

# enclave Multi Cloud Platform

Your Gateway to Next-Generation Cloud Security

The enclave Multi-Cloud Platform revolutionizes cloud security, offering seamless access and management of resources within a confidential cloud environment.



The enclave Multi-Cloud Platform (eMCP) is a comprehensive solution for managing and securing your cloud resources.

With eMCP, effortlessly transition to a confidential cloud environment and maintain control over your data and applications. Leveraging hardware-based trust and a software-secured architecture, eMCP ensures your data and code remain encrypted and thus protected at all times—meaning at rest, in motion, and in use.

We call this 3D encryption.

## About Confidential Computing



Confidential computing represents a breakthrough advancement in data security. It enables environments - whether container, application or VM - to run in a **fully encrypted form**.

This means that throughout the entire operational cycle, from startup to termination, these environments remain encrypted. Data and program flows are **cryptographically isolated from the rest of the system** thanks to this runtime encryption.

Only the CPU - and no other components or processes - can decrypt this encrypted environment, execute instructions, and then store results in encrypted form again.

## Current Challenges



### Security

Storing sensitive data in the cloud raises concerns about unauthorized access and data breaches due to single points of attack.



### Compliance

Meeting regulatory requirements for data protection can be challenging in a shared environment, especially when managed by third-parties.



### Unpredictable Costs

While cloud computing can provide cost savings, it can also lead to unpredictable costs if usage isn't carefully monitored and managed.



### Vendor Lock-In

Organizations may become dependent on a specific cloud service provider's technologies, making it difficult to switch providers.

## Virtual HSM:

- Protect Key Management Systems and Identity Access Management with hardware-graded security. Manage secrets and control user access to workloads in any environment with ease.
- Decouple trust from the cloud environment using Vault and Nitride to achieve a secure and comprehensive cloud ecosystem.

## Confidential Virtual Machines (VMs):

- High-Performance Backbone: Create a secure and isolated infrastructure backbone. Protect data and applications from unauthorized access, even in public clouds.
- No Code Changes Needed: Maintain existing code and infrastructure with seamless integration.

## Confidential Kubernetes:

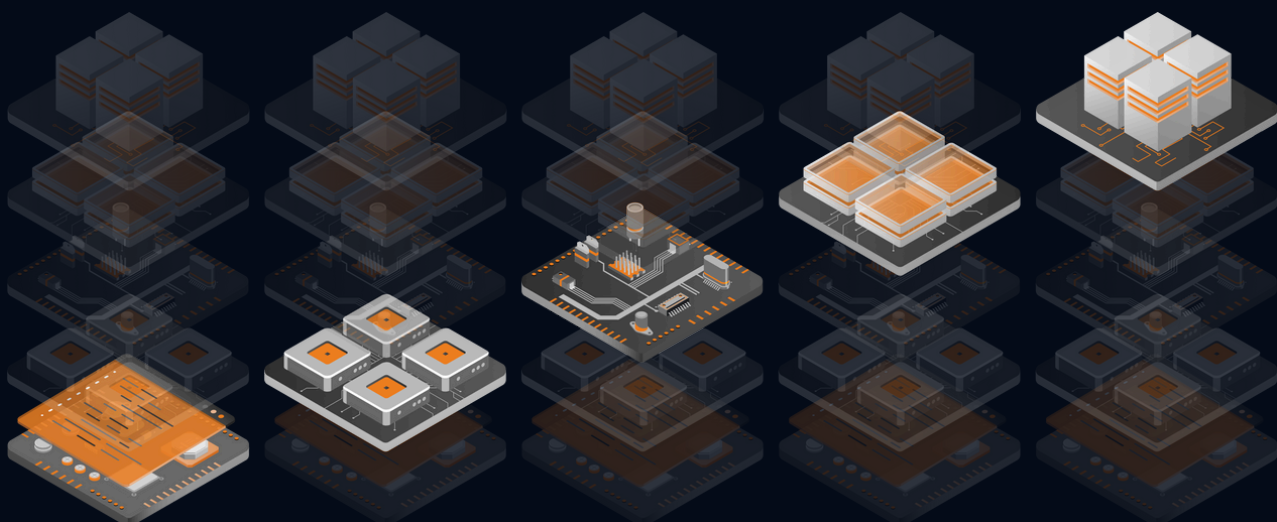
- Secure Kubernetes Environment: Deploy and scale containerized workloads with zero-trust infrastructure, ensuring data remains confidential throughout its lifecycle.
- Compliance and Authenticity: Verify application components for authenticity and regulatory compliance.

## Managed Databases:

Advanced Security: Host sensitive data with industry-leading security and privacy protection, keeping data encrypted at rest, in transit, and in use.

## Managed Applications:

Managed Solutions: Choose from a portfolio of pre-configured confidential applications, managed by enclave, to save time and resources.



Virtual HSM

Confidential VMs

Confidential Kubernetes

Managed Databases

Managed Applications

## Why Choose eMCP?

### ▶▶ Flexibility

Supports various IT environments and is multi-tenant, ideal for Managed Service Providers (MSPs).

### ▶▶ Customizable

Easily create and manage your own applications and environments.

### ▶▶ No Data Access

eMCP never accesses personal or application data.

### ▶▶ Scalable

Add admin and user accounts as needed, with flexible monthly billing.

### ▶▶ Provider agnostic

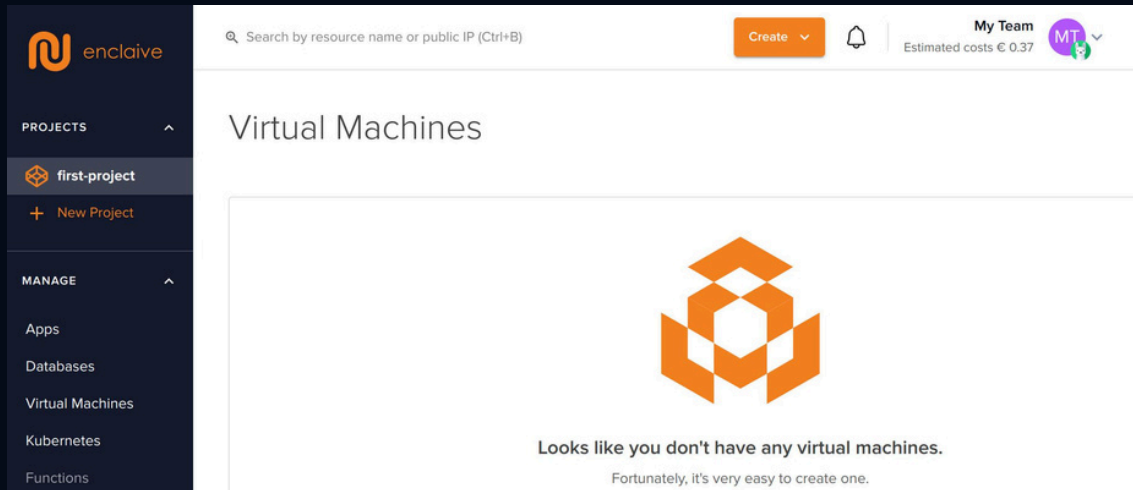
Compare between various cloud providers. We've got the infrastructure and price for you.



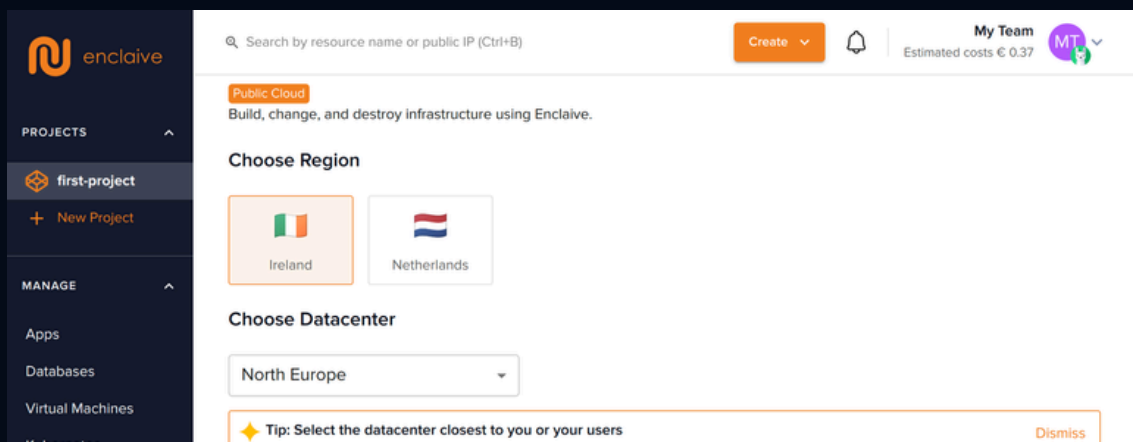
▶▶ Get your own Confidential Multi-Cloud environment under: <https://console.enclave.cloud/>

# eMCP allows you to easily create your secure Multi-Cloud environment.

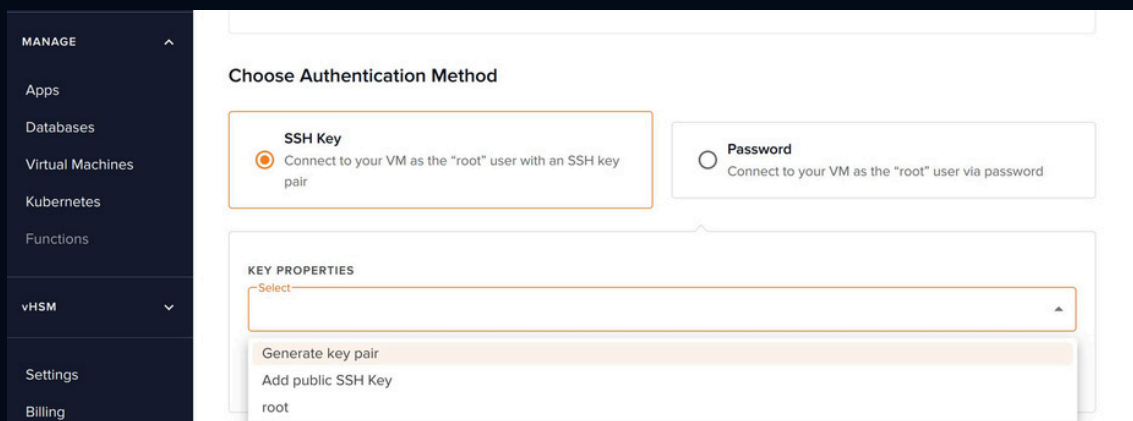
## 1. Create your Buckypaper



## 2. Fill in the details

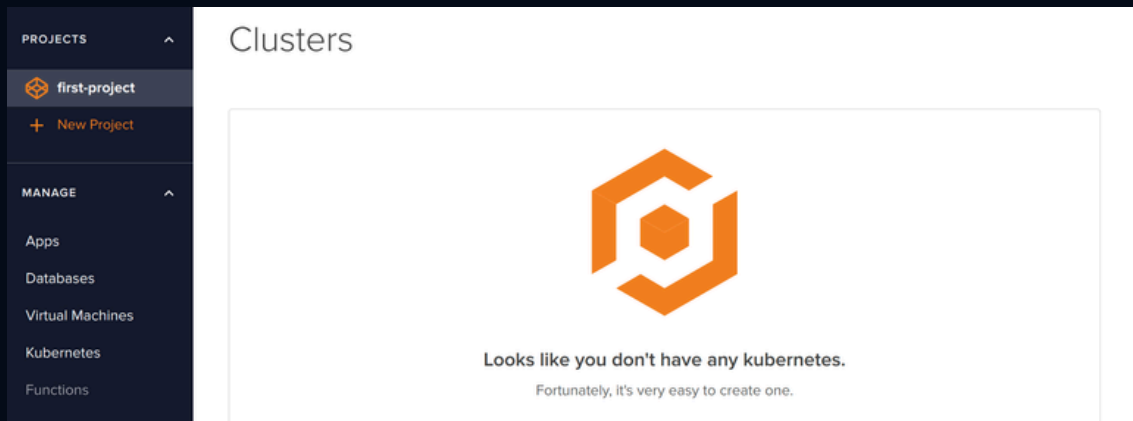


## 3. Choose the authentication method

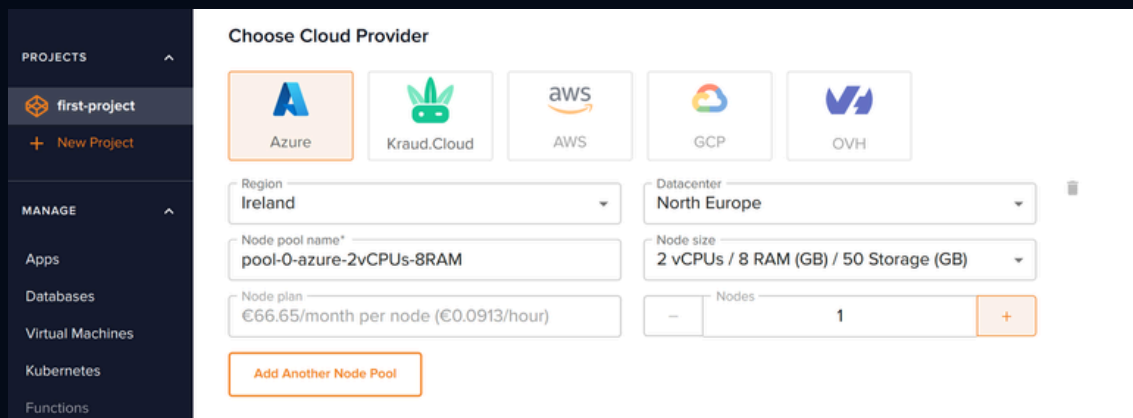


# eMCP allows you to easily create your secure Multi-Cloud environment.

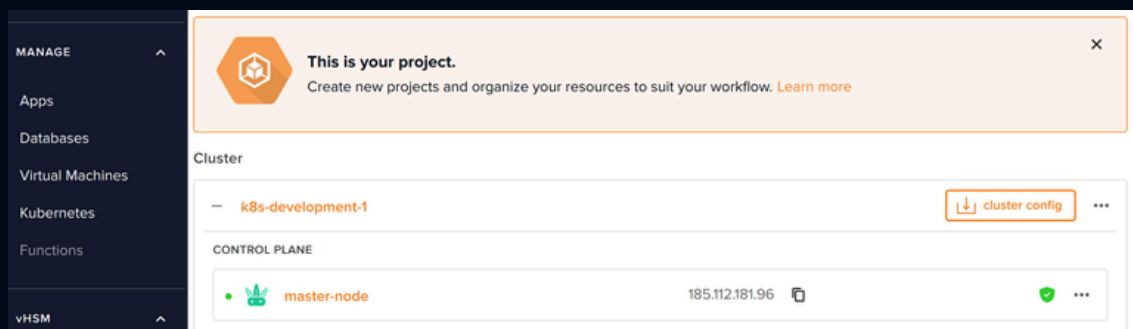
## 4. Create your Kubernetes Cluster



## 5. Fill in the details



## 6. Finalize your project



# Learn more

## About enclave

enclave enables businesses to securely protect their sensitive data and applications in untrusted cloud environments by leveraging the use of Confidential Computing.

Its comprehensive, multi-cloud operating system allows for **Zero Trust security** by encrypting data in use and shielding applications from both the infrastructure and solution providers.

With enclave, businesses can confidently build, test, and deploy a wide range of cloud applications, all while **maintaining complete control over their confidential information**. enclave's goal is to provide a universal, cloud-independent technology for enclaving sophisticated multi-cloud applications, that can be deployed with confidence and ease.

## Contact details



[github.com/enclave](https://github.com/enclave)



[linkedin.com/company/enclave](https://www.linkedin.com/company/enclave)



<https://enclave.io>



[youtube.com/@confidentialcompute](https://www.youtube.com/@confidentialcompute)



## CONTACT

[contact@enclave.io](mailto:contact@enclave.io)

+49 30233292973

Chausseestr. 40, 10115 Berlin, Germany



# Making the Cloud the safest place for digital businesses