Edgeless Systems

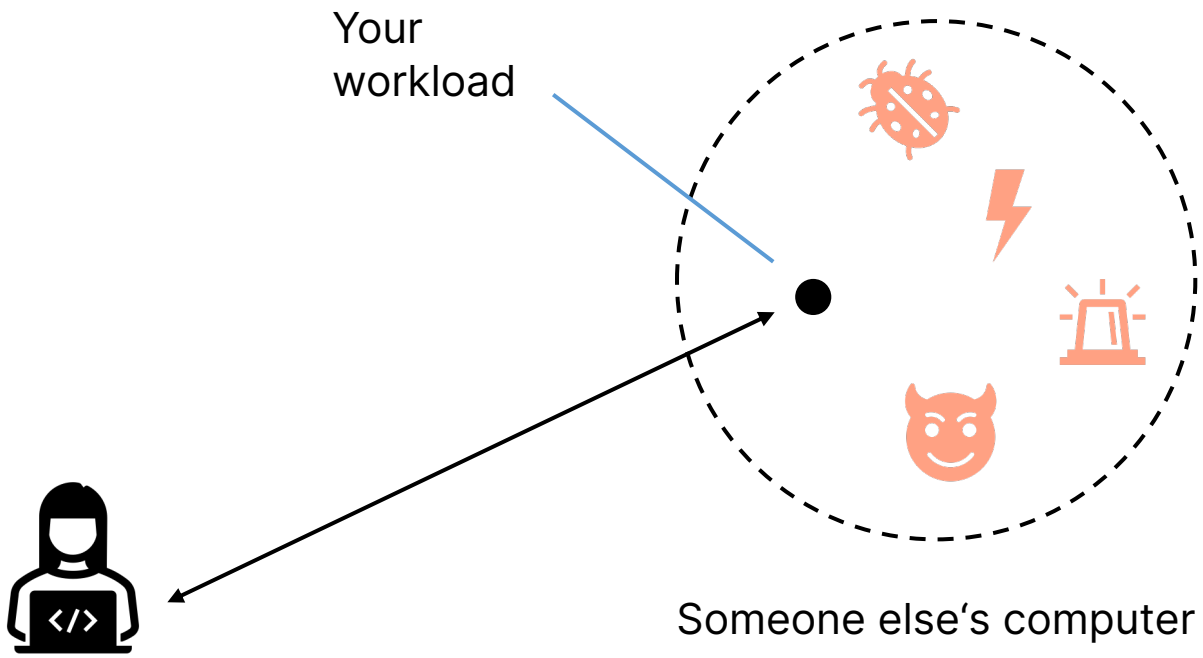
Confidential Computing on Kubernetes Workshop

01.08.2024 Kubesimplify

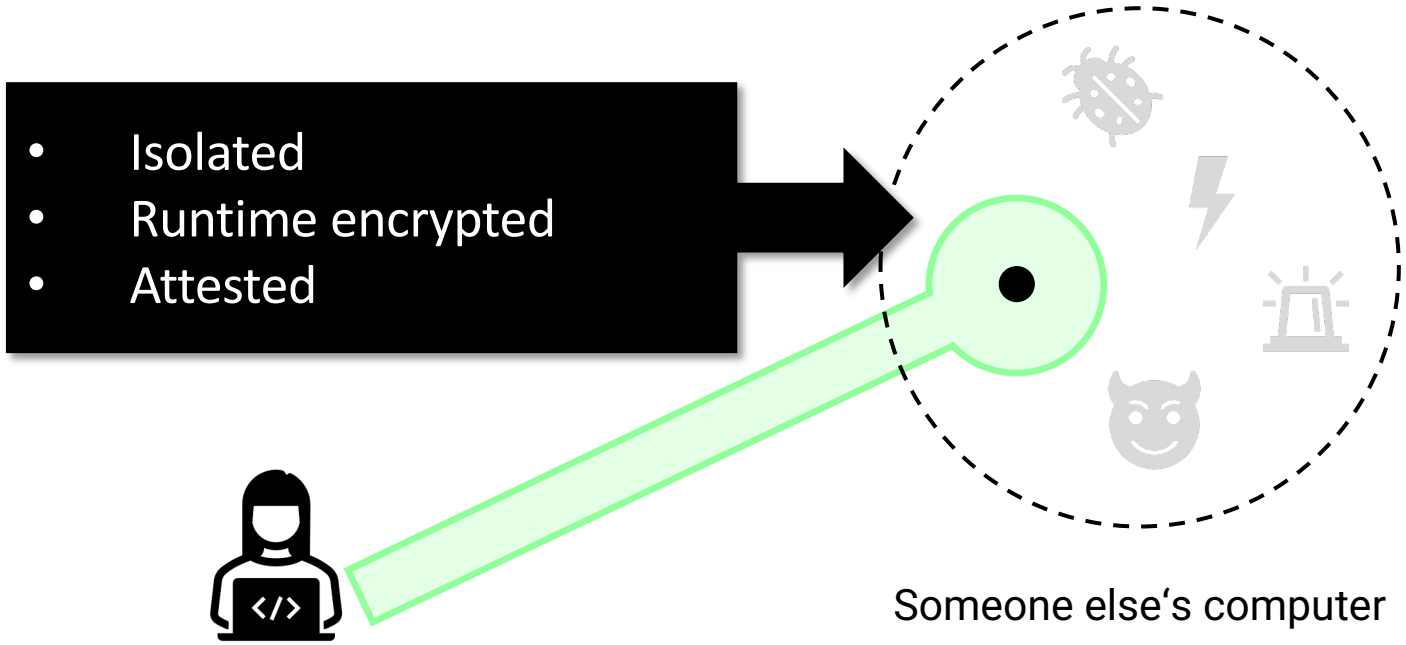
Edgeless Systems

01 Confidential Computing

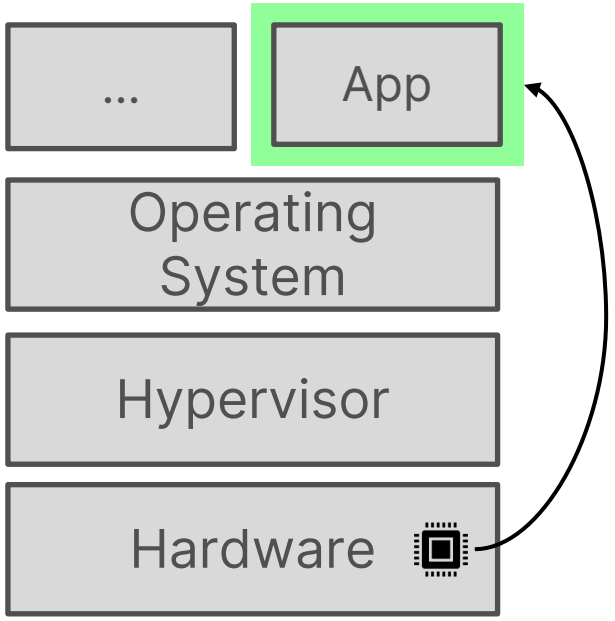
What is confidential computing?



What is confidential computing?

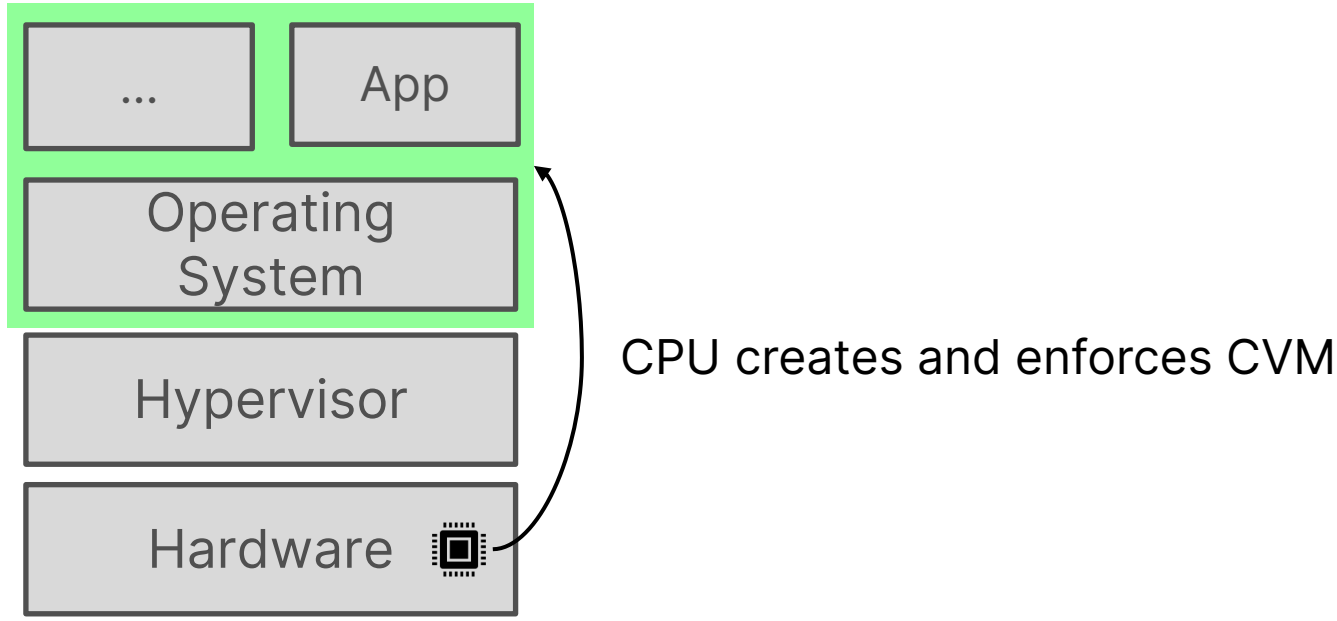


Secure Enclaves

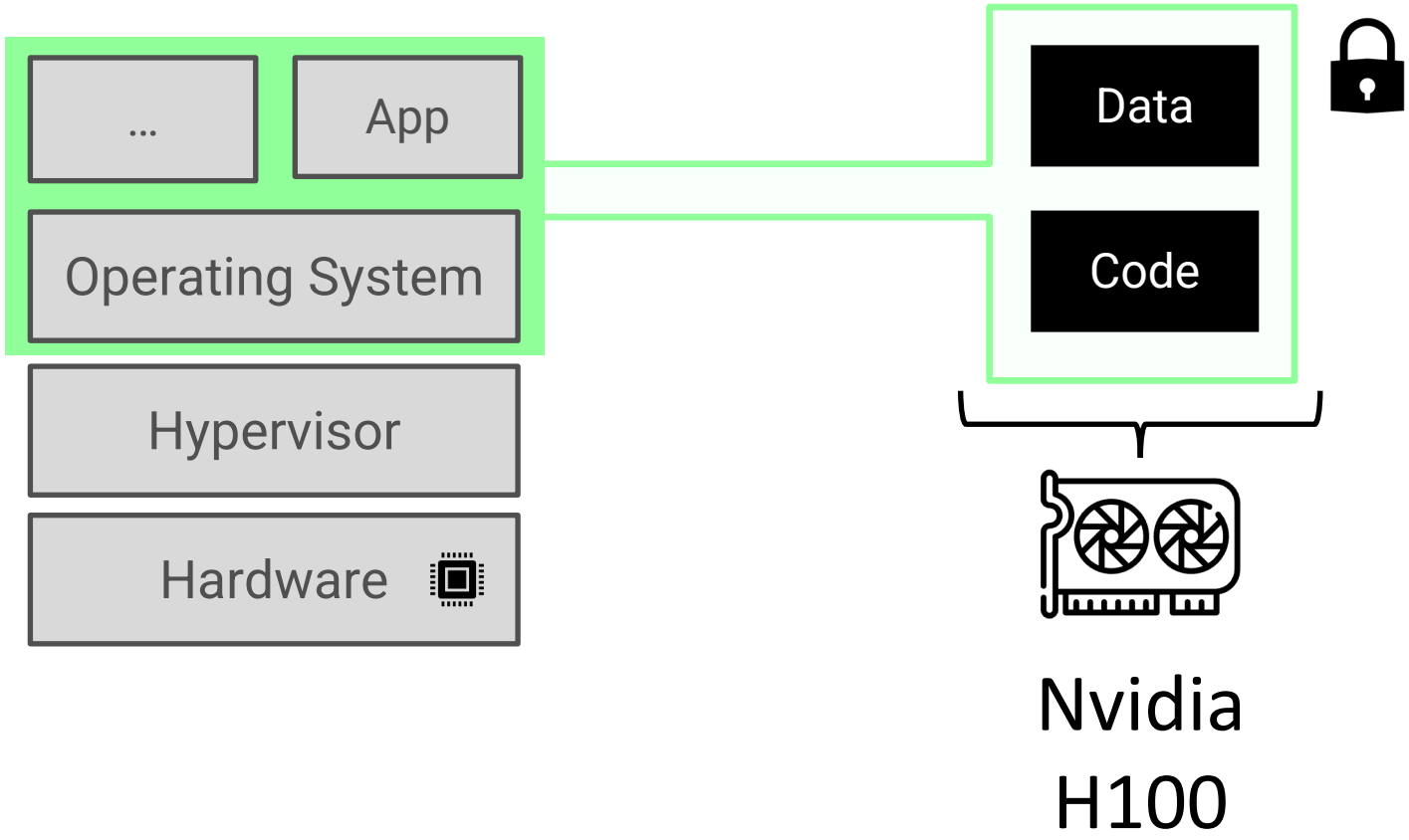


CPU creates and enforces enclave

Confidential VMs

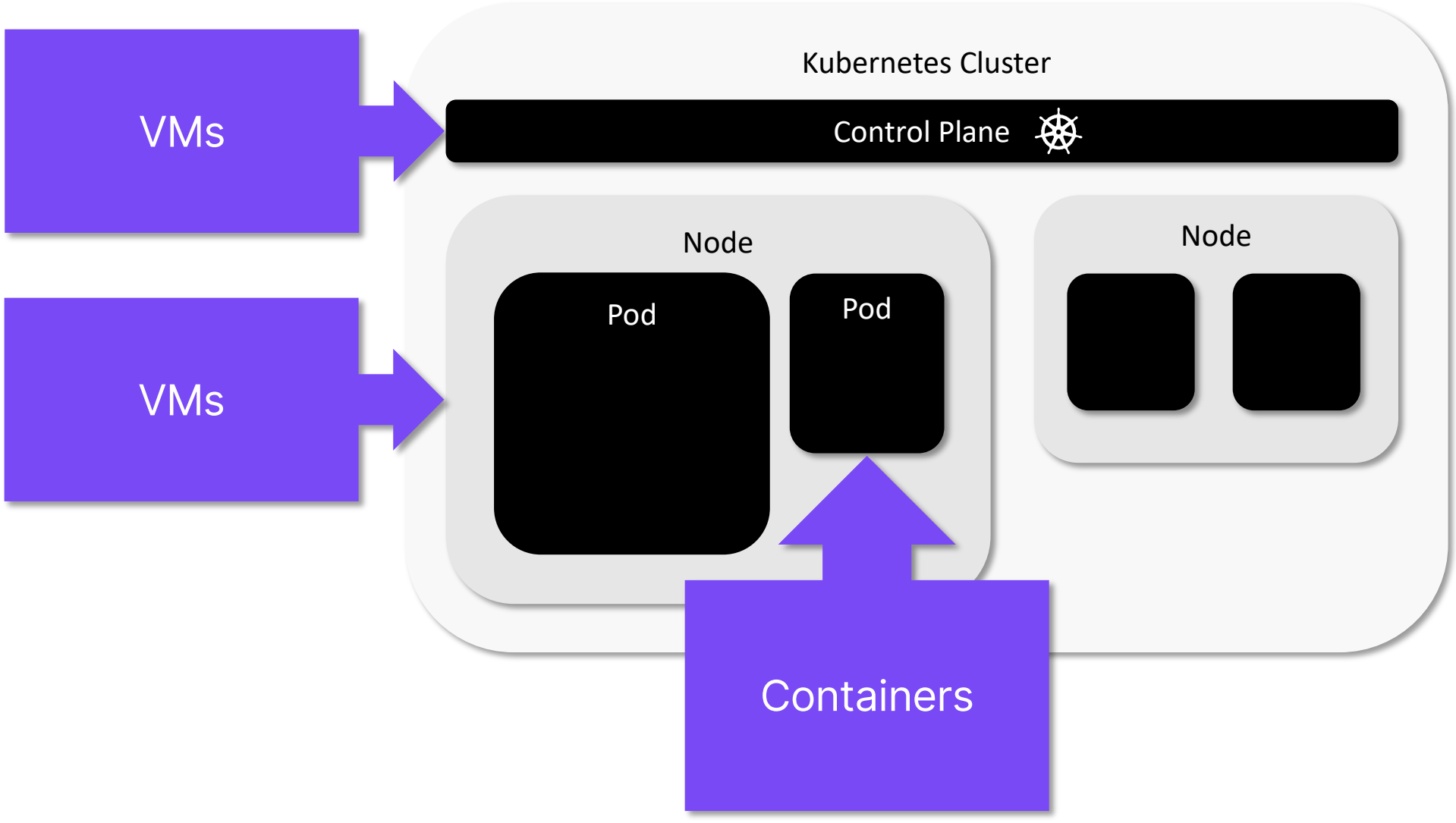


Confidential Accelerators

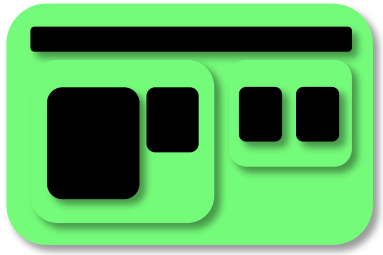


Edgeless Systems

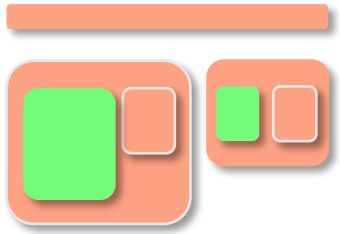
02 Confidential Containers


VMs
VMs
Kubernetes Cluster
Control Plane
Node
Pod
Pod
Node
Containers

Confidential cloud native spectrum

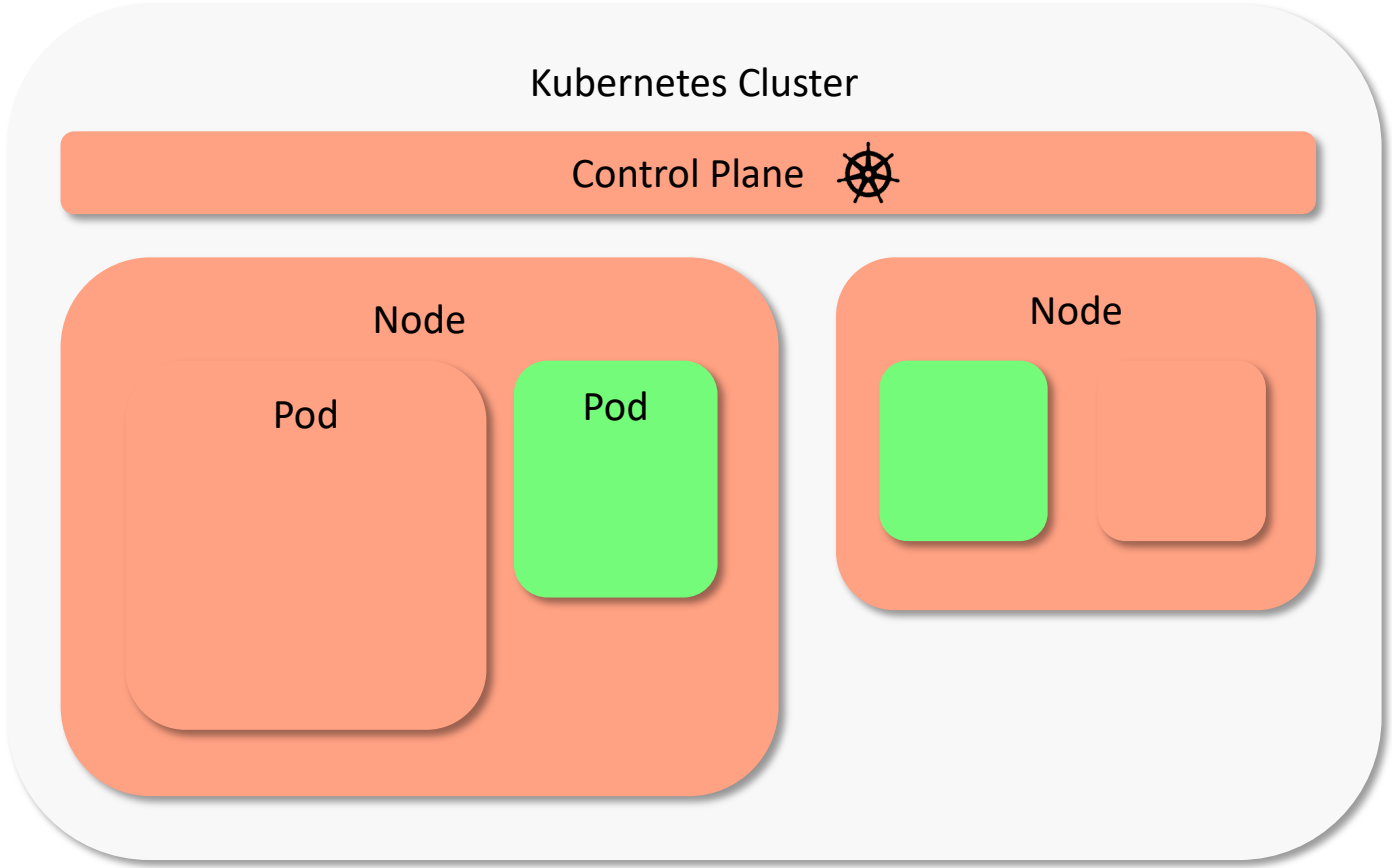


Confidential Cluster: K8s Nodes in CVMs

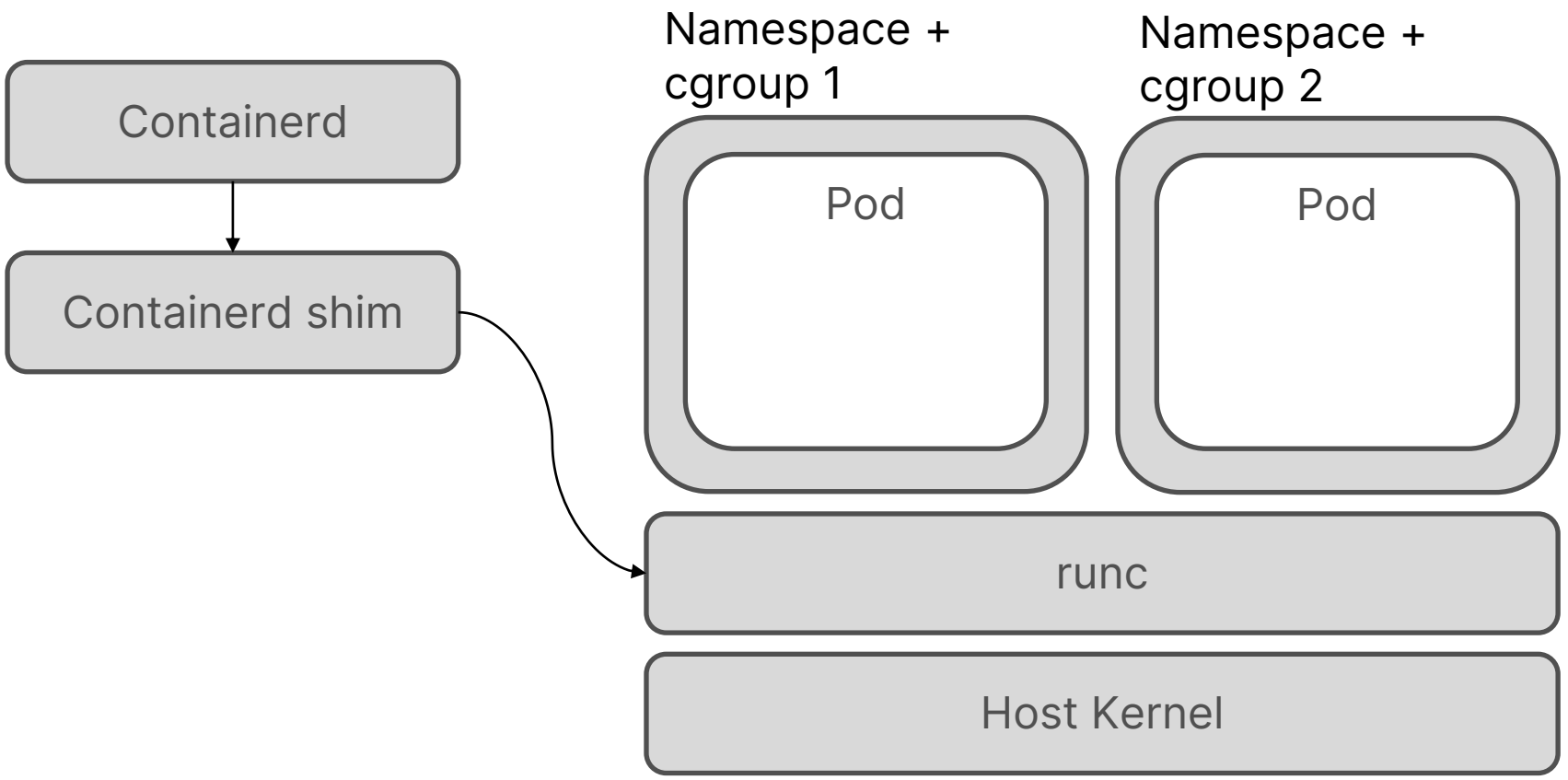


Confidential Containers: K8s Pods in CVMs

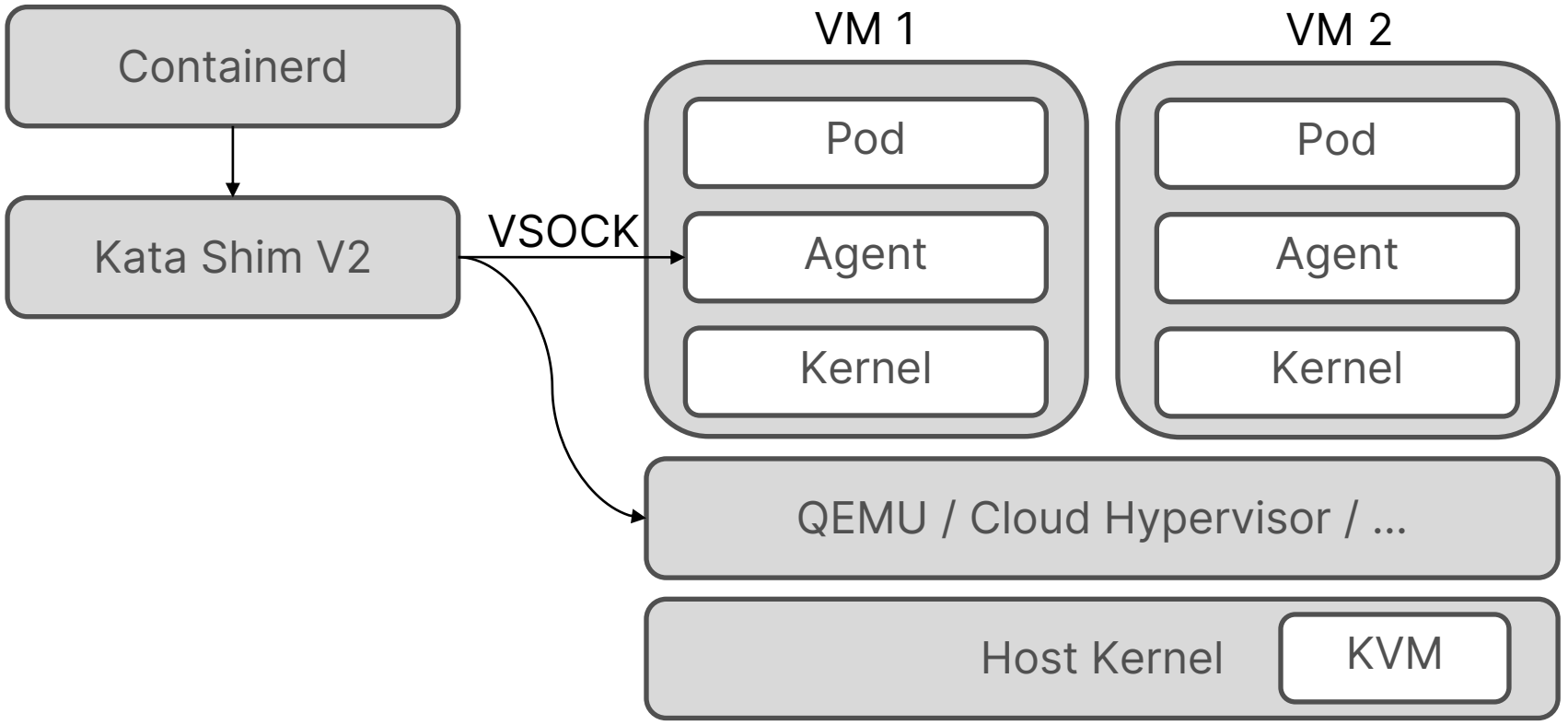
Confidential containers



Regular Containers

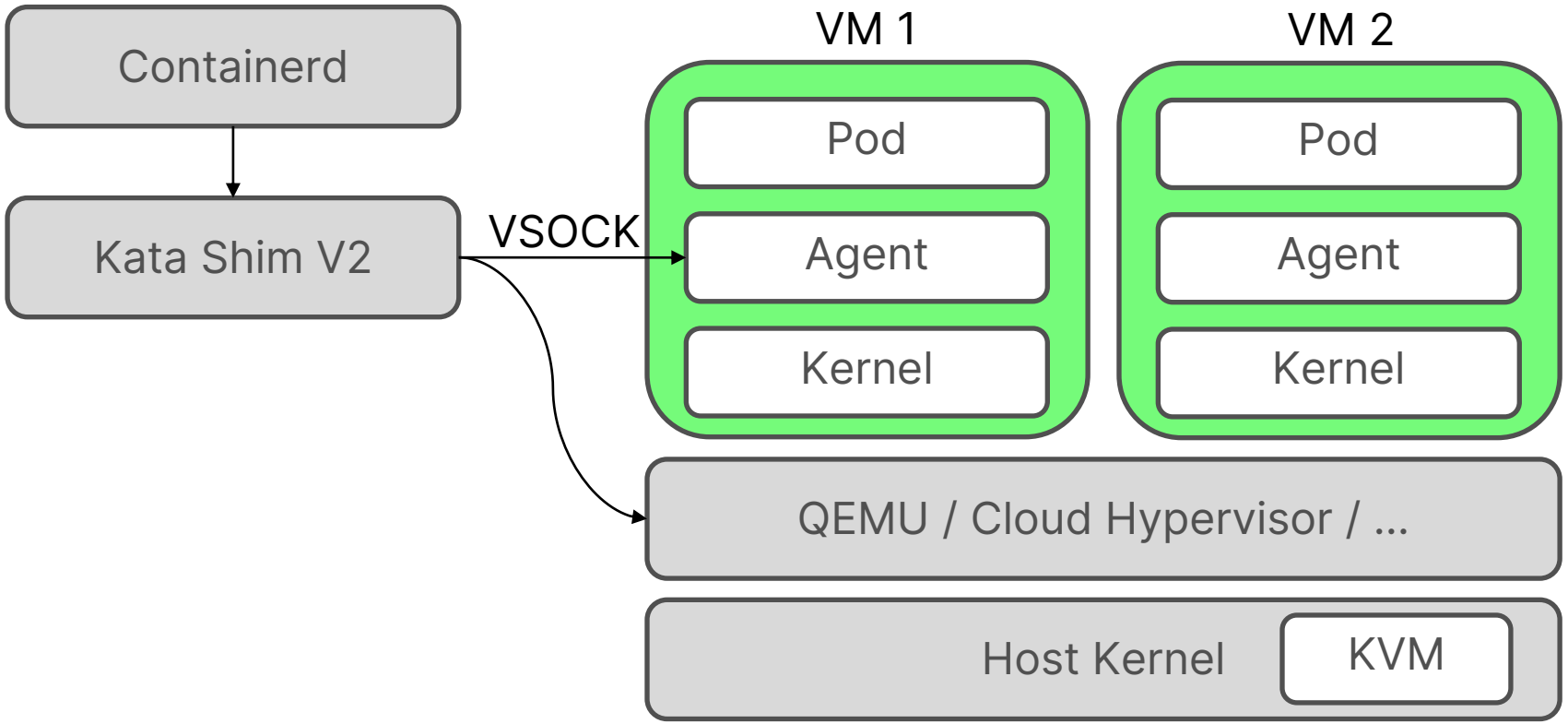


Kata Containers



kata containers

Confidential Containers



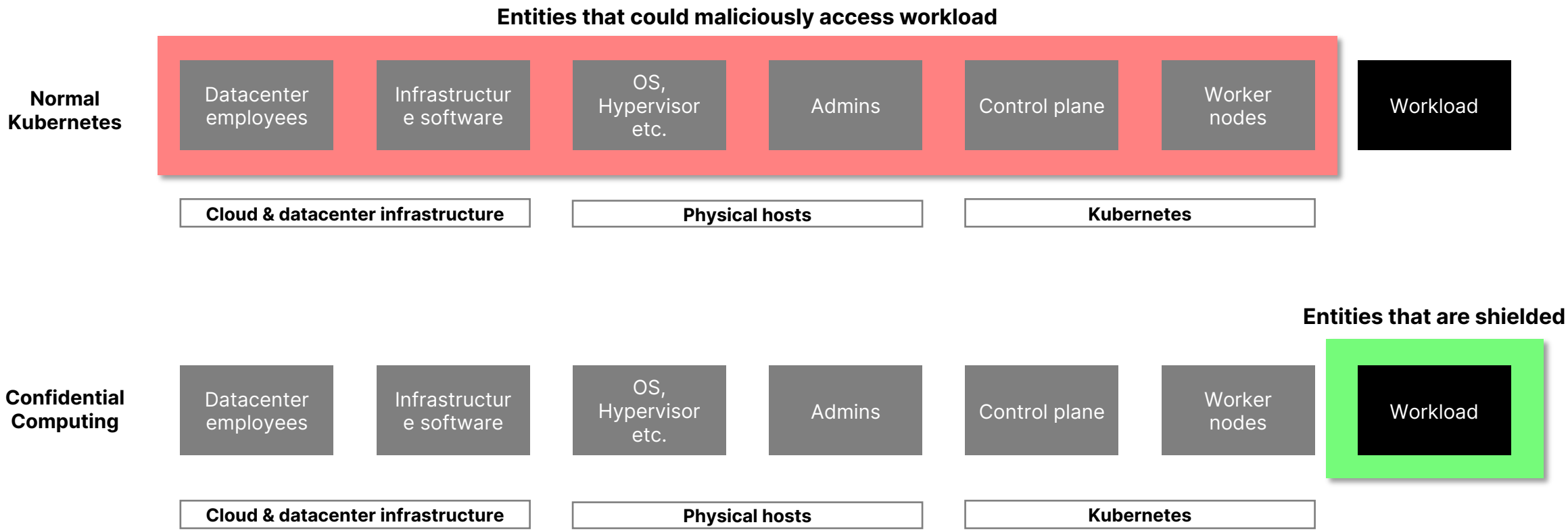
CONFIDENTIAL CONTAINERS

Confidential Containers

- CNCF Sandbox Project
- Kubernetes Container Runtime
- Supports AMD SEV, Intel TDX, IBM Z SE, NVIDIA H100
- Available on bare-metal, nested CVMs, or via remote hypervisor (Peerpod)

CONFIDENTIAL
CONTAINERS

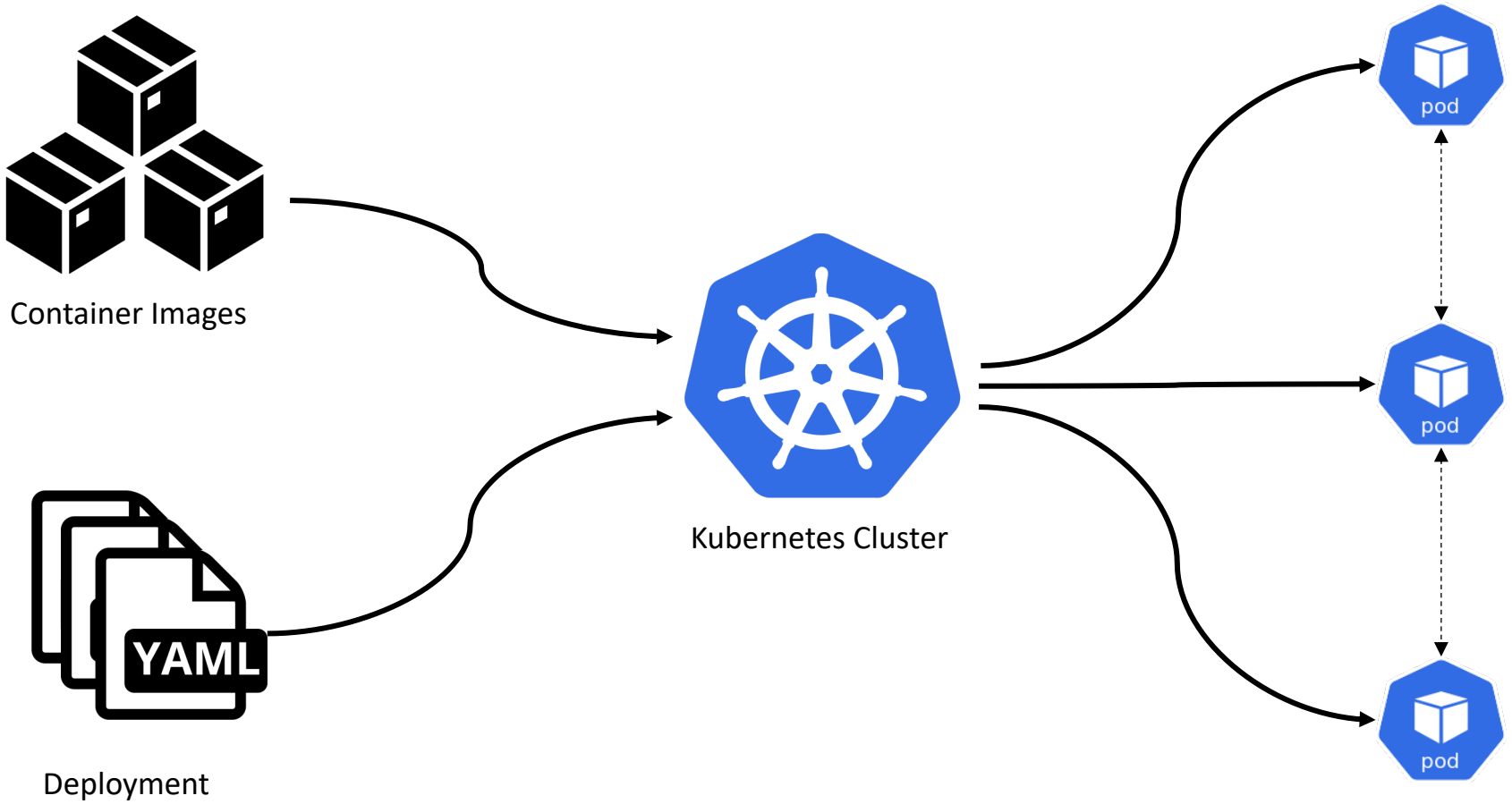
Threat model



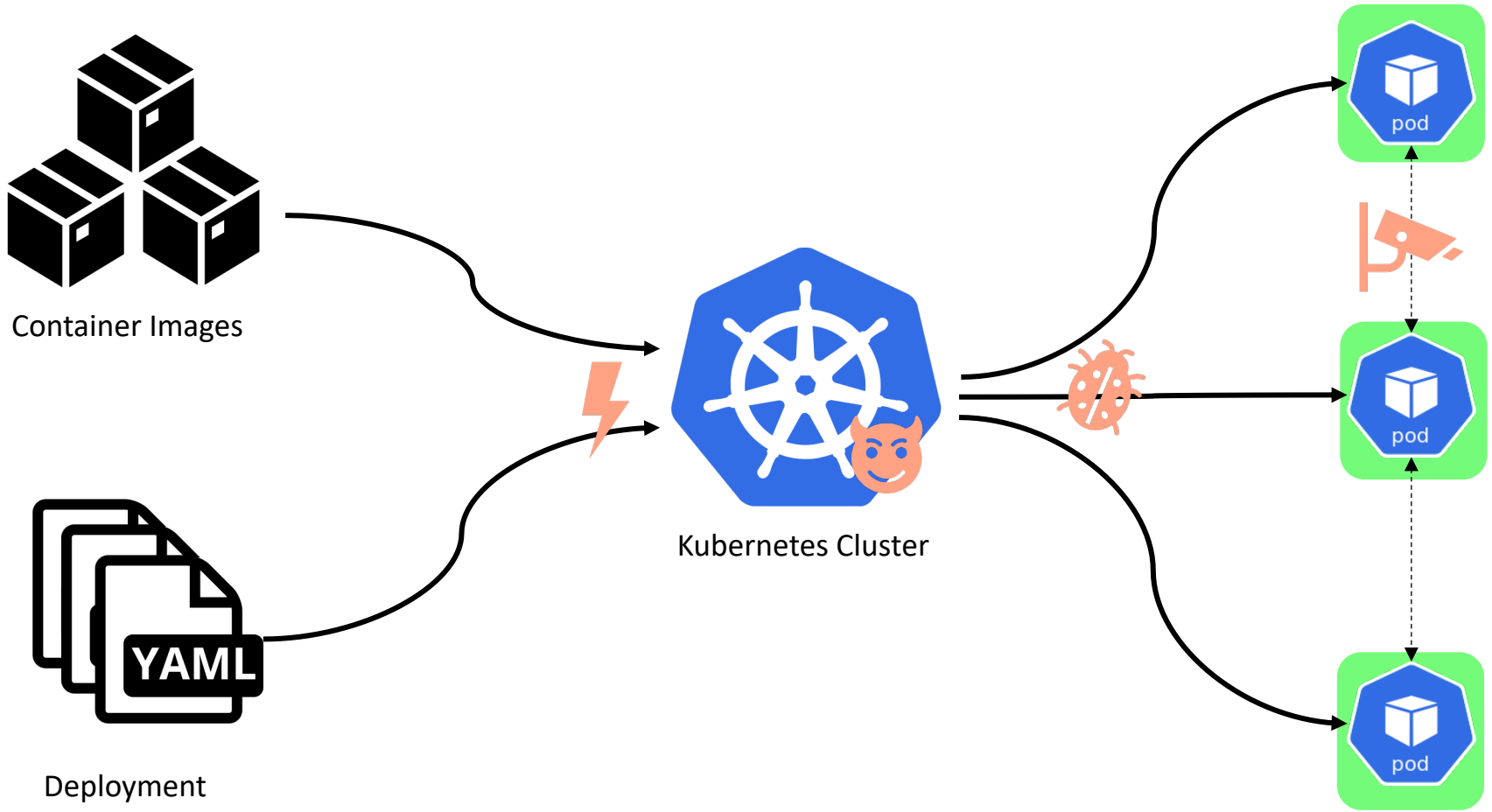
Edgeless Systems

03 Remaining Challenges

K8s deployment



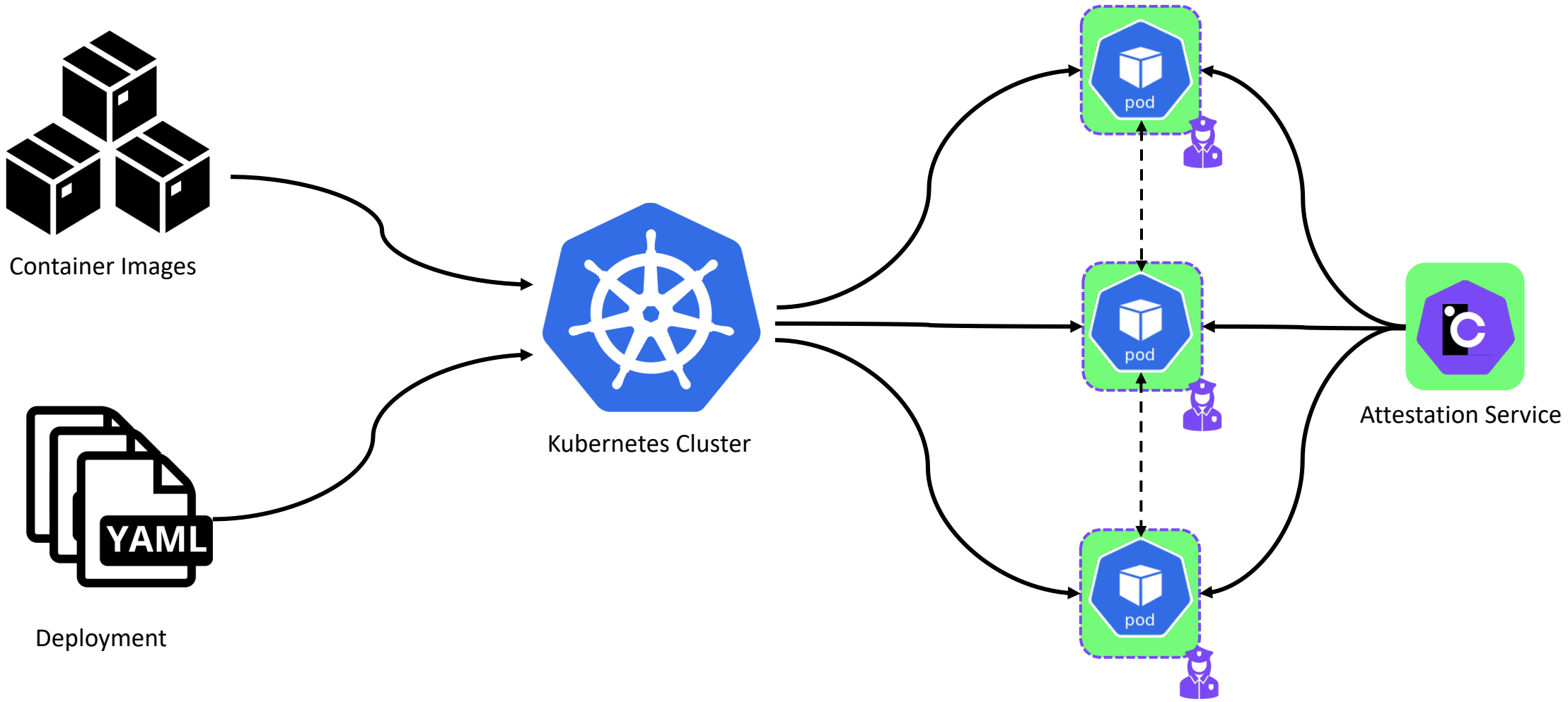
Confidential K8s deployment



Edgeless Systems

04 Contrast

Contrast


Container Images
YAML
Deployment
Kubernetes Cluster
pod
pod
pod
Attestation Service

Contrast details