

# SECURING CONTAINERS WITH OPENSHIFT

---

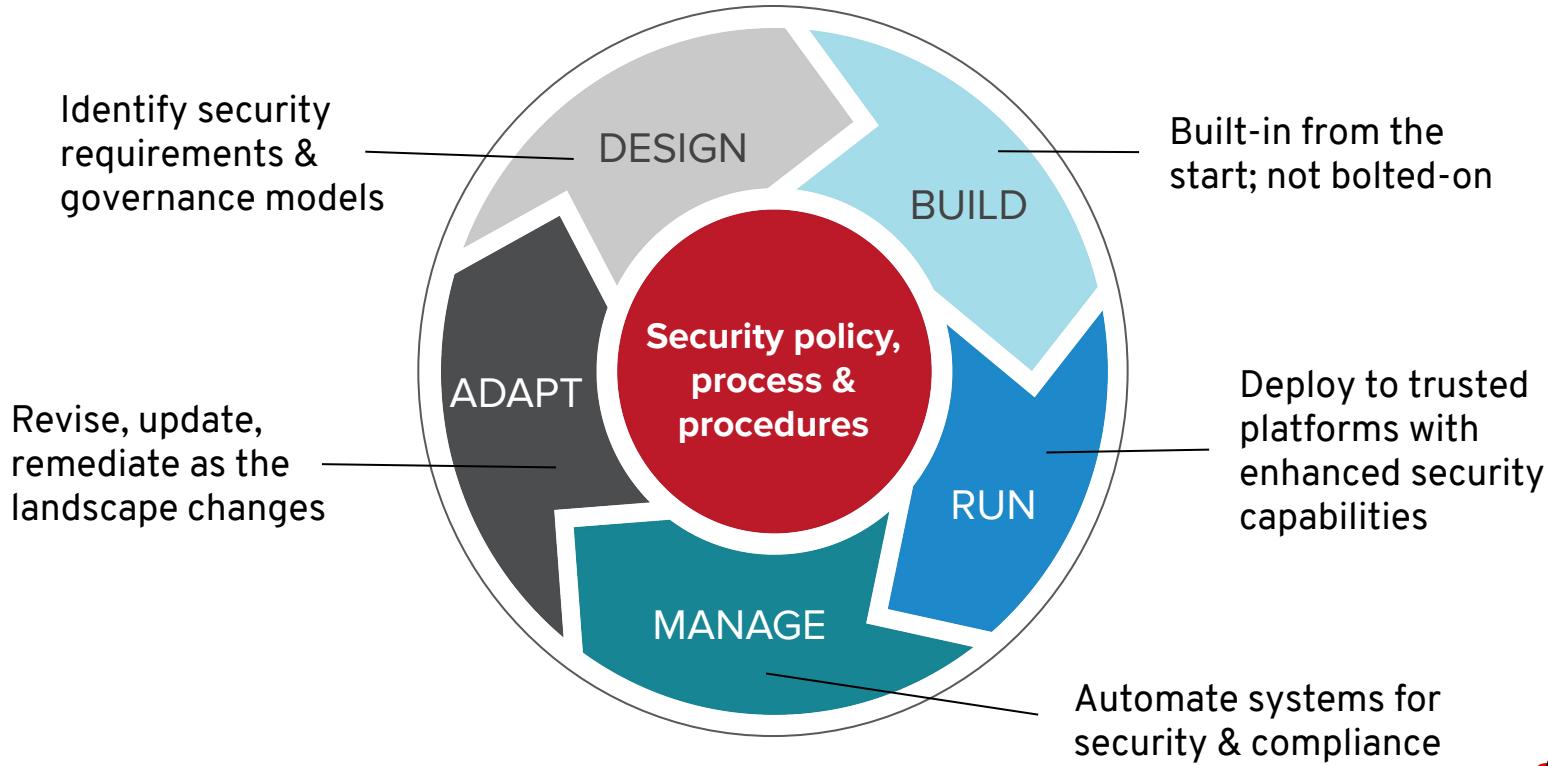
<Name>

<Title>

<Date>

# SECURITY MUST BE CONTINUOUS

And integrated throughout the IT lifecycle



# COMPREHENSIVE CONTAINER SECURITY



## CONTROL

Application  
Security

Container Content

CI/CD Pipeline

Container Registry

Deployment Policies



## DEFEND

Infrastructure

Container Platform

Container Host Multi-tenancy

Network Isolation

Storage

Audit & Logging

API Management



## EXTEND

Security Ecosystem

# HARDENING TOOLS & APPLICABILITY GUIDES

## Product Applicability Guides

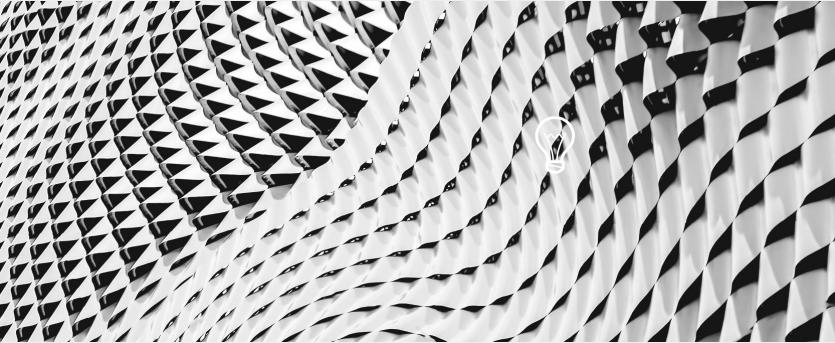
- [FISMA Moderate](#) & [FISMA](#) (NIST)
- [ISO 27001](#)
- [PCI-DSS](#)
- [PCI-DSS Reference Architecture](#)

OpenShift Hardening Guide for 3.10 & 3.11 - OpenShift 4 Guide planned for Fall 2019

## Upstream, 3rd party tools

- [docker-bench](#) supports versions 1.13 and 17.06
- [kube-bench](#) → WIP, support for OCP 3.9 & 3.10

# CONTROL APPLICATION SECURITY



# DEVSECOPS

## THROUGH THE ADOPTION OF CONTAINERS

We created Dev and Ops and Security user stories and tackled them together.



DEVELOPER

I can break builds if security and compliance rules aren't followed...



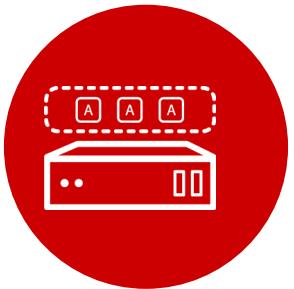
SECURITY

We're empowering the developers and ideally empowering them straight to production.

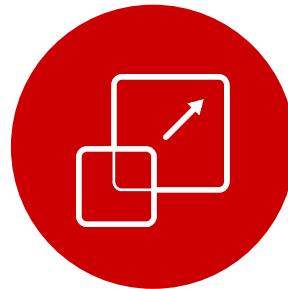


OPERATIONS

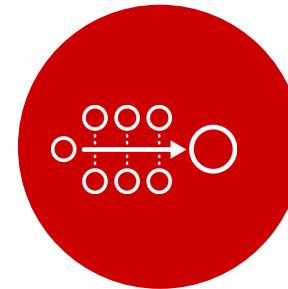
# OPENSHIFT LOVES CI/CD



JENKINS-AS-A SERVICE  
ON OPENSHIFT

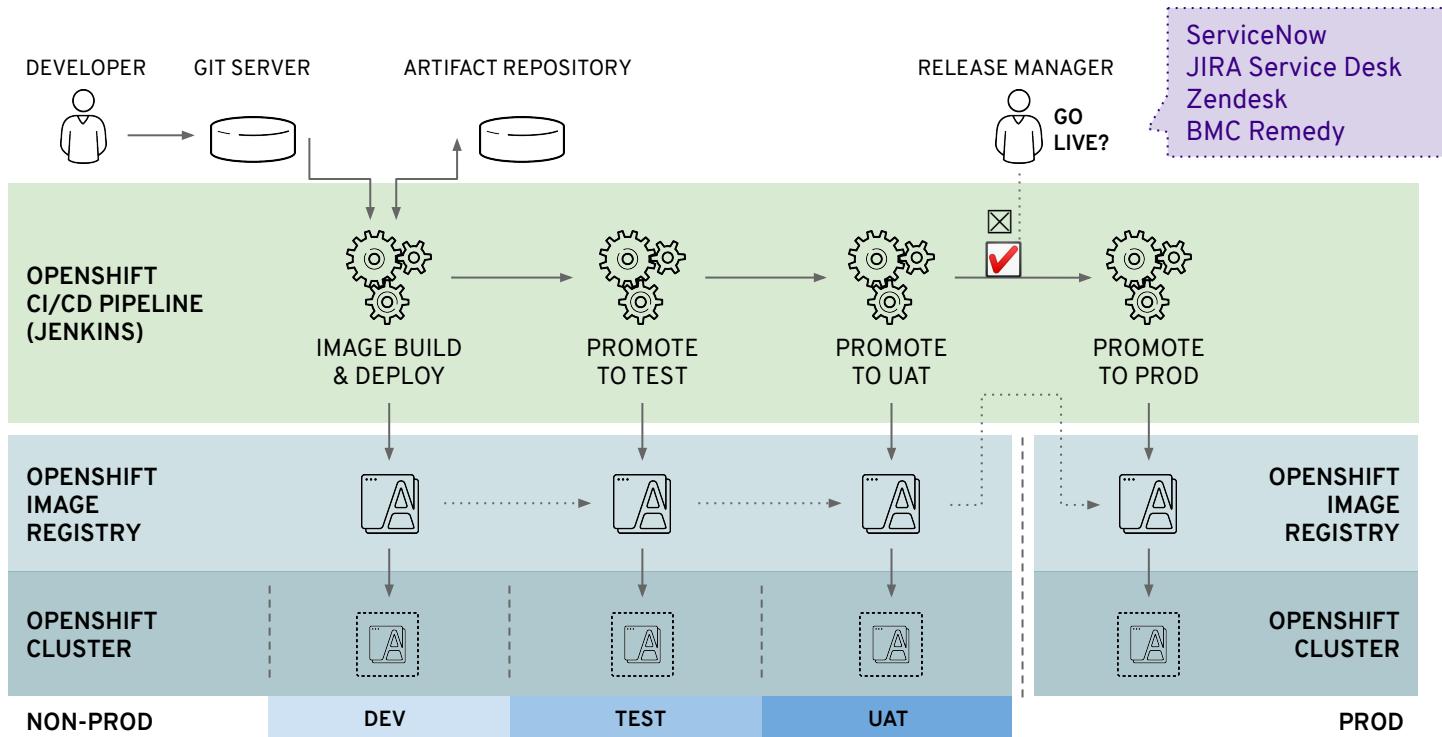


HYBRID JENKINS INFRA  
WITH OPENSHIFT



EXISTING CI/CD  
DEPLOY TO OPENSHIFT

# USE THE OPENSOURCE PIPELINE



# OR USE EXISTING DELIVERY PROCESSES

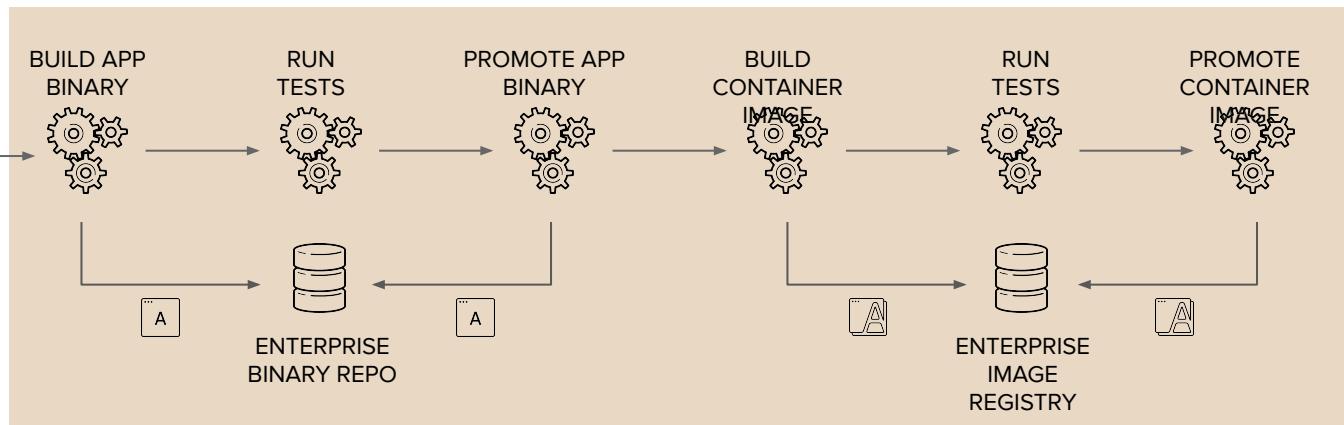


GitLab  
GitHub  
Bitbucket

Microsoft Visual Studio Team Foundation

SOURCE VERSION CONTROL

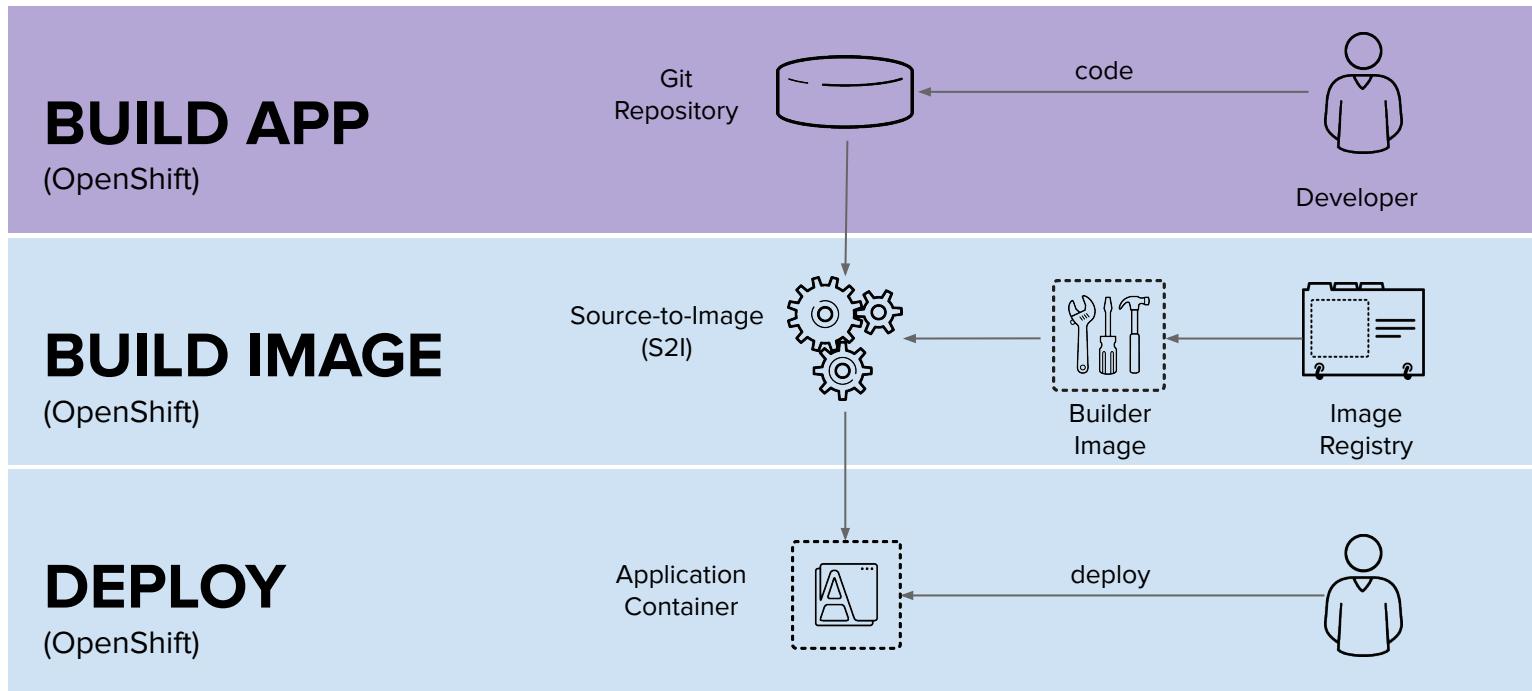
Jenkins CI, Bamboo, Travis CI, CircleCI, GitLab, Microsoft Visual Studio Team Foundation, Codeship, Tekton



JFrog Artifactory Nexus

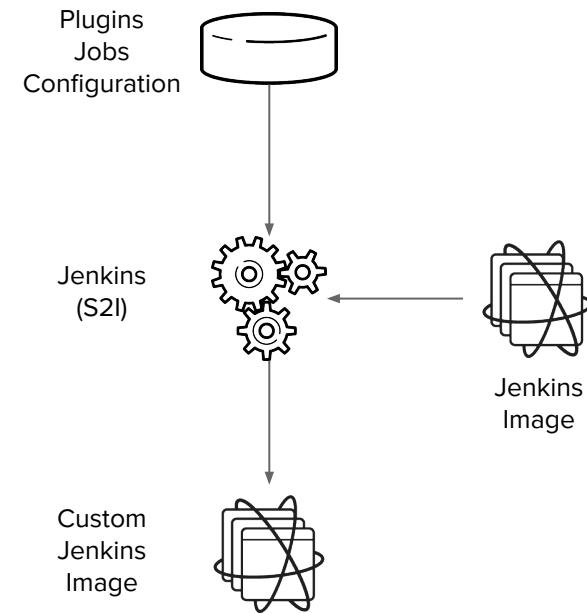
JFrog Artifactory Nexus Sonatype QUAY by CoreOS AWS ECR

# DEPLOY IMAGES, APPLICATION BINARIES OR SOURCE CODE WITH OPENSHIFT



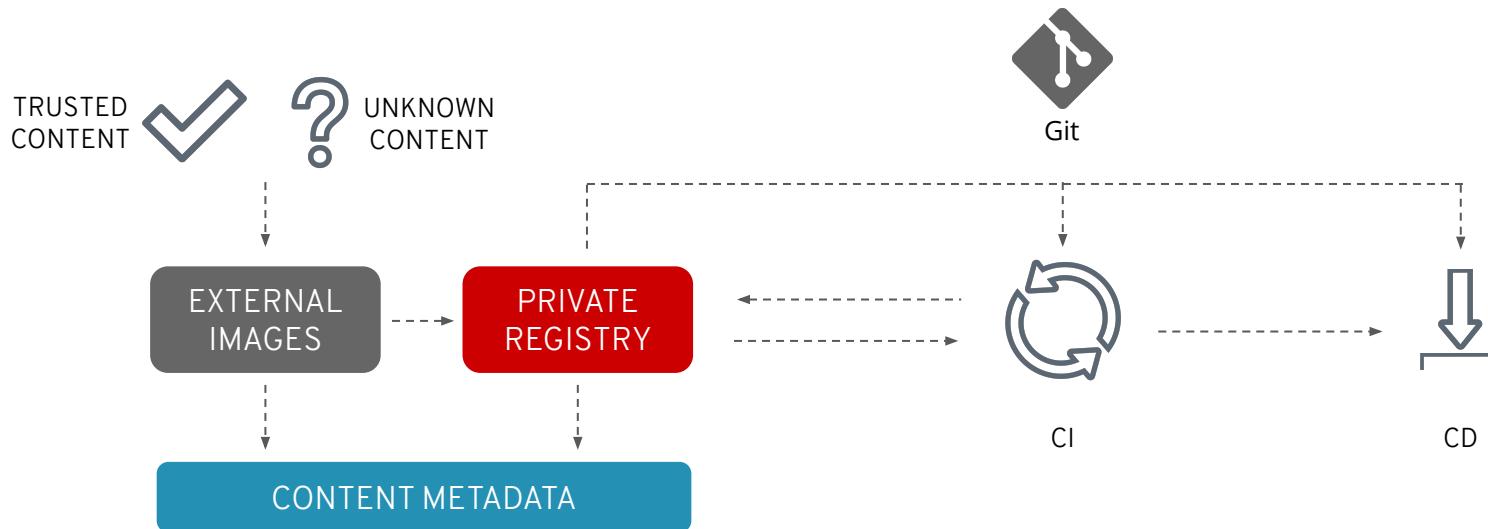
# JENKINS-AS-A-SERVICE ON OPENSHIFT

- Certified Jenkins images with pre-configured plugins
  - Provided out-of-the-box
  - Follows Jenkins 1.x and 2.x LTS versions
- Jenkins S2I Builder for customizing the image
  - Install Plugins
  - Configure Jenkins
  - Configure Build Jobs
- OpenShift plugins to integrate authentication with OpenShift and also CI/CD pipelines
- Dynamically deploys Jenkins slave containers



# SECURE & AUTOMATE THE CONTENT LIFECYCLE

Elements of the Openshift container pipeline



# EXTERNAL CONTENT: USE TRUSTED SOURCES

## Red Hat Container Images

- Signed Images
- Health Index (A to F grade)\*
- Security advisories & errata (patches)

The screenshot shows the Red Hat Container Catalog interface. At the top, there is a search bar with the text "python". Below the search bar, there are navigation links: "Explore", "Get Started", and "FAQ". On the right side of the header, there are icons for "Service Accounts" and a user profile.

The main content area displays a container image entry for "rhscl/python-36-rhel7". The title is "rhscl/python-36-rhel7" and the description is "Python 3.6 platform for building and running applications". It is listed as "by Red Hat, Inc." in the "Product Red Hat Enterprise Linux".

Below the description, there are tabs: "Overview" (which is selected), "Get This Image", "Tech Details", "Support", and "Tags".

The "Description" section contains a detailed paragraph about Python 3.6 as a container platform, highlighting its features like high-level data structures and dynamic typing.

The "Repository Specifications" section includes "Registry" (registry.redhat.io) and "Namespace/Repository" (rhscl/python-36-rhel7). There is also a "Screenshot" button.

On the right side, there is a sidebar titled "Most recent tag" with a "View All Tags" link. It shows a single tag entry: "Updated 6 days ago" followed by a blue tag icon with the number "1-55".

Below the tag sidebar, there are sections for "Health Index" (grade A) and "Security" (status: Signed, Unprivileged).

# RED HAT QUAY ENTERPRISE CONTAINER REGISTRY

- Offered as self-managed and as-a-service
- Vulnerability Scanning (Clair)
- Geographic Replication
- Build Image Triggers
- Image Rollback with Time Machine

RED HAT QUAY EXPLORE REPOSITORIES TUTORIAL

search + ⚡ 0 opentic...

← example/python 3f86e14b88f9

Quay Security Scanner has detected 718 vulnerabilities.  
Patches are available for 144 vulnerabilities.

47 High-level vulnerabilities.  
220 Medium-level vulnerabilities.  
177 Low-level vulnerabilities.  
266 Negligible-level vulnerabilities.  
8 Unknown-level vulnerabilities.

Vulnerabilities

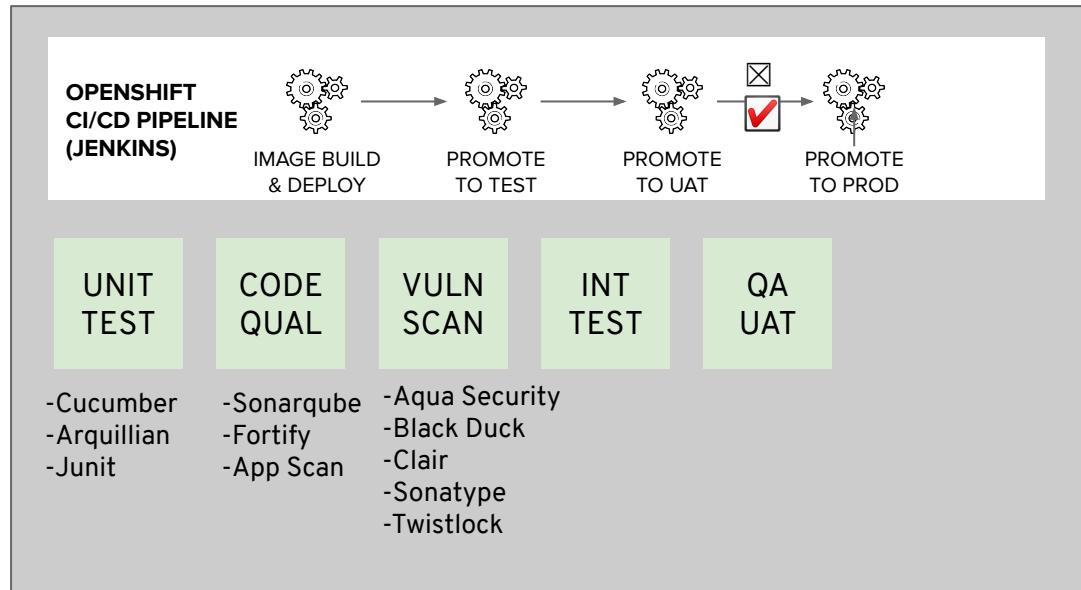
Showing 144 of 718 Vulnerabilities   Only show fixable

CVE	SEVERITY	PACKAGE	CURRENT VERSION	FIXED IN VERSION	INTRODUCED IN LAYER
» CVE-2018-15686	10 / 10	systemd	232-25+deb9u6	232-25+deb9u10	<input type="button" value="ADD"/> file:a61c14b18252183a4719980da97ac483044bca...
» CVE-2019-3855	9.3 / 10	libssh2	1.7.0-1	1.7.0-1+deb9u1	<input type="button" value="RUN"/> apt-get update && apt-get install -y --no-i...
» CVE-2019-3462	9.3 / 10	apt	1.4.8	1.4.9	<input type="button" value="ADD"/> file:a61c14b18252183a4719980da97ac483044bca...
» CVE-2017-16997	9.3 / 10	glibc	2.24-11+deb9u3	2.24-11+deb9u4	<input type="button" value="ADD"/> file:a61c14b18252183a4719980da97ac483044bca...
» CAE-SO17-00001	8.3 / 10	dlipc	5.5.2-11+deb9u3	5.5.2-11+deb9u4	<input type="button" value="ADD"/> file:a61c14b18252183a4719980da97ac483044bca...
» CAE-SO17-00005	8.3 / 10	ebpf	1.4.8	1.4.8	<input type="button" value="ADD"/> file:a61c14b18252183a4719980da97ac483044bca...

 Red Hat

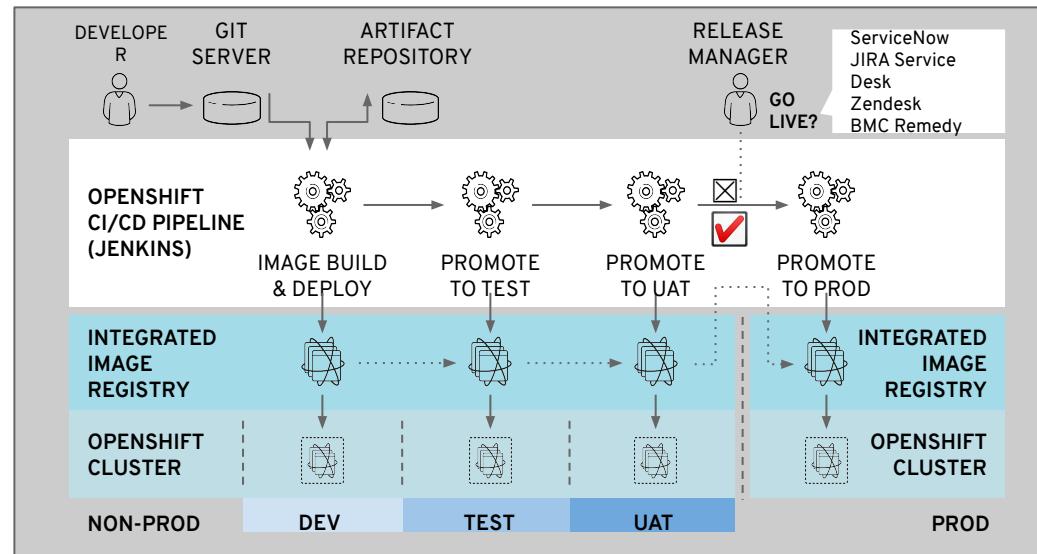
# CI/CD MUST INCLUDE SECURITY GATES

- Integrate security testing into your build / CI process
- Use automated policies to flag builds with issues
- Sign your custom container images



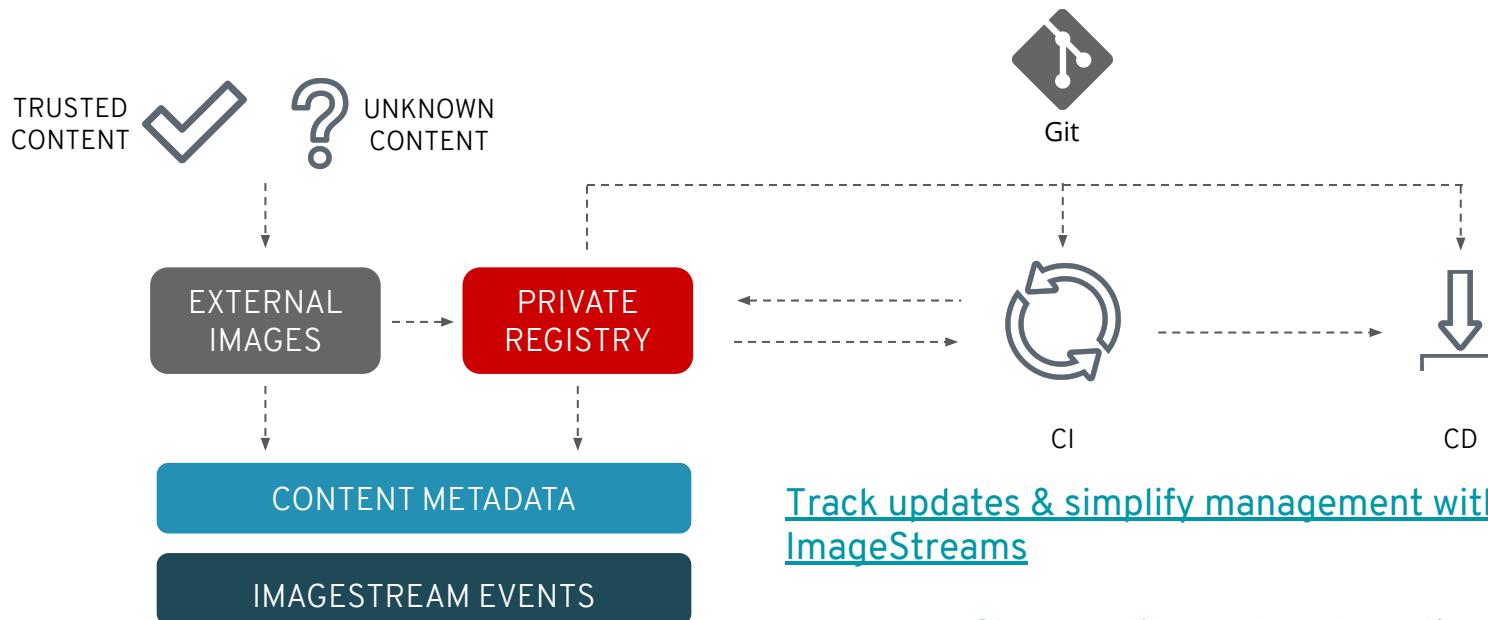
# MANAGING CONTAINER DEPLOYMENT

- Deployments: Containerized App Configuration as Code
- Whitelist / Blacklist external repos
- Apply runtime security policies
- Validate image signatures
- Monitor for new vulnerabilities
- Trust is temporal:  
rebuild & redeploy as needed



# SECURE & AUTOMATE THE CONTENT LIFECYCLE

Trust is temporal; rebuild and redeploy as needed



[Track updates & simplify management with ImageStreams](#)

Use [Image Change Triggers](#) to automatically rebuild custom images with updated (patched) external images

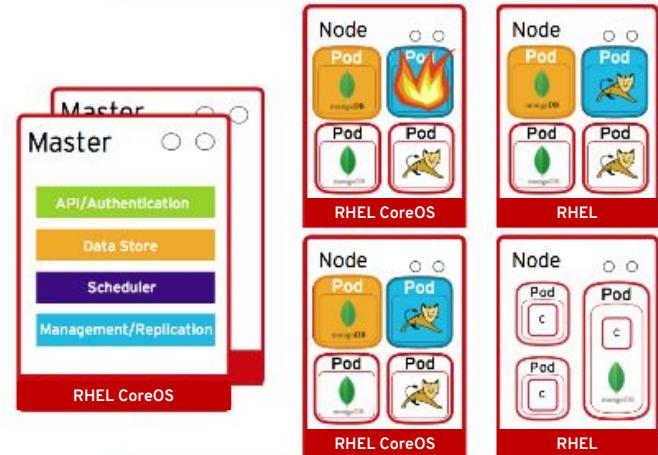
# DEFEND INFRASTRUCTURE



# SECURING THE CONTAINER PLATFORM

## Security Features Include

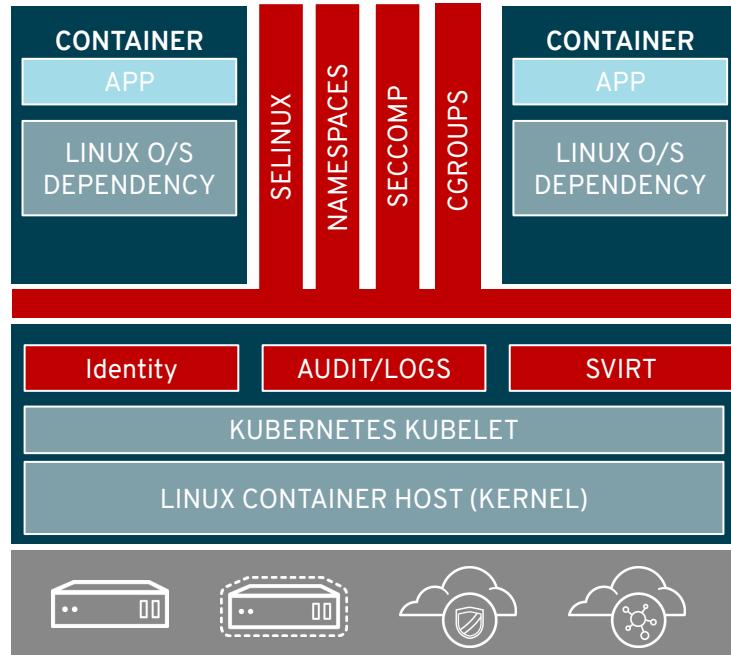
- Host & Runtime security
- Identity and Access Management
- Role-based Access Controls
- Project namespaces
- Integrated SDN - Network Policies is default
- Integrated & extensible secrets management
- Logging, Monitoring, Metrics



# HOST OS CONTAINER MULTI-TENANCY

Container Security starts with Linux Security

- Security in the RHEL host applies to the container
- SELINUX and Kernel Namespaces are the one-two punch no one can beat
- Protects not only the host, but containers from each other
- RHEL CoreOS provides minimized attack surface
- Common Criteria certification



# Container Host Vision

An Ideal Container Host would be	RHEL CoreOS
Minimal	Only what's needed to run containers
Secure	Read-only & locked down
Immutable	Immutable image-based deployments & updates
Always up-to-date	OS updates are automated and transparent
Updates never break my apps	Isolates all applications as containers
Updates never break my cluster	OS components are compatible with the cluster
Supported on my infra of choice	Inherits majority of the RHEL ecosystem
Simple to configure	Installer generated configuration
Effortless to manage	Managed by Kubernetes Operators

# IMMUTABLE OPERATING SYSTEM

## OPENSHIFT 4

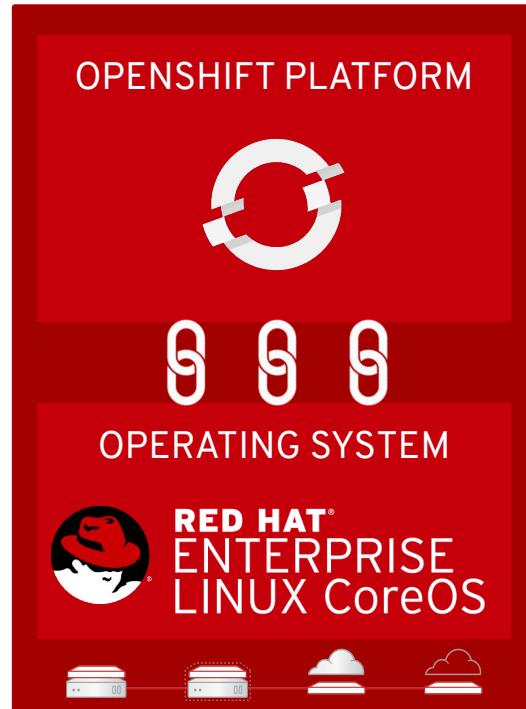
### Red Hat Enterprise Linux CoreOS is versioned with OpenShift

CoreOS is tested and shipped in conjunction with the platform. Red Hat runs thousands of tests against these configurations.

### Red Hat Enterprise Linux CoreOS is managed by the cluster

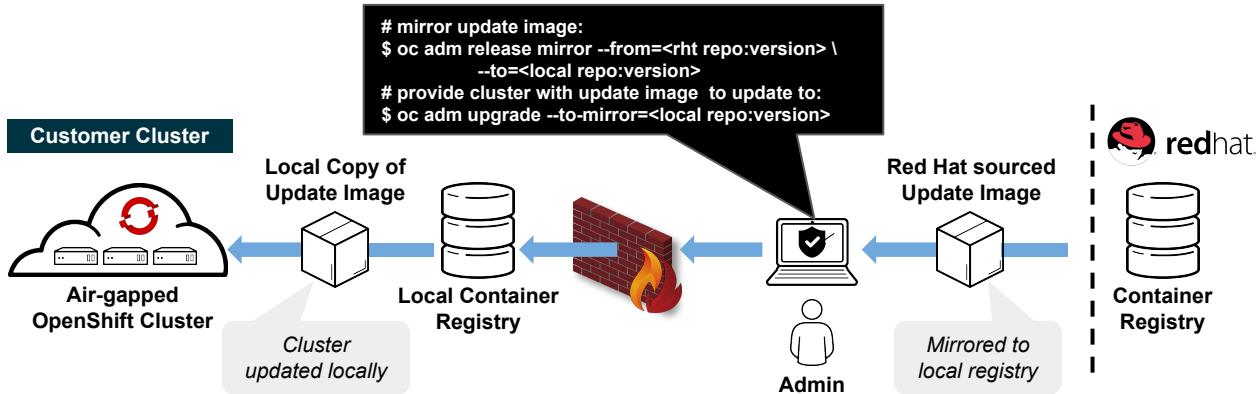
The Operating system is operated as part of the cluster, with the config for components managed by Machine Config Operator:

- CRI-O config
- Kubelet config
- Authorized registries
- SSH config



# Air-gapped Environments

## Disconnected Installation & Updating



- Support for installing and updating of OpenShift clusters in air-gapped environments is targeted for 4.2
- Admins first need to mirror installation and update payload images to a local container registry, then `openshift-install` and '`oc adm upgrade`' can be configured to leverage the offline content
  - RH CoreOS images for AWS will also need to be copied to a local S3 bucket and AMI ID defined in `install-config`



# cri-o

A lightweight, OCI-compliant container runtime

Optimized for  
Kubernetes

Any OCI-compliant  
container from any  
OCI registry  
(including docker)

Improve Security and  
Performance at scale

[CRI - the Container Runtime Interface](#)

[OpenShift 4 defaults to CRI-O](#)

[Red Hat contributes CRI-O to the Cloud Native Computing Foundation](#)

# RUNTIME SECURITY POLICIES

## SCC ([Security Context Constraints](#))

Allow administrators to control permissions for pods

Restricted SCC is granted to all users

By default, no containers can run as root

Admin can grant access to privileged SCC

Custom SCCs can be created

```
$ oc describe scc restricted
Name:                      restricted
Priority:                  <none>
Access:
  Users:                   <none>
  Groups:                  system:authenticated
Settings:
  Allow Privileged:        false 
  Default Add Capabilities: <none>
  Required Drop Capabilities: KILL,MKNOD,SYS_CHROOT,SETUID,SETGID
  Allowed Capabilities:    <none>
  Allowed Seccomp Profiles: <none>
  Allowed Volume Types:    configMap,downwardAPI,emptyDir,persistentVolumeClaim,projected,
                            ...
  Allow Host Network:       false
  Allow Host Ports:         false
  Allow Host PID:          false
  Allow Host IPC:          false
  Read Only Root Filesystem: false
  Run As User Strategy: MustRunAsRange
```

# IDENTITY AND ACCESS MANAGEMENT

OpenShift includes an OAuth server, which does three things:

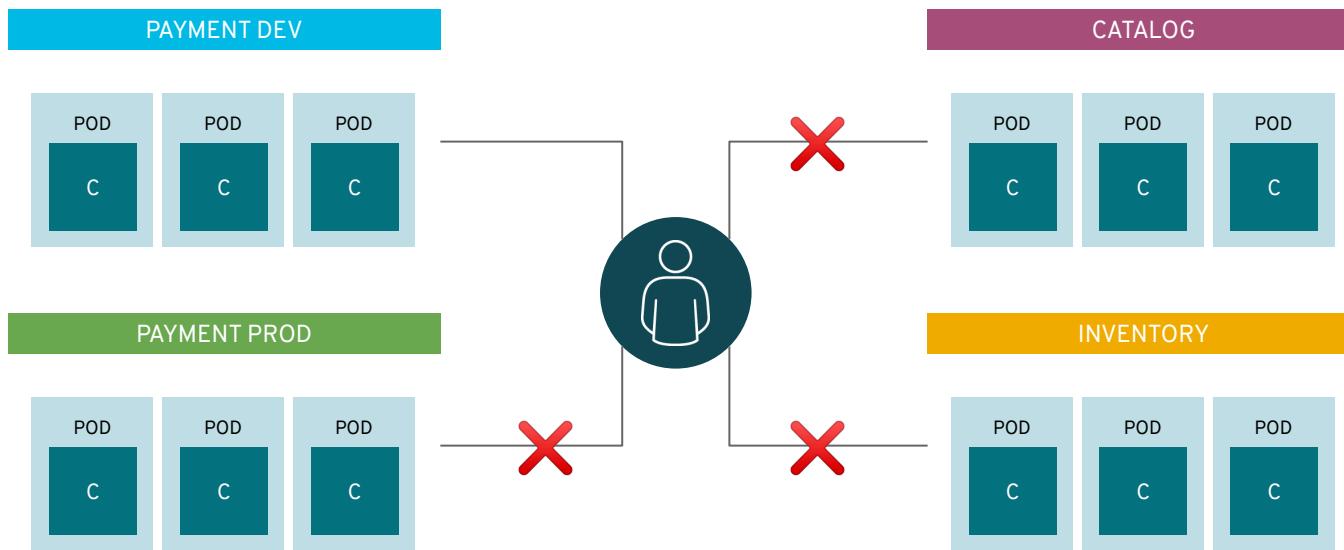
- Identifies the person requesting a token, using a configured identity provider
- Determines a mapping from that identity to an OpenShift user
- Issues an OAuth access token which authenticates that user to the API  
[Managing Users and Groups in OpenShift](#)  
[Configuring Identity Providers](#)

Supported Identity Providers include

- Keystone
- LDAP
- GitHub
- GitLab
- GitHub Enterprise (new with 3.11)
- Google
- OpenID Connect
- Security Support Provider Interface (SSPI) to support SSO flows on Windows (Kerberos)

# PROJECTS ISOLATE APPLICATIONS

## across teams, groups and departments



# RESTRICT ACCESS BY NEED TO KNOW

## Role based authorization

- Project scope & cluster scope available
- Matches request attributes (verb,object,etc)
- If no roles match, request is denied ( deny by default )
- Operator- and user-level roles are defined by default
- Custom roles are supported

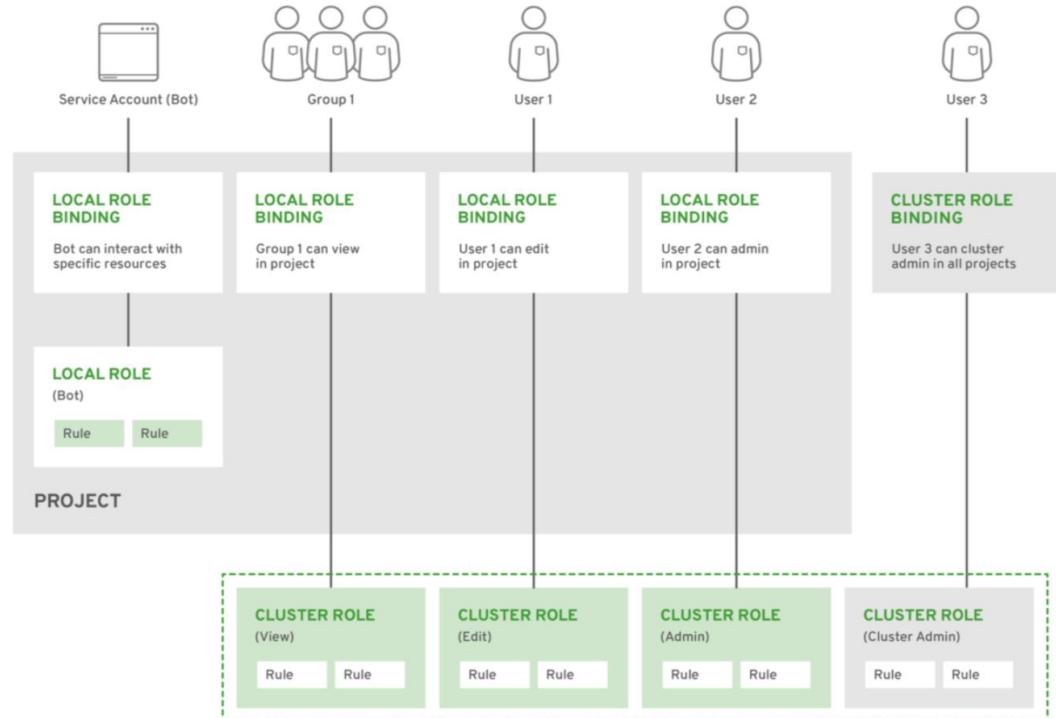
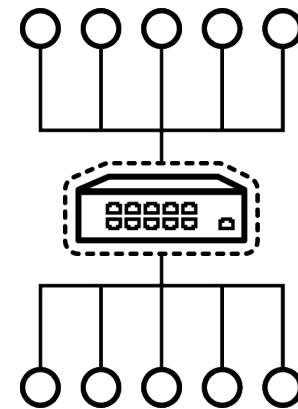


Figure 12 - Authorization Relationships

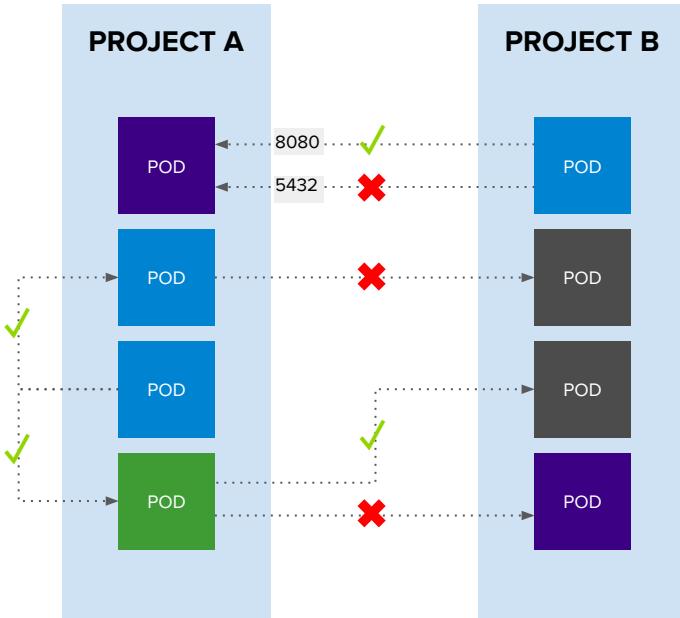
# OPENSIFT NETWORKING

- Built-in internal DNS to reach services by name
- Software Defined Networking (SDN) for a unified cluster network to enable pod-to-pod communication
- OpenShift follows the Kubernetes Container Networking Interface (CNI) plug-in model
- Isolate applications from other applications within a cluster
- Isolate environments (Dev / Test / Prod) from other environments within a cluster



# OPENShift SDN

## Network Policy enabled by default in OpenShift 4



### Example Policies

- Allow all traffic inside the project
- Allow traffic from green to gray
- Allow traffic to purple on 8080

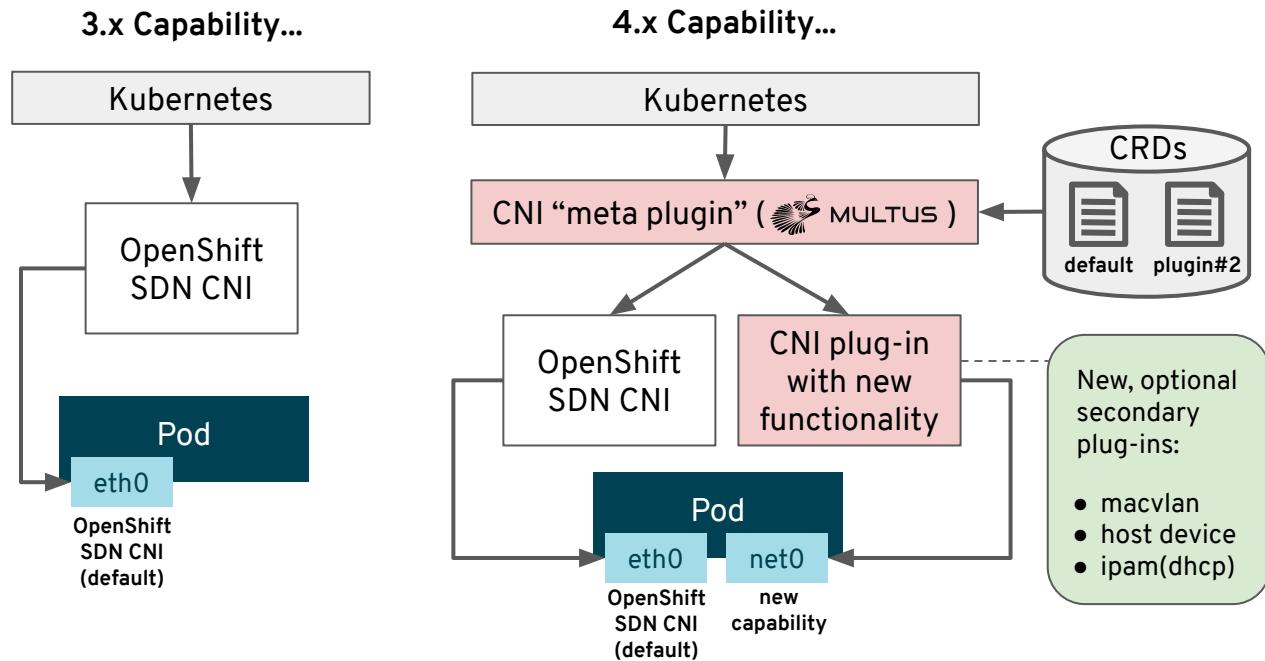
```
apiVersion: extensions/v1beta1
kind: NetworkPolicy
metadata:
  name: allow-to-purple-on-8080
spec:
  podSelector:
    matchLabels:
      color: purple
  ingress:
    - ports:
        - protocol: tcp
          port: 8080
```

# OPENShift MULTUS

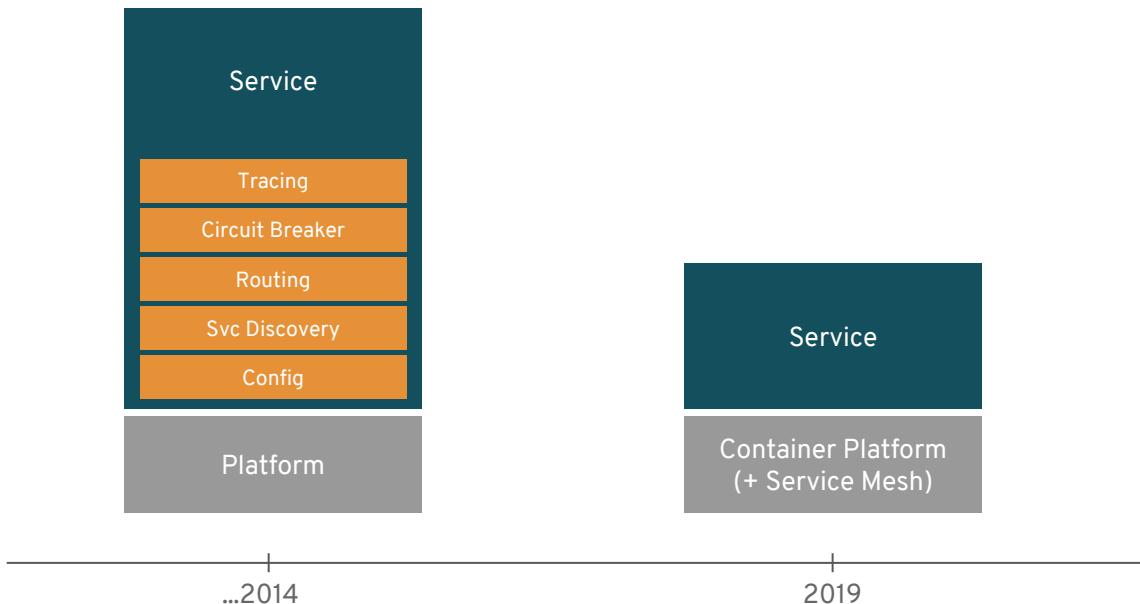
## Multus Enables Multiple Networks & New Functionality to Existing Networking

The Multus CNI “meta plugin” for Kubernetes enables one to create multiple network interfaces per pod, and assign a CNI plugin to each interface created.

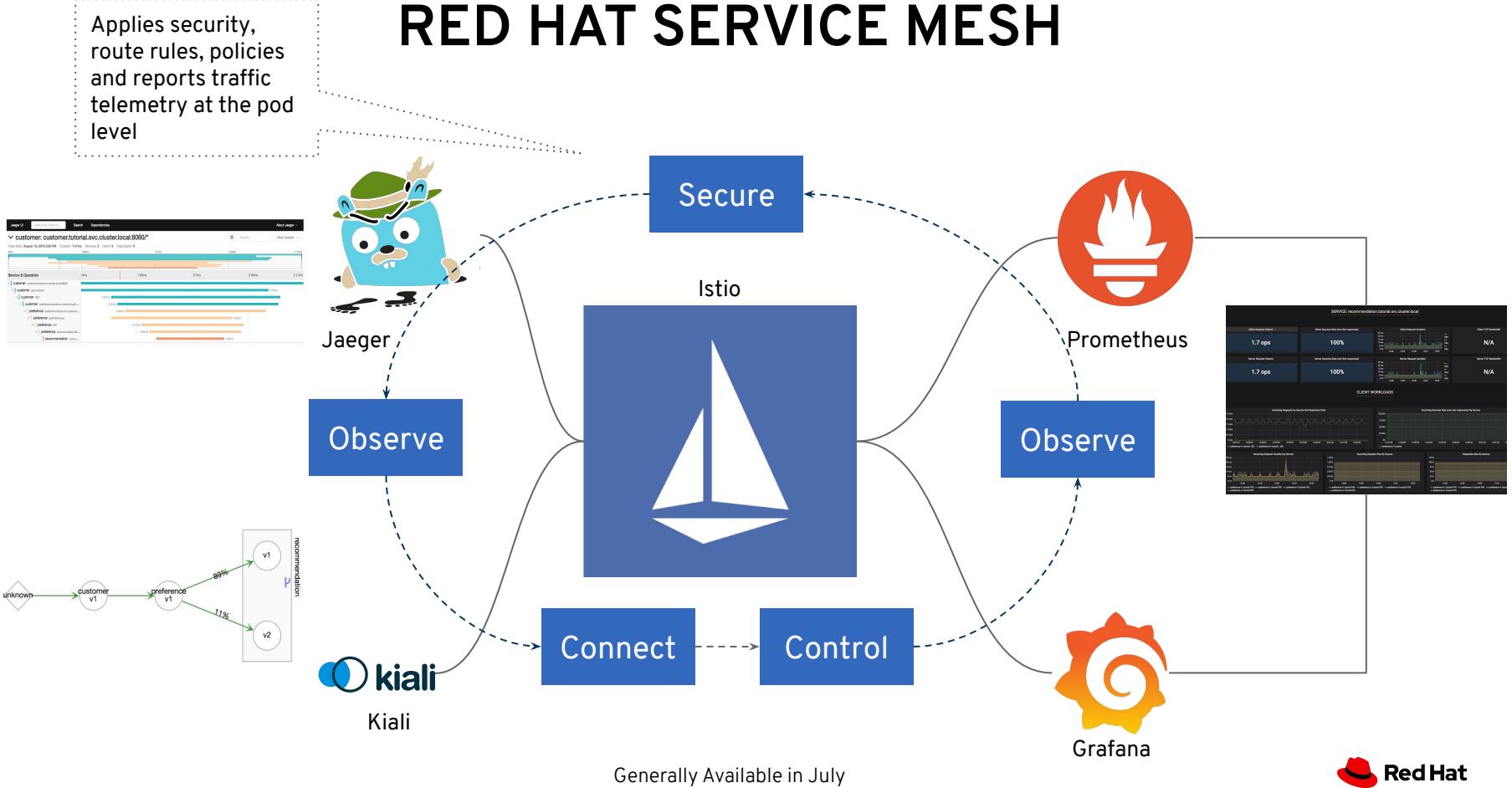
1. Create pod annotation(s) to call out a list of intended network attachments...
2. ...each pointing to CNI network configurations packed inside CRD objects



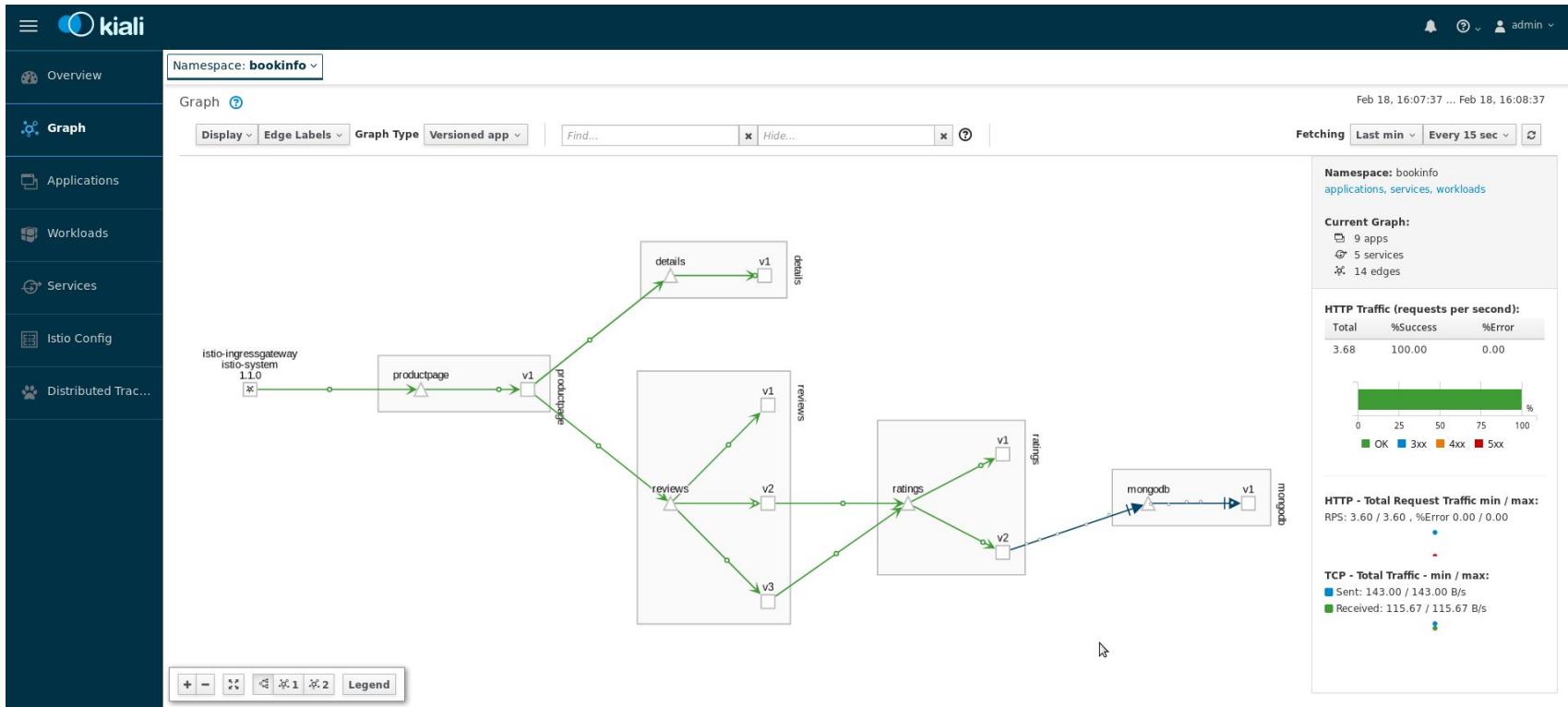
# MICROSERVICES EVOLUTION



# RED HAT SERVICE MESH

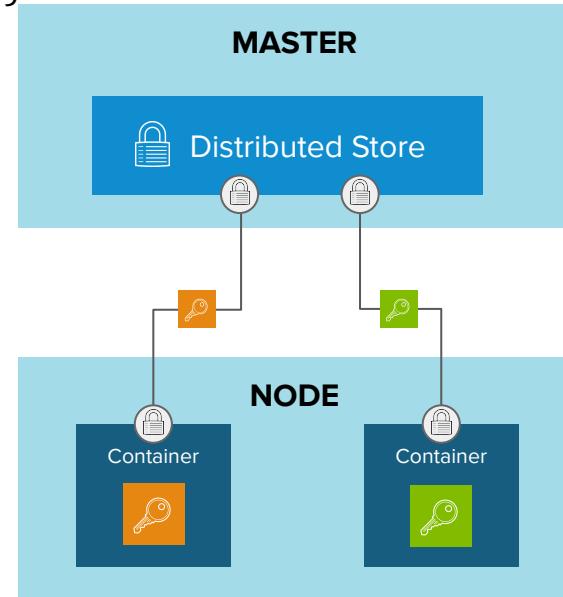


# OBSERVABILITY WITH KIALI



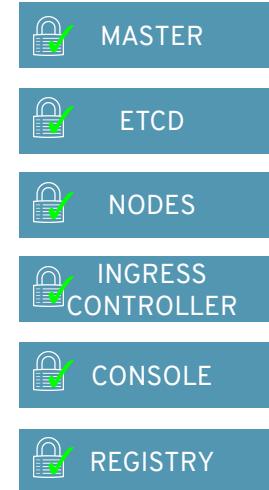
# SECRETS MANAGEMENT

- Secure mechanism for holding sensitive data e.g.
  - Passwords and credentials
  - SSH Keys
  - Certificates
- Secrets are made available as
  - Environment variables
  - Volume mounts
  - Interaction with external systems (e.g. vaults)
- Encrypted in transit and at rest\*
- Never rest on the nodes



# CERTIFICATE MANAGEMENT

- Certificates are used to provide secure connections to
  - master and nodes
  - Ingress controller and registry
  - etcd
- Certificate rotation is automated
- Optionally configure external endpoints to use custom certificates
- For example:  
[Requesting and Installing Let's Encrypt Certificates for OpenShift 4](#)



# CLUSTER LOG MANAGEMENT

## Install the Elasticsearch and Cluster Logging Operators from OperatorHub

- EFK stack aggregates logs for hosts and applications
  - Elasticsearch: a search and analytics engine to store logs
  - Fluentd: gathers logs and sends to Elasticsearch.
  - Kibana: A web UI for Elasticsearch.
- Access control
  - Cluster administrators can view all logs
  - Users can only view logs for their projects
  - Central Audit policy configuration
- Ability to send logs elsewhere
  - External elasticsearch, Splunk, etc

## Create Operator Subscription

Keep your service up to date by selecting a channel and approval strategy. The strategy determines either manual or automatic updates.

### Installation Mode \*

All namespaces  
This mode  
Operator will be available in a single namespace only.

A specific namespace on the cluster  
Operator will be available in a single namespace only.

PR openshift-logging

### Update Channel \*

preview

### Approval Strategy \*

Automatic

Manual

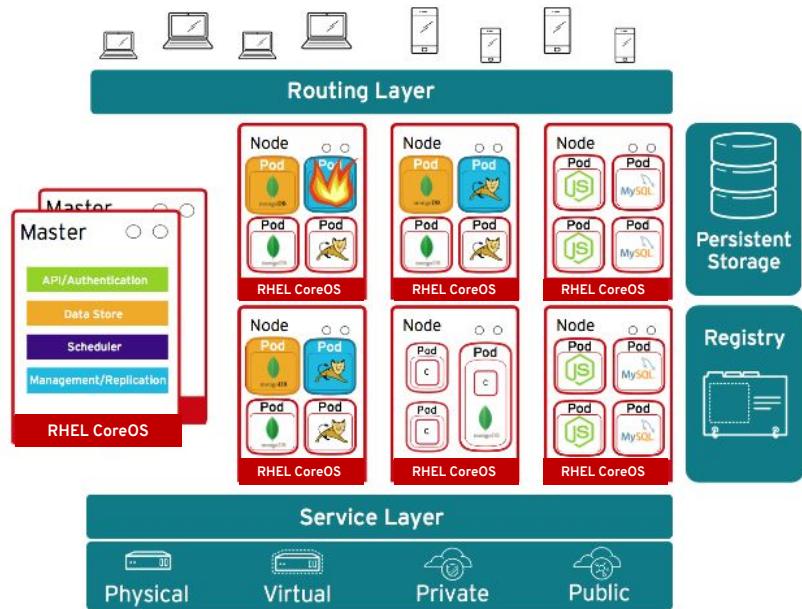
Subscribe Cancel

```
# configure via CRD
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance"
  namespace: "openshift-logging"
spec:
  managementState: "Managed"
  logStore:
    type: "elasticsearch"
    elasticsearch:
      nodeCount: 3
      resources:
        limits:
          cpu: 800m
          memory: 1Gi
        requests:
          cpu: 800m
          memory: 1Gi
      storage:
        storageClassName: gp2
        size: 100G
        redundancyPolicy: "SingleRedundant"
    visualization:
      type: "kibana"
      kibana:
        replicas: 1
    curation:
      type: "curator"
```

# ATTACHED STORAGE

Secure storage by using

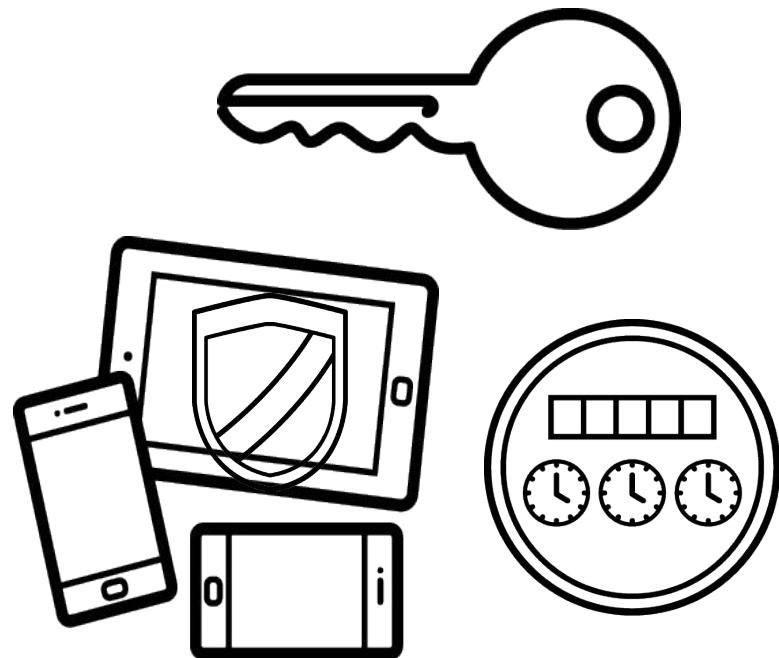
- SELinux access controls
- Secure mounts
- Supplemental group IDs for shared storage



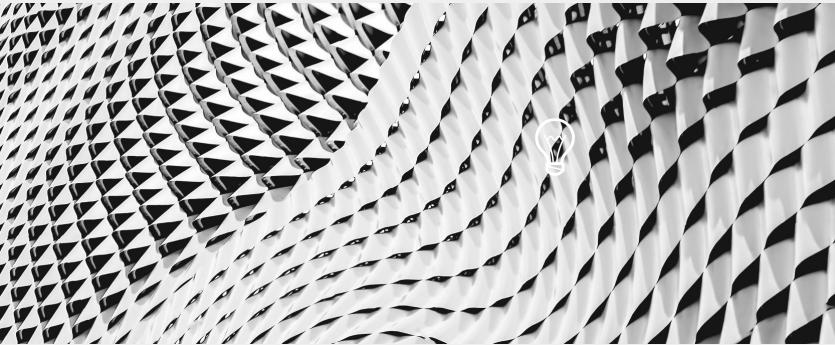
# APPLICATION API MANAGEMENT

Container platform & application APIs

- Authentication and authorization
- LDAP integration
- End-point access controls
- Rate limiting



# EXTEND SECURITY



# RED HAT CERTIFIED OPERATORS

DEVOPS



APM



DATA SERVICES



DATABASE



SECURITY



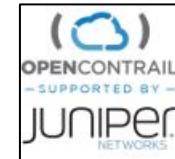
STORAGE



# THE BROAD SECURITY ECOSYSTEM



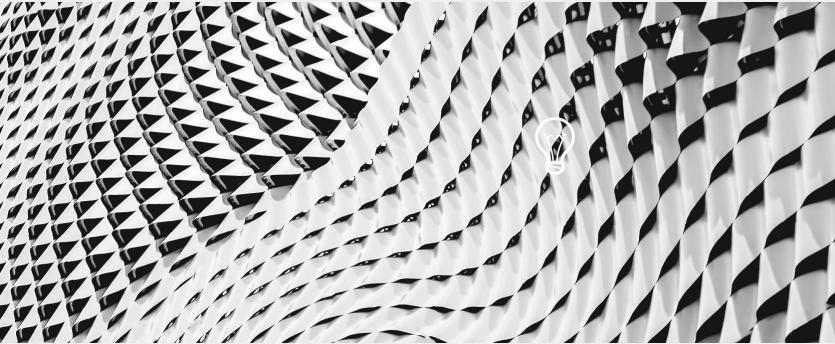
BLACKDUCK  
BY SYNOPSYS®



THALES



# ROADMAP



# SECURITY FEATURE ROADMAP

DEFENSE IN DEPTH - Control, Defend, Extend

## Linux Host Security

- RHCOS FIPS mode
- RHCOS Auditd

## Authentication & Authorization

- Integration with external Keycloak
- Use group membership from external IPs

## Secrets & Certificates

- Improved cert management and Integration with external CAs via ACME
- Integration with external Key Management Systems

## Integrated Audit & Logging

- East / West traffic tracing with OpenShift Service Mesh (GA summer 2019)

## Network Policies

- Control service access flow with OpenShift Service Mesh (GA summer 2019)

## Networking Isolation

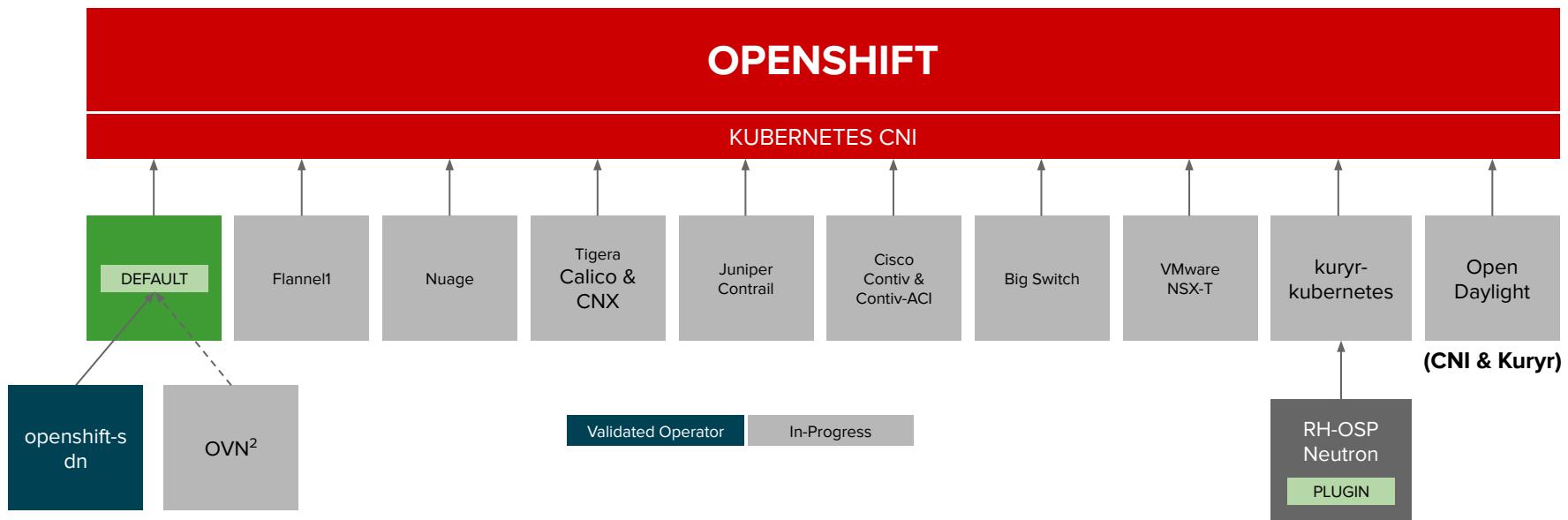
- East / West mutual TLS authentication with OpenShift Service Mesh (GA summer 2019)

## Image Security

- Clair v3 covers more content

Trusted Container Content	CI/CD Pipeline
Quay Registry with Image Scanning	ImageStreams
Built-In IAM	Deployment Policies (SCCs)
Secrets Management	Network Policy & Isolation
Audit & Logging	API Management
Container Host Multi-tenancy / Container Optimized Immutable OS	
Security Ecosystem	

# OPENShift NETWORK PLUGINS

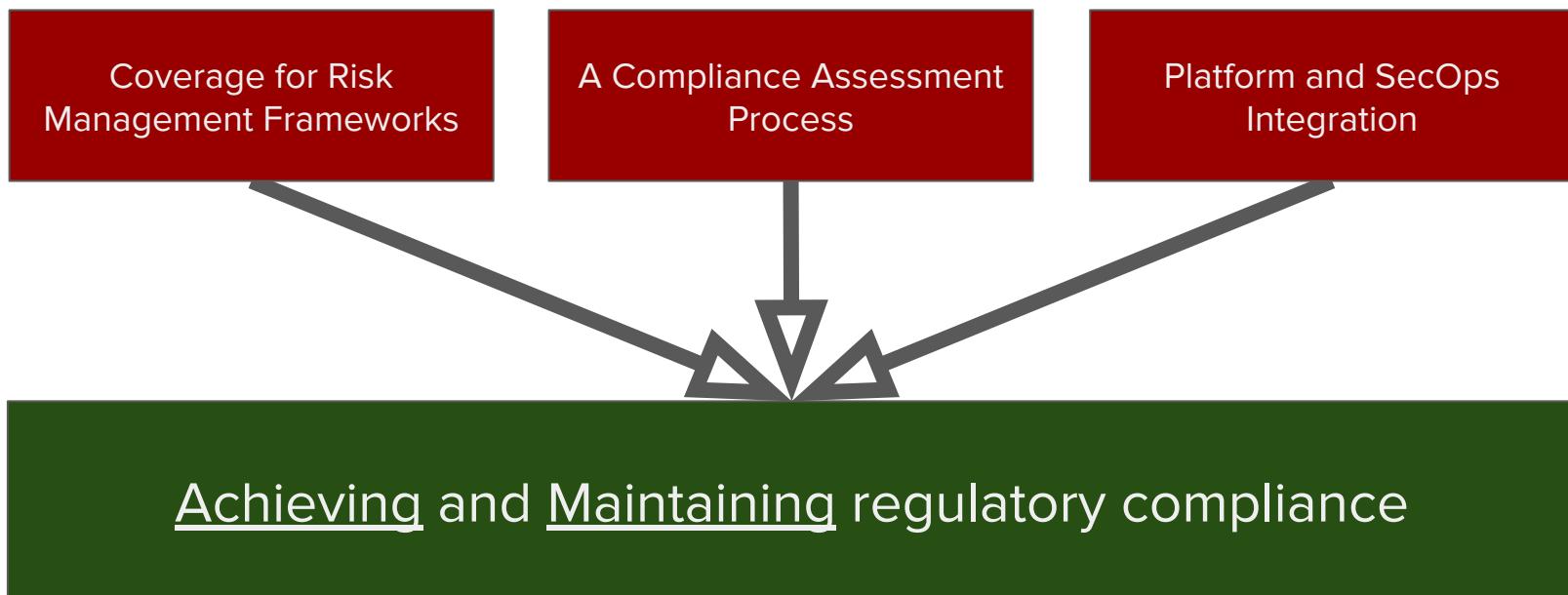


<sup>1</sup> Flannel is minimally verified and is supported only and exactly as deployed in the OpenShift on OpenStack reference architecture

<sup>2</sup> Targeting OCP 4.2 GA

# RISK MANAGEMENT AND COMPLIANCE GOALS

*Automate compliance audit and remediation*



# VIRT-BASED CONTAINERS

What is the future for KVM isolated containers?

- Lots of interest from customers in this area
- All of these solutions have limitations, compatibility issues, and are not mature enough to support
- Customers seem to get less excited as they learn about the gaps
- Not mature enough to be on our product roadmaps
- Kata seems to be the most promising solution and community
  - We are engaged upstream and currently bringing kata into Fedora



gVisor

# Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.



[linkedin.com/company/red-hat](https://www.linkedin.com/company/red-hat)



[youtube.com/user/RedHatVideos](https://www.youtube.com/user/RedHatVideos)



[facebook.com/redhatinc](https://www.facebook.com/redhatinc)

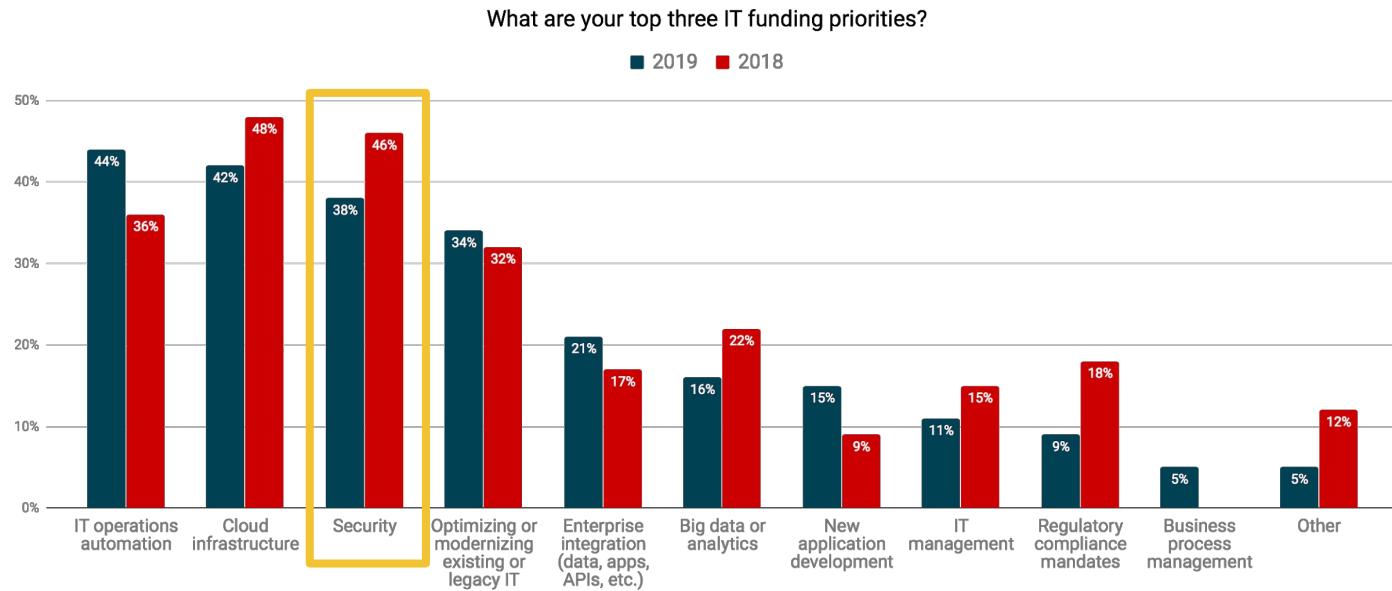


[twitter.com/RedHat](https://twitter.com/RedHat)

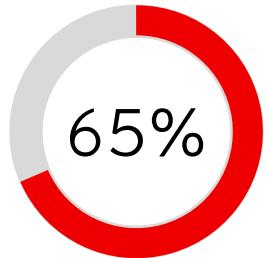
---

# Appendix: Security challenges and priorities

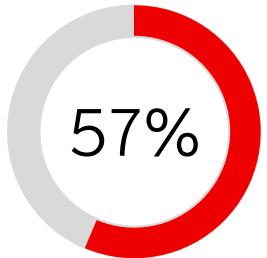
## Top Funding Priorities for 2019: Automation, Cloud, & Security



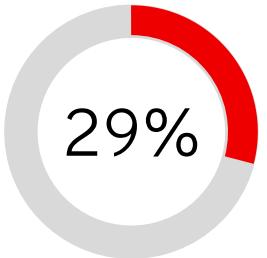
## The Cyber Security Challenge is not Getting Easier



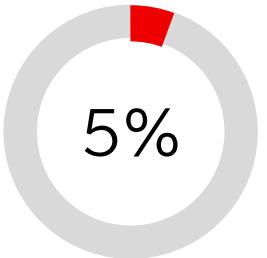
Reported increased Severity of attacks



Said the time to resolve an incident has grown



Have their ideal security-skilled staffing level, making it the #2 barrier to Cyber resilience

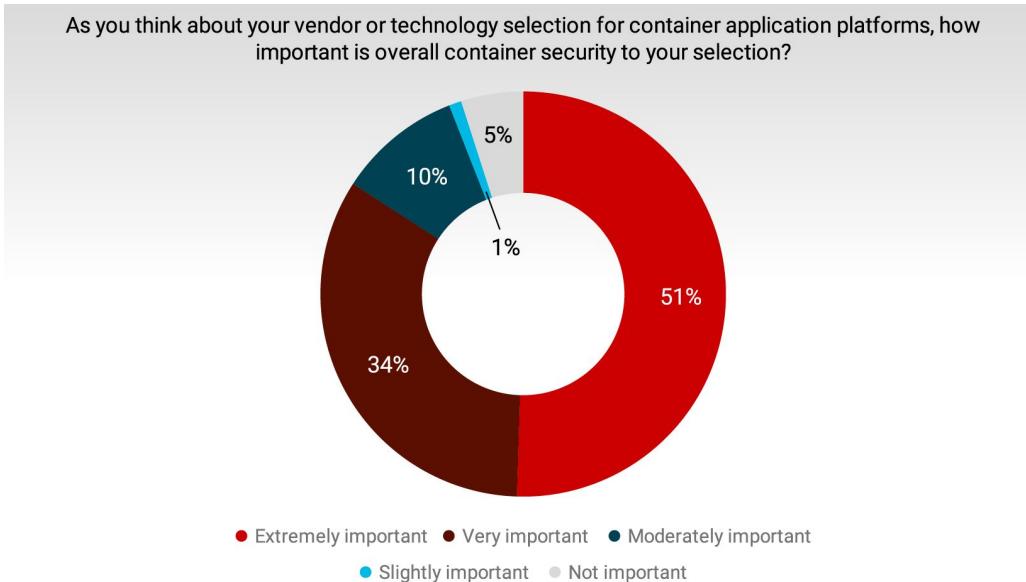


Portio of alerts coming in that the average security team examines every day

<sup>1</sup> [The Third Annual Study on the Cyber Resilient Organization](#) - Ponemon Institute, 2018 (Sponsored by IBM)

<sup>2</sup> <https://venturebeat.com/2017/12/16/the-lesson-behind-2017s-biggest-enterprise-security-story/>

## Choosing a Container Platform Vendor? Security is Critical



---

# Appendix: Storage

**Just like  
money,  
containers  
need safe and  
reliable storage  
and  
transmission**



---

# Appendix: Red Hat Quay

# RED HAT QUAY V3

## Quay v3 Key Features

- Full support for Docker Registry API v2\_s2
- Multi-arch (manifest) and Windows images
- Rebranded and rebased (RHEL)
- New config UI to save & upload Quay config
- Parallel upgrade (2x 5min downtime only)

## Red Hat Quay and OpenShift

Red Hat Quay and OpenShift work well together. This includes both running Quay **on** and using Quay **with** OpenShift.



[Introducing Red Hat Quay 3](#)

# REGISTRY FEATURES



- **Vulnerability Scanning (powered by Clair)**  
Continually scan your containers for vulnerabilities, giving you complete visibility into known issues and how to fix them
- **Geographic Replication**  
Reliably store, build and deploy a single set of container images across multiple geographies
- **Automated software deployments**  
Streamline your continuous integration/continuous delivery (CI/CD) pipeline with build triggers, git hooks, and robot accounts
- **Advanced Access Control Management**  
Fine-grain access control of the registry with multiple identity and authentication providers as well as support for teams and organization mapping

# VULNERABILITY SCANNING - CLAIR

Quay integrates with Clair to continually scan your containers for vulnerabilities.

You get complete visibility into known issues and how to fix them.

RED HAT QUAY EXPLORE REPOSITORIES TUTORIAL

search + 🔍 opentic...

← example/python 3f86e14b88f9

Quay Security Scanner has detected **718** vulnerabilities.  
Patches are available for **144** vulnerabilities.

47 High-level vulnerabilities.  
220 Medium-level vulnerabilities.  
177 Low-level vulnerabilities.  
266 Negligible-level vulnerabilities.  
8 Unknown-level vulnerabilities.

Vulnerabilities

Showing 144 of 718 Vulnerabilities   Only show fixable

CVE	SEVERITY ↓	PACKAGE	CURRENT VERSION	FIXED IN VERSION	INTRODUCED IN LAYER
» CVE-2018-15686	10 / 10	systemd	232-25+deb9u6	232-25+deb9u10	<input type="button" value="ADD"/> file:a61c14b18252183a4719980da97ac483044bc...
» CVE-2019-3855	9.3 / 10	libssh2	1.7.0-1	1.7.0-1+deb9u1	<input type="button" value="RUN"/> apt-get update && apt-get install -y --no-i...
» CVE-2019-3462	9.3 / 10	apt	1.4.8	1.4.9	<input type="button" value="ADD"/> file:a61c14b18252183a4719980da97ac483044bc...
» CVE-2017-16997	9.3 / 10	glibc	2.24-11+deb9u3	2.24-11+deb9u4	<input type="button" value="ADD"/> file:a61c14b18252183a4719980da97ac483044bc...
» CAE-S011-19881	8.3 / 10	dpkg	2.19.1-1+deb9u3	2.19.1-1+deb9u4	<input type="button" value="ADD"/> file:a61c14b18252183a4719980da97ac483044bc...
» CAE-S010-2465	8.3 / 10	ebf	1.4.8	1.4.9	<input type="button" value="ADD"/> file:a61c14b18252183a4719980da97ac483044bc...

---

# Appendix: Next generation container tools

# NEXT-GEN CONTAINER TOOLS

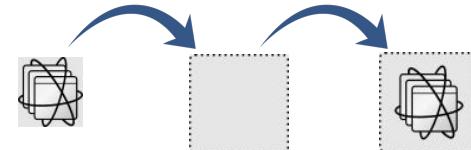
Providing stability, flexibility and performance with containers and images

**Container-tools** - OCI tooling to create, run, and manage, Linux Containers with an enterprise life cycle.

- Conform to the OCI image and runtime specifications
- Daemon-less, OS-native container tooling
- Separation of concerns



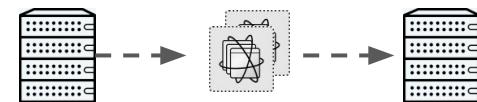
**buildah**



Build OCI/docker Images



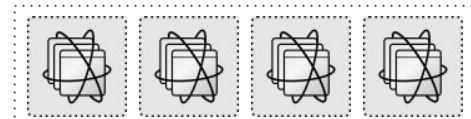
**skopeo**



Inspect, copy, & sign Images



**podman**



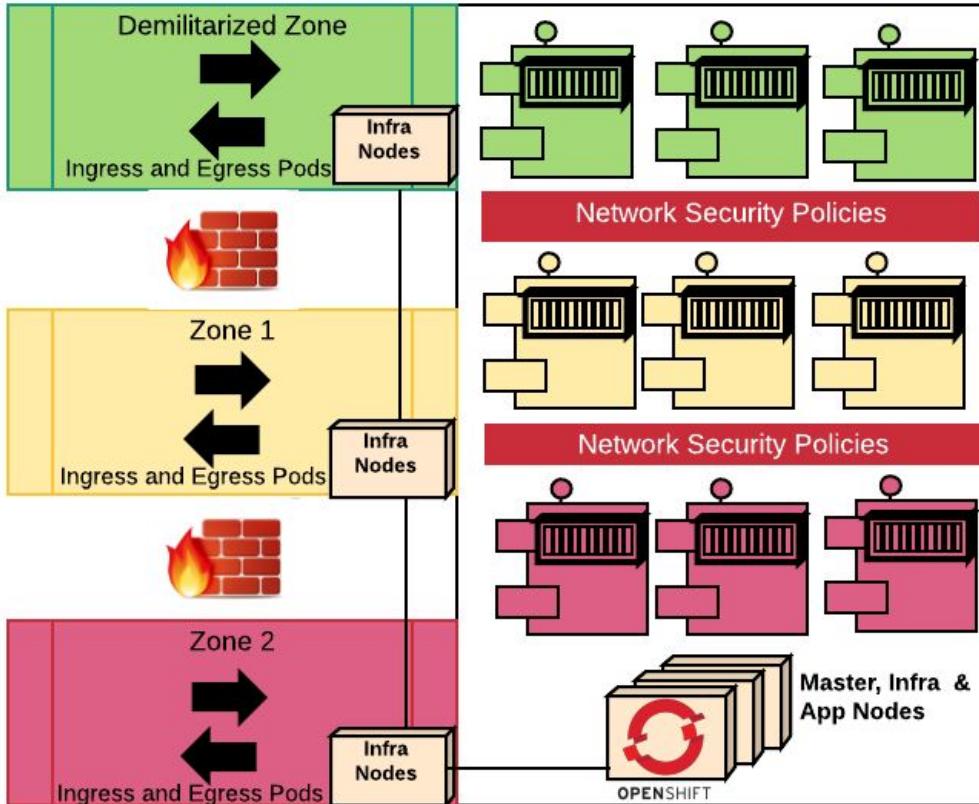
RHEL

run, manage, debug containers

---

# Appendix: Network security

# OPENSHIFT CLUSTER COVERING MULTIPLE ZONES



Application pods run on one OpenShift Cluster.

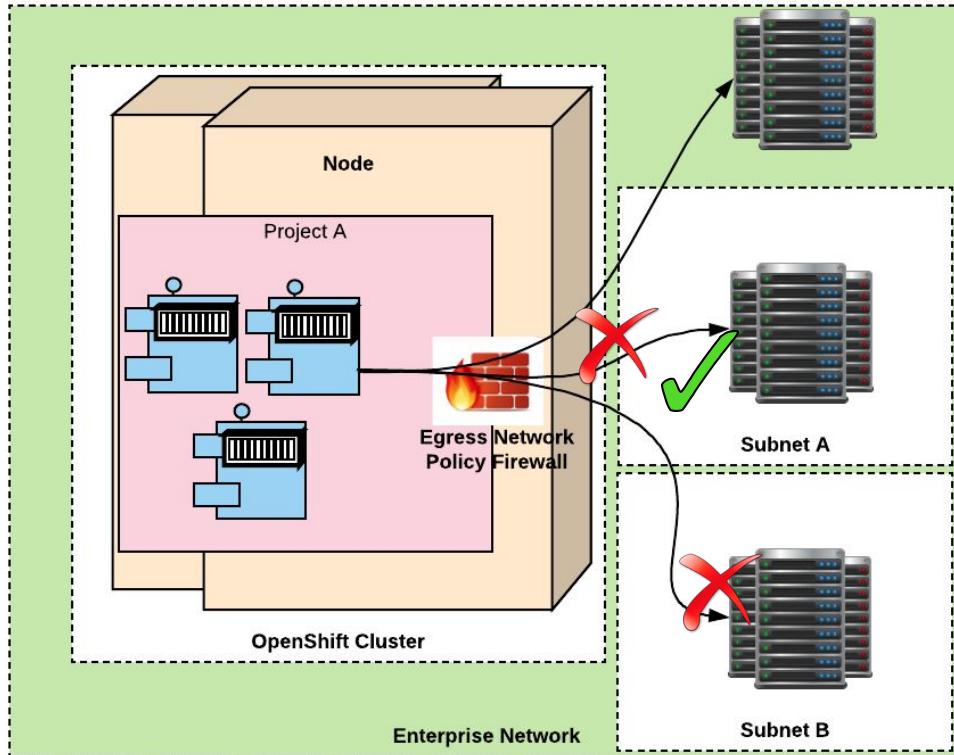
Microsegmented with Network Security policies.

Infra Nodes in each zone run Ingress and Egress pods for specific zones.

If required, physical isolation of pods to specific nodes is possible with node-selectors. But that can reduce worker node density.

# EGRESS FIREWALL TO LIMIT ACCESS

Cluster admin can limit the external addresses accessed by some or all pods



Examples:

A pod can talk to hosts (outside OpenShift cluster) but cannot connect to public internet

A pod can talk to public internet, but cannot connect to hosts (outside OpenShift cluster)



A pod cannot reach specific subnets/hosts

# BUILDING UPON MULTUS

Development is now unblocked for a number of customer use cases

- Functional separation of control/data planes
  - Default SDN on primary interface for management traffic
  - Data-plane traffic on secondary (or tertiary...) interface
- Link aggregation for network redundancy
- Different network protocol stacks, capabilities, SLAs
- Network traffic isolation, segregation and security
- User-space networking (e.g. VPP, OVS-DPDK)
- VLAN, MACVLAN, host device networking
- Video Streaming (Multicast)
- High Performance Networking - e.g. SR-IOV
  - Openshift-SDN/OVN-Kubernetes as primary interface for management traffic
  - SR-IOV Device Plugin for VF hardware resource scheduling
  - SR-IOV CNI plugs VFs assigned by device plugin into pods as data plane interfaces
- QoS
- CNV (kubenvirt) Networking
- SDN Migration (e.g. our next-gen SDN)

---

# Appendix: Pod Security Policies

# SECURITY CONTEXT CONSTRAINTS & POD SECURITY POLICIES

Security Context Constraints (SCCs) allow administrators to control permissions for pods.

SCCs define a set of conditions that a pod must run with in order to be accepted into the system. Red Hat has contributed this feature to Kubernetes as Pod Security Policies (PSPs).

PSPs are not yet as mature as SCCs. We will enable customers to migrate from SCCs to PSPs as soon as we have feature parity. We are also working to ensure that SCCs support new settings available with PSPs. Additional information on these new settings is available in Kubernetes documentation.

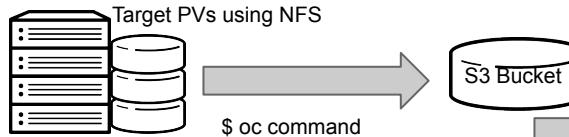
\$ oc describe scc restricted	
Name:	restricted
Priority:	<none>
Access:	
Users:	<none>
Groups:	system:authenticated
Settings:	
Allow Privileged:	false
Default Add Capabilities:	<none>
Required Drop Capabilities:	KILL,MKNOD,SYS_CHROOT,
Allowed Capabilities:	<none>
Allowed Seccomp Profiles:	<none>
Allowed Volume Types:	configMap,downwardAPI,
Allow Host Network:	false
Allow Host Ports:	false
Allow Host PID:	false
Allow Host IPC:	false

---

# Appendix: Cluster migration

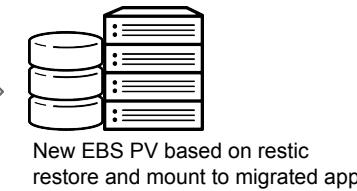
# CLUSTER MIGRATION OPENSHIFT 3 to 4

vSphere OpenShift 3.10 Cluster



Full Backup  
Increment Diff Backup  
(like rsync)

AWS OpenShift 4.1 Cluster



- Deploy a replication of your applications from one OpenShift cluster to a different OpenShift cluster
- Enable cluster specific configuration from OpenShift 3 to work on a OpenShift 4 cluster
- Documentation on how to handle common network, storage, and machine/node re-use scenarios between OpenShift 3 and OpenShift 4 clusters