PRODUCT

CYSEC

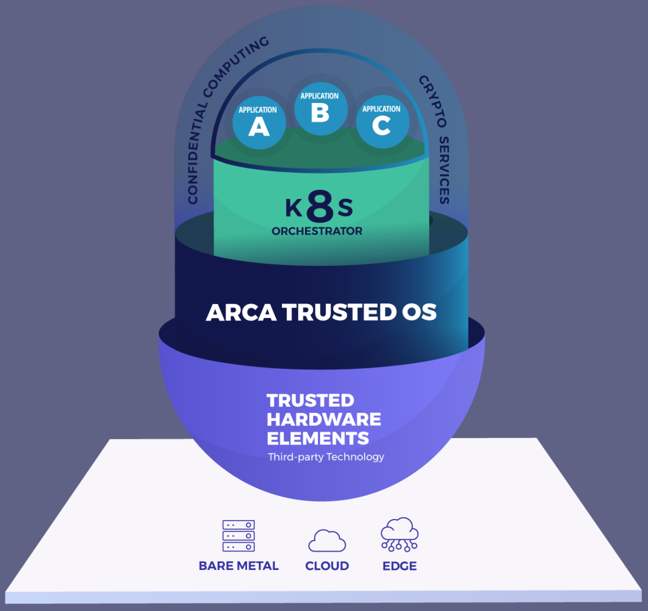
ARCA TRUSTED OS (for x86 architecture)

A secure minimalist Linux OS to host containers

ARCA Trusted OS is a hardened Linux-based microdistribution designed to host containers orchestrated by Kubernetes.
It includes only what is required to run containers and is designed to contain system intrusion and avoid data compromission.

BENEFITS

A strong foundation for your container security strategy on-premise, in the cloud, at the edge



- **Minimize** the overall attack surface
- **Secure** your containers on infrastructure you do not own or control
- **Protect** your data at rest, in transit and in use
- **Reduce** your management and maintenance costs
- **Scale** your business with a secure enterprise ready OS.

"Use a container-specific OS instead of a general-purpose one to reduce attack surfaces"
NIST SP 800-190

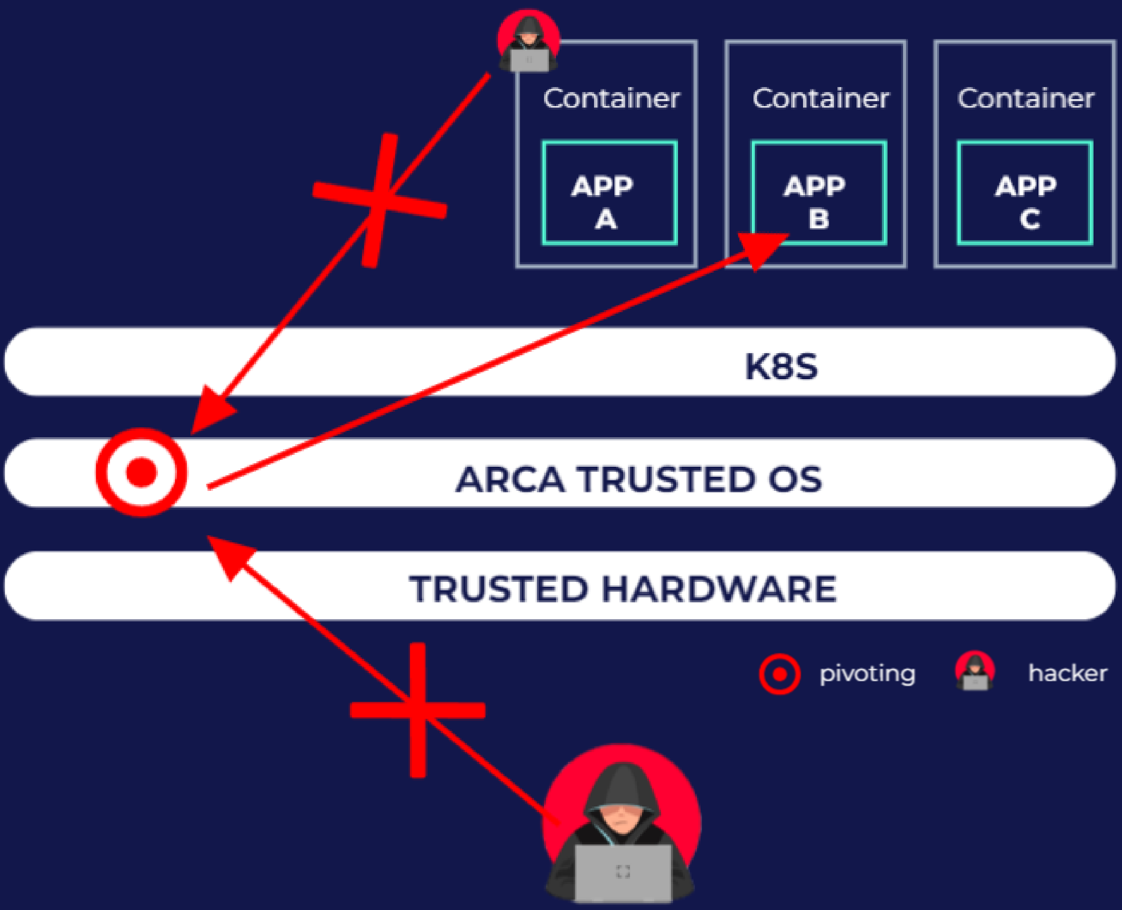
PROTECT YOUR CONTAINERS AGAINST SYSTEM INTRUSION AND DATA COMPROMISSION

ARCA Trusted OS has two main security objectives:

- containing the intrusion of an attacker within the container software infrastructure (OS + k8s platform)
- protecting the integrity and confidentiality of the data handled by this infrastructure

CYSEC's threat model considers attackers having either a physical access to your infrastructure or a remote access to at least one of your containers. In both cases, ARCA Trusted OS blocks attacks targeting the OS to later pivot towards containers orchestrated by the Kubernetes orchestrator.

ARCA TRUSTED OS - THREAT MODEL



Protection of data and business logics against compromised workloads (Top-down) and hardware-up (Bottom-up) attacks

KEY FEATURES

The main security challenge is to ensure data protection when your containers are executed on an infrastructure you don't own and control (Cloud & Edge).
ARCA Trusted OS includes all security mechanisms to isolate your containers from such infrastructure.

SECURITY FEATURES*

UEFI & TPM2.0	to provide a hardware roots of trust
SECURE BOOT	to verify the execution environment authenticity and integrity
IMMUTABLE FILE SYSTEM	to prevent unauthorized file system modifications
FULL DISK ENCRYPTION	with key protection, to protect data at rest
SECURITY MAINTENANCE	to maintain your OS with up-to-date security patches
CONTAINER RUNTIME PROTECTION	to strengthen the isolation between your containers and their host OS
CONFIDENTIAL COMPUTING	with AMD-SEV, to protect data in use
REMOTE ATTESTATION	to verify the launch of a VM in a Confidential Computing context

MANAGEMENT FEATURES

CENTRALLY MANAGED	to simplify management for distributed architecture
SIMPLE AND SECURE UPDATE PROCESS	to keep your OS up to date with authorized updates
STANDARD MONITORING INTERFACE	to integrate with your monitoring tools
AUTOMATED CONFIGURATION AND DEPLOYMENT	to fastly and simply follow your container infrastructure needs

**For more details, request our solution sheet "ARCA Trusted OS for X86 architecture"*

USE CASES

Arca Trusted OS for your mission-critical activities

Sensitive data migration on the cloud

Work securely in a hybrid architecture

Blockchain node and digital assets

Protect data processed at the Edge

Multi-party Data collaboration

Typical Industries users:

Defence & Space

Government

Financial services

Critical infrastructures (Oil & gas, Telecom, Energy, Healthcare)

SETTINGS

Hardware prerequisites

CPU	x86-64 - Intel	x86-64 - AMD	ARM (1)
FIRMWARE	OVMF/UEFI		ROM
SECURE ELEMENTS	vTPM/TPM 2.0		TPM 2.0
(Optional) CONFIDENTIAL COMPUTING	N/A TDX under investigation	AMD-SEV	ARM TrustZone

Software compatibility

APPLICATION	OCI CONTAINER			
ORCHESTRATOR OR RUNTIME MANAGER	KUBERNETES	PODMAN	DOCKER	KUBEEDGE (2)
CONTAINER RUNTIME	runc	gVisor	Kata Container	-

Deployment/Compatibility

CLOUD		Azure (3)	aws (4)
DATA CENTER /EDGE	Bare Metal	VMWare	Virtual Box

(1) Detailed information provided on dedicated Arca Trusted OS ARM datasheet
(2) under investigation for ARCA Trusted OS running on ARM
(3) planned for 2023
(4) planned for 2024

CYSEC

www.cysec.com | info@cysec.com

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