SOLUTION BRIEF

CYSEC ARCA TRUSTED OS

Remove data security barriers.
Accelerate innovation.

DATA YOU CAN TRUST

SECURE YOUR CRITICAL DATA IN USE

Protect your weakest link

Data-in-use is probably your number one security gap. Whatever your environment – public cloud, data centers, or edge – you need to address this point of least resistance.

Secure collaboration in the cloud with high-value data or IP is key to innovating new business models and working with a high level of trust in a zero-trust environment. Like cloud, edge computing is developing rapidly, driven by next-generation connected devices and faster communication links. As value is shifting towards the edge, security gaps emerge in the cloud-edge integration.

Edge servers, lacking in the necessary built-in security to counter threats, open wide the door to data theft or attack. Malicious attackers can take control of edge devices, view, manipulate or steal data as well as move laterally within the network.

For instance, it is important to provide adequate protection of medical data such as personal data and health records at the edge of connected biomedical devices, as well as other types of digital assets, such as organization data, collected credentials and warehouse monitoring data.

By 2025, 75% of enterprisegenerated data will be created and processed at the edge.

- Gartner

INTRODUCING CYSEC ARCA TRUSTED OS

Solution

A trusted execution environment (TEE) for hosting containerized platforms, applications, and workloads that delivers optimal protection for highly sensitive data in all its states and can be used on-premises, in the cloud or within embedded hardware platforms.

CYSEC ARCA protects the entire stack, guarding against attacks from all angles, whether they are software-down or hardware-up, and includes a built-in certified hardware crypto engine for key management and encryption. Clients can securely run containerized Kubernetes workloads, use cryptographic functionalities in their workloads, and have greater assurance that their data maintains its integrity and confidentiality, achieving compliance throughout its entire lifecycle.

Unlike data security solutions from industry and innovation players, CYSEC does not require expensive, vendor-specific hardware, nor relies on one type of cryptographic solution. Further, CYSEC ARCA equals or surpasses the robust security provided by market players at a fraction of the price.

The CYSEC ARCA Trusted OS - confidential computing environment is also unique because it combines full-stack security of containerized workloads - with certified hardware crypto engine, with a range of other benefits. These include value and immediate return on investment, and a user-friendly experience that includes rapid integration, simple installation and use.

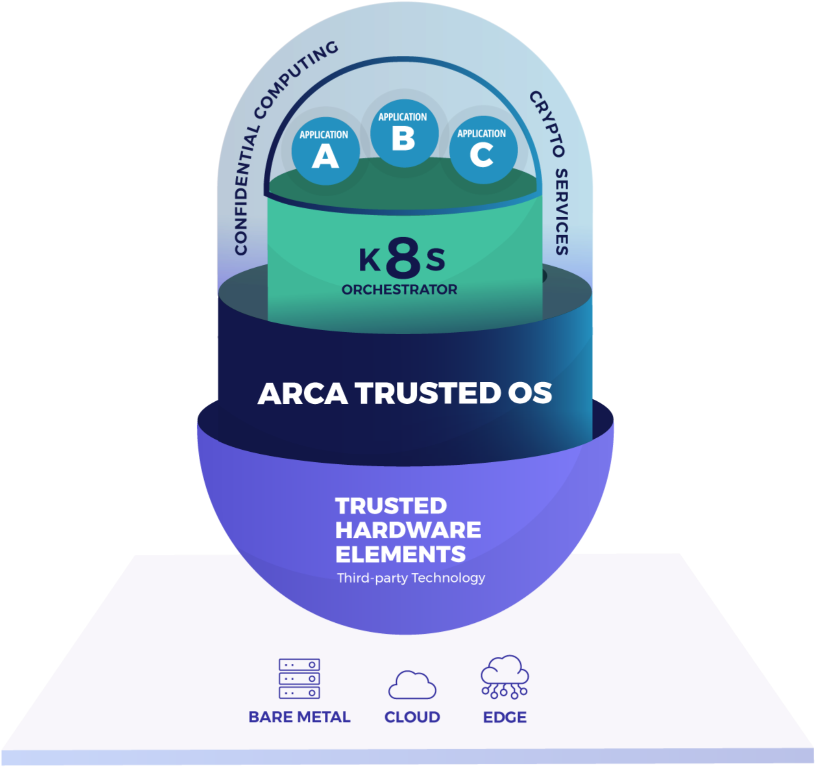

Figure 1 : CYSEC ARCA Trusted OS

INTRODUCING CYSEC ARCA TRUSTED OS

Features

Protects data in use by rendering confidential computing technology accessible and seamless for containerized applications, without any changes in the applications

Establishes a hardware root of trust with a trusted boot chain that uses UEFI firmware boot services and a TPM for decryption of system and data partitions. It guarantees a higher-level of resilience against attacks. ARCA's root of trust is placed within a physical device - a Trusted Platform Module (TPM) - a crypto-processor used for device identification, authentication and encryption, as well as verification ofoperating system integrity.

Reduced attack surface, compared to a generalpurpose OS, with a hardened OS, Linux based, built from source using safe programming languages for system components and libraries, that installs only the necessary software, with a filesystem that enforces strict read-only policy, a hardened Kernel with secure configuration options such as lockdown integrity and safe defaults, and minimal OS images.

Certified crypto engine – Key Management System (KMS) & encryption. The certified cryptographic backend can either be a hardware security module (HSM) certified FIPS 140-2 Level 3, ensuring tamper resistance, a secure element certified CC EAL4+ and FIPS 104-2 Level 2, or a software implementation.

Cryptographic API that can easily integrate within critical workloads, applications and CI/CD chains, to perform cryptographic operations such as generating, storing and using cryptographic keys. Encryption and access control included, to prevent API calls connection tapping and unauthorized access. Access the cryptographic API either via a KMS gRPC interface or via legacy or native cryptographic interfaces, incl. JCE.

High availability and redundancy – distributed and scalable environment adapted for modern DevOps practices, with the capacity to run applications on many compute nodes (e.g., a cluster) as if all those nodes were a single, enormous machine.

Security ensured threefold – by securing the host, the image and the runtime.

Deploy only signed images – CYSEC ARCA allows to verify container image signatures, to ensure that only signed images are admitted for deployment.

Full stack security – from application to bare metal.

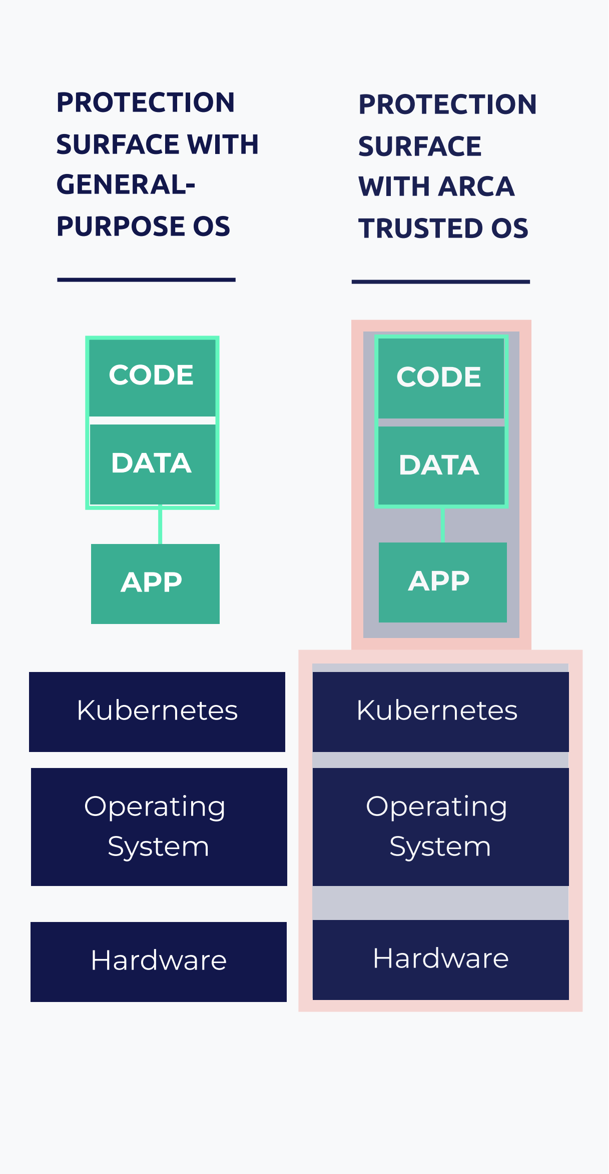

Figure 2 : Protection surface comparison between a general-purpose OS and CYSEC ARCA Trusted OS

DEPLOYMENTS

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

CYSEC ARCA LICENSE

A trusted execution environment (TEE), 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.
CYSEC ARCA is inexpensive, rapid to deploy and easy to integrate and maintain.

INCLUDES

Key management and encryption, through an easy-to-use cryptographic API, managing encryption keys across multiple locations

Software backend (OpenSSL) included by default

Certified HSM backend within appliance *(Option)*

Blockchain compatible algorithms *(Option)*

Quantum resistant algorithms *(Option)*

Effective onboarding, including setup and training

Hardware root of trust for your workloads

Maintenance, updates, technical support and recovery - L1/L2/L3 DevOps

Non-disruptive rollout/rollback of updates enables frequent change without downtime

CERTIFICATIONS

HSM FIPS 140-2 L3 compliant

Open Container Initiative (OCI)

Figure 1 : CYSEC ARCA Trusted OS

• CLOUD DEPLOYMENTS

Confidential Container as a Service (CCaaS)

• PRIVATE CLOUD

A cloud-based and multi-tenant managed hosting of Kubernetes containers and workloads. 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.

High availability and redundancy guaranteed with two data centers. CCaaS is delivered in your private-access Kubernetes cluster.

YOUR CHECKLIST

1 **Workload Performance Requirements** *(#CPUs, RAM, disk space, #external IPs)*

2 **Deployment Type**

3 **Optional KMS and Encryption add-ons**
(certified HSM backend, quantum resistant algorithms, blockchain compatible algorithms)

• PUBLIC CLOUD

CYSEC ARCA Trusted OS can be deployed on top of Google Cloud Platform (GCP) IaaS - Confidential VM, in order to protect sensitive Kubernetes workloads on top of GCP. Google Cloud Default Settings: N2D Machine Types.

Move safely to the cloud without extending trust to public cloud providers.

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.

Protection of sensitive data in use

- Uses AMD SEV 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.

• HYBRID CLOUD

CYSEC ARCA Trusted OS can be deployed on top of Google Cloud Platform (GCP) IaaS - Confidential VM, in order to protect sensitive Kubernetes workloads on top of GCP. Google Cloud Default Settings: N2D Machine Types.

ON-PREMISE DEPLOYMENTS

Companies who want to maintain complete responsibility for hardware and software can access CYSEC ARCA installed on a lightweight appliance, deployed on premise in an average of just three weeks.

The appliance, with CYSEC ARCA Trusted OS included as baseline, gives you direct access to the cryptographic backend as well as oversight of key lifecycle management.

CYSEC ARCA appliance secures containerized workloads from the application to the bare metal and includes the following features:

- TPM 2.0
- UEFI with secure boot
- Certified HSM (optional)
- CYSEC ARCA Trusted OS

BENEFITS

- **High availability**
- **Full stack security**
- **Monitoring,updates**
- **Lower overheads**
- **Compliance**

EMBEDDED DEPLOYMENTS

CYSEC ARCA embedded is a custom distribution of the CYSEC ARCA Trusted OS, designed to run on a variety of embedded hardware platforms. It offers the same security performance of ARCA Trusted OS while being compatible with embedded
designs and provides a hardware root of trust at the edge for many applications such as IoT, Space payloads and Maritime.

CYSEC ARCA embedded provides a secure computing environment at the edge, ensuring confidentiality, authenticity and integrity of critical data generated by connected devices and processed at the edge.

Edge security provided by ARCA embedded involves aspects such as securing access to edge computing resources, securing applications and associated IP data running on top of those resources, and securing user data in its entire lifecycle (data at rest, in transit and most important, data in use).

ARCA embedded also provides an early threat detection mechanism, meaning that if a connected device has been tampered with, it will be detected, reported and blocked before it can propagate damage to the back end.

Deployment Options of ARCA Embedded

- 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 spacegrade versions

COMPREHENSIVE

Combine deployment types for edge-to-coud protection in one solution.

BENEFITS OF ARCA TRUSTED OS

Rapid deployment
3 weeks for on-premise, 3 days for cloud – accelerating your goto-market.

Ensured data confidentiality and integrity
Ensuring the security of sensitive data in transit, in use, and at rest for critical applications and data.

Secured deployment ande xecution of Kubernetes workloads
Hostile workloads are not able exploit the host OS, nor the kernel, and cannot access the CPU without explicit permission.

Augmented innovation
Open up the possibility of using public cloud services to collaborate securely with your high value data.

Simplified compliance
Achieve compliance with key management and encryption through an easy-to-use cryptographic API. Using a certified
solution to encrypt or digitally sign sensitive data across the entire data encryption lifecycle: at rest, in transit and in use.

Immediate return on investment
Inexpensive, rapid to deploy, and easy to integrate and maintain.

Weakest link protected
Access to data-in-use is blocked from unauthorized third-party.

Minimal OS i mages r educes the attack surface
OS includes just the software that is needed.

Use KMS to shift workloads between onpremise and cloud resources while controlling your keys, sparing complexities and costs of managing multiple encryption keys.

ABOUT CYSEC

CYSEC

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 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. For more information, please visit www.cysec.com.

CYSEC SA
EPFL Innovation Park, Building D
CH- 1015 Lausanne, Switzerland

info@cysec.com

www.cysec.com

www.linkedin.com/company/cysecsystems