Akraino ICN Family:
Multi-Tenant Secure Cloud Native Platform

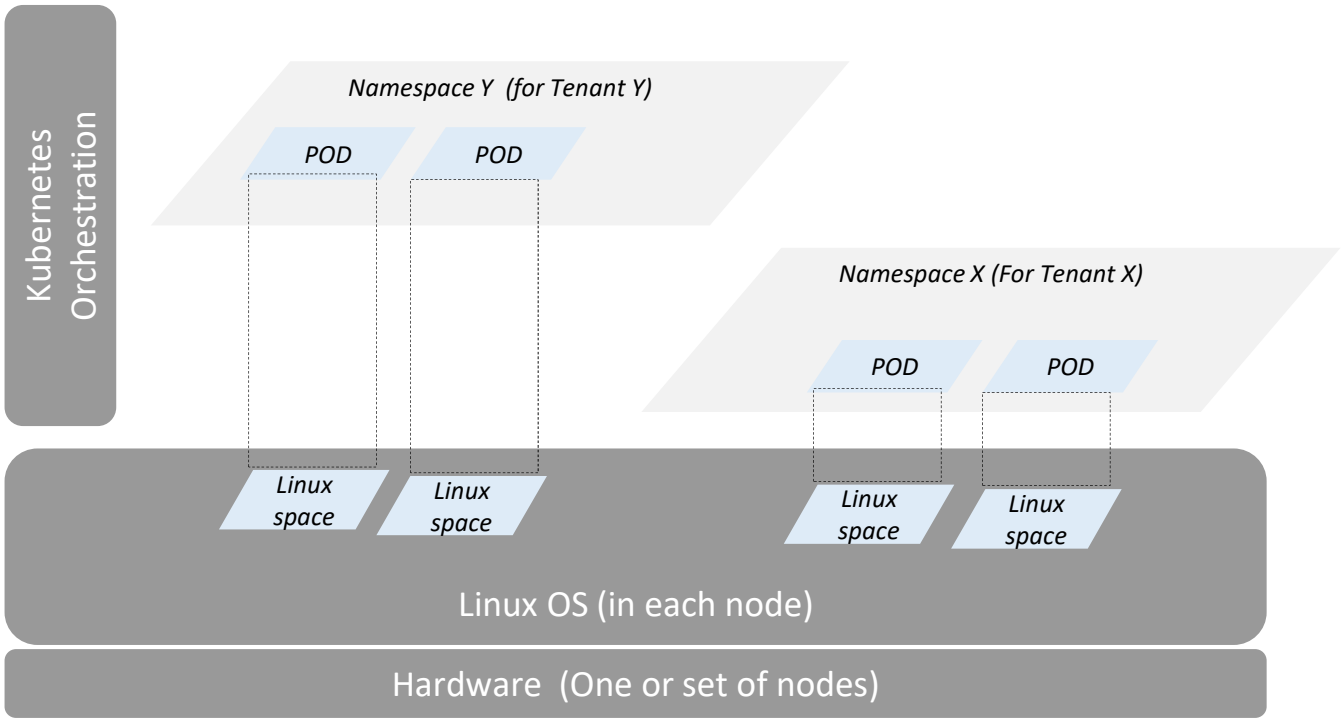
Agenda

- Overview
- Challenges of current multi-tenancy in K8s environments
- Kata Containers
- Enhancing multi-tenancy with Kata
- Architectural changes to current ICN stack

Overview

- This is a new BP, part of the ICN family
- The new BP will reuse most ICN components integrating Kata secure container runtime
- First release targeted for next ICN release in Q2
- Contact: Salvador Fuentes (salvador.fuentes@intel.com)

Multi-tenant isolation in Kubernetes Environments

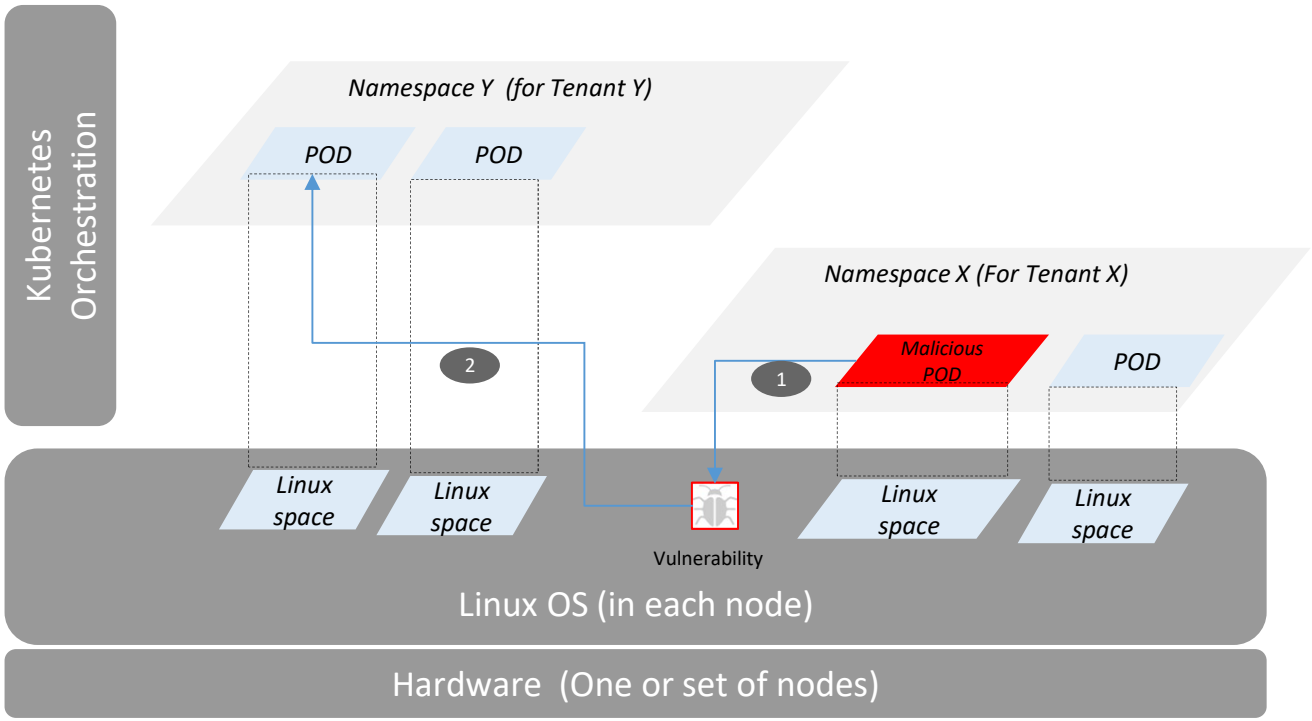


Current solution for Multi-tenancy is based on K8s namespaces.

Namespace does provide operational isolation – Different users and RBAC permissions.

They all share the same Kernel.

Challenges in shared kernel – One example



Problem: Any vulnerability in Linux kernel may be exploited by malicious POD and possibly can inject code in kernel. It can lead to data exfiltration of other tenants and can launch other attacks.

Methods followed today:

- *Dedicated nodes for each namespace.*
- *Dedicated K8s clusters for each tenant*

Challenge: Inefficient usage of resources.

Kata Containers overview

Standard Containers

Cgroups
Namespaces
Capability Filters
Seccomp filtering
Mandatory Access Control (MAC)

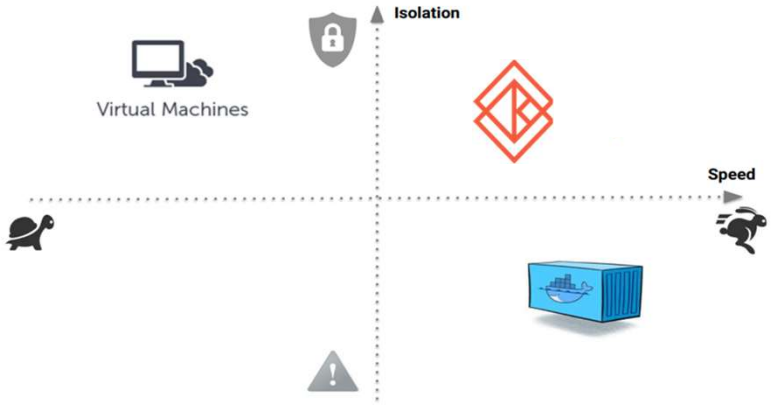
+

Virtual Machines

Separate Guest Kernel
  VMX non-root
Hardware control
  CPU Access
  Memory Access
  Device Access

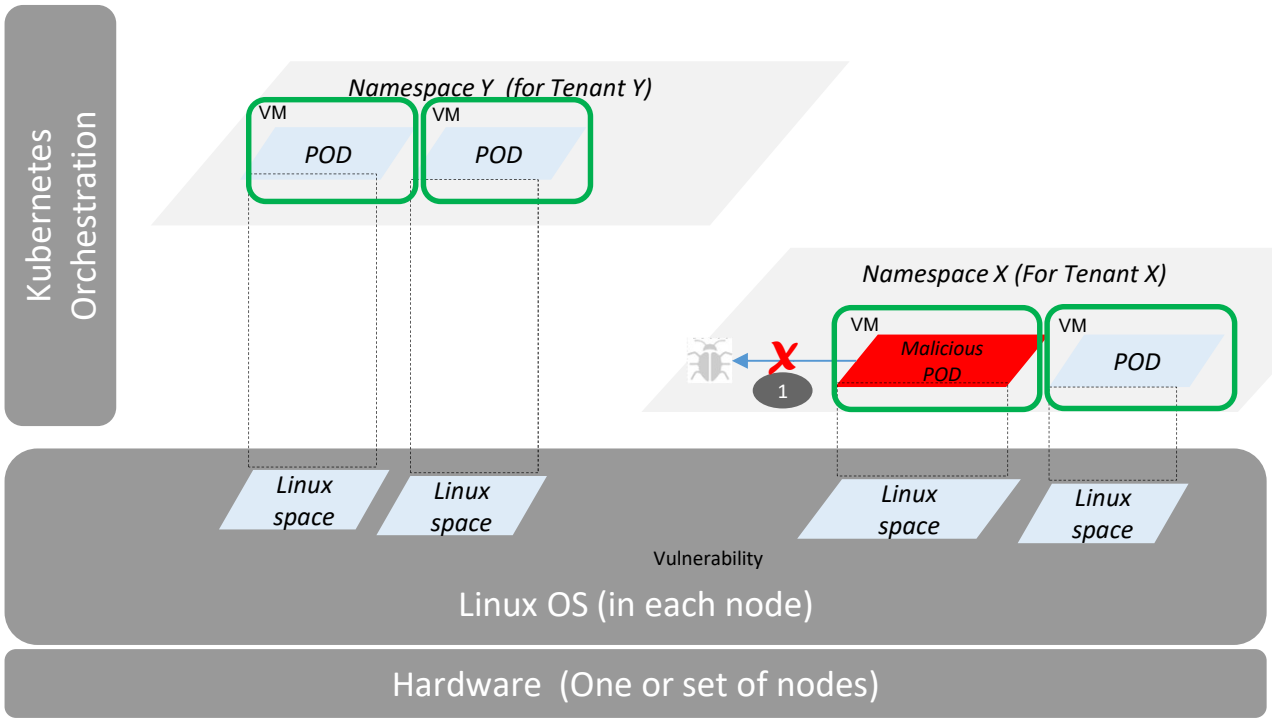
=

Kata Containers



The speed of containers,
the security of VMs.

Securing containers from exploiting others



Need:

- *Use same set of nodes for all tenant workloads, yet provide security isolation*

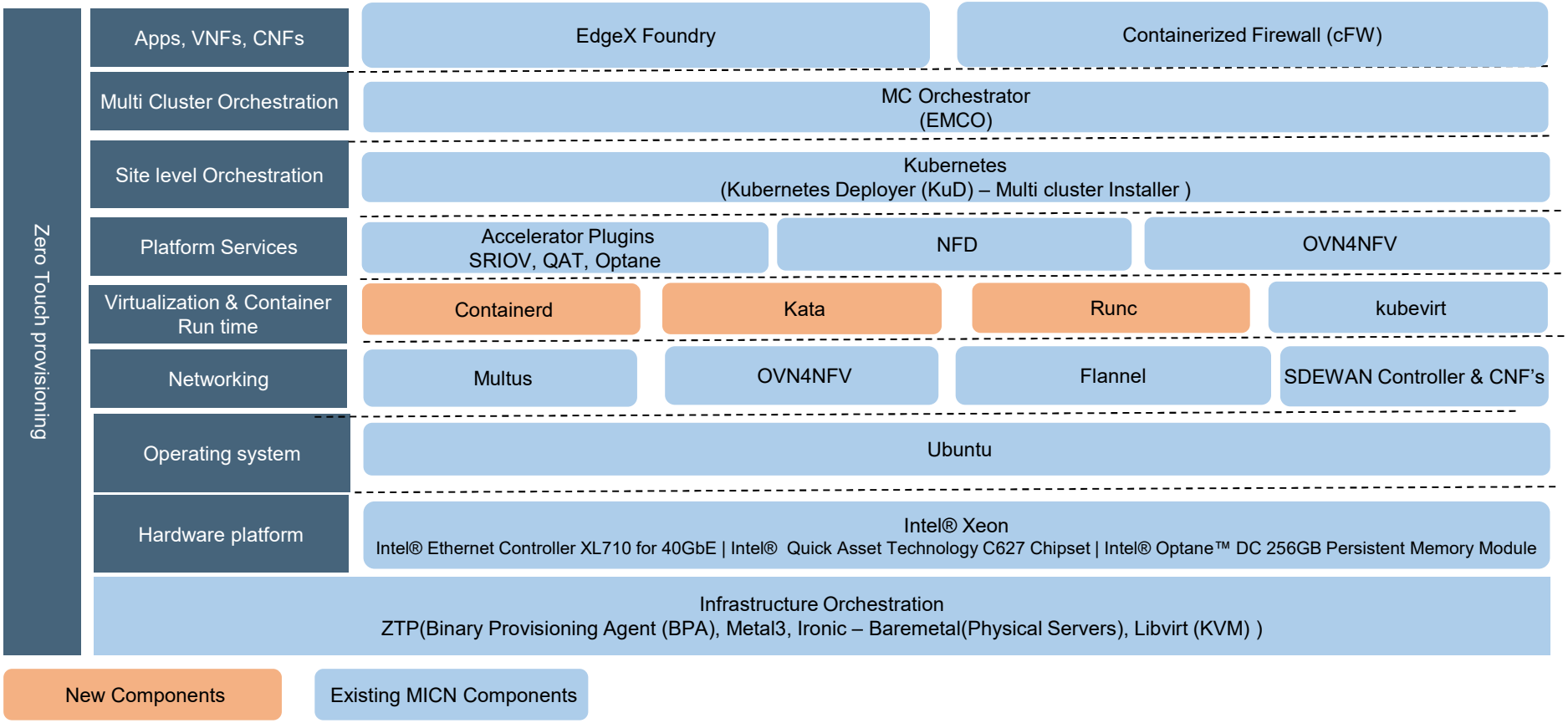
Solution:

- *Kata Containers (Uses hardware virtualization)*

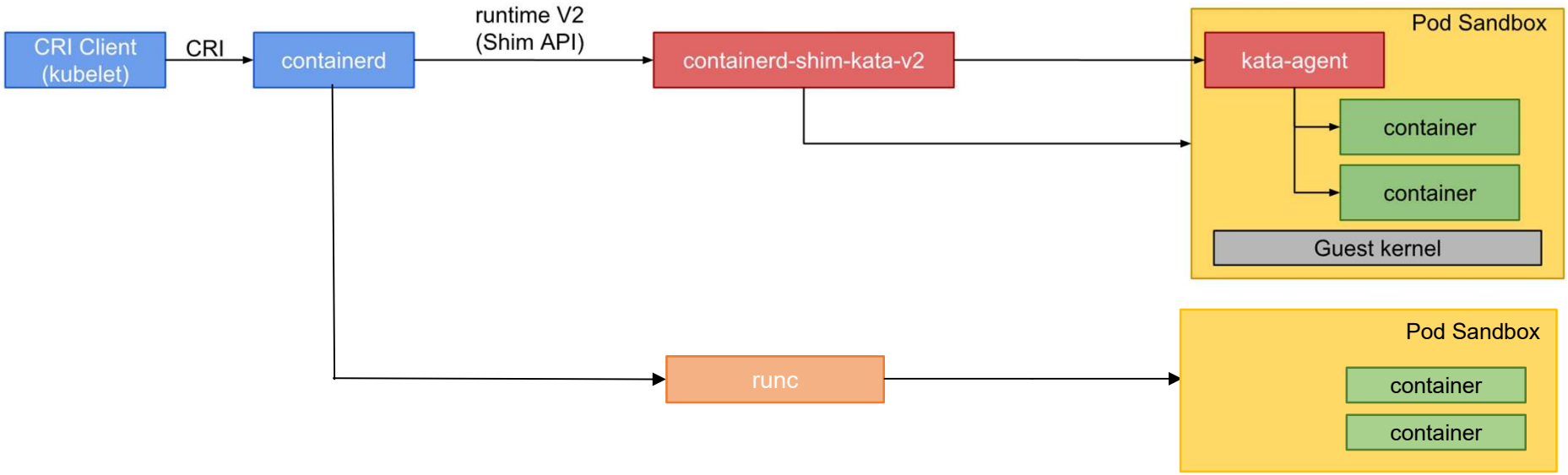
Transparent to developers

- *No changes to container images.*
- *Same images can be used in both Kata and non-Kata environments*

Changes to current ICN stack



Kubernetes Architecture with Containerd using Kata and runc



Call to Action

- Interested? Please reach out:
  - Wiki page
    - https://wiki.akraino.org/pages/viewpage.action?pageId=28973559
  - BP community call on Fridays at 7 AM Pacific Time (bi-weekly)
    - https://lists.akraino.org/g/blueprints/calendar
  - Kata Community
    - https://github.com/kata-containers/community/blob/master/CONTRIBUTING.md

Thank you