CONFIDENTIAL
CONTAINERS

KubeCon | CloudNativeCon

Europe 2023

Confidential Containers Made Easy

Fabiano Fidêncio (Intel, fabiano.fidencio@intel.com)
Jens Freimann (Red Hat, jfreimann@redhat.com)

Agenda

Agenda

- Confidential Containers in a Nutshell
- Basics: Kata Containers
- From Kata to Confidential Containers
- Different flavours of Confidential Containers
- Use Cases for Confidential Containers
- Demos

Confidential Containers in a Nutshell

Confidential Containers in a Nutshell

This is an umbrella project, which has its **Operator** as the project's front door

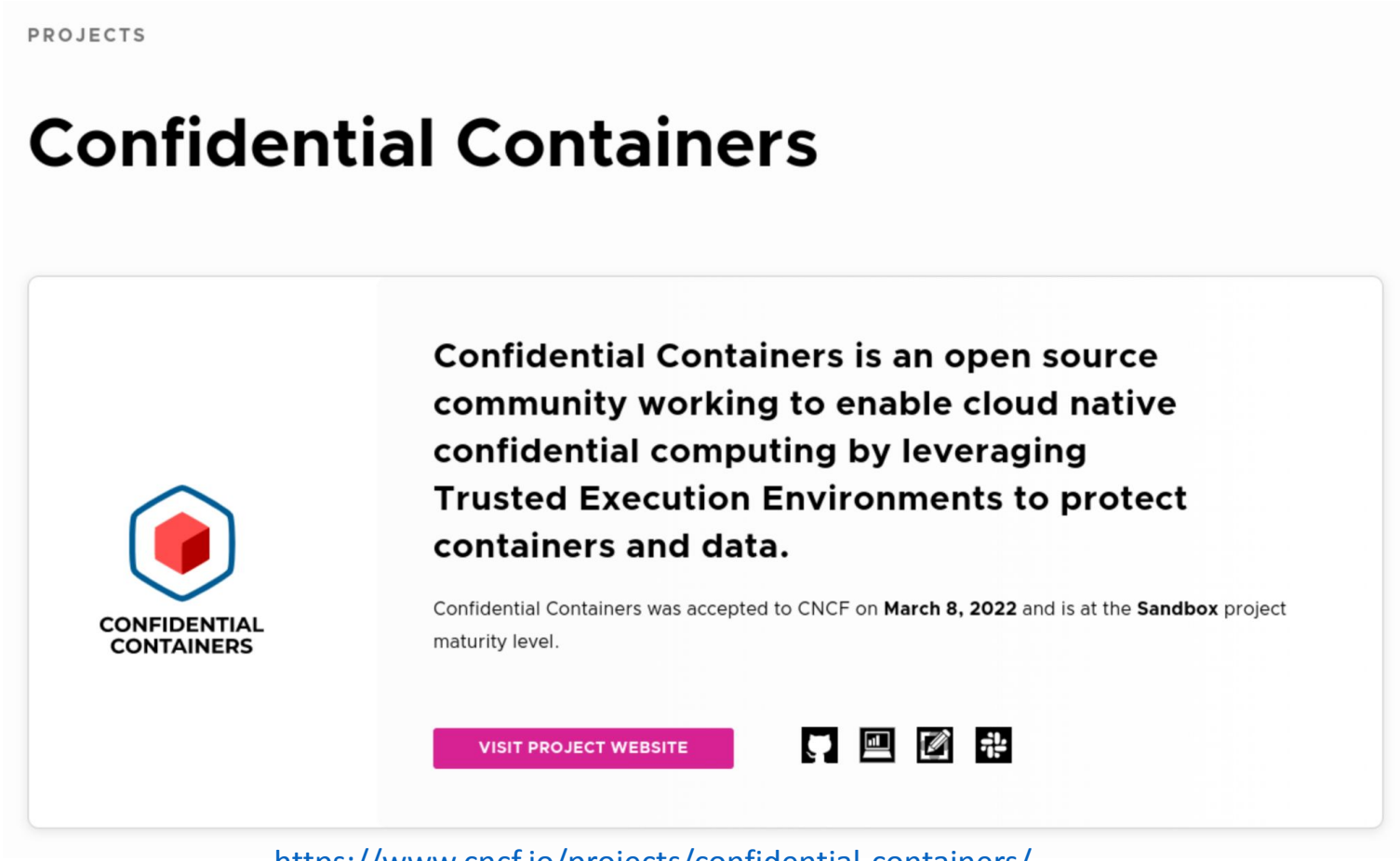
Apart from the Operator, we also develop:

- A key broker service
- An attestation agent and an attestation service
- A lightweight firmware for the Confidential Containers VMs (td-shim)
- Rust libraries for pulling, decrypting, and encrypting images (image-rs and ocicrypt-rs)
- Different flavours of Confidential Containers (cloud-api-adaptor, enclave CC)
- Have a strong relationship with Kata Containers

Confidential Containers in a Nutshell

Cloud Native Computing Foundation member

- Since March 8th, 2022



https://www.cncf.io/projects/confidential-containers/

Confidential Containers in a Nutshell

Community members

- Alibaba Cloud
- AMD
- ARM
- IBM
- Intel
- Microsoft
- NVIDIA
- Red Hat
- RivOS
- and others … :-)

Confidential Containers in a Nutshell

What is the value proposition of Confidential Containers?

Protect **data-in-use**, at the **pod level**, by leveraging **Trusted Execution Environments (TEE)**

- Simplify TEE technology usage for cloud native software with Confidential Containers
- Enforce security requirements and transparent deployment of unmodified containers
- Support multiple TEE and hardware platforms
- Separate Cloud Service Providers from guest applications, following least privilege principles for Kubernetes administration

Confidential Containers in a Nutshell

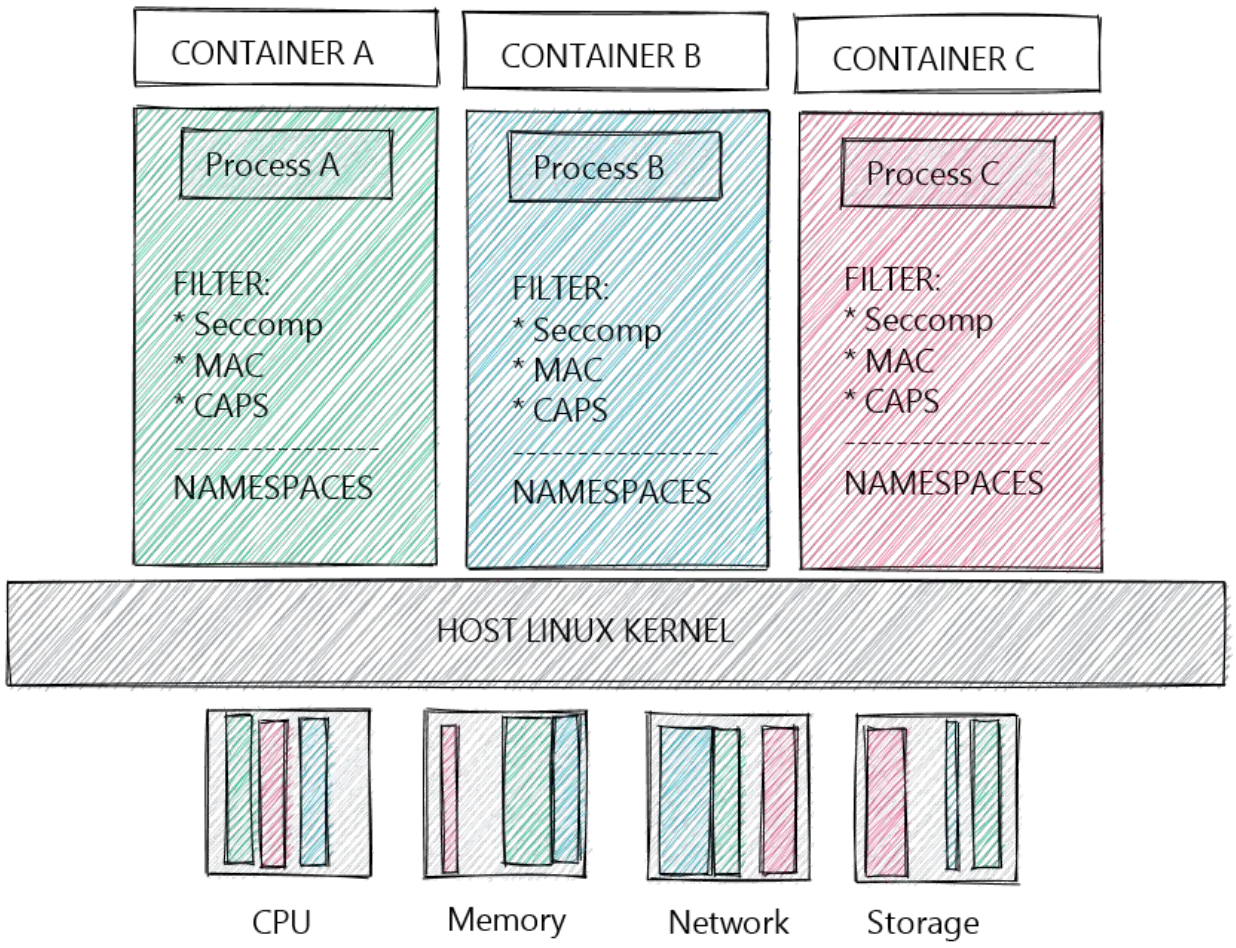
The project focuses on protecting …

- Hold on! Let's talk about it a little bit later!

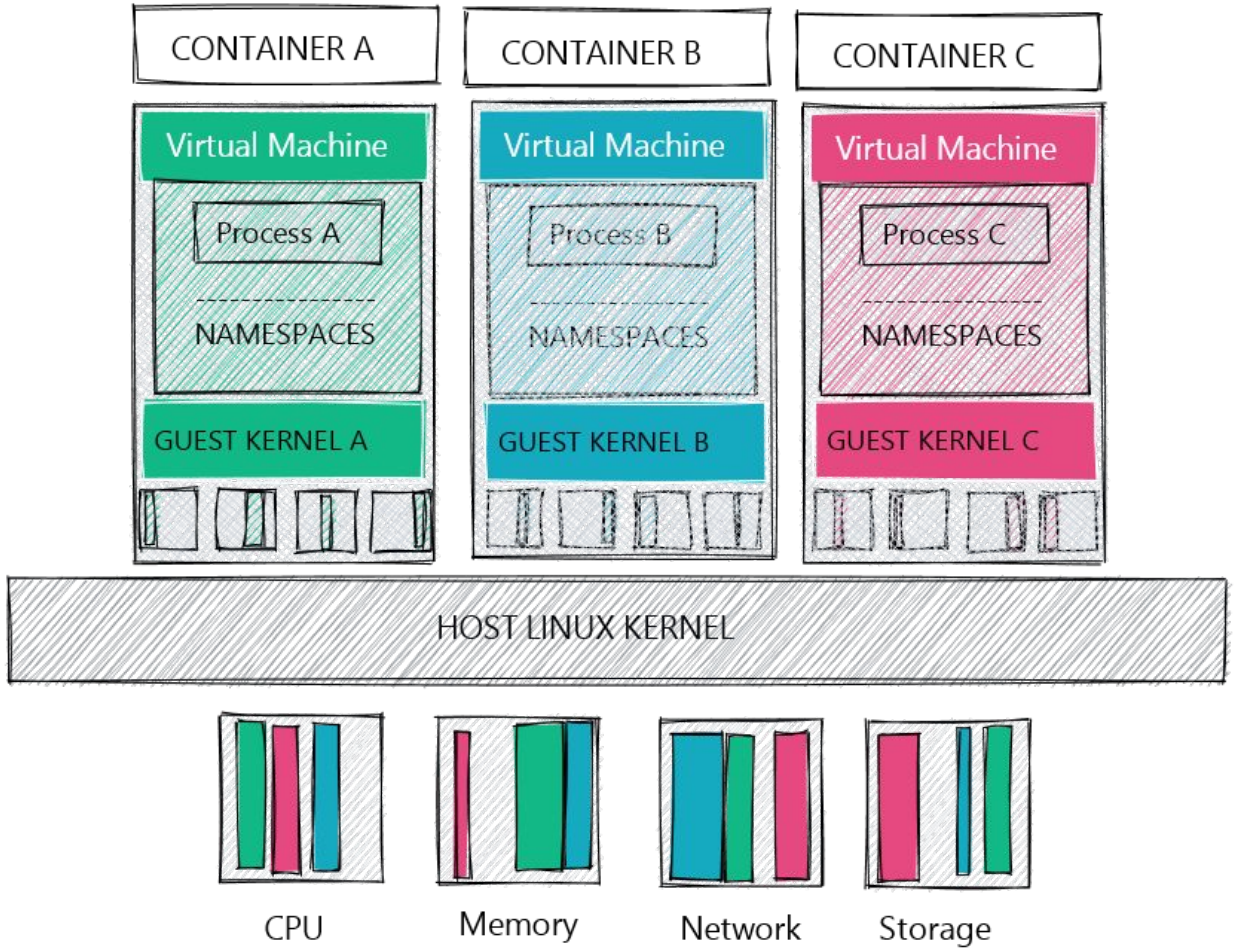
Basics: Kata Containers

Basics: Kata Containers

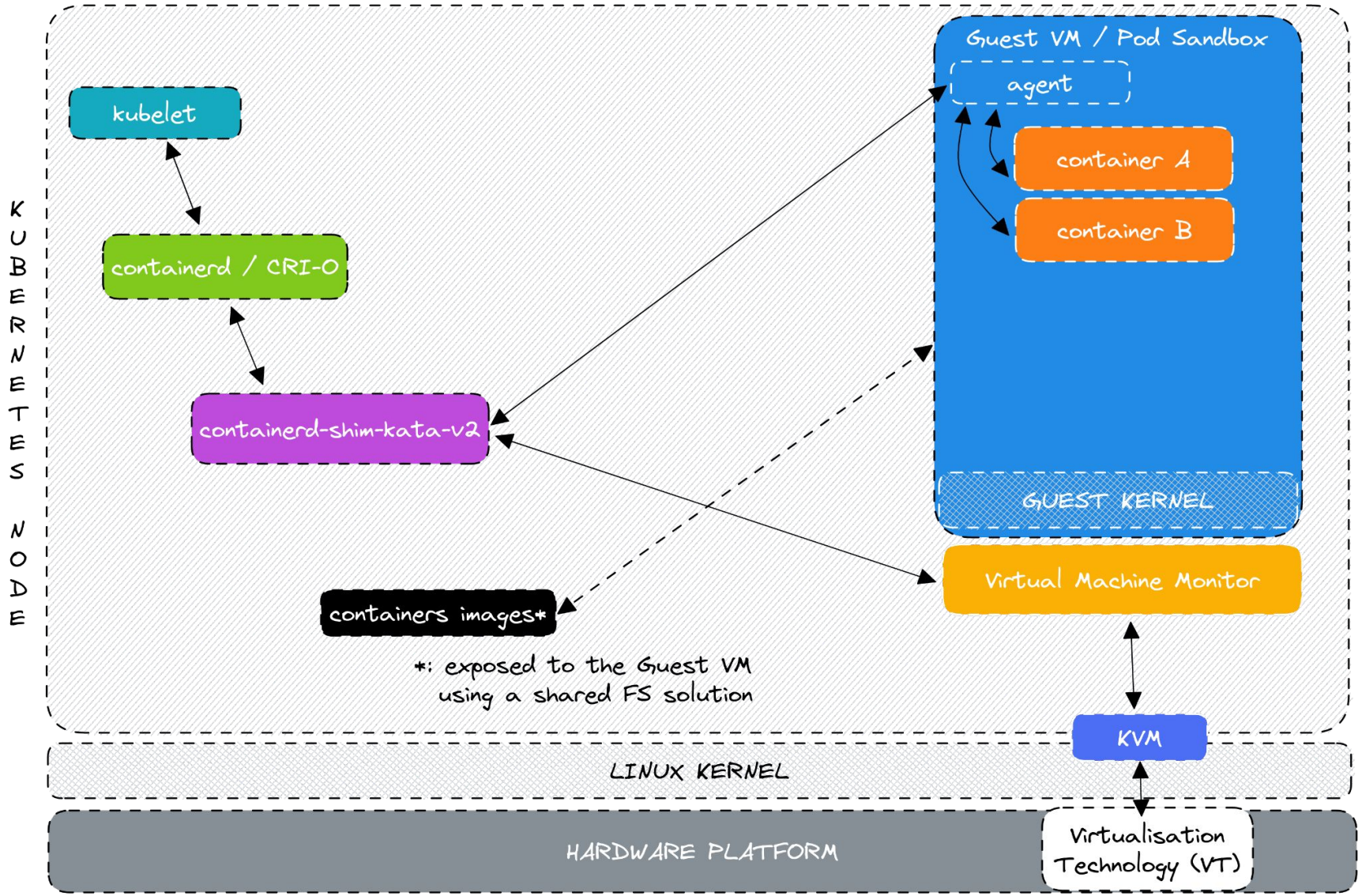
Traditional Containers



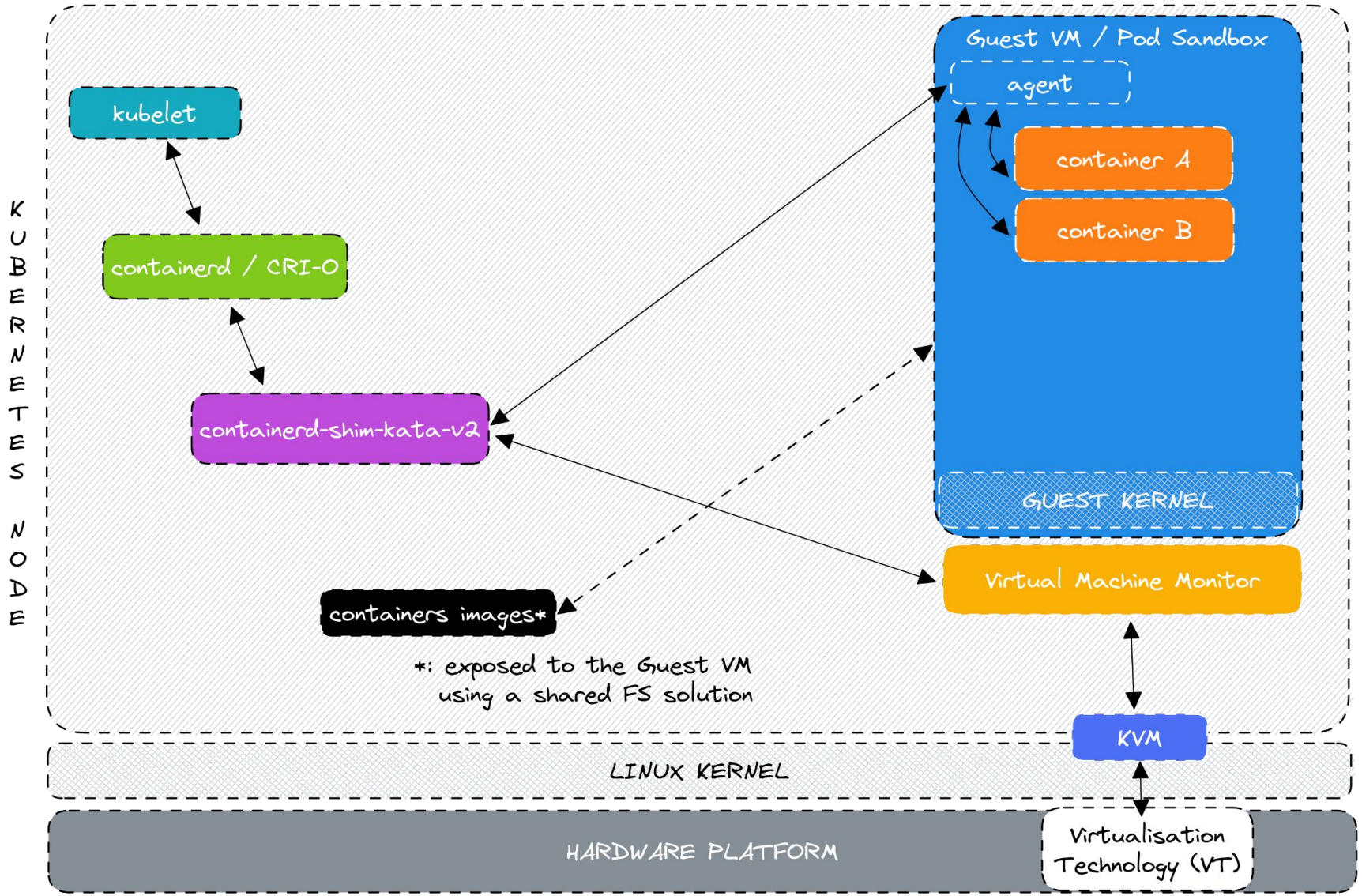
Kata Containers



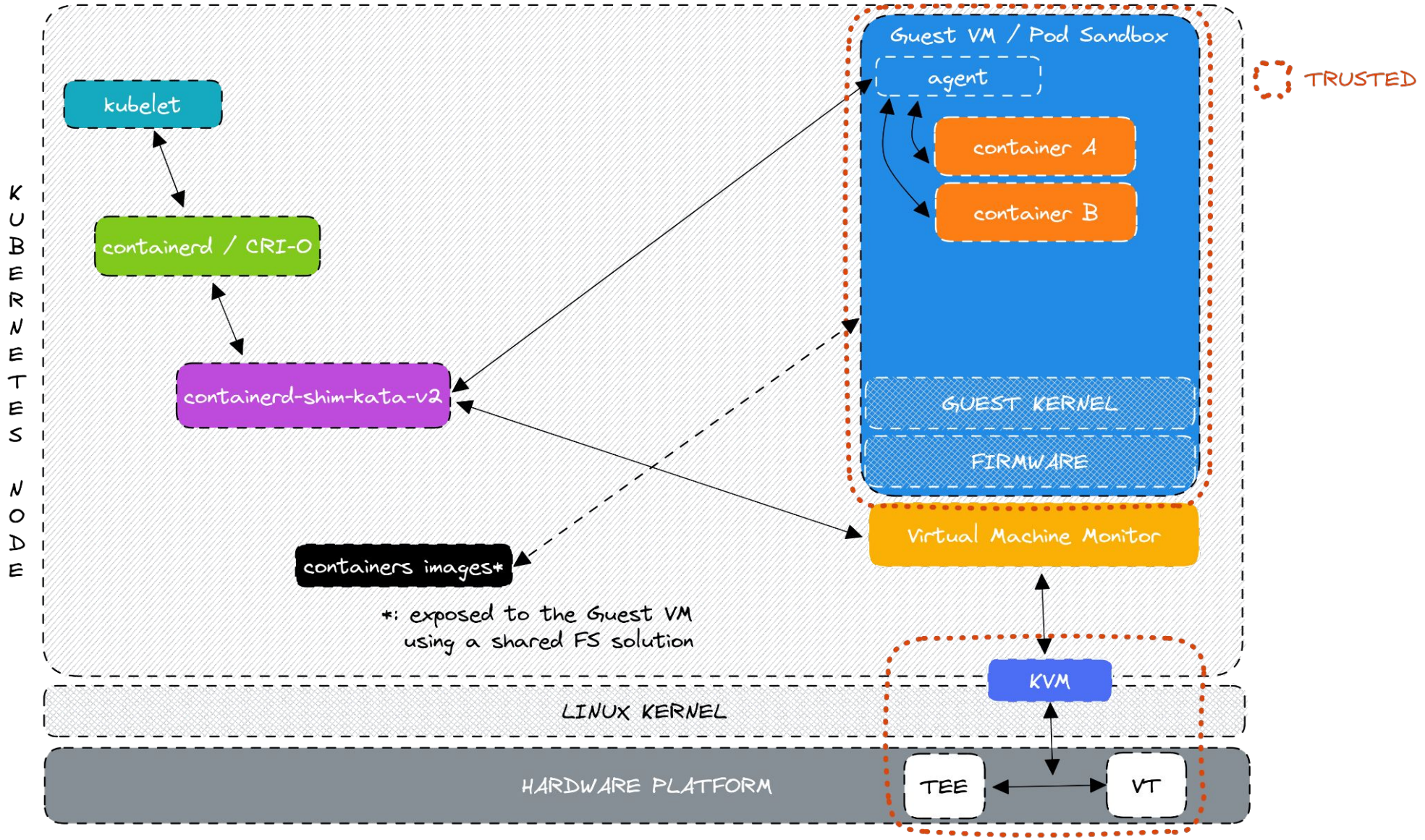
Basics: Kata Containers



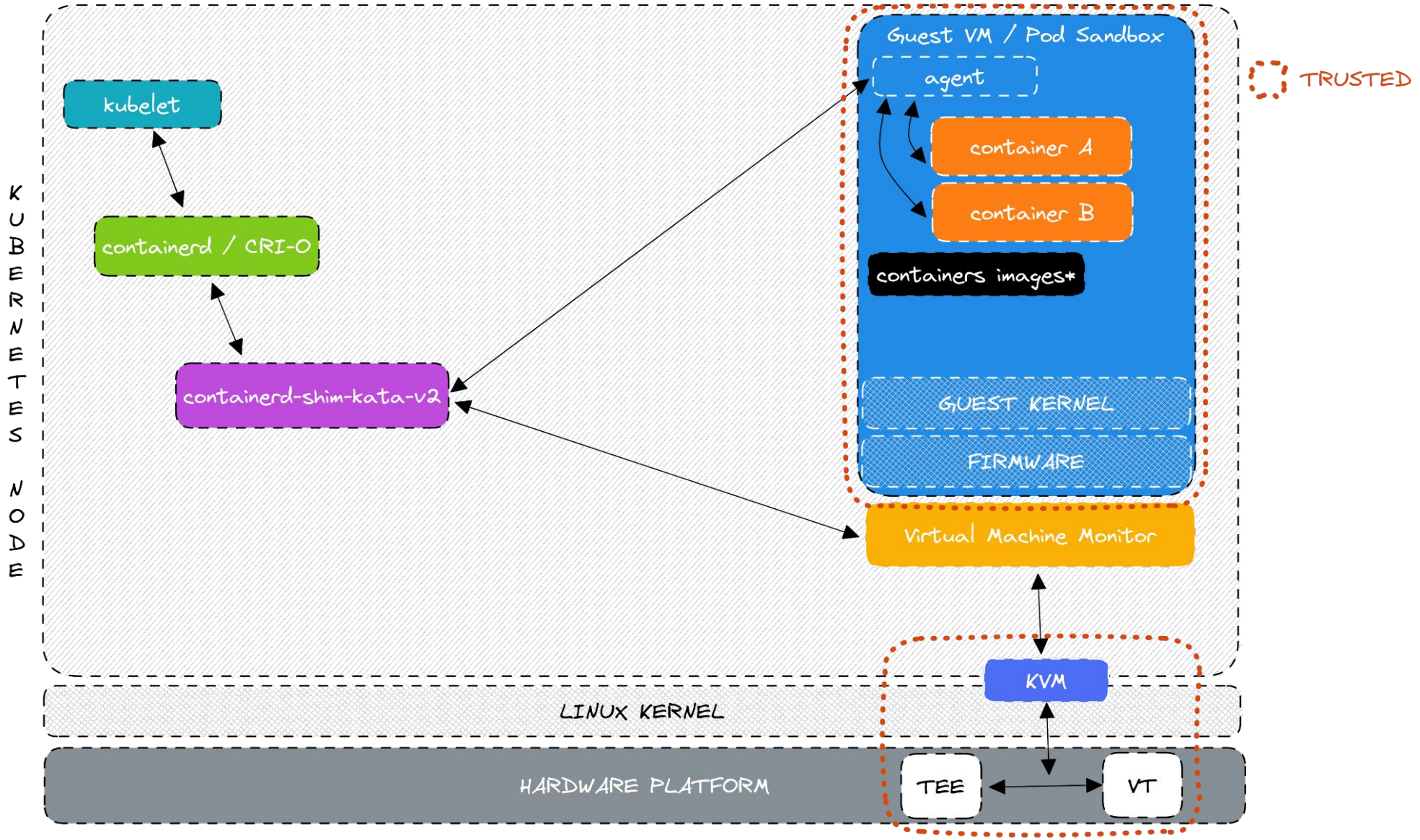
From Kata to Confidential Containers



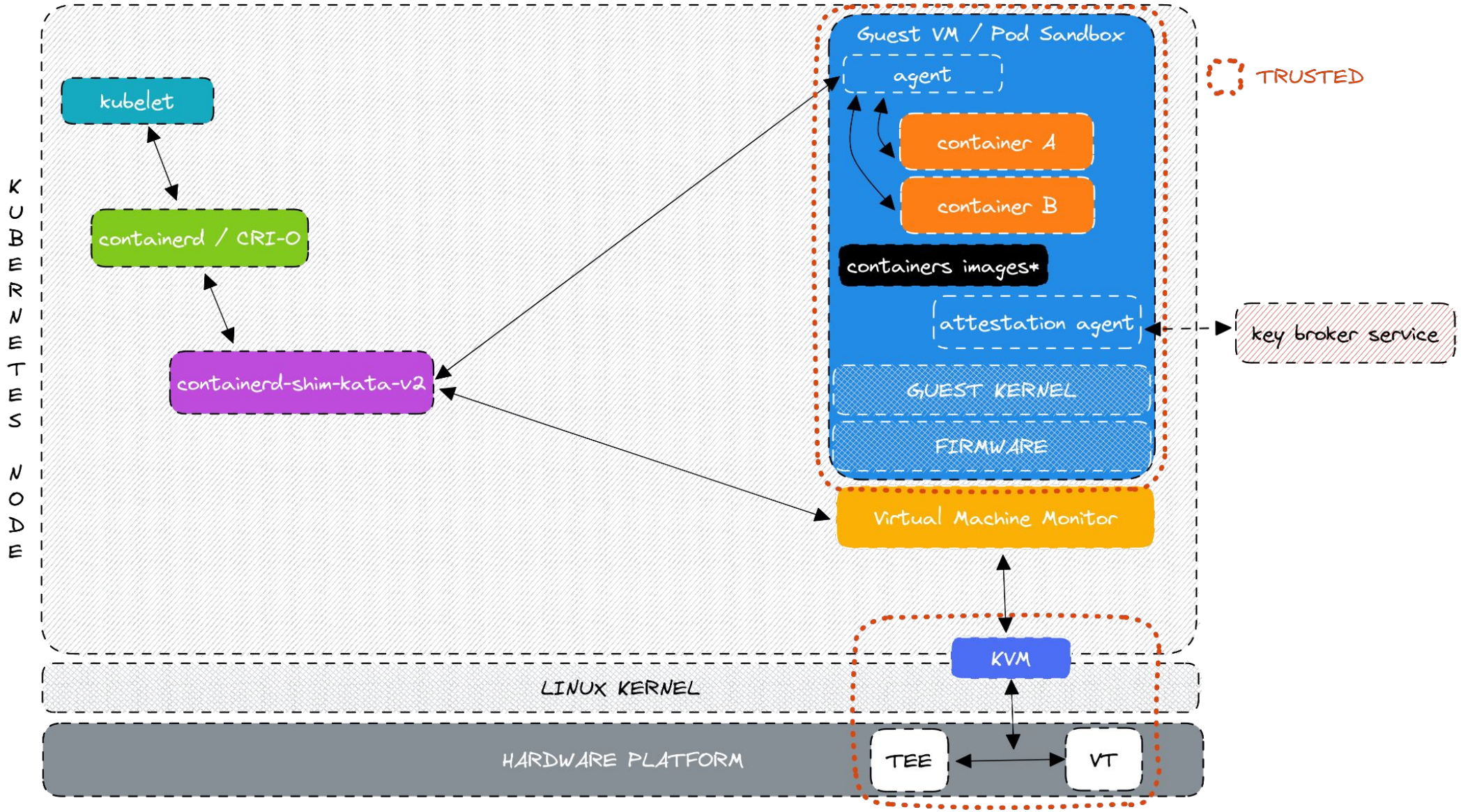
From Kata to Confidential Containers



From Kata to Confidential Containers



From Kata to Confidential Containers



From Kata to Confidential Containers

The projects focus on …

- Kata Containers:
  - Protecting the Host from a non-trusted workload
  - Protecting workloads from each other

- Confidential Containers adds:
  - Protecting the workload from a non-trusted infrastructure

From Kata to Confidential Containers

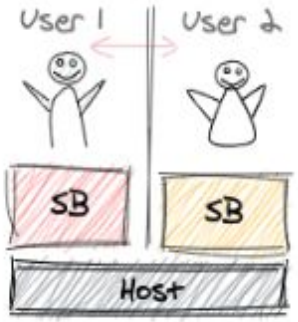
Types of Sandboxing

VTx, Linux namespaces, Seccomp, SE-Linux, …

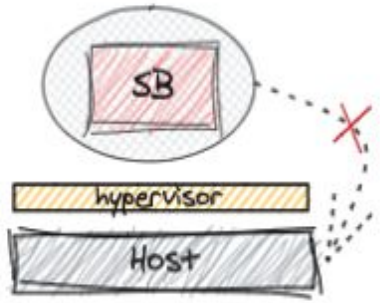
AMD SEV-*, IBM SE, Intel SGX, and Intel TDX

Virtualization: Hypervisor + Container-based

Workload from Workload

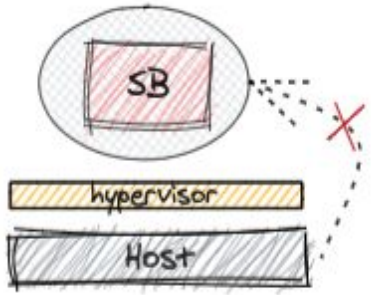


Host From Workload



Trusted Execution Environments

Workload from Host



The different flavours

The different flavours

Process-based isolation

- Provided by Enclave CC
  - SGX (Intel)

VM-based isolation

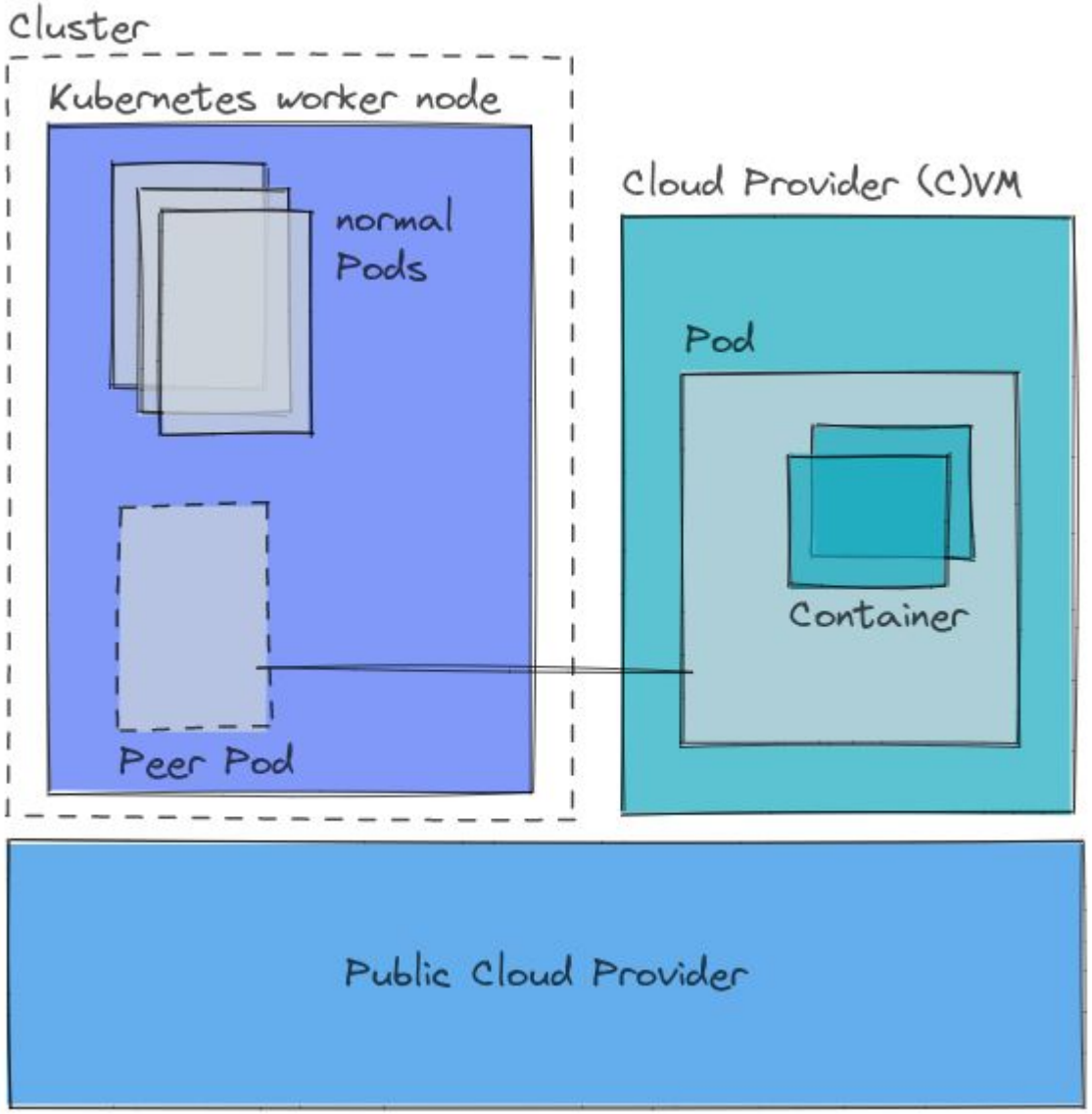
- Provided by Kata Containers
  - SE (IBM) / SEV-ES (AMD) / TDX (Intel)

The different flavours

Cloud API Adaptor (aka, Peer Pods)

- It could be its own talk!
- Takes advantage of the Kata Containers' remote hypervisor support
- Allows users to use a CSP's VM as the Guest VM / PodSandbox
  - AWS
  - Azure
  - GCP
  - IBM Cloud

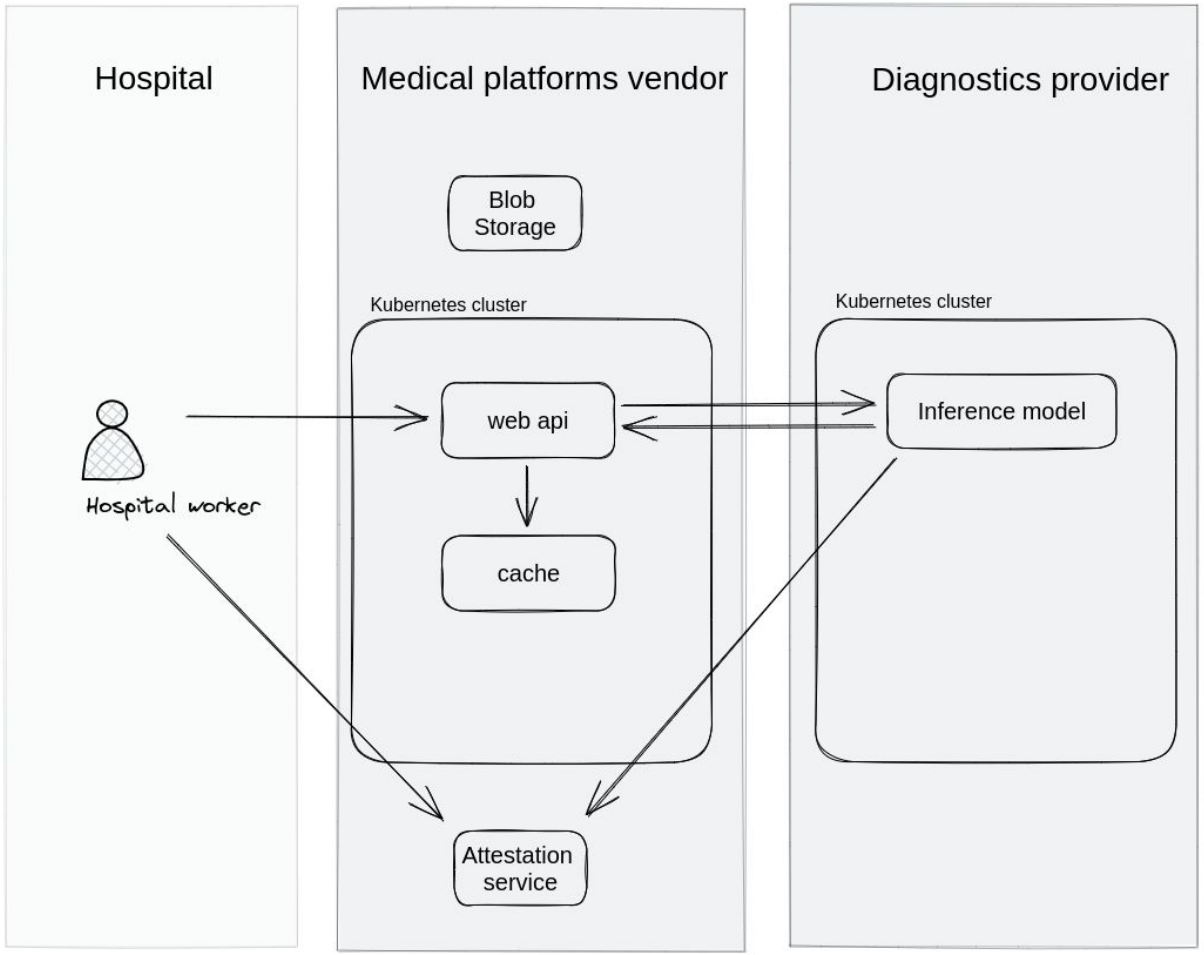
https://www.youtube.com/watch?v=QPOcEGcgYfU



Use cases of Confidential Containers

Confidential Containers in Healthcare Data Analysis

- Collaborate on sensitive patient data for research and analysis while ensuring data privacy and complying with regulations
- Use Confidential Containers to safeguard patient data in a Trusted Execution Environment
- Build your solution with Kubernetes cluster and Confidential Computing technologies, like TEEs
- Rely on Attestation Services, Key Management and other Confidential Computing building blocks for secure data sharing and analysis among collaborating institutions
- Achieve compliance with data privacy regulations and enhance trust in the execution environment

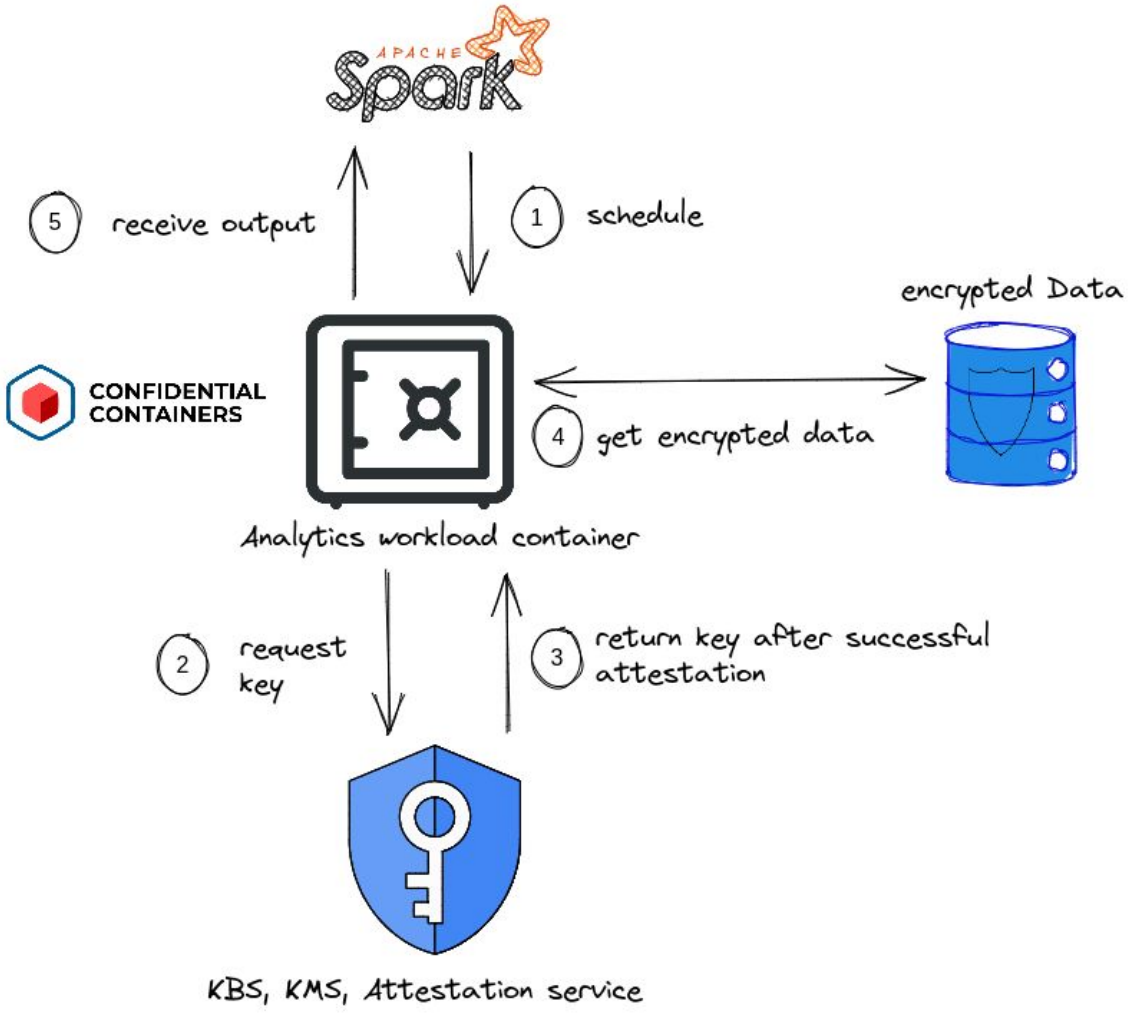


Source: https://learn.microsoft.com/en-us/azure/architecture/example-scenario/confidential/healthcare-inference

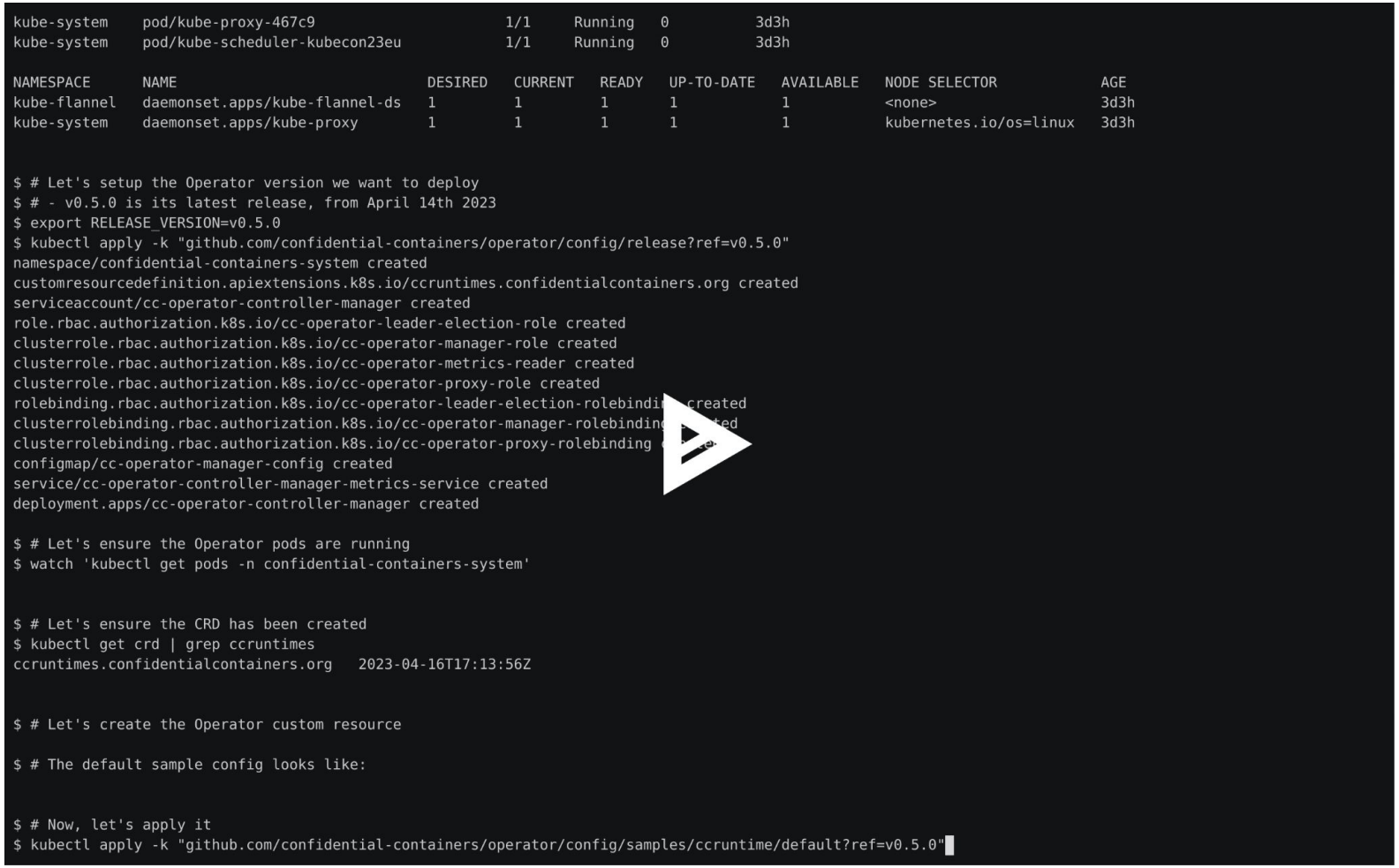
Use cases of Confidential Containers

Confidential Data Analytics with Apache Spark/PySpark

- Container Encryption: Datasets are encrypted, not the containers
- Remote Attestation: Used for secure key release
- K8s Dependency: Optimized for K8s deployments, HPA for large datasets
- Multi-Party Analytics: Extendable for data schema contracts between parties
- Forked Scenarios: Apache Spark Master Scheduler modified for secure job scheduling



DEMO



https://asciinema.org/a/577943

Confidential Containers 0.5.0 Release

Expanding Cloud-Native Confidential Computing Capabilities

- Largest release to date, featuring:

1. Generic Key Broker Service (KBS)
   - Attestation Service and Resource Value Provider Service for diverse platforms and use cases
2. Peer-pods for Kata Containers on multiple public clouds
3. Resource URL for uniform attestation resources and secrets identification
4. Enclave-CC for process-based confidential containers using Intel SGX

Q/A

Check out the Confidential Containers project

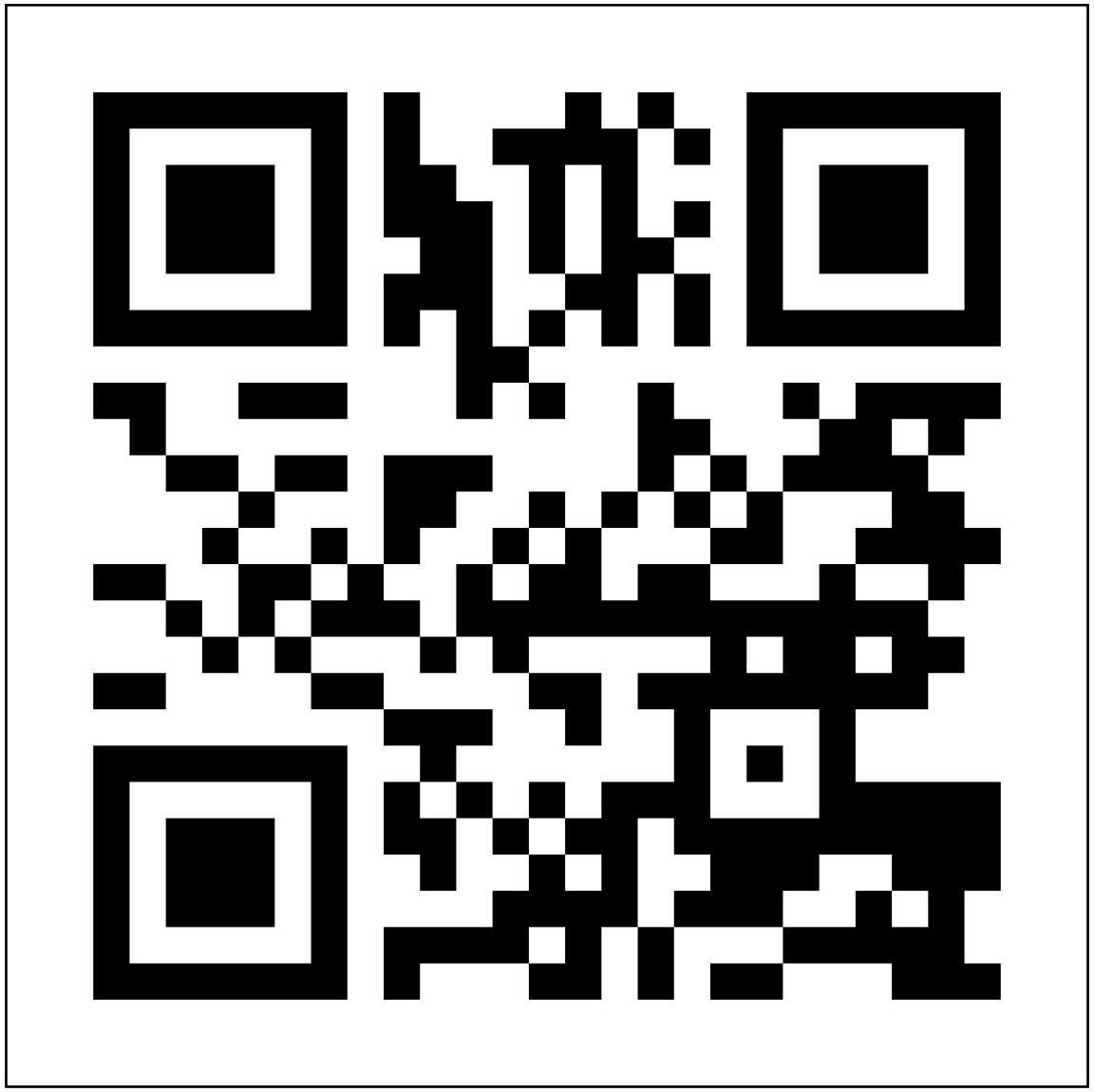
- Contribute, join community meetings
- Slack: #confidential-containers in CNCF workspace

Also watch this talk which will happen directly after lunch
The Next Episode in Workload Isolation: Confidential Containers - Jeremi Piotrowski

Talks from previous KubeCon + CloudNativeCon editions
Trust No One: Bringing Confidential Computing to Containers- Samuel Ortiz & Eric Ernst
Confidential Containers Explained - James Magowan & Samuel Ortiz

KubeCon CloudNativeCon Europe 2023

KubeCon CloudNativeCon North America 2021



Please scan the QR Code above
to leave feedback on this session

Why Confidential Computing?

- Confidential Computing technology is already being used in everyday devices such as smartphones and game consoles to protect biometric data, payments, and against cheating and piracy.

- Confidential Computing can be used for existing programming languages, toolchains, and applications, without requiring developers to change their programming approach.

- Confidential Computing ensures the code executed, data processed, and output results cannot be tampered with or disclosed.