# Secure Lifecycle Management of Confidential Virtual Machines in Public Clouds

João Sereno, Daniel Castro, Nuno Santos, Luis Rodrigues

## Can Confidential Computing unlock Federated Learning?

Federated Learning requires **strong privacy guarantees** across all participants.

Confidential Computing (CC) offers **verifiable isolation through trusted hardware** (e.g., AMD Secure Processor).

This work improves the **practicality and accessibility of Confidential Virtual Machines**, enabling **privacy-preserving computation at scale**.

## Confidential Virtual Machines

Confidential Virtual Machines (CVMs) offer **low performance overhead**, **no application-level modifications**, and **no memory limits**.

CVMs still face some challenges for general adoption: each cloud provider offers **different security guarantees**, deployment and attestation **complexity is handled by the user**, and **lack of cloud-agnostic tooling**.

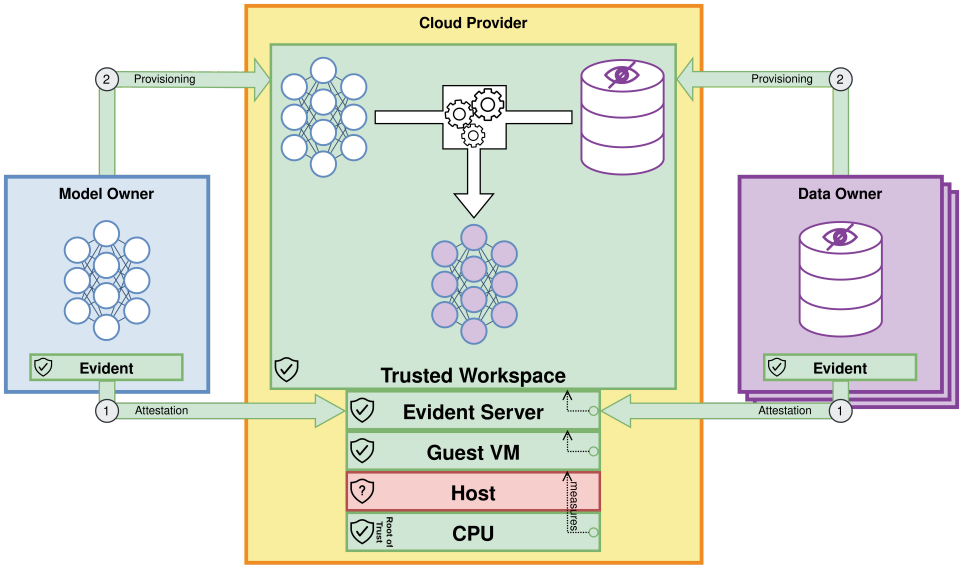
## Our solution: Evident

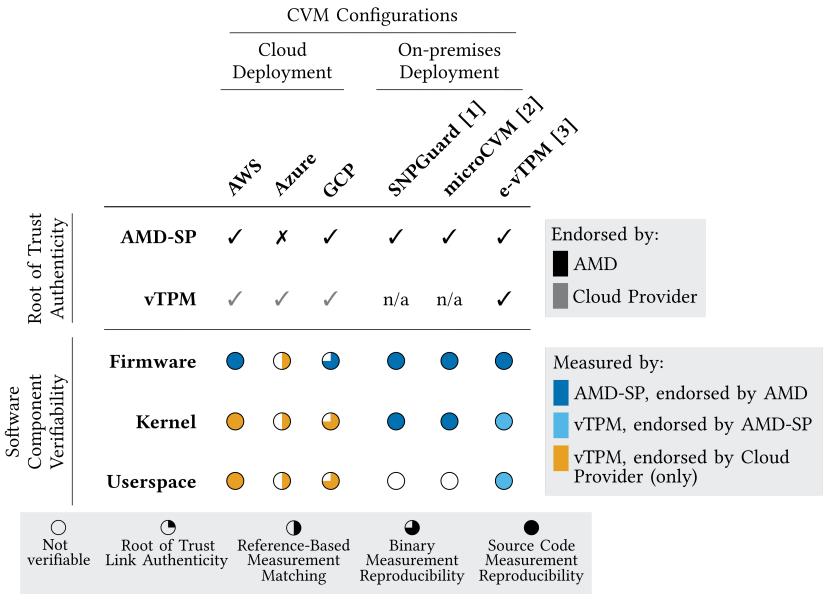
Offers a unified interface to create and attest **multi-cloud deployments** with Confidential Virtual Machines (CVMs).

Ensures **users understand the security guarantees of each attested deployment** through **transparent communication**, backed by verifiable audit evidence.

Designed to **accommodate any use case** that may find value in using CVMs as a security primitive, such as Federated Learning, generic Kubernetes cluster, and more.

**Remote attestation is unified and done from scratch**, trusted elements are transparently sourced, **measurements are reproduced and verified from source code** (when available).




## Verifiability *Status Quo* and Prospects

Major cloud service providers (CSPs) have **incomplete or sub-optimal hypervisor configurations** that limit trust in CVMs, and these settings cannot be modified by users.

While CSPs provide a virtual TPM (vTPM) as an additional root of trust, it is not anchored to the trusted hardware (AMD-SP), unlike the e-vTPM [3] approach.

**CSPs restrict firmware customisation and AMD-SP configuration**, meaning only the VM firmware can be endorsed by AMD-SP. If it was allowed, one could instead configure AMD-SP to **endorse the subsequent boot components' measurements** (as in SNPGuard [1] and microCVM [2] approaches) or **endorse the vTPM device itself**, rooting its measurements in AMD-SP (as in e-vTPM [3] approach).

Currently, **no existing solution implements all verification mechanisms** required to provide comprehensive security guarantees across CSPs.

- **Evident is expected to change this.**

## References

[1] L. Wilke, G. Scopelliti, "SNPGuard: Remote Attestation of SEV-SNP VMs Using Open Source Tools," in 2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2024, pp. 193–198.
[2] Decentriq, "Swiss cheese to cheddar: securing AMD SEV-SNP early boot," https://www.decentriq.com/article/swiss-cheese-to-cheddar-securing-amd-sev-snp-early-boot (Accessed Mar. 27, 2025).
[3] Narayanan, V., et al, "Remote attestation of confidential VMs using ephemeral vTPMs," ACSAC, 2023, pp. 732–743.

## Acknowledgements

This work was developed within the scope of: proj. no.62–"Responsible AI", financed by European Funds, namely "Recovery and Resilience Plan"– Component 5: "Agendas Mobilizadoras para a Inovação Empresarial", included in the NextGenerationEU funding program; the EU's Horizon Europe research and innovation programme under Grant Agreement No 101189689; FCT under grants UID/50021/2025 and UID/PRR/50021/2025; and, IAPMEI under grant C6632206063-00466847 (PT Smart Retail)