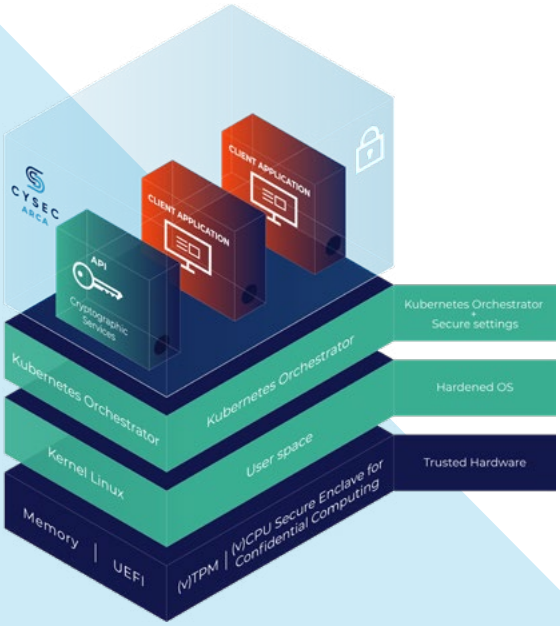
CYSEC
ARCA

CYSEC ARCA
Confidential Computing for Your Container Workloads

Deployment Datasheet

info@cysec.com | www.cysec.com



CYSEC ARCA

CYSEC ARCA Trusted OS

Your Cloud Workload Protection Platform

Protecting critical data in the cloud is a key challenge for data-driven businesses. CYSEC ARCA offers an answer – securing high-value data in all its states.

CYSEC ARCA is a hardware-based trusted execution environment designed for data-sensitive workloads that require high levels of protection and quality of service.

- COMPREHENSIVE - combine deployment types for edge-to-cloud protection in one solution
- CONTAINER SECURITY ENSURED THREEFOLD - host, image and runtime
- FULL-STACK SECURITY - from application to bare metal
- HARDWARE ROOT OF TRUST - guarantees a higher-level of resilience against attacks
- SECURELY COLLABORATE on your high-value data with confidential computing technology
- DATA-IN-USE remains confidential and intact – any memory dump is encrypted

Your Checklist

- WORKLOAD PERFORMANCE REQUIREMENTS - # of CPU cores, RAM, Disk, space, # of external IP addresses
- DEPLOYMENT TYPE - options vary across on-premise, private CYSEC cloud, Google cloud, embedded, or a combination of these
- OPTIONAL SERVICE - Cryptographic API with an integrated FIPS 140-2 L3-certified HSM

Deployment Architecture

Deployment is rapid, and options adaptable to the level of trust you require for different data. Deploy highly sensitive workloads in one environment, and workloads with lower data sensitivity in another – all within the same Kubernetes cluster.

Mission-Critical Workload

FIPS Level 3 Validated 140-2

On Premise
with AMD-SEV

Cloud (CCaaS)
with AMD-SEV

Embedded
with Arm v8/v9 TrustZone

info@cysec.com | www.cysec.com

CYSEC ARCA

Confidential Container as a Service (CCaaS)

CYSEC ARCA removes the barriers to digital transformation among enterprises that deal with high-value data, such as intellectual property, or client data.

Mission-Critical Workload

FIPS Level 3 Validated 140-2

Private Cloud

Swiss based CYSEC private cloud for sensitive workloads. Highly available, redundant, scalable, post-effective and DevOps friendly

Hybrid Cloud

Deploy highly sensitive workloads in one environment, and workloads with lower data sensitivity in another - all within the same Kubernetes cluster

Public Cloud

Secure highly sensitive workloads and access the benefits of Google cloud - AI, big data, ML and agility

Private Cloud Deployment

CONFIDENTIAL CONTAINER AS A SERVICE - a managed hosting of Kubernetes containers and workloads. Cloud-based multi-tenant deployments. Clients can deploy sensitive workloads and applications in CYSEC's private cloud, supported by Tier 3 and 4 data centers in Switzerland and delivered in a Kubernetes cluster.

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

Our approach meets the different trust-level requirements of the modern enterprise. We propose a hybrid cloud architecture that allows you to mix workloads with different trust-level requirements on the same infrastructure.

Default Settings:

- 16 CPU cores
- 256 GB disk space
- 32 GM RAM
- 1 external IP address

Includes

- HIGH AVAILABILITY AND REDUNDANCY guaranteed with two data centers. CCaaS is delivered in your private-access Kubernetes cluster.
- KEY MANAGEMENT AND ENCRYPTION, managing encryption keys across multiple locations.
  - Software backend included by default.
    - Option: certified HSM backend
    - Option: blockchain compatible
    - Option: quantum resistent
  - Administrator access to the Kubernetes clusters.
  - Effective onboarding, including setup and training.
  - Hardware root of trust (RoT) for your workloads.
  - 24/7 monitoring, maintenance, updates, technical support and recovery.
  - Non-disruptive rollout/rollback of updates enables frequent change without downtime.

info@cysec.com | www.cysec.com

CYSEC ARCA Public Cloud CCaaS on Google Cloud Platform

Multi-tenant deployments in a container execution environment

FEATURES:

- Dedicated Kubernetes cluster enabling high availability and redundancy
- Key management and encryption, software backend included by default.
  - Option: blockchain compatible
  - Option: quantum resistent
- Administrator access to the Kubernetes clusters
- Technical support - L1/L2/L3 DevOps

info@cysec.com | www.cysec.com

CYSEC ARCA

Public Cloud Deployment

Move safely to the cloud without extending trust to public cloud providers. Deploy CYSEC ARCA Trusted OS on top of Google Cloud Platform (GCP) IaaS - Confidential VM. This will enable you to protect your sensitive Kubernetes workloads on top of GCP.

Your security benefits

A SECURE BOOT CHAIN

- UEFI firmware verification mechanism ensures code launched by the computer's firmware can be trusted
- Established root of trust with vTPM
- Secure boot to detect tampering with bootloaders and OS files
- Integrity monitoring to monitor and verify the runtime boot integrity

PROTECTION OF DATA IN USE

- Use AMD Secure Encrypted Virtualization (SEV) secure enclave accessible from GCP for confidential computing
- Any memory dump activity is encrypted and not readable

A HARDENED OS

- Increased protection of data and code from all types of attacks, whether hardware or software-based
- Safe programming languages for system components and libraries
- Reduced attack surface with a hardened kernel and a filesystem that enforces a strict read-only policy

Google Cloud

CYSEC
ARCA

Google Cloud Default Settings: N2D Machine

- N2D machine types run on the second-generation AMD EPYC Rome Processor.
- They are the largest general-purpose machine type with up to 224 vCPUs and 896 GB of memory.
- N2D VMs support vCPU to memory ratios of 1:1, 1:4, and 1:8 with the option to customize your machine to your workload needs.
- N2D machine types run on AMD EPYC Rome processors with a base frequency of 2.25 GHz, an effective frequency of 2.7 GHz, and a max boost frequency of 3.3 GHz.

N2D machine types

- Support up to 224 vCPUs and 896 GB of memory.
- Are available in predefined and custom machine types.
- Offer higher memory-to-core ratios for VMs created with the extended memory feature. Using the extended memory feature helps you avoid per-CPU software licensing costs while providing access to more than 8 GB of memory per vCPU.
- Are powered by the second-generation AMD EPYC Rome processor.
- Support committed use and sustained use discounts.

Your Benefits

TRUST
Access the benefit provided by cloud (AI, big data, ML, collaboration) without extending trust to public cloud providers

CONTROL OVER VISIBILITY AND ACCESS
Ensure data and code visibility and access is limited to the people you want

WEAKEST LINK PROTECTED
Access to data in use is blocked from unauthorized third party

ACCELERATE
Secure innovation and business value creation

info@cysec.com | www.cysec.com

CYSEC ARCA

On-Premise Deployment

Companies who want to maintain complete responsibility for hardware and software can access CYSEC ARCA installed on a lightweight appliance, which is deployed on premise in an average of just three weeks. The appliance gives you direct access to the cryptographic backend as well as oversight of key lifecycle management.

Physical Appliance

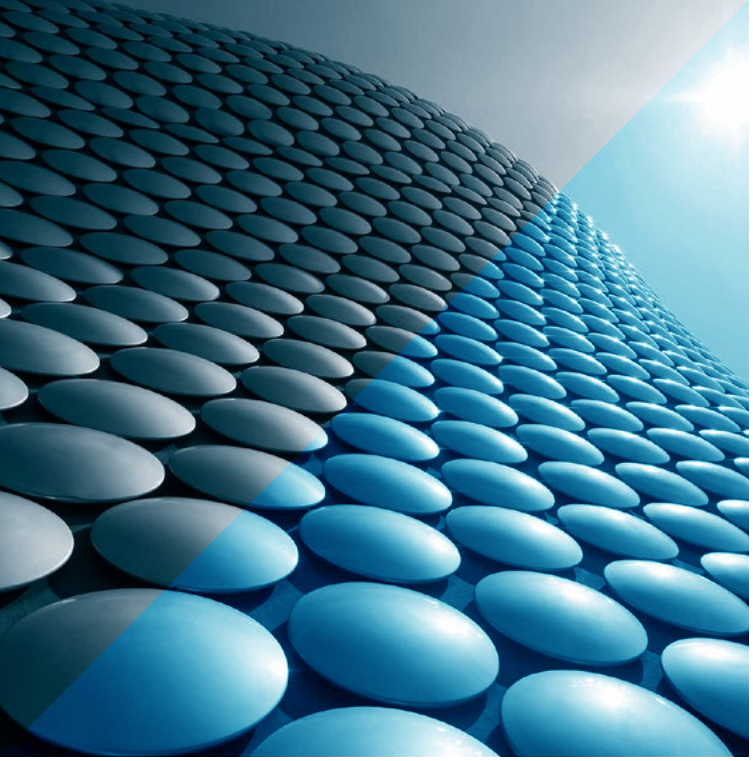
CYSEC ARCA appliance includes the following features:

- TPM 2.0
- UEFI with secure boot
- Certified HSM (optional)

Supported Platforms and Environments

CPU	AMD® EPYC® 7002 Series Gen 2 up to 64 core
Memory	32 GB to 2TB DDR4 RDIMM
Disk	SSD 256 GB to 4 TB
Power	2N redundant hot-swap PSU
Network	4x +Gbps, 1x Gbps IPMI (can be upgraded)

✉ info@cysec.com | www.cysec.com



CYSEC ARCA

CYSEC ARCA License

Confidential Computing environment fully protected to the bare metal, enables you to securely run and protect containerized Kubernetes workloads in all deployment types, and provides full protection of your data across its entire lifecycle.

Includes

- Key management and encryption, software backend included by default.
  - Option: certified HSM backend within appliance
  - Option: blockchain compatible
  - Option: quantum resistent
- Effective onboarding, including setup and training
- Hardware root of trust (RoT) for your workloads
- Quarterly updates and support - L1/L2/L3 DevOps
- Non-disruptive rollout/rollback of updates enables frequent change without downtime

Supported Platforms and Environments

Hardware	Intel x86, AMD SEV
OS	CYSEC ARCA (Linux-based)
Containers	Docker, Kubernetes (OCI compliant)

Certifications

- HSM FIPS 140-2 L3 compliant
- Container

FIPS 140-2

OPEN CONTAINER INITIATIVE

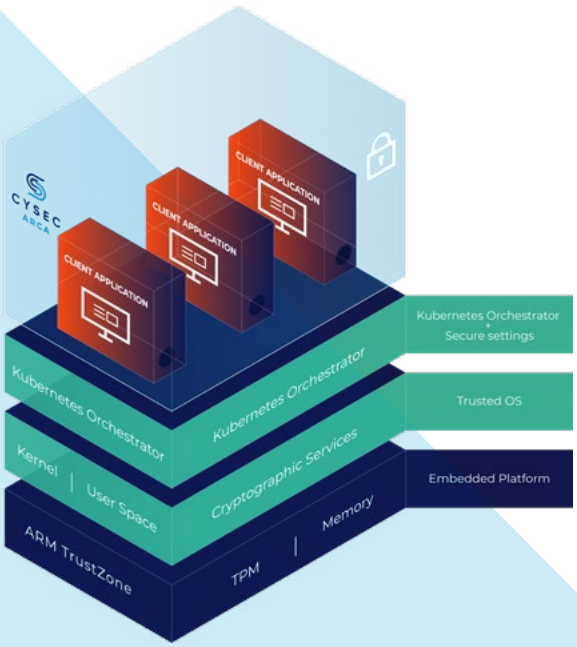
Technical specifications of the Cryptographic API

Software backend	OpenSSL, OpenSSL post quantum
Integrated HSM	OEM with code share, EU-based, PCI 2.0, FIPS 140-2 Level 3
Access	gRPC
Supported Programming languages	Rust, GO, Python, Scala, C#, C++, Node .js, Java and other
Supported Interfaces	PKCS#11, JCE
Cryptographic functionalities	• Asymmetric: RSA (2048-4096) and Elliptic Curves (ECDSA and ECIES) • Symmetric: AES (128-256) • Hash: SHA-2 (256-512) and BLAKE-2 (256-512) • Wallet Key Derivation: BIP-32 and SLIP-10 • Easy implementation of other crypto primitives

info@cysec.com | www.cysec.com

CYSEC ARCA

Embedded Deployment



CYSEC ARCA Embedded is a custom distribution of the CYSEC ARCA Trusted OS, designed to run on a variety of embedded hardware platforms. ARCA Embedded offers the same security performance of ARCA Trusted OS while being compatible with embedded designs.

CYSEC ARCA Embedded provides a hardware root of trust at the edge for many applications such as IoT, Space payloads and Maritime.

HARDWARE OR SOFTWARE- based storage of secrets and provisioning of certificates

EXTENSIVE CRYPTOGRAPHIC LIBRARY featuring industry-standard cryptographic operations

POST-QUANTUM resilient cryptographic services

TRUSTED key lifecycle management

Your applications are executed in an isolated containerized TRUSTED ENVIRONMENT

SECURE ACCESS CONTROL

Your Benefits

CONFIDENTIAL COMPUTING
Get security at the edge with a hardware root of trust

SECURITY FROM THE CLOUD TO THE EDGE
Get end-to-end security

FLEXIBLE DEPLOYMENTS
Compatible with most edge applications

FIPS VALIDATED 140-2 LEVEL 2

CERTIFIED EAL4+

Deployment Options

- Integration on a variety of embedded hardware platforms implementing Arm TrustZone architecture
- Custom embedded implementations designed and developed by CYSEC for specific needs
- Hardware platforms – available in commercial and space-grade versions

info@cysec.com | www.cysec.com

CYSEC

TOP 100 WINNER 2020

CONFIDENTIAL COMPUTING CONSORTIUM

OPEN CONTAINER INITIATIVE

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