

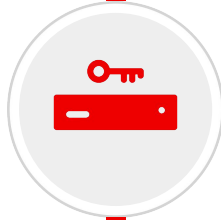


# RED HAT QUAY

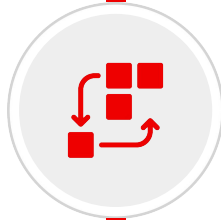
Secure Enterprise Registry



Industry-leading, **trusted, and open source registry platform** operating at scale since 2014



Built to **efficiently manage content** under governance and security **controls** globally



Runs **everywhere**, easy to **integrate** and **automate** but works best with **OpenShift**



Developed in **collaboration** with a broad open source, customer, and ecosystem **community**

# Red Hat Quay Key Features

Massive Scale Testing Quay.io  
Real Time Garbage Collection  
Automated Squashing

## SCALABILITY

Seamless Git Integration  
Build Workers  
Webhooks

## BUILD AUTOMATION

Extensible API  
Webhooks, OAuth  
Robot Accounts

## INTEGRATION

## REGISTRY

High Availability  
Full Standards / Spec Support  
Long-Term Protocol Support  
Application Registry  
Enterprise Grade Support  
Regular Updates

## SECURITY

Vulnerability Scanning  
Logging & Auditing  
Notifications & Alerting

## CONTENT DISTRIBUTION

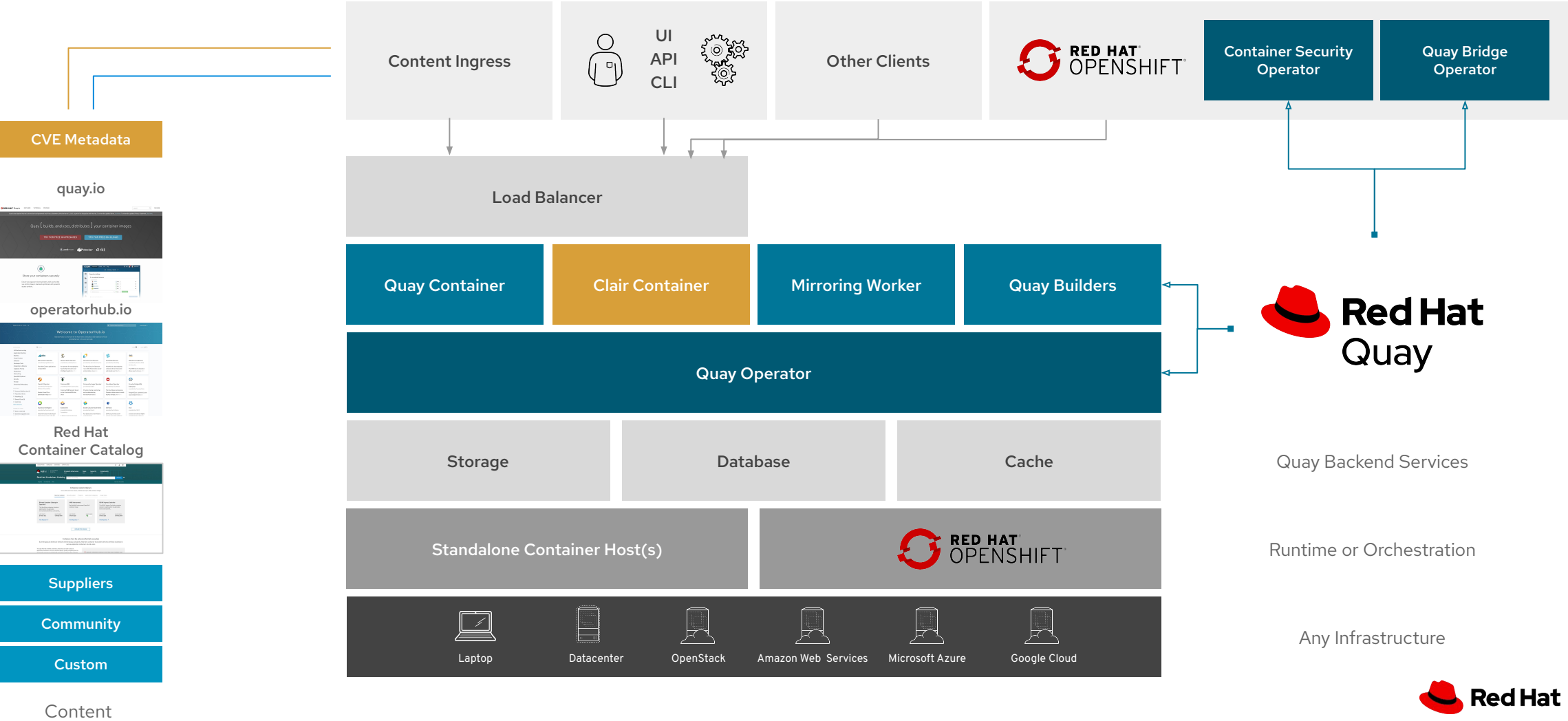
Geo-Replication  
Repository Mirroring  
Air-Gapped Environments

## ACCESS CONTROL

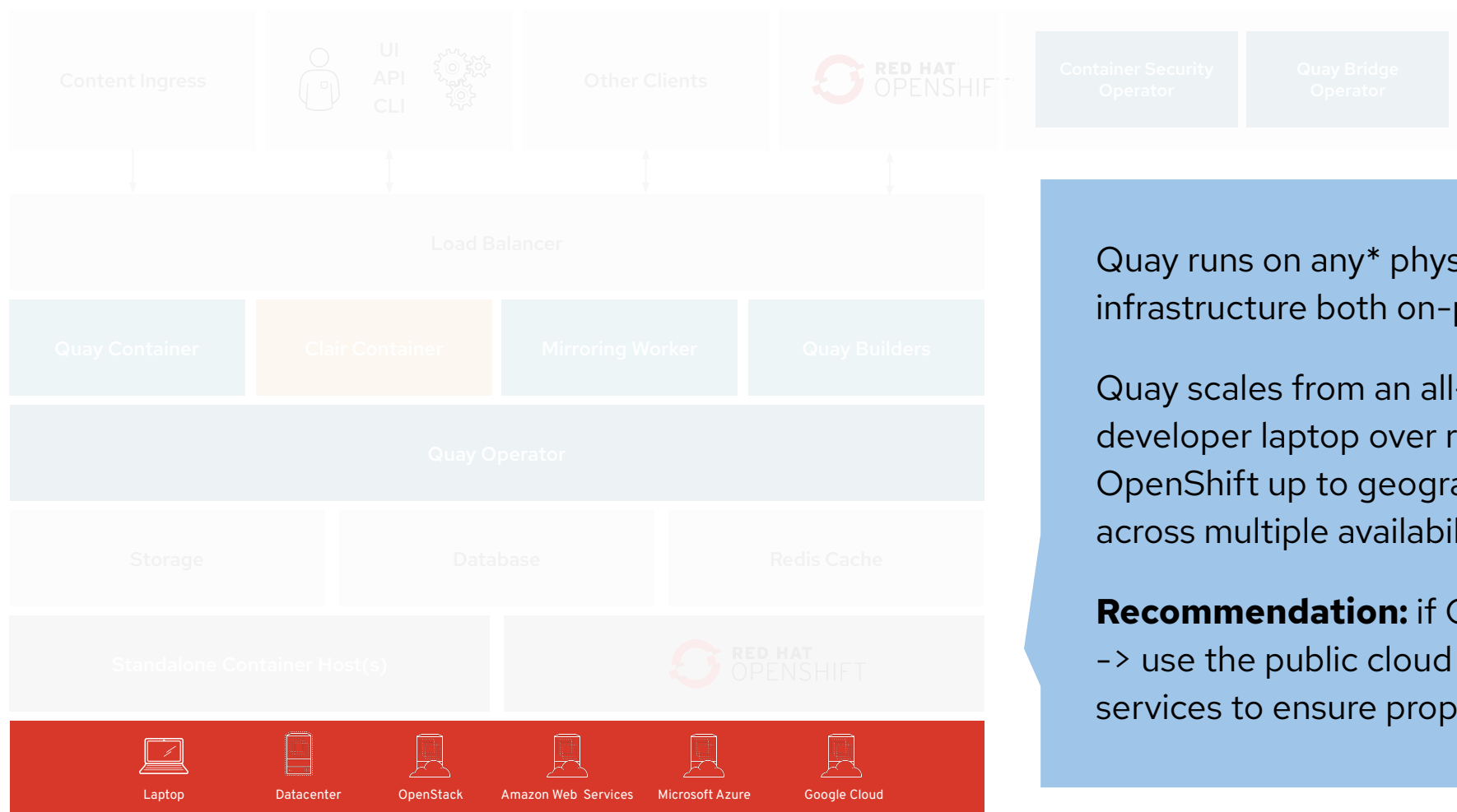
Authentication Providers  
Fine-Grained RBAC  
Organizations & Teams

# Quay Architecture

# Red Hat Quay Architecture



# Prerequisite: Infrastructure



Quay runs on any\* physical or virtual infrastructure both on-premise or public cloud\*\*

Quay scales from an all-in-one setup on a developer laptop over running highly available on OpenShift up to geographically dispersed setup across multiple availability zones and regions

**Recommendation:** if Quay runs on public cloud -> use the public cloud services for Quay backend services to ensure proper HA and scalability

\* Further details can be found in the Quay 3.x tested configuration matrix: <https://access.redhat.com/articles/4067991>

\*\* Further details can be found in the Quay Support Policy: <https://access.redhat.com/support/policy/updates/rhquay/policies>

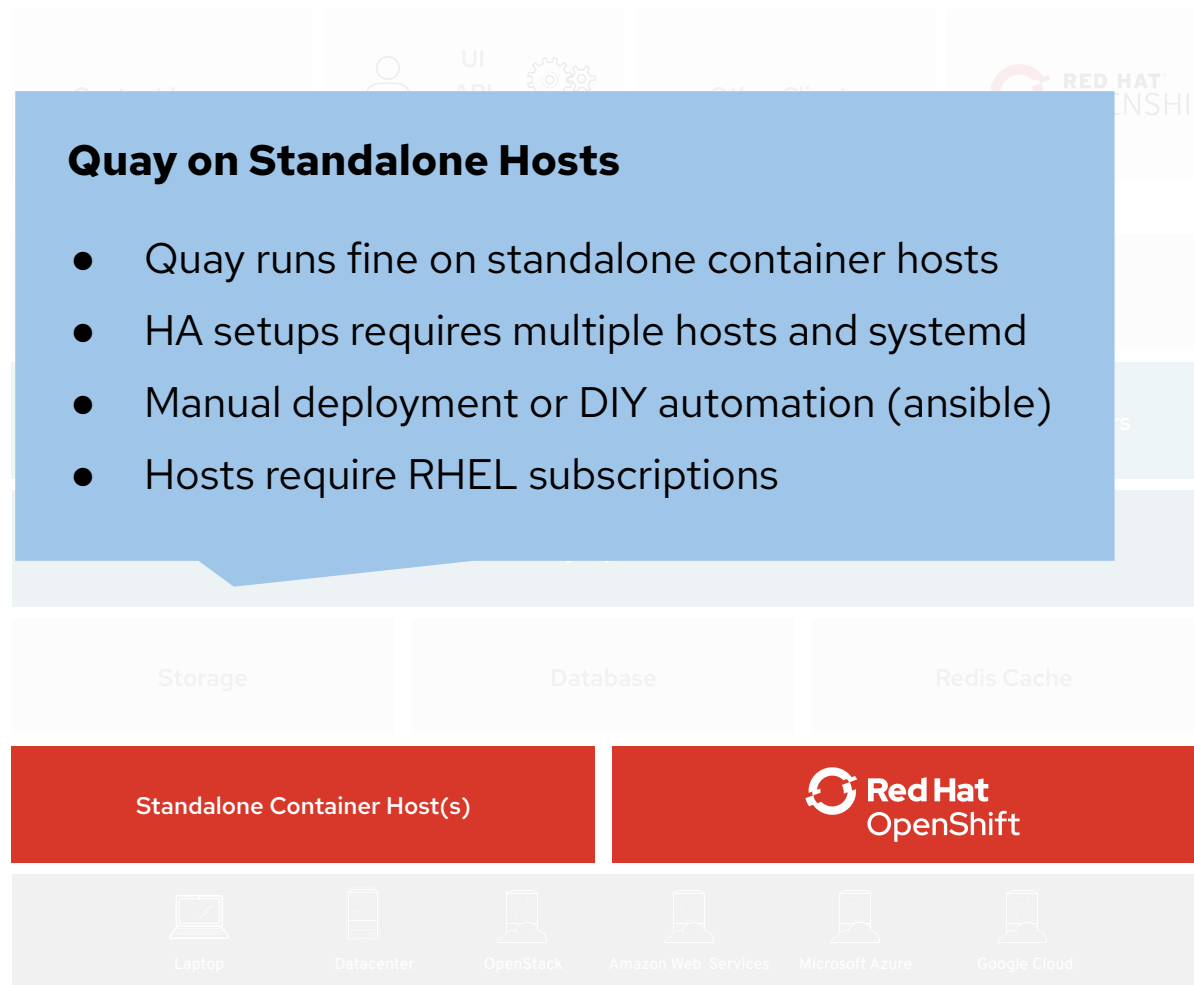
# Prerequisite: Container Runtime or Orchestration

## Quay on Standalone Hosts

- Quay runs fine on standalone container hosts
- HA setups requires multiple hosts and systemd
- Manual deployment or DIY automation (ansible)
- Hosts require RHEL subscriptions

## Benefits of running Quay on OpenShift:

- Run Quay where you run all other container workloads and services
- Seamless deployment and day2 management of Red Hat Quay via the Quay operator and OLM
- Leverage all orchestration and management capabilities of Red Hat OpenShift incl. Operator Lifecycle Mgt (OLM), monitoring, dashboards, ...
- Quay can run on OpenShift infra nodes (no further subscriptions required)



# Quay and OpenShift



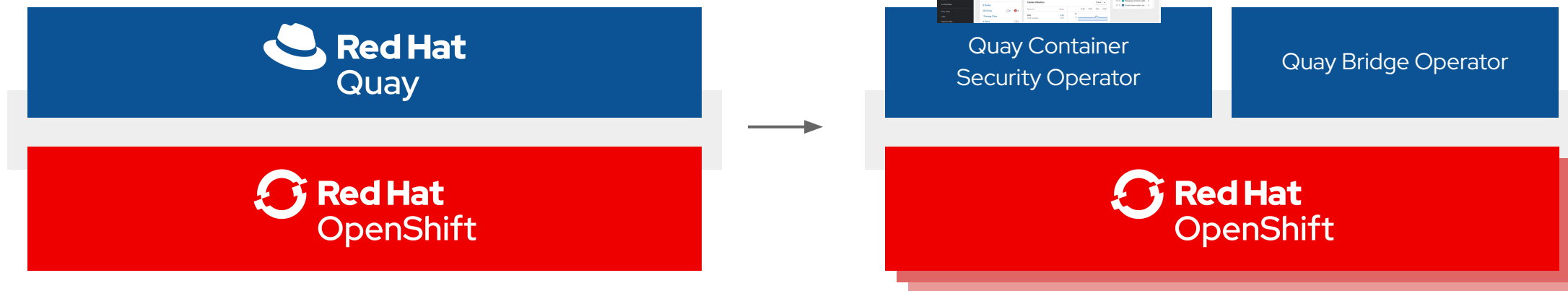
# Red Hat Quay works best with OpenShift

Red Hat Quay runs on any infrastructure  
but **runs best on OpenShift**

The **Quay Operator** ensures seamless deployment  
and management of Quay running on OpenShift

**CSO** brings Quay / Clair  
vulnerability data into the  
OpenShift Console

The **Quay Bridge  
Operator** ensures  
seamless integration and  
user experience for using  
Quay **with** OpenShift



Quay serves content to **one or many OpenShift clusters**, wherever they're running.

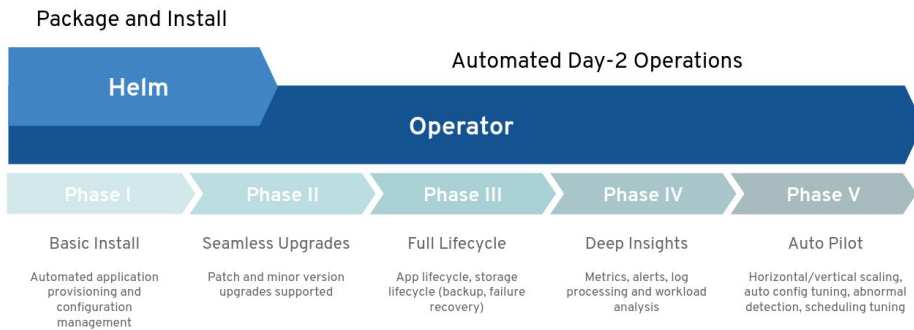
With or without using the OpenShift internal registry but leveraging all OpenShift capabilities.

# Benefits of running Quay on OpenShift



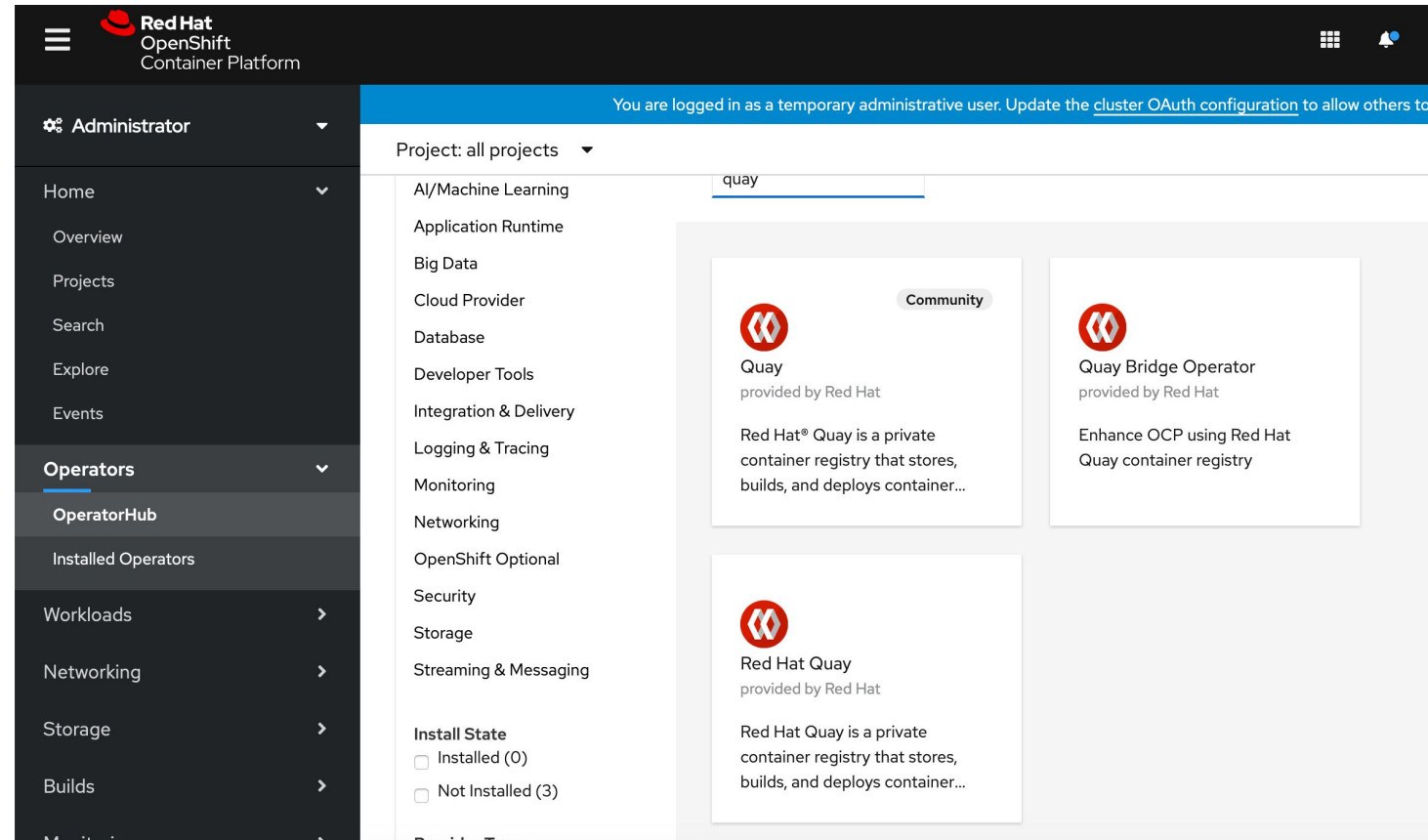
- **Zero to Hero** - Simplified deployment of Quay and associated components means that you can start using the product immediately
- **Scalability** - Leverage cluster compute capacity to manage expected demand
- **Simplified Networking** - Diverse ingress options using well established patterns for any application deployed on the platform
- **Centralized configuration management** - Configurations stored in etcd provide a centralized source of truth
- **Repeatability** - Consistency regardless of the number of replicas of Quay / Clair
- **Expanded Options** - Additional solutions that are specifically designed to take advantage of an OpenShift deployment

# Quay - Focus on Operators



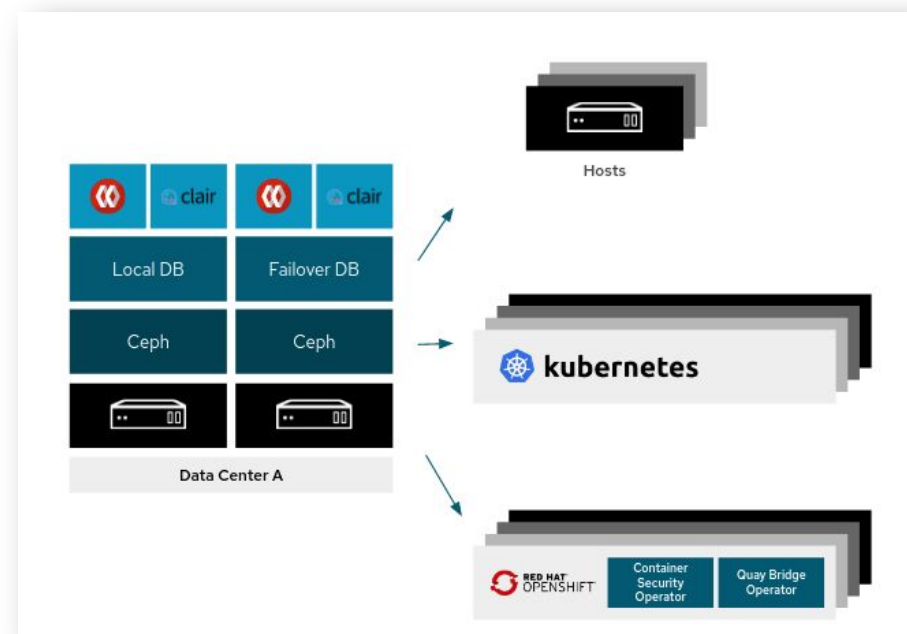
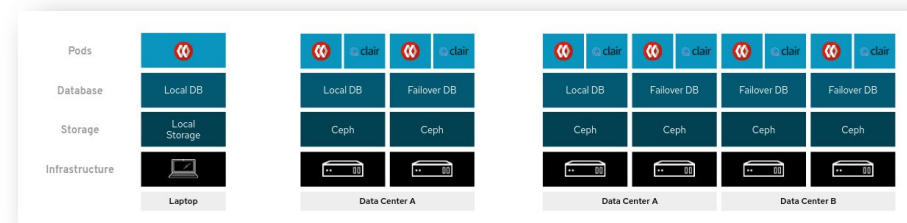
Focus and direction for the Quay product are kubernetes operators and running Quay on OpenShift / kubernetes given the advantages of operators compared with its alternatives

Maintaining another deployment and management tooling for non-k8s deployments is not feasible and not aligned to our prioritization and roadmap (Quay v4 will run on k8s by default)



# Quay Deployment Examples

- Quay can run on standalone container hosts or OpenShift (recommended)
- A Quay deployment can be distributed across multiple DCs or even OCP clusters (geo-repl)
- Typically Quay is used for **more than one / many OpenShift clusters**
- Components which can run **on-cluster**: Quay, Clair, mirroring workers
- Components which should / must run **off cluster** (today): Quay builders, databases (if not an operator), storage

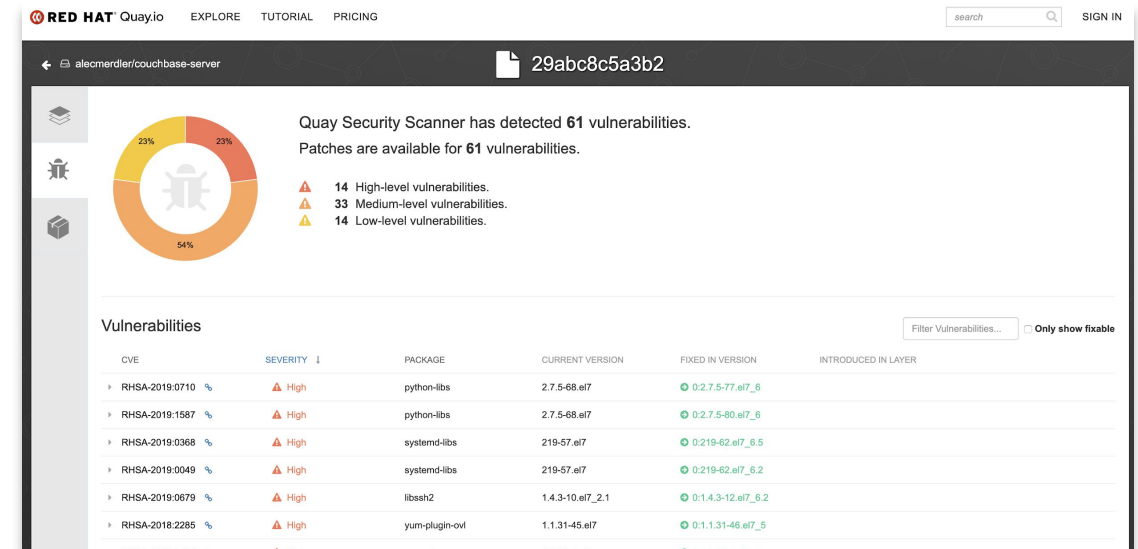


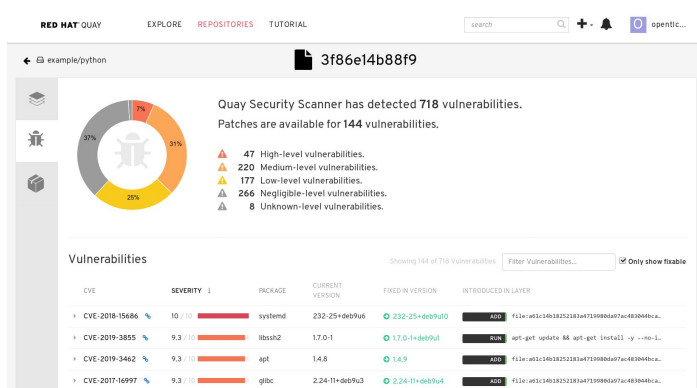
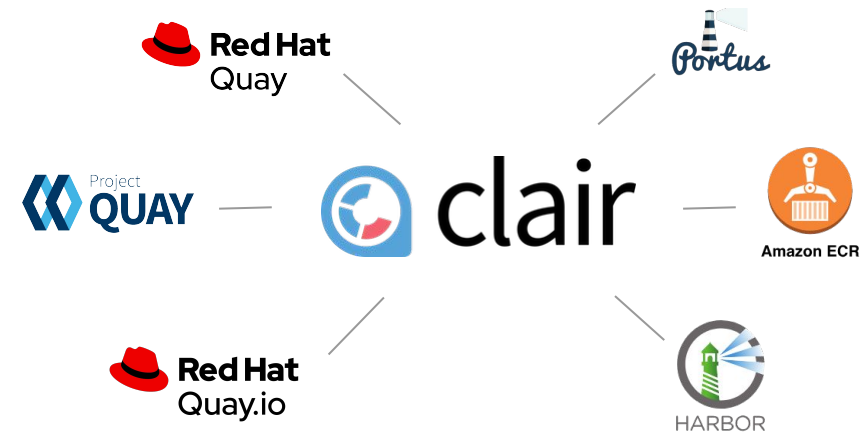
# Built-In Vulnerability Scanning via Clair

# Clair Overview



- Clair is an open source tool for static analysis of vulnerabilities in application containers
- Developed by CoreOS for Quay and it's massive scale usage at Quay.io
- Used by various other projects and third party products
- Upstream Repositories:  
<https://github.com/quay/clair>





## Clair v4 (Tech Preview with Quay 3.3)

Clair v4 is the newest version of Clair after a massive refactoring in order to make several big enhancements possible. This includes:

- Support for programming language package managers (3.3: python)
- immutable data model & new manifest-oriented API
- Refocus on latest container specifications (OCI) (Content addressability)

# Notifications for Vulnerabilities found by Clair

- **Quay triggers different notifications for various repository events** (depends on enabled features)
- This includes the event type **“Package Vulnerability Found”**
- Additional Filter can be applied for **Severity Level**
- **Various Notification Methods**
- Custom Notification Title (optional)

The image displays two overlapping screenshots of the Quay notification configuration interface.

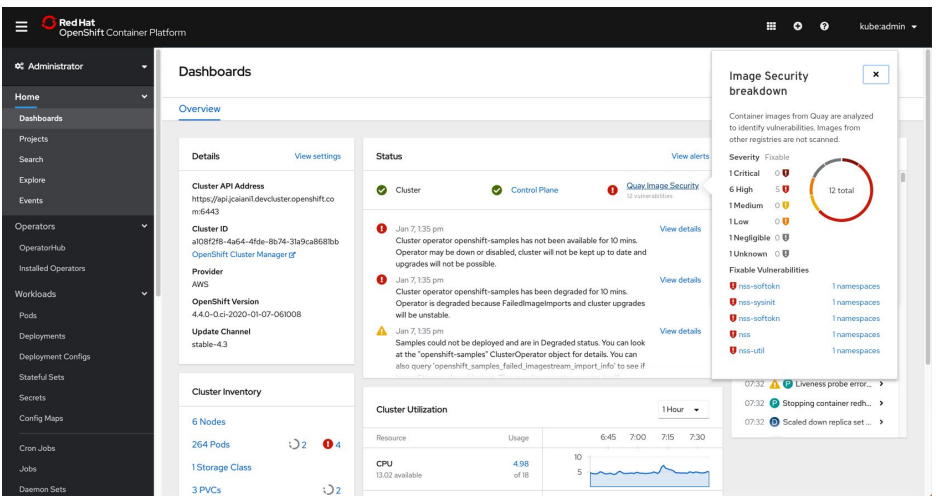
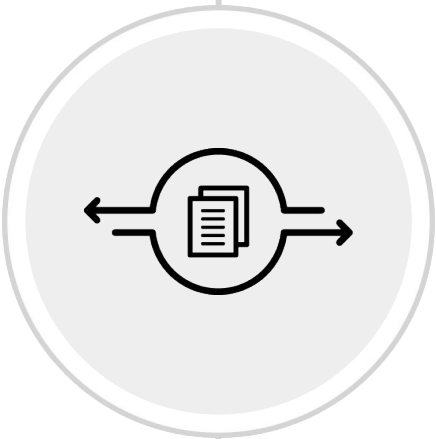
**Left Screenshot:**

- When this event occurs:** A dropdown menu is set to "Package Vulnerability Found".
- With minimum severity level:** A dropdown menu is set to "Critical".
- Text:** "A vulnerability must have a severity of the chosen level (or higher) for this notification to fire. Defcon 1 is a special severity level manually tagged by the Red Hat Quay team for above-critical issues".
- Then issue a notification:** A dropdown menu is set to "Please select a notification method".
- Notification Methods:** A list of methods is shown: Red Hat Quay Not, Webhook POST, Flowdock Team N, HipChat Room No, and Slack Room Notif.
- Create Notification:** A button is visible at the bottom.

**Right Screenshot:**

- When this event occurs:** A dropdown menu is set to "Please select the event".
- Event List:** A list of events is shown: Push to Repository, Repository Mirror Started, Repository Mirror Success, Repository Mirror Unsuccessful, Dockerfile Build Queued, Dockerfile Build Started, Dockerfile Build Successfully Completed, Dockerfile Build Failed, Docker Build Cancelled, and Package Vulnerability Found.
- Create Notification:** A button is visible at the bottom.






# Container Security Operator - Vulnerability Data in OpenShift


Operator which runs on OpenShift and fetches vulnerability from Quay / Clair if Kubernetes pod objects change


Synchronous Updates of vulnerability information

Prerequisite to leverage / show vulnerability data in OpenShift Console

**RED HAT<sup>®</sup> QUAY**

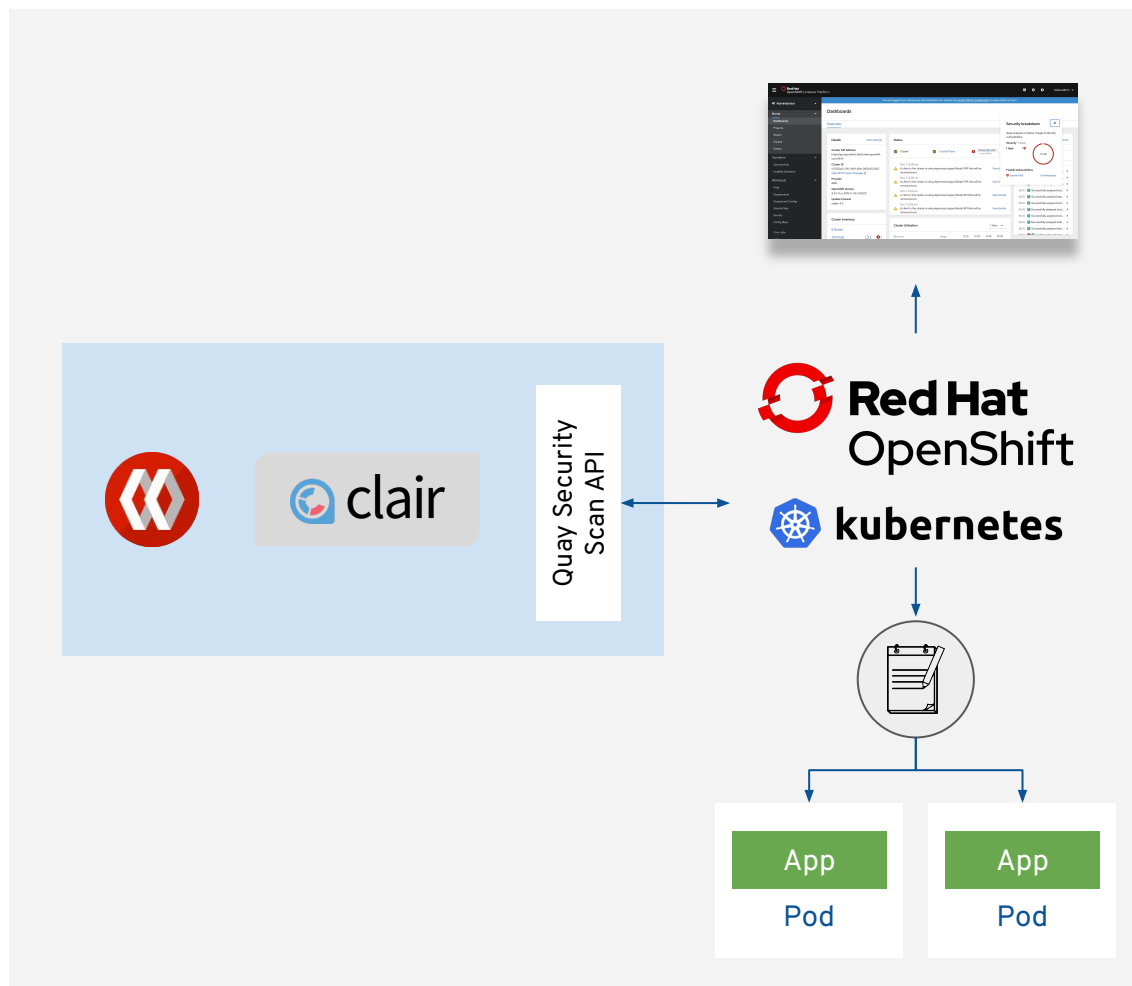
Scans images running on OpenShift and exposes data via API



**Red Hat OpenShift Container Platform**

Operator monitors pod objects and updates vulnerability data

## Container Security Operator (CSO)



- Container Security Operator (CSO) runs on OpenShift and watches pod objects
- Pod object changes triggering a data fetch from Quay/Clair and stores vulnerability information in CRs (by image manifest ID)
- CRs gets deleted if pod gets deleted
- Configurable interval to update vulnerability data from Quay / Clair (default: 5min)
- Data available via k8s CLI / APIs
- Supposed to be used by partner security products as well (consistent data ingress)

# Vulnerability Data inside the OpenShift Console

Administrator

Home

Operators

Workloads

Networking

Storage

Builds

Monitoring

Compute

User Management

Administration

Project: all projects

Image Manifest Vulnerabilities

Filter by name...

Image Name	Namespace	Highest Severity	Affected Pods	Fixable	Manifest
VULN alecmerdler/bad-pod	NS default	Medium	1	0	35c1c5688e7
VULN alecmerdler/bad-image	NS skynet	Unknown	1	1	4bc210f89d7
VULN alecmerdler/bad-pod	NS default	Critical	1	0	7d4aae77622
VULN 3scale/3scale-operator	NS default	High	1	24	9a6536efbb5
VULN alecmerdler/bad-image	NS skynet	Unknown	1	1	b025832c073
VULN alecmerdler/bad-pod	NS default	Low	1	0	e94c22ba519
VULN alecmerdler/bad-pod	NS default	Defcon 1	1	0	f4cd12ac979

ImageManifestVuln list view

# Vulnerability Data inside the OpenShift Console

Administrator

Home

Operators

Workloads

Networking

Storage

Builds

Monitoring

Compute

User Management

Administration

Project: default

ImageManifestVuln > ImageManifestVuln Details

VULN

3scale/3scale-operator@9a6536efbb5

Overview

YAMLAffected Pods

Image Manifest Vuln Overview

Quay Security Scanner has detected 24 vulnerabilities.  
Patches are available for 24 vulnerabilities.

24 total

6 High vulnerabilities.

12 Medium vulnerabilities.

6 Low vulnerabilities.

Name

sha256:9a6536efbb5f23ff4a2c2d76065c1c37a84dc7404da259cd9e5f71b637d28f6

Registry

quay.io/3scale/3scale-operator

Namespace

default

Labels

default/3scale-operator-7864b9bb5d-frhint=true

Annotations

0 Annotations

Created At

Dec 23, 2019 10:30 am

Owner

Administrator

Home

Operators

Workloads

Networking

Storage

Builds

Monitoring

Compute

User Management

Administration

Project: skynet

0 Annotations

Created At

Jan 6, 11:42 am

Owner

No owner

Vulnerabilities

CVE	Severity	Package	Current Version	Fixed in Version
<a href="#">RHSA-2019-4190</a>	High	nss-softokn	3.36.0-5.el7_5	0:3.44.0-8.el7_7
<a href="#">RHSA-2019-4190</a>	High	nss-sysinit	3.36.0-7.1.el7_6	0:3.44.0-7.el7_7
<a href="#">RHSA-2019-4190</a>	High	nss-softokn-freebl	3.36.0-5.el7_5	0:3.44.0-8.el7_7
<a href="#">RHSA-2019-4190</a>	High	nss-util	3.36.0-11.el7_6	0:3.44.0-4.el7_7
<a href="#">RHSA-2019-4190</a>	High	nss	3.36.0-71.el7_6	0:3.44.0-7.el7_7
<a href="#">RHSA-2019-4190</a>	High	nss-tools	3.36.0-71.el7_6	0:3.44.0-7.el7_7
<a href="#">RHSA-2019-2237</a>	Medium	nss-softokn	3.36.0-5.el7_5	0:3.44.0-5.el7
<a href="#">RHSA-2019-2237</a>	Medium	nss-sysinit	3.36.0-71.el7_6	0:3.44.0-4.el7
<a href="#">RHSA-2019-2237</a>	Medium	nss-softokn-freebl	3.36.0-5.el7_5	0:3.44.0-5.el7
<a href="#">RHSA-2019-2237</a>	Medium	nss-util	3.36.0-11.el7_6	0:3.44.0-3.el7
<a href="#">RHSA-2019-2304</a>	Medium	openssl-libs	1:1.0.2k-16.el7_6.1	1:1.0.2k-19.el7
<a href="#">RHSA-2019-2118</a>	Medium	glibc-common	2:17-760.el7_6.4	0:2.17-292.el7

ImageManifestVuln detail view

# Vulnerability Data inside the OpenShift Console

The screenshot shows the OpenShift console interface. On the left is a dark sidebar with navigation links: Administrator, Home, Operators, Workloads, Networking, Storage, Builds, Monitoring, Compute, and User Management. The main content area is titled 'Project: default' and shows the 'ImageManifestVuln' details for '3scale/3scale-operator@9a6536efbb5'. A blue 'VULN' badge is next to the image name. Below the title are tabs for 'Overview', 'YAML', and 'Affected Pods', with 'Affected Pods' being the active tab. A search bar 'Filter by name...' is on the right. A table lists the affected pods:

Name ↑	Namespace ↑	Created ↑
P 3scale-operator-7864b9bb5d-frhnt	NS default	11 days ago

ImageManifestVuln detail view (affected pods)

# Vulnerability Data inside the OpenShift Console

The screenshot shows the OpenShift console interface. On the left is a dark sidebar with navigation links: Administrator, Home, Operators, Workloads, Networking, Storage, Builds, Monitoring, Compute, and User Management. The main content area shows the 'Project: default' dropdown at the top. Below it is a breadcrumb 'ImageManifestVuln > ImageManifestVuln Details'. A blue 'VULN' badge is next to the text '3scale/3scale-operator@9a6536efbb5'. There are three tabs: 'Overview', 'YAML', and 'Affected Pods', with 'Affected Pods' being the active tab. A search bar on the right says 'Filter by name...'. Below this is a table with columns 'Name', 'Namespace', and 'Created'. The table contains one row: a pod icon, '3scale-operator-7864b9bb5d-frhnt', a namespace icon, 'default', and '11 days ago'. A kebab menu icon is at the end of the row.

Name	Namespace	Created
3scale-operator-7864b9bb5d-frhnt	default	11 days ago

Kebab action on Pods list view

# 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://linkedin.com/company/red-hat)



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



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



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