anjuna

Secure Enclaves:

The Powerful Way to Prevent Insider Threats

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

Secure Enclaves:
The Powerful Way to Prevent Insider Threats

anjuna

Executive Summary

A major threat to enterprise IT already exists inside your organization: insiders. While most enterprises already take steps to protect systems from end users, credentialed insiders with unfettered access are even more dangerous, and this is not limited to employees. Third parties, including employees at cloud providers, are often to blame for insider breaches. Nation-states and other bad actors, can also present credentials that make them look like insiders.

Current methods and technologies to prevent IT insider threats have had severe limitations. Now there's a new approach being implemented by nearly every major hardware and cloud vendor. Secure enclaves provide a comprehensive, more secure solution that protects data, applications, and storage from insiders and third parties—on premises, and in both private and public clouds.

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 Enterprise Enclaves 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.

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.

Insiders: The Threat No One Wants to Talk About

Until now, most cybersecurity efforts have focused on controlling network access by outsiders or end users. The greatest harm, however, is likely to come from insiders—system administrators, network architects, system analysts, developers, and site reliability engineers—who often have authorized access to data, networks, and applications. They may misuse or abuse their access to steal or damage sensitive data. Breaches may also occur unintentionally due to lax security protocols. It's estimated that 43% of all breaches are committed by insiders—both accidental and intentional.[1]

In 2019, two Twitter employees were charged with spying for Saudi Arabia by accessing information on Saudi Arabian dissidents who used the Twitter platform.[2] Even when organizations secure their own systems internally, the threat of intrusion through third parties remains. The more third parties that may access your IT data and networks, the higher the risk of a breach. One of the more publicized early breaches involved the hack of Target's point of sale systems using the login of an approved HVAC supplier, resulting in stolen data of 40 million debit and credit cards.

Bad actors present credentials that make them appear to be insiders. Marriott revealed unauthorized hacking had exposed the personal information of 383 million guests—and that the hacking had occurred undetected for nearly five years. The company blamed foreign hackers for the breach.

In high-risk geographies, government agencies may cross the line as well. Hostile state actors may be using hardware attacks that can't be detected until the stolen information is used months or years later.

The move to cloud-based computing only compounds the problem, since there is limited accountability and control over the personnel at IT cloud platform providers who are able to access your files. A data breach at Capital One in early 2019 exposed the personal data of over 100 million bank customers and applicants—including social security numbers, credit scores, dates of birth, and linked bank account numbers. The perpetrator was a former employee of Amazon Web Services (AWS), who boasted online about what she'd done.

The costs of these threats are enormous. In addition to direct financial losses in the millions of dollars and a negative impact on the stock price, disclosure of trade secrets may have long-term implications. Business reputation take a hit as customers lose confidence in the company's ability to safeguard personal information. There may be fines for noncompliance with privacy regulations, such as GDPR in Europe or the California Consumer Privacy Act (CCPA), or significant regulatory implications in some industries. Marriott was hit with a $123 million GDPR fine. The fine against British Airways for exposing payment and personal information of 500,000 customers was even worse: $230 million.

Current Efforts Don't Work

With all the attention and money spent on cybersecurity, why is this still such a serious problem?

Until now, cybersecurity solutions have focused on **detecting** hacking and incursions. While detection technologies continue to improve, the problem is detection is after the fact. Breaches may not be revealed until months or years later (as was the case with Marriott, where the incursion went on undetected for years). By then, damage may very well have already occurred.

Detection is usually incomplete. Attackers can still exploit zero-day vulnerability to gain access and circumvent software defenses. Infrastructure insiders have such an elevated level of access they can delete detection logs and bypass any software security mechanism. System administrators or programs with access to host memory can delete logs, circumvent security audits, and access data at rest (which appears to have been the case in the Capital One attack).

Encryption of data at rest is not the answer either. Applications and data still must be decrypted for runtime processing. Furthermore, IT insiders have access to encryption keys; smart system administrators can delete audit logs. Inadequate security within containers or virtual machines results in additional risk.

What's needed is an approach that makes security automatic without constricting IT insiders from adequately doing their jobs. There should be a way to enable secure productivity by segregating IT duties from access to enterprise data and networks.

Recent Options Aren't Enterprise-Ready

A number of new options have become available over the last few years from protection vendors. Most of these are point solutions—they are neither end-to-end or ready to be deployed enterprise-wide. Encrypting data and programs is fragmented and complicated. As a result, these offerings are often complex to implement or require significant disruption to normal IT operations.

There's another important limitation. Point products only protect data at rest or on the network—not data in use. Running applications in memory exposes data, master keys, encryption keys, and other secrets in plain text. Privileged Access Management (PAM) only protects credentials. Anyone who has authorized credentials can still see data and applications.

All of these options reduce productivity by requiring additional unnecessary layers of software complexity. The challenge is how to balance security and privacy with usability and ease of implementation.

Prevention Not Detection

In today's environment, enterprises can never be sure all threats have been detected and handled in a timely manner. Moving to **prevention** changes the focus from chasing malicious acts that have already occurred to maintaining secure resources and networks.

To ensure enterprise security, protecting data and applications is not sufficient. Memory and networks need to be protected as well. This protection should include not only on-premises applications and data, but also operations that run in both private and public clouds. While today's approaches protect data at rest and in transit, data in use has not been properly addressed, because it is the most complicated and difficult state to protect.

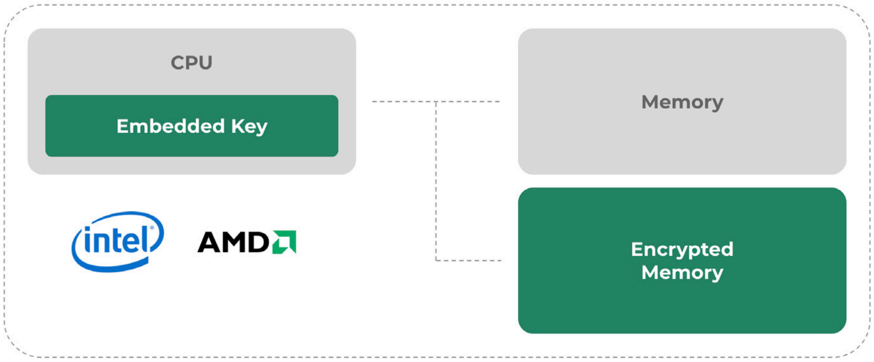
> "Organizations are now investing in tools that are more sensitive and are focusing on a balance between response and detection versus prevention."[3]
>
> Gartner

The Confidential Computing Consortium was founded in 2019, under the auspices of The Linux Foundation, to address this problem. The consortium's goal is to define and promote the adoption of **confidential computing**—specifically to protect sensitive data within system memory. 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.[4]

Secure Enclaves Deliver High-Level Hardware Security

Secure enclaves (also known as Trusted Execution Environments or TEE) are at the core of confidential computing. Secure Enclaves are sets of security-related instruction codes built into new CPUs. They protect data in use, because the enclave is decrypted on the fly only within the CPU, and then only for code and data running within the enclave itself.

Introduced by Intel as Software Guard Extensions (SGX)[5], secure enclaves are based on hardware-level encrypted memory isolation. AMD now offers similar functionality with its SEV technology, built into Epyc. By the end of 2020, secure enclaves will be supported by nearly every server and cloud platform, including Intel, AMD, Amazon AWS (with their new Nitro Enclaves)[6], Microsoft Azure[7], VMware, Google, Docker, and Red Hat[8].



In a secure enclave, applications run in an environment that is isolated from the host. Memory is completely isolated from anything else on the machine, including the operating system. Private keys are hard-coded at the hardware level. A process called attestation allows enclaves to authenticate the hardware inside which they run as genuine, and to attest to the integrity of enclave memory to a remote party. Secure enclaves protect applications, data, and storage—locally, across the network, and in the cloud—simply and effectively.

Application code and data are completely inaccessible to any other entities while running inside a secure enclave. Insiders with root or physical access to the system do not have access to memory. Even privileged users on the guest operating system, hypervisor, or the host operating system are blocked. Consolidating the security stack reduces complexity, which results in lower costs.

A New Level of Enterprise Security

Secure enclaves offer a significantly higher level of security for enterprise IT operations. With secure enclaves, IT insiders are blocked from taking malicious actions—but still able to do their jobs. The process is totally transparent to the IT user.

With secure enclaves, enterprises are also protected against Zero-Day exploits. Currently, "known unknowns" allow attackers to penetrate the operating system as a client task is executed. Applications running inside a secure enclave, however, are isolated even from the host operating system on any level of permission—even if the operating system, hypervisor, or container software are compromised. This allows true data separation and segregation.

The more third parties that have access to data and systems, the higher the risk. Privately hosted clouds and data centers open the possibility for malicious insiders to copy sensitive data or steal drives. In the cloud, sensitive data is not protected when used by cloud-based software applications. Secure enclaves solve these critical operational concerns without the need for rigid security zones that would result in overprovisioned or underutilized server infrastructure. Optimizing server utilization helps lower both infrastructure and operational costs.

Equinix, a leading datacenter company, says the rise in cybersecurity threats is a key issue impacting the digital information infrastructure. In 2020, Equinix predicts that "new data processing capabilities such as multiparty secure computation, fully homomorphic encryption (operating on encrypted data) and secure enclaves (where even cloud operators cannot peer into the code being executed by a cloud consumer) will move toward mainstream and will allow enterprises to run their computation in a secure manner."[9]

Secure Enclaves Prevent Critical Threats

As a CISO, you face multiple threats to your enterprise–from stolen data to unauthorized access by systems administrators or SREs. Secure Enclaves can help you prevent a wide range of threats with a consolidated easily implemented approach.

#	Risk	Hardware Disk-level Encryption	Software Disk-level Encryption	File-level Encryption	Client-side Encryption	Secure Enclaves
1	Data protected when disk is stolen	Yes	Yes	Yes	Yes	Yes
2	Data protected from unauthorized cloud provider admins with valid credentials	No	No	Yes	Yes	Yes
3	Data protected from unauthorized system admins or SREs with valid sysadmin credentials	No	No	Yes	Yes	Yes
4	Data protected from unauthorized database admins via valid file level access	No	No	Yes	Yes	Yes
5	Data protected from unauthorized applications (via APIs)	No	No	No	No	Yes
6	Data and encryption keys are protected in-use	No	No	No	No	Yes
	Implementation Effort	Low	Low	Medium	High	Low
	Examples	Self-encrypting drive	Bitlocker, Cloudlink, LUKS	Vormetric, SafeNet ProtectFile	SDK, custom application encryption	Anjuna
	Notes				All server-side functionality is lost	

Obstacles to Adoption

Until now, implementing secure enclaves was complex and costly. Applications had to be significantly rewritten to work with a secure enclave, and changes to IT processes were often needed. Furthermore, each chip provider has their own software developer kit (SDK). This means implementation requires significant design, development, and testing resources, which makes the process expensive and time consuming.

There are several open source alternatives in this space, including offerings from Asylo, Open Enclaves, and Intel's SGX. However, these also require recompilation of each application and the use of an SDK. Additionally, these offerings do not currently provide either the support or deployment features required at the enterprise level, such as disaster recovery, high-availability, and scaling in cloud environments.

There are new solutions that address these issues—eliminating the need for software rewrites or implementing new processes. See the Anjuna White Paper: Preventing Insider Threats for more detailed information.

Next Steps: Prepare Now

The move to secure enclaves is gaining momentum. Secure enclaves will become standard security technology for the enterprise within the next few years. With the increased use of multiple computing environments—from on premises datacenters to public cloud to edge—now is the time to prepare to implement this level of protection for your operation.

ASK YOUR TEAM THESE QUESTIONS:

- Does your current hardware include Intel SGX or AMD SEV chips? Are there plans for deploying machines with this functionality in the future?
- How do you protect your applications and data in places like China?
- Are you concerned with the possibility a government subpoena might demand access to customer data?
- Do you completely trust all your SREs and system admins?
- How do you protect your sensitive applications in the public cloud?
- What are your cloud providers doing to address this ongoing insider threat?
- Are you developing plans to use AWS Nitro?
- Are you prepared to re-write applications to take advantage of secure enclaves?
- How important will it be to have a solution that can automatically move applications into a secure environment?

To learn more about how Anjuna makes the deployment of secure enclaves simple and straightforward without the need to rewrite software, see the white paper *Preventing Insider Threat*.

REFERENCES

[1] https://www.infosecurity-magazine.com/news/insider-threats-reponsible-for-43/

[2] https://www.washingtonpost.com/national-security/former-twitter-employees-charged-with-spying-for-saudi-arabia-by-digging-into-the-accounts-of-kingdom-critics/2019/11/06/2e9593da-00a0-11ea-8bab-0fc209e065a8_story.html

[3] https://www.gartner.com/smarterwithgartner/gartner-top-7-security-and-risk-trends-for-2019/

[4] https://confidentialcomputing.io

[5] https://software.intel.com/en-us/sgx

[6] https://aws.amazon.com/ec2/nitro/

[7] https://azure.microsoft.com/en-us/solutions/confidential-compute/

[8] https://www.ibm.com/cloud/blog/data-use-protection-ibm-cloud-using-intel-sgx?mhsrc=ibmsearch_a&mhq=secure%20enclaves

[9] https://www.equinix.com/newsroom/press-releases/pr/123853/Top--Technology-Trends-to-Impact-the-Digital-Infrastructure-Landscape-in-/

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 confines 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**

AS02-0520