anjuna®

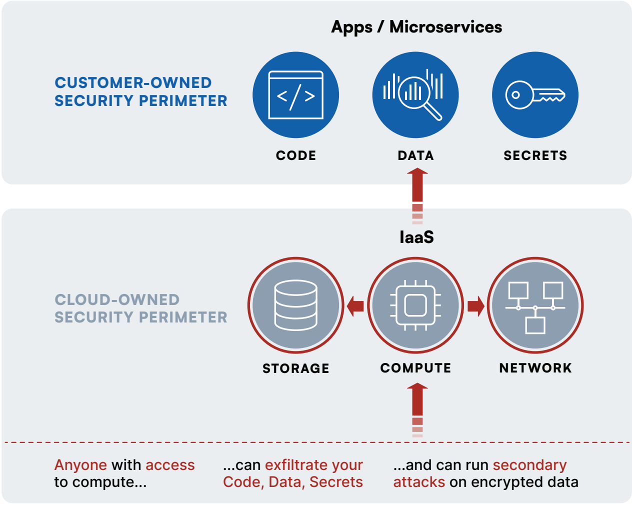
SOLUTION BRIEF

Confidential Computing for Government

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

Data Security and Privacy Concerns Hinder Cloud Adoption

Cloud computing continues to drive digital transformation, but the public sector remains hesitant due to longstanding concerns about data security, privacy, and sovereignty compliance. According to a survey conducted by Gartner, **64% of government organizations listed security and privacy concerns as a top challenge in moving to the cloud.** Decisions to delay cloud adoption result in higher costs, sustained operational complexity, slower pace of innovation, and missed opportunities for collaboration and data sharing.


Apps / Microservices
CUSTOMER-OWNED SECURITY PERIMETER
CODE
DATA
SECRETS
IaaS
CLOUD-OWNED SECURITY PERIMETER
STORAGE
COMPUTE
NETWORK
Anyone with access to compute...
...can exfiltrate your Code, Data, Secrets
...and can run secondary attacks on encrypted data

Root Access to Compute: A Significant Risk

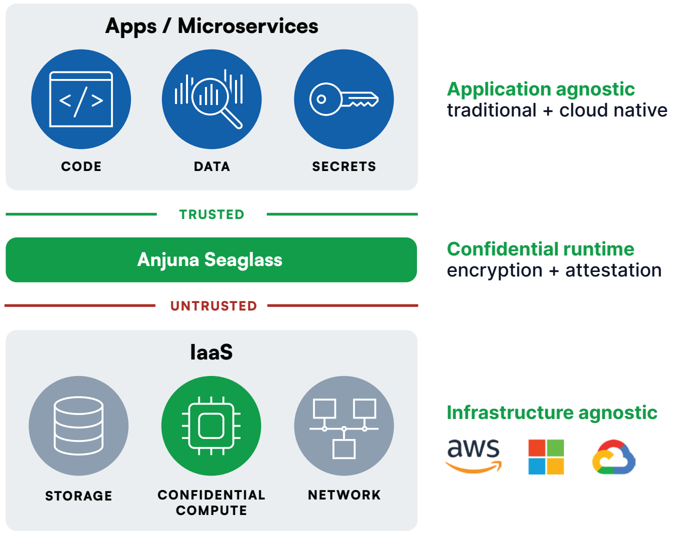
Security in cloud computing is a shared responsibility between the provider and the user. This model introduces fundamental risks that government agencies cite as critical obstacles to adopting cloud services. In cloud environments, **anyone with root access to the compute layer, be that a third party of an insider, can extract code, data, and secrets from memory**, opening up opportunities for secondary attacks on encrypted data. While traditional security tools are important, they are not sufficient to protect against the threat of opening up systems to third parties. Additionally, security vulnerabilities, both witting and unwitting, exist throughout the information operations lifecycle as evidenced by numerous security instances involving insider threats, espionage, and unauthorized disclosure highlight the importance of protecting sensitive data and operations at the classified and unclassified levels. It is crucial to find a solution that effectively bridges this compute security gap.

Anjuna Seaglass Secures the Cloud with Confidential Computing

Anjuna Seaglass offers an application-agnostic, multi-cloud software platform that creates “air-gapped like” Confidential Computing environments, ensuring **data is always isolated and protected**, including while in use, and **code is always verified for authenticity**, ensuring a **zero-trust model for application deployment.** Anjuna Seaglass enables agencies to secure traditional, cloud-native and Kubernetes-managed applications without rearchitecting or refactoring them. It provides government agencies a significantly enhanced security and privacy posture, mitigates the risk of data breaches and unauthorized disclosure, and improves public trust across the information enterprise.

Anjuna Seaglass Makes Confidential Computing Simple

Anjuna Seaglass is a unified software solution that orchestrates, hardens, and simplifies the process of setting up and running applications inside a **trusted execution environment (TEE),** also referred to as a **secure enclave.** This includes building the applications, deploying them to the cloud, running them in protected environments with fully encrypted memory, storage and networking, all while ensuring trust throughout the entire operation.



Anjuna Seaglass creates a barrier to prevent upward access, neutralizing risks

What Government Agencies Can Achieve with Anjuna Seaglass

Anjuna Seaglass can help government agencies **achieve mission success** by allowing them to:

- **Accelerate cloud adoption:** lift and shift highly sensitive or regulated workloads to reap the benefits of cloud economics, enabling more agile decision-making and faster response times to changing circumstances in contested environments.
- **Provide data-centric security:** lock down apps and classified information in specialty air-gapped clouds (C2S, C2E, etc) using hardware rooted zero-trust defense. This protects sensitive data from unauthorized access, theft, insider threats, and eliminates adversarial lateral movement across networks.
- **Collaborate and share data securely:** create confidential clean rooms using multi-party computation (MPC) to allow cross-agency (Allied Nations and Militaries) sharing of information and analytics without leaking private data to one another.
- **Simplify regulatory compliance:** meet regulatory compliance requirements related to data security, privacy and sovereignty. Avoid regulatory penalties and maintain public trust.
- **Promote public trust:** demonstrate commitment to data security and privacy to enhance public trust, and increase citizen engagement and participation.

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

REV-1123