Leveraging Trusted Execution Environments to protect containers and data

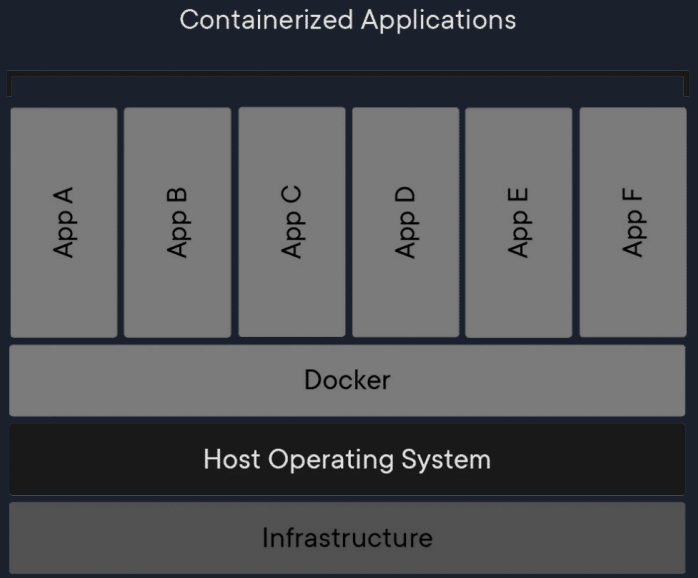
Alvaro Soto - Senior Software Maintenance Engineer at RedHat

About me

Senior Software Maintainer Engineer at Redhat

Enhanced OpenShift support for Telcos

Containers


Containerized Applications
App A
App B
App C
App D
App E
App F
Docker
Host Operating System
Infrastructure

Understanding the problems

01 Using per container administration does not scale

02 Shell scripts or more robust platforms (ansible, chef, etc.) does not fix the issue either

03 Using containers at scale needs a mindset change!!!

Solution? Kubernetes!!!

OPENSHIFT

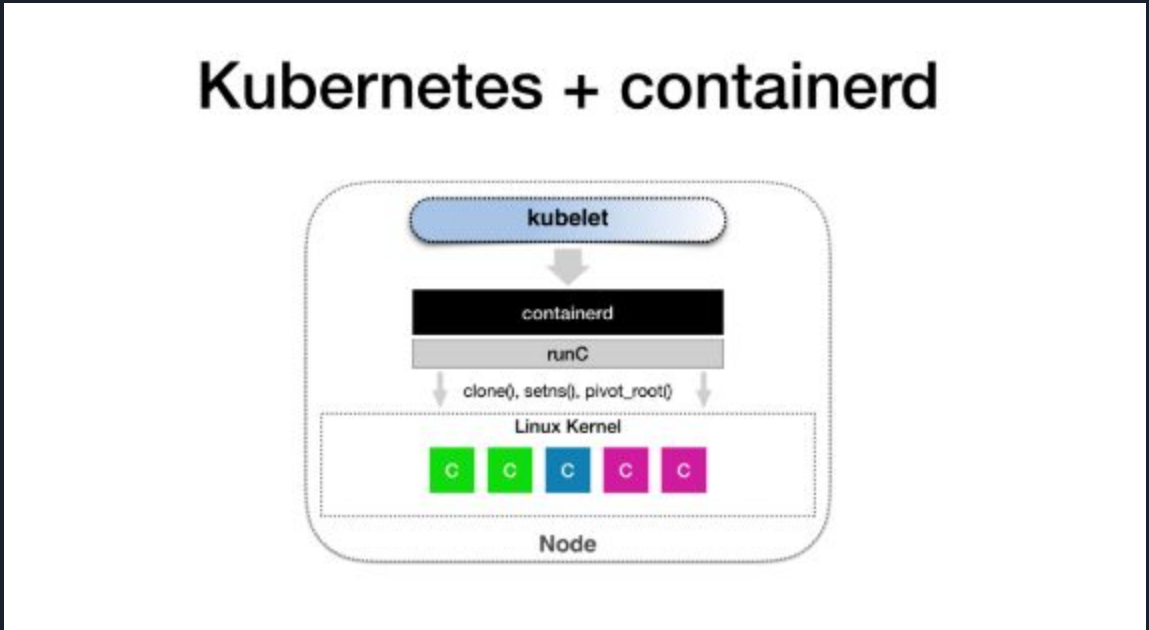
some inherited “issues”

01 All guest containers share the same kernel

02 Host has 100% visibility on guest containers

03 Host has zero restriction on guest containers

Container runtime



A few kubernetes runtimes

rkt

MESOS

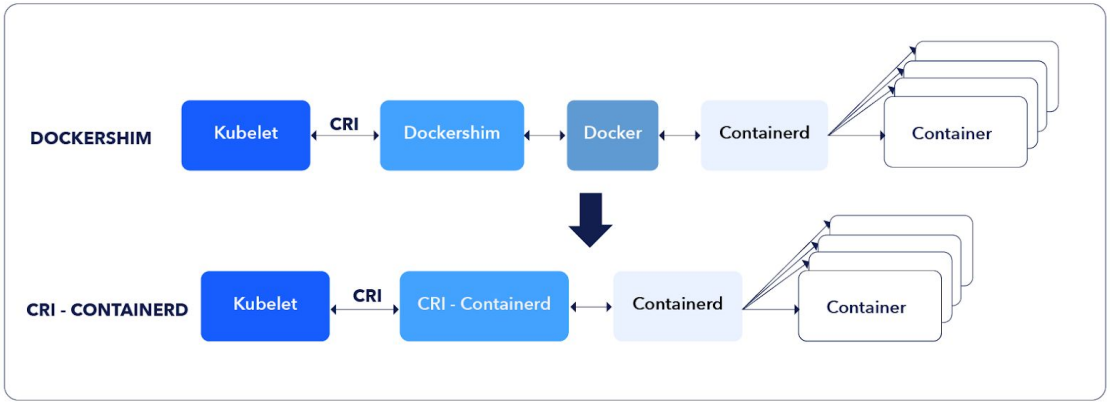
cri-o

OpenVZ
Virtuozzo Containers

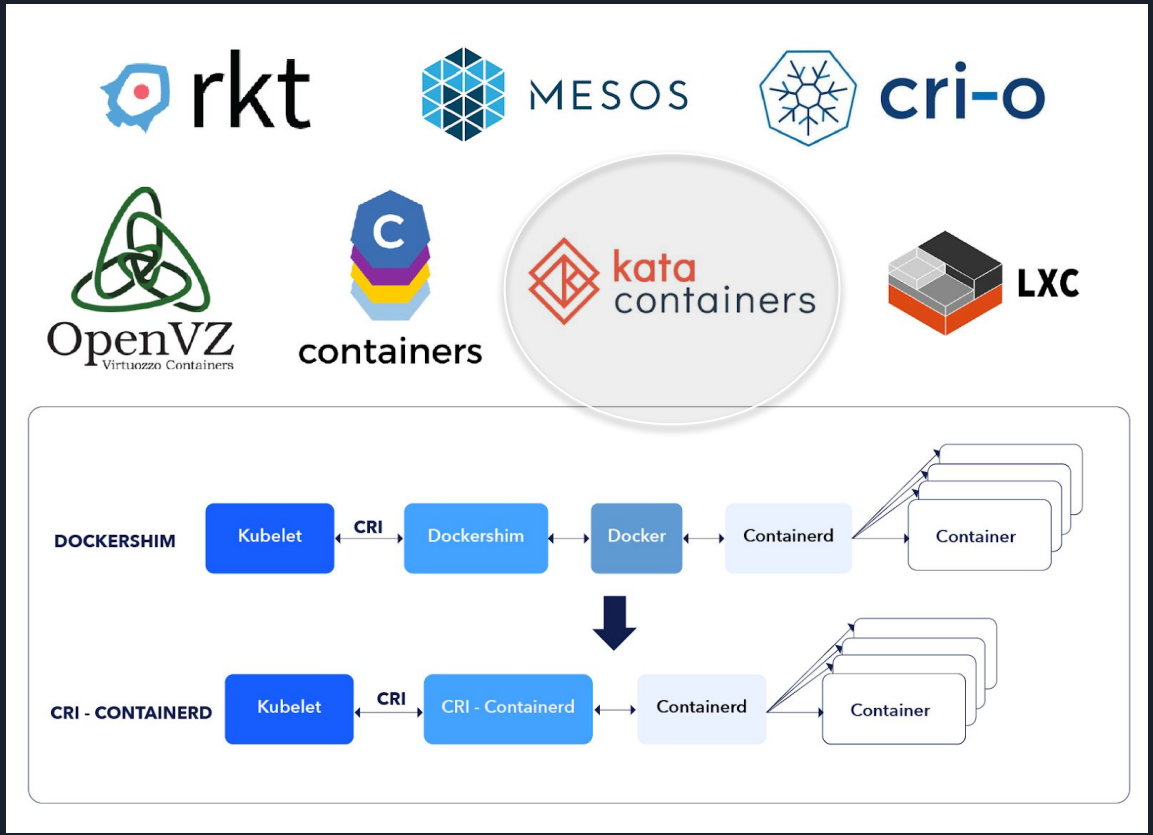
containers

kata containers

LXC



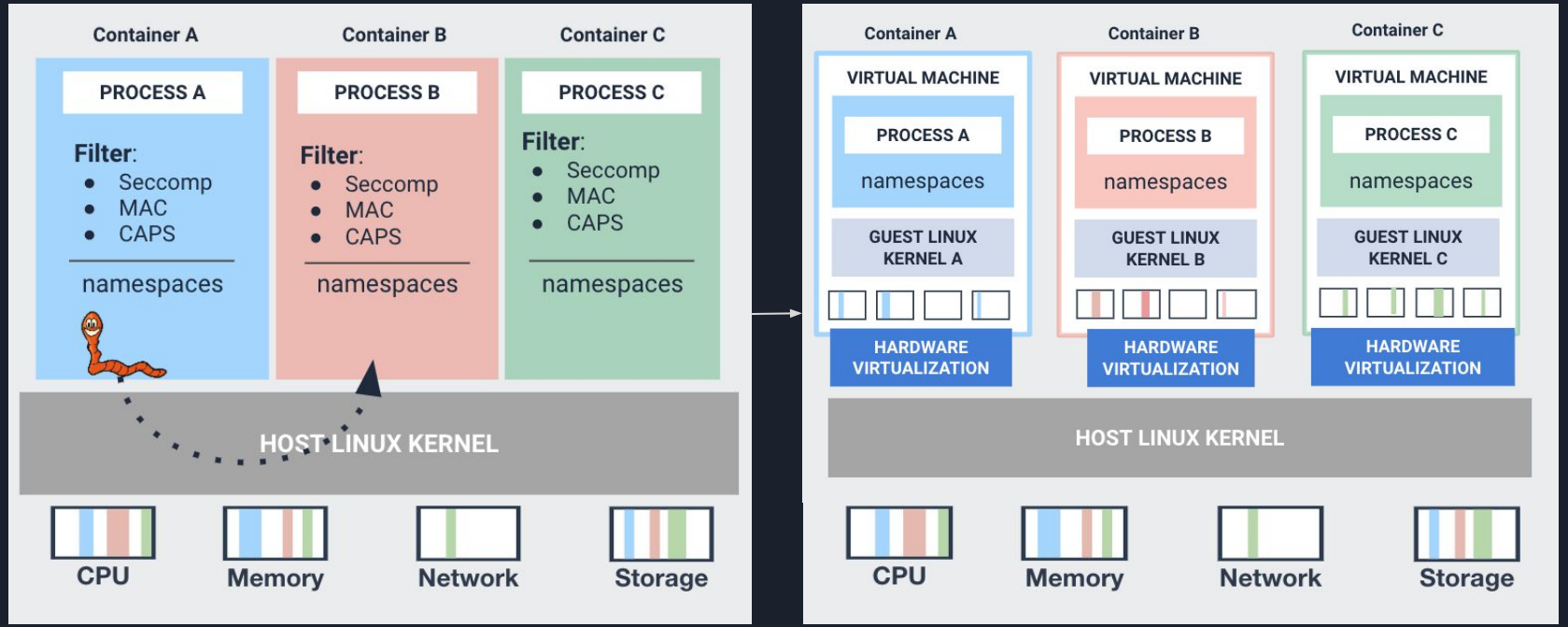
A few kubernetes runtimes



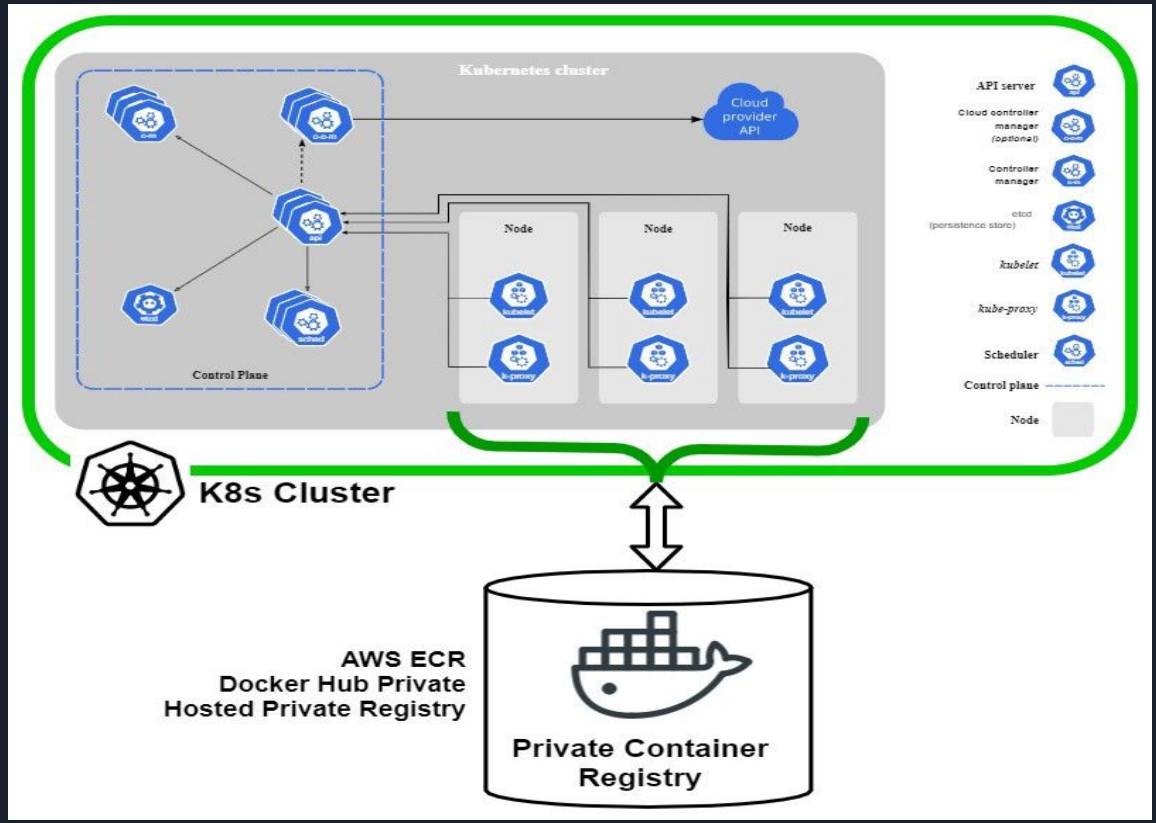
Kata Containers

Open Infrastructure
FOUNDATION

Proposed Kata Runtime solution



Kubernetes architecture



Recap

Kube + Kata runtime

some inherited “issues”

01 All guest containers share the same kernel

02 Host has 100% visibility on guest containers

03 Host has zero restriction on guest containers

some inherited “issues”

01 All guest containers share the same kernel

02 Host has 100% visibility on guest containers

03 Host has zero restriction on guest containers

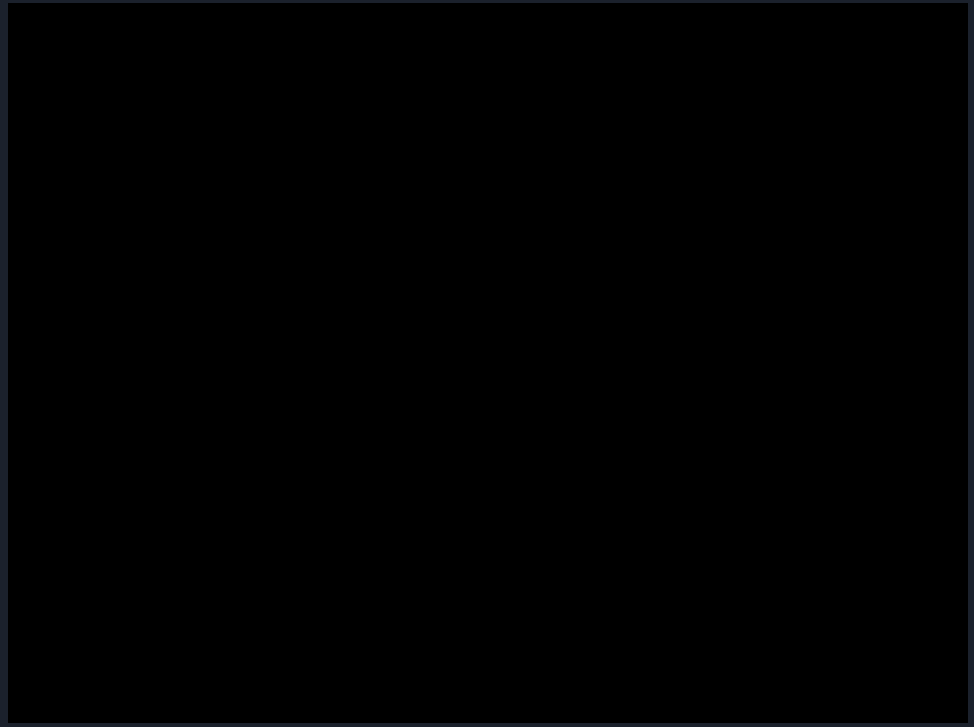
04 Image registry semi-private or worst case scenario, public

Confidential Containers

Confidential Containers

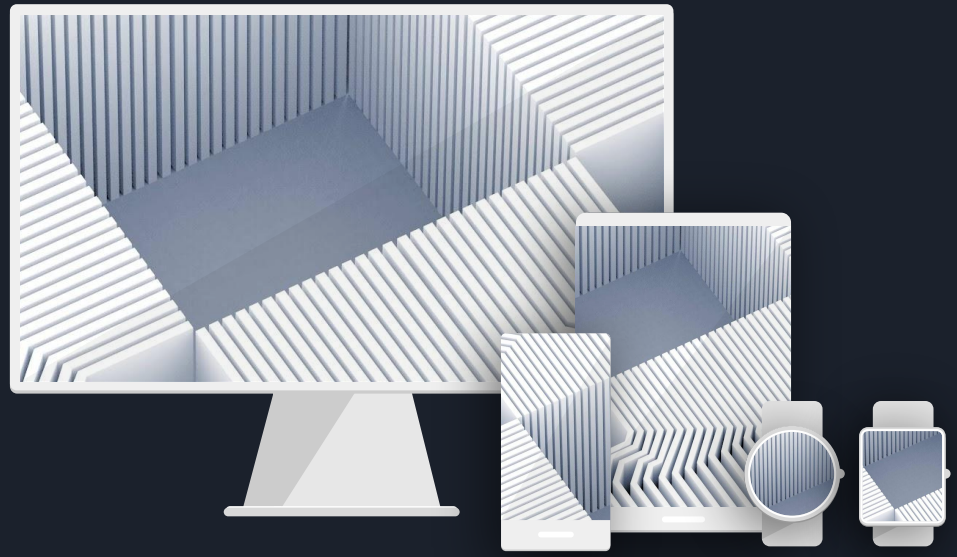
- Allow cloud native application owners to enforce application security requirements
- Transparent deployment of unmodified containers
- Support for multiple TEE and hardware platforms
- A trust model which separates Cloud Service Providers (CSPs) from guest applications
- Least privilege principles for the Kubernetes Cluster administration capabilities which impact delivering Confidential Computing for guest application or data inside the TEE

Confidential Containers, video demo



https://www.youtube.com/watch?v=1v1hxAWwHDo

Thank you!



@alsotoes

alsotoes@gmail.com