KubeCon | CloudNativeCon
Europe 2022

# Confidential Containers Demystified

James Magowan, IBM
Samuel Ortiz, Apple

# A Panel…But Not a Panel

Initially supposed to be a panel format with:

Archana Shinde, Intel
Jiang Liu, Alibaba Cloud
Pradipta Banerjee, Red Hat

And ourselves…

# A Panel…But Not a Panel

Initially supposed to be a panel format with:

Archana Shinde, Intel
Jiang Liu, Alibaba Cloud
Pradipta Banerjee, Red Hat

And ourselves…

5 speakers, 5 time zones, one live pre-recording.
What could possibly go wrong?

# What You Will Learn

What is the confidential containers project?
How does it relate to confidential computing?
How does it protect Kubernetes workloads?
How can you use and deploy it?
What are the use cases?
What’s next for the project?

# What is the Confidential Containers Project?

# What is This Project?

A CNCF Sandbox project 🎉

https://github.com/confidential-containers

# What is This Project?

A CNCF Sandbox project 🎉

CONFIDENTIAL
CONTAINERS

https://github.com/confidential-containers

# What is This Project?

A CNCF Sandbox project 🎉

CONFIDENTIAL
CONTAINERS

A set of open source components to

- Seamlessly run k8s workloads in Confidential Computing enclaves
- Remove CSPs from the Trusted Computing Base (TCB)
- Support multiple Trusted Execution Environments (SEV, TDX, SE, SGX, etc)

https://github.com/confidential-containers

# What is This Project?

A CNCF Sandbox project 🎉

CONFIDENTIAL
CONTAINERS

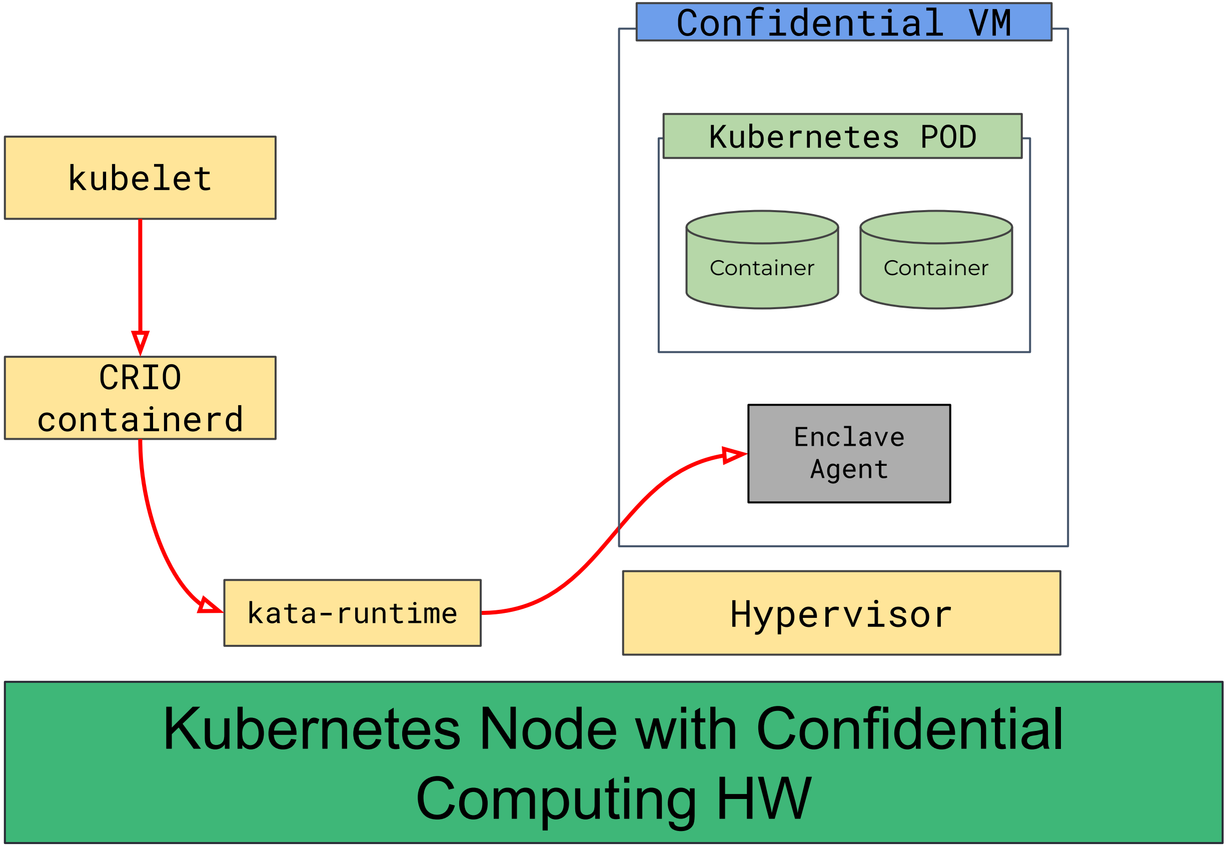
A set of open source components to

- Seamlessly run k8s workloads in Confidential Computing enclaves
- Remove CSPs from the Trusted Computing Base (TCB)
- Support multiple Trusted Execution Environments (SEV, TDX, SE, SGX, etc)

An open source community

- Cloud service providers - Alibaba, IBM
- Silicon vendors and TEE providers - AMD, ARM, IBM, Intel
- Open Source vendors - Red Hat

https://github.com/confidential-containers



kubelet

CRIO
containerd

kata-runtime

Confidential VM

Kubernetes POD

Container

Container

Enclave
Agent

Hypervisor

Kubernetes Node with Confidential Computing HW

# How Does it Relate to Confidential Computing?

# Cloud Native Confidential Computing

Each k8s pod gets its own confidential computing enclave

Each k8s pod memory, data, code and state is hardware encrypted

Each k8s pod runs its own enclave stack (firmware + kernel + initrd)

- The enclave stack is the confidential VM software stack
- The enclave stack is measured by the CC hardware
- The enclave stack can be verified through remote attestation

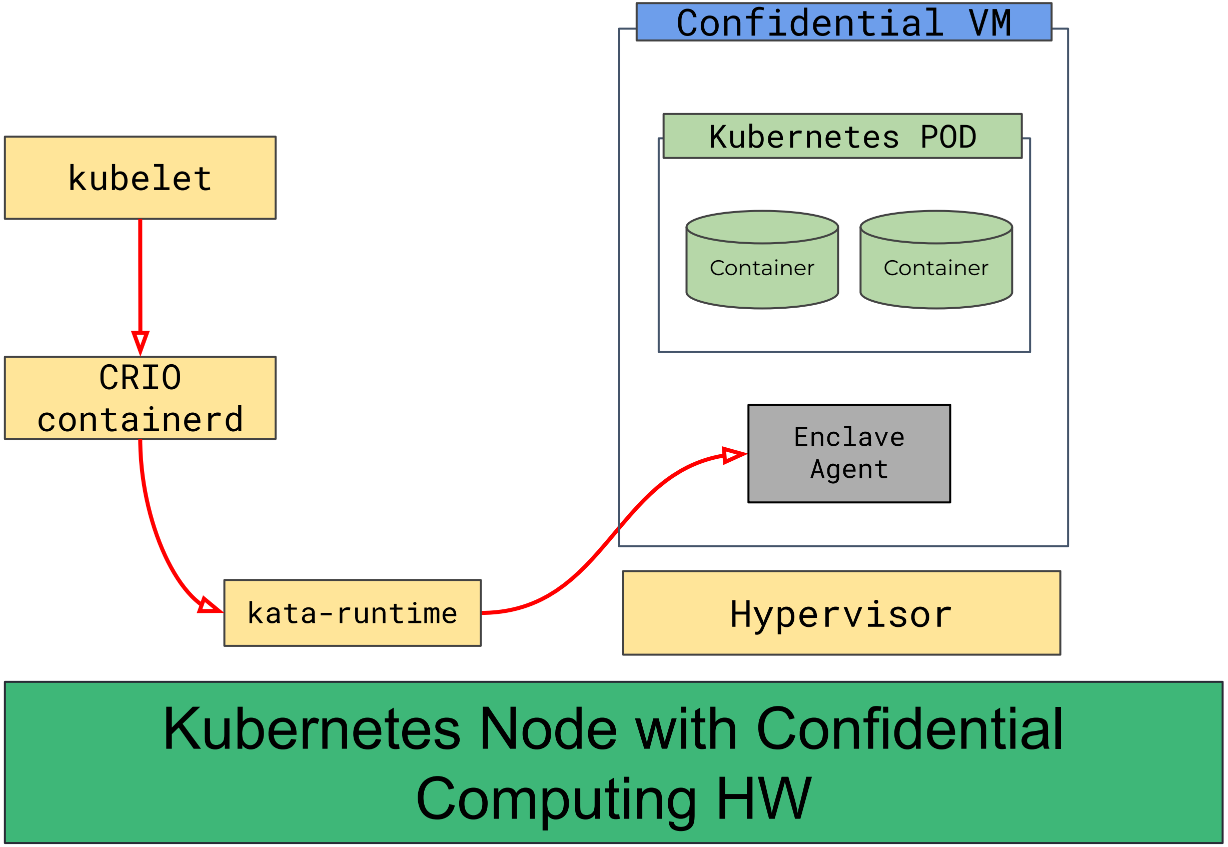
# Cloud Native Confidential Computing

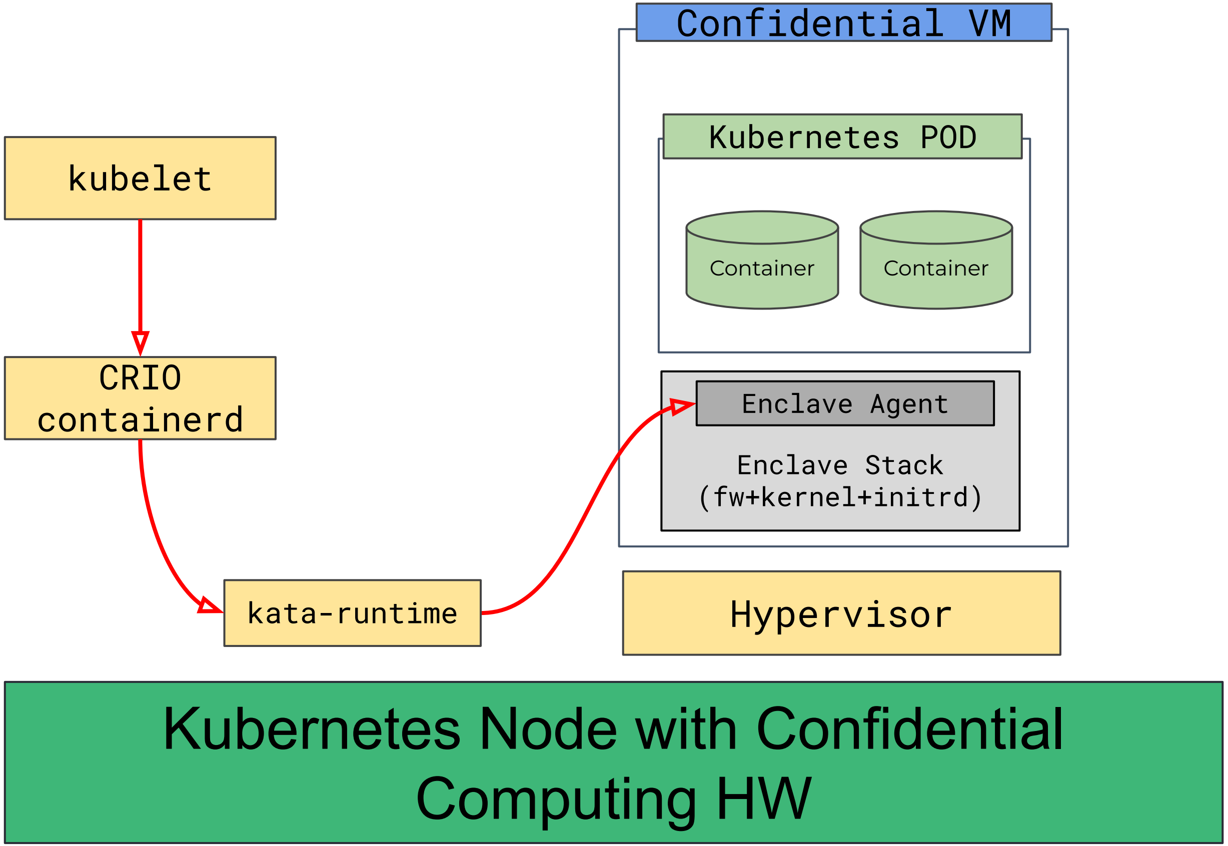
Each k8s pod gets its own confidential computing enclave
Each k8s pod memory, data, code and state is hardware encrypted
Each k8s pod runs its own enclave stack (firmware + kernel + initrd)

The enclave stack is the confidential VM software stack
The enclave stack is measured by the CC hardware
The enclave stack can be verified through remote attestation

A Confidential Containers k8s pod

Runs a measured and attested software stack
Runs with encrypted memory and HW state


kubelet
CRIO
containerd
kata-runtime
Confidential VM
Kubernetes POD
Container
Container
Enclave Agent
Hypervisor
Kubernetes Node with Confidential Computing HW



kubelet

CRIO
containerd

kata-runtime

Confidential VM

Kubernetes POD

Container

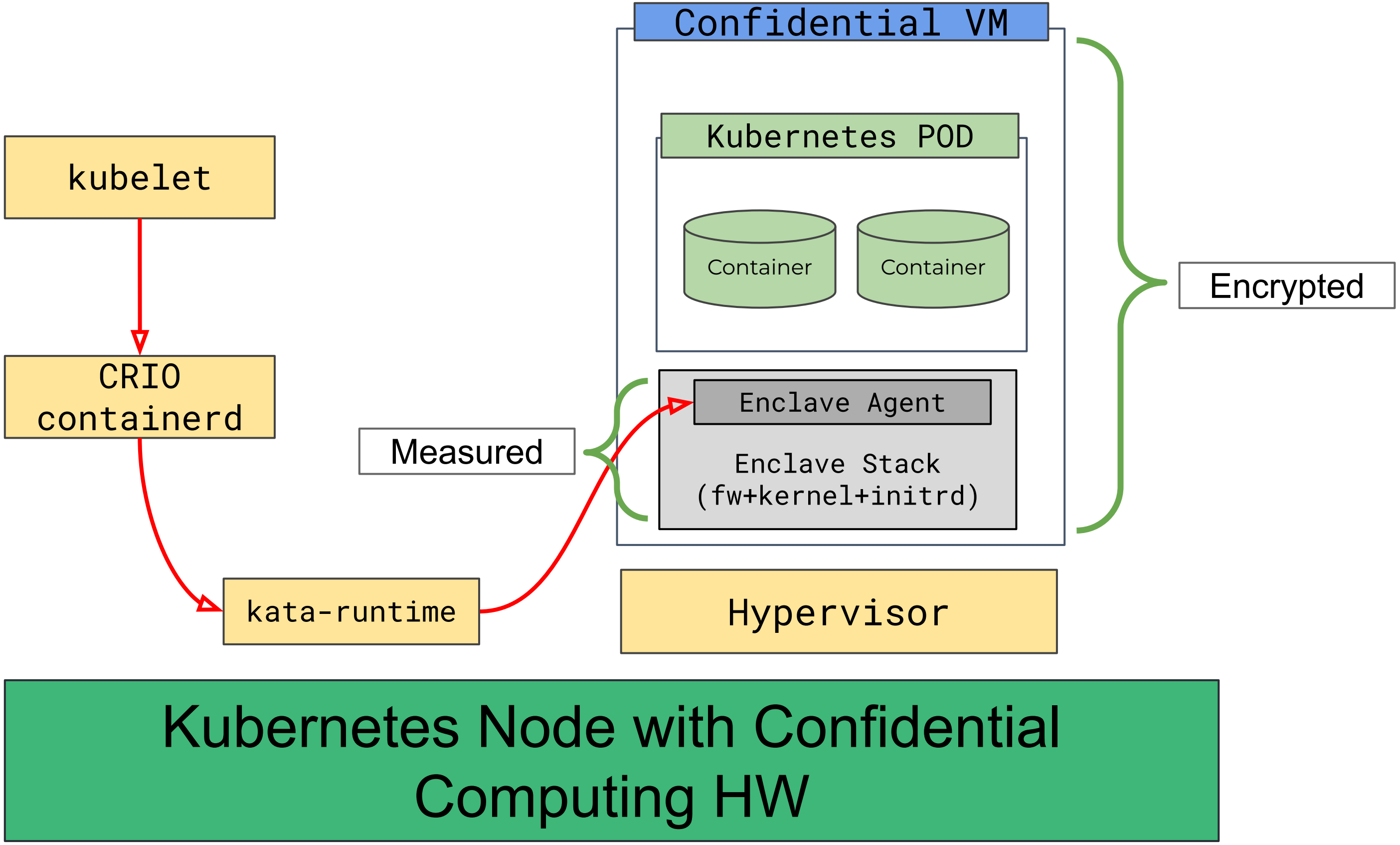
Container

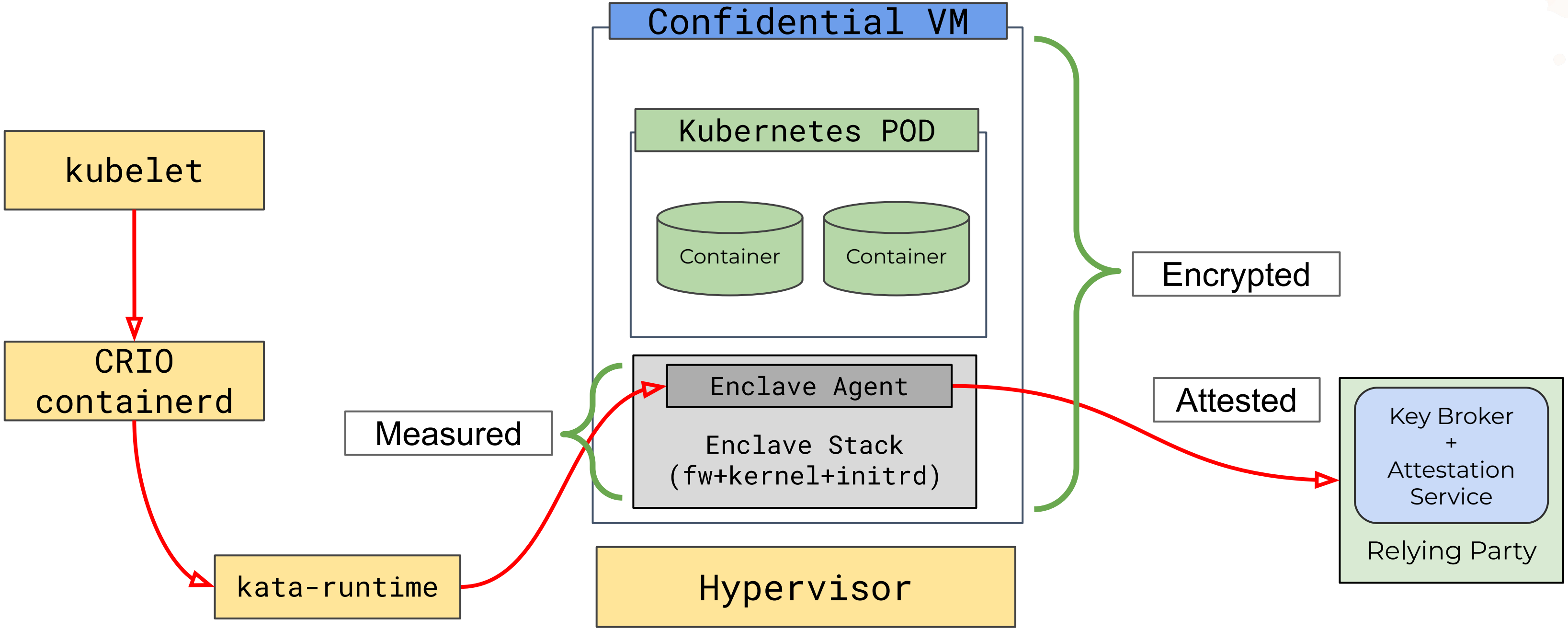
Enclave Agent

Enclave Stack
(fw+kernel+initrd)

Hypervisor

Kubernetes Node with Confidential Computing HW


kubelet
CRIO
containerd
kata-runtime
Measured
Confidential VM
Kubernetes POD
Container
Container
Enclave Agent
Enclave Stack
(fw+kernel+initrd)
Encrypted
Hypervisor
Kubernetes Node with Confidential Computing HW



Kubernetes Node with Confidential Computing HW

# How Does it Protect Kubernetes Workloads?

# Horizontal and Vertical Protection

Confidential Containers take the host out of the trust boundary

# Horizontal and Vertical Protection

Confidential Containers take the host out of the trust boundary

Hardware Encryption

- The host can not see or tamper with the workload data and HW state

# Horizontal and Vertical Protection

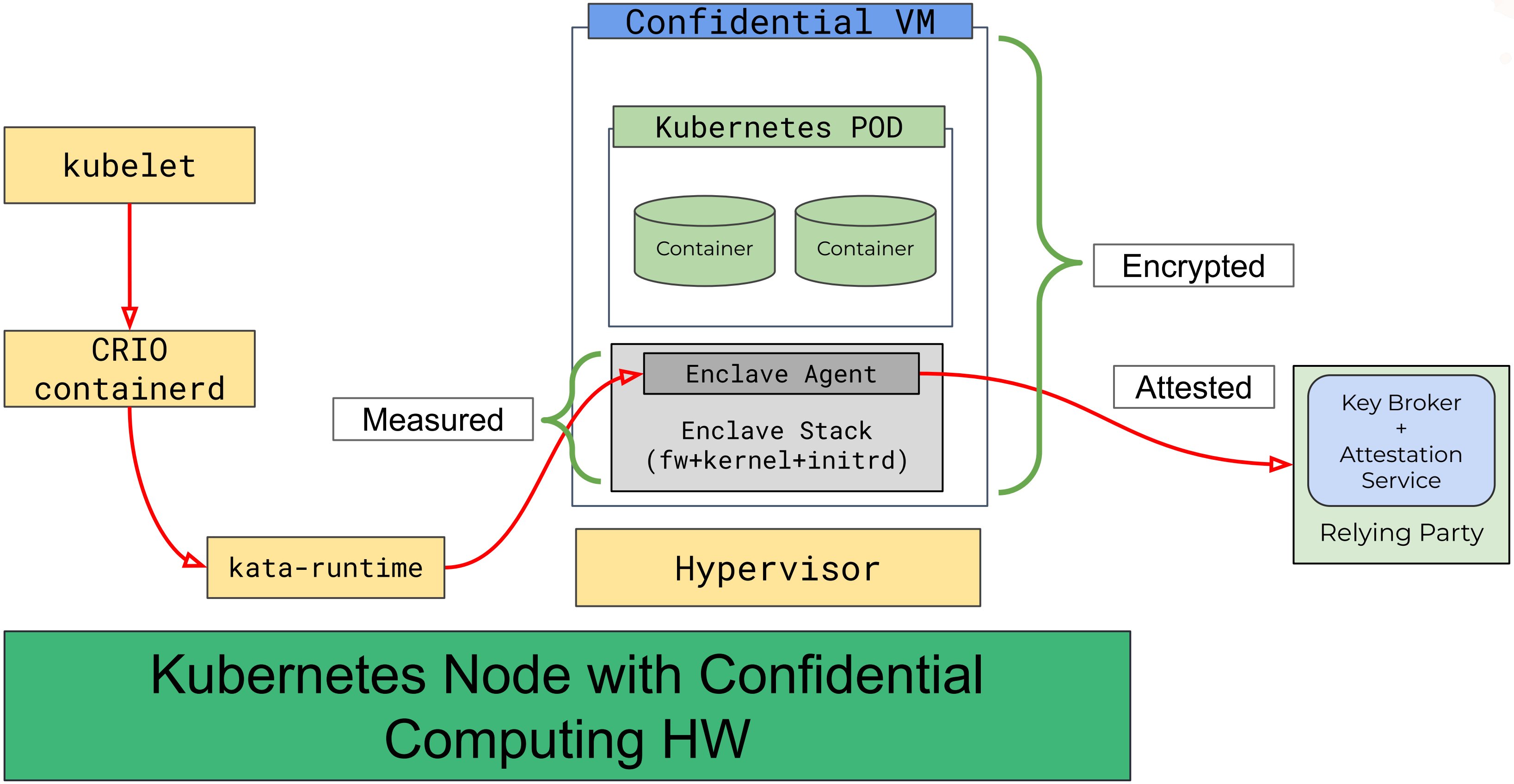
Confidential Containers take the host out of the trust boundary

Hardware Encryption

- The host can not see or tamper with the workload data and HW state

Measurement and Attestation

- The guest runs a verified and trusted enclave stack
- The trusted enclave pulls and runs encrypted containers images
- Pod container images no longer belong to the host
- The host can not see or tamper with the pod container images



Confidential VM

Kubernetes POD

Container

Container

Enclave Agent

Enclave Stack (fw+kernel+initrd)

Encrypted

Measured

Attested

kubelet

CRIO containerd

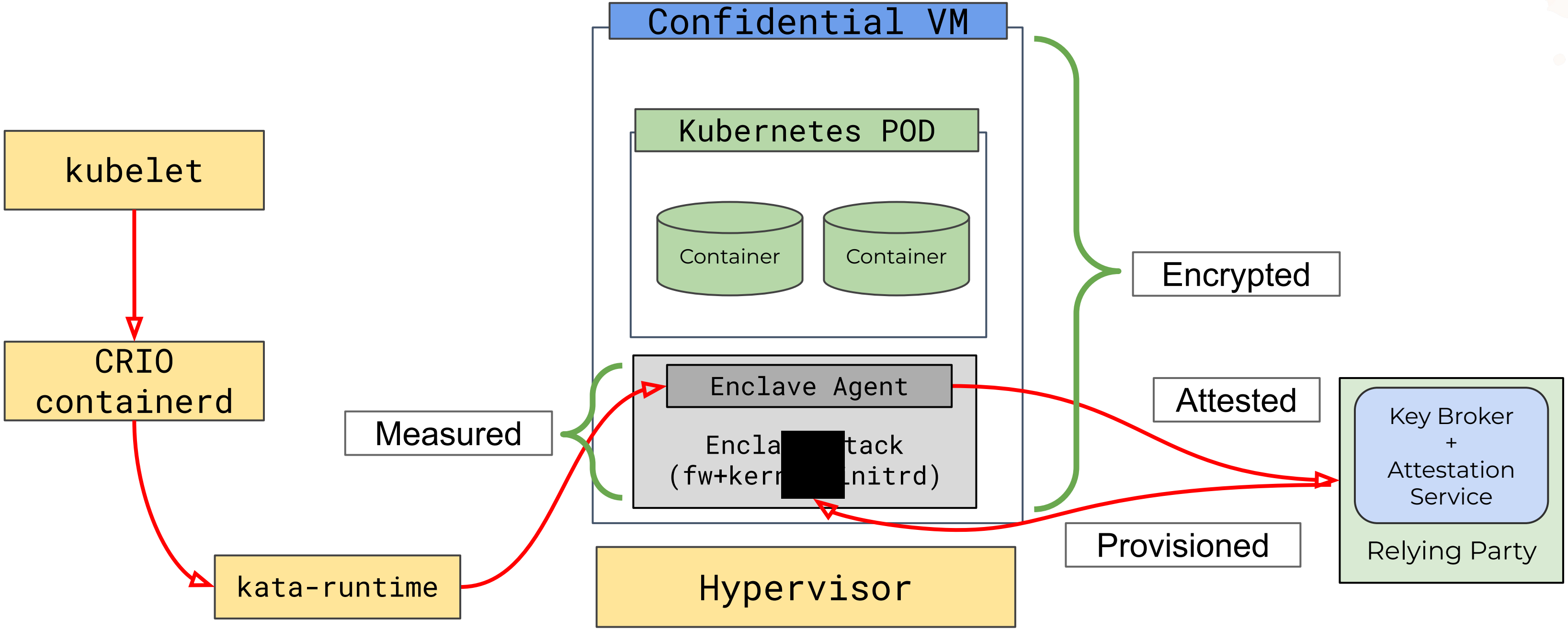
kata-runtime

Hypervisor

Key Broker + Attestation Service

Relying Party

Kubernetes Node with Confidential Computing HW



kubelet

CRIO
containerd

kata-runtime

Measured

Confidential VM

Kubernetes POD

Container

Container

Enclave Agent

Encla[redacted]tack
(fw+ker nitrd)

Hypervisor

Encrypted

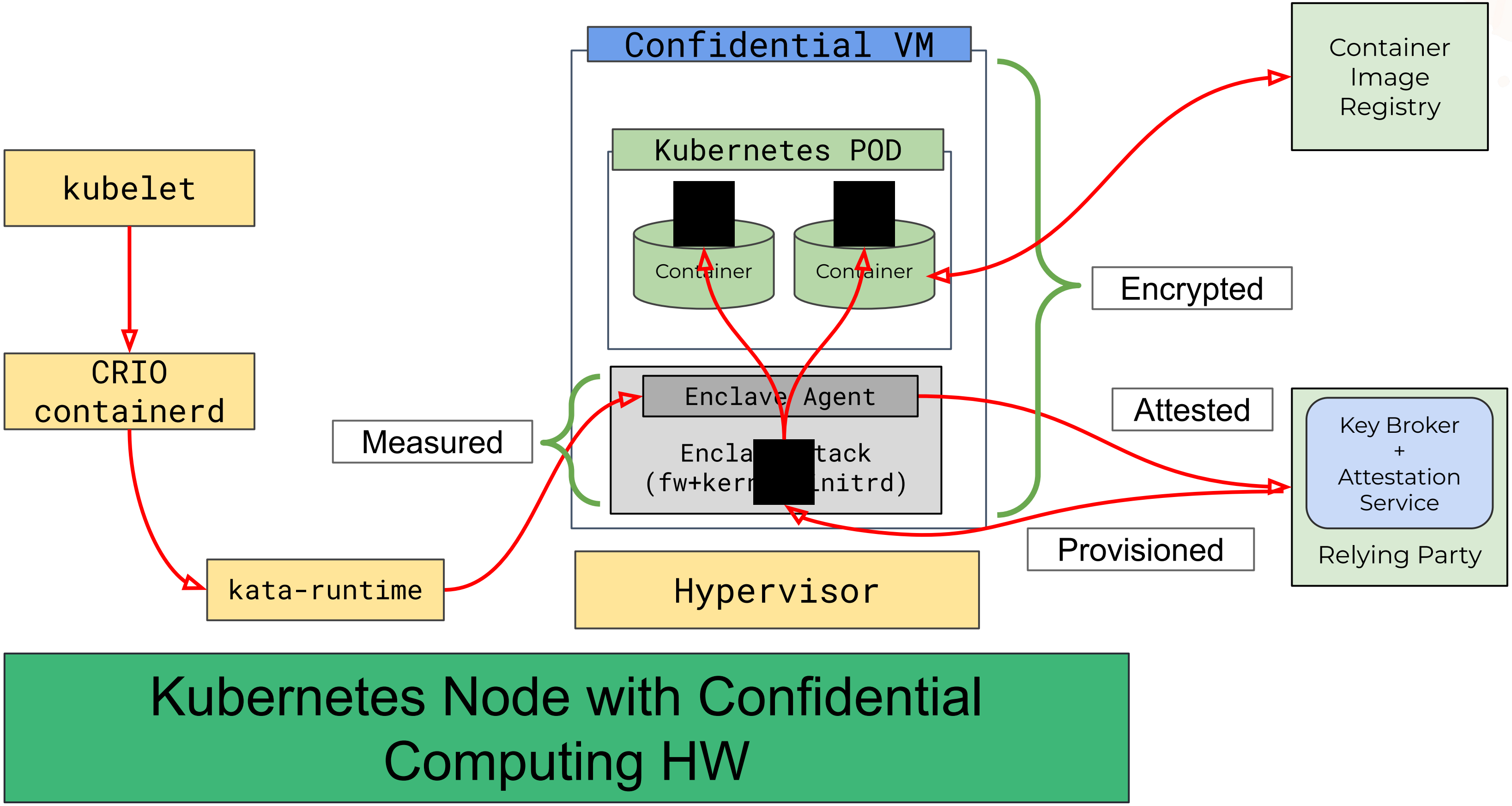
Attested

Provisioned

Key Broker
+
Attestation
Service

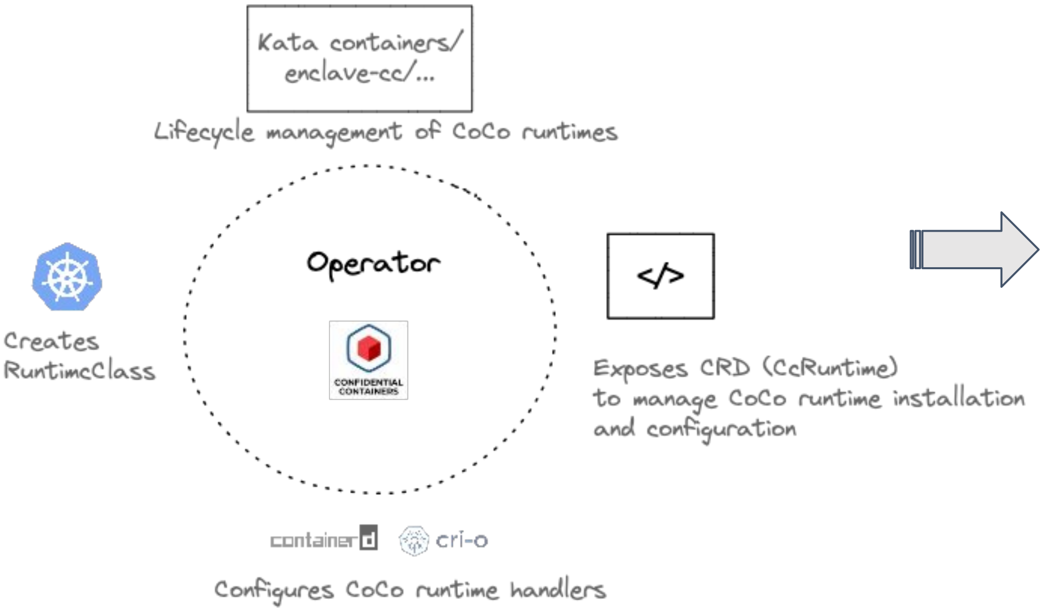
Relying Party

# Kubernetes Node with Confidential Computing HW


Confidential VM
Kubernetes POD
[redacted]
[redacted]
Container
Container
Enclave Agent
Encla[redacted]tack
(fw+kern nitrd)
Hypervisor
kubelet
CRIO
containerd
kata-runtime
Measured
Encrypted
Attested
Provisioned
Container Image Registry
Key Broker + Attestation Service
Relying Party
Kubernetes Node with Confidential Computing HW

# How Can You Use and Deploy Confidential Containers?

# Kubernetes Operator and Custom Resource



Kata containers/ enclave-cc/...

Lifecycle management of CoCo runtimes

Creates RuntimeClass

Operator

Exposes CRD (CcRuntime) to manage CoCo runtime installation and configuration

Configures CoCo runtime handlers

```
apiVersion: confidentialcontainers.org/v1beta1
kind: CcRuntime
metadata:
  name: ccruntime-kata
  namespace: confidential-containers-system
spec:
  runtimeName: kata
  ccNodeSelector:
    matchLabels:
      node-role.kubernetes.io/worker: ""
  config:
    installType: bundle
    payloadImage:
https://quay.io/confidential-containers/runtime-payload:v0
…
```

https://github.com/confidential-containers/operator

# What are the Use Cases For Confidential Containers?

# Use Cases

- Infrastructure owner no longer sees workloads data
- Seamlessly run sensitive workloads **anywhere**
  - Confidential databases
  - AI inference
  - Finance, Medical, all regulated workloads
- Move workloads from private to public clouds
  - **Any** public cloud with confidential computing support

# What’s Next for Confidential Containers?