

# OpenShift Security

Best Practice

# What are we going to talk about?



**Understanding the security culture in most enterprises**



**Common OpenShift security related customer concerns**

- Calling out landmines



**OpenShift security best practices**

- Addressing customer concerns with key (not all) OpenShift security technologies
- Setting correct expectations given current gaps



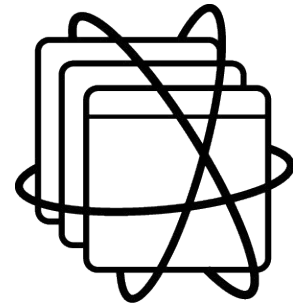
**OpenShift security roadmap**

# Common OpenShift Security Related Customer Concerns

CONFIDENTIAL designator

*What are the typical questions we hear from our customers?*

- Are container secure?
- Host security
- Audit and Logging
- Network security
- Certificates
- Application secrets management
- Image scanning and signing
- When to use 3rd party OpenShift security vendors and who to pick
- OpenShift compliance to security standards
- Other OpenShift security concerns

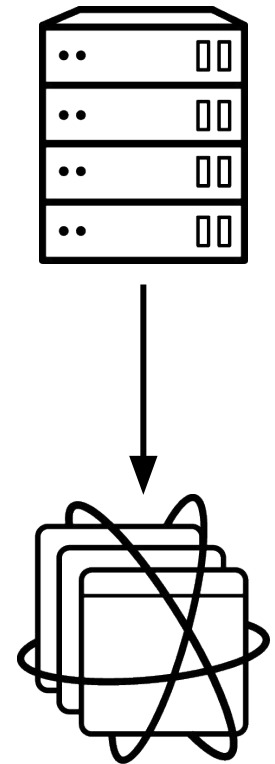


# Are containers secure?

# Deploying in Containers

*Helping customers understand the paradigm shift to containers*

- Deploying in containers requires a mind-shift from traditional “applications on servers” mindset.
- **Application on Servers**
  - Rigid startup sequences; don’t expect restarts
- **Containers**
  - Restart at any time; loosely coupled components



# Are containers secure?

*Combination of container constructs and OpenShift features embrace a secure runtime*

## Container Fundamentals

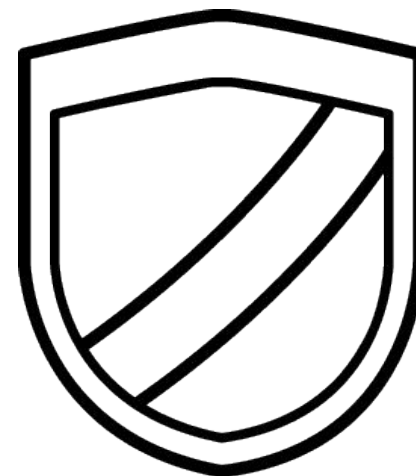
- Container runtime, which provides resource isolation between processes
- User namespace, which provides the Linux context in which the process runs and basic file permissions for those processes
- SELinux, which ensures namespace boundaries are not crossed

## Red Hat Container Catalog with Container Health Index:

- Red Hat vetted container images with container freshness grade

## OpenShift Features

- Security Context Constraints (SCC), which when Restricted, ensures each container runs as a unique, arbitrary userid



# Host security

# Host Security

## *Areas of considerations for OpenShift nodes*



- Management secrets will exist
  - SSH keys, certificates, cloud configurations
- Avoid placing privileged information or put any privileges on a cluster node where it's not required.
  - Compute nodes need minimal privileges.
  - Master nodes need slightly higher privileges
    - Eg: Attach/detach cloud based storage devices



# Audit/Logging

# Audit/Logging

*How do I know what is happening in my environment?*

- Log forwarding to security
- OpenShift Auditing Capabilities
  - Basic and Advanced audit
- Don't forget Linux/RHEL tools including auditd
- How can I monitor for abnormal behavior?
  - Most customers point their logging at a SIEM tool
  - Most NA public sector customers are using Splunk and others are looking at Twistlock/Sysdig to augment the alerting capabilities
- Red Hat Insights can also be used to provide predictive analysis of OpenShift environment



## Kernel Side-Channel Attacks (Meltdown & Spectre) [1/3/18]

Red Hat Product Security has been made aware of vulnerabilities affecting modern microprocessors for all operating systems on all hardware platforms that could allow unauthorized read access to memory. This issue has been assigned CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754. All currently supported versions of Red Hat Enterprise Linux, Red Hat OpenShift, Red Hat Virtualization, and Red Hat OpenStack Platform are affected.

## Kernel Side-Channel Attacks (Meltdown & Spectre) [1/3/18]

[illegible]

These vulnerabilities in many of the operating customers in understa

[rhev-m.insights.redhat.com](http://rhev-m.insights.redhat.com)

12 hours ago

[controller2.insights.redhat.com](http://controller2.insights.redhat.com)

12 hours ago

[View actions](#)[View planner](#)

## Plan Summary

[✓ You have a new plan suggestion \(4 actions\)](#)

## Newest Plans

### Actions

OCP

16/24

Lets fix these issues

3/3

## Privilege escalation

0/5

28 issues can be resolved automatically using  Ansible

### Create a new Plan/Playbook

### Plan Summary

☒ You have a new plan

### Newest Plans

OCP

Lets fix these issues

## Privilege escalation

0/5

28 issues can be resolved automatically using  Ansible

**Create a new Plan/Playbook**

Virtual Network will not work when network bridge is on bonding mode 5 or 6  
Published 3 days ago

[View all 10 new rules](#)

# INSIGHTS RULES FOR OPENSIFT

CONFIDENTIAL designator

- Communication fails between components when certificates have expired in OpenShift
- Image build failure when creating a large number of concurrent builds
- Containers allow non-privileged user to modify filesystem inside containers when created with cri-o
- Docker registry pod restarts occasionally when liveness and readiness probes collide
- Failed api connection between docker and OpenShift when version of docker and openshift are incompatible
- Insufficient space available when image garbage collection fails to run in OpenShift
- GlusterFS storage disconnects from pods when restarting atomic-openshift-node server
- Master controller fails to start when changes are made to the SDN plugin if there are headless services in the cluster
- Failure to connect to service when configured IP is in use by another service
- Pod creation fails when is under high load due to iptables-restore process
- Excessive load time for new routes when a large number of routes exist

[Overview](#)[Actions](#)[Inventory](#)[Planner](#)[Rules](#)[Executive Report](#)[Configuration](#)[Customer Portal](#)

## Inventory



Check in status

All ▾

System Health

All ▾

Actions ▾

4 Systems

[+ Register More](#)

<input type="checkbox"/>	System Type ▾	System Name	▲ Last Check In ▾	Actions ▾
<input type="checkbox"/>	RHEL Server	<a href="#">infranode1.learningpurposes.internal</a>	an hour ago	7 <span>🔴</span>
<input type="checkbox"/>	RHEL Server	<a href="#">master1.learningpurposes.internal</a>	an hour ago	7 <span>🔴</span>
<input type="checkbox"/>	RHEL Server	<a href="#">node1.learningpurposes.internal</a>	an hour ago	7 <span>🔴</span>
<input type="checkbox"/>	RHEL Server	<a href="#">node2.learningpurposes.internal</a>	an hour ago	7 <span>🔴</span>



## infranode1.learningpurposes.internal

Hostname: infranode1.learningpurposes.internal  
UUID: 93e50b5c-c8b2-477f-bda7-8f1658f94b20

Groups:

OCP cluster

Registration Date an hour ago

Operating System RHEL Server release 7.5 (Maipo)

Last Check-in an hour ago

System

Network

### RULES

Expand All

> Availability > Kdump does not work due to XEN/AWS's limitation.

Impact Likelihood Total Risk Risk of change: Very Low

> Security > Kernel vulnerable to local privilege escalation via exceptions triggered after the POP SS and MOV to SS instructions (CVE-2018-8897, CVE-2018-1087)

Impact Likelihood Total Risk Risk of change: Moderate

Search plans

## Plans

ocp-sec (36798)



Actions

Systems

[Playbook](#)

[Kdump does not work due to XEN/AWS's limitation.](#)

[Edit](#)

[Impact](#) [Likelihood](#) [Total Risk](#)

	System	Last check in	Status
<a href="#">infranode1.learningpurposes.internal</a>		a few seconds ago	—
<a href="#">master1.learningpurposes.internal</a>		a few seconds ago	—
<a href="#">node1.learningpurposes.internal</a>		a few seconds ago	—
<a href="#">node2.learningpurposes.internal</a>		a few seconds ago	—

[Download Playbook](#)

[Export CSV](#)

[Add actions](#)



```
[root@master1 ~]# ls
anaconda-ks.cfg  ocp-issues.yml  openshift_bootstrap  original-ks.cfg  project-template.yml  rebreak-ocp.yml
[root@master1 ~]# ansible-playbook ocp-issues.yml

PLAY [Disable kdump service] *****

TASK [Gathering Facts] *****
ok: [node1.learningpurposes.internal]
ok: [node2.learningpurposes.internal]
ok: [master1.learningpurposes.internal]
ok: [infranode1.learningpurposes.internal]

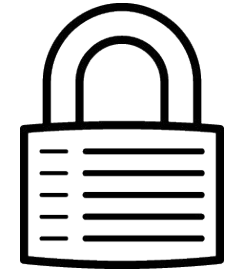
TASK [disabled and stop kdump service] ****
```



# Network security

# Network security concerns

*Networking can be complex. Keep it simple*



- Single cluster straddling multiple network zones
  - Just don't do it
  - Can deploy across multiple networks (e.g. AWS multi-AZ). All networks must have same security posture.
- When higher level security requirements are in place, the one cluster per network zone is most common
- Encryption over the wire
  - Management traffic already uses SSL. Use SSL/TLS at the application layer
- Traffic management
  - Applications no longer have distinct source IPs (may appear anywhere within the clusters).
    - Use egress routers or IP with application specific addresses
  - Access control using NetworkPolicy SDN plugin

# Certificates

# Infrastructure Certificates

- OpenShift contains its own certificate authority for generating infrastructure certificates
  - These are considered “self-signed”
  - Cannot be replaced or substituted
- Common customer concerns
  - Certificate expiration/renewal
    - Can be managed with operational procedures with Red Hat provided playbooks.
  - “Self signed certificates are insecure”
    - Not a true statement

# Application Wildcard DNS/Certificates

*OpenShift's router can use a default certificate that matches the default DNS subdomain for applications running on the platform*

- Customers can be uncomfortable with wildcard DNS and certificates
- *Only* really required for truly dynamic environments - typically sandbox and development
  - Not required for production deployments as the applications are typically planned
- Suggest wild-card with an obviously stupid domain name
  - \*.notforreal.cloudapps.myorg.com
- Can customer generate certificates in real-time?
  - Custom controller in OCP can communicate with CA API to register and configure

# Application Certificates

TLS certificates are utilized throughout the OpenShift cluster

- Use certificates from CA trusted by customer for externally facing uses including the OpenShift API, web console and applications.
  - The OpenShift CA can also generate certificates for non-critical uses.
- End users have the ability to define how certificates are managed for their applications by OpenShift router
  - Different ways of managing certificates
    - SSL Termination types: None, Edge, Passthrough, Reencrypt



# Application secrets management

# Application Secrets

*Sensitive application configuration must be managed in a secure fashion*

- OpenShift Secrets
  - Secrets are not secret (instead of being encrypted, they are merely base-64 encoded at rest). Etcd now has the option to encrypt the data at rest.
- Accept and use compensating controls
  - Controls may make platform unmanageable
- Use external vault/secure storage
  - Most customers use Hashicorp Vault and Cyberark Conjur
  - Some also use Twistlock and Sysdig
  - Bootstrap problem - Need to establish container identity to access vault

*No solution is 100% secure*



# Image Management

# Image Policy

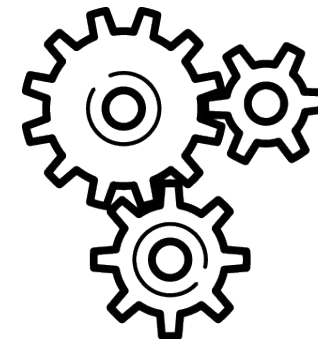
*OpenShift ecosystem supports controlling the images that can be run on the platform*

- Container runtime level
  - Block vulnerable image registries (DockerHub)
- OpenShift
  - ImagePolicy Admission Plugin
    - Block images from running
      - Based image source, label or annotation
        - Annotation: `images.openshift.io/deny-execution`



# Image Scanning

*Reduce threat vector by assessing image contents*



- OpenSCAP scanning integrated into OpenShift Ecosystem
  - Supports only RPM analysis. Most organizations want deeper inspection
  - Image-inspector image available for standalone use or integration in CFME
- Red Hat Solutions
  - Atomic scan, Clair (Quay ecosystem)
  - Red Hat Container Catalog (RHCC) provides health index
- Multiple 3rd Party vendor solutions
  - Twistlock, BlackDuck, Sysdig, Aqua

Many customers evaluating 3rd party integrations - Trust but verify

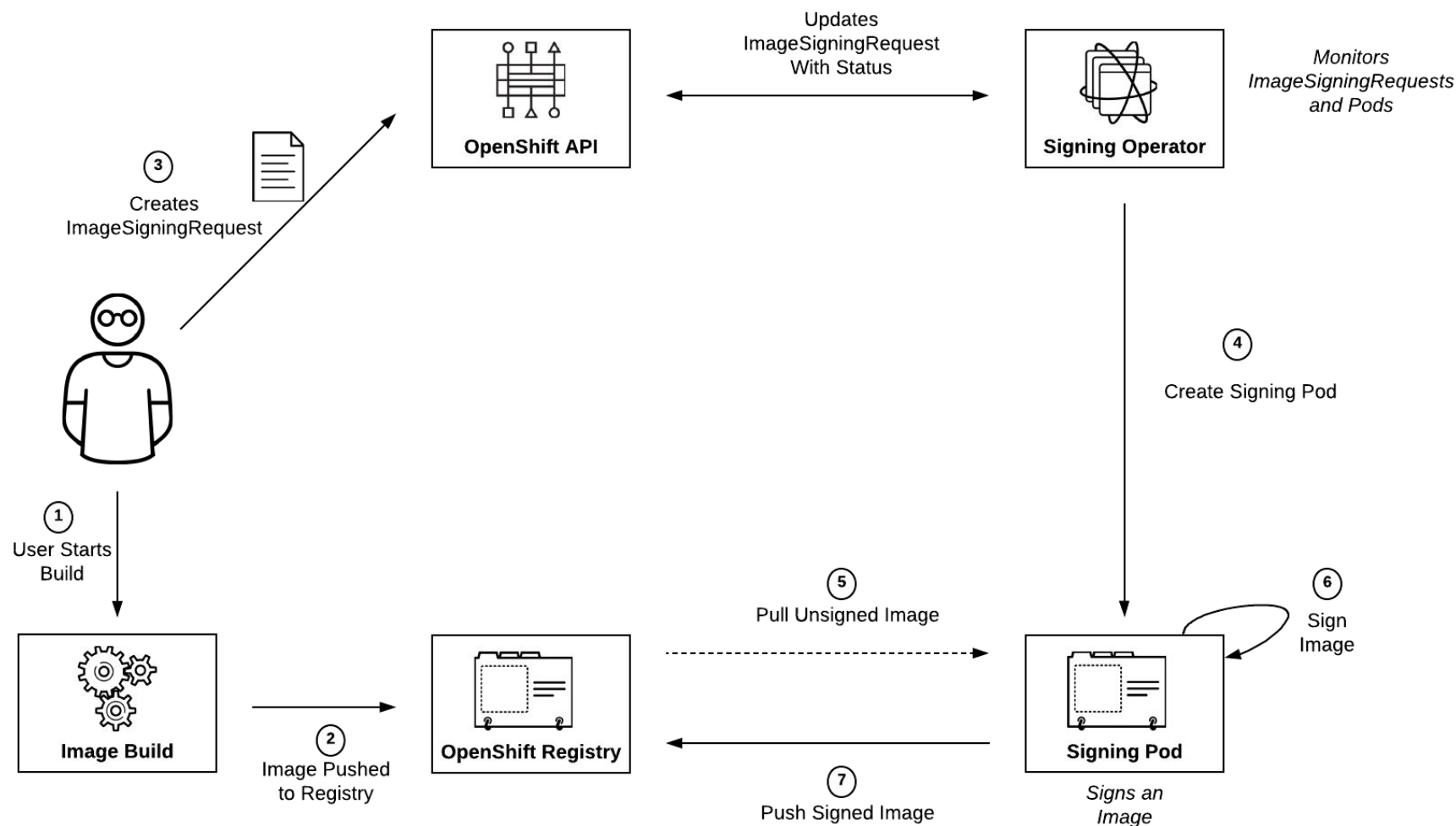
# Image Signing

*Digital signature applied to container images to aid in verifying trust*

- Organizations want to leverage signing to certify images at various stages of SDLC
- `atomic sign` is the current supported method
  - GPG key based
  - Each node must have GPG key used to sign image
- Container runtime can also be configured to enforce image signatures
- Docker Notary one of the most popular implementations
- Future:
  - Clair as part of Quay to do scanning, signing and policy enforcement in OpenShift (act on it). Targeted for 4.1.

Several projects of interest in the Kubernetes community including Grafeas and Kritis. Progress in these communities is slow.

# Image Signing Example



# Extending OpenShift Security capabilities with 3rd Party security vendor solutions

# When do I have to use a 3rd party vendor solution and who do I pick?

CONFIDENTIAL designator



NGINX



Black Duck



F5

Networking



Code  
Scanning



Twistlock

Image  
Scanning



Sonatype

JFrog

Repositories



Cyberark

Secrets  
Management



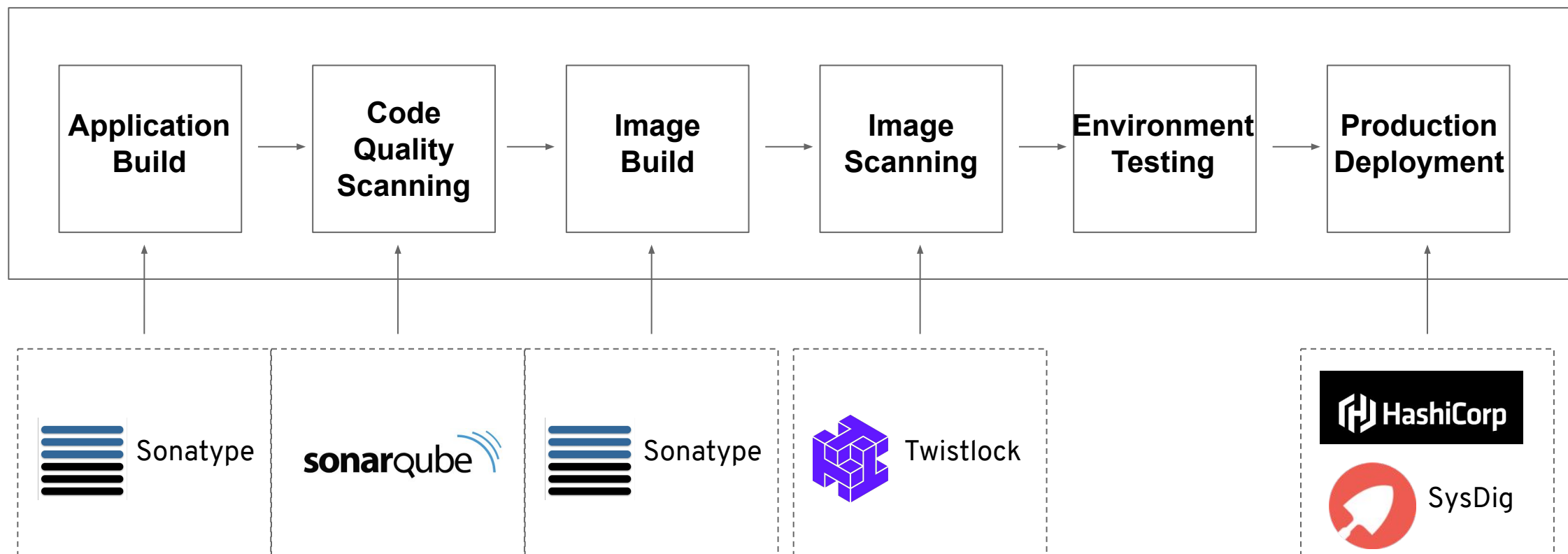
SysDig



Dynatrace

Monitoring

# Secure CI/CD Pipeline





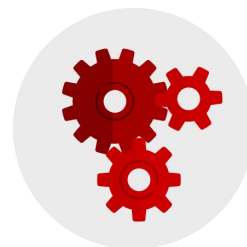
# Security Roadmap

# Security Themes



## Control Application Security

Connect workload identity to Cloud  
provider authorization  
Application certificate lifecycle  
management



## Defend the Infrastructure

Encrypt etcd datastore  
Enhanced certificate management  
RHEL CoreOS disk encryption  
VPN / VPC support  
Consume group membership from  
Identity Provider  
External Keycloak integration



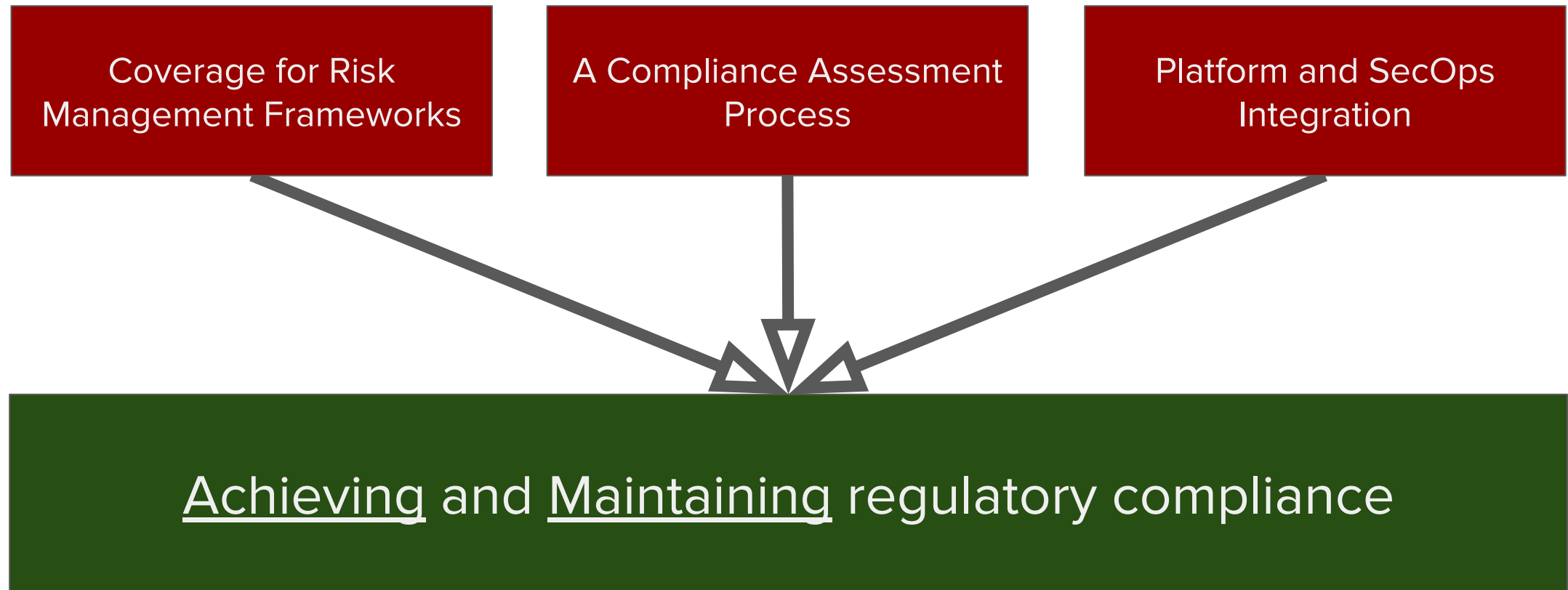
## Automate Compliance

Disconnected / air-gapped install  
FIPS compliance  
Cipher Suite Configuration  
Compliance Operator

# OPENSIFT COMPLIANCE OPERATOR

CONFIDENTIAL designator

*Automate compliance audit and remediation*



# OpenShift Security Roadmap

CONFIDENTIAL designator

## Near Term (4.3)

- VPC / VPN support
- Encrypt etcd datastore
- FIPS compliance
- RHCOS disk encryption
- Reference architecture for GitOps based cluster config management with [Argo CD](#)
- External DNS (DNS Forwarding)
- IPv6 (secondary data plane interfaces)
- Global Cipher and TLS Policy API


## Longer Term (4.4+)

- Automate rotation of Service CA
- Global Options to Enable HTTP Strict Transport Security (HSTS)
- Full Support for IPv6, HTTP/2
- External Keycloak integration
- Service for application certificate lifecycle management
- Integration workload identity with Cloud Provider IAM solutions
- Compliance operator
- Consume group membership from external Identity Provider

# 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)