Securing containers and Kubernetes in hybrid cloud

Kirsten Newcomer  
Director, Cloud Security Strategy

Wei Lien Dang  
Senior Director, Product Management
Innovation at speed. Flexibility to adapt. New customer experiences and lines of business.

That’s what hybrid cloud can deliver.
Containers and Kubernetes enable hybrid cloud

**Containers** make it easier to deliver applications faster
- Packaging dependencies with application
- Simpler, lighter, greater utilization than VMs
- Portable across environments
- Shorter development cycle
- Quickly deploy to any environment
- And much more

**Kubernetes** makes it easier to manage containerized applications
- Scaling
- Resiliency
- Networking and Routing
- Persistent data storage
- Platform HA
- Application HA
Considerations for Securing Containers and Kubernetes

NIST 800-190

"Use container-specific host OSs instead of general-purpose ones to reduce attack surfaces."

CNCF Kube Security Audit

"...the underlying hosts, components, and environment of a Kubernetes cluster must be configured and managed. This management has a direct impact on the capabilities of the cluster..."

Gartner Market Guide for Cloud Workload Protection

"The best way to secure these rapidly changing and short-lived workloads is to start their protection proactively in the development phase ...”

"Replace antivirus (AV)-centric strategies with a “zero-trust execution”/default deny/application control approach to workload protection where possible...."
Containers and Kubernetes require DevSecOps

Control Application Security

Protect The Platform

Detect & Respond At Runtime

Dev

Ops

MANAGE

RUN

DEPLOY

ADAPT

PACKAGE

BUILD

DESIGN

ADAPT

DEPLOY
Improve Security
THROUGH THE ADOPTION OF CONTAINERS

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

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

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

DEVELOPER
SECURITY
OPERATIONS

DevNation Federal - The Journey to DevSecOps
Red Hat OpenShift Platform Plus

Enabling hybrid and multi-cloud deployments

Multi-cluster layer
- Multicluster Management
  - Observability
  - Discovery
  - Policy
  - Compliance
  - Configuration
  - Workloads
- Cluster Security
  - Declarative security
  - Container vulnerability management
  - Network segmentation
  - Threat detection & response
- Global Registry
  - Image management
  - Security scanning
  - Geo-replication Mirroring
  - Image builds

Router layer
- OpenShift Routing

Node layer
- Pod
- OpenShift Application Nodes
- Node

Cluster 1
- Node
- Node
- Node

Cluster n
- Pod
- OpenShift Application Nodes
- Node

East/West
Red Hat Advanced Cluster Security for Kubernetes

The first Kubernetes-native security platform

Red Hat Advanced Cluster Security for Kubernetes

Build
Secure supply chain

Deploy
Secure infrastructure

Run
Secure workloads

Policy engine

API

Run anywhere
- Public cloud
- Private cloud
- Hybrid/Multi-cloud

Image scanning
- anchore
- clair
- QUAY
- tenable
- StackRox

Registries
- Amazon ECR
- Nexus
- docker
- Ansible
- Docker Registry

CI/CD tools
- Jenkins
- GitHub
- GitLab
- CircleCI
- Travis CI

DevOps notification
- Jira Software
- Slack
- Microsoft Teams
- PagerDuty

SIEM
- splunk
- sumo logic
- AWS Security Hub
Advanced Cluster Management

**Application-centric Management**
Deploy, upgrade, and manage applications with consistency across multiple clouds

**Policy-Based Governance**
Enforce configuration policies and ensure compliance across clusters, applications and infrastructures

**Cluster Lifecycle Management**
Centrally, create, update, delete clusters across the enterprise
Layers of container & Kubernetes security

- **Control**
  - Application Lifecycle and Locality
  - Vulnerability analysis
  - App config analysis
  - APIs for CI/CD integrations
  - Trusted content
  - Container registry
  - Build management
  - CI/CD pipeline

- **Protect**
  - Fleet Configuration Management
  - Policy admission controller
  - Compliance assessments
  - Risk profiling
  - Kubernetes platform lifecycle
  - Identity and access mgmt
  - Protect platform data
  - Deployment policies

- **Detect & Respond**
  - Fleet Observability & Alerts
  - Runtime behavioral analysis
  - Auto-suggest network policies
  - Threat detection / incident response
  - Container isolation
  - Network isolation
  - Application access and data
  - Observability

---

DevSecOps

BUILD

DEPLOY

RUN
Best practices

- Use trusted sources for external content
- Use a private registry with integrated vulnerability scanning to manage images
- Automate your container pipeline with Jenkins or Tekton
- Integrate security into the pipeline
  - Image vulnerability analysis
  - App configuration analysis
- Automate multi-cluster application deployment / locality
Deploy: Securing Kubernetes

- Configuration and lifecycle management
  - Container optimized OS for controlled immutability
  - Policy-based fleet configuration management
- Identity and Access Management
- Protect platform data at rest and in motion
- Automated compliance management
- Automated risk assessment
- Policy based deployment
  - Prevent admission of privileged pods
  - Prevent admission of pods with critical vulnerabilities
Run: Securing the container runtime

- Container isolation & resource management
- Application and network isolation
  - Integrated RBAC for fine grained control
  - Network policies for SDN microsegmentation
  - Auto-suggest network policies
  - Service Mesh encrypts pod-to-pod traffic
- Securing application access
  - Multiple options for managing ingress and egress
  - RH SSO for user management / 3Scale API Gateway
- Observability
  - Application monitoring & logging
  - Network policy and service mesh visualization
- Threat detection and response
  - Alert or kill pods based on anomalous behavior
  - Detect privilege escalation, cryptomining
Future of Security: Zero Trust

**Control**
- KubeLinter with GitHub Actions
- Rootless Builds
- Encrypted Containers
- Keyless image signing

**Protect**
- Enabling Hard Multitenancy
- Attestation
- Pod Security, OPA Gatekeeper
- DISA STIG for OCP 4

**Detect & Respond**
- Kata containers
- Automate Service Mesh Policies
- Active Recommendations
- Kubernetes User Namespaces

**What's Next?**

BUILD

DEPLOY

RUN

DevSecOps
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.