anjuna

Protect Sensitive Applications In Untrusted Environments.

Anyone with root access to a host or a VM can access all application data in runtime. Anjuna moves the software perimeter to be around applications and provides hardware-grade security for the applications, without requiring any changes.

THE RUNTIME APPLICATION RISK EXPLAINED

Many applications contain extremely sensitive information and are a single point of failure. Anyone with access to the infrastructure can gain access to all the sensitive data held by the application or tamper with the way the application is running.

This means that in many cases the organization cannot adopt new and agile environments like the public cloud or containers and is forced to use legacy environment or deployment methods.

The following situations create increased risk:

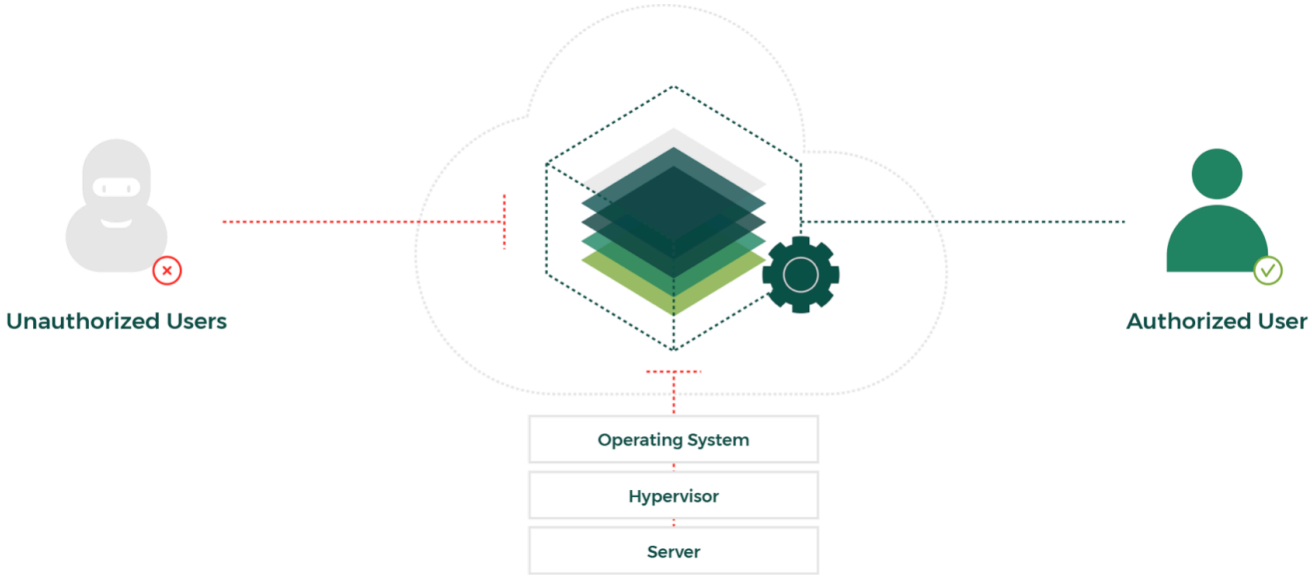
- **Multiple admins:** when organizations can't limit the number of people with root access to the machine running these applications
- **Limited security zones:** when these applications run alongside other applications that might have unknown vulnerabilities
- **Unhardened machines:** when the machines running these applications are not hardened and might contain a zero-day vulnerability in the operating system that will allow someone unauthorized to gain root access
- **Public or private cloud:** when the admins managing the machines running these applications and not part of the organization

ANJUNA USE CASES

Protecting the data in memory
The application itself and its data are protected from anyone, even if they have root access to the host, the VM, the container or the hypervisor.

Application identity and integrity assurance
Utilizing remote attestation to verify that the application itself and the data within it have not been tampered with.

Secure auto-unseal without requiring an HSM
Protecting the unseal token with HSM-grade security without requiring an HSM or any shared-secret stored on the machine. This helps solve the last-mile problem of initiating the auto-unseal process with a shared secret stored on a machine.



anjuna

KEY FUNCTIONS

Runtime Application Security

Provides in-memory encryption to secure secrets-management applications in runtime (data-in-use) to deliver security and integrity.

Memory Isolation

Completely isolates the memory used by an application from anything else on that machine including the operating system and the kernel. The data used in memory does not leave the CPU unencrypted. No one can access the memory, even with root or physical access to the host.

Remote Attestation

Establishes a secure trusted channel to the back-end server application and provides integrity and confidentiality. Attestation helps verify an application identity and helps verify that the expected code is running in a protected enclave.

BENEFITS

Security
Protects the master key and the secrets in any environment, regardless of who has root access.

Flexibility
Eliminates the need for rigid server security zones and minimizes reliance on HSMs. Also, removes the need to secure or patch the host, VM or container.

Simplicity
Requires no code changes, meshes with existing DevOps processes.

Agility
Allows adopting new environments and deployment methods without having to worry about the security of the infrastructure.

Performance
Allows secrets to be adjacent to applications to improve performance.

ANJUNA RUNTIME SECURITY

Protecting your sensitive applications is extremely important, but you want to be more agile and deploy application in modern environments and using modern deployment methods. This requires better security. Anjuna Runtime Security protects applications at runtime with a hardware-grade security perimeter, allowing any application to be deployed securely in any infrastructure, including public and remote clouds, and using any deployment method, like containers and serverless. Anjuna Runtime Security establishes the security boundary around the application without requiring modification to the application.

Anjuna's security envelope surrounding applications enables enterprises to deploy sensitive applications in untrusted environments and protect the application and its data even if someone has root or physical access to the host. While existing technologies protect data-at- rest and data-in-motion, Anjuna secures applications in runtime (data-in-use) leveraging modern CPU technology including Intel® SGX. Secured applications can be deployed in any environment and run alongside untrusted applications on the same host. Anjuna removes the need to harden the machine and secure or patch the host, VM or container. Anjuna is ideal for protecting sensitive data such as secrets-management applications and enables a secure auto-unseal process without requiring an HSM.

Anjuna Runtime Security requires no code changes or recompilation and integrates with existing DevOps automation processes.

ABOUT ANJUNA

Anjuna is in the business of protecting all of your applications in any infrastructure, so you don’t have to worry about the security of the infrastructure. We are a full-service data security company that is headquartered in Palo Alto, California.

Anjuna is backed by Y Combinator, DCVC, Playground Global, and Founder Collective.