Overview

The Public Cloud. Secured.

Harden Your Cloud Workloads

Every time an enterprise processes data in the cloud, that data is vulnerable to attack. Today, bad actors and malware simply bypass perimeter cloud security—taking direct and full advantage of "data in use" exposed by default in the memory of every cloud host.

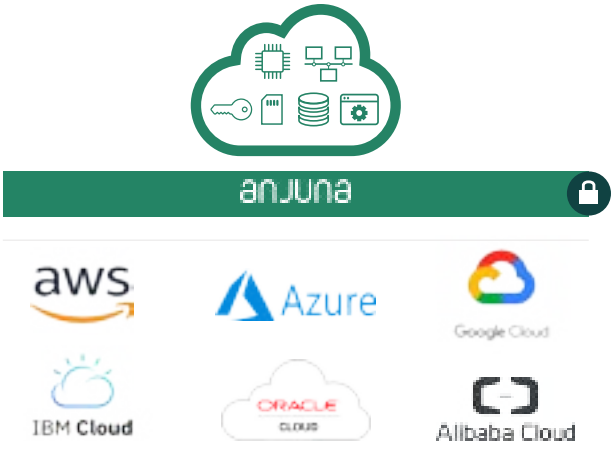
To counter these data security and privacy risks, AWS, Azure, Google, and others have deployed hardware-based Confidential Computing technology that effectively addresses these data-in-use attacks, establishing the strongest data protection available anywhere.

Unfortunately, the effort required for enterprises to take advantage of these confidential computing technologies is too difficult, cumbersome, and costly for virtually any IT organization.

Secure Data by Default. Everywhere. In Minutes.

Anjuna accelerates time-to-value (TTV) of Confidential Computing, enabling any enterprise to take full advantage of cloud economics AND establish the strongest possible data and computing security.

Now, even the most sensitive applications, data, and workloads can be instantly protected by a combination of strong hardware-grade encryption and memory isolation—placing data in a zero-trust data posture by default. This simple, powerful, and complete data security approach opens up a new era of computing with virtually no risk to data security.



Any application. Any cloud. Anywhere.

Anjuna Makes Confidential Cloud Computing Adoption Easy

The Anjuna® Confidential Computing software deploys transparently with no changes to applications and no disruption to IT operations. Anjuna software is implemented as part of public cloud infrastructure, working behind the scenes to keep all data—including data in use, data at rest, and data in motion—secured, everywhere. Anjuna is uniquely effective in securing cloud-native applications at scale—effortlessly protecting data and workloads across multi-cloud deployments.

Learn more at www.anjuna.io