Four Steps to Securing the AWS Cloud

The Case for Confidential Clouds

For CISOs, cloud computing has been eyed with concern for security. Up until now, keeping data secure meant keeping your data in your own datacenter. Computing in the public cloud meant loss of control and added compliance complexity.

That's changed.

Now, using a simple to deploy security approach called the Confidential Cloud, your applications and data can be measurably more secure on Amazon Web Services (AWS) than in your private datacenter. In fact, a Confidential Cloud may arguably be the safest place to compute anywhere.

What is a Confidential Cloud? It's a secure computing environment completely private to its owners, formed over one or more public cloud providers. A Confidential Cloud leverages and extends powerful hardware-grade secure computing capabilities, such as AWS Nitro Enclaves. Together with other technologies, this establishes an invisible, exclusive, and contiguous perimeter around data—regardless of whether it is stored, transmitted, or processed. Even better, a Confidential Cloud implementation is invisible to applications, people, and processes. This dramatically upgrades data security simply and automatically.

Applications, data, and workloads within a Confidential Cloud are physically or cryptographically isolated from all users, administrators, and computing processes—both on a specific host and across the entire collective public cloud. The Confidential Cloud creates a private cloud computing infrastructure so isolated and so secure that even the most sensitive workloads can operate in hostile public computing environments with complete privacy, utilizing the strongest protection available anywhere, automatically, and by default.

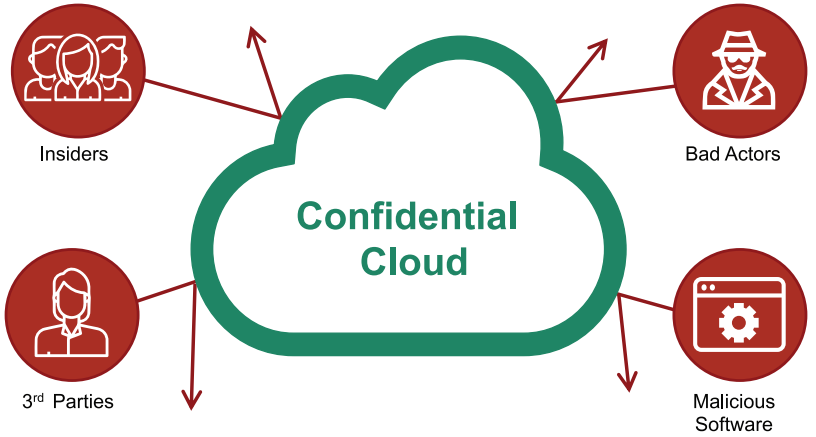

Figure 1: The Confidential Cloud protects data and applications from entire classes of threats by default

There are many ways to create Confidential Cloud computing environments the hard way. But there's no need to do that!

Here, we'll show you how to how to run your applications within your own Confidential Cloud quickly and easily using AWS Nitro Enclaves. With our guidance, you can deploy Confidential Clouds and applications with little technical effort, using a simple recipe for success based on the well-trodden path of experienced IT and security professionals. A little reading here will save you many headaches later. Even better, the simplicity and power of the Confidential Cloud will make you and your security team into IT superheroes.

Let's talk about why.

Risk vs. Business Opportunity – What's the Answer?

Many businesses are driving hard to use cloud computing—and for good reason. Using AWS provides cost, scalability, ubiquity, and ease-of-consumption benefits unrivaled by on-premises hardware. Cloud-enabled organizations gain cost and agility advantages that can give them an unfair competitive advantage.

Here's the problem: As attractive as the public cloud might be, it also increases cyber risk. Cloud data and workloads are exposed to insiders, third parties, bad actors, and malicious software, even your own IT operations team—all of whom have no reason to be exposed to this at all. This exposure changes unpredictably over time—especially as employees, third parties, threats, and the cloud itself evolve. With enough time and effort, data loss is an eventuality. For this reason, few organizations have moved their entire IT infrastructure—including their most sensitive applications and data—to the public cloud. Some of those that have done so have paid dearly for it.

Let's dig a little deeper as to why the public cloud can create risk. Consider your organization's data—wherever it's used, stored, or networked. All data is vulnerable by nature. You might have layers of firewalls, IPS/IDS, data leak protection, encryption, and other security offerings protecting your data. But underneath all those layers of protection, data remains exposed and accessible to malicious software, insiders, and bad actors. This is because data isn't self-securing. It remains easily accessible—especially as it sits exposed in host memory awaiting use.

This exposure is the heart of the problem. From a compliance standpoint, anyone or any application with access to a host must be considered to have exposure to data on that host, whether or not they have malicious intent. From a pure security threat standpoint, access to a host, and thus to unencrypted data in memory, is the first step in undermining all data security layers and the gold mine of valuable data. Compromising the host practically guarantees access to all the data stored on that host.

Figure 2: Layers of overlapping security products leave gaps for hackers to take unprotected data

This is why over 95% of security professionals resist cloud migration efforts.[1] But when the choice comes down to security versus business opportunity, security often loses. The enterprise usually choses to accept the risk—until it's too late. Meanwhile, we cross our fingers and hope that the next breach won't have our name on it. As most security professionals know, hope is not a sustainable cybersecurity strategy.

Figure 3: Businesses too often accept more risk to seize opportunity

[1] anjuna.io/451report

The Solution: AWS Nitro and Nitro Enclaves

AWS has recognized the need to close this gap. Their goal was to not just make the cloud safe enough for all applications, but also to give IT organizations complete responsibility and control of their data—rather than sharing this responsibility with their cloud provider.

And that's what AWS delivered. In 2017, AWS deployed the **Nitro System**, consisting of Nitro peripheral cards built upon a Nitro security chip and running Nitro hypervisor software.[2] It's the Nitro System that enhances AWS instances with "a locked down security model [that] prohibits all administrative access, including those of Amazon employees, eliminating the possibility of human error and tampering."[3] With Nitro, AWS has guaranteed that AWS employees don't have access to your data if it's stored or running on the Nitro hardware—ending data overexposure at the cloud provider level.

To make the Nitro System more secure, AWS then created **AWS Nitro Enclaves**, a physically isolated compute-only environment (without storage or networking), which operates within the Nitro System. Data and applications within a Nitro Enclave have virtually no attack surface: They can't be accessed locally or remotely, nor can there be storage or networking to or from the enclave. According to David Brown, AWS Vice-President of EC2, "Nitro enclave provides a means of protecting particularly sensitive elements of customer code and data not just from AWS operators but also from the customer's own operators and other software."[4]

[2]https://aws.amazon.com/blogs/hpc/bare-metal-performance-with-the-aws-nitro-system/
[3]https://aws.amazon.com/ec2/nitro/
[4]https://aws.amazon.com/blogs/security/confidential-computing-an-aws-perspective/

Thus, the combination of Nitro and Nitro Enclaves can provide hardware-grade data protection and isolation from AWS insiders, enterprise insiders, bad actors and malicious software—by default.

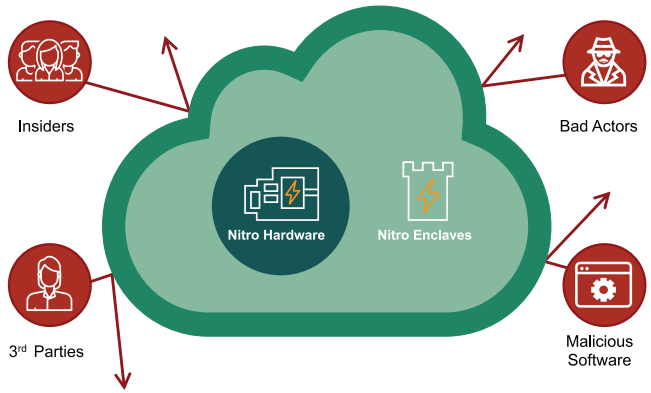

Figure 4: Nitro Hardware and Nitro Enclaves protect against all classes of insiders

AWS does not charge extra for EC2 instances with Nitro or Nitro Enclave capability. This makes adoption a seemingly "no-brainer" for customers and a winner for AWS: They no longer share security and compliance responsibility for customer data applications they can't possibly touch.

Free, secure, and powerful computing. Sounds amazing, doesn't it? Well, there's a small catch.

Unfortunately, packaged and existing applications can't run within a Nitro Enclave environment without substantial development and change to operations and processes. That's because even simple applications often require some form of storage or networking, which is not supported in Nitro Enclaves by design. To practically create, validate, instantiate, manage, and terminate secure enclave environments requires important management capabilities and other integrated services. The effort to build out these capabilities takes expertise and time most organizations don't have. That keeps these powerful data security capabilities out of reach.

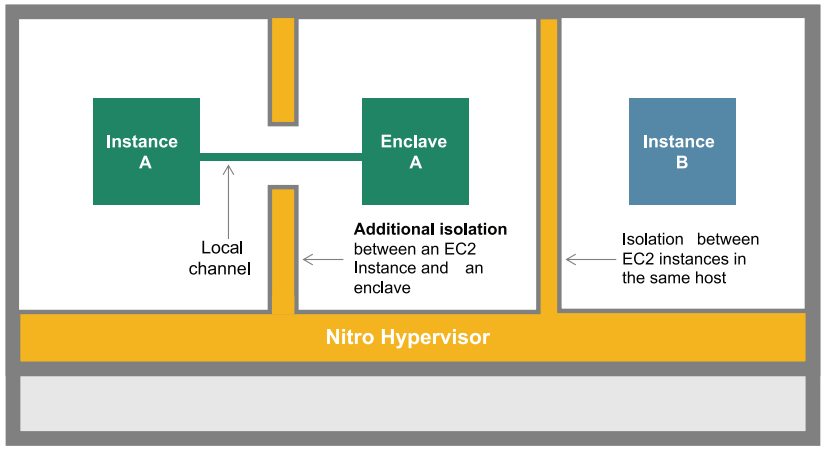

Figure 5: AWS Nitro Enclaves create isolated compute environments to further protect and securely process highly sensitive data within EC2 instances. Nitro Enclaves use the same Nitro Hypervisor technology that provides CPU and memory isolation for EC2 instances.

Simple Implementation of Secure Computing

Fortunately, software vendors such as Anjuna Security have done the hard work already, enabling enterprise IT organizations to easily operate virtually any applications within a Confidential Cloud and Nitro Enclave with virtually no effort. Applications, data, and workloads are not just isolated within a specific host but from the entire collective public cloud. This creates a private cloud computing infrastructure so isolated and so secure that even the most sensitive workloads can operate in hostile public computing environments with complete privacy and the strongest protection available anywhere.

How You Win With the Confidential Cloud

What does this mean to enterprise IT organizations like yours?

- The cloud becomes the most secure place for your organization to compute—demonstrably more secure than other alternatives, even private data centers and hardware.
- Hardware-grade security protects all your applications by default.
- Your IT organization can easily migrate workloads and effectively eliminate data exposure to insiders, bad actors, and malicious software.
- Your existing workloads are protected without costly software rewrites.

As a result, you'll see substantial cost savings and your security posture will be dramatically improved. Compliance and risk modeling efforts will be simplified and data breaches will become virtually impossible.

In short, with the Confidential Cloud, you'll become an IT superhero—able to leap over impossible security goals in a single bound (and at very low cost, too!).

Addressing Your Existing Enterprise Initiatives

Your enterprise likely has a number of IT initiatives already in place. Aligning with these funded company initiatives is key to any security project's success. Enterprises IT groups use Confidential Cloud capabilities to implement and support key initiatives that include:

- **Digital Transformation:** CIOs want the economic benefits of the cloud without making security compromises. The Confidential Cloud makes the public cloud the safest place to compute—even safer than on-premises data centers.

- **Insider Risk:** By eliminating IT insider access, the Confidential Cloud wipes out misuse, data exfiltration, and account or host compromises. With data effectively isolated, the threat of insider risk from either enterprise or third party IT teams is also gone. No person or process is exposed to data unless explicitly allowed by policy.

- **Zero-Trust:** The Confidential Cloud effectively implements a zero-trust IT infrastructure. Access to data is strictly and continuously managed by least-privilege policy. The access you choose to allow is continuously monitored and recorded.

- **Compliance Acceleration and Simplification:** Correctly implemented confidential computing technologies can put applications out of scope and in compliance with GDPR, PCI, CDPA, NIST, and other compliance rules. This makes compliance simple and worry-free.

- **Software Supply Chain Security:** The recent SolarWinds breach highlights the critical need to secure and protect the software supply chain. With Nitro Enclaves, only certified software can operate in certified and isolated Confidential Cloud environments. And because applications are completely isolated from each other in a zero-trust posture, there is no way for even certified but compromised software to execute horizontal attacks.

- **Hybrid Cloud Security:** Data and applications increasingly extend outside the private data center. Enterprises need to make sure these remain secure. With the Confidential Cloud, computing can happen anywhere, but access will still be exclusively controlled and secured by the enterprise.

- **Risk and Vulnerability Mitigation:** When application code and sensitive data are physically isolated and secured from potential bad actors, the enterprise can potentially mitigate tens of thousands of host, application, storage, and networking vulnerabilities. Operating system flaws and zero-day exploits are no longer a security concern. From a data security standpoint, misconfigurations—and even direct exposure to the Internet—no longer matter.

Four Simple Steps to Building Your Own Confidential Cloud

The potential impact of the Confidential Cloud on enterprise security is extremely broad. But successful adoption of the Confidential Cloud requires planning. Here's how to make the process smooth and simple.

1 Find a High-Priority Executive Initiative Solved by The Confidential Cloud

We've already mentioned many initiatives where the Confidential Cloud could significantly impact enterprise IT. Here are several uses cases that address these initiatives.

- **Database user protection:** Protect not only the core database, but the clients attached to that database as well.
- **Key protection:** Ensure the keys to enterprise data, including secret 0, are secure.
- **Secure Machine Learning:** Allow valuable machine learning algorithms to process data at the network edge, fully protecting intellectual property and sensitive data.
- **Multi-Party Compute:** Allow applications that require two or more parties to share data and algorithms to work effectively without either party seeing or touching the other's data.
- **Cloud Migration:** Eliminate the compromise between cloud economics and increased risk.
- **PII Protection:** Put PII in a zero-trust posture by default. Prevent access during processing—fully protecting this information from any insider exposure.
- **Cloud Native Application Protection:** Protect highly elastic cloud-native workloads by delivering seamless and strong protection that follows applications and data wherever they operate.
- **Microsegmentation:** Isolate computing, storage, and networking resources of a single host or across public and private clouds.

The goal is simple: Find a funded initiative where you can be successful. Then set success criteria that are easily achievable. These may include:

- **Simplicity of implementation:** Deploying a new security technology can be extremely disruptive—generating new costs and risks that disrupt the business environment and undermine ROI. A successful technology should ideally be simple to deploy and non-disruptive to current operations. When implemented correctly, a Confidential Cloud delivers protection that is transparent to both applications and IT personnel, and it does so without requiring recoding applications or rearchitecting IT processes.

- **Reduced Threat ROI:** Quantify the threats expected to be eliminated because of the reduced attack surface. A simple way to calculate ROI is to show the reduced need for threat modeling—a human-intensive and expensive manual process. Eliminating threats reduces the amount of threat modeling required, as well as the potential cost and implications of a threat itself.

- **Vulnerability ROI:** The average organization has tens of thousands of vulnerabilities—many of which are hidden. Computing within a Confidential Cloud mitigates many of these issues instantly. This not only reduces the risks they represent, but it virtually eliminates the high cost of patching against both known and unknown vulnerabilities.

2 Leverage a Confidential Cloud Platform

You've already made the smart decision to use AWS as your cloud platform. Creating a confidential computing environment on AWS can be labor intensive. Existing and packaged applications are all great targets for a first project, but they won't be supported out of the box with AWS Nitro alone unless they are rearchitected and rewritten to work with underlying Nitro technology.

Fortunately, this work can be avoided altogether by leveraging such software as Anjuna's Confidential Cloud™ software platform. A platform such as this makes migrating applications to AWS Nitro extremely simple. With the Anjuna Confidential Cloud software platform, applications don't need to be rewritten. In fact, existing and packaged applications run securely isolated as-is, unmodified, and fully managed.

Choosing a Confidential Cloud software platform greatly simplifies and accelerates deployment without disrupting development or operations. This allows more applications to be protected much more quickly, reducing the most risk for the enterprise.

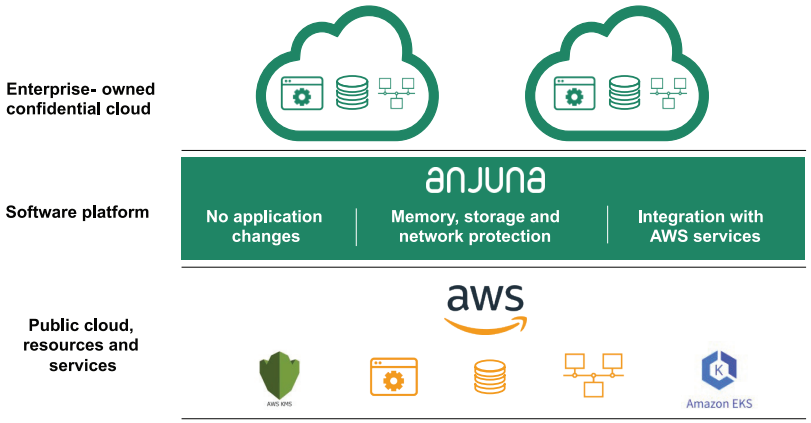

Figure 6: The Confidential Cloud is a completely private hardware-grade secure computing environment.

3 Walk Before You Run – Select a simple application to prove the point

Whether your application is as simple as "Hello World" or a massive application serving thousands of users, the effect of shifting that application to a Confidential Cloud will be the same:

- Data and applications previously exposed while running in memory will be hidden.
- Data previously exposed on disk will be fully encrypted.
- Data transmitted over a network within a Confidential Cloud will be fully encrypted.
- All data, applications, and algorithms will be protected by a single contiguous security perimeter established by the Confidential Cloud.

Databases are an ideal choice for a proof of concept (POC) project. They are, after all, where most sensitive data is stored, used, and sent.

Keep this simple to start. You'll still be able to show a big impact, but without a big time investment. Because the process is so painless, the next expansion can happen rapidly. With Anjuna, the transition from walk to run can be quick. It pays to outline several moves, so you know where the Confidential Cloud can next deliver value for your organization.

Anjuna's Confidential Cloud platform is especially useful in protecting highly distributed cloud-native applications and data. Kubernetes-based applications, for example, are transparently protected even as they scale across geographies and hosting locations. This protection is delivered as part of the underlying software stack, with no additional effort from the development team. It's a simple and effective security solution for protecting even multi-cloud Kubernetes-based applications and workloads.

After implementing your first applications in a Confidential Cloud, your enterprise can start to realize the full value of the cloud with faster innovation. Anjuna enables companies to maximize business impact the same way you do with new applications: Start small with low risk, learn how to maximize impact, and then scale.

Figure 7: Start with a few simple applications before enterprise deployment.

4 Partner with Anjuna

Having a trusted and experienced partner can help immensely with integrating any new technology—even one that is as non-disruptive as Confidential Cloud computing. Anjuna, a pioneer in this space, is working with every major confidential computing and cloud vendor, including AWS and their Nitro Enclaves team.

A strong partner can help you take the lead on confidential computing in your organization by providing the resources and support to move forward. Anjuna has an experienced customer success team and other resources to help you negotiate the potential resistance that often comes with change.

Security hero-level success comes in steps. Anjuna will be there to help each step of the way.

Get Started Today

Anjuna's team stands ready to help with your Confidential Cloud journey wherever it may lead. To get started today, go to www.anjuna.io/StartMeUp.

anjuna

Anjuna Security makes the public cloud secure for business. Software from Anjuna Security effortlessly enables enterprises to safely run even their most sensitive workloads in the public cloud. Unlike complex perimeter security solutions easily breached by insiders and malicious code, Anjuna leverages the strongest hardware-based secure computing technologies available to make the public cloud the safest computing resource available anywhere. Anjuna is based in Palo Alto, California.

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

AS07-1021