Four Steps to getting unbeatable security on the Microsoft Azure cloud

anjuna

Executive Summary

Maintaining security while taking advantage of the power of cloud computing is an ongoing challenge for security professionals. Now there's a new way for your IT organization to have the best of both worlds: Cloud scalability and economics, plus uncompromising security for data and workloads.

A Confidential Cloud is a secure computing environment completely private to its owners, formed over one or more public cloud providers. It leverages and extends powerful hardware-grade secure computing capabilities, such as those found within Intel® SGX CPUs used by Microsoft Azure confidential computing instances. This enables organizations to create protected, isolated, and secure compute environments, known as secure enclaves, to process highly sensitive data. Intel SGX provides the foundation for a private cloud computing infrastructure that will remain completely isolated from open and exposed public computing environments. The result: Highly sensitive workloads operate with the strongest protection available anywhere—even more secure than private, on-premises data centers.

In this document, we'll show you how to securely run applications and workloads within your own Confidential Cloud built on a Microsoft Azure cloud environment quickly and easily. The scalability and economics of the cloud, unbeatable security, and an environment you control…the best of all worlds!

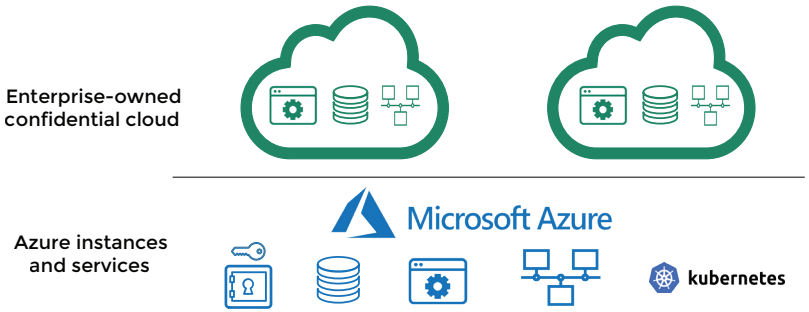

Figure 1: Confidential Clouds are built on top of Microsoft Azure services.

The Case for Confidential Clouds

CISOs have long had concerns with the security of cloud computing. Keeping data secure meant keeping it in your own datacenter. Computing in the public cloud meant a loss of control, shared data security responsibility, and added compliance complexity.

Now, however, using the simple-to-deploy security approach of a Confidential Cloud, your applications and data can be measurably more secure on Microsoft Azure confidential computing than in your private datacenter. With hardware-grade encryption, physical isolation, and the ability to attest to the validity of both applications and the operating environment, Confidential Clouds are arguably the safest place to compute anywhere.

A Confidential Cloud is a secure computing environment formed over one or more public cloud providers. Applications, data, and workloads within a Confidential Cloud are physically and cryptographically isolated from all users, administrators, and computing processes—both on specific hosts and across the entire collective public cloud. A Confidential Cloud environment is completely private to its owners, leveraging and extending powerful hardware-grade secure computing capabilities such as Intel SGX (Software Guard Extensions). Together, Microsoft Azure confidential computing, Intel SGX-enabled CPUs, and Anjuna Confidential Cloud software enable organizations to use existing applications and process highly sensitive data in a protected, isolated, and secure compute environment.

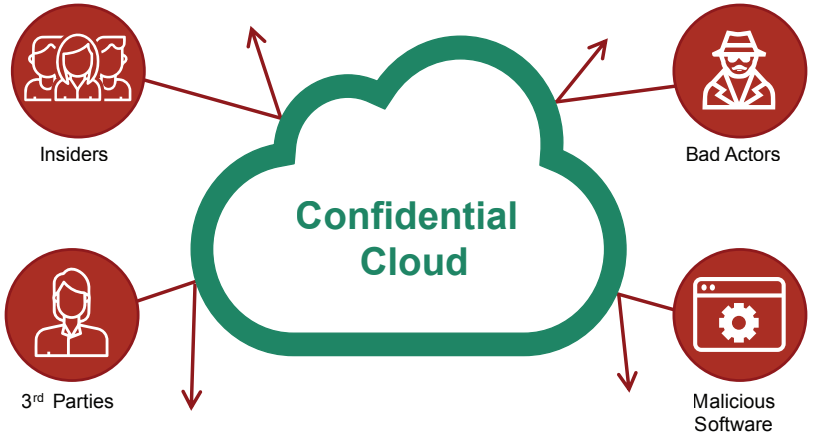

Figure 2: The Confidential Cloud protects existing data and applications from entire classes of threats by default.

A Confidential Cloud establishes an invisible, exclusive, and contiguous perimeter around data—regardless of where the data is stored, transmitted, or processed. The result is a "zero-trust" cloud computing infrastructure so isolated and so secure that nothing inside that perimeter can be observed or exported. By default, nothing inside can get out and nothing outside can get in. This allows for even the most sensitive workloads to operate in hostile, untrusted geographies with complete privacy, utilizing the strongest protections available anywhere.

Risk vs. Business Opportunity

Most businesses are moving towards cloud computing—and for good reason. Microsoft Azure confidential computing delivers cost, scalability, ubiquity, and ease-of-consumption benefits unrivaled by on-premises infrastructure. Cloud-enabled organizations get cost and agility improvements that result in tangible competitive advantages.

Here's the problem. As attractive as the public cloud might be, it also increases cyber risk. In the cloud, data and workloads are exposed to insiders, third parties, bad actors, and malicious software—not to mention your own IT operations teams. This exposure changes as people, processes, and the cloud itself change. With enough time and effort on the part of a bad actor, data will eventually need to be considered exposed. For this reason, few organizations have moved their entire IT infrastructure—including their most sensitive applications and data—to the public cloud.

Let's dig a little deeper to understand why the public cloud can create risk. Your organization's data—wherever it's used, stored, or transferred—is vulnerable by nature. Underneath your security stack (which may include firewalls, IDS/IPS, DLP, encryption, and other layers), data remains vulnerable. That's because data isn't self-securing. It remains easily accessible, for example, as it sits in host memory.

Memory exposure is the heart of a vexing data security problem many have simply come to accept. From a compliance standpoint, anyone or any application with access to a host must be considered to have exposure to the data available on that host. From a pure security threat standpoint, this means that any access to a host (and thus access to unencrypted data in memory) is the first step in undermining all data security layers. Compromising the host virtually guarantees access to all the data stored there.

Figure 3: Layers of overlapping security products leave gaps for hackers to take unprotected data

This is why over 95% of security professionals resist full cloud migration efforts.[1] That said, when the choice comes down to security versus business opportunity, security often loses. Typically, organizations choose to accept the risk—crossing their fingers and hoping the next breach won't have their name on it. Unfortunately, hope is not a sustainable cybersecurity strategy.

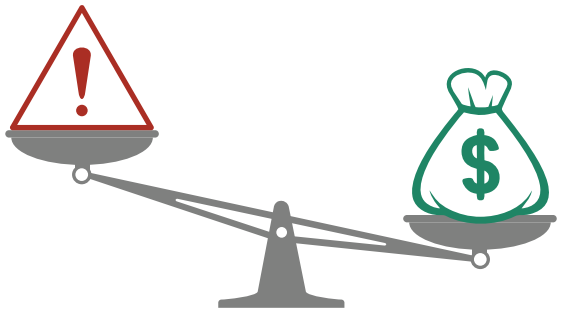

Figure 4: Risk vs. opportunity: Businesses will always accept more risk to seize opportunity

[1] anjuna.io/451report

The Solution: Microsoft Azure confidential computing, Intel® SGX, and Anjuna Confidential Cloud Software

Microsoft Azure and Intel recognized the need to address this security gap. Their goal is not just to make the cloud safe enough for all applications and to facilitate digital transformation, but to also give IT organizations complete responsibility and control of their own data.

In 2015, Intel introduced Software Guard Extensions (Intel SGX), a set of proprietary, security-related machine-code instructions built into their CPUs. These instruction sets solve the problem of memory vulnerability by encrypting memory and only decrypting it within the CPU itself when used.

These CPU security features can be used to create what is commonly known as a secure enclave—effectively an isolated private computing environment within an SGX-enabled host. Data and executable code are isolated on the host computer in a way that's invisible to all users and processes. The enclave cannot be directly accessed. By default, it can't reach outside of its own environment. Even users and processes with privileged root access to the host system can neither see the enclave itself nor reach the data and processes within it. This means the enclave is effectively a private computer-within-a-computer.

Not only is Intel SGX enclaving technology leveraged and supported directly by Microsoft Azure confidential computing services, this broad range of instance sizes and configurations also comes at no extra charge to enterprise customers.

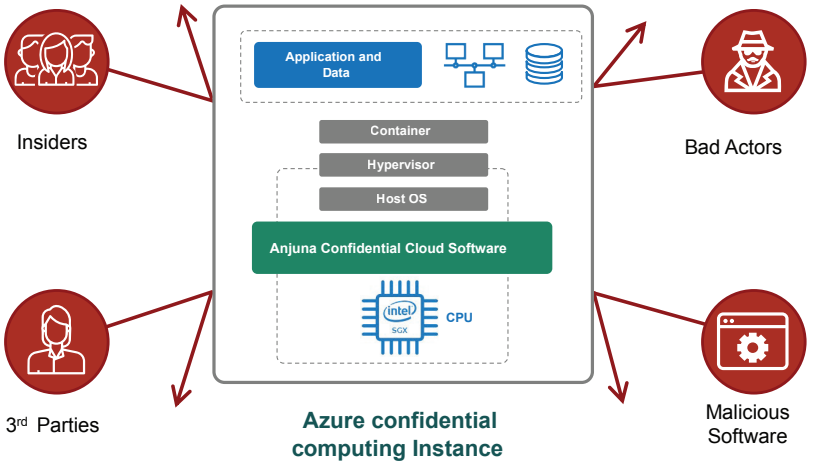

Figure 5: The combination of Microsoft Azure hosts, Intel SGX-enabled hardware, and Anjuna Confidential Cloud software protect applications and workloads from entire classes of threats.

This powerful combination makes the decision to adopt simple for both customers and Microsoft Azure. Customers get a level of security in the public cloud that was previously unattainable. Microsoft Azure no longer shares security and compliance responsibility for customer data and applications which they can't possibly touch or access.

A Simple Path to Secure Cloud Computing

Intel SGX enables hardware-protected execution, but software running inside an SGX enclave must still be integrated into SGX and enterprise environments.

To do this, the pioneers of confidential computing and those writing their own new code, modified application code specifically for Intel SGX. This is more of a time and resource investment than most mainstream adopters are able or willing to make. End-to-end enterprise-ready deployment also requires additional important management capabilities and lifecycle management.

That's where software companies such as Anjuna Security come in. Anjuna enables enterprise IT organizations to easily operate any application, data, and workload within a Confidential Cloud based on Intel SGX and Azure—isolated not just within a specific host, but from the entire public cloud. This creates a private cloud computing infrastructure so secure that even the most sensitive workloads can be trusted to work in hostile public computing environments with complete privacy—and with the strongest protection available anywhere.

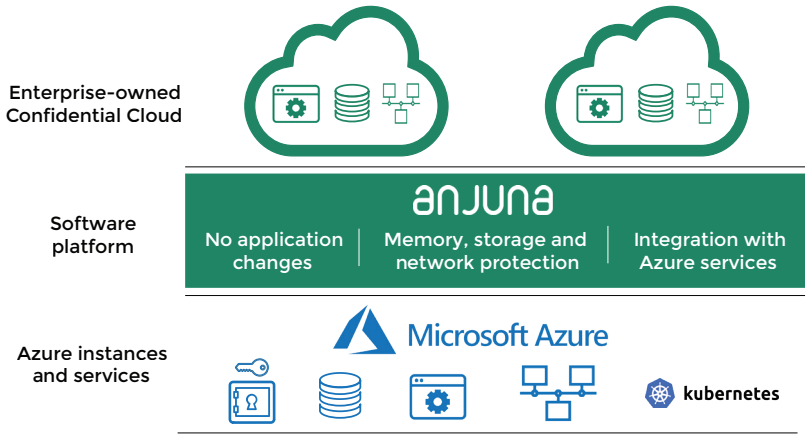

Figure 6: Anjuna leverages Microsoft Azure cloud services and Intel SGX technologies to create isolated compute environments on physical hosts that support applications at scale.

Winning With the Confidential Cloud

What does this mean to enterprise IT organizations like yours?

- The cloud is now the most secure place for your organization to compute—more secure than other alternatives, even private data centers.
- All your applications will be protected with hardware-grade security by default.
- You can easily migrate workloads and effectively eliminate data exposure to insiders, bad actors, and malicious software.
- Protecting your existing workloads will not require costly, time-consuming software rewrites.

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

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 the success of any security project. Enterprise IT groups use Confidential Cloud capabilities to implement and support such key initiatives as:

- **Digital Transformation and Cloud Migration:** 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—without the cost and complexity of layered perimeter security.

- **Insider Risk:** By eliminating IT insider access, the Confidential Cloud wipes out the risk of data 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 eliminated. 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 completely restricted by default. Any access granted is strictly and continuously managed by least-privilege policy, and all access is continuously monitored and recorded.

- **Compliance Acceleration and Simplification:** Confidential computing technologies can put applications out of scope and in compliance with mandates such as NISTIR 8320[2] and GDPR—making compliance simple and worry-free.

- **Software Supply Chain Security:** The recent Solar Winds breach highlights the critical need to secure and protect the software supply chain. With the combination of Microsoft Azure confidential computing and Anjuna, only certified software can operate in isolated Confidential Cloud environments. And, because applications are completely isolated from each other in a zero-trust posture, there's no way for even certified but compromised software to execute horizontal attacks.

- **Hybrid Cloud Security:** Data and applications increasingly extend beyond the private data center. With the Confidential Cloud, workload and data protections extend everywhere applications and data are used, while access is exclusively controlled 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—even direct exposure to the Internet—no longer matter.

[2]https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8320-draft2.pdf

Building Your Own Confidential Cloud

The potential impact of the Confidential Cloud on enterprise security is extremely broad. To get started on your Confidential Cloud journey, here are recommendations for simple, smooth, and successful adoption.

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

The Confidential Cloud can significantly impact many enterprise IT initiatives. It's likely that your organization has at least one of the following initiatives underway.

- **Database user protection:** To protect not only the core database, but the clients attached to that database as well.
- **Key and Key Management protection:** To ensure the keys to enterprise data, including secret 0, are secure.
- **Secure Machine Learning:** To allow valuable machine learning algorithms to confidentially process data at the network edge, fully protecting intellectual property and sensitive data.
- **Multi-Party Compute:** To 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:** To eliminate the compromise between cloud economics and increased risk.
- **PII Protection:** To put PII in a zero-trust posture by default. This involves preventing access during processing—fully protecting this information from any insider exposure and simplifying compliance.
- **Cloud Native Application Protection:** To deploy elastic cloud-native workloads with seamless and strong protection that follows application and data wherever they operate.
- **IT Microsegmentation:** To implement a simple zero-trust micro-segmentation by isolating computing, storage, and networking resources using a single technology.

Successful implementation of initiatives like these often hinges on simple success criteria, such as a reduced attack surface, fewer vulnerabilities, and simple deployment. Confidential Clouds deliver on all three criteria by offering protection that is transparent to both applications and IT personnel without requiring re-coding or re-architecting IT processes.

2 Leverage a Confidential Cloud Platform

You've already made the smart decision to use Microsoft Azure as your cloud platform. However, creating a confidential computing environment on Microsoft Azure 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 unless they're rearchitected and rewritten to work with underlying Intel SGX technology by the software developer.

Fortunately, this hassle can be avoided altogether by leveraging Anjuna's Confidential Cloud software platform, which makes migrating applications to Microsoft Azure confidential computing extremely simple. With Anjuna's software, applications don't need to be rewritten. In fact, existing and packaged applications run securely isolated as-is, unmodified, and fully managed. Applications simply run the way they are today. Anjuna Confidential Cloud software takes care of ensuring security.

The 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 your enterprise.

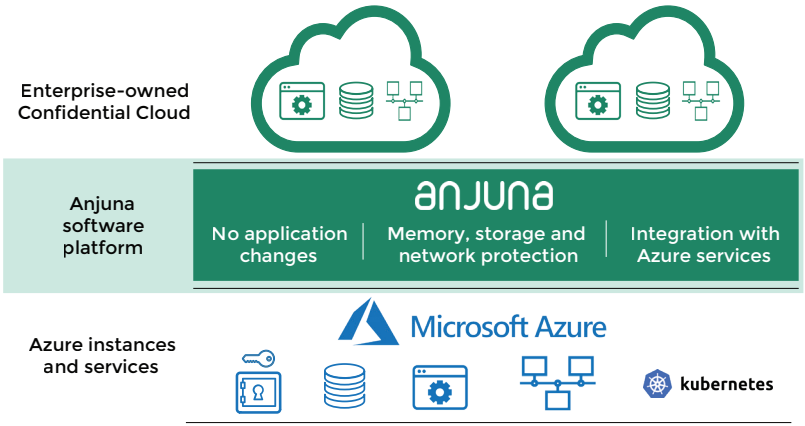

Figure 7: Anjuna leverages Microsoft Azure cloud services and Intel SGX technologies to create isolated compute environments on physical hosts that support applications at scale.

3 Walk First, Then Run

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.

Figure 8: Start with a few simple applications before enterprise deployment.

Anjuna’s Confidential Cloud platform is especially useful in protecting highly distributed cloud-native applications and data. Kubernetes-managed 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 that will protect even multi-cloud Kubernetes-based applications and workloads.

Keep it simple to start.

With Anjuna, the transition from walking to running can be quick. It pays to outline several moves, so you know where the Confidential Cloud can next deliver value for your organization.

4 Partner with Anjuna

Having a trusted and experienced partner can help immensely with integrating any new technology into your enterprise—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 Microsoft Azure, to make the adoption process as smooth as possible.

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.

Get Started Today

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

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

AS08-0122