anjuna®

Preventing Insider Threats

With Anjuna® Confidential Computing Software

Anjuna Security, Inc. **anjuna.io**

Preventing Insider Threats With Anjuna® Confidential Computing software

anjuna

Executive Summary

One of the biggest threats to enterprise IT security today is already inside your organization. Insiders with administrative credentials are more dangerous than end users because of the broad systems access they require to do their jobs. The list of insiders includes employees, contractors and third parties, as well as bad actors who present credentials that make them appear to be insiders.

Neutralizing insider threats and enabling unbreakable data security has been a vexing problem since the dawn of computing. Ideally, insiders would have total freedom to do their work, but with no ability to access, view, or alter sensitive data. This protection would be transparent to administrative users, allowing them to do their work unimpeded by security controls.

Today, encryption schemes can hide data from insiders. But they require decryption and other software to run applications. Other solutions that detect IT insider threats are complex to manage and maintain, and they fall far short of comprehensive protection.

This situation is about to change, with options that not only simplify data encryption but can change the focus from data loss **detection** to comprehensive **prevention**.

Secure enclave technology, now available from Intel, AMD, Microsoft Azure and Amazon AWS, leverages CPU hardware-level memory isolation and encryption features. These provide enterprises with ironclad data controls that protect data, applications, storage, and even network communications from inside— on site, in the cloud, or wherever workloads execute . Because they can operate at the chip level and deliver hardware-grade protection, secure enclaves are quickly becoming the ubiquitous standard for securing enterprise applications and data from insiders everywhere.

WHAT IS A SECURE ENCLAVE?

A secure enclave provides CPU hardware-level isolation and memory encryption on every server, by isolating application code and data from anyone with privileges, and encrypting its memory.

With additional software, secure enclaves enable the encryption of both storage and network data for simple full stack security. Secure enclave hardware support is built into all new CPUs from Intel and AMD.

But implementing secure enclaves can be both time-consuming and expensive. Virtually no software—including packaged and proprietary enterprise software applications—has been written to run directly within a secure enclaves. The effort required to rewrite applications puts the hardened protection of secure enclaves out of reach of most IT organizations.

Until now. Anjuna Confidential Computing software makes enclaves simple. Instead of re-coding applications, Anjuna enables “lift and shift” of existing packaged and proprietary software into secure enclaves—meaning applications and data securely are operating in enclaves in minutes. With Anjuna, enterprises can transform their vulnerable data and applications into fully protected resources, without requiring changes to applications or operations.

Prevention Not Detection

There will never be a foolproof way to be certain all threats to enterprise IT operations have been detected and mitigated in a timely manner. Moving from detection to **prevention** changes the focus from identifying and chasing malicious acts that have already occurred to preventing them in the rst place.

Secure Enclaves leverage security instruction sets, such as Intel's Software Guard Extensions (SGX) and AMD's Secure Encrypted Virtualization (SEV), that are built into modern CPUs. These segment, isolate, and encrypt computer resources away from all other applications, privileged users and even the host itself. Application code and data located in these "enclaves" are decrypted only by the CPU when needed, and are rendered useless to anyone, even in the event of a complete host compromise. Enclaves are now dramatically improving data security. SGX and SEV-enabled CPUs have been adopted by every major server and cloud platform.

The Con dential Computing Consortium, founded in 2019, is driving the adoption of con dential computing to protect data in use by performing computation in a hardware-based secure enclave, or Trusted Execution Environment (TEE). Secure instruction sets (and the second enclaves they enable) form the most direct, secure path to enabling an industry-standard solution.

For more information about secure enclaves, see the Anjuna white paper *Securing Enclaves: The Powerful Way to Prevent Insider Threats*.

The Tradeoff: Security vs. Productivity

Current cybersecurity practice is to focus on controlling network access by outsiders or end users, and to detect hacking and incursions as they occur. The problem with detection is that it's after the fact, costly, ineffective, and incomplete.

Infrastructure insiders—system administrators, network architects, system analysts, developers, and site reliability engineers—can easily misuse or abuse their level of access. Not only can they steal or damage sensitive data, they can cover their tracks by deleting detection logs or bypassing software security mechanisms, including security audits, which allows them to access data without being detected.

Software encryption schemes don't offer suf cient protection, because encryption keys are stored decrypted in memory, where insiders have easy access to them. Attackers can also exploit zero-day vulnerability to gain access to data and circumvent software defenses.

Maintaining security without impacting IT productivity has been a classic security challenge. Cloud-based computing only compounds the problem, since there is limited accountability and control over the personnel at IT cloud platform providers. What's needed is an approach that keeps data protected and businesses in control of their data and applications without constricting IT insiders from doing their jobs.

Adoption Has Been Limited by the Need to Recode Applications

Implementing secure enclaves can be a daunting challenge. Applications have to be signi cantly rewritten, and changes to IT processes are often needed. Each chip provider offers its own software developer kit (SDK), providing low-level tools that require considerable understanding of intricate design details, as well as knowledge of cryptography concepts.

Because existing applications were not designed to be used in conjunction with this technology, implementation requires signi cant design, development, and testing resources. SDKs change with every chip revision, and applications need to be rewritten on an ongoing basis to keep up with those changes. This is both complicated and costly.

Given this situation, most enterprises won't realistically have the resources and expertise to take advantage of the full potential of secure enclaves.

Taking Secure Enclaves to the Enterprise Level - With No Recoding

To be ready for large-scale deployment within an enterprise, secure enclaves must meet several criteria.

First, adopting enclaves must be simple and straightforward. There should be no need to either rewrite applications or reengineer IT processes. That means having a path to implementation that does not rely on ever-changing SDKs from individual hardware suppliers.

Protecting data at-rest is extremely important, but not suf cient. Today's applications are highly distributed and elastic. They may run across multiple systems or virtual machines. Storage and networks must be protected as well, and this protection should extend beyond on-premises systems to both public and private clouds.

The solution should offer cross-platform support for all hardware enclaves, rather than be limited to one or two chip suppliers. And it should include support for such critical enterprise functions as disaster recovery, high availability, and data sharing between applications running on different machines, as well as the ability to easily upgrade the application and the hardware when necessary.

Anjuna Makes Enclaves Simple and Enterprise-Ready

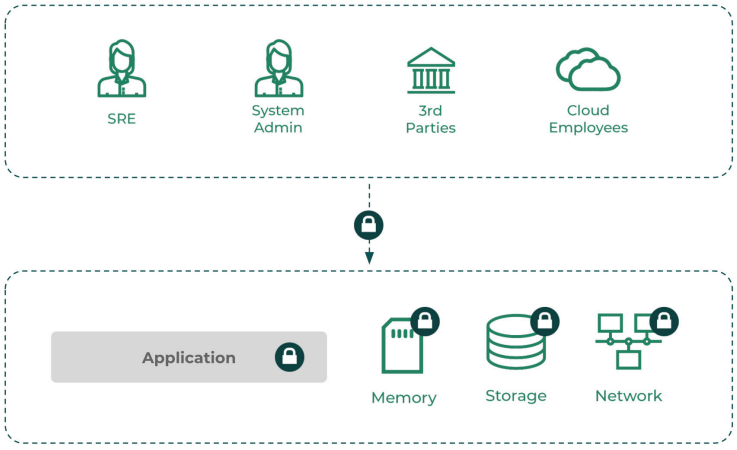
Anjuna meets these criteria to take enclaves to the enterprise Level by supporting ve main requirements for enclaves in the enterprise:

Adoption should be simple and straightforward.

Anjuna Confidential Computing software enables enterprises to "lift and shift" applications and data to secure enclaves quickly and easily in minutes. There is no rewriting of applications, no recompilation, no change to operating processes, and no need for training the IT team. Within seconds, Anjuna automatically creates an isolated and ironclad hardware-encrypted Anjuna enclave in which applications run. All types of applications, including proprietary or legacy programs, run unmodi ed within the enclave. Even privileged users on the guest operating system, hypervisor, or the host operating system cannot access the data or applications.

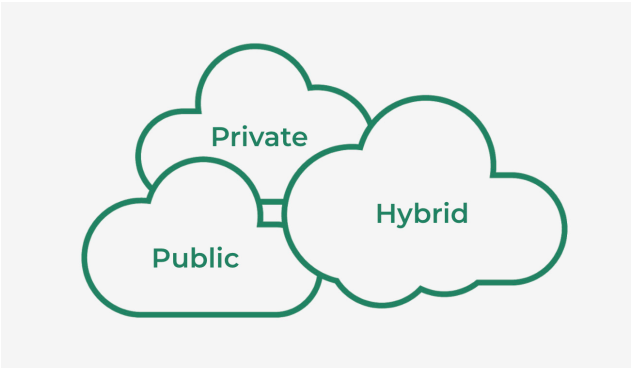
Full Stack Coverage

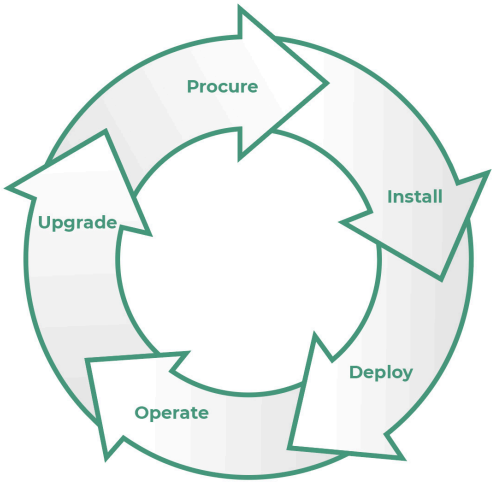
Anjuna software extends enclave protections beyond memory to automatically protect storage and networks with full stack encryption. The full stack is secured—both hardware and software. Data is isolated and completely inaccessible to any other entities while running an application, while memory is completely isolated from anything else on the machine, including the operating system. Neither root nor physical system access enables data access. The host will simply and automatically encrypt data written to storage—with no changes to applications or operations. Anjuna ensures TLS connections are terminated in trusted secure enclaves at both ends of the connection—securing the network from full stack.



Attestation

Anjuna uses attestation to develop a hardware root of trust by authenticating the hardware inside which the secure enclave is running as genuine, and attesting to the integrity of enclave memory to a remote party. This allows secure enclaves to protect applications, data, and storage—locally, across the network, and in the cloud—simply and effectively.





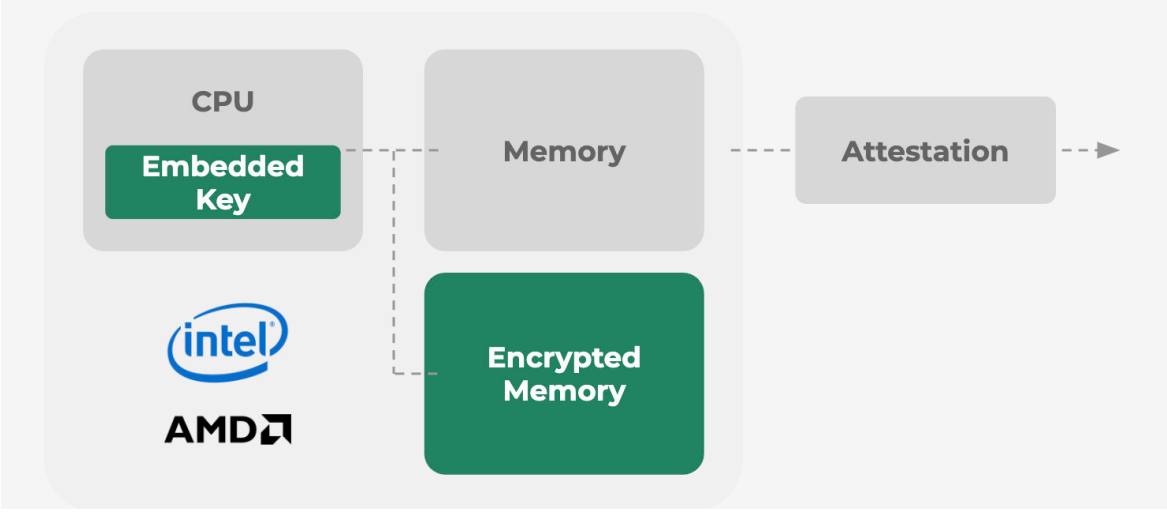
Enterprise-Ready

Enterprises also need to ensure enclaves work within their environments and with established processes. They need to support high availability and disaster recovery scenarios, to scale in the cloud, to access les and applications running on different machines, and to easily upgrade the application, firmware, and hardware. Anjuna Confidential Computing software offers options to protect security and business continuity in these scenarios by integrating with existing key management solutions.

Multi-Platform and Multi-Cloud Support

Enterprises can't afford to be locked into one hardware platform or cloud. Anjuna supports Intel and AMD platforms today and will shortly add support for Amazon Nitro Enclaves.

In addition, Anjuna Confiential Computing software runs on Microsoft's Azure Confidential Computing, with Azure Kubernetes Services (AKS), and integrated with Azure Key-Vault. Workloads can be executed across any enclave platform without modification. This provides the flexibility to secure data—no matter what server or cloud on which they are running.



A Single Solution for All Environments

Until now, an enterprise was never completely secure. Existing solutions are expensive and dif cult to deploy. Some required computationally intensive software hardware and software add-ons. Only limited applications were protected because of complexity and cost. Separate solutions were required for networks, data at rest, and data in use.

Anjuna Confidential Computing software enables applications to be securely deployed anywhere enclave-based hardware is supported. This includes all clouds—private, public, and hybrid—as well as containers, virtual machines, and bare-metal servers. Enterprises are never locked into a given technology. Anjuna allows enterprises to execute anywhere—on premises or in the cloud—and still maintain secure control. In addition to Intel® and AMD, Anjuna Confidential Computing software will run under AWS Nitro Enclaves, introduced by Amazon in December 2019 and expected to be generally available in 2020.

Anjuna protects high value applications, such as secrets management, service mesh and web services, databases, and machine learning applications. Anjuna Confidential Computing software also helps enterprises more effectively manage and mitigate high exposure situations. This includes high-risk geographies (where there is significant potential for bad state actors), geographies where it's not possible to monitor employees due to privacy concerns (such as the European Union), and areas of high data concentration.

ANJUNA USE CASES

Confidential Computing can be used to protect enterprise data and applications in many ways, including:

Databases

- Protect in-memory databases without losing speed or functionality
- Extend protection to data at rest with the same solution
- Maintain performance with minimal latency impact

Machine Learning Algorithms

- Protect high-value algorithms stored in memory
- Secure the algorithms and data at rest or on the network
- Protect nancial trading applications and other sensitive intellectual property (IP) from prying eyes

Application-to-Application Communications

- Validate applications with secure enclave keys
- Restrict communications to only speci ed applications
- Ensure applications run on the expected target server

Secret/Key Management Applications

- Secure both data and applications within secrets management platforms
- Protect encryption keys, tokens, and passwords while data is in use
- Solve the secret-zero problem

Sensitive Information Repositories and Applications

- Safeguard personally identi able information (PII)
- Protect private keys, such as those used with Transport Layer Security (TLS), against bad actors

Simple and Secure Enclaves Are the Future

Secure enclaves are well on the way to becoming standard practice in enterprise security, just as TLS (including https) and levault have become integrated into today's IT environments. More than 20 industry leaders have come together to form the Con dential Computing Consortium to advance the adoption of secure enclaves in trusted execution environments (TEEs).

By the end of 2020, secure enclaves will be supported by nearly every server and cloud platform, including Intel, AMD, Amazon AWS (with the new Nitro Enclaves), Microsoft Azure, VMware, Google, Docker, Red Hat, and others

Over time, enterprises will utilize secure enclaves to protect all of their assets. Why take the risk of running an insecure application or network, when a much more secure alternative is available that can be implemented simply and cost effectively?

Preparing for Secure Enclave Adoption

IT teams will not want to take the risk of rolling out new technologies across an entire enterprise simultaneously. That's why enterprises are now creating pilot programs that will test the viability of secure enclaves with a few critical applications, before moving to larger scale deployments.

Given that secure enclaves are becoming the industry standard, it makes good business sense to start exploring implementation strategies now. Anjuna can be your partner in deploying secure enclave protection quickly and simply without impacting the productivity of your team.

CONFIDENTIAL COMPUTING

The Con dential Computing Consortium was founded in 2019, under the auspices of the Linux Foundation to de ne and promote the adoption of con dential computing—the protection of data in use by performing computation in a hardware-based secure enclave, or Trusted Execution Environment (TEE).

More than 20 industry leaders have joined the group, including Alibaba, Anjuna, ARM, Baidu, Facebook, Google Cloud, IBM, Intel, Microsoft, Oracle, Red Hat, Tencent, and VMware.

About Anjuna

Anjuna makes hardware-grade application and data protection simple, fast, and enterprise-ready, enabling IT to "lift and shift" applications and data into the hardware-encrypted con nes of a secure enclave. Available from every major chip, cloud, and system vendor, secure enclaves are the data security gold standard. In minutes, Anjuna enables enterprises to protect memory, storage, networks, and clouds from malicious software, insiders, and bad actors—without recoding. Anjuna is based in Palo Alto, California.

anjuna.io | info@anjuna.io | 650-501-0240

AS01-0520