



Introduction to Anjuna Confidential Computing Platform

Introduction

Any organization that deals with sensitive data, especially in the cloud, is challenged by the risk of data exposure and compromise when security controls are limited to strictly software. Software is always vulnerable to those who can access lower layers in the compute stack. Anyone with host access can easily get data. Without hardware-backed roots of trust and trusted execution, software-only security remains the weakest point in even the most resilient infrastructure. It cannot adequately shield data from attackers, insiders, or cloud operators. These concerns have kept many organizations from migrating sensitive workloads to the cloud.

An innovative technology called Confidential Computing delivers a breakthrough approach to protecting data. Confidential Computing secures the processing and handling of sensitive data through hardware-level technologies in modern CPUs such as AMD (AMD-SEV), Intel (SGX), and AWS (Nitro Enclaves). Cloud providers have embraced these chip advancements and made Confidential Computing features widely available, enabling organizations to process workloads securely with trusted hardware. However, hardware alone is insufficient to fully embrace this new approach, as organizations would need to rearchitect their application and hire developers with kernel and cryptographic expertise. Moreover, the heterogeneous nature of Confidential Computing hardware would lead to operational silos and management complexity.

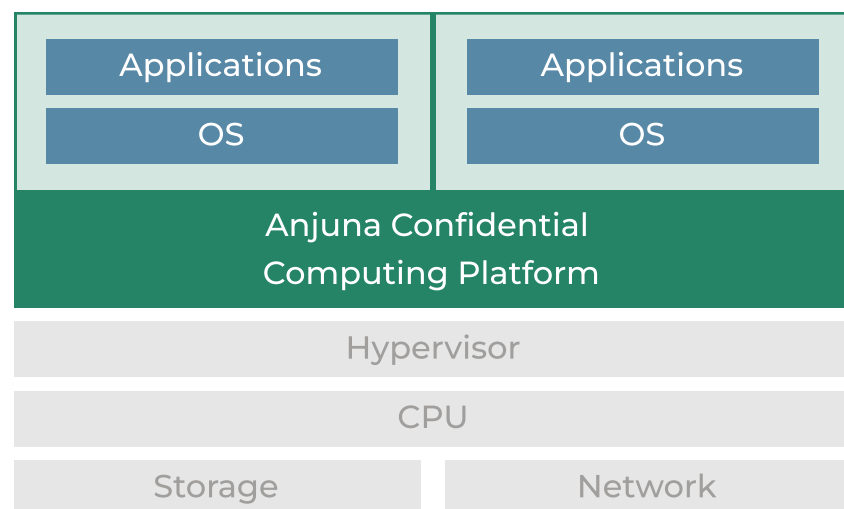
Anjuna eliminates this heavy lifting by offering a software platform that abstracts the underlying confidential CPU hardware and interfaces directly with customers' applications at runtime to provide complete protection of data in use, at rest, and in motion without requiring changes to the application. Furthermore, Anjuna provides additional capabilities that organizations need to take full advantage of Confidential Computing and offers a uniform approach across clouds and processors.

Anjuna Protects Workloads With Unprecedented Security

Anjuna's Confidential Computing Platform helps enterprises create high-trust environments in the cloud where data is always encrypted and code is verified for authenticity. With Anjuna, workloads stay confidential and trusted during execution, enabling enterprises to embrace the cloud and innovate without the threat of attackers or insiders eavesdropping on or tampering with code or data. Unlike other data security solutions, Confidential Computing is rooted in chip hardware, which offers substantially higher levels of trust, integrity, and security. Anjuna lets enterprises leverage those properties through its platform to protect applications with minimal performance impact. Using Anjuna, enterprises can instantly secure all aspects of data, memory, storage, networks, and the cloud without needing to recode their applications.

Additionally, Anjuna supports multi-cloud and hybrid environments and does not require specialized skills to deploy or run, making it flexible and easy to use. Organizations leverage Anjuna to run existing applications in the cloud with complete privacy, security, and isolation. Anjuna supports applications, containers, and Kubernetes and runs workloads in trusted and secure hardware processors or enclaves. The powerful attestation capabilities of the hardware are simple to use with Anjuna, enabling organizations to prove their workloads are authentic and haven't been tampered with and that their workloads are running on secure hardware. This mechanism allows organizations to establish the most robust levels of trust in their applications.

Anjuna creates a barrier and provides hardware isolation, securing applications from modern cloud risks.



After customers deploy workloads to enclaves, their sensitive data and processes become fully shielded from modern cloud risks. Customers benefit from the following:

1. Memory encrypted by a dedicated processor protects code and data in use

All code, AI/ML models, and data are now secure in memory. Only a secure portion of the processor can decrypt memory with a key that it contains. Unlike traditional secure processors (e.g., HSMs), Confidential Computing chipsets operate with full core capability and large memory capacities. Memory encryption is handled by dedicated on-chip accelerators, ensuring no performance impact on running applications.

2. Compute that is logically isolated and separated from untrusted infrastructure

Workloads and data are no longer vulnerable if attackers, malware, insiders, or cloud admins access infrastructure. Not even admins or users who gain root access to hosts can view running workloads.

3. Hardware-isolated process management

The previously vast attack surface, comprising many parts of the infrastructure and compute stack, shrinks to an absolute minimum: the CPU.

4. Strong attestation enables workloads to be trusted by others

Workloads can prove that they 1) are authentic and have not been tampered with and 2) are running on trusted hardware. Confidential Computing provides hard evidence, control, and proof of this. The most common use for attestation is securely bootstrapping applications with the secrets they need. Anjuna's platform cryptographically binds initial secrets to workloads at runtime, solving the "secret zero" issue. The Anjuna platform and Policy Manager can securely distribute secret data, initial tokens, keys, and sensitive environment variables to applications. This is impossible to do securely in traditional workloads. But attestation provides a unique hardware-based application identity that serves as a trust anchor for further trusted processing and application interaction.

5. Comprehensive protection at run time for data in use, at rest, and in motion

Anjuna automatically protects the entire workload, including code, data, dependencies, files, temporary files, caches, and other data usually exposed on disk or in memory. This dramatically reduces risk.

6. Hardware-based evidence of workload execution, location, and instance type

Strong guarantees that a workload ran as expected, in a specific location, or on a particular machine can aid in compliance reporting. They can also help in novel use cases requiring data to be processed in particular locations or jurisdictions with preferred regulatory conditions.

How The Anjuna Platform Works

Anjuna helps organizations deploy Confidential Computing simply and quickly with a comprehensive approach that comprises build, deploy, run, and trust stages.

Build

Customers take their applications, including containerized ones, and leverage Anjuna to build an image of it that is compatible with their cloud provider's Confidential Computing solution.

Deploy

Customers enable other systems to trust their applications by configuring attestation. Customers first measure their image to get a fingerprint, which serves as an identity for their application. Then, for example, they create access policies in an attestation-aware secrets manager using the fingerprint. If the application presents the correct fingerprint at runtime, the secrets manager can securely give it secrets. This pattern can be extended to other systems.

Run

Applications run fully protected by the Anjuna Confidential Runtime. They are shielded from eavesdropping and tampering. Even those who gain root access to the host machine cannot access or modify code and data.

Trust

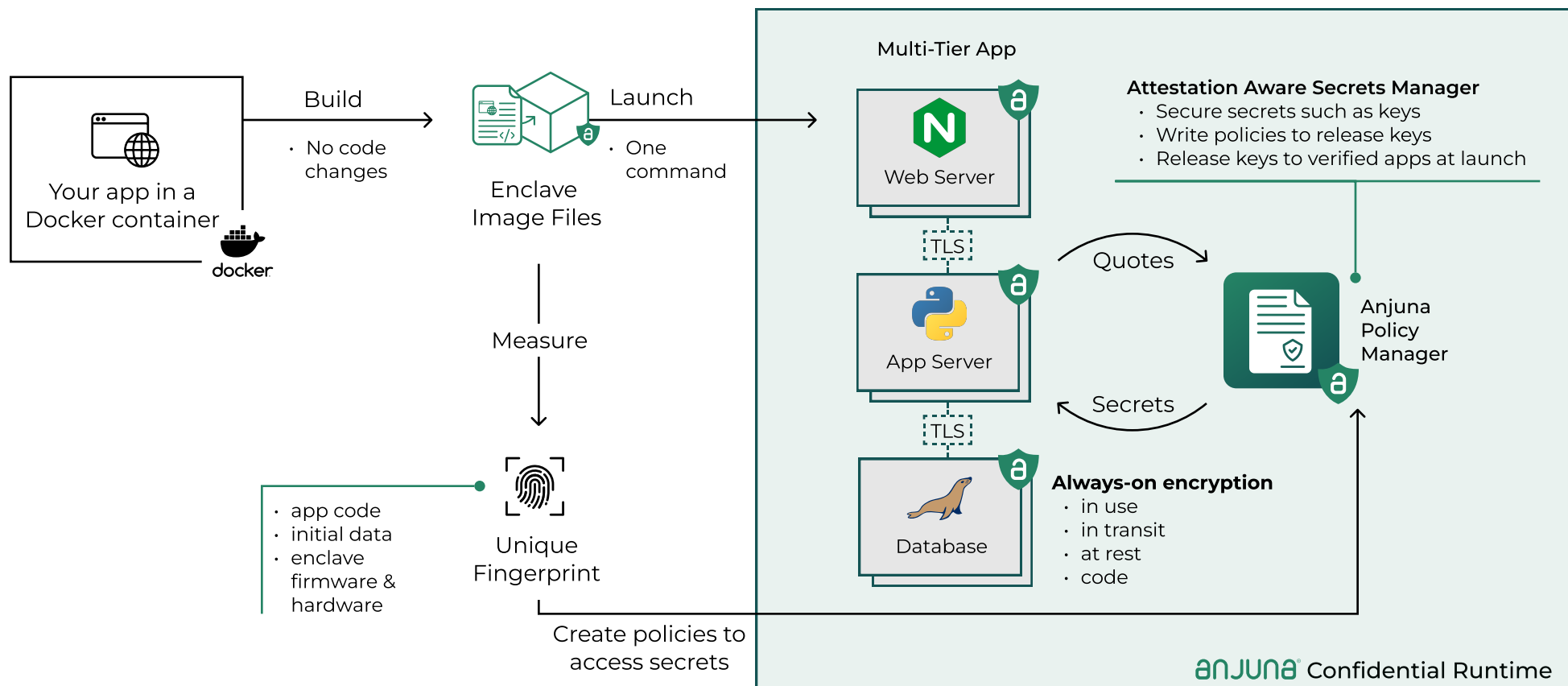
Using the previously configured policies, applications securely establish trust with external services, such as a secrets manager from which it can get secrets such as keys, configuration settings, API tokens, etc. This mechanism eliminates the secret zero problem.

Build

Deploy

Run

Trust



Anjuna Hardware Security Virtualization



On Prem



AWS



Azure



GCP



Kubernetes

Anjuna Platform Features

The Anjuna Confidential Computing Platform comprises the following features:

Confidential Runtime (CORE)
Anjuna Confidential Containers
Performance Optimization
Enclave Lifecycle Management
Multi-Cloud And Hybrid-Cloud Support
Kubernetes Support
Always-On Encryption
Confidential Data In Use
Confidential Data In Transit
Confidential Data At Rest
Confidential Code
Always-On Trust
Trusted Build
Trusted Start
Trusted Execution
Policy-Based Verification
Anjuna Policy Manager
3rd Party Key Management Policy
Platform Operations
Image Builder
Debug Mode
Monitoring, Events And Logs
Platform Extensions And Integrations
AWS KMS Integration
AWS Elastic Kubernetes Services (EKS) Support
Azure Kubernetes Service (AKS) Support

How Customers Deploy Anjuna

The Anjuna Confidential Computing Platform is software. It functions as a hardware security virtualization layer and installs on the operating systems that run on supported Confidential Computing chipsets. To support scalable deployments, most customers choose to instrument Anjuna into their CI/CD or runtime launch processes. Anjuna gives customers complete flexibility to deploy on multi-cloud, hybrid-cloud, and on-premises environments. Customers run Anjuna with a single command and point to the application they wish to protect. It's that simple. Anjuna protects custom, open-source, and commercial applications - all without modification. Anjuna also supports containerized applications and Kubernetes.

Organizations Can Securely Transform And Rapidly Innovate

With Anjuna, organizations can deploy Confidential Computing technology to solve various challenges. Indeed, securing workloads and keeping them private are often the primary goals, but organizations also apply the technology to unleash innovation, reduce risks, and collaborate in new ways. Common goals include:

- Rapidly protect code and data in use**
 Protect intellectual property and sensitive data - including AI models, next-generation payment transactions, application code, and PII - even from root users with the highest privilege levels, insiders, and attackers.
- Protect keys in key management or caching systems**
 Secrets exposed in memory in cleartext can be quickly protected, reducing a critical risk for many organizations that handle credentials, keys, and API tokens.

3. Unblock stalled cloud migration initiatives

Organizations blocked from moving sensitive workloads to the cloud because of concerns over data privacy or regulations can unblock those initiatives with Confidential Computing technology.

4. Secure Web3 infrastructure

Key exposure in blockchain processing is a significant risk. Confidential computing can protect the keys and protocols as transactions occur on validator or signing nodes.

5. Enable multi-party computing and multi-party analytics

In scenarios that require multiple entities to share data for analysis but cannot see each other's data, Confidential Computing enables complete analysis while preserving privacy.

6. Embrace simpler architectures for privacy compliance

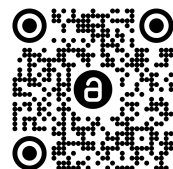
Organizations can deploy an end-to-end Confidential Computing model that enables immediate data analytics without the complexity of traditional privacy tools. They can create computing instances that are the sole operator on data, yielding results on data whose privacy must be protected.

7. Prepare for future quantum computing risks

Running sensitive workloads on confidential hardware allows organizations to adapt to future quantum risks straightforwardly. This is important for future quantum-resistant strategies. Rather than refactoring applications, organizations can update the underlying hardware to new processors.

About Anjuna

Anjuna is a US-based software company headquartered in Palo Alto. We enable Confidential Computing to be ubiquitous and accessible by unlocking Confidential Computing CPU technology across different clouds and chipsets. Anjuna delivers unprecedented security and performance without requiring code changes, providing flexibility and shortening time to value. Organizations of all sizes, from Web3 organizations to governments, leverage Anjuna to prevent costly data breaches, secure workloads on infrastructure they don't own or control, and accelerate cloud and digital transformation projects.



Join us for a live demo

anjuna.io