— PRODUCT

CYSEC

ARCA Trusted OS (for ARM architecture)

A secure minimalist Linux OS to host containers at the far edge

ARCA Trusted OS for ARM is a hardened Linux-based microdistribution designed to run containers on small footprint boards deployed at the edge. It includes only what is required to run containers and is designed to reduce the attack surface and avoid data compromission.

The ARM version of ARCA Trusted OS has been designed with the same security philosophy than the x86 version. This family of hardened OSs ensures a continuity of IT software infrastructure from datacenter/cloud up to the edge. ARCA Trusted OS comes with cryptographic functions executed in Trusted Execution Environment (TrustZone or TPM2.0).

BENEFITS

A strong foundation to protect your containerized AI/ML applications 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 your keys in use (i.e.TrustZone or TPM2.0)
- **Simplify** the maintenance of your edge device fleets with OTA updates
- **Deploy** your containerized applications on small footprint devices
- **Extend** your business to the edge with a secure enterprise ready OS
- **Keep** your software infrastructure up-to-date thanks to Cysec OS security maintenance

Arca Trusted OS for ARM is also designed for selected Single Board Computers (SBC)

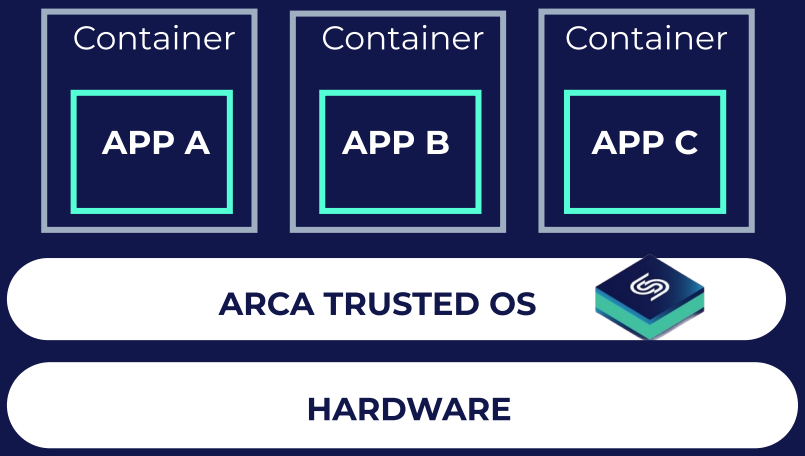
Board name		
	Raspberry Pi	Raspberry PI 4B
	ST Microelectronics	STM32MP157F-DK2 (1)

(1) planned for Q4 2023

For other ARCA Trusted OS SBC compatibility, please contact CYSEC

PROTECT YOUR CONTAINERS AGAINST SYSTEM INTRUSION AND DATA COMPROMISSION

CYSEC threat model considers attackers having both 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 hosted by this OS.



ARCA Trusted OS has two main security objectives:

- Reducing the attack surface of your container software infrastructure (OS + runtime manager)
- Protecting the confidentiality of your data stored in this infrastructure.

Threat types	Threat name	Description
Top-down	Container escape to host	Attack attempts to compromise the host OS from a compromised container.
	Exploitation for privilege escalation	Attack attempts to gain higher-level permissions on the host OS or the network
Bottom-up	Hardware theft	Attack attempts to compromise data and business logics stored on a hardware that has been stolen
	Modify OS image	Attack attempts to gain knowledge or control on the data or business logics by modifying the OS image

KEY FEATURES

The main security challenge is to ensure data and business logics protection when your containers are executed on an infrastructure you don't own and control at the edge.
ARCA Trusted OS for ARM includes all security mechanisms to provide that protection level in such infrastructure while having the ability to connect to k8s clusters in core networks.

SECURITY FEATURES

ROM CODE & TPM2.0	to provide 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
SECURE MANAGEMENT	of device fleets to securely configure and maintain edge devices from the core

MANAGEMENT & OPERATIONS FEATURES

RUN CONTAINERS ON SMALL FOOTPRINTS	to extend your containerized applications further down to the edge
CENTRALLY MANAGED	to simplify management on distributed architecture
AUTOMATED CONFIGURATION AND DEPLOYMENT	to fastly and simply follow your container infrastructure needs
SIMPLE AND SECURE UPDATE PROCESS	to keep your OS up to date with authorized updates
ABILITY TO INTEGRATE EDGE NODES IN A K8S CLUSTER (2)	to accelerate the optimization of your business at the edge

(2) Under investigation

USE CASES

ArcaTrusted OS for your mission-critical activities

- Protect data and business logics on edge nodes
- Work securely in hybrid architecture extended to the edge
- Protect and centrally manage fleet of devices

Typical Industries users:

- Defence & Space
- Government
- Retail
- Critical infrastructures (Oil & gas, Telecom, Energy, Healthcare)

SETTINGS

Hardware Compatibility

CPU	ARM	x86-64 (3)
Firmware	ROM CODE	OVMF/UEFI
Secure elements	OTP or TPM 2.0	vTPM/TPM 2.0
(Optional) Confidential	ARM TrustZone	AMD-SEV, (Intel TDX) (4)

(3) Detailed information provided on dedicated Arca Trusted OS x86 datasheet
(4) Under investigation

Software Compatibility

Application	OCI Container	
Runtime manager	Docker	Kubeedge (5)

(5) under investigation

CYSEC

www.cysec.com/arca

EPFL Innovation Park - Building D - CH 1015 Lausanne - Switzerland
257 Boulevard Saint-Germain, 75007 Paris - France