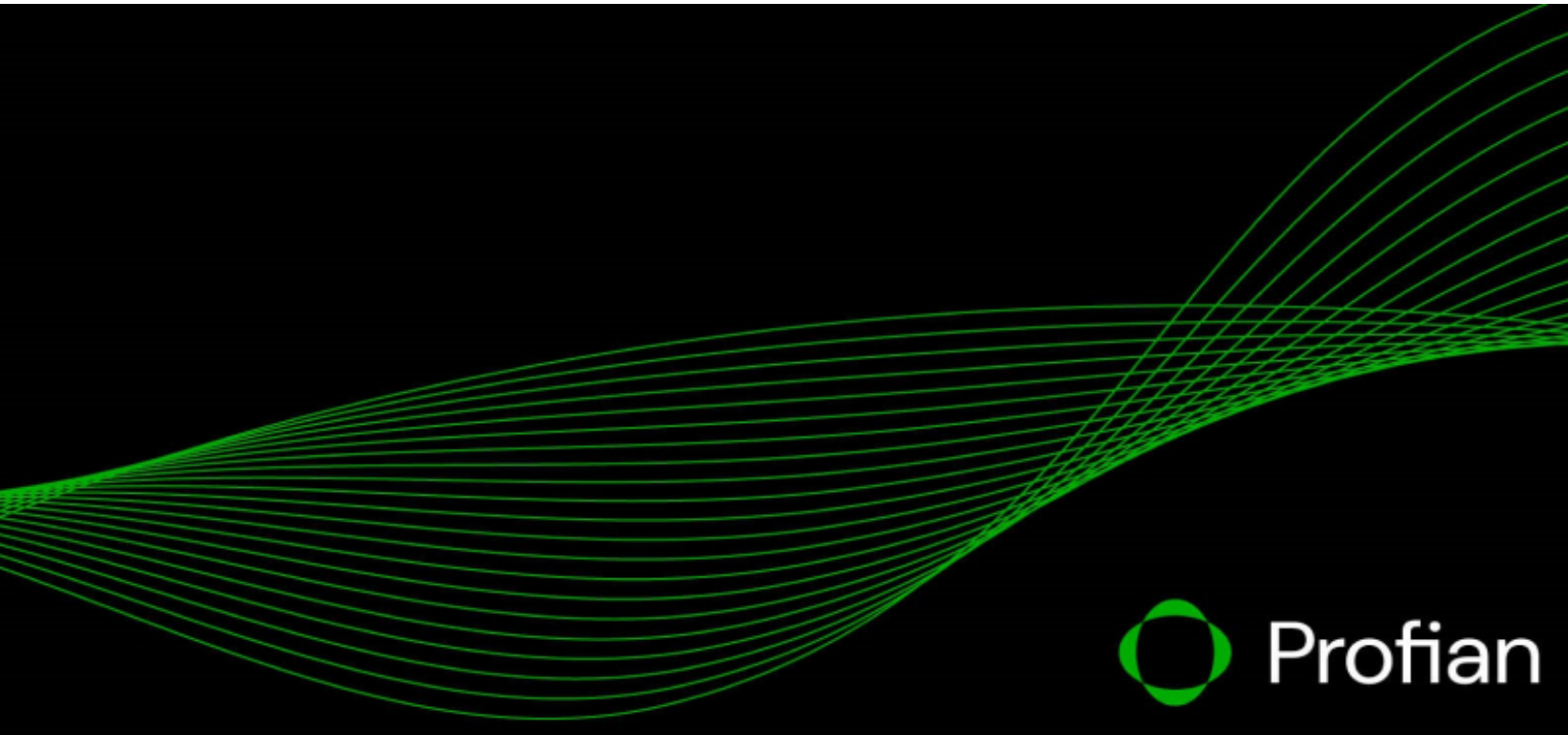
Profian

AN INTRODUCTION TO CONFIDENTIAL COMPUTING

The untrusted cloud, TEEs, and attestation.



Profian

The untrusted cloud

Deploying to the untrusted cloud means that you cannot control access.

"The cloud is just somebody else's computer." This simple statement underpins both the key benefits of cloud computing and its greatest challenge. Organizations can "rent" time on a Cloud Service Provider's computer systems, significantly reducing capital costs, management, patching and administrative overhead and delivering the ability to prototype quickly and scale up in record time: these are all enormous benefits to organizations in multiple sectors worldwide. Deploying your apps and your data to somebody else's computer, however, means you cannot control who accesses them: this is the challenge.

While cloud computing is good at protecting applications from other workloads, the same does not hold for protecting them from the host itself. The problem exists because existing cloud computing technologies require that the computer running applications has complete control over all of the processes and data it is running. The owner of the computer - and anyone who has access to it, whether by design or malicious compromise - controls the computer, which means that they, in turn, have complete control over your applications and data. And while there are commercial and legal agreements that can be put in place to discourage Cloud Service Providers from accessing your apps and data, in the existing, untrusted cloud, there are no technological controls to stop them from doing so.

Confidential Computing

Confidential Computing uses hardware-based TEEs.

"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 that 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.

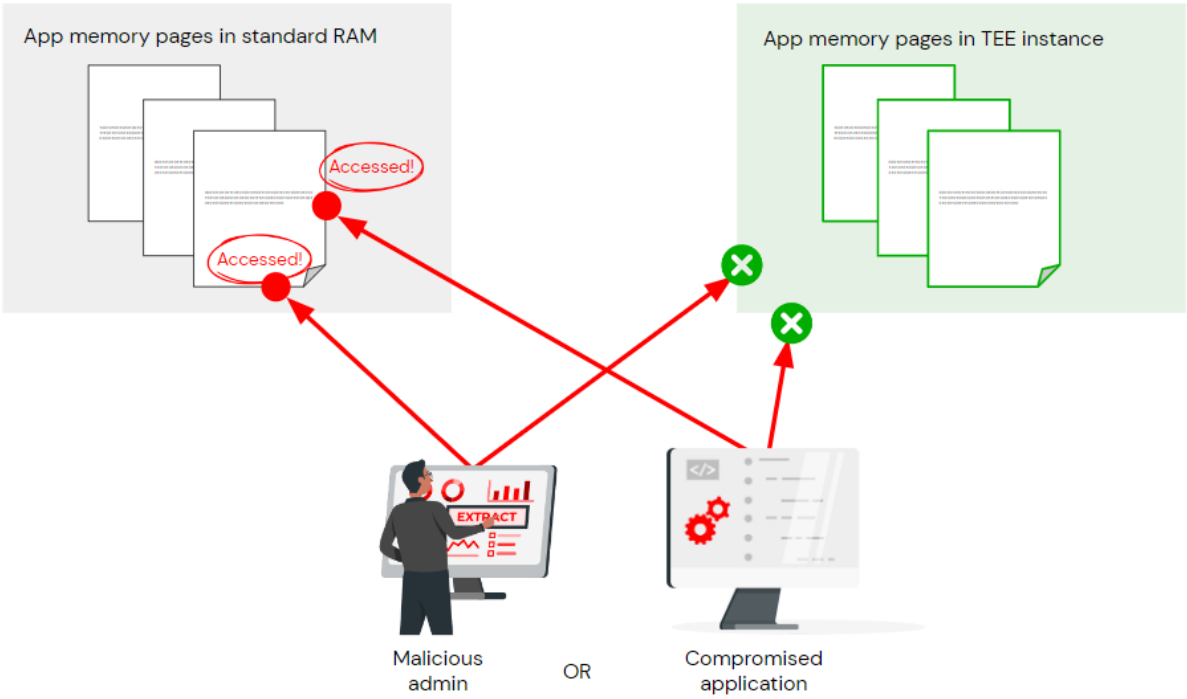
Encrypting memory

Trusted Execution Environments

- can be set up by chips with specific capabilities
- protect data in use
- employ memory page encryption in RAM

[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.



Malicious users and process are blocked from accessing TEE-protected memory pages

The basic mechanism behind TEEs is encryption. Most organizations already use encryption on a daily basis to protect stored data ("data at rest") and data on the network ("data in transit"). Encryption is the well-established minimum mechanism when protecting data. Protecting data – and applications – with encryption when it is actually being processed ("data in use") is, however, impossible without specific hardware capabilities: this is what TEEs provide.

In standard computing, all of the memory in which data is kept when it is in use (RAM) is unencrypted, allowing any sufficiently privileged users and processes such as administrators, the operating system, hypervisor and compromised processes to look at data and change it. TEEs solve this problem by encrypting the memory pages of sensitive applications, including both the code and data, in such a way that they are never unencrypted ("in the clear") in RAM. This prevents all other processes from being able to look inside them or change them, providing confidentiality and integrity protection.

Confidential Computing requires the availability of computers with the relevant chip capabilities (e.g. SGX and SEV). It also requires the availability of mechanisms to create TEE instances on specific machines and to deploy applications and data into them safely.

Attestation

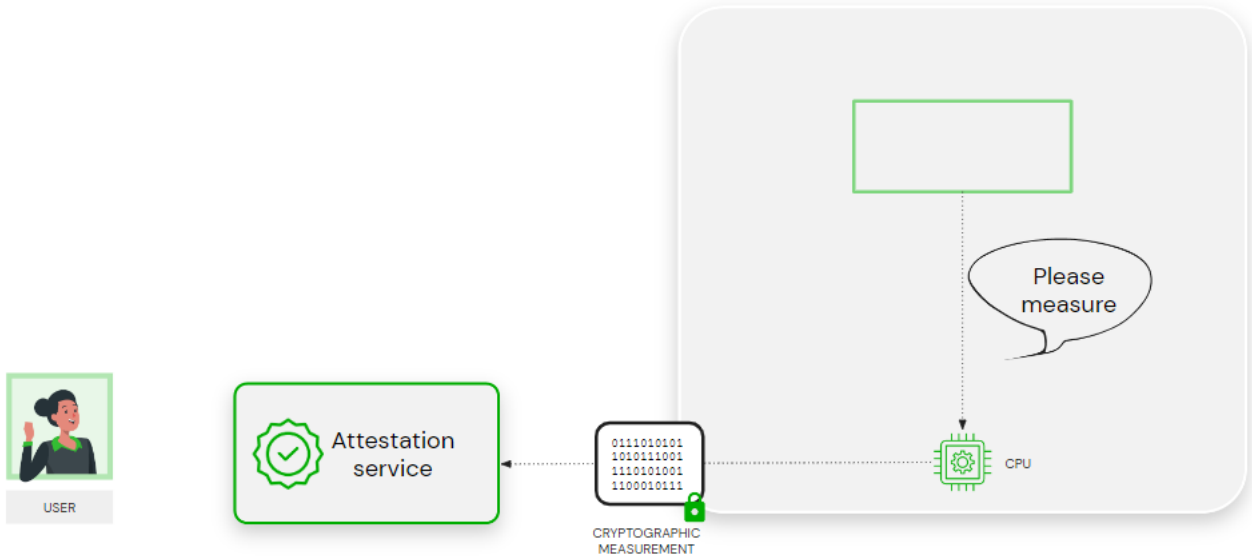
A successful attestation allows you to trust a TEE instance.

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.

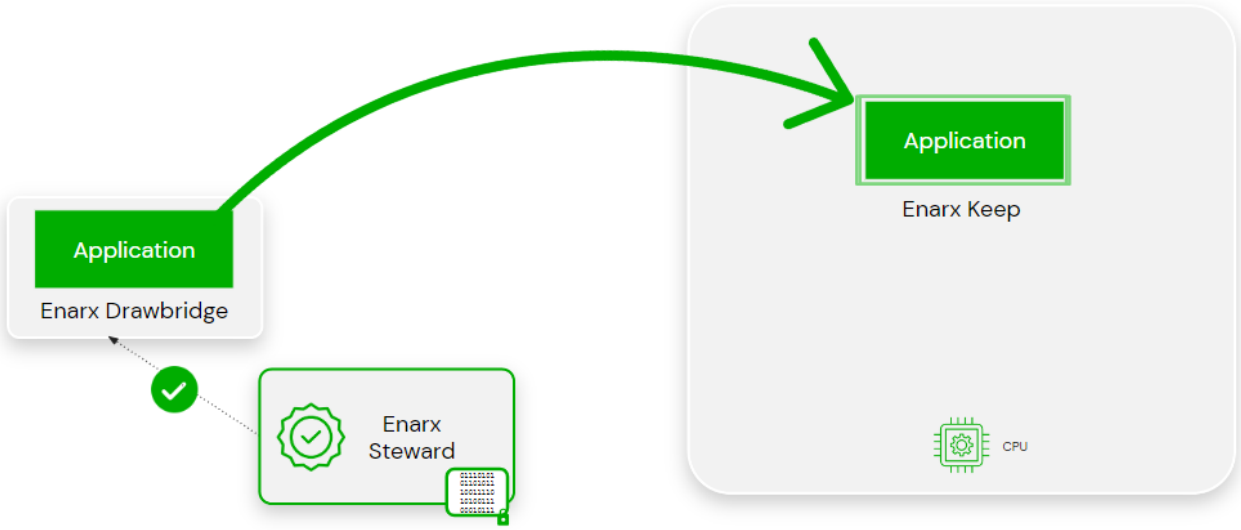
Once a TEE instance has been set up, it is possible to request that the CPU chip[3] that created it produces a cryptographic measurement of the memory the instance contains. This measurement is then cryptographically signed by the chip, and can be sent to an attestation service which checks that the 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.

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



The TEE instance requests a measurement from the CPU, which is passed to an Attestation service

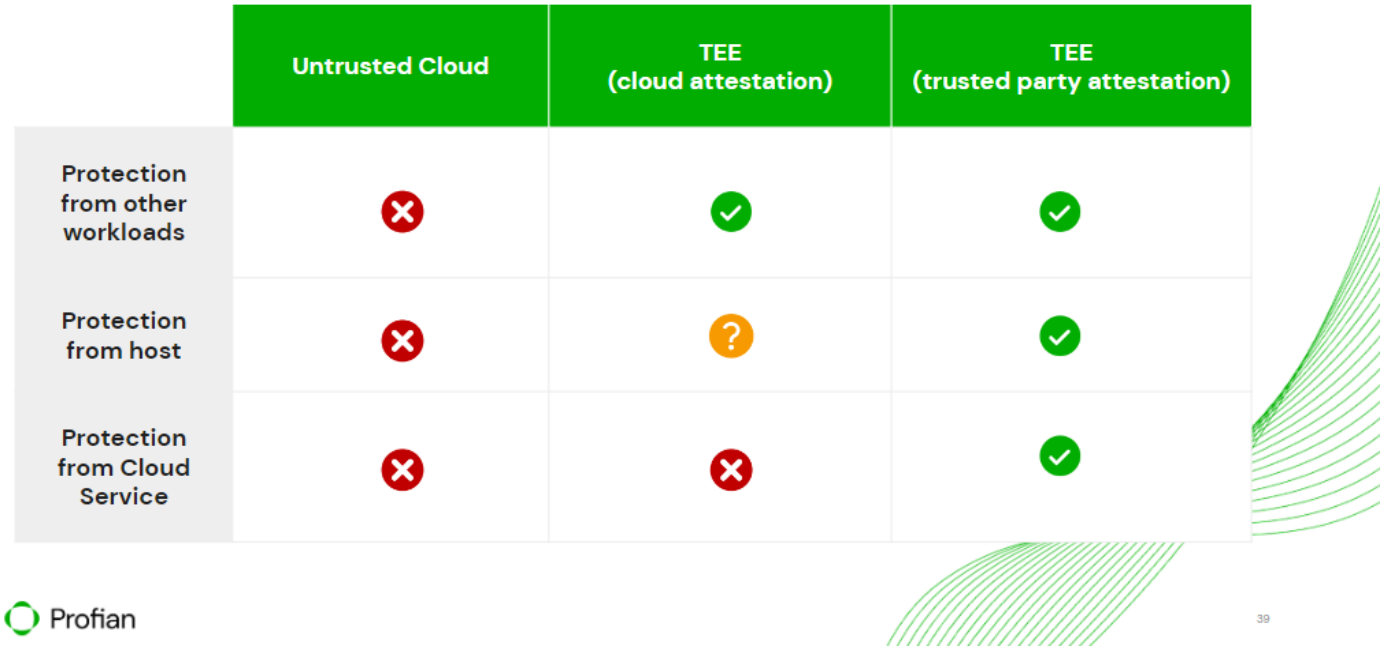


If the Attestation service validates the measurement, the application can be safely deployed.

Because the measurement is performed by the chip, and not the operating system, this attestation process allows the assurance that there is no opportunity for a malicious or compromised host to “spoof”

a TEE instance. As long as the attestation is properly validated, this means there is a cryptographic proof that the Cloud Service Provider cannot interfere with the application. This validation must, however, be performed by an independent trusted party: in order to allow a true trust relationship to the TEE instance to be established, the entity providing the attestation must not be associated with the Cloud Service Provider.

If the entity performing the attestation is associated with the owner or operator of the systems running the TEE instances, it would be easy for them to provide false assertions that attestation was successful, all-the-while spoofing the TEE instance: there is no way for the organization deploying the application to know.



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.