Protect Your Data Even If You Are Breached

Datasheet

anjuna®

At-a-Glance

Anjuna® makes it easy to use a breakthrough technology in data security called Confidential Computing. Developed and embraced by the biggest names in tech, such as Intel, AMD, AWS, Azure, and GCP, Confidential Computing protects your data's privacy, enabling you to securely embrace the cloud. It also creates new opportunities to drive innovations and business growth that was not previously possible.

Benefits

- **Reduce your attack surface** and blast radius
- **Ensure privacy** of crucial data, IP, and algorithms
- **Meet compliance requirements** for protecting PII
- **Gain operational agility and cut costs** as you confidently migrate workloads to the cloud
- **Strengthen customer trust** and brand reputation by treating their data with care

> "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*

The transformative shifts to both cloud infrastructure and modern application architecture are challenging the ways we've traditionally protected data. We used to secure networks and servers but now offload infrastructure to cloud providers. We used to create self-contained apps but now build with microservices. The traditional security model struggles to contain modern risks and protect what matters most: your data.

What is Confidential Computing?

Chipmakers and cloud providers developed Confidential Computing, a type of Privacy-Enhancing Technology, to give organizations a greater sense of confidence in the security of their data, specifically data in use, which has long been vulnerable to exfiltration from memory. Confidential Computing uses "secure enclaves" - a protected part of the CPU and memory encrypted by hardware - to lock out prying eyes, including malware, insiders, and cloud providers. This paradigm decouples data security from infrastructure and keeps your data private even if your IT infrastructure gets breached.

What Does Anjuna Do?

Anjuna makes it easy to use the chipmakers' and cloud providers' secure enclaves, which are complex and require developers to refactor and recode applications without degrading speed and performance. Now, instead of all that engineering work, simply launch your app with Anjuna. It's a lift-and-shift approach. Anjuna creates an isolated environment within a secure enclave, runs your app in it, and keeps your data confidential. It takes mere minutes to set up, not years to develop.

What Makes Anjuna Unique?

LIFT & SHIFT

You don't want to refactor or recode your applications. Simply launch your app with Anjuna and get instant protection.

MULTI-PLATFORM AND MULTI-CLOUD SUPPORT

Now you can avoid vendor lock-in and have choice. Anjuna works on any cloud, multi-cloud, hosted, hybrid, and chip architecture.

NO PERFORMANCE IMPACT

Anjuna does not diminish the performance of your applications.

SCALE PROTECTION WITH COMPUTE

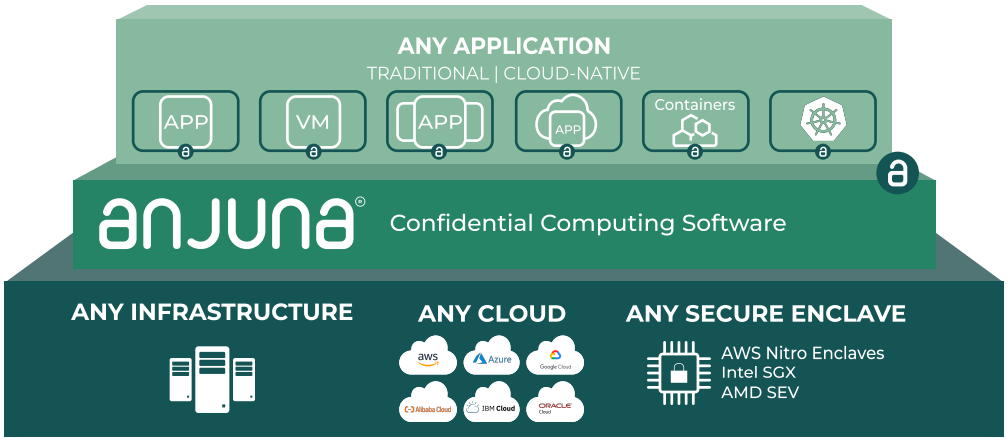
Your apps will grow and scale. Anjuna seamlessly extends protection horizontally as that happens.

FULL-STACK COVERAGE

You need data to stay private wherever it goes. Anjuna extends protection beyond memory to storage and networks with full-stack encryption.

How is Anjuna Deployed? What Can It Protect?

Anjuna provides Confidential Computing software, a single binary that can be run anywhere you desire - on any infrastructure including hosted data centers, any cloud, and any server chipset with secure enclave capabilities (e.g. Intel SGX, AMD SEV, and AWS Nitro Enclaves). Additionally, Anjuna works transparently with container infrastructure and orchestration systems, such as Kubernetes, to secure modern application architectures. This flexibility is unparalleled and gives you plenty of options as you embark on your Confidential Computing journey.



What are Common Use-cases?

Confidential Computing is exciting because it solves traditional security use-cases and unlocks new ones that can drive business growth. Common customer use-cases include, but are not limited to, the following:

- **Secure cloud migration** - You want to migrate workloads to the cloud to gain agility and cut costs, but also be secured
- **PII protection** - You must comply with regulations for protecting PII from breaches
- **Database protection** - You need to protect against breaches and prevent IT insiders from over-exposure for compliance reasons
- **IP protection** - You want to run proprietary algorithms in the cloud and safeguard IP from adversaries
- **Key security** - You need to secure your app's cryptographic keys and/or access to vaults
- **Vulnerability mitigation** - You want to reduce the blast radius of zero-day attacks
- **Multi-party computation**
  - You want to train AI/ML models but need to access datasets that were previously off limits
  - You want to collaborate with other parties, even competitors, to aggregate data without exposing it to draw inferences to fight a common problem (i.e. money laundering, financial fraud, rare diseases, etc.)

Customer Validation

Israel's Ministry of Defense (IMOD) put workloads into the public cloud for the first time with Anjuna. During the evaluation phase, IMOD's highly-skilled red team tested Anjuna's ability to secure against rogue or accidental insiders, third parties, criminal hackers, and nation-states and could not breach the protection.

Want to See a Demo?

People are amazed by how easy it is to protect an application with Confidential Computing using Anjuna. Let us prove it with a live demo: anjuna.io/demo

Visit us at www.anjuna.io