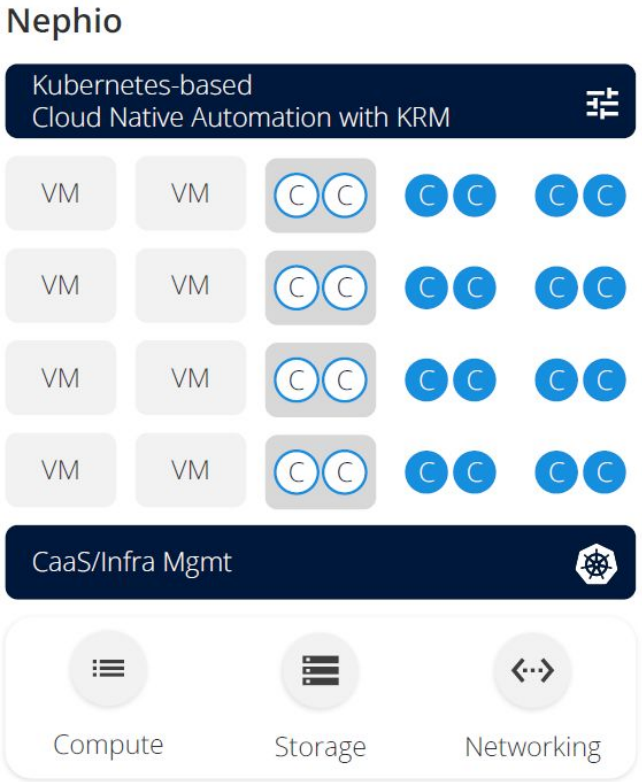
Nephio Security

Tech Talk

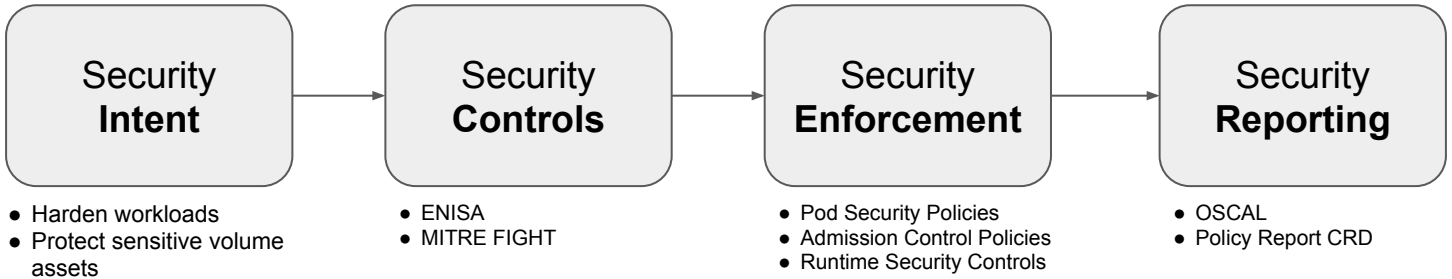
Nephio Security Considerations

- K8s-native design
  - Pod as an execution unit
- Having co-located workloads from different vendors has risks
- Heterogeneous environments
- Assume that basic security practices are in place:
  - Code Scanning
  - Secrets Scanning
  - Image Vulnerability Scanning
  - Cloud Account Configuration Scanning

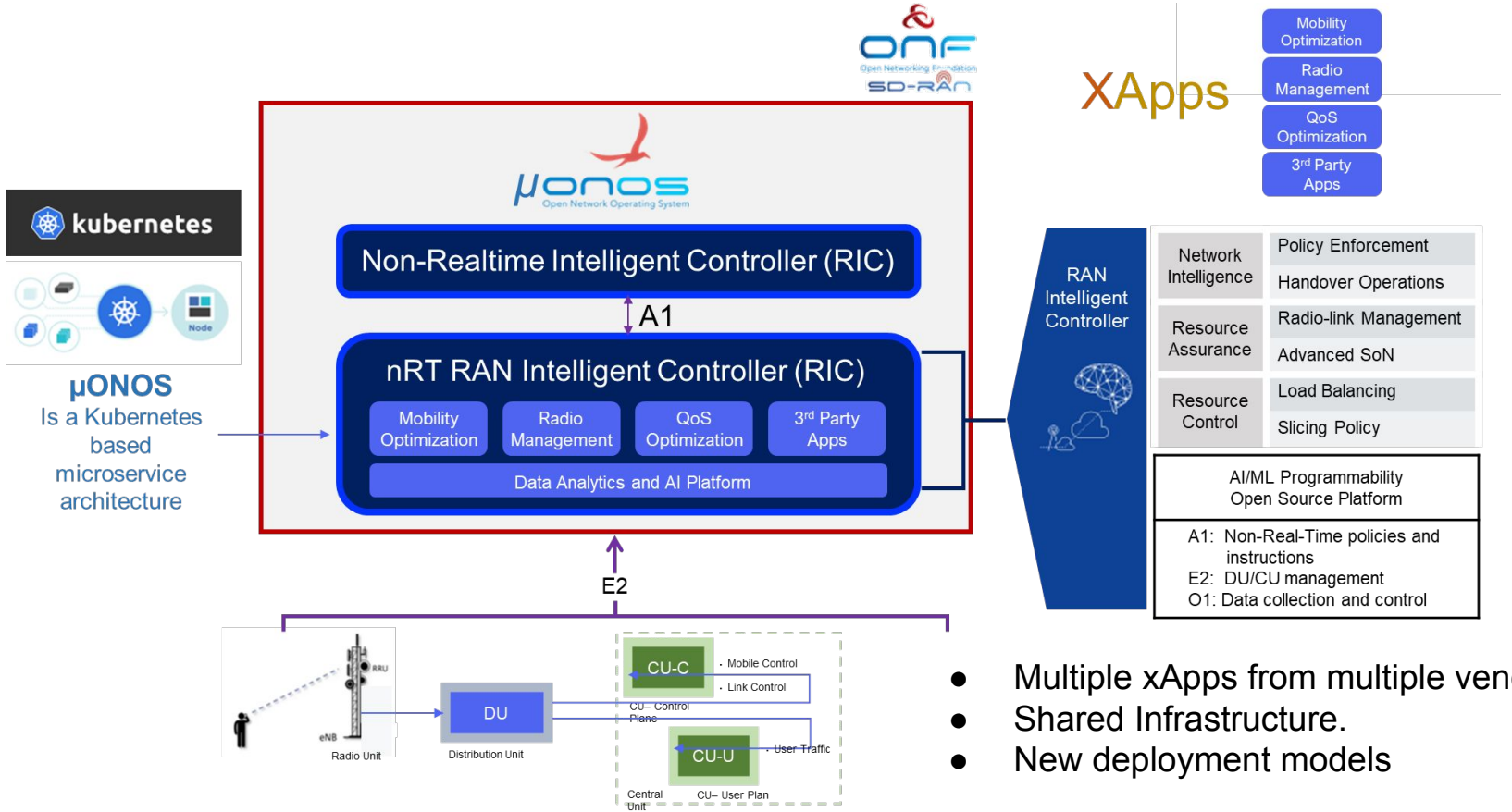


Intent Driven Security Automation

- Intent driven security automation
  - Specify intent using k8s resource model
  - Deploy appropriate k8s resources to enforce given intent

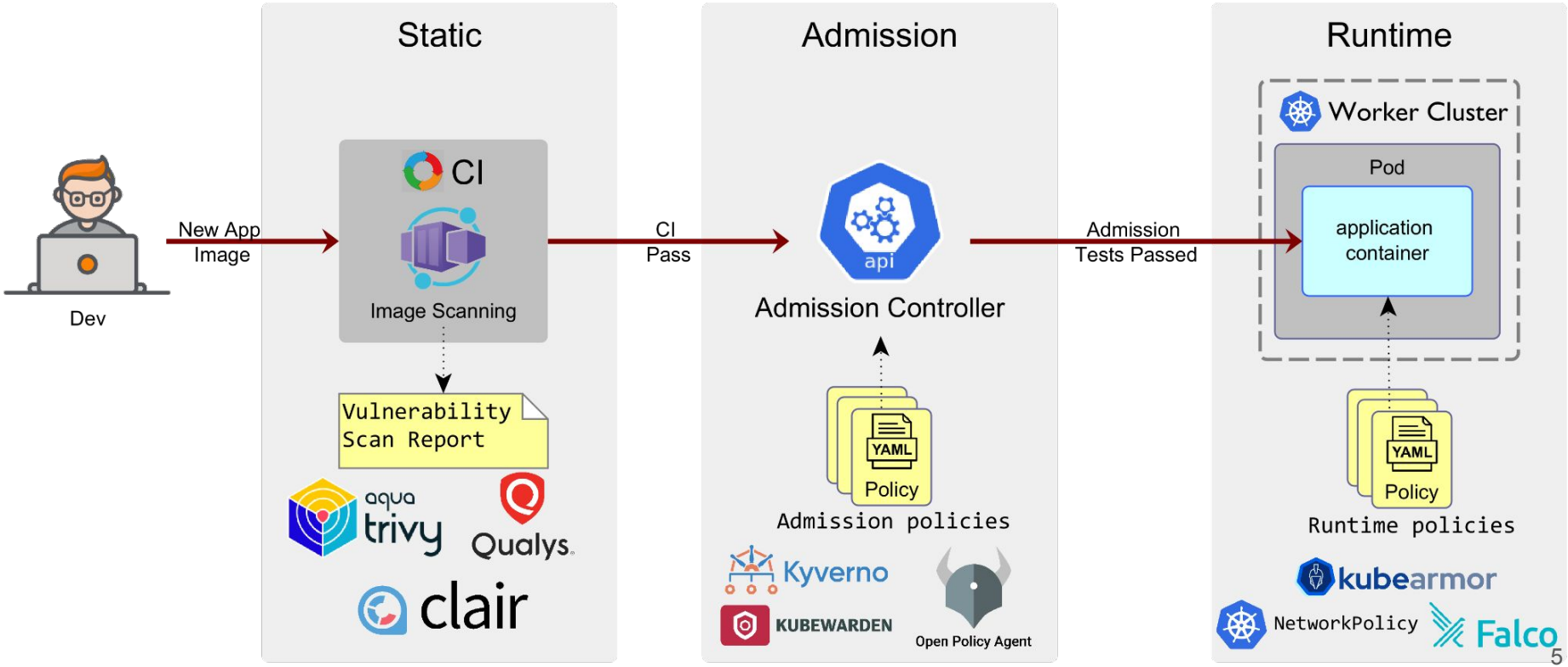


Use-case: Securing RIC



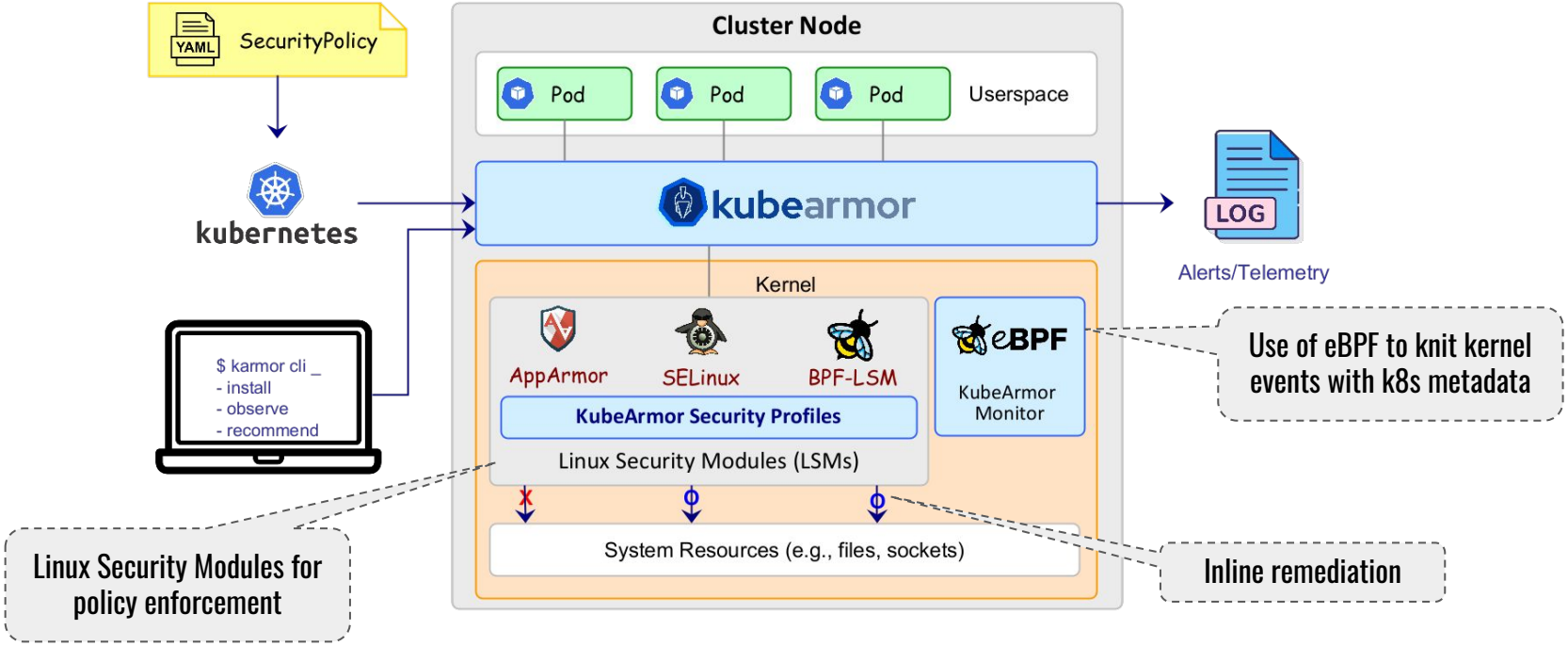
- Multiple xApps from multiple vendors
- Shared Infrastructure.
- New deployment models

Static vs Admission vs Runtime Security



KubeArmor Runtime Security

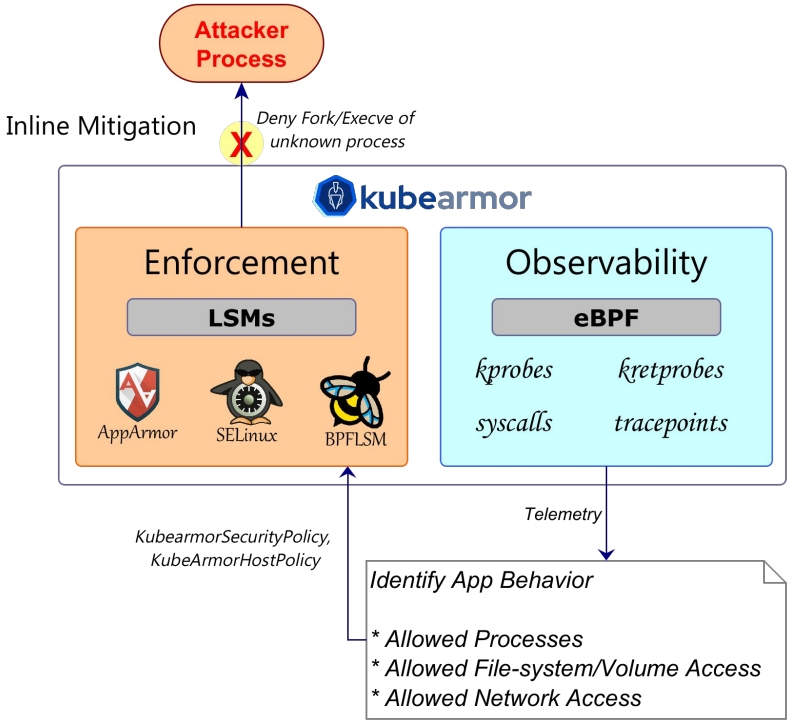
CLOUD NATIVE SANDBOX

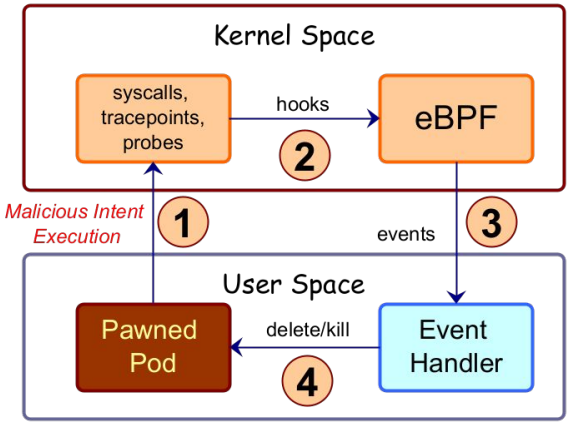


https://github.com/kubearmor/

kubearmor.io

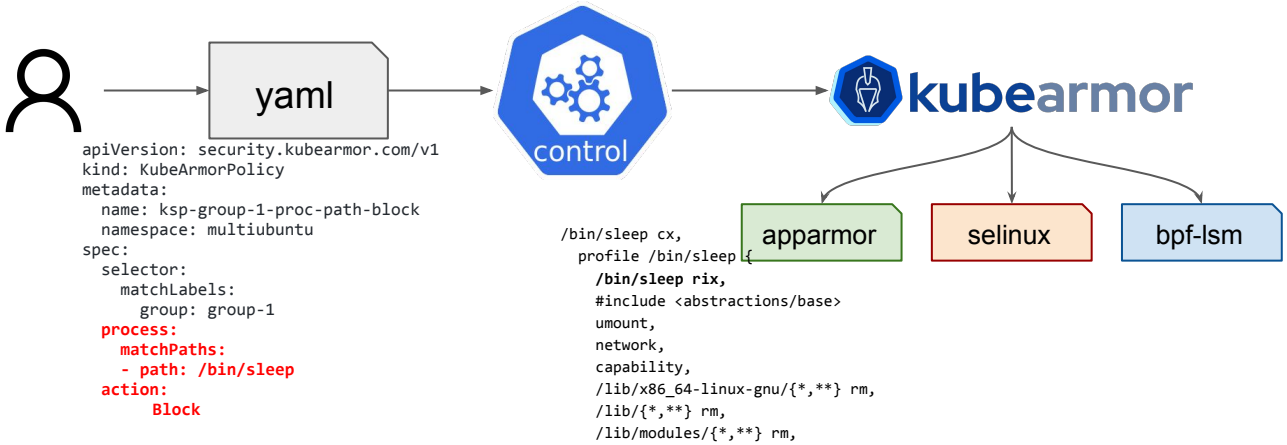
Inline Mitigation vs Post-Attack Mitigation



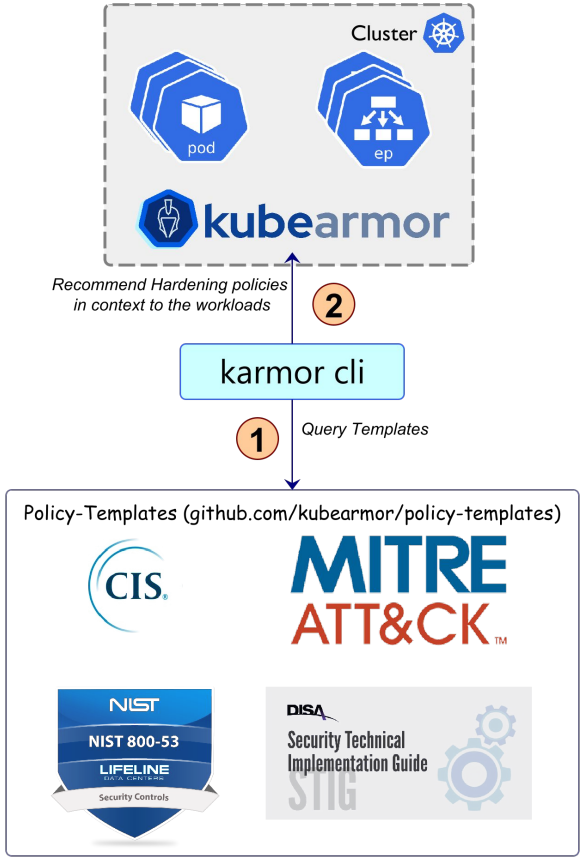


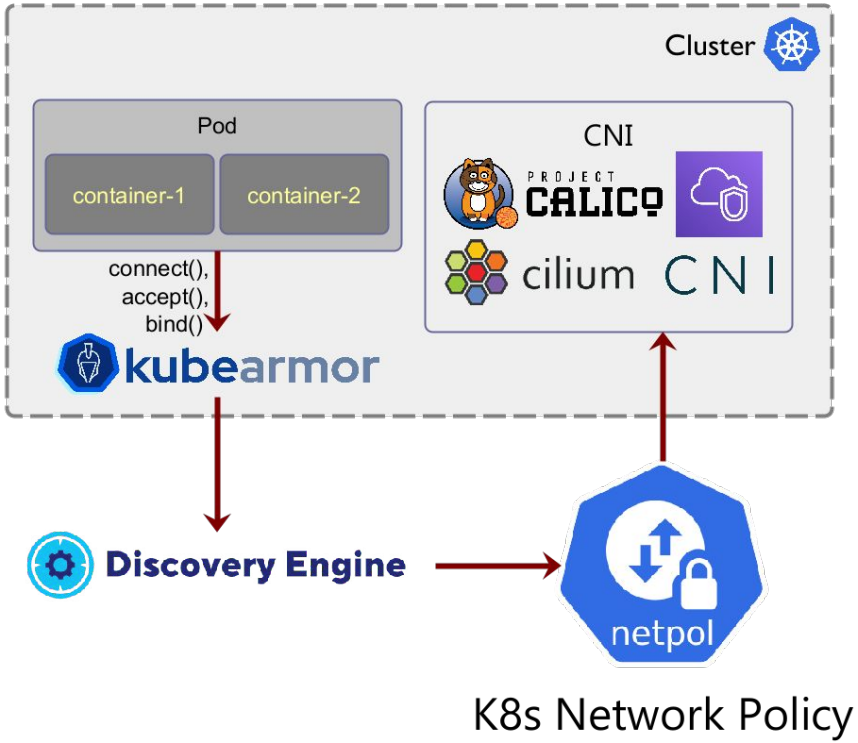
KubeArmor: Abstracting LSMs

- Makes LSMs easier to consume
  - Deploys as daemonset. Maps YAML rules to LSM (apparmor, bpf-lsm) rules.
- Consistent Alerting
  - Handles kernel events and maps k8s metadata using ebpf.



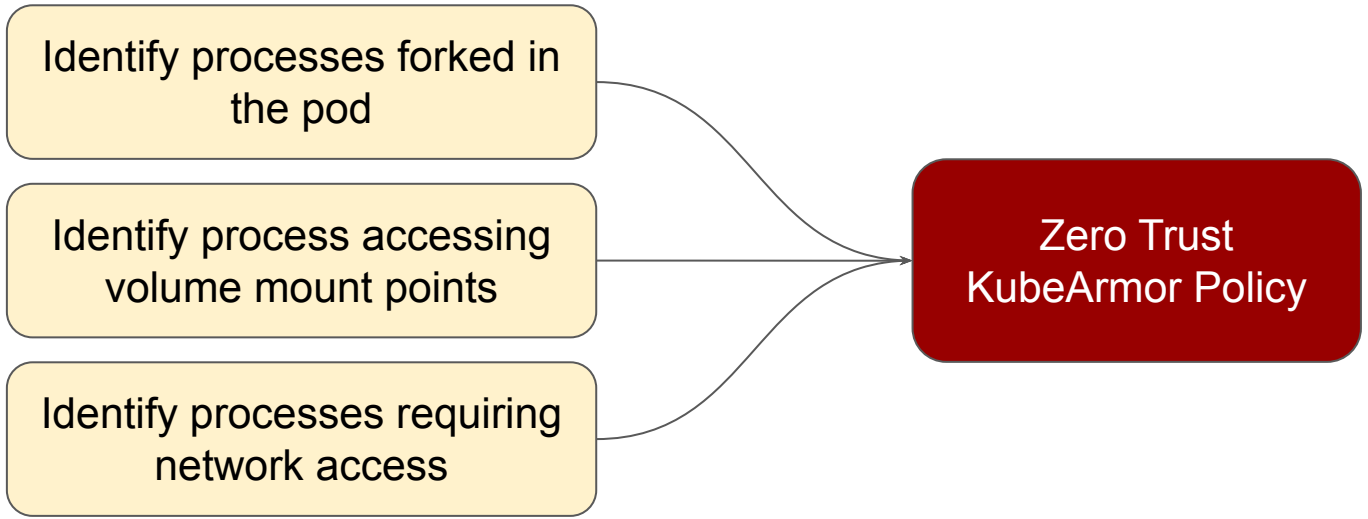
Use-cases: Continuous Compliance, Network Segmentation





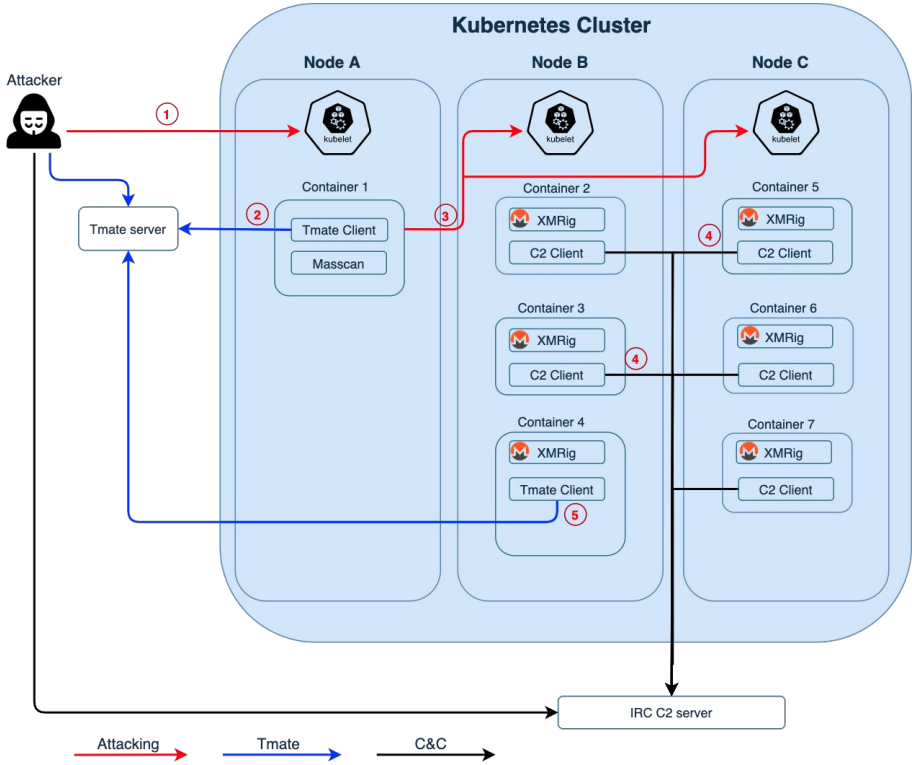
Use-case: Zero Trust Policies

- Allow specific, deny/audit everything else
  - Process Whitelisting
  - Volume Mount point / File System access whitelisting
  - Process based Network Access whitelisting



Hildegard Attack: K8s based TTPs

- Initial Access: Misconfigured kubelet allows anon access
- Malware attempted to spread over as many containers as possible using service account tokens and eventually launched cryptojacking operations.
- Two C&C conns: Reverse tmate shell and IRC channel
- Uses a known Linux process name (bioset) to disguise the malicious process.
- LD_PRELOAD to hide the malicious processes.
- Encrypts the malicious payload inside a binary to make automated static analysis more difficult.



Recap on Hildegard attack: KubeArmor protection

- Malware attempted to spread over as many containers as possible using service account tokens and eventually launched cryptojacking operations.
  - *Service account token access is strictly controlled.*
  - *Allow only specific processes to access service account token.*
- Two C&C conns: Reverse tmate shell and IRC channel
  - *Network access is allowed for known binaries only.*
- Uses a known Linux process name (bioset) to disguise the malicious process.
  - *FIM disallows modifications in systems binary folder*
- LD_PRELOAD to hide the malicious processes.
  - *Process execution is tapped in kernel space*
- Encrypts the malicious payload inside a binary to make automated static analysis more difficult.
  - *Process whitelisting and binary tracking audits all the events.*

KubeArmor Demo Policies

```yaml
apiVersion: security.accuknox.com/v1
kind: KubeArmorPolicy
metadata:
  name: ksp-mysql-dir-audit
  namespace: wordpress-mysql
spec:
  selector:
    matchLabels:
      app: mysql
  file:
    matchDirectories:
    - dir: /var/lib/mysql/
      recursive: true
  action:
    Audit
  severity: 1
```

```yaml
apiVersion: security.accuknox.com/v1
kind: KubeArmorPolicy
metadata:
  name: ksp-wordpress-process-block
  namespace: wordpress-mysql
spec:
  severity: 3
  selector:
    matchLabels:
      app: wordpress
  process:
    matchPaths:
    - path: /usr/bin/apt
    - path: /usr/bin/apt-get
  action:
    Block
```

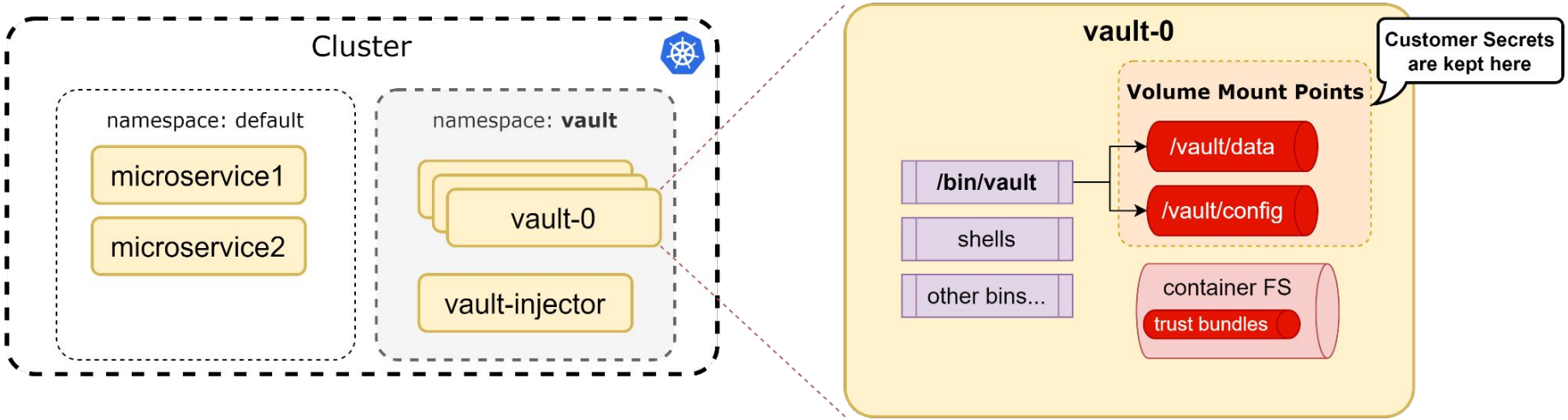
```yaml
apiVersion: security.accuknox.com/v1
kind: KubeArmorPolicy
metadata:
  name: ksp-wordpress-config-block
  namespace: wordpress-mysql
spec:
  severity: 10
  selector:
    matchLabels:
      app: wordpress
  file:
    matchPaths:
    - path: /var/www/html/wp-config.php
      fromSource:
        path: /bin/apache2

  # cd /var/www/html
  # cat wp-config.php

  action:
    Allow
```

```yaml
apiVersion: security.accuknox.com/v1
kind: KubeArmorPolicy
metadata:
  name: ksp-wordpress-sa-block
  namespace: wordpress-mysql
spec:
  severity: 7
  selector:
    matchLabels:
      app: wordpress
  file:
    matchDirectories:
    - dir: /run/secrets/kubernetes.io/serviceaccount/
      recursive: true

# cat /run/secrets/kubernetes.io/serviceaccount/token
# curl https://$KUBERNETES_PORT_443_TCP_ADDR/api --insecure --header \
  "Authorization: Bearer $(cat /run/secrets/kubernetes.io/serviceaccount/token)"

  action:
    Block
```

MITRE | ATT&CK®

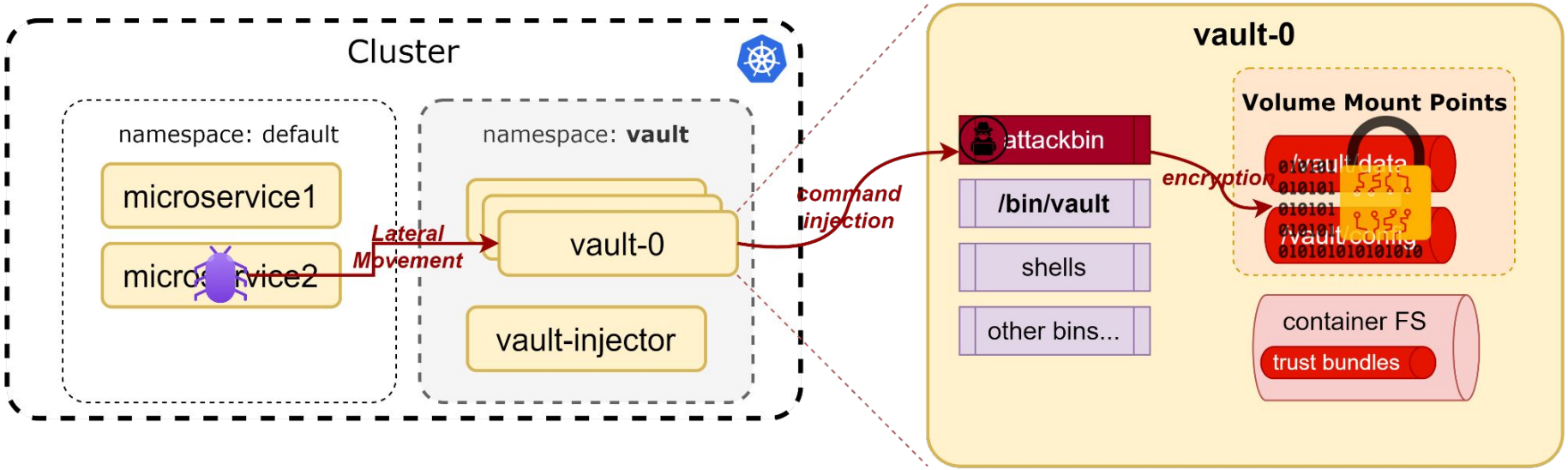
Lateral Movement	Credential Access	Execution
Access cloud resources	App credentials in config files	bash/cmd inside container
App credentials in config files	Access container service account	

Point in case (demo): HashiCorp Vault



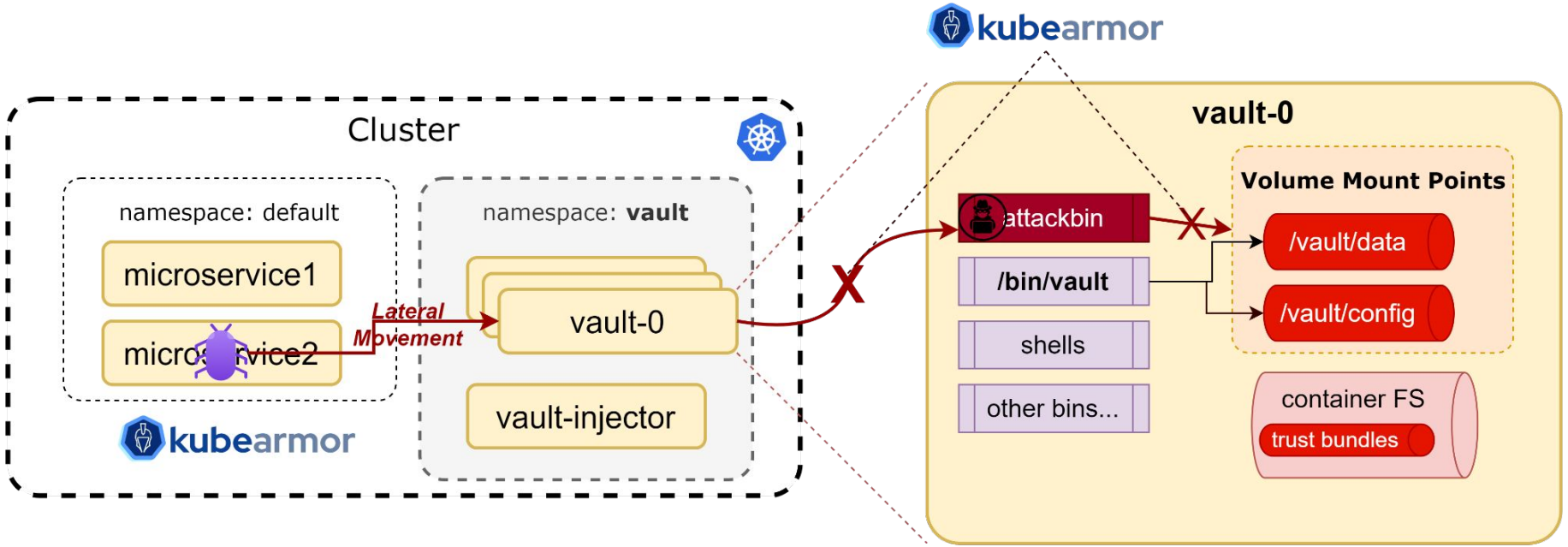
- Customer secrets are kept in persistent volume mounted in *vault-** stateful sets/pods
- Usually on */bin/vault* accesses this volume mount points

Ransomware Attacker's sweet spot



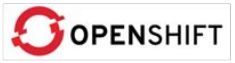
Organizations will pay for getting back access to their secrets.

KubeArmor Protection



KubeArmor Protection

- Only */bin/vault* process to access */vault/* folder.
- Allow execution of specific processes only
  - /bin/vault
  - /bin/vault-tool
- Multicloud support
  - Supported on all managed/unmanaged cloud platform
- Integrate in CI/CD pipeline




```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  name: ksp-vault-protect
  namespace: vault
spec:
  severity: 7
  selector:
    matchLabels:
      app.kubernetes.io/name: vault
      component: server
  file:
    matchDirectories:
      - dir: /vault/
        recursive: true
        action: Block
      - dir: /
        recursive: true
      - dir: /vault/
        recursive: true
        fromSource:
          - path: /bin/vault
  process:
    matchPaths:
    - path: /bin/busybox
    - path: /bin/vault
  action: Allow
```

Block access to /vault/

Allow access to /vault/ from /bin/vault only

Process Whitelisting

Google Kubernetes Engine

Amazon EKS

RED HAT® OPENSHIFT Container Platform

Amazon Linux

Bottlerocket

Red Hat Enterprise Linux

ORACLE

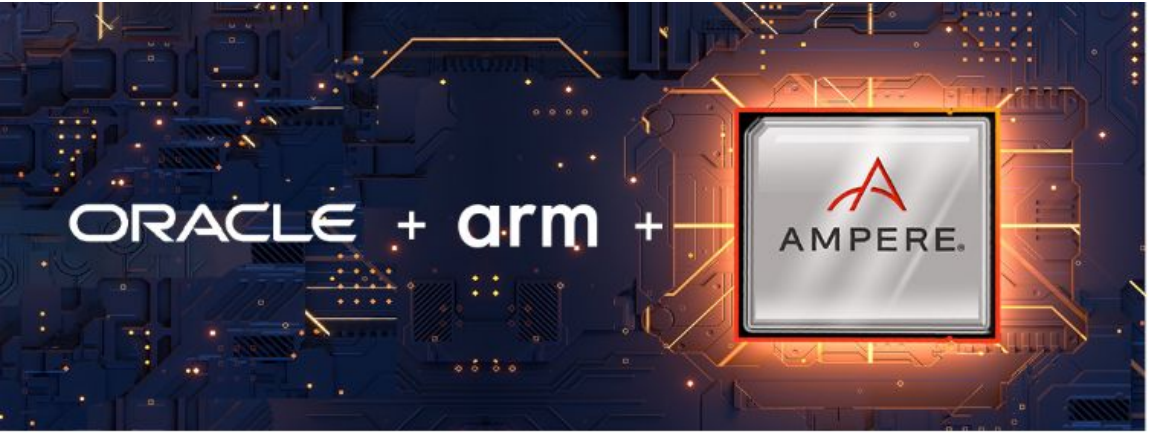
IBM Cloud Kubernetes Service

Azure Kubernetes Service (AKS)

On-prem

RANCHER BY SUSE

- Deploys as a DaemonSet
- Operates across any k8s provider or onprem
- CRI supported: docker, containerd, crio



5G security work in progress context to KubeArmor

- 5gsec.com
  - SRI + Ohio State University + KubeArmor
- 5G SBP (Super Blue Print) (ref)
- LF Edge Open Horizon POC (ref)

What could be the next steps?