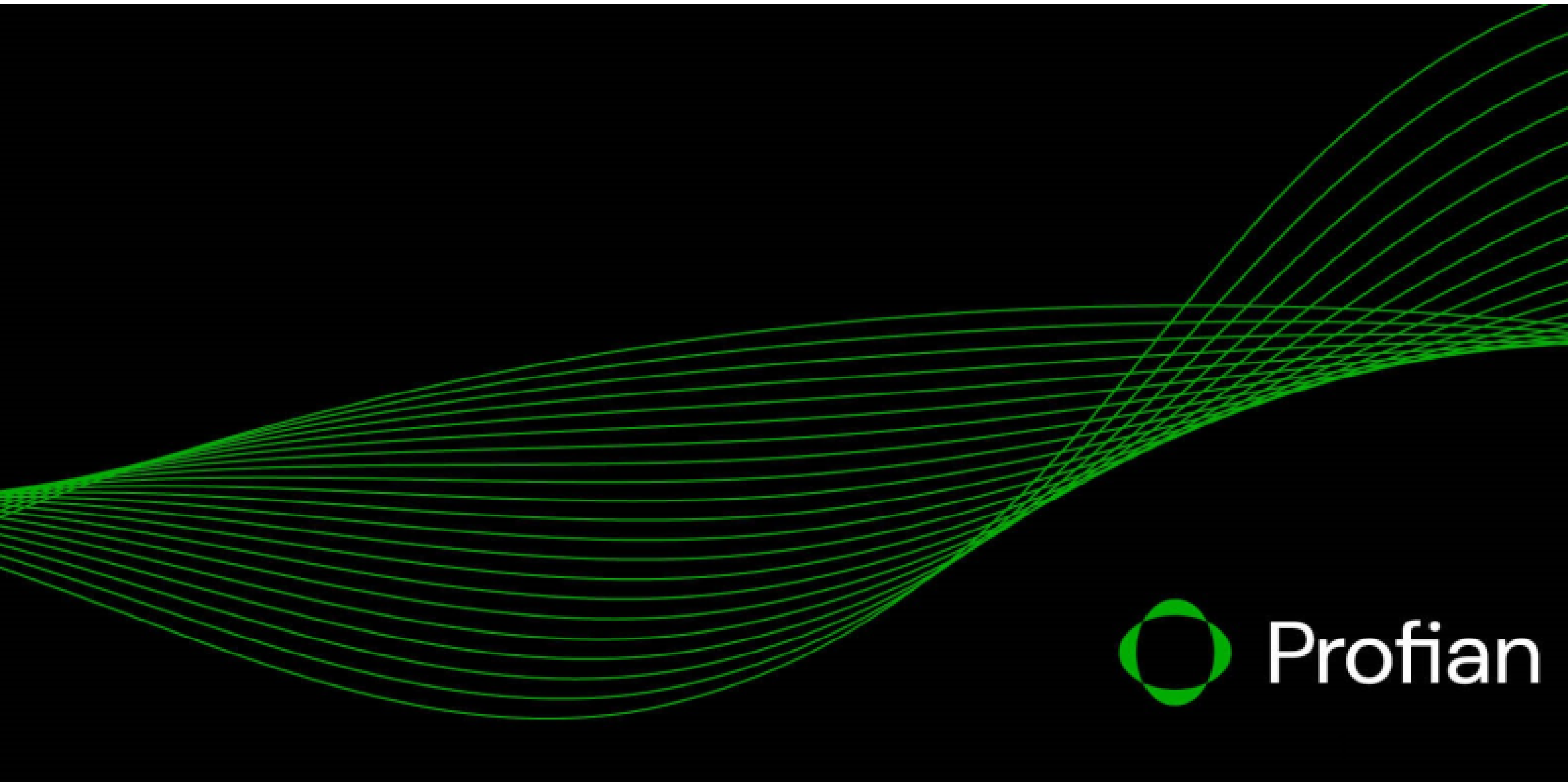
Profian

ENARX AND CONFIDENTIAL VMs COMPARED

Let’s see how these two technologies are similar and different.



Confidential Computing

Confidential Computing

- **uses hardware-based TEEs**
- **provides protection from malicious or compromised hosts**

“Confidential Computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment” as defined by the Confidential Computing Consortium[1]. Examples of hardware-based Trusted Execution Environments (TEEs) include Intel® SGX and AMDI® SEV technologies, which provide chip-based capabilities to allow the creation of applications which are protected from the host computer, including its administrators[2], allowing the protection of both the data they are processing and the applications themselves. These approaches address the problem inherent in existing cloud computing technologies by restricting access to the applications running on a host to the CPU only, blocking all other access by applications or users of the system.

Confidential Computing allows a new approach to cloud native computing that focuses on “security first”, rather than perpetuating existing approaches which have typically attempted to bolt on security measures after development, or which rely on a multiple semi-connected processes through the development process to provide marginal improvements the overall security of an application and its deployment. Confidential Computing allows for cryptographic assurances of the security of a running application, extending or sometimes supplanting approaches such as supply chain security, DevSecOps and dynamic workload scanning.

[1] Confidential Computing Consortium, 2021, A Technical Analysis of Confidential Computing, v1.2, https://confidentialcomputing.io/wp-content/uploads/sites/85/2022/01/CCC-A-Technical-Analysis-of-Confidential-Computing-v1.2.pdf

[2] Note that the AWS Nitro Enclaves® service does not meet this definition, as it does not provide sufficient protection from administrators and operators of the system to ensure that they cannot access data or applications.

Attestation

A successful attestation allows you to trust Confidential Computing

TEE instances allow organizations to protect their applications and data in use, but there is one important step that must be taken before it is safe to deploy applications into TEEs: attestation. It is vital to ensure that a TEE instance has both been correctly set up and is also not the result of a malicious actor pretending to have set one up. Attestation is the process that allows this to take place.

Once a TEE instance has been set up, it is possible to request that the CPU chip[3] that created it produces a cryptographic measurement of the memory the instance contains. This measurement is then cryptographically signed by the chip, and can be sent to an attestation service which checks that the measurement is correct (against a set of expected values) and that the entity which performed the measurement and signing is a real chip from a trusted vendor, with the expected capabilities. If this validation check fails, the TEE instance should not be used, and the application should not be deployed to it.

What are Confidential VMs?

Confidential VMs

- are aimed at "lift and shift" legacy workloads
- do not mix well with cloud native computing
- reduce manageability, increasing cost
- are very difficult to attest
- do not allow for protection from a malicious or compromised host

[3] The process involves the chip and its associated firmware, which are cryptographically linked.

The Confidential Computing Consortium defines a Confidential VM as "a virtual machine that is executed inside a hardware-based TEE, whereby code and data within the entire VM image is protected from the hypervisor and the host operating system."[4] Cloud Service Providers (CSPs), eager to provide opportunities for their customers to embrace these new capabilities, have started to offer Confidential VMs as a stepping stone into Confidential Computing. The prospect of a simple way to enjoy the benefits offered by TEEs is attractive, but the use of Confidential VMs requires careful consideration, as there are many application or deployment types to which they are not suited. In particular, one of the key benefits of Confidential Computing - protection from the host and the CSP - cannot be assured when using these offerings.

Like "normal" VMs, Confidential VMs are intended to allow a "lift and shift" approach to deploying applications. While this approach is attractive for some application types, it loses many of the benefits that organizations have come to expect from cloud native DevOps or DevSecOps deployment methodologies: agility, dependency tracking, ease of update, size of deployment image, speed of start up and microservice-centric architectures.

One of the more obvious challenges with managing VM images for Confidential Computing is immutability. In order to allow for attestation, "known-good" versions of the image to be deployed must be created and measured beforehand. One of the major differences between VMs and other cloud native approaches is the size of image to be deployed. This includes an operating system and libraries which must be bundled together with the image into the application. Given the frequent need for patches and updates to all of these components, maintaining an immutable, measurable image - or, alternatively multiple images and multiple measurements - becomes a logistical nightmare.

[4] Add link to (not yet published) Common Terminology document from the CCC.

Confidential VMs include a major security vulnerability. In order for any Virtual Machine to run, it requires a UEFI image to be provided as part of the deployment. This is tailored to the host on which the VM will run, and must therefore be provided by the CSP. This means that every Confidential VM deployment includes code provided by the CSP, removing any possibility that a cloud customer can be cryptographically assured that their application is free from tampering by a compromised host or malicious CSP. Even if a valid attestation can be performed (given the issues with VM images noted above), it cannot be trusted as it will provide no assurances of protection from the host.

Confidential VMs offer an easy approach for organizations to start using the technologies associated with Confidential Computing. However, they fail to deliver assured protection from a compromised or malicious host: which is the main benefit of true Confidential Computing. Confidential VMs are also ill-suited to cloud native methodologies and represent a step backwards away from the agility, ease of deployment manageability that are key reasons for organizations to embrace the public cloud.

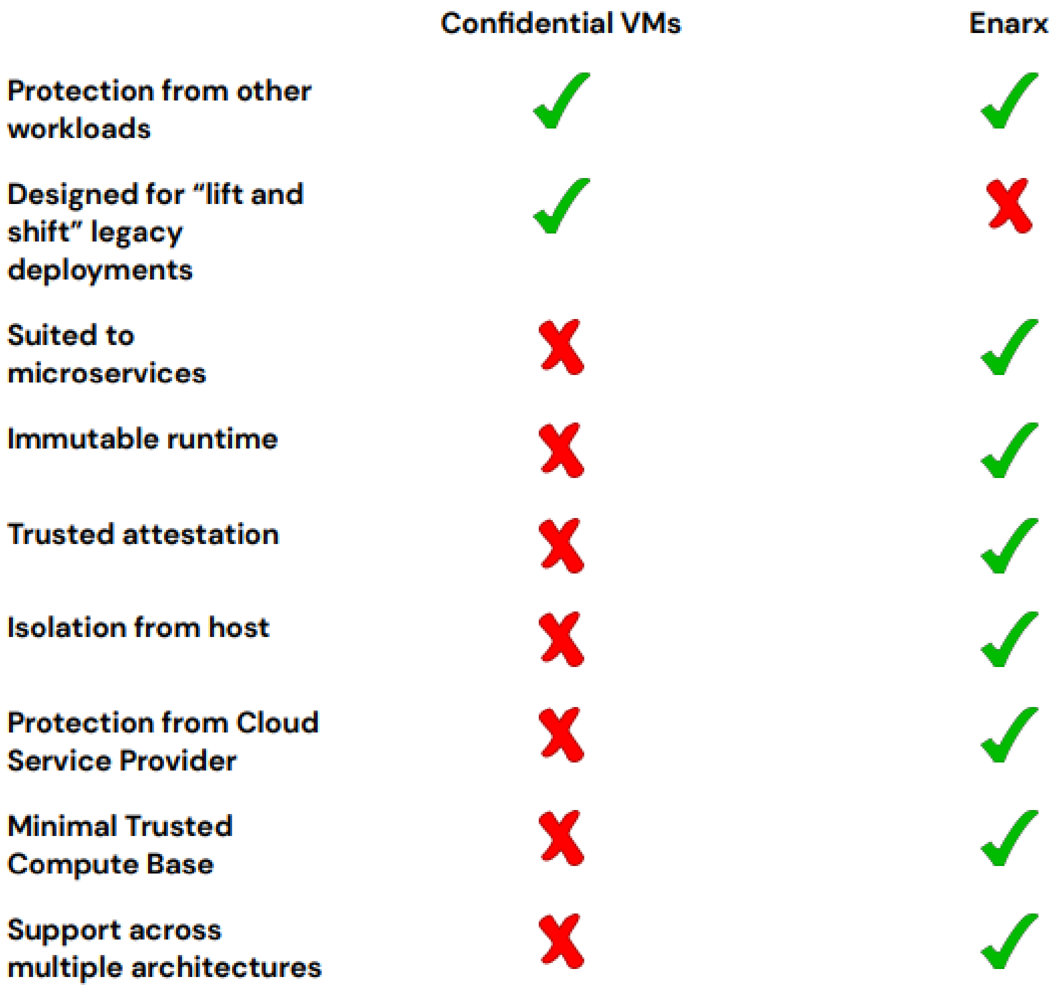
What is Enarx?

- **A deployment framework for Confidential Computing**
- **Designed for cloud native deployments**
- **Applications only deployed after attestation**
- **Small Trusted Compute Base for immutability**
- **Reproducible builds**
- **Uses WebAssembly**

Enarx (https://enarx.dev) is a 100% open source deployment framework for Confidential Computing applications. It handles set up and attestation of TEE instances and performs the deployment of applications to fully attested TEE instances, as well as providing debugging and testing environments. Each TEE instance is measured and a certificate is provisioned by the Enarx framework back into the instance, which is called an Enarx Keep. The Enarx Keep does not include any external components from the host, such as a CSP-provided UEFI. The Enarx Keep is designed to suit cloud native deployment, being as small as possible, both in terms of source code (for simplicity in code coverage and auditing) and in its executable size, to reduce overhead and optimize workload density. Core to the approach taken by Enarx is each Keep runtime is instantiated from a reproducible build, providing immutability as a base building block for the system. Applications running within an Enarx Keep are only deployed once the core runtime has already been measured and attested by a trusted attestation service, removing the need to manage multiple measurements from the application provider and deployer. Enarx deploys applications as WebAssembly binaries. WebAssembly is an open standard for executing applications across architectures, and is supported by many programming languages, including: C, C++, Rust, Go, Kotlin, Python, JavaScript, .NET and Ruby. In many cases, creating a WebAssembly binary from an existing application is as simple as changing the options at compilation time, and WebAssembly is perfectly suited for cloud native deployments such as microservices[5].

[5] "If WASM+WASI existed in 2008, we wouldn't have needed to created [sic] Docker. That's how important it is. Webassembly on the server is the future of computing." Solomon Hykes, co-founder of Docker, @solomonstre on Twitter, 2019-03-27.

Comparison between Confidential VMs and Enarx



	Confidential VMs	Enarx
Protection from other workloads	✓	✓
Designed for "lift and shift" legacy deployments	✓	✗
Suited to microservices	✗	✓
Immutable runtime	✗	✓
Trusted attestation	✗	✓
Isolation from host	✗	✓
Protection from Cloud Service Provider	✗	✓
Minimal Trusted Compute Base	✗	✓
Support across multiple architectures	✗	✓

A comparison between Confidential VMs and Enarx

Profian and Enarx

Profian is a security company providing products and services for Confidential Computing based on the open source Enarx project and is based in Raleigh, NC. It was founded in 2021 by the two co-founders of the Enarx project - Mike Bursell and Nathaniel McCallum - and acts as the custodian for the project, providing engineering and other resources and working to build a strong, welcoming and diverse community of developers and contributors. Profian is a member of both the Confidential Computing Consortium and the Bytecode Alliance. As well as contributing to the Enarx project, Profian is committed to the wider open source community and is involved with multiple upstream projects to improve the security and user experience associated with Enarx.

If you are interested in a demo or to learn more about our solutions, please contact us via http://profian.com.

CONFIDENTIAL COMPUTING
CONSORTIUM

CLOUD NATIVE
COMPUTING FOUNDATION

BYTECODE
ALLIANCE