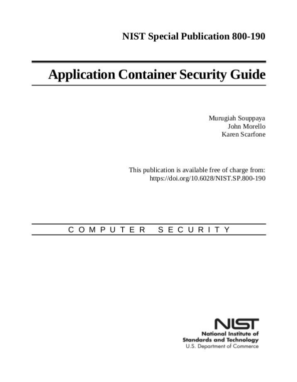
Executing on NIST SP 800-190

How organizations are leveraging Red Hat OpenShift, Red Hat Quay, and Palo Alto Networks Prisma Cloud to deploy, manage, and secure a cloud native environment.

Dirk Herrmann
Product Manager Quay

What is a NIST Special Publication?



NIST Special Publication 800-190

Application Container Security Guide

Murugiah Souppaya
John Morello
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-190

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

- Created for significant advancements in technology
- Vendor-agnostic, high level recommendations
- Designed for government and private sector use

The foundation of a collaborative effort between Red Hat and Palo Alto Networks to address items inside this publication for our customers.

"Many organizations struggle with the burden of managing security across **hundreds of VMs**.

As container-centric architectures become the norm and these organizations are responsible for **thousands or tens of thousands of containers**, their security practices should emphasize automation and efficiency to keep up."

NIST

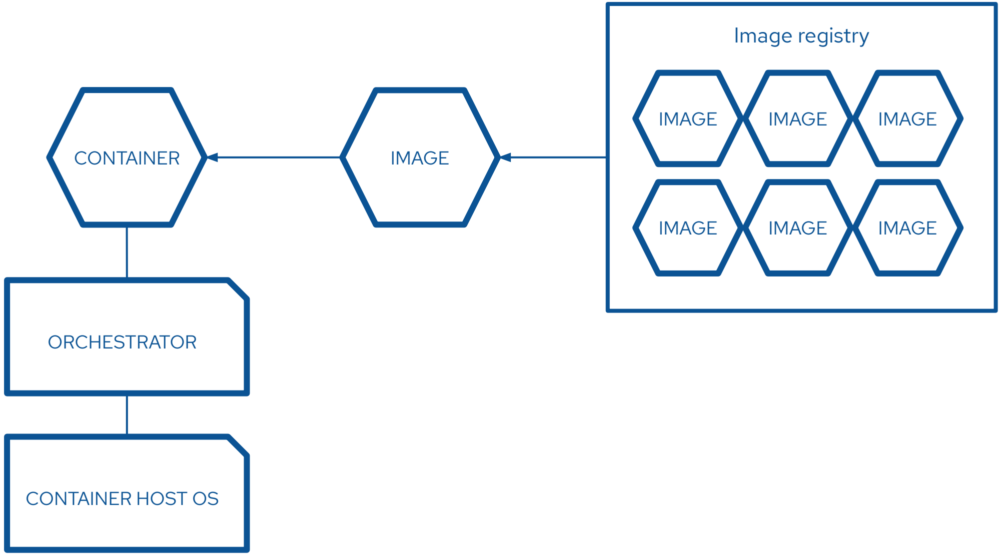
Source: NIST Special Publication 800-190 - Application Container Security Guide

The Challenges of Securing Containers

- Limited expertise and experience with emerging technologies
- Massive amount of entities compared with the traditional world with a high rate of change and things are much more ephemeral
- multi-X (cluster | cloud | product | vendor) environments
- Security is largely in the hands of the developer (“shift left”)
- Security must be as portable as the containers
- Traditional operation model, processes and tooling not applicable

The Five Major Risk Areas

According to NIST SP 800-190



A **container** is the smallest compute unit.

Containers are created from container **images**.

Container images are stored in an image **registry**.

The container runs on an **orchestration** platform.

The orchestrator runs on a **container host OS**.

Image Risks and Countermeasures

- ★ Image vulnerabilities
- ★ Image configuration defects
- ★ Embedded malware
- ★ Embedded clear text secrets
- ★ Use of untrusted images

- ❑ Use container-specific technology for vulnerability, compliance and secrets management
- ❑ Integrate checks and monitoring across the image lifecycle
- ❑ Automated, policy-driven enforcement
- ❑ Mitigate risks with trusted images

NIST SP 800-190: Key Takeaways

- Adapt your IT organization and operational model to reflect new paradigms
- Use container host operating system variants for smaller attack surface
- Keep workloads separated by sensitivity levels
- Use tools and processes built for the new paradigms and technologies
- Carefully select content and implement a content governance process
- Choose tools that give you visibility into your full stack – containers, hosts and orchestration.

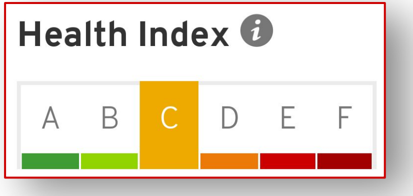
Red Hat and Palo Alto Networks help you **implement** the NIST SP 800-190 recommendations.

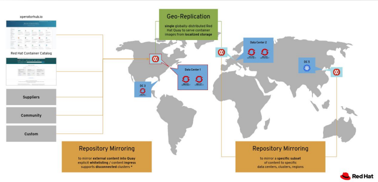
4.1 Image Countermeasures

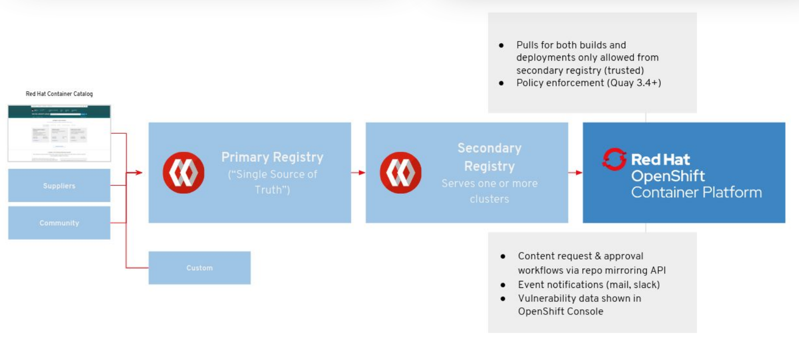
IMAGES

- ❑ Use container-specific technology for vulnerability, compliance and secrets management
- ❑ Integrate checks and monitoring across the image lifecycle
- ❑ Automated, policy-driven enforcement
- ❑ Mitigate risks with trusted images

Image Countermeasures – Trusted Images




operatorhub.io
Red Hat Container Catalog
Suppliers
Community
Custom
Geo-Replication
single globally-distributed Red Hat Quay to serve container images from localized storage
Data Center 1
Data Center 2
DC 3
DC 5
Repository Mirroring
to mirror external content into Quay explicit whitelisting / content ingress supports disconnected clusters *
Repository Mirroring
to mirror a specific subset of content to specific data centers, clusters, regions
Red Hat


Red Hat Container Catalog
Suppliers
Community
Custom
Primary Registry
("Single Source of Truth")
Secondary Registry
Serves one or more clusters
Red Hat OpenShift Container Platform

- Pulls for both builds and deployments only allowed from secondary registry (trusted)
- Policy enforcement (Quay 3.4+)

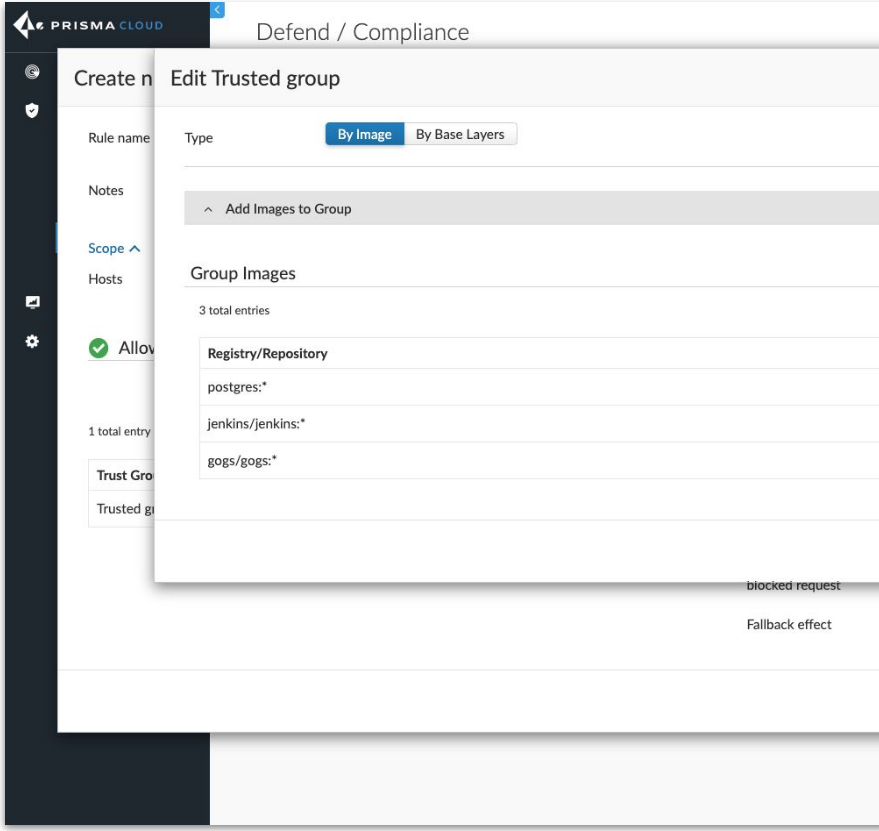
- Content request & approval workflows via repo mirroring API
- Event notifications (mail, slack)
- Vulnerability data shown in OpenShift Console

- Red Hat Container Health Index as a security impact metric for all Red Hat images
- Quay manages content ingress point for explicitly whitelisted (trusted) content
- Content federation and promotion to different lifecycle environments
- Quay controls access to content via RBAC, content promotions, org's and teams
- Read-only ("locked") repository mode
- Registry whitelisting on RHEL CoreOS

Image Countermeasures

Untrusted Images

- Capability to centrally control exactly what images and registries are trusted in their environment
- Discrete identification of each image by cryptographic signature
- Enforcement that all hosts only run images from these approved lists
- Validation of image signatures before image execution to ensure images are from trusted sources and have not been tampered with
- Ongoing monitoring and maintenance of these repositories to ensure images within them are maintained and updated



Edit Trusted group

Type: By Image | By Base Layers

Group Images

3 total entries

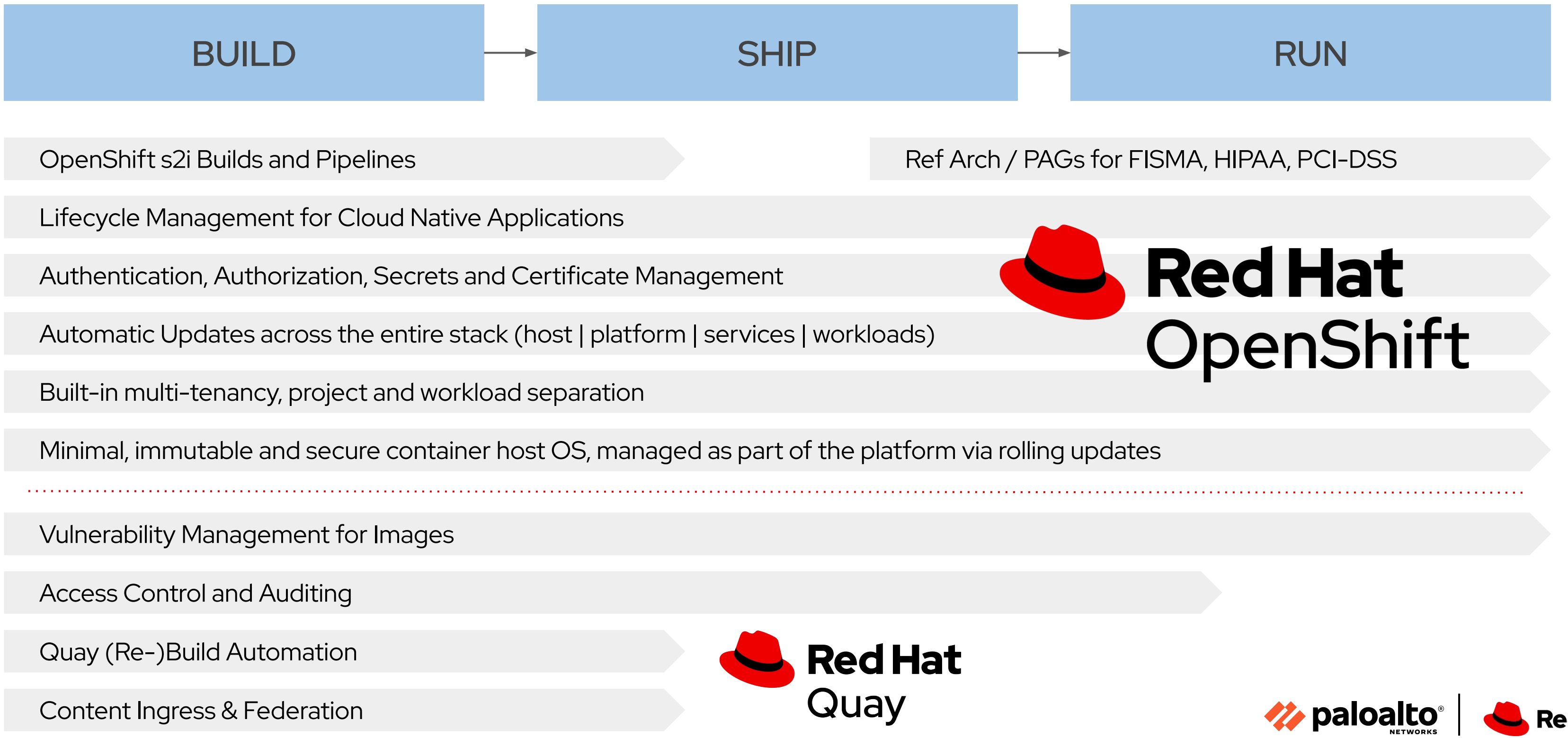
Registry/Repository
postgres:*
jenkins/jenkins:*
gogs/gogs:*

4.1 Image Countermeasures

IMAGES

- ❏ Use container-specific technology for vulnerability, compliance and secrets management
- ❏ Integrate checks and monitoring across the image lifecycle
- ❏ Automated, policy-driven enforcement
- ❏ Mitigate risks with trusted images

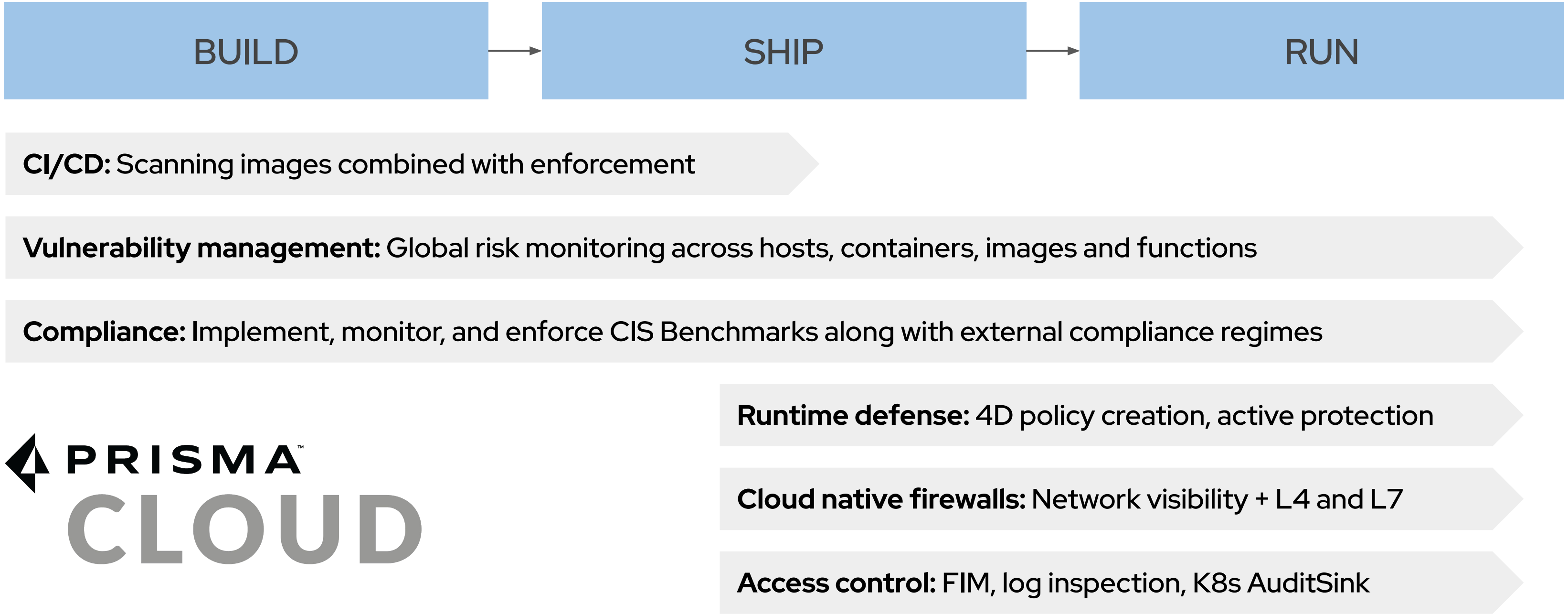
Security Across the DevSecOps Lifecycle



- OpenShift s2i Builds and Pipelines
- Ref Arch / PAGs for FISMA, HIPAA, PCI-DSS
- Lifecycle Management for Cloud Native Applications
- Authentication, Authorization, Secrets and Certificate Management
- Automatic Updates across the entire stack (host | platform | services | workloads)
- Built-in multi-tenancy, project and workload separation
- Minimal, immutable and secure container host OS, managed as part of the platform via rolling updates

- Vulnerability Management for Images
- Access Control and Auditing
- Quay (Re-)Build Automation
- Content Ingress & Federation

Security Across the DevSecOps Lifecycle



BUILD → SHIP → RUN

CI/CD: Scanning images combined with enforcement

Vulnerability management: Global risk monitoring across hosts, containers, images and functions

Compliance: Implement, monitor, and enforce CIS Benchmarks along with external compliance regimes

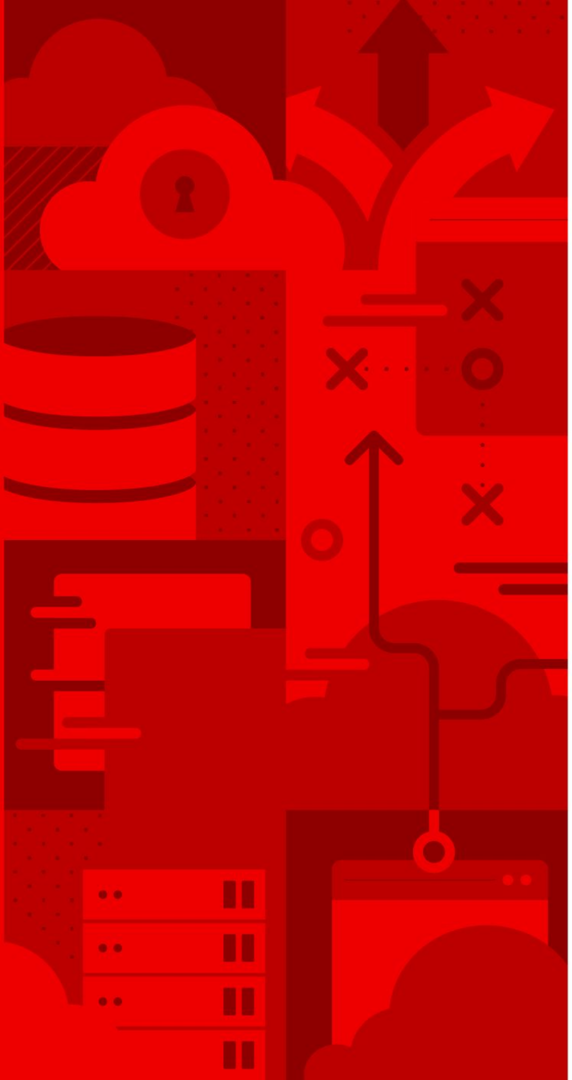
Runtime defense: 4D policy creation, active protection

Cloud native firewalls: Network visibility + L4 and L7

Access control: FIM, log inspection, K8s AuditSink

PRISMA CLOUD

Optional section marker or title



Thank you

Send us your questions throughout each day to infrastructure@redhat.com

- linkedin.com/company/red-hat
- youtube.com/user/RedHatVideos
- facebook.com/redhatinc
- twitter.com/RedHat

- linkedin.com/company/palo-alto-networks
- youtube.com/user/PaloAltoNetworks
- facebook.com/PaloAltoNetworks
- twitter.com/prisma_cloud

Red Hat

paloalto® NETWORKS