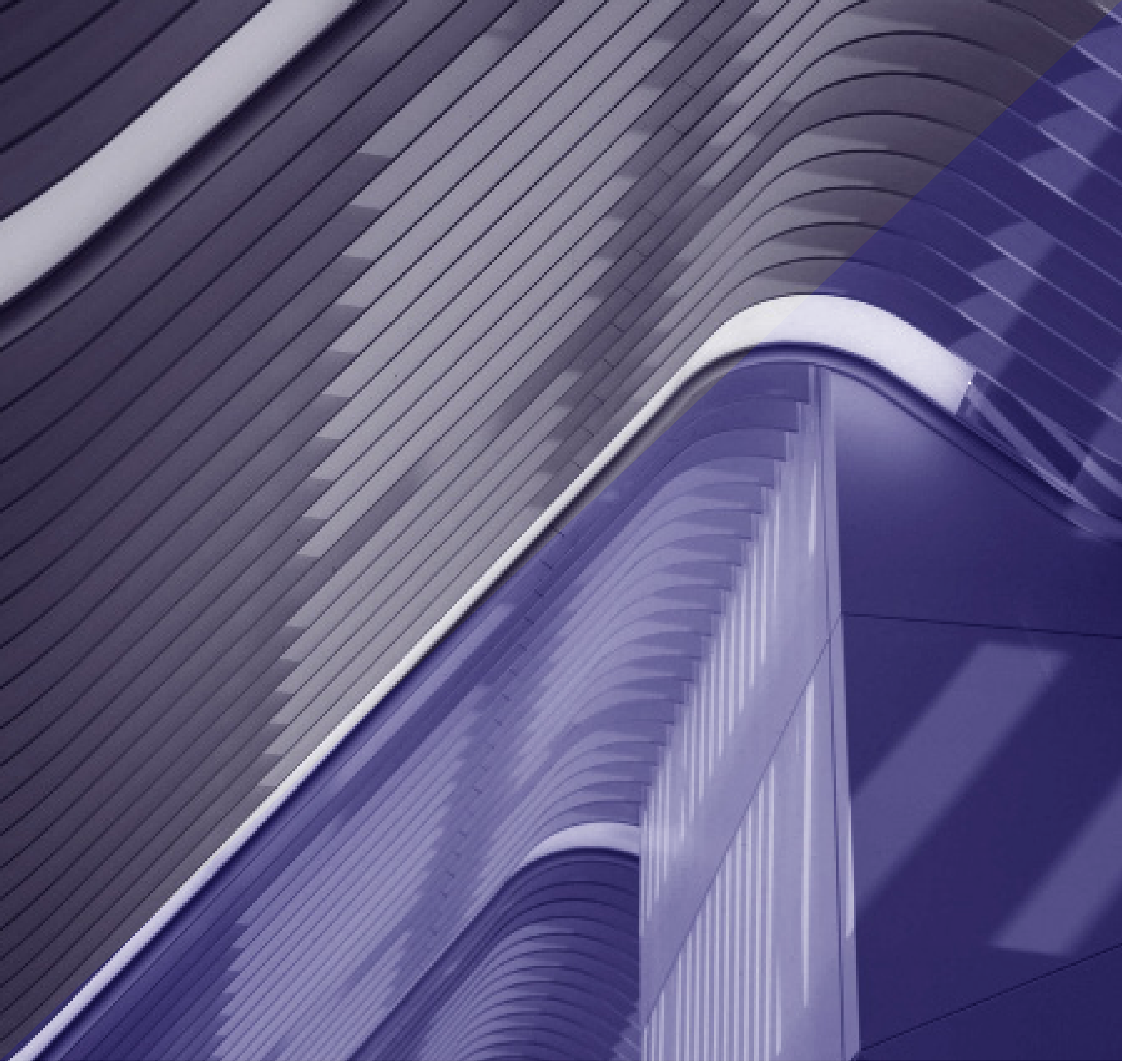


CYSEC
ARCA SPACE

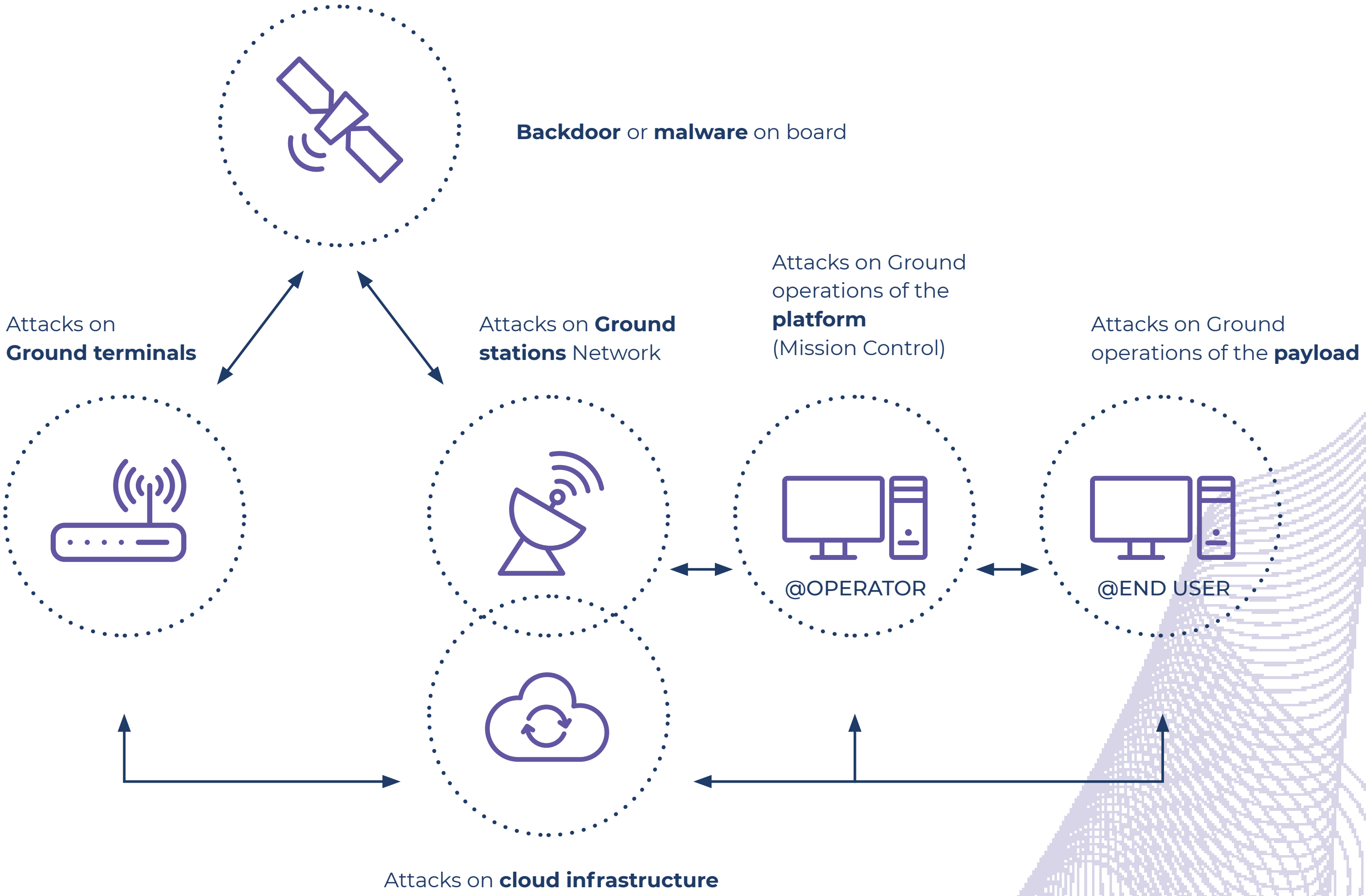
ARCA SPACE
End-to-end Security for commercial space missions

CYSEC
ARCA SPACE

CYSEC ARCA Space

Prevent cyber-attacks on space systems with an end-to-end confidential computing environment on ground and on board

Satellites are built to be robust and durable, but not designed with security in mind. In a complex environment, with a large attack surface that is difficult to secure, structural vulnerabilities are widespread. The increasing amount of valuable data collected and transmitted in space, has become low-hanging fruit for cyber criminals.



Backdoor or **malware** on board

Attacks on **Ground terminals**

Attacks on **Ground stations** Network

Attacks on Ground operations of the **platform** (Mission Control)

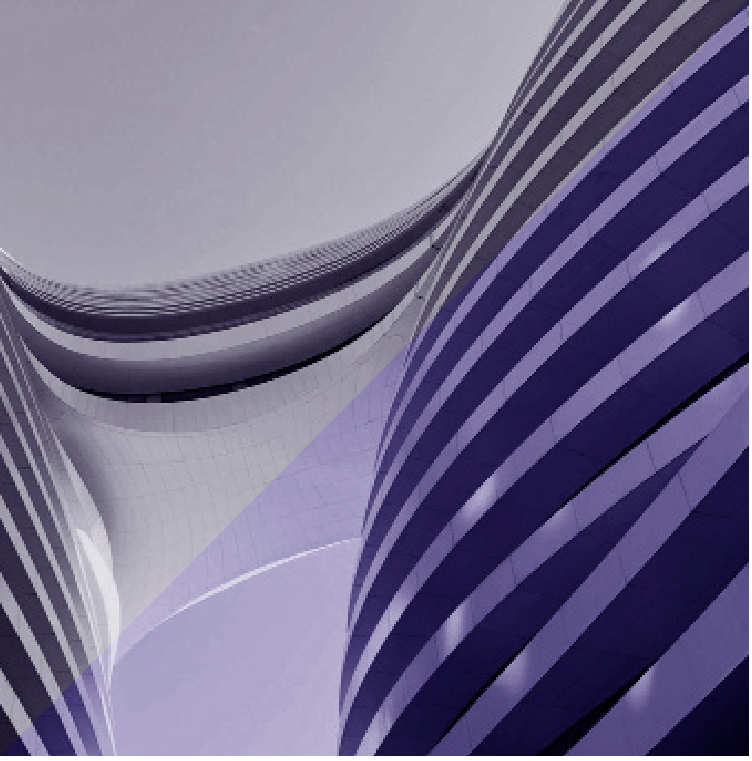
Attacks on Ground operations of the **payload**

Attacks on **cloud infrastructure**

Since a physical attack on an orbiting satellite can still be reasonably considered science fiction, it's important to recognize, that a cyber attack against a satellite will be rooted from the ground.

A ground attack can occur during the satellite's development phase e.g., by placing an invisible backdoor or malware on board before launch or through the ground infrastructure during operation e.g., by accessing cloud services, ground stations or mission control.

Only a comprehensive solution covering both the ground infrastructure and the satellite itself during the entire mission lifecycle will prove to be efficient.

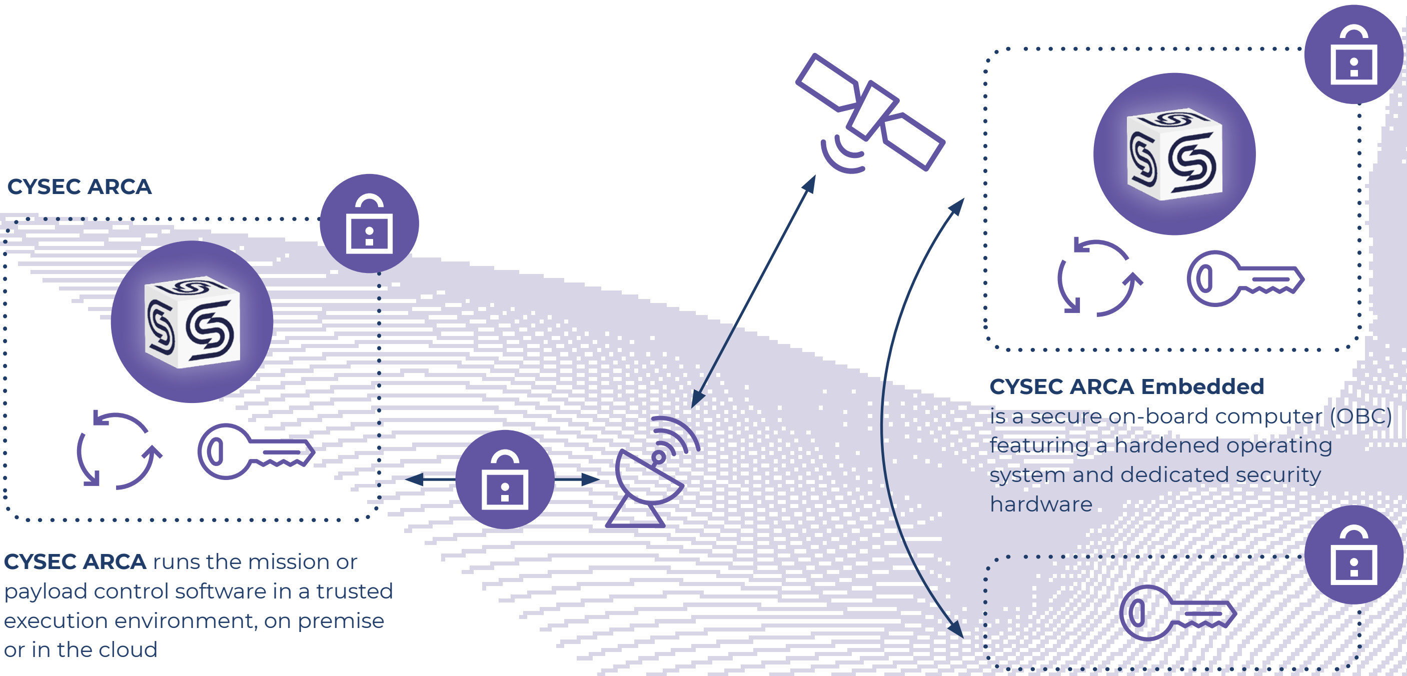


CYSEC
ARCA SPACE

CYSEC ARCA Space

A comprehensive solution to secure the entire satellite communications ecosystem thanks to dedicated products for ground-based and in-orbit assets and data. CYSEC ARCA Space products are based on the CYSEC proprietary technology CYSEC ARCA, a confidential computing environment ensuring the protection of data in its three states: at rest, in transit and in use.

CYSEC ARCA on ground is a hardware-based Trusted Execution Environment (TEE) to host mission-critical applications and data on premises or in the cloud. The flight version, CYSEC ARCA Embedded, comes in the form of an innovative On-Board Computer (OBC). Together they provide an end-to-end, accessible and reliable security solution for commercial space missions.



CYSEC ARCA runs the mission or payload control software in a trusted execution environment, on premise or in the cloud

CYSEC ARCA Embedded is a secure on-board computer (OBC) featuring a hardened operating system and dedicated security hardware

Cryptographic secrets are securely injected on ground before launch into **CYSEC ARCA Embedded** to create a root of trust on board the satellite

CYSEC ARCA Space Advantages

END-TO-END PROTECTION

360-degree protection of ground and space environments with the CYSEC ARCA Trusted Operating System combined with dedicated security hardware.

FLEXIBLE DEPLOYMENT

On ground mission-critical software can be deployed either on CYSEC ARCA on premise, or in the CYSEC private cloud in Switzerland or in Google Cloud. On board, CYSEC ARCA Embedded is available as a plug-and-play OBC.

EASY INTEGRATION

On ground CYSEC ARCA natively supports containerized mission control software using Docker or Kubernetes while CYSEC ARCA Embedded on board uses standard interfaces and communication protocols similar to other OBCs.

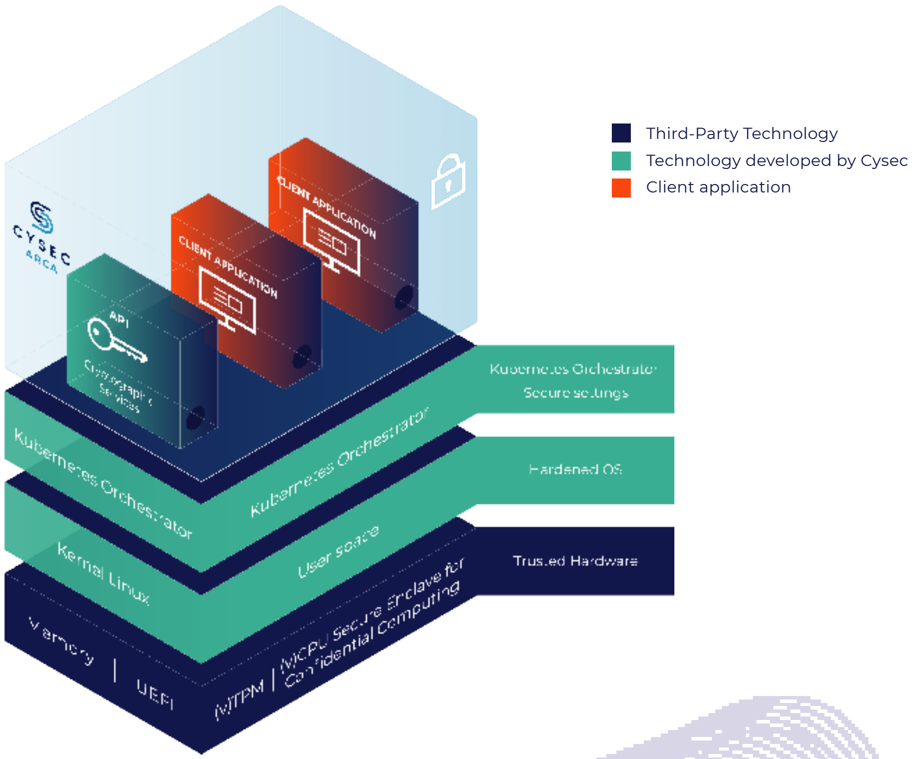
✉ info@cysec.com | www.cysec.com

CYSEC
ARCA SPACE

CYSEC ARCA

Securing mission-critical applications on ground

CYSEC ARCA, the on-ground element of CYSEC ARCA Space, is a confidential computing environment that secures all mission-critical applications like the Mission Control Software (MCS) and its associated secrets. Confidential computing protects data in use by hosting software applications in a hardware-based Trusted Execution Environment (TEE) in order to prevent unauthorized access or modification of applications and data while they are in use, in transit or at rest. Flexible deployment options, as a physical appliance on premise, or cloud.



CYSEC ARCA Advantages

STATE-OF-THE-ART DATA PROTECTION

Protection of mission-critical applications on ground ensuring data confidentiality and integrity.

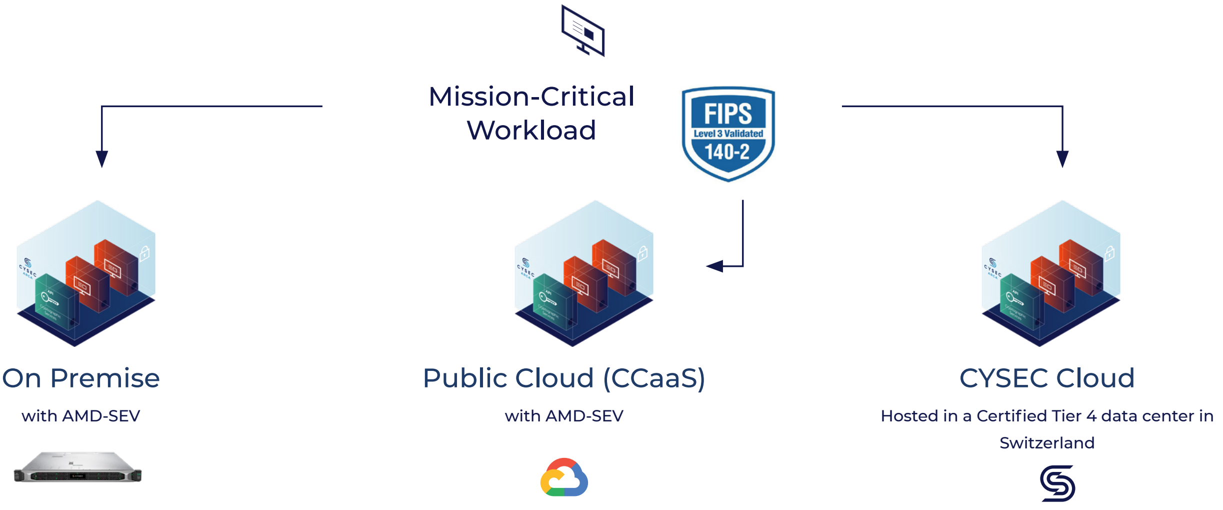
SIMPLE INTEGRATION

Simple API designed for software developers, no security or cryptography expertise required, and natively compatible with Docker and Kubernetes.

FLEXIBLE DEPLOYMENT OPTIONS

Choose between hosting your mission-critical applications and data on premise, in the CYSEC private cloud or in the Google cloud.

✉ info@cysec.com | www.cysec.com



Mission-Critical Workload

On Premise
with AMD-SEV

Public Cloud (CCaaS)
with AMD-SEV

CYSEC Cloud
Hosted in a Certified Tier 4 data center in Switzerland

Key Capabilities

CONFIDENTIAL COMPUTING

Secure code execution through AMD Secure Encrypted Virtualization (SEV) enclave and ARM TrustZone enclave. Only authorized code can access your data – meaning it's protected in use, at rest, in transit.

HARDENED OS

CYSEC ARCA features full-disk encryption, read-only system images, and secure boot. Only trusted kernels and system images can boot on the ARCA software, for increased protection against software and hardware attacks.

CERTIFIED KEY MANAGEMENT AND ENCRYPTION

CYSEC ARCA provides an accessible certified cryptographic service, which enables clients to easily manage keys and comply with regulations. It is also crypto agile, designed to integrate with most cryptographic back-ends.

SECURE HARDWARE BASE

CYSEC ARCA features UEFI firmware used for secure boot and a TPM for decryption of system and data partitions to protect against hardware attacks.

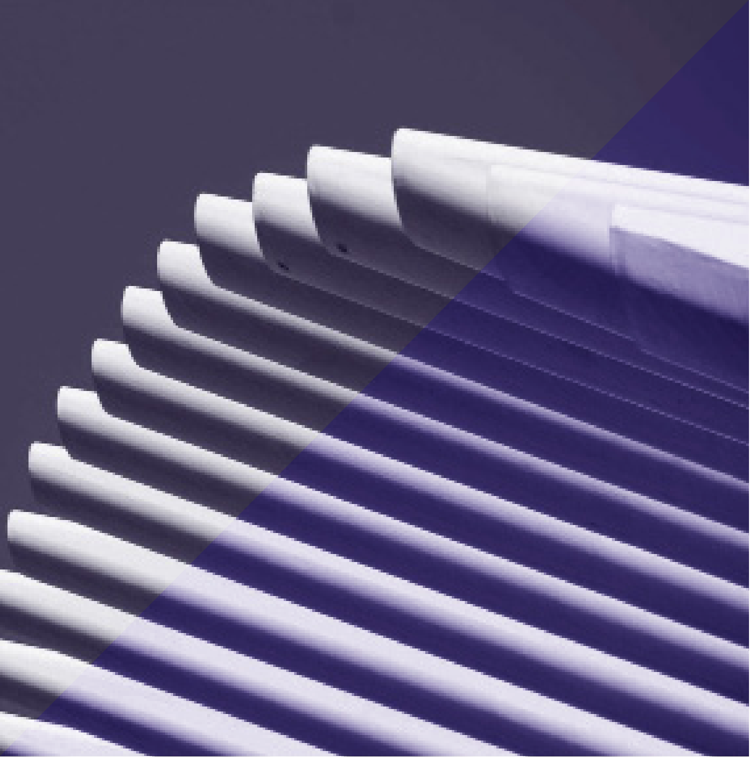
SECURE KUBERNETES

CYSEC ARCA features minimal images, a hardened kernel, container sandboxing, and protection of the host OS kernel and OS files to protect against software-based attacks.

GET IN TOUCH WITH US

To receive a free access to test the deployment of your mission-critical applications in CYSEC ARCA.

✉ info@cysec.com | www.cysec.com



CYSEC
ARCA SPACE

CYSEC ARCA

A secure On-Board Computer (OBC) protecting sensitive data and critical flight software

CYSEC ARCA Embedded is the flight component of ARCA Space, an end-to-end solution to protect satellite communications and data from cyber threats. Complementing ARCA on ground, ARCA Embedded is a secure on-board computer (OBC) featuring a lightweight distribution of CYSEC ARCA Trusted OS to provide a root of trust on board the spacecraft. CYSEC ARCA Embedded has been designed to securely store secrets in a dedicated security hardware and to host all sensitive operations on board like encryption, authentication or signature. CYSEC ARCA Embedded can be either used as the main OBC or as an add-on to the main OBC for cryptographic operations.

CYSEC ARCA Embedded

MISSION-CRITICAL APPLICATIONS

HARDENED OPERATING SYSTEM
with built-in cryptographic service and Key Management System (KMS)

HARDWARE ROOT-OF-TRUST for cryptographic secrets

CYSEC ARCA Embedded Advantages

ROOT OF TRUST ON BOARD
CYSEC ARCA Embedded protects secrets and sensitive software from physical „hand-on” attacks, as well as remote software attacks.

END-TO-END SECURITY
CYSEC ARCA Embedded is natively interoperable with CYSEC ARCA on ground, making CYSEC ARCA SPACE the most accessible and complete solution for commercial missions.

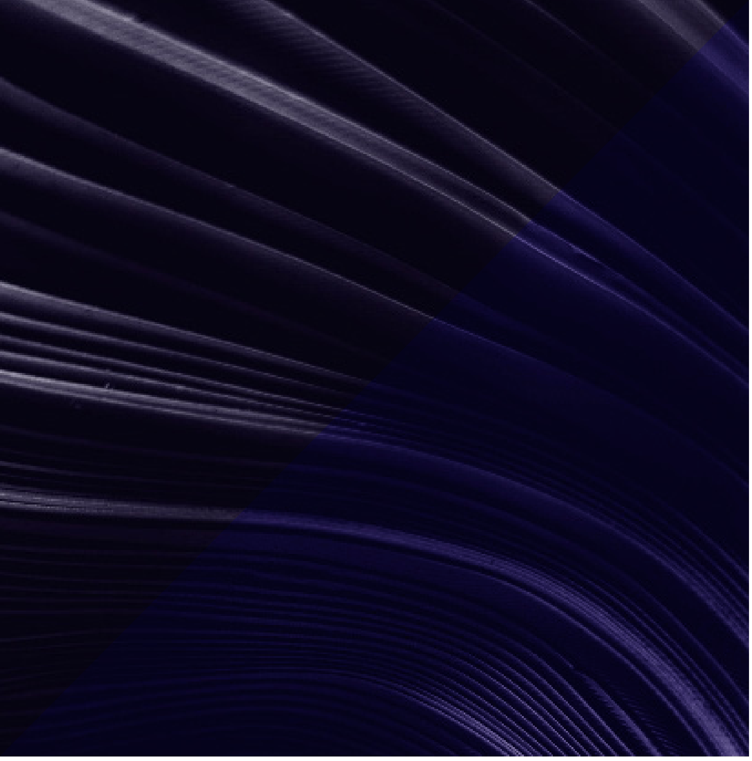
EASY INTEGRATION
Thanks to its standard interfaces, CYSEC ARCA Embedded is easy to integrate, seamless such as any other OBC on the market.

Key Capabilities

- DEDICATED SECURITY HARDWARE
  CYSEC ARCA Embedded integrates a Common Criteria EAL4+ certified root-of-trust to generate and store cryptographic secrets, offering a similar level of protection as in financial services industry.
- HARDENED OPERATING SYSTEM
  CYSEC ARCA Embedded features a miniature version of CYSEC ARCA Trusted OS, including a secure boot mechanism ensuring integrity of data and code loaded onto the OBC.
- BUILT-IN CRYPTOGRAPHIC SERVICE
  CYSEC ARCA Embedded features a cryptographic service accessible through a straightforward API specifically designed for software engineers with no security or cryptography expertise.
- BUILT-IN KEY MANAGEMENT SYSTEM (KMS)
  CYSEC ARCA Embedded includes a KMS facilitating key lifecycle management during the entire mission from development to launch to in-orbit operations.
- POWERFUL COMPUTING ON BOARD
  Built on top of the state-of-the-art Xilinx Zynq UltraScale+ MPSoCs, CYSEC ARCA Embedded provides powerful on-board computing units with dual/quad-core ARM Cortex-A53 and Cortex-R5 combined with LPDDR4 memory.
- STANDARD INTERFACES
  Mechanical and electrical interfaces are compatible with PC-104 CubeSat standard.

Technical Specifications of the Cryptographic API

Processing	Cortex-A53 Dual core @ 1.3 Ghz with ARM TrustZone Cortex-R5 Dual core @ 0.5GHz
FPGA	0.24 DSP blocks, 103k Logic cells
DRAM	2GB (EDAC)
Security hardware	CC EAL4+ cerified AIS-31 Class P2 compliant true random number generator (TRNG)
Cryptographic algorithms	AES-128 and AES-256 in CTR mode RSA key generation from 512 to 2048 with a 2-byte step RSA signature and encryption SHA-1 and SHA-256
General interfaces	4xI2C Master/slave, 4xSPI Master/slave, 4xRS422/RS485, 2x CAN, 1x USB 2.0, Ethernet 10/100/1000Mbps
High-speed interfaces	Up to 40x LVDS @ 1.2Gbps, 4x PCIe Gen2
Operating temp. Range	-30°C to +60°C
Operating Voltage	7 – 25 V
Power Consumption	0.5 – 8W
Dimensions	48x45x7mm
Mass	30g (120g with heat sink)



CYSEC
ARCA SPACE

CYSEC ARCA

Assessing and designing the security of space missions

The CYSEC LAB is a team of ethical hackers and security architects combining cybersecurity expertise with experience in assessing and designing space missions. The CYSEC LAB helps satellite operators and manufacturers at all stages of their mission, to respond to end-user security requirements and to mitigate specific cyber risks potentially detrimental to the sustainability of their business.

The security assessments provided by CYSEC LAB include threat modeling and risk analysis and aim to reveal the architecture's weak points. The security design service, provided by the LAB, starts with a risk trade-off and defines security mechanisms to mitigate the unacceptable risks.

CYSEC LAB Advantages

FLEXIBILITY

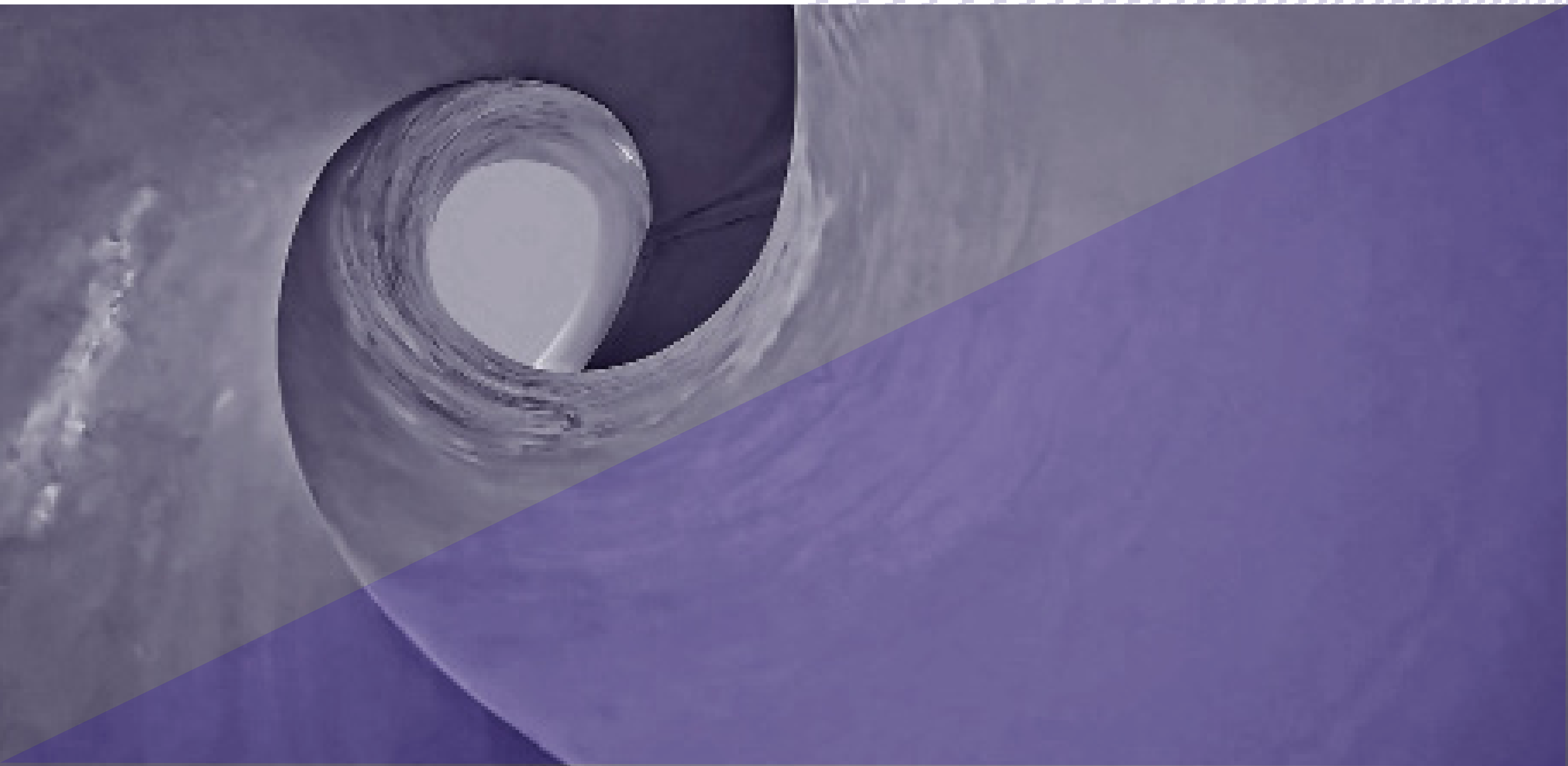
The CYSEC LAB can either be used for its offensive capabilities to identify vulnerabilities or for its defensive capabilities to design a security architecture down to the details of each individual protection mechanism.

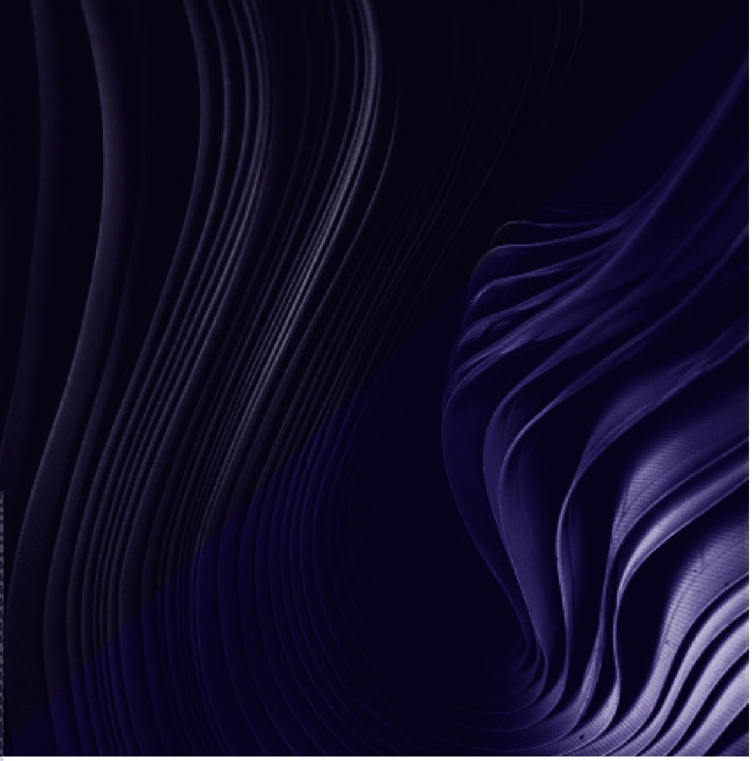
CONCRETE RESULTS

Each mandate has clear deliverables and actionable items for the client, facilitating the decision-making process towards implementation.

EFFICIENCY

The team is experienced in working on space missions thus maximizing efficiency.





CYSEC
ARCA SPACE

CYSEC ARCA

How we engage

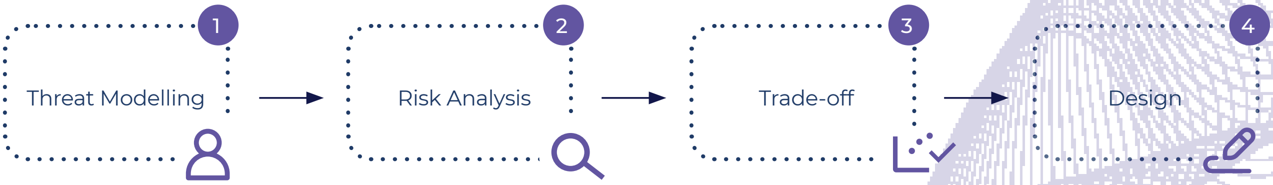
The CYSEC LAB implements a simple 4-step methodology

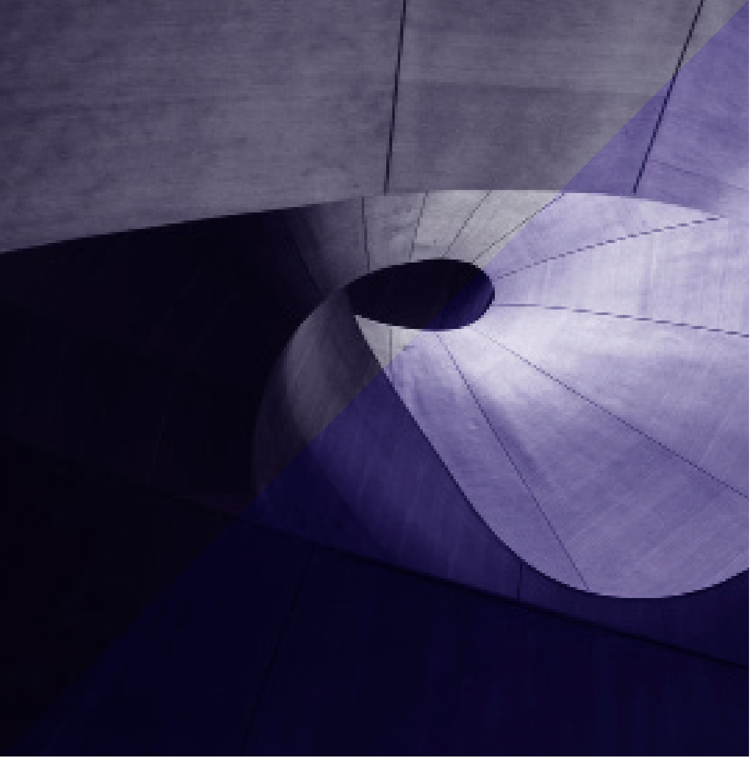
1 DEFINE RELEVANT THREATS AND ASSESS IMPACTS
During the threat modeling phase, the CYSEC LAB helps small at operators to define the profile of potential attackers, their level of knowledge, their resources and their motivations, as well as the impacts to the system should an attack occur. This phase is essential as it sets the foundation for the rest of the process and drives the ultimate outcome.

2 RISK ANALYSIS
Once attacker profiles have been defined, the CYSEC Lab helps operators to detail all potential risk scenarios. This phase usually takes the form of a brainstorming session with inputs from both the operator’s technical team and an external offensive team of qualified ethical hackers.

3 RISK TRADE-OFF
Once the list of scenarios has been created, the CYSEC Lab helps operators determine which risks can be considered acceptable and which ones must be mitigated.

4 ARCHITECTURE DESIGN
Obviously, each use case and mission scenario is unique, and each operator or client will have its risk appetite. This will result in a unique architecture design, which includes central security concepts. Depending on the need, the CYSEC Lab can also assist operators in the mitigation of risks related to outsourcing products and services critical for the mission.





CYSEC
ARCA SPACE

CUSTOMER TESTIMONIAL

CYSEC carried out a risk assessment of Astrocast's existing architecture, reviewed the threat model and defined the architecture for Astrocast's global, two-way, IoT satellite communication system. Security is ensured from the end customer, to the 80 satellites of the constellation and all-the-way to the IoT terminals on ground and oceans.

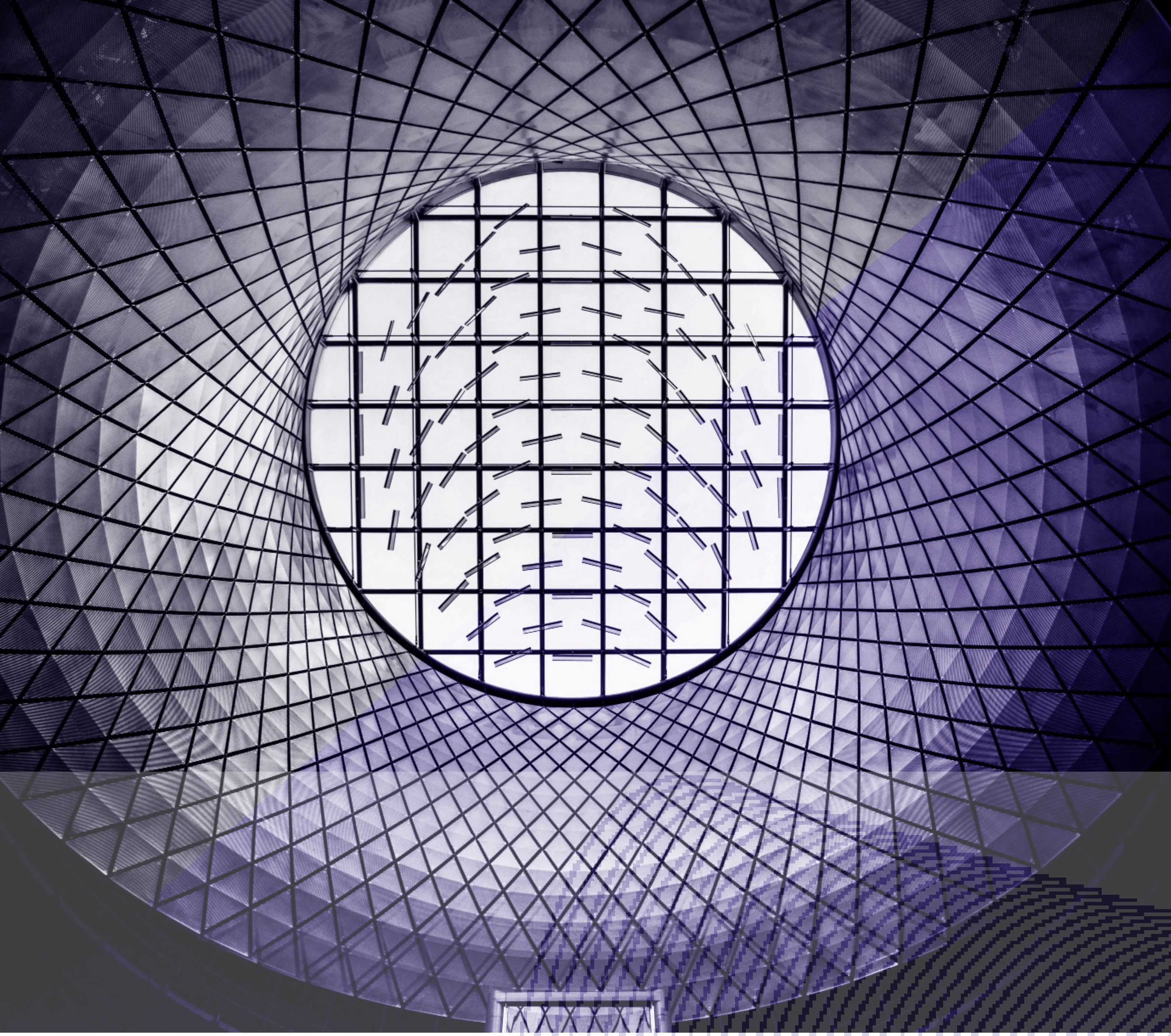
astrocast

> "We needed security engineers familiar with space architecture. We found in CYSEC exactly what we were looking for: a team with a unique set of skills, combining cryptography, embedded systems and security architecture applied to space systems."
>
> FEDERICO BELLONI, CTO OF ASTROCAST

CYSEC performed a security architecture review for the ClearSpace-One Mission, with the objective to ensure that the ground segment architecture design for the ClearSpace-One mission met their rigorous security standards.

clearspace today

> "We are very happy with the service provided by CYSEC LAB. We were impressed with their security expertise in space architectures and appreciated their clear advice and high availability."
>
> KEES VAN DER POLS, OPERATIONS AND GROUND SYSTEMS, CLEARSPACE



About us

CYSEC SA is a data security company based at the EPFL Innovation Park in Lausanne, Switzerland. CYSEC brings 360° security in one click for container-based workloads and platforms through its CYSEC ARCA trusted OS software. CYSEC partners with leading cybersecurity research centers to develop technological innovations in the area of Confidential Computing and delivers its cybersecurity solutions for any vertical sector.

Interested to learn more?

info@cysec.com | www.cysec.com