RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **OST-M05**

Scalable Confidential Computing on Kubernetes with MarbleRun

Moritz Eckert
Chief Architect
Edgeless Systems
@m1ghtymo

Felix Schuster
CEO
Edgeless Systems
@flxflx

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

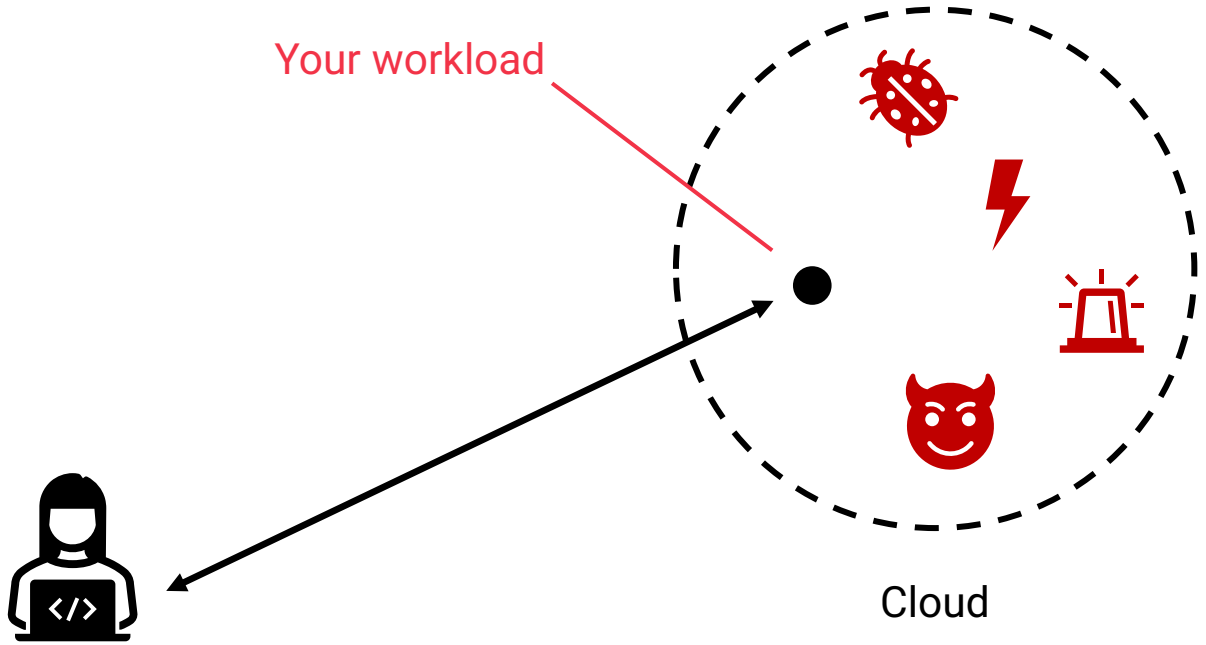
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

What is the biggest roadblock for cloud adoption?

Security, Privacy, and compliance concerns!

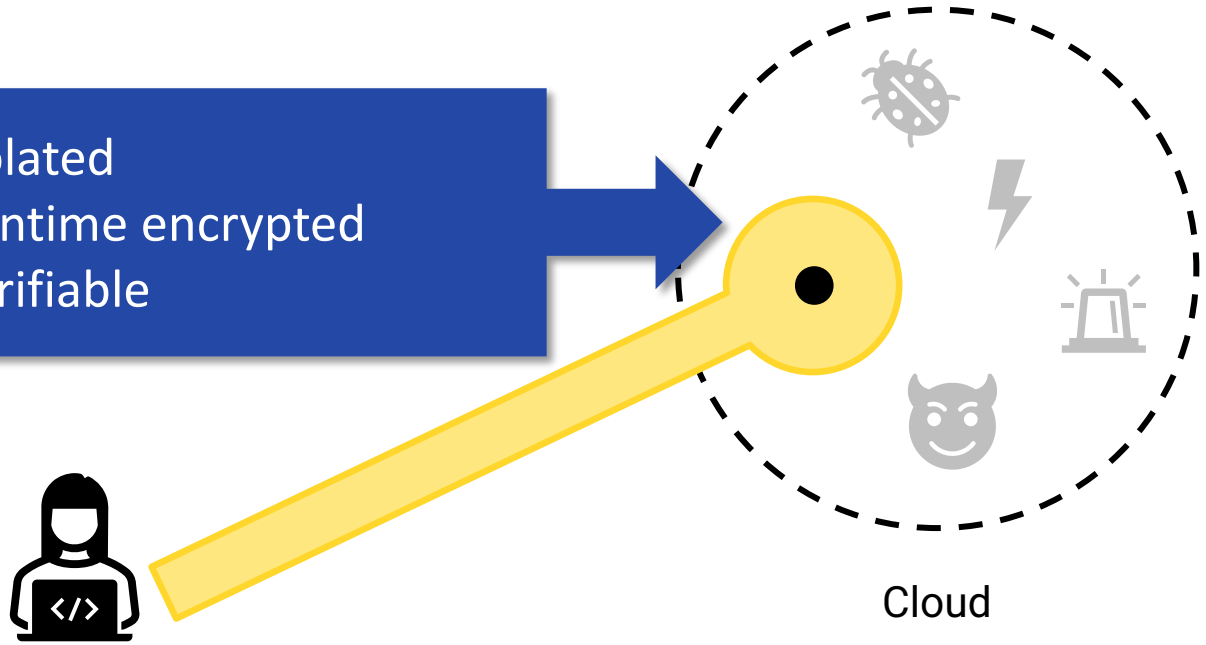
Imagine one could fundamentally solve this…

Confidential computing takes you from here …



… to here

- Isolated
- Runtime encrypted
- Verifiable



Everyone's Excited

IDC

FUTURE ENTERPRISE

Confidential Computing in the Public Cloud: Why Should You Protect Data-in-Use for Privacy & Trust?

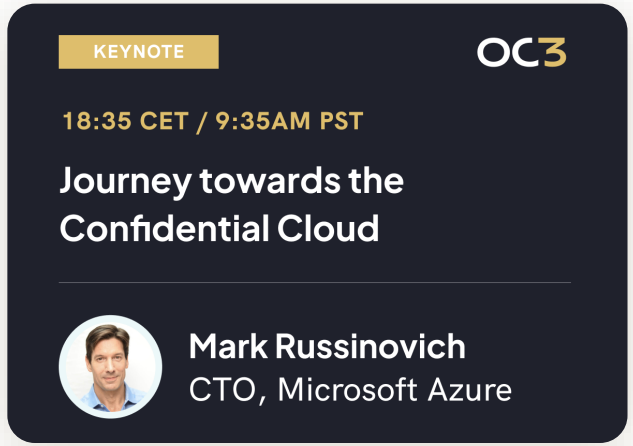
Learn how to protect your data with Confidential Computing with IDC's Amita Potnis.

APRIL 26, 2021 - 5 MINS READ

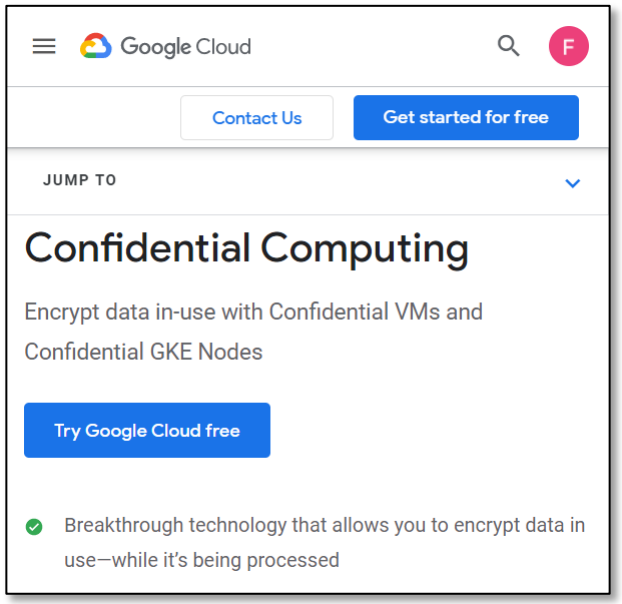
Share on Facebook | Share on Twitter | +

Everyone's Excited

> Confidential computing is the future of computing in general.
>
> We will see an expectation that data is always encrypted while it is in use, regardless of how sensitive it may be.



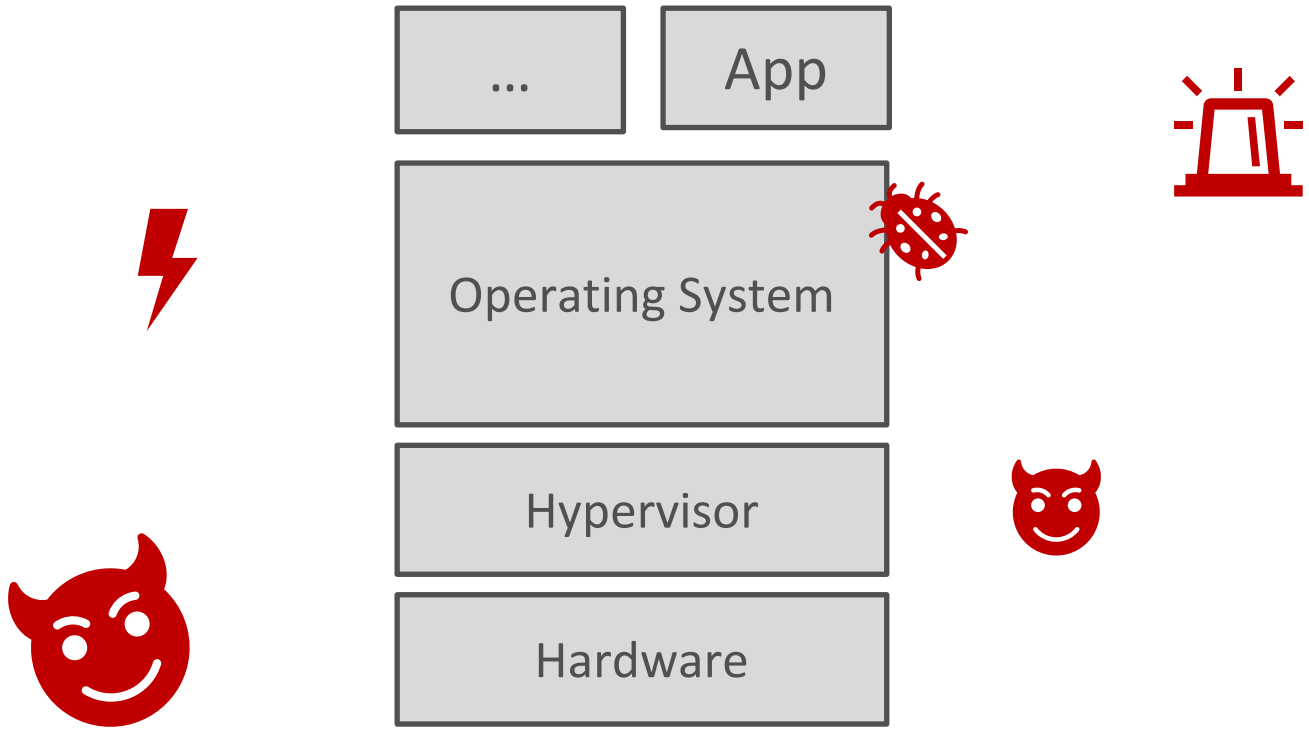
The Cloud's Getting Ready



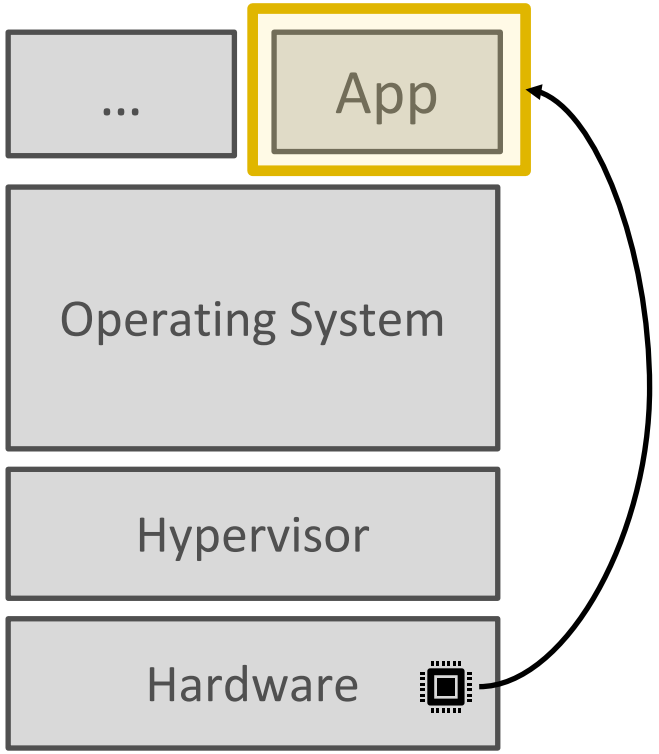
RSAConference2022

Confidential Computing

Secure Enclaves

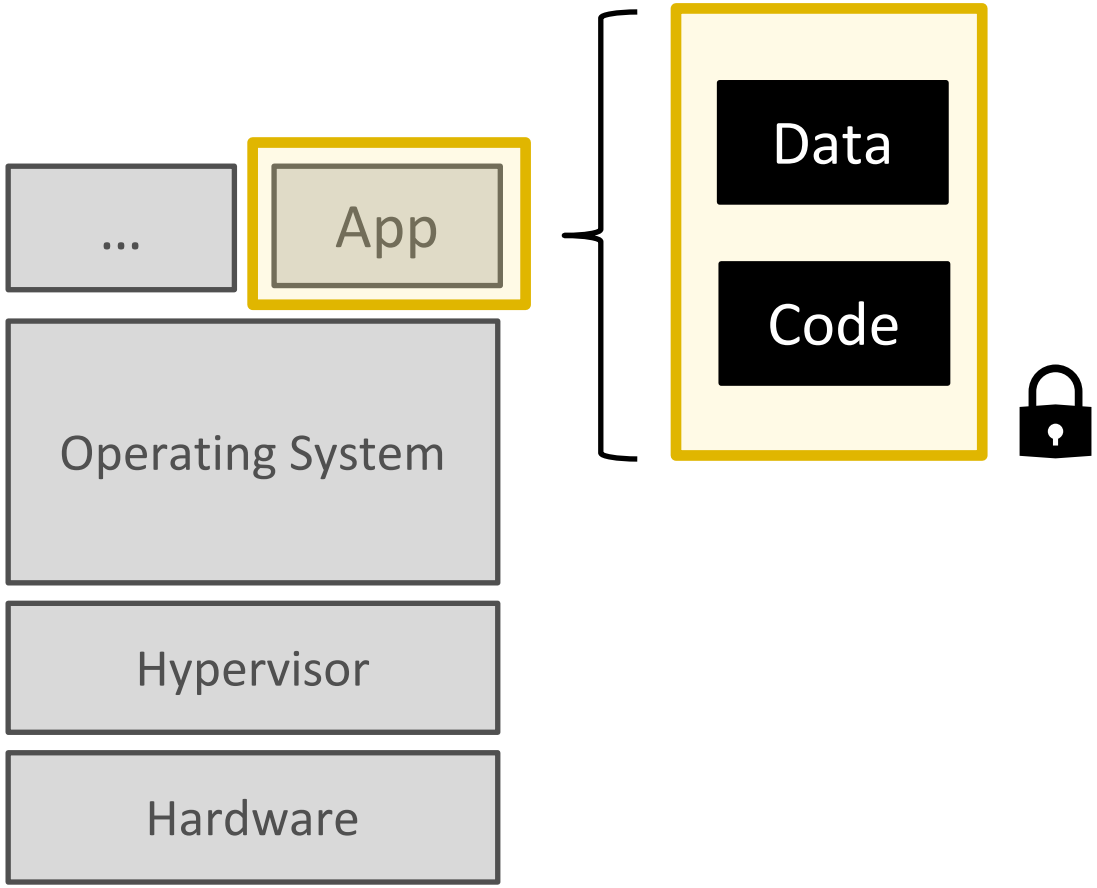


Secure Enclaves



CPU creates and enforces enclave

Secure Enclaves

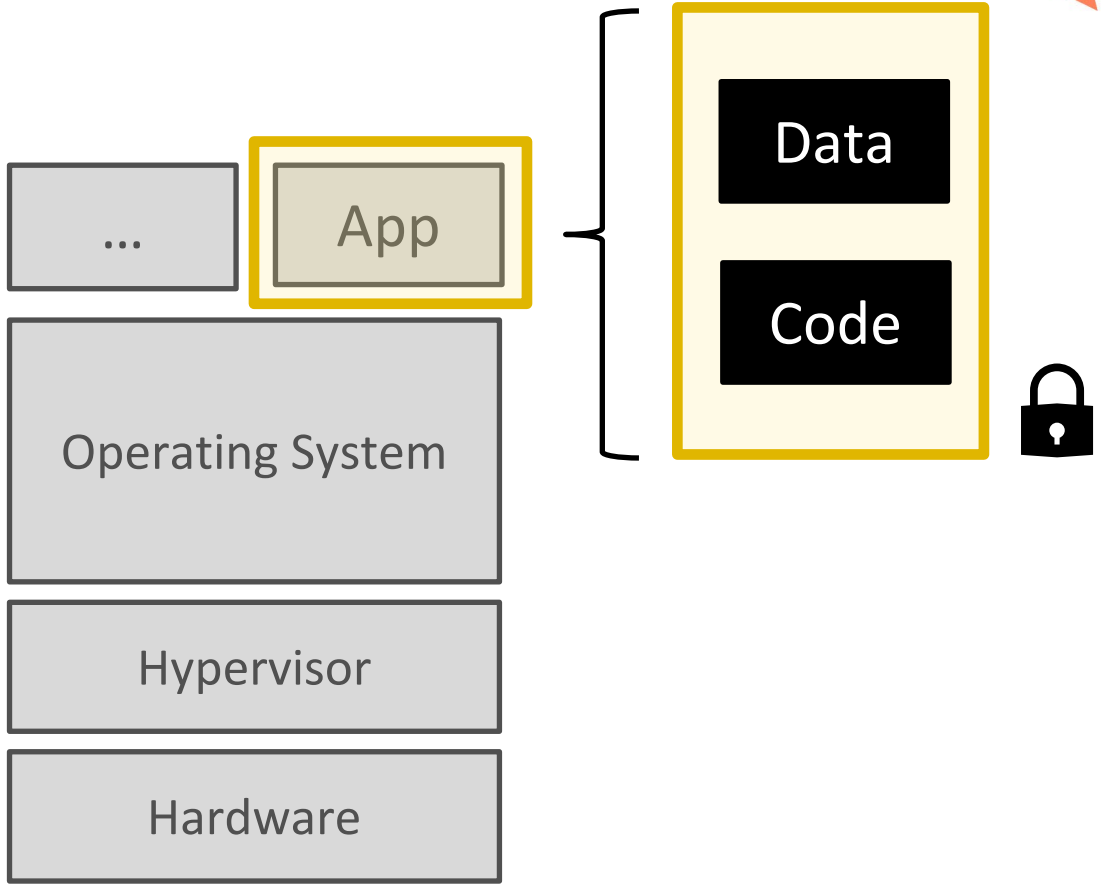


Secure Enclaves

Defining properties

- Isolation
- Runtime memory-encryption
- Remote attestation

Intel SGX



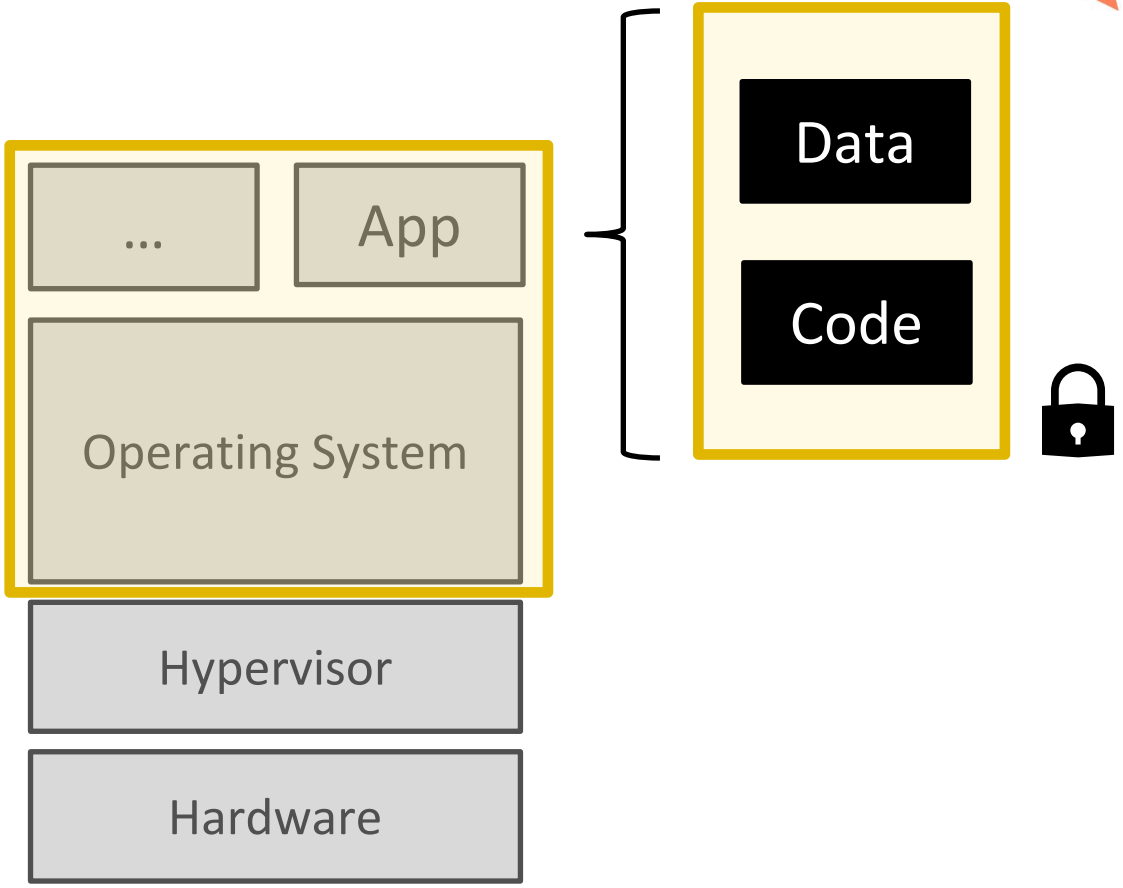
Confidential VMs

Defining properties

- Isolation
- Runtime memory-encryption
- Remote attestation

AMD SEV

Intel TDX, Arm Realms



RSAConference2022

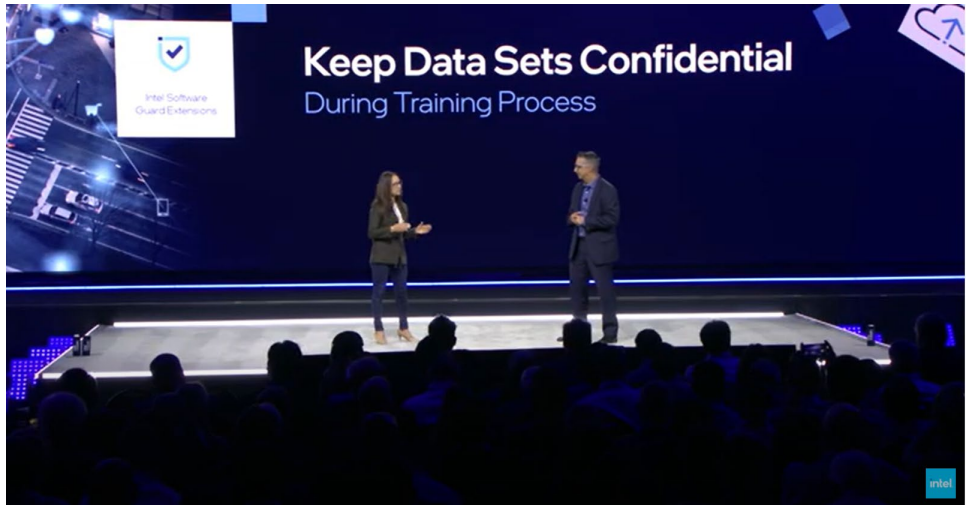
What can we use this for?

Use Cases

1. Make existing workloads more secure & compliant
2. Build new privacy-preserving apps

Privacy-preserving AI Training for Driver Assistance Systems

Intel Vision, May 2022



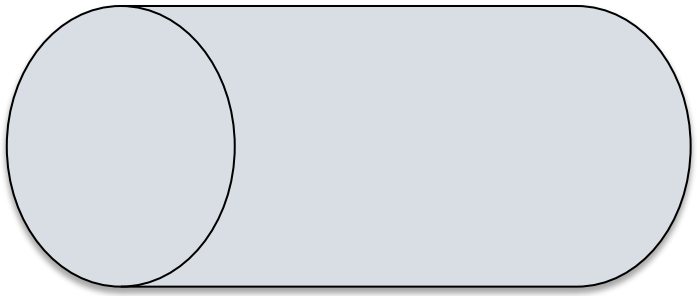
Microsoft Build, May 2022

Privacy-Preserving AI Training for Driver Assistance Systems

Acquisition

De-Identification

Training

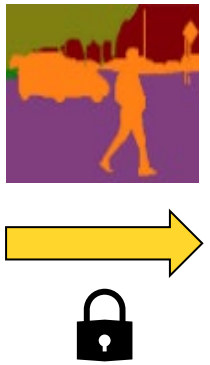


Privacy-Preserving AI Training for Driver Assistance Systems

Acquisition

De-Identification

Training

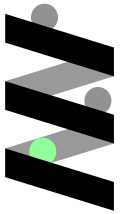


RSAConference2022

How to make this end-to-end confidential?

Our Open-Source Portfolio

EGo SDK



MarbleRun

EdgelessDB

EGo SDK

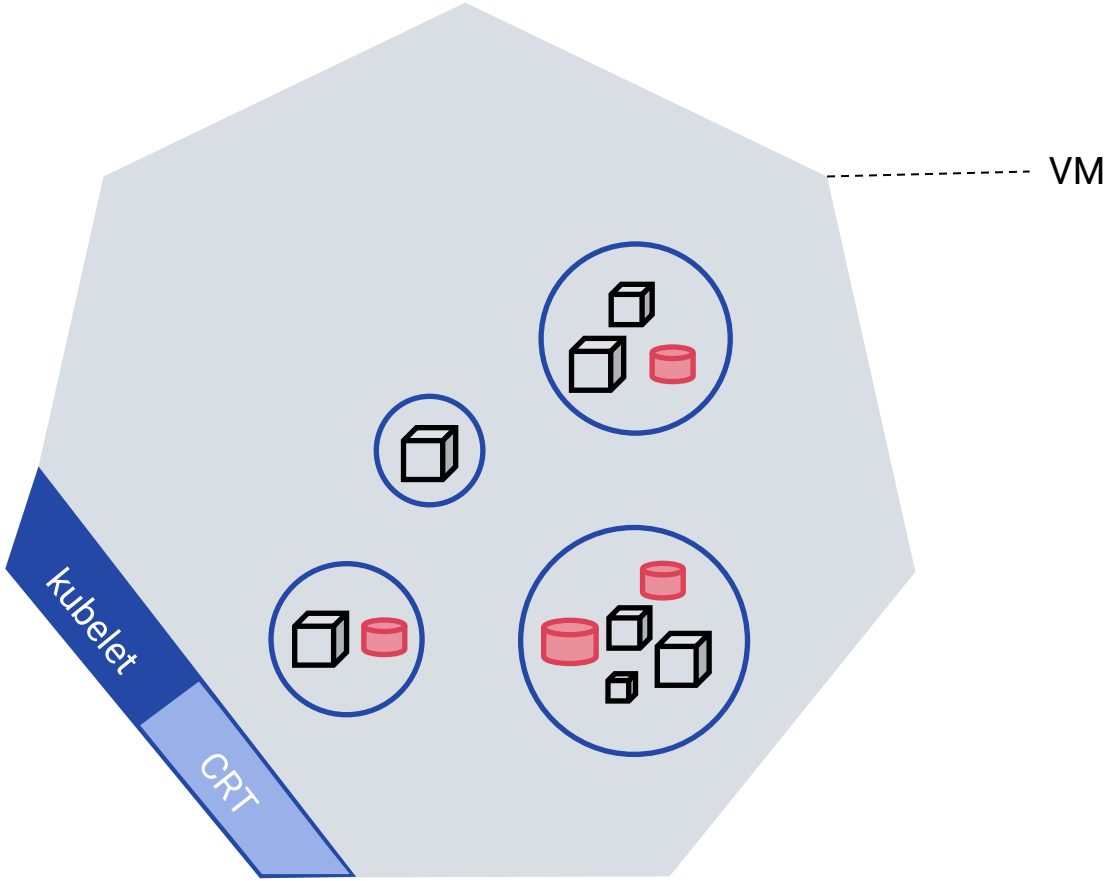
The easiest way to develop confidential apps

EGo in a Nutshell

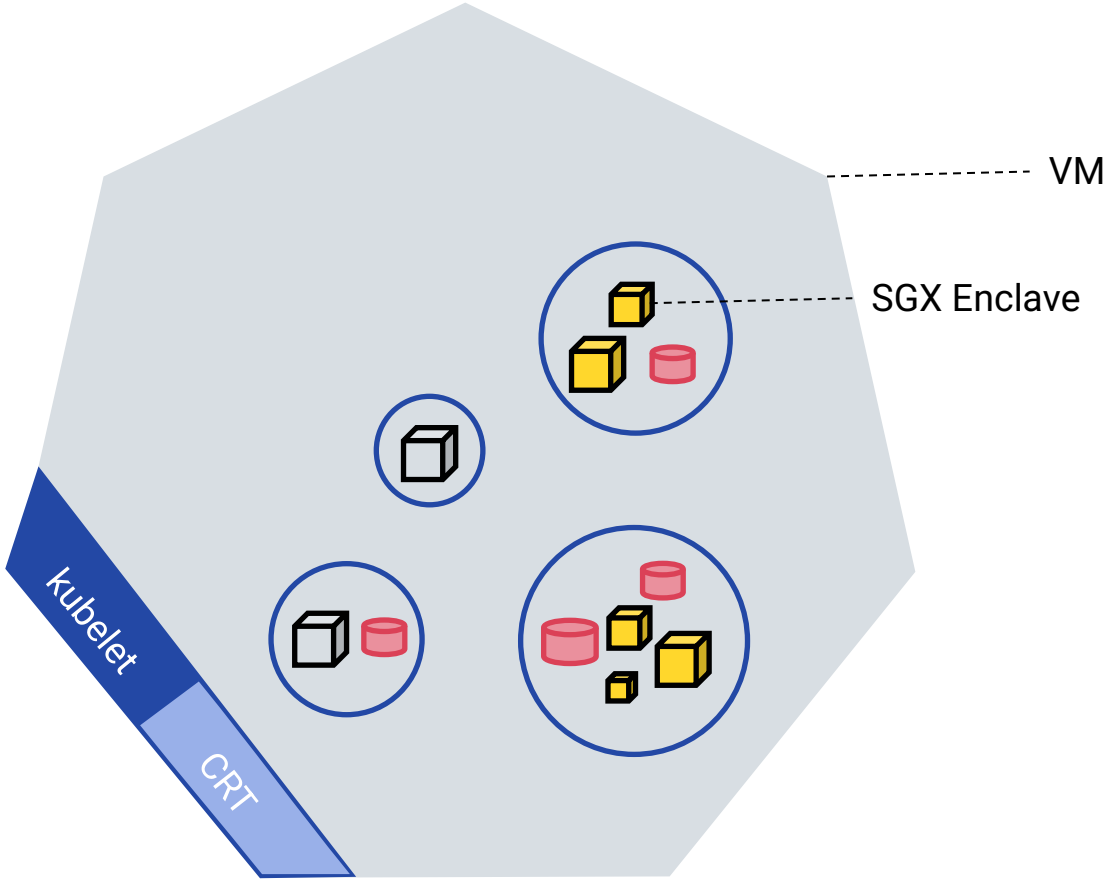
- Modified Go compiler
- SGX-specific tooling
- Inside-enclave and outside-enclave libraries

```
$ sudo snap install ego-dev --classic
$ ego-go build helloworld.go
$ ego sign helloworld
$ ego run helloworld
Loading enclave...
Entering enclave...
Hello from enclave!
```

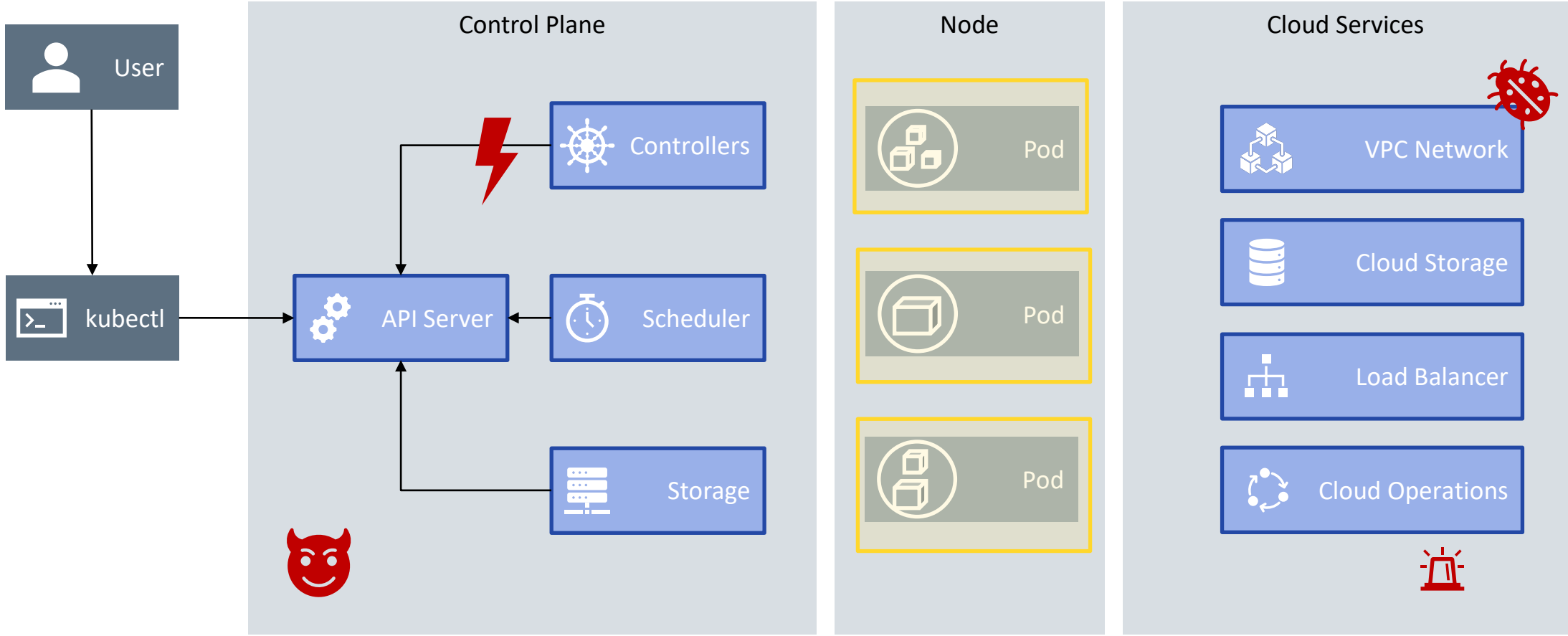
EGo Concept

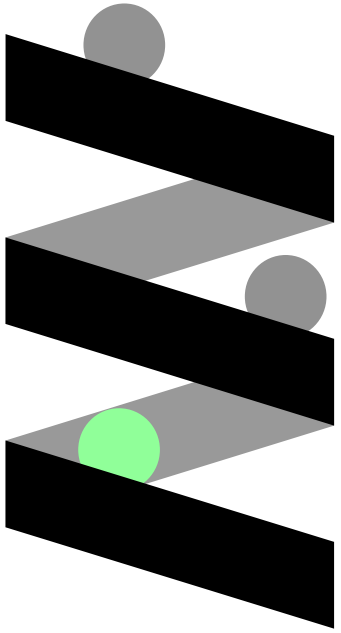


EGo Concept



Are we there yet? No…

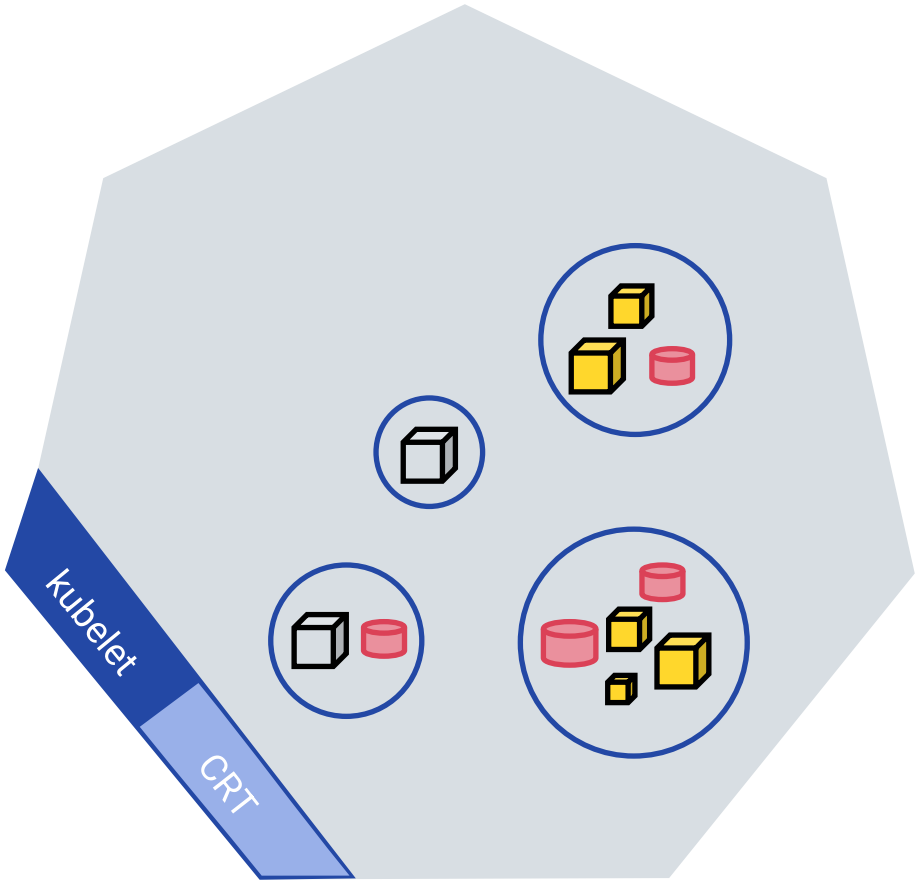


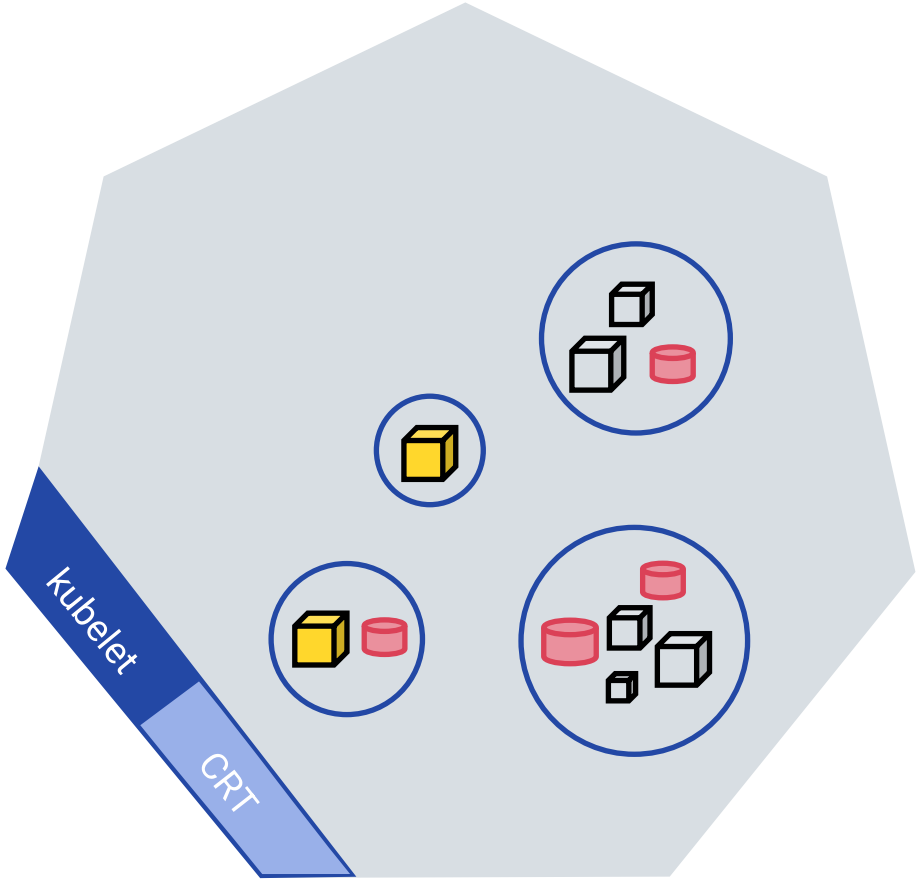


MarbleRun

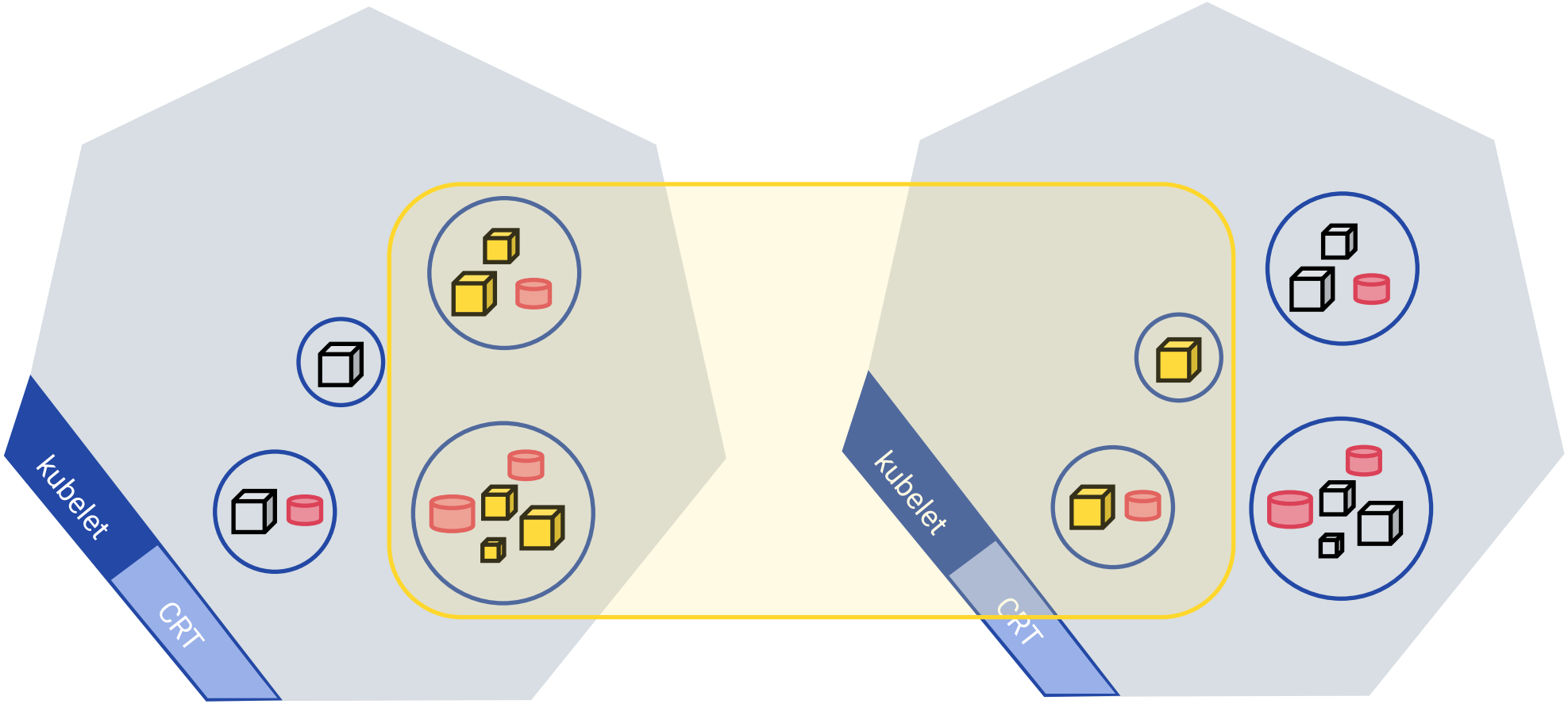
The control plane for scalable confidential apps

MarbleRun Concept

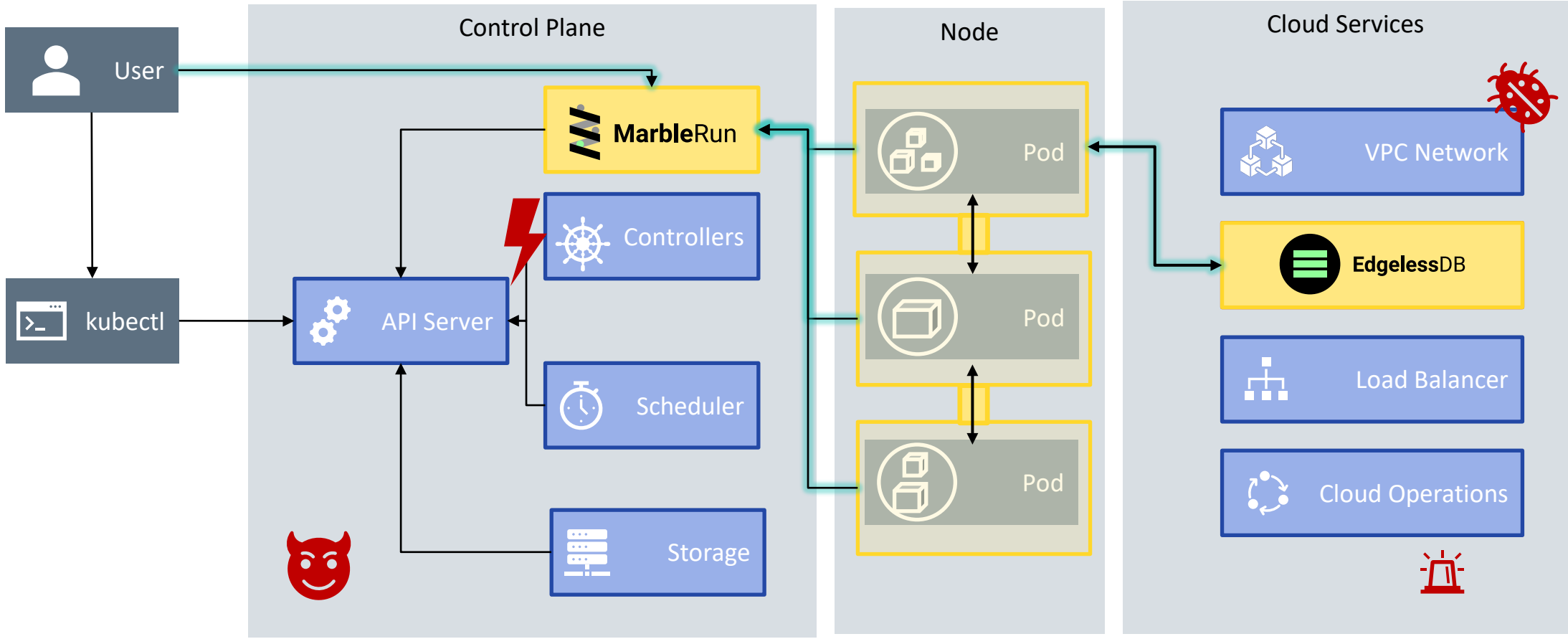




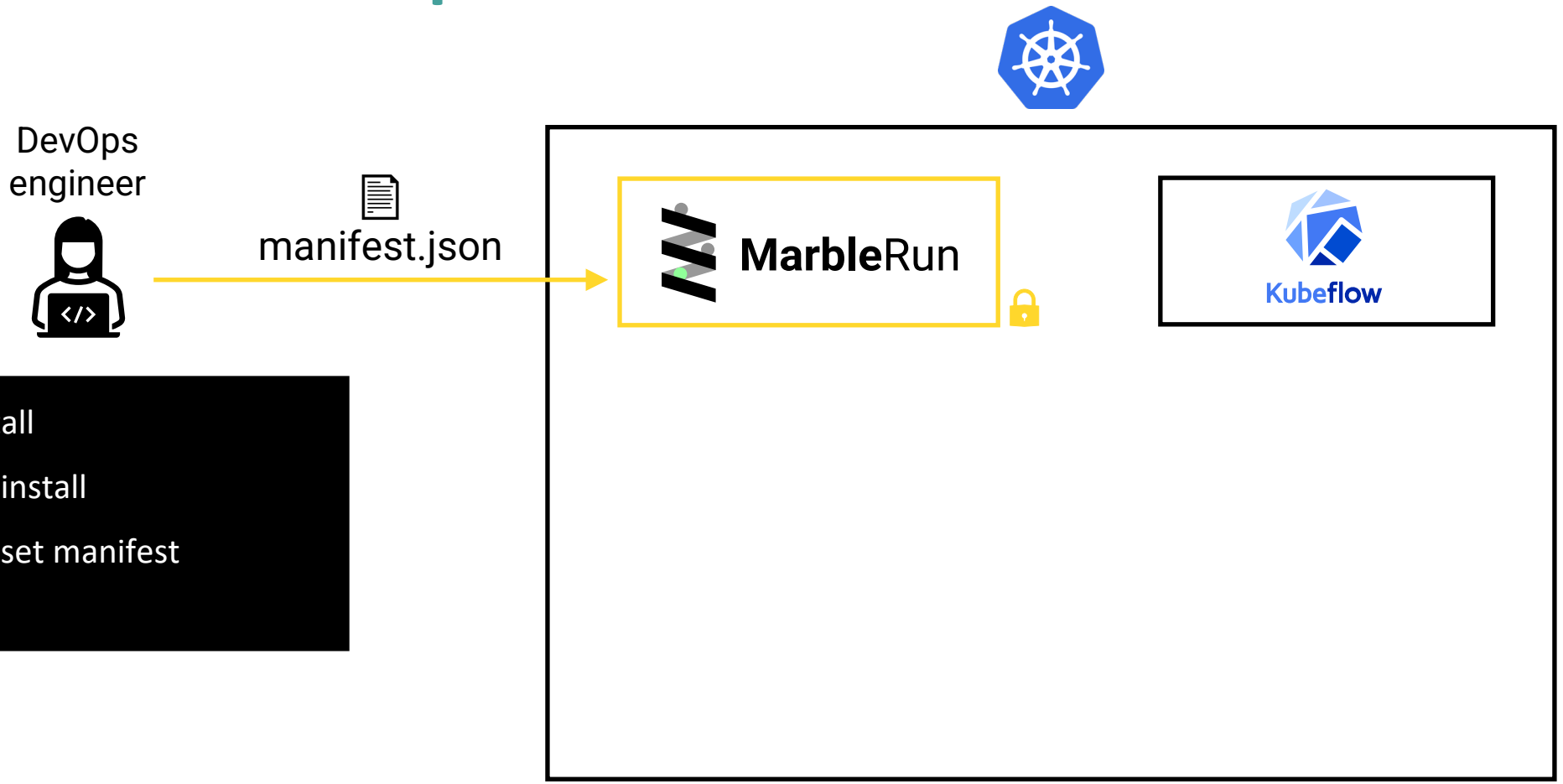
MarbleRun Concept



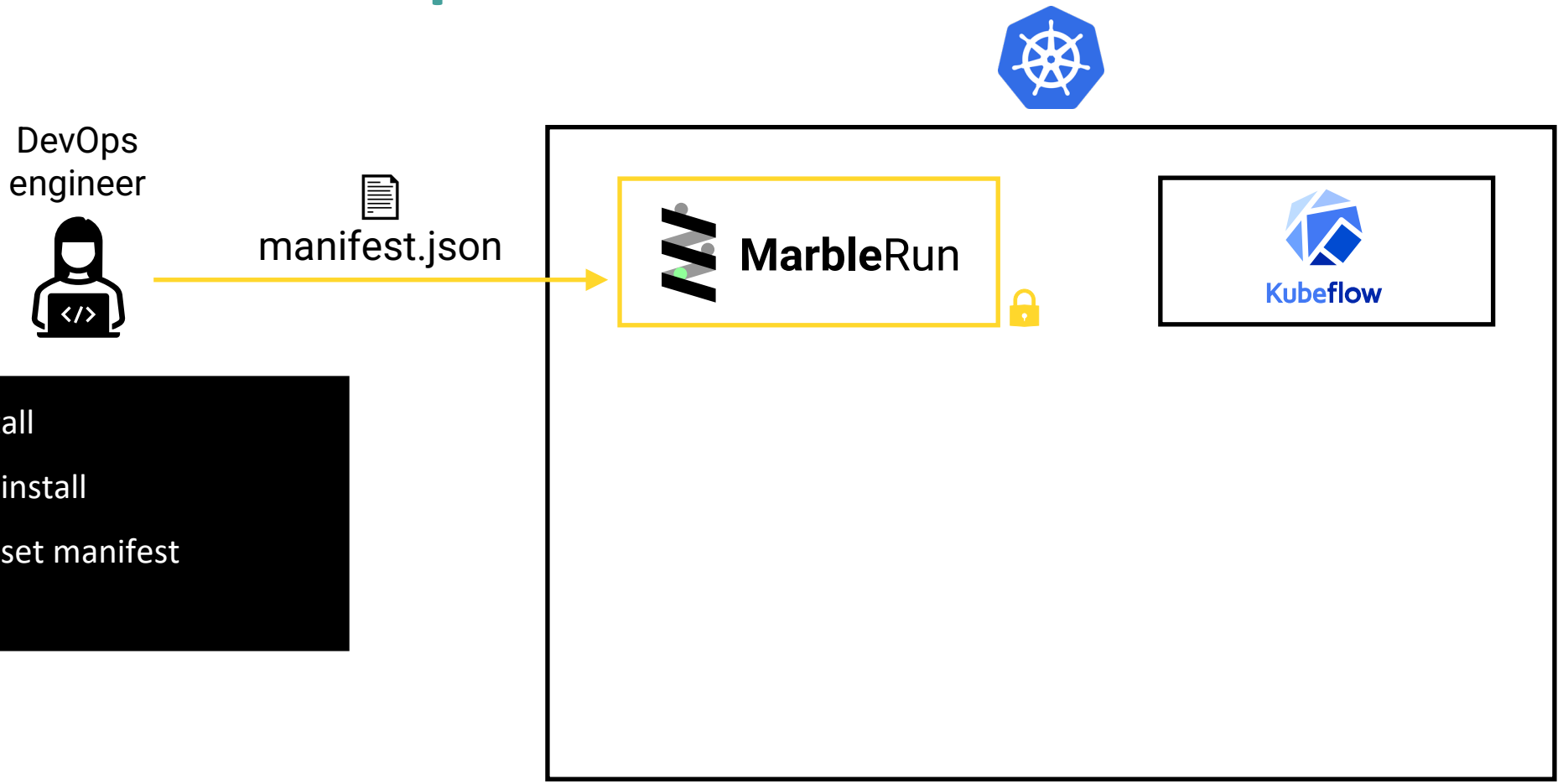
MarbleRun Concept



Confidential AI Pipeline



Confidential AI Pipeline

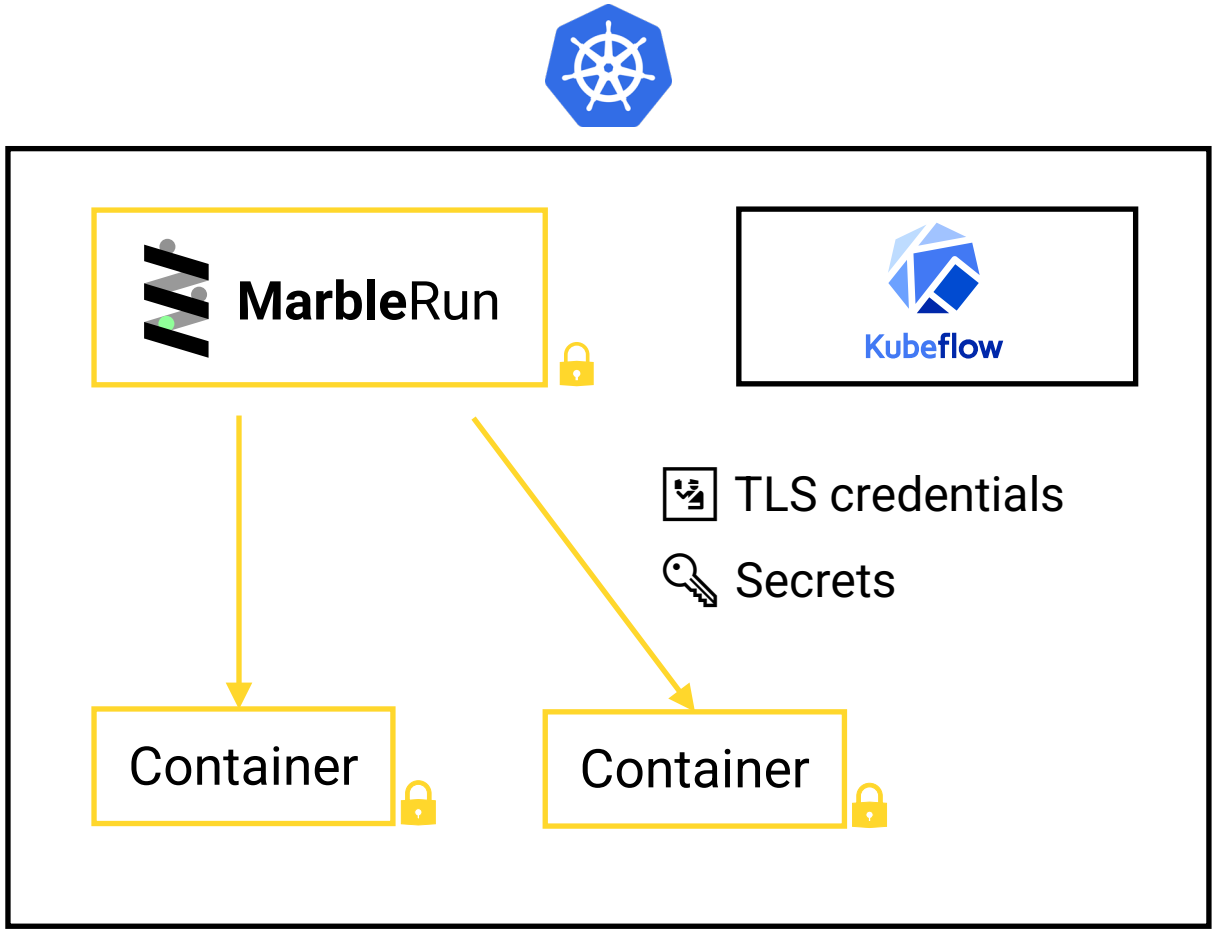



```
$ linkerd install
$ marblerun install
$ marblerun set manifest
```

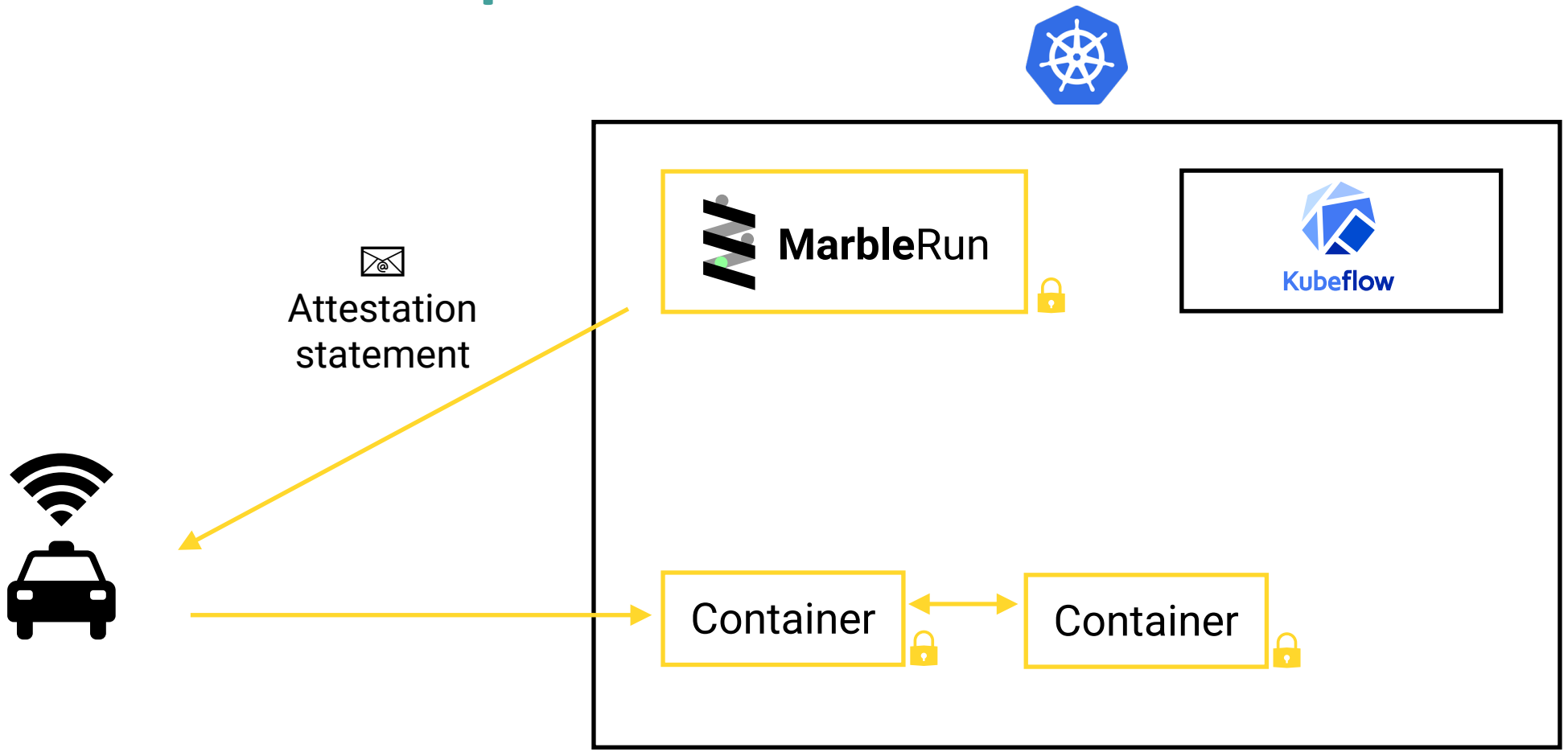
Confidential AI Pipeline

DevOps engineer

```
$ linkerd install
$ marblerun install
$ marblerun set manifest
$ helm install pipeline
```



Confidential AI Pipeline



Summary

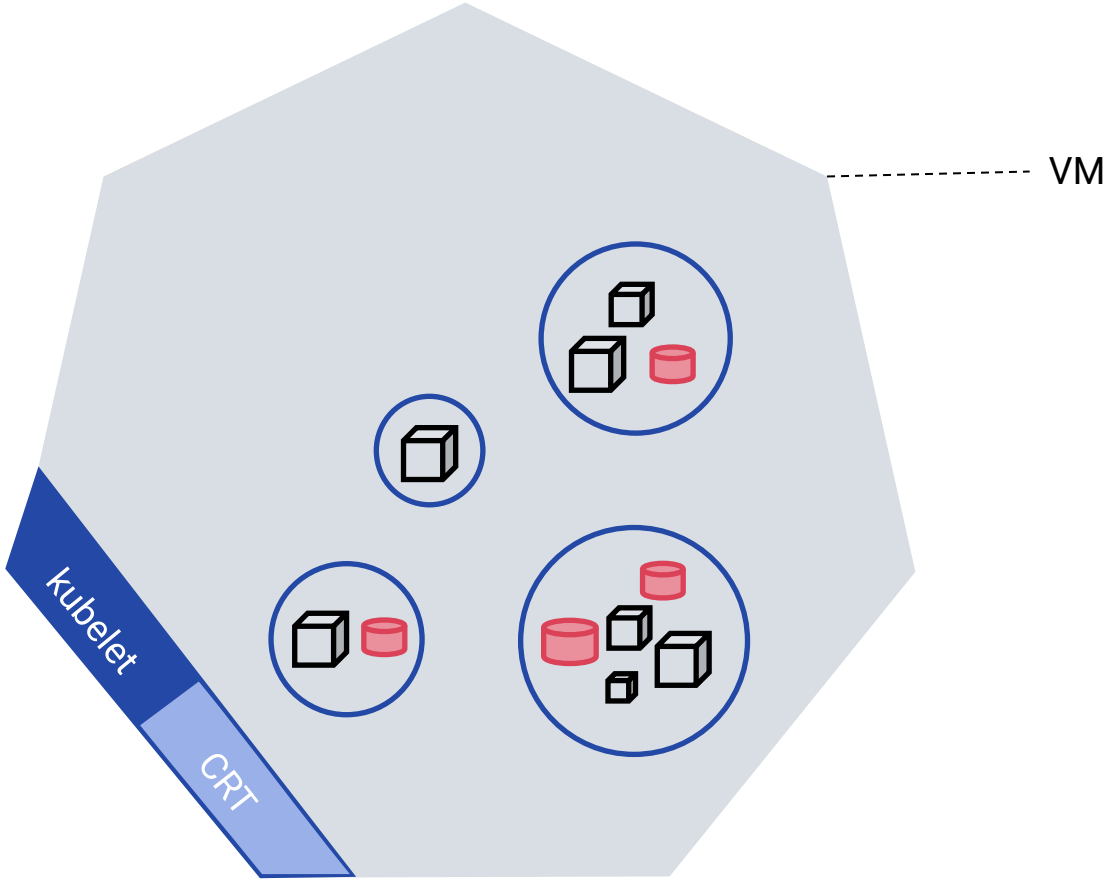
MarbleRun turns your deployment into a ✨confidential deployment✨

- Everything always encrypted
- Everything verifiable
- Protects against malicious admins, insiders, infrastructure, …
- Enables cool new privacy-preserving apps

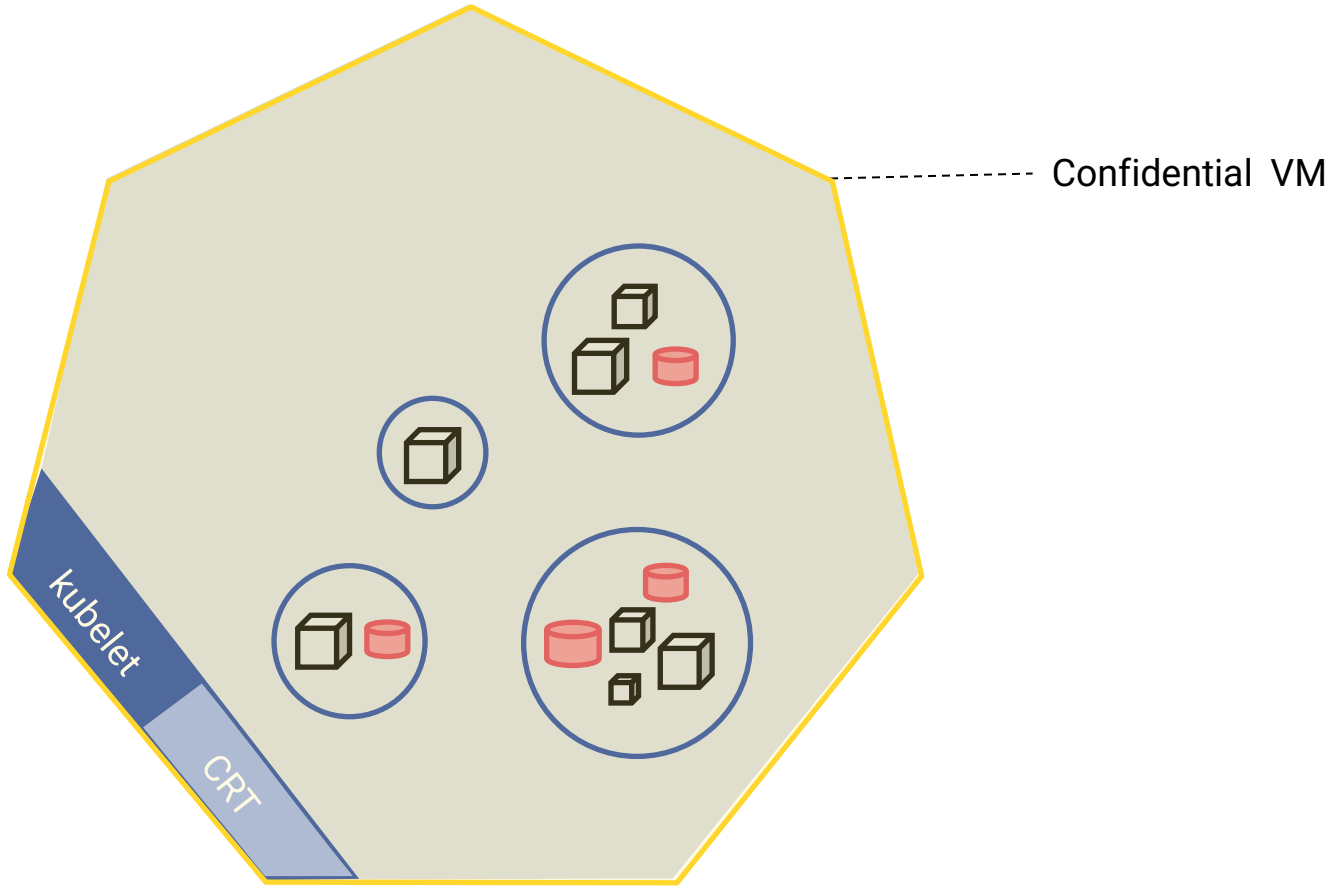
Constellation

The confidential Kubernetes distribution

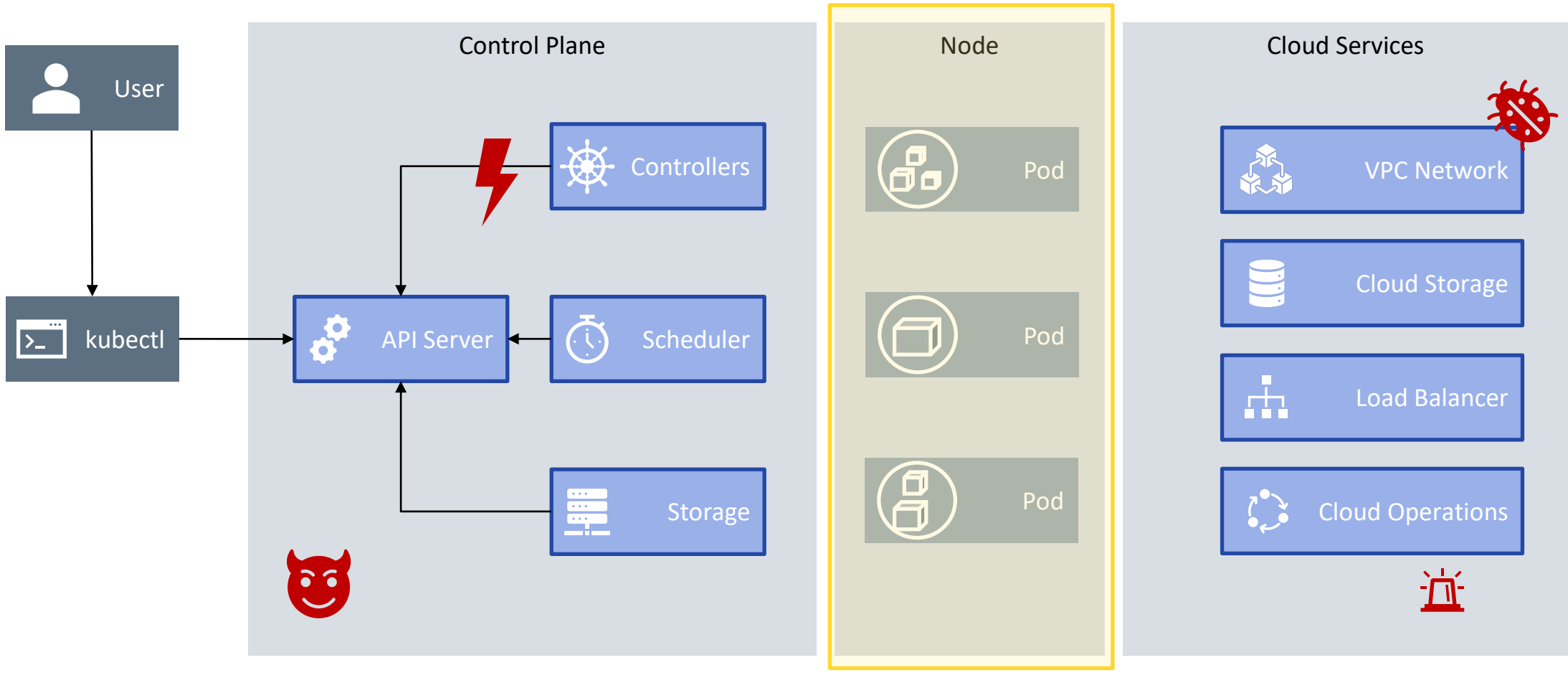
Confidential Kubernetes Nodes



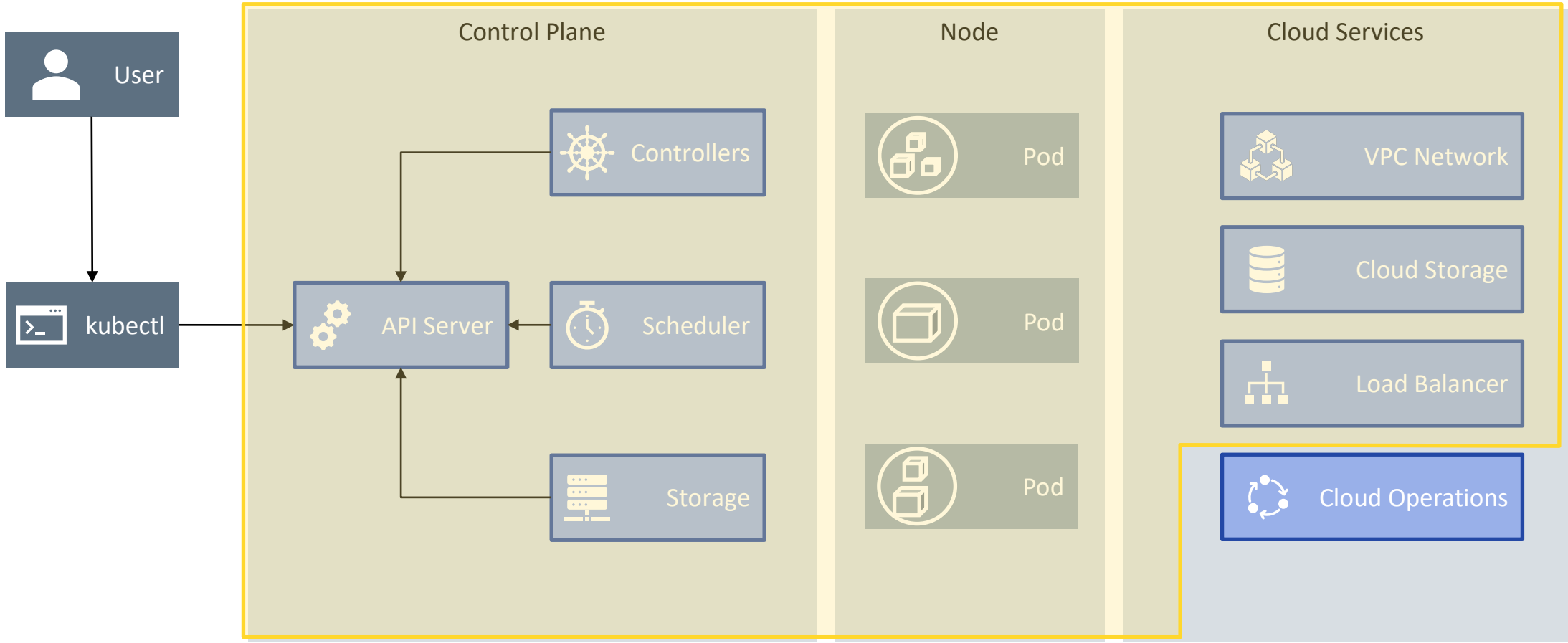
Confidential Kubernetes Nodes



Managed Kubernetes with CVMs



Constellation



Summary

Constellation turns your K8s cluster into a ✨confidential cluster✨

- Everything always encrypted and verifiable
- Run and scale any container-based service
- Protects against malicious admins, insiders, infrastructure, …
- Easy-to-use CLI
- Use Kubernetes as always `kubectl […]`

Summary

Tools for building confidential apps

EdgelessDB

MarbleRun

EGo SDK

Solution for lift & shift

Constellation

Apply

- Examples, docs, code, and Discord: https://edgeless.systems/
- Get in touch:
  - fs@edgeless.systems, me@edgeless.systems
  - @flxflx, @m1ghtym0

RSAConference2022

Let's Make the Cloud Confidential