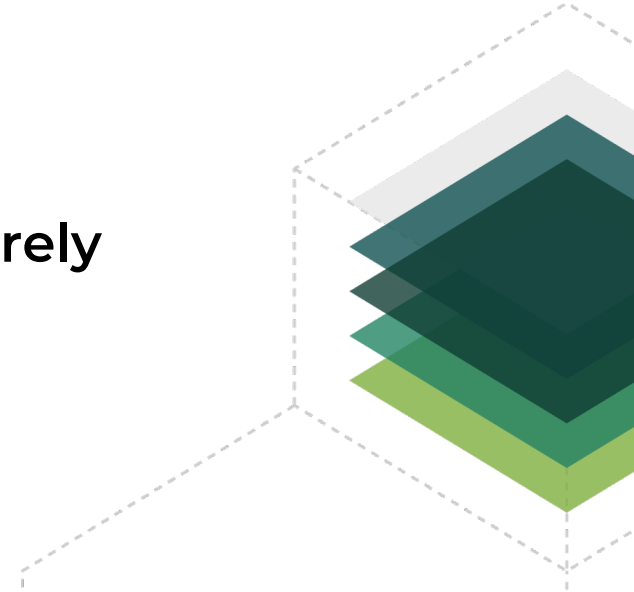
anjuna

Allowing enterprises to securely embrace the cloud



https://anjuna.io

Confidential Compute

- Compute environments with workload isolation guarantees that provide for the protection of applications and data utilizing hardware-based secure enclave or trusted execution environment (TEE)

- Capabilities of a specific confidential computing environment are defined by the hardware, with a means provided to applications to verify guarantees independent of the software stack they run on (an immutable root of trust)

Application

Application range

100k machines

- Google Search
- Lambda/Serverless
- Micro Service
- SOA
- nTier
- Monolithic multi-threaded
- Monolithic single process
- Hello World

1 machine

- Set of code, data and connections that collectively perform a business function
- Defines the set of things that need to function as a logical group that are desired to be isolated from other applications or components of the software stack
- This is the ideal boundary of what is to be trusted

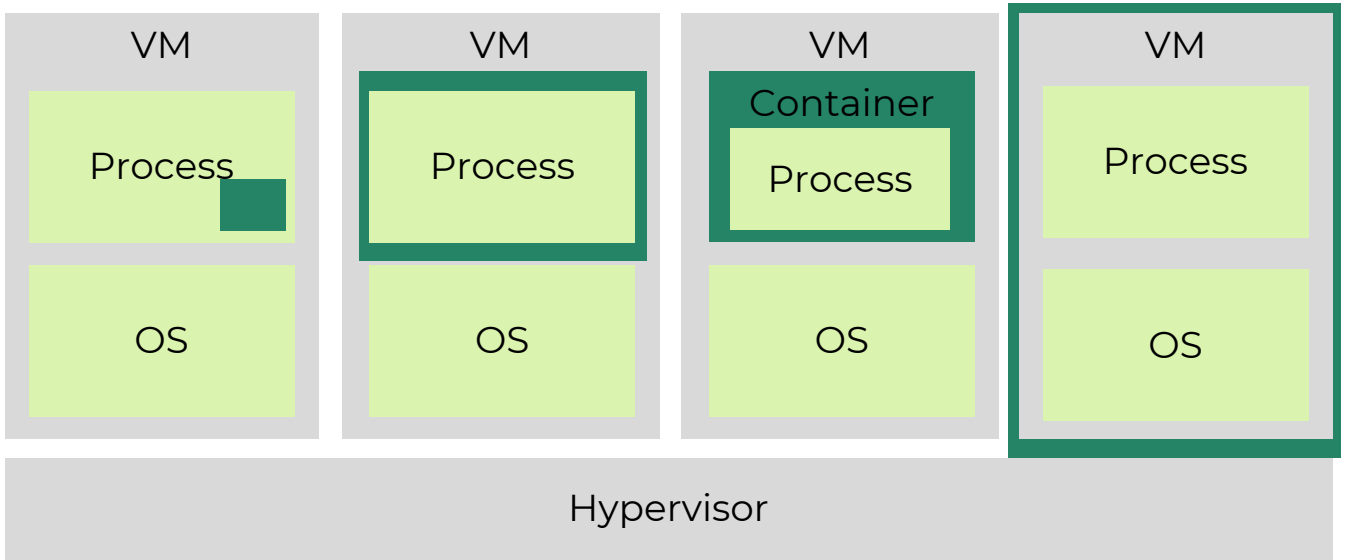
Full Stack

- Refers to the complete set of basic components and functions that enable modern software to run CPU, memory, all kinds of storage, and network communications
- The “full software stack” also includes hypervisors, operating systems, virtual machines, containers and other applications (including security software) that support the final application

Isolation Perimeter

- Defines where in the software stack the boundary of isolation is enforced. Also defines what needs to change and what software needs to be added to the full stack to support the isolation Perimeter.

- Intra-Process
- Process
- Container
- VM
- Machine



Trusted Code Base

- All executable code that is inside the isolation perimeter enforced by the confidential compute environment

Creating Trusted Code

- Application Development
  - Application is modified at development time with tools like SDK's and libraries that enable developers to add the ability to take advantage of confidential compute
- Compile time
  - Application is modified by compilers and assemblers, patching tools, etc. that inject code to take advantage of confidential compute. Used while building applications.
- Lift and Shift
  - Tools to enable running an application in a confidential compute environment with little or no modification. Used while deploying applications.
- Runtime
  - Adding capabilities to components in the Full Stack that allow taking advantage of confidential compute capabilities. Added to hypervisor, VM, container, Interpreter or OS. Used when the application is executed.

Enterprise Enclave Software

- A secure enclave solution enhanced to address the specific needs and requirements of enterprise IT organizations. Enterprise enclaves provide enclave protection and management **that extend beyond memory and compute to storage and network communications**. They enable existing applications to be run unchanged within an enclave, and they provide the functionally complete capabilities that enable a Confidential Cloud.

Confidential Cloud

- A confidential cloud is a private and secure computing environment typically formed over public cloud infrastructure, leveraging enterprise enclave software as its foundation