DATASHEET

anjuna®

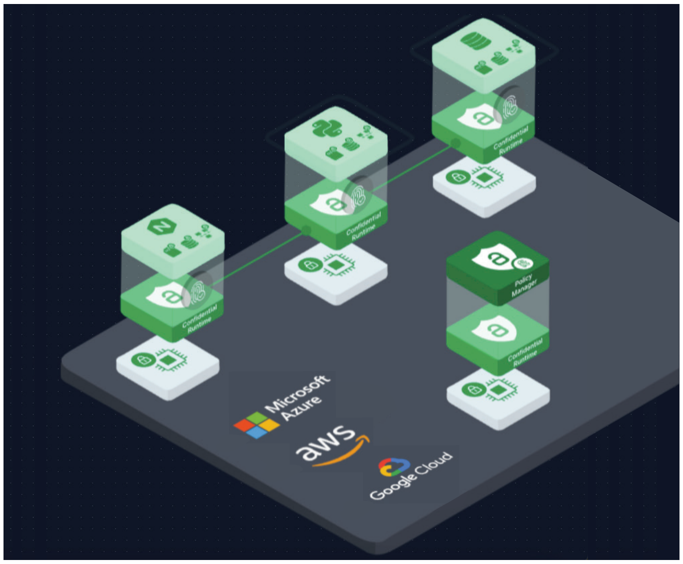
Anjuna Seaglass™

Universal Confidential Computing Platform

```
$ anjuna-[your-cloud]run [your-application]
```

Root Access to Compute: A Significant Risk

Many enterprises remain hesitant to move the majority of their workloads to the cloud due to concerns surrounding data security, privacy, and compliance. Traditional security tools fall short of addressing the risks that arise from the shared responsibility between you and your cloud provider in cloud computing. Those with **root access to the compute layer can extract code, data, and secrets from memory**, opening up opportunities for secondary attacks on encrypted data. It is crucial to find a solution that effectively bridges this **compute security gap.**



Anjuna Seaglass Secures the Cloud with Confidential Computing

Anjuna Seaglass is the first Universal Confidential Computing Platform to run any application in any major cloud with complete data security and privacy. It creates trusted execution environments where your data is protected in every state — in use, in transit and at rest — and your code is always verified for authenticity, safeguarding the chain of trust.

Anjuna Seaglass virtualizes modern Confidential Computing CPUs available on the leading clouds: AWS, Azure and Google Cloud. By abstracting away the complexity of the underlying infrastructure, Anjuna Seaglass enables you to run any application - traditional, containerized, or Kubernetes-managed - with a consistent operational model, without the need to rearchitect or refactor.

At a Glance

Anjuna Seaglass is the first Universal Confidential Computing Platform to run any application in any major cloud with complete data security and privacy. Seaglass isolates your workloads in a protected environment that intrinsically secures your data in every state -- in use, in transit, and at rest. It allows you to control application-level trust policies, ensuring that only trusted code can access sensitive data.

What You Can Achieve

- **Adopt AI safely** by reducing the risk of handling sensitive or regulated training data
- **Embrace the cloud with confidence** to benefit from its agility, elasticity, and at-scale economics.
- **Protect sensitive data and intellectual property** from unauthorized access from outsiders and insiders.
- **Simplify and ensure compliance** with security, privacy, and data sovereignty regulations.
- **Create new revenue streams** with inherently secure cloud services that customers can trust.
- **Enable secure collaboration** leveraging confidential Multi-Party Computation (MPC) clean rooms.

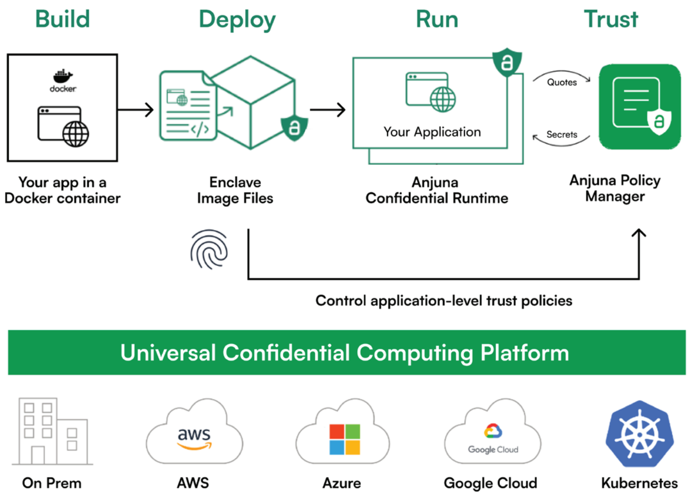
> “Anjuna provided the level of security we envisioned for our Parfin MPC Custody system. Now, we can ensure our customers’ distributed key shares are protected by an additional layer of secure enclaves that wasn’t possible without Anjuna.

ALEX BUELAU
CTO and Co-founder, Parfin

How It Works

Confidential Computing protects your data and code using a hardware-enforced root of trust called a trusted execution environment (TEE), also referred to as a secure enclave. The TEE is an isolated area within the CPU processor that is inherently protected against unauthorized access, regardless of privilege level, including those with root access to infrastructure and compute, such as insiders or cloud providers.

Anjuna Seaglass is a unified software solution that orchestrates, hardens, and simplifies the process of setting up a TEE and running your application inside it. This includes **building** the applications, **deploying** them to the cloud, **running** them in protected environments, and forging **trust** throughout the entire operation.



Build with no code changes

The platform creates **Anjuna Confidential Containers**, which are secure enclave-ready hardened images that leverage your original application without requiring any code changes.

Deploy with one command

Anjuna Confidential Containers can be deployed with a single command across clouds from multiple service providers and even on-premises environments, all without the hassle of building and integrating vendor-specific components.

Run with always-on encryption

Eliminate all types of eavesdropping and tampering threats by running your workloads inside the **Anjuna Confidential Runtime** with complete data protection - in-use, at-rest, and in-transit - with minimal performance overhead.

Trust with policy-based verification

Ensure trust through policy-based cryptographic attestation. **Anjuna Policy Manager** is an attestation-aware secrets store that manages policies and evaluates them to release secrets to verified apps/containers.

Key Differentiators

- Application-agnostic, no code changes needed
- Multi-server, multi-cloud deployment
- Data protection for all states: in use, at rest, in transit
- Secure, policy-based secrets distribution
- Minimal performance overhead

Supported Servers

- AMD SEV-SNP
- AWS Nitro Enclaves
- Intel SGX

Supported Clouds Services

- Amazon Web Services
    - Nitro Enclaves on EC2
    - Nitro Enclaves on EKS (Kubernetes)
    - Key Management Service (KMS)
- Microsoft Azure
    - Application Enclaves (Intel SGX)
    - Confidential VMs (AMD SEV-SNP)
    - Support for Azure Kubernetes Service (AKS)
- Google Cloud Platform
    - Confidential VMs (AMD SEV)

Anjuna Security evaluated the complete MITRE ATT&CK® matrix and discovered 77 attacks that are instantly shut down forever through Confidential Computing.

Get started with Anjuna Seaglass