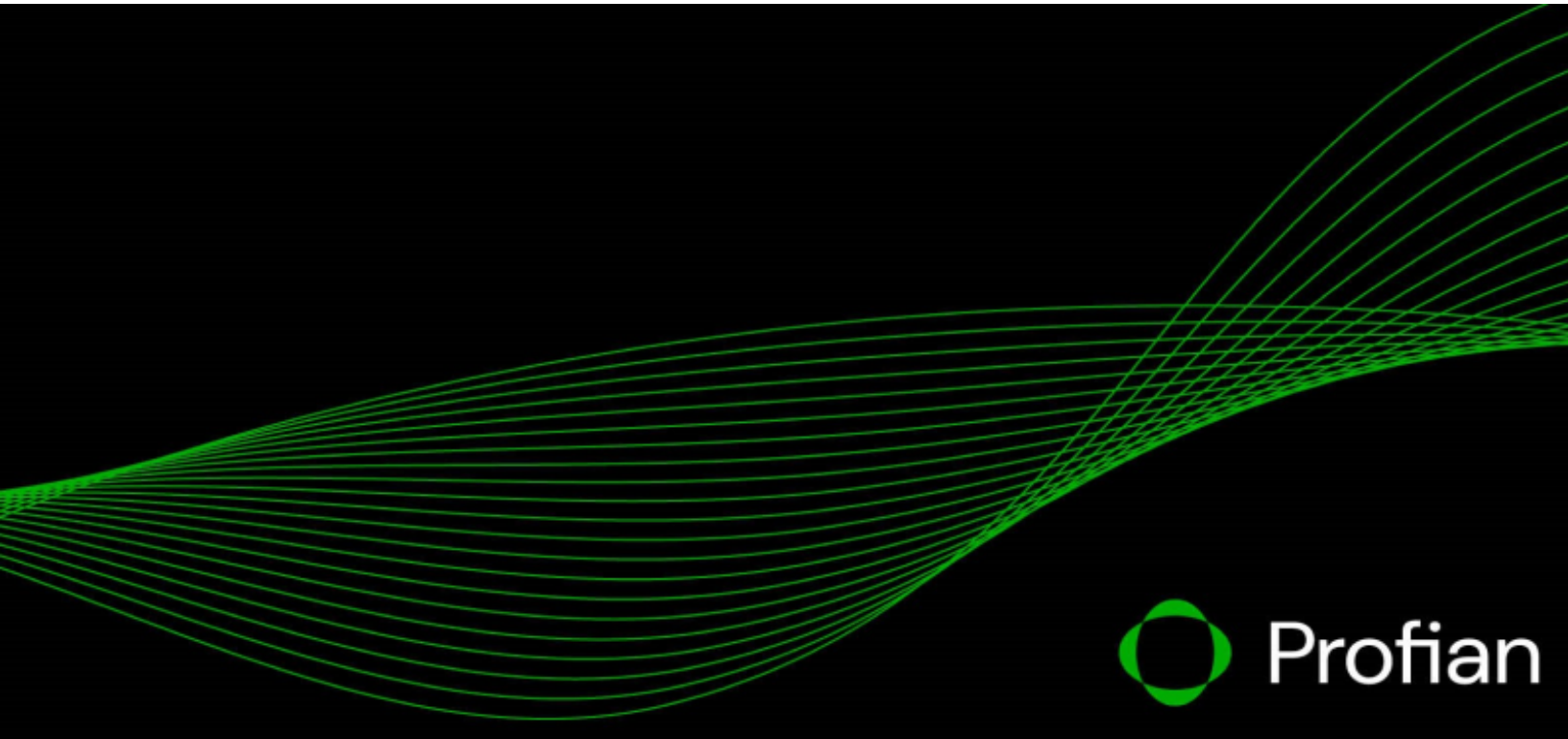
Profian

RUNTIME SECURITY ISOLATION AND CONFIDENTIAL COMPUTING

Learn more about protection
from the application host



What is isolation?

Every time an application runs on any platform - from the largest mainframe to the smallest IoT device - it executes code as on physical hardware. An increasing number of applications, particularly on public or private cloud servers and also on the Edge, actually execute using virtualization technologies. These technologies allow multiple applications, also known as *workloads*, to run on the same physical machine, or host system, without needing to know everything about it. They are isolated from the host to varying degrees, depending on the specific platform and application.

Common virtualization technologies include:

- Virtual machines (VMs)
- Containers
- Serverless functions
- WebAssembly sandboxes

Given that not all applications, nor all users, are friendly in all cases (and applications which are friendly may be badly written or compromised), there is a need to isolate them from each other and from the host system.

For a deeper dive into managing insider risk with Confidential Computing, download our white paper.

Isolation can allow protections for the host and/or workload. The most common are referred to as the C.I.A. triad:

- Confidentiality - stopping another entity from seeing information
- Integrity - stopping another entity from changing information
- Availability - stopping another entity from interfering with the functioning of a workload, including its execution and communications

© Profian 2022

There are three different types of runtime isolation[1], all of which are important in different situations. They are:

- Type 1 isolation - workload-from-workload isolation
- Type 2 isolation - host-from-workload isolation
- Type 3 isolation - workload-from-host isolation

TYPE 1

Workload from workload isolation

VMs and containers handle this pretty well

TYPE 2

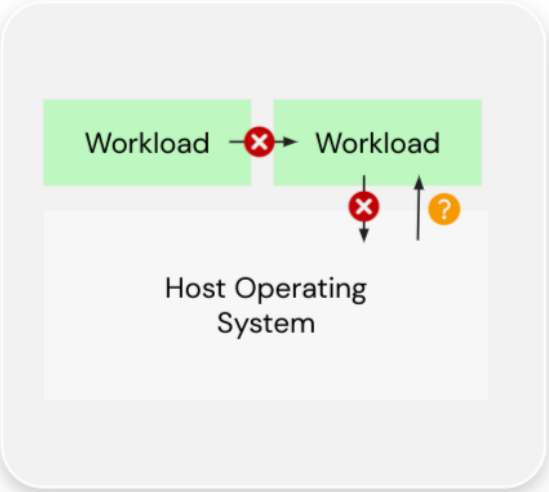
Host from workload isolation

VMs and containers handle this pretty well

TYPE 3

Workload from host isolation

Not possible with standard virtualization



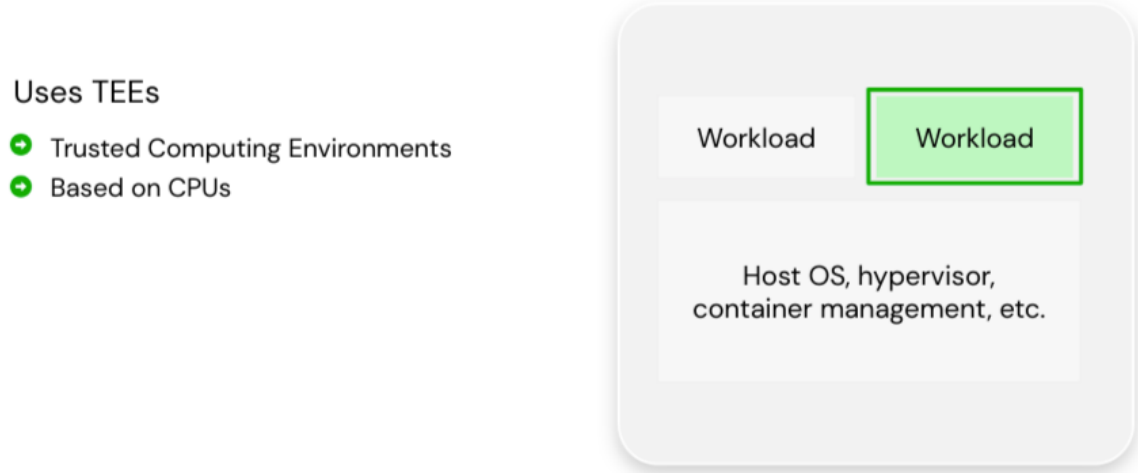
These types of isolation typically provide a variety of protections. Standard virtualization technologies can provide only type 1 (workload-from-workload) and type 2 (host-from-workload) isolation. While this is good enough for certain types of application, and allows providers of hosts such as Cloud Service Providers (CSPs) with protection for their systems, there is a large set of workloads for which this is insufficient. These are workloads that contain sensitive data or applications, and therefore require protection from the host, which itself may be compromised or malicious: they require type 3 (workload-from-host) isolation.

[1] Bursell, 2021, Trust in Computer Systems and the Cloud, Wiley, Hoboken, p.202

© Profian 2022

Confidential Computing provides type 3 runtime isolation

Confidential Computing is specifically designed to address type 3 (workload-from-host) runtime isolation, and provide protection from the host on which an application is running.



"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[2]. Examples of hardware-based Trusted Execution Environments (TEEs) include Intel® SGX and AMD® SEV technologies, which provide chip-based capabilities to allow the creation of applications which are protected from the host computer, including its administrators, 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

[2] 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

© Profian 2022

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 and on-premises 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 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.

Secure workloads with Profian Assure

Confidential Computing with Profian Assure:

- uses hardware-based TEEs
- provides type 3 (workload-from-host) runtime isolation
- enables integrity and confidentiality protection for data and applicatiions

Profian’s flagship Confidential Computing solution, Profian Assure, makes it easy to create encrypted, private environments on public cloud hardware to protect both data and applications while in use.

Profian Assure provides an added layer of security to your Confidential Computing environment through an automatic attestation process, which restricts the deployment of your workload to the secure environment until the attestation process is complete. Receive neutral, third-party validation that your “virtual vault” has been created properly to protect both your applications and data before they are deployed.

© Profian 2022

Profian

Profian delivers Confidential Computing solutions that solve for security of data in use, a well-known vulnerability of cloud computing. We help security teams seamlessly create private environments on public cloud hardware so organizations can enjoy the speed, scale and cost-saving benefits of cloud computing for even the most sensitive workloads. Profian's third-party attestation service helps meet regulatory standards and build trust with customers. Our solution builds on the open source project Enarx, of which Profian is the custodian.

Profian is a a member of the following organizations:

© Profian 2022