WHITE PAPER

CYSEC ARCA OS GCP – AMD-SEV

DATE: **October / 2021**

CYSEC SA is a data security company based at the EPFL Innovation Park in Lausanne, Switzerland. CYSEC brings one-click security to container-based workloads and platforms through its CYSEC ARCA trusted OS software. CYSEC also 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.

CYSEC

CYSEC

WHITE PAPER

INTRODUCTION

Enterprises are accelerating their migration to digitalization and to adopting cloud-based services but remain reluctant to move sensitive and mission-critical data and workloads onto the cloud because of concerns that include.

- Integrity and confidentiality of data, particularly while that data is in use
- Ownership and management of the security and encryption keys
- Cloud provider access to the data and workloads
- Regulatory and other government legislation to access data

We also evaluate on-premises technology deployments where internal breaches and attacks are common threats that must be addressed, such as misuse of data and applications initiated by legitimate users or malicious code installed in the enterprise software architecture.

Combining the AMD SEV platform and CYSEC software stack offers enhanced security and data encryption, whether on-premises or in the cloud. Users receive enhanced control over how their data is accessed and used with no need to involve a third-party service provider.

CONFIDENTIAL COMPUTING: AMD EPYC HARDWARE SUPPORT

Confidential computing can help ensure data privacy and integrity by employing hardware-based encryption when enabled on both the host and the VM guest.

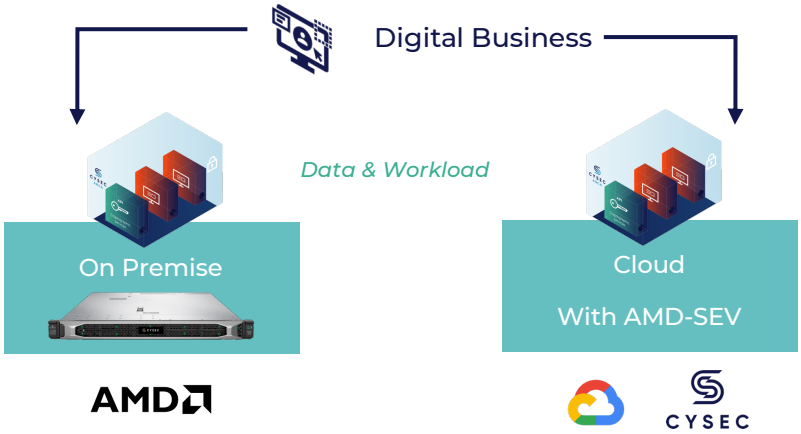
AMD EPYC™ processors contain an AMD Secure Processor that provides a hardware root of trust. Secure Encrypted Virtualization (SEV) uses the AMD Secure Processor to issue and manage keys that encrypt each virtual machine. This helps isolate the hypervisor and guests from each other. Enabling SEV on both the hypervisor and guest allows the guest OS to indicate which memory pages to encrypt. The hypervisor communicates with the AMD Secure Processor to manage the appropriate keys in the memory controller. AMD Secure Encrypted Virtualization-Encrypted State (SEV-ES) builds on this by encrypting CPU register contents when a VM stops running, thereby helping prevent CPU register information from leaking to the hypervisor. SEV-ES can also detect malicious modifications to a CPU register state.

FUNCTION	BENEFIT	CYSEC USAGE AND INTEGRATION
AMD Secure Memory Encryption (SME)	Single key manages full encryption through hardware support	**Intrinsic usage through SEV function**
AMD Secure Encrypted Virtualization (SEV)	VMs are Isolated from each other	**Isolation of ARCA Trusted OS from CSP or appliance administrator/hypervisor**
AMD SEV with Encrypted State (SEV-ES)	CPU registers are encrypted	**Higher security assurance**

AMD SME is enabled either via BIOS or through direct integration into the Linux kernel. Enabling and activating AMD SME usage in BIOS encrypts memory access and one need not activate Linux memory encryption.

The Linux kernel implements Content Security Policy (CSP) and provides the interaction between the AMD Secure Processor (AMD-SP) and the hypervisor. The AMD-SP provides a secure key management interface that performs common hypervisor activities, such as encrypting bootstrap code, snapshots, migrating, and debugging the guest.

AMD SEV-ES expands on AMD SEV by protecting the guest register state from the hypervisor. It encrypts the VM register state on each hypervisor transition to help prevent the hypervisor from seeing the data being used by the VM.



CONFIDENTIAL COMPUTING: CYSEC ARCA ON-PREMISES

ARCA by CYSEC is a full software stack that accelerates deployment of AMD SEV-based services by running natively on a server equipped with one or more AMD EPYC CPU(s) and offering a user-friendly Linux interface and Kubernetes API for service and workload development. Combining AMD SEV with CYSEC ARCA facilitates on-premises or cloud technology deployments while helping enhance security. On-premises deployments that use AMD SEV and ARCA receive the following benefits:

- Patched kernel with hardening patches and safe system defaults.
- Minimal trusted images. CYSEC owns the software tree and masters versions and features. Only required software is installed on ARCA Trusted OS.
- ARCA OS images are read-only and have a robust A/B update mechanism.

- Trusted boot chain (secure boot) with OS image signatures.
- Safe Kubernetes stack on top of ARCA Trusted OS with sandboxing and least privileges by default.
- available to use AMD-SEV features inside containers or run ARCA Trusted OS inside the confidential VM.

SEV services help secure the overall system by encrypting:

- Data being processed and operated by the ARCA Trusted OS VM.
- Clusters and pods being handled by Kubernetes layer..

CONFIDENTIAL COMPUTING: CYSEC ARCA IN THE CLOUD

Cloud Service Providers (CSPs) began launching VM offerings based on AMD SEV technology along with the emergence of Confidential Computing efforts, such as the Confidential Computing Consortium where CYSEC is among the founders.

CYSEC ARCA uses existing Google components for initiating ARCA OS processes, such as the virtualized UEFI bootloader and virtual TPM, and boots only if components such as the bootloader, kernel, and OS bundle have not been tampered with. Once booted, the system forms a Trusted Computing Base (TCB) on which applicative workloads can be deployed using Kubernetes. ARCA manages the full stack and forms an integral part of the TCB. Integrating ARCA with AMD SEV encrypts data in use and active memory spaces. All services and workloads run in CYSEC ARCA, thereby isolating the system from Google services to further enhance security.

End users benefit from this architecture that allows them to use CYSEC ARCA to retain control of their execution environment, data set, and workloads by leveraging AMD SEV technology. They only need to trust Google Cloud during the initial sequence of launching CYSEC ARCA.

FUNCTION	BENEFIT	CYSEC USAGE AND INTEGRATION
UEFI verification	Code executed by computer firmware can be trusted.	**CYSEC-Provisioned secure boot keys help verify the bootloader and kernel bundles**

vTPM support	Data owners retain control of the keys used to protect their data.	**Automated disk encryption is only unlocked if boot conditions are satisfied, that is, if the authenticity of the boot components can be verified)**
Monitoring runtime boot integrity	Only secured and authorized workloads and services are enabled to run, with protection from evil maid attacks.	**ARCA OS are read-only minimal trusted images.**
Full disk encryption	**Enhanced data confidentiality and protection against evil maid attacks.**	**OS components and application data are protected at rest.**
Memory space encryption	**data is protected while in use.**	**ARCA OS leverages AMD-SEV and SEV-ES security features.**

AMD and CYSEC: DATA USAGE IN END USER CONTROL

Combining of AMD SEV technology with the CYSEC ARCA full software stack gives users enhanced control over their data via encryption services that limit both which workloads that can access what data and elements of the operating system. This helps ensure that the end user is the only owner and controller of the entire system.

The model is valid for both on-premises and cloud deployments using CSPs such as Google Cloud. Users can take advantage of Google's scalability and availability services while using AMD SEV and CYSEC ARCA to segregate their datasets and applications from external access by the CSP.

DEPLOYMENT TYPE	AMD SEV	CYSEC ARCA	END USER BENEFIT
On premise	AMD SEV platform and HW based encryption services for memory and data-in-use.	**Full control of the key management system, secure authentication and boot of all services, signed and authorized workloads, and remote attestation control and reporting.**	• **Full control of the system.** • **Simple access to AMD services through ARCA.** • **Full stack for secure trusted execution environment.**
Cloud-Based (GCloud)	Platform availability through GCloud services. GCloud Scalability for IaaS. HW secure primitives managed through CYSEC ARCA.	Using GCloud IaaS scalable infrastructure. Full stack isolated from GCloud access. Access to AMD SEV services. Full encryption of memory and data in use to help prevent access by the CSP.	• **Leverage scaling capabilities of Google Cloud IaaS services.** • **Control of data through CYSEC ARCA+AMD SEV.** • **Data and encryption services are under end-user control.**

THANK YOU

CYSEC