redhat.

# SECURING CONTAINERS WITH OPENSHIFT

Jason Dudash
Specialist Solutions Architect
Red Hat

# SECURING CONTAINERS: THE TOP TEN LIST

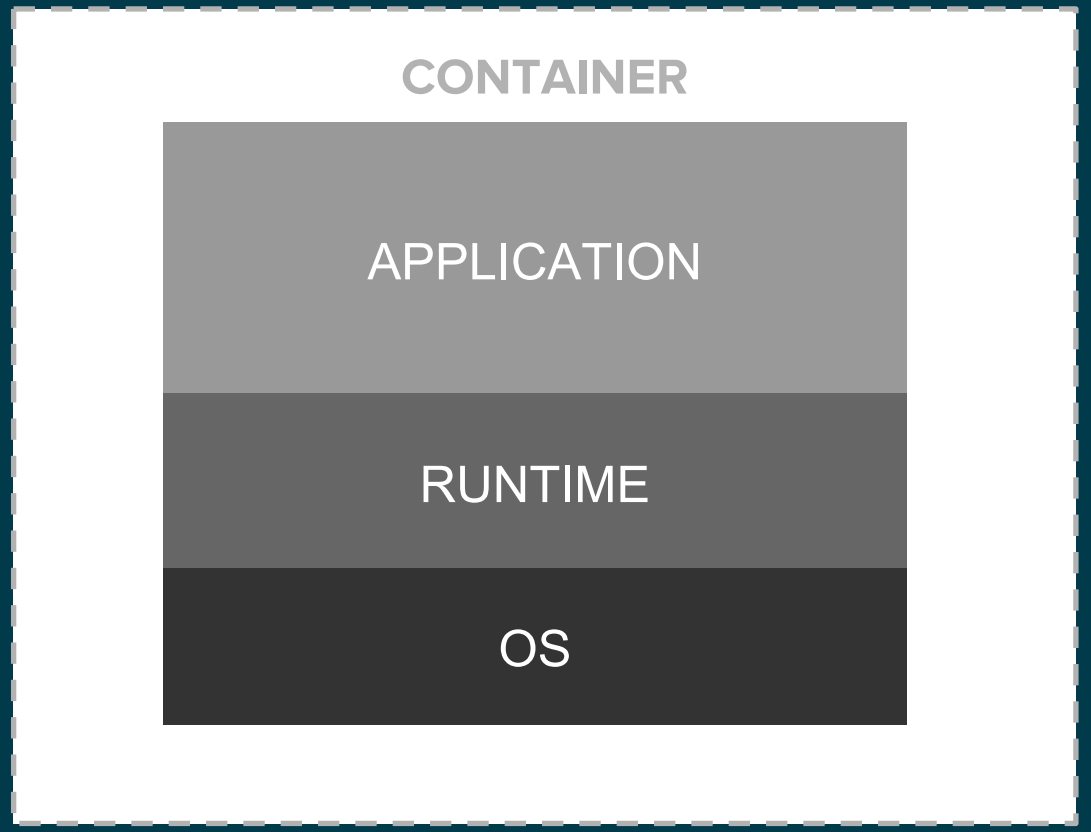
1. Container Host & Multi-tenancy
2. Public Images
3. Private Registries
4. Building Containers
5. Deploying Containers
6. Container Platform
7. Network Isolation
8. Storage
9. API Management
10. Federated Clusters

# SECURING CONTAINERS: THE TOP TEN LIST

1. Container Host & Multi-tenancy
2. **Public Images**
3. **Private Registries**
4. **Building Containers**
5. **Deploying Containers**
6. Container Platform
7. Network Isolation
8. Storage
9. API Management
10. Federated Clusters

# CONTENT: EACH LAYER MATTERS

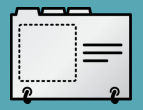
- Are there known vulnerabilities in the application layer?
- Are the runtime and OS layers up to date?
- How frequently will the container be updated and how will I know when it's updated?



# THE VALUE OF TRUSTED CONTENT

**Red Hat Registry Stats**

- 227 repositories
- 2,169 images
- 1+ TB storage



**Red Hat Security Statistics 2016**

- 97 critical RHSA
- 286 important RHSA
- 100% fixed in <1d

**Red Hat Customer Portal Stats 2016**

- 13,100,000 visitors
- 2,400,000 searches
- 108,300,000 views

- Image Documentation
- Image Advisories

RED HAT® CONTAINER CATALOG

- Container Health Index
- Extensive Image Metadata

Red Hat rebuilds container images when security fixes are released

# Java Applications

by Red Hat, Inc. | in Product Red Hat OpenShift Container Platform

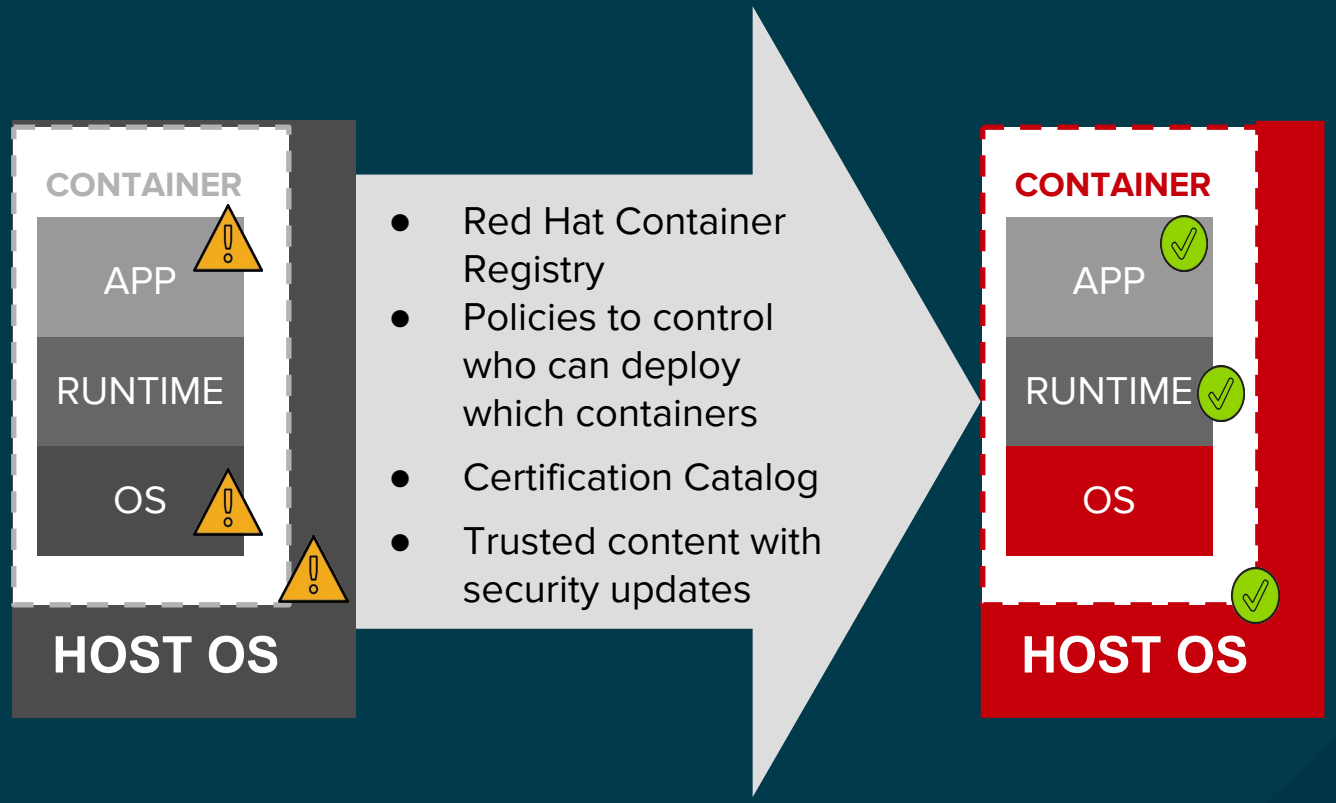
registry.access.redhat.com/redhat-openjdk-18/openjdk18-openshift Updated 7 days ago 1.0-3 : Health Index A


| Tag Name | Date Pushed | Image Advisory | Health Index | Docker Image ID |
|---|---|---|---|---|
| 1.0-3 1.0 latest | 7 days ago | RHBA-2017:1168 | A | af2b44054a5d |
| 1.0-2 | 2 months ago | RHEA-2017:0291 | C | 0e4bec3a7491 |

# PRIVATE REGISTRIES:
## SECURE ACCESS TO IMAGES

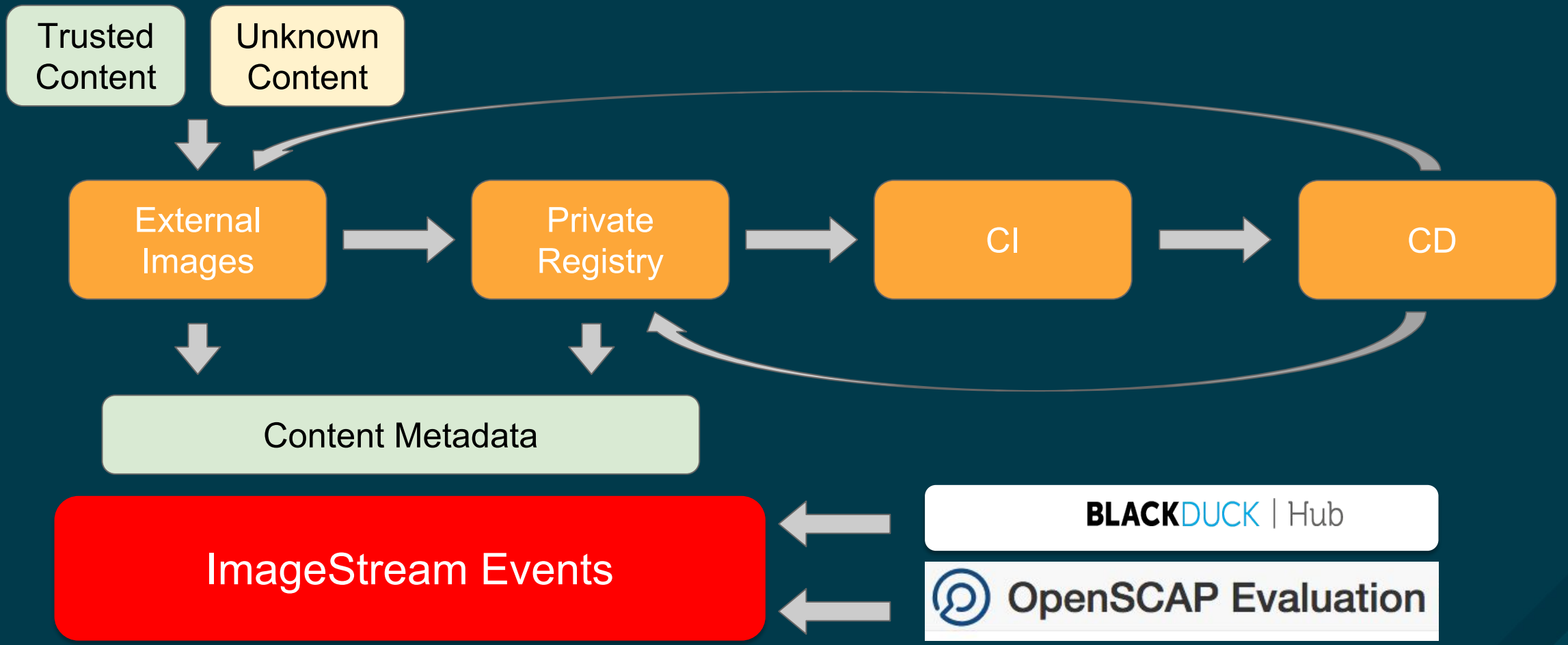
Image governance & private registries

- Are there access controls on the registry? How strong are they?
- What security meta-data is available for your images?
- How is the data kept up-to-date?



# THE CONTAINER CONTENT LIFECYCLE

Trust is temporal; re**build** and re**deploy** as needed



# CD: MANAGING CONTAINER DEPLOYMENT

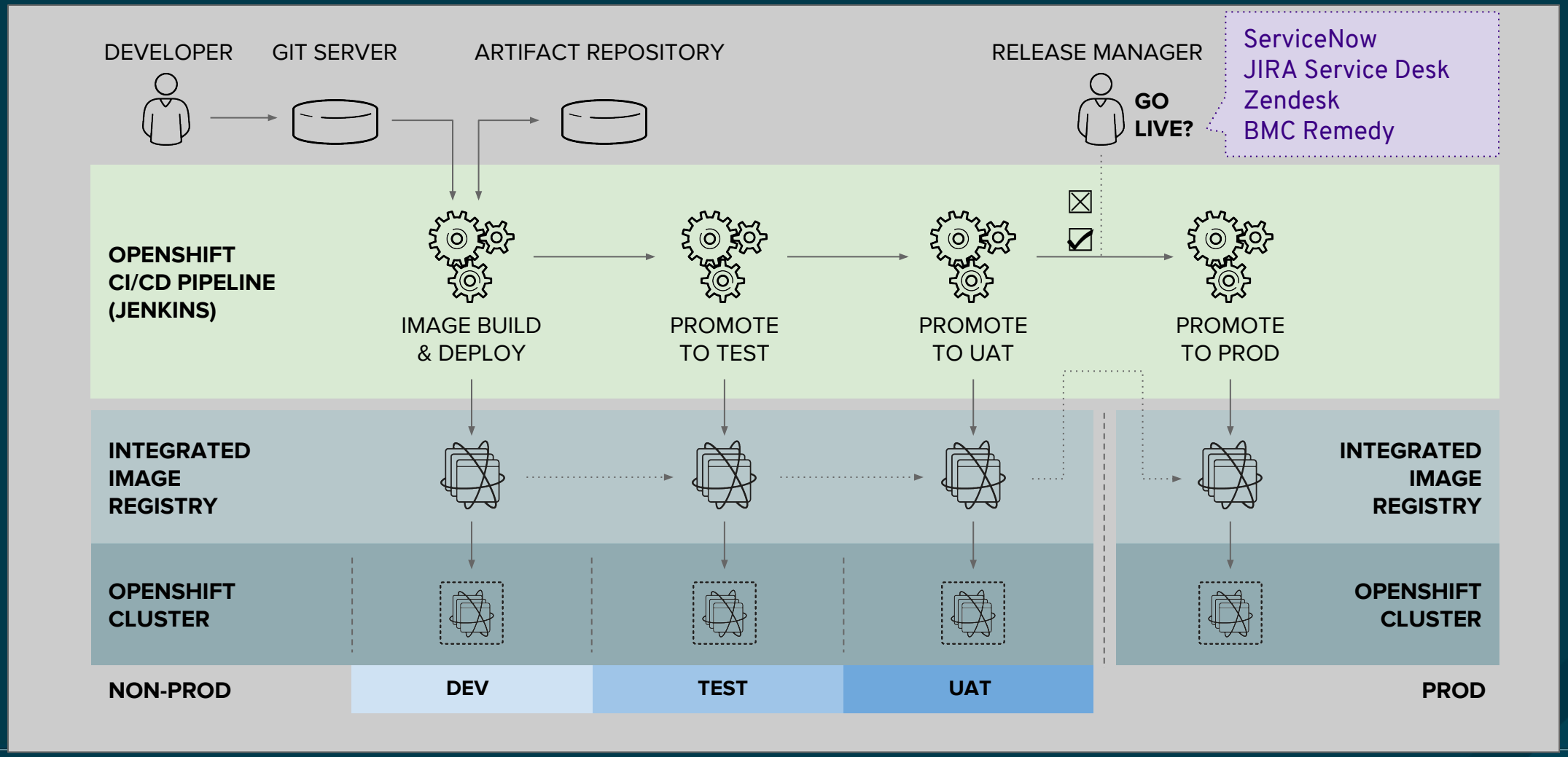
Security & continuous deployment

- Monitor image registry to automatically replace out-of-date images
- Use policies to gate what can be deployed: e.g. if a container requires root access, prevent deployment
- Monitor images for vulnerabilities

```
$ 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 Volume Types:       configMap,downwardAPI,emptyDir,persistentVolumeClaim,secret
  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
    UID:             <none>
    UID Range Min:            <none>
    UID Range Max:            <none>
  SELinux Context Strategy:         MustRunAs
    User:               <none>
    Role:               <none>
    Type:               <none>
    Level:              <none>
  FSGroup Strategy:                 MustRunAs
    Ranges:             <none>
  Supplemental Groups Strategy:     RunAsAny
    Ranges:             <none>
```

Policies control the actions that a pod can perform and what it has the ability to access

# THE OPENSHIFT CI/CD PIPELINE



RED HAT® OPENSHIFT Container Platform

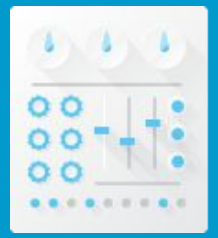
# SECURITY THROUGHOUT THE STACK AND THE LIFECYCLE

Self-Service

Service Catalog
(Language Runtimes, Middleware, Databases)

Build Automation | Deployment Automation

OpenShift Application Lifecycle Management
(CI/CD)



Container Orchestration & Cluster Management
(Kubernetes)

Networking | Storage | Registry | Logs & Metrics | Security

Infrastructure Automation & Cockpit

**Enterprise Container Host**

Container Runtime & Packaging
(docker)

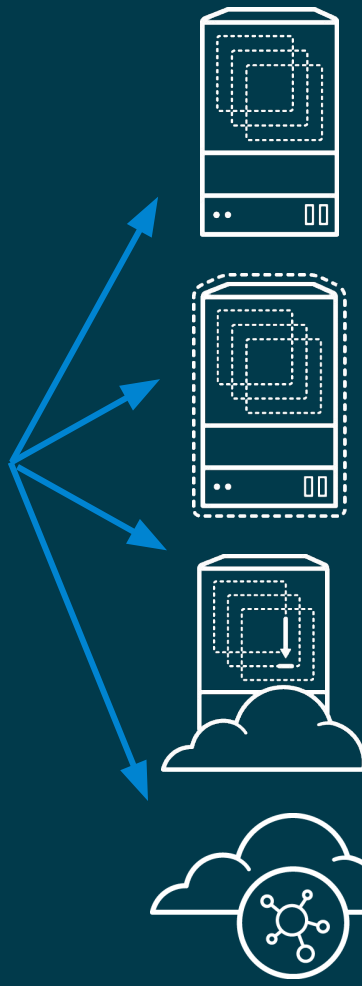
Atomic Host | Red Hat Enterprise Linux

Web & Mobile
Contaner

Data & Storage
Container

Integration
Container

Business Automation
Container



Physical

Virtual

Private cloud

Public cloud



redhat.

Learn more about OpenShift Online and sign up for free

Read the Ten Layers of Container Security whitepaper

Read the 2016 Red Hat Product Security Risk Report

Deeper Technical Details - OpenShift Container Security

redhat.

# THANK YOU