SECURING CONTAINERS

OpenShift Security Workshop

Alfred Bach
Principal Solution Architect
Red Hat EMEA

Security must be continuous and holistic

FedRAMP

ANSSI

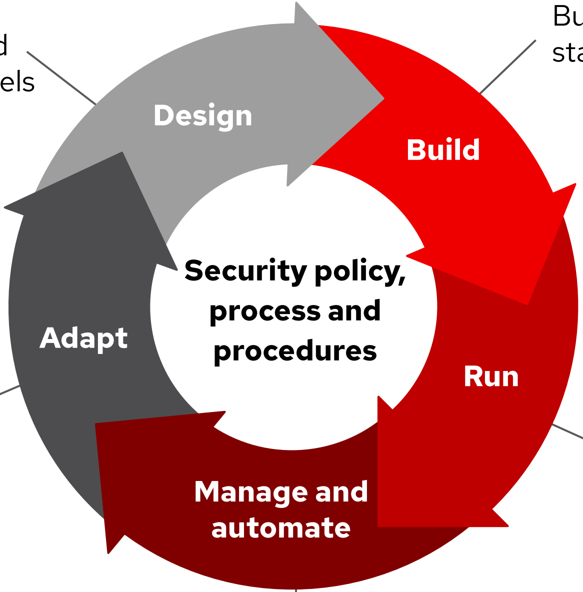
NIST National Institute of Standards and Technology U.S. Department of Commerce

CIS Center for Internet Security

National Cyber Security Centre

PCI Security Standards Council

HIPAA Health Insurance Portability & Accountability Act



Identify security requirements and governance models

Built-in from the start; not bolted-on

Deploy to trusted platforms with enhanced security capabilities

Automate systems for security and compliance

Revise, update, remediate as the landscape changes

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...."

Sources

NIST Special Publication 800-190 Application Container Security Guide

CNCF Cloud Native Security Whitepaper

Kubernetes Security Whitepaper, Trail of Bits, May 31, 2019

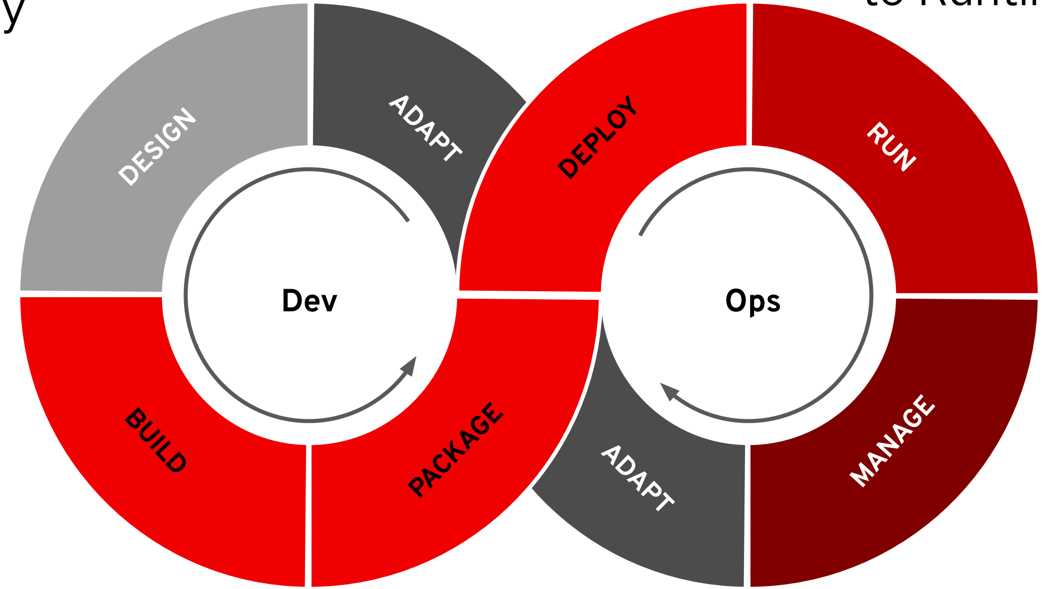
Gartner: Market Guide for Cloud Workload Protection Platforms, ID G00356240, April 8, 2019

Containers and Kubernetes need DevSecOps

Control Application Security

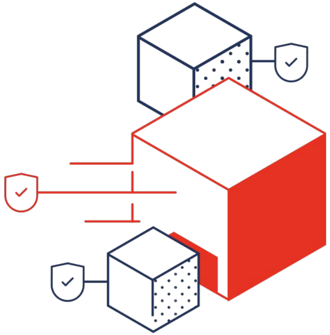
Protect the Platform

Detect & Respond to Runtime Threats



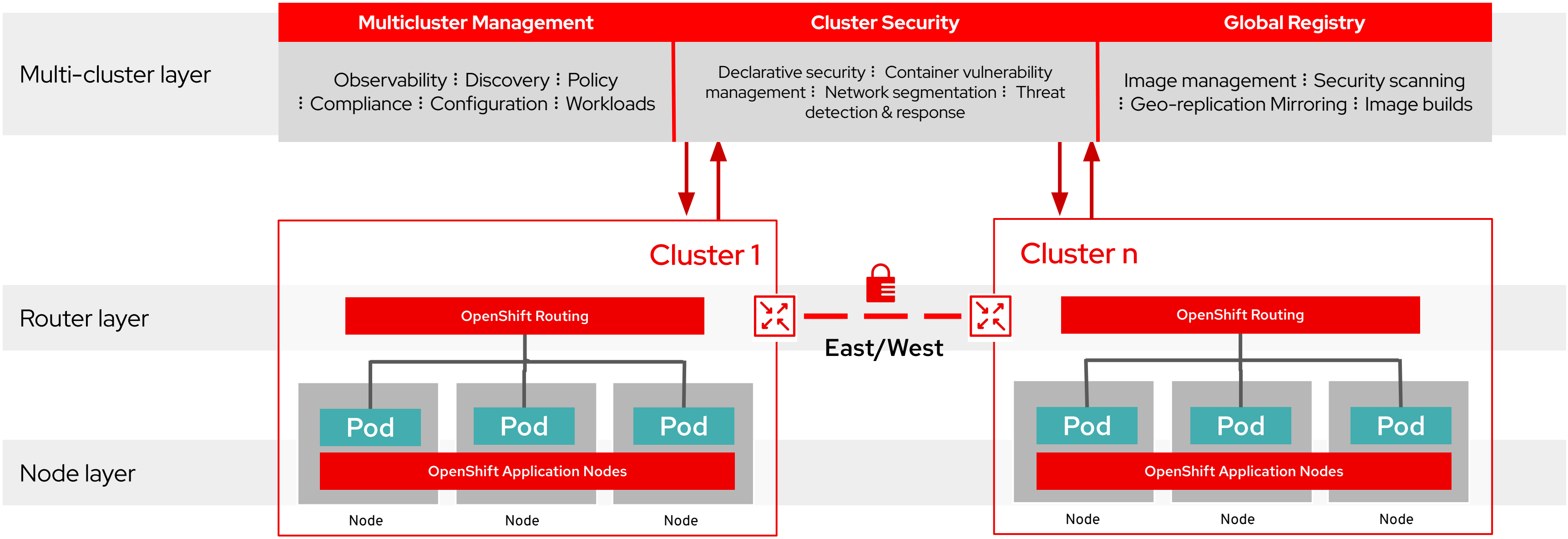
The OpenShift platform vision:

A single hybrid-cloud platform for enterprises to build, deploy, run and manage intelligent applications securely at scale.



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

Node layer

Cluster 1

OpenShift Routing

Pod

Pod

Pod

OpenShift Application Nodes

Node

Node

Node

East/West

Cluster n

OpenShift Routing

Pod

Pod

Pod

OpenShift Application Nodes

Node

Node

Node

Red Hat contributions to Kubernetes

RBAC Authorization | Stateful Sets | Init Containers | Rolling Update Status | Pod Security Policy Limits | Memory based Pod Eviction | Quota Controlled Services | 1,000+ Nodes | Dynamic PV Provisioning | Multiple Schedulers | SECCOMP | Audit | Job Scheduler | Access Review API | Whitelisting Sysctls | Secure Cluster Policy | Evict Pods Disk IO | Storage Classes | Azure Data Disk | etcdv3 | RBAC API | Auth to kubelet API | Pod-level cGroups QoS | Kublet Eviction Model | RBAC | Storage Class | CustomResourceDefinitions | API Aggregation | Encrypted secrets in etcd | Limit Node Access | HPA Status Conditions | Network Policy | CRI Validation Test Suite | Local Persistent Storage | Audit Logging |

Build: Control application security

Shift Security left

Best practices

Red Hat UBI

- Use trusted sources for external content such as base images

Quay

- Use a trusted private registry to manage supply chain risk

OCP Pipelines

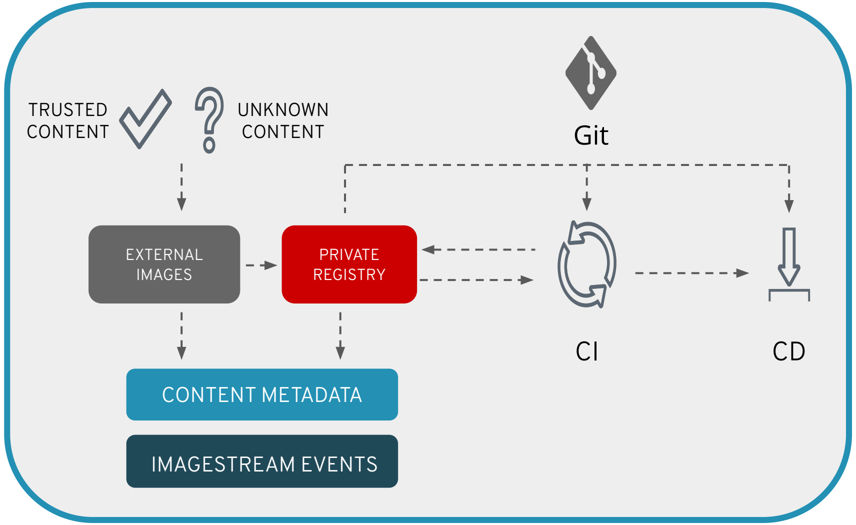
- Automate your CI/CD pipeline to enable rapid updates

Quay scanner (registry)
Code Ready (IDE)
ACS scanner (CI)
KubeLinter (CI)

- Integrate security tools / gates in your pipeline to identify
  - Known vulnerabilities
  - Application misconfigurations

ACM

- Use policy-based deployment tools to manage application placement (e.g. locality)



TRUSTED CONTENT

UNKNOWN CONTENT

Git

EXTERNAL IMAGES

PRIVATE REGISTRY

CI

CD

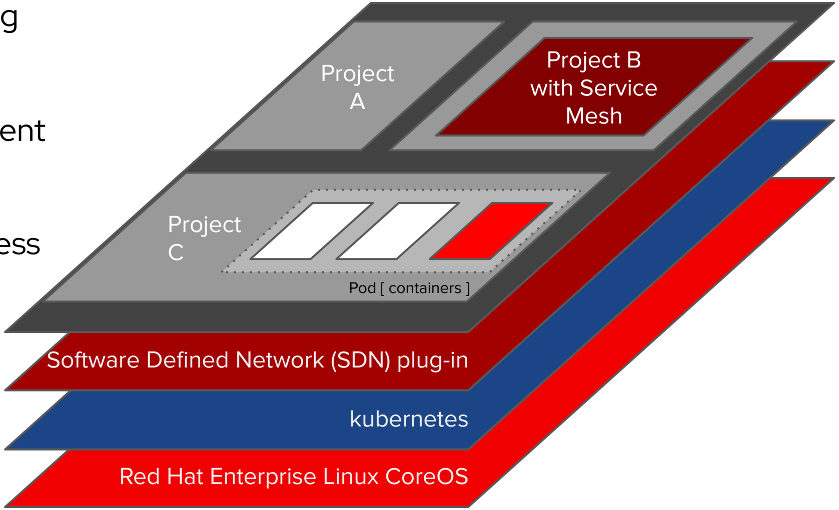
CONTENT METADATA

IMAGESTREAM EVENTS

Deploy: Protect the application platform

Best practices

RHEL CoreOS	▶ Reduce attack surface with a container optimized operating system
OCP Operators ACM	▶ Use automated and policy-driven configuration management across your fleet
OCP RBAC ACS to monitor ACM to enforce	▶ Implement least privilege with fine-grained role based access control (RBAC)
OCP CAs Service mesh OCP IPSec RHCOS NBDE Encrypt etcd	▶ Encrypt platform data in transit and at rest
OCP Compliance Operator ACS ACM	▶ Use automated compliance, risk assessment and remediation solutions
OCP Security Context Constraints ACS	▶ Reduce deployment risk with admission control policies that ▪ Minimize admission of privileged pods, pods with host capabilities ▪ Prevent admission of pods with critical vulnerabilities



Project A
Project B with Service Mesh
Project C
Pod [containers]
Software Defined Network (SDN) plug-in
kubernetes
Red Hat Enterprise Linux CoreOS

Run: Securing the container runtime

Best practices

OCP
ACS

- Minimize the impact of an attack by isolating running applications with
  - SELinux & Security Context Constraints
  - Kubernetes namespaces (Projects), RBAC
  - Network Policies for microsegmentation

OCP
ACM

- Use resource quotas to prevent resource exhaustion

OCP

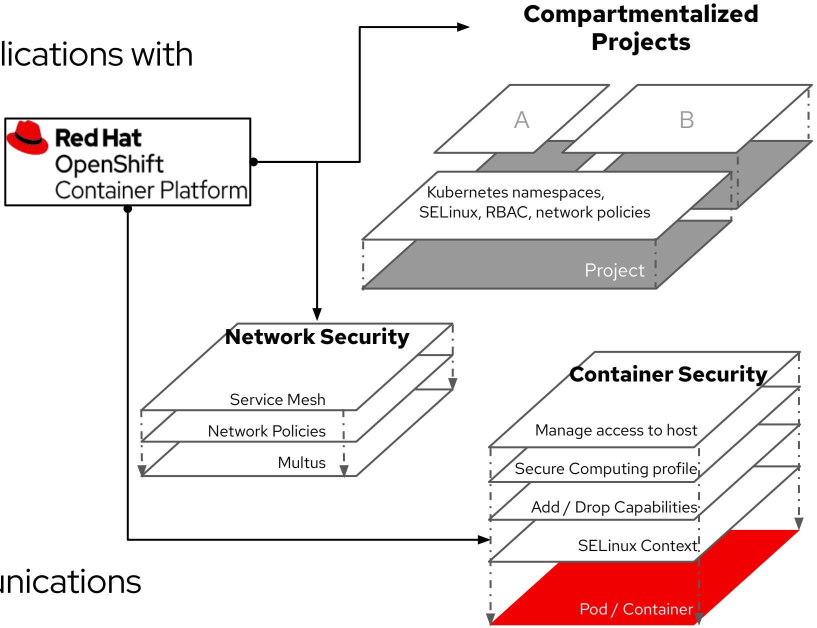
- Manage application access and protect application data
  - Red Hat Single Sign On for user management
  - Secure routes / ingress, 3Scale API Gateway
  - Service mesh to encrypt pod-to-pod traffic
  - Egress IPs / firewall

OCP
ACS
ACM

- Monitor application metrics, logging and network communications

ACS

- Automate threat detection and response
  - Alert or kill pods based on anomalous behavior
  - Detect privilege escalation and risky processes such as cryptomining



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

Multicluster Management

Infrastructure Management

Application Management

Event Management

Existing Tools & Processes

Configuration & Compliance Management

Red Hat Advanced Cluster Security: Use Cases

Security across the entire application lifecycle

Vulnerability Management

Protect yourself against known vulnerabilities in images and running containers

Security Configuration Management

Ensure your deployments are configured according to security best practices

Risk Profiling

Gain context to prioritize security issues throughout OpenShift and Kubernetes clusters

Network Segmentation

Apply and manage network isolation and access controls for each application

Compliance

Meet contractual and regulatory requirements and easily audit against them

Detection and Response

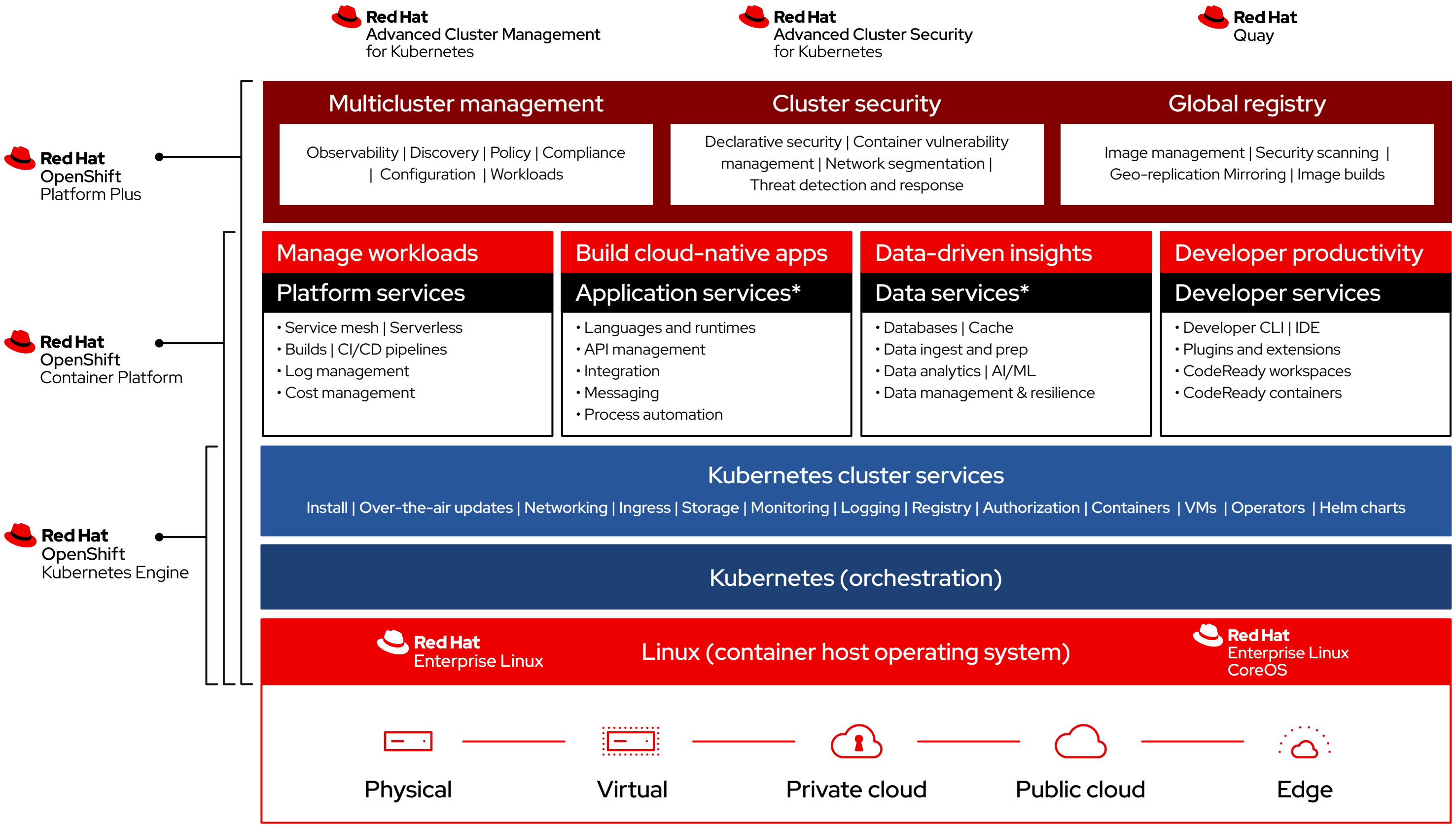
Carry out incident response to address active threats in your environment

OpenShift delivers continuous security

	Control	Protect	Detect & Respond
ACM	Application Lifecycle and Locality	Fleet Management	Fleet Observability & Alerts
ACS	Vulnerability analysis	Policy admission controller	Runtime behavioral analysis
	App config analysis	Compliance assessments	Auto-suggest network policies
	APIs for CI/CD integrations	Risk profiling	Threat detection / incident response
OCP	Trusted content	Kubernetes platform lifecycle	Container isolation
	Container registry	Identity and access management	Network isolation
	Build management	Platform data	Application access and data
	CI/CD pipeline	Deployment policies	Observability
	BUILD	DEPLOY	RUN

DevSecOps

OpenShift Platform Plus



Red Hat Advanced Cluster Management for Kubernetes

Red Hat Advanced Cluster Security for Kubernetes

Red Hat Quay

Red Hat OpenShift Platform Plus

Red Hat OpenShift Container Platform

Red Hat OpenShift Kubernetes Engine

Multicluster management

Observability | Discovery | Policy | Compliance | Configuration | Workloads

Cluster security

Declarative security | Container vulnerability management | Network segmentation | Threat detection and response

Global registry

Image management | Security scanning | Geo-replication Mirroring | Image builds

Manage workloads

Platform services

- Service mesh | Serverless
- Builds | CI/CD pipelines
- Log management
- Cost management

Build cloud-native apps

Application services*

- Languages and runtimes
- API management
- Integration
- Messaging
- Process automation

Data-driven insights

Data services*

- Databases | Cache
- Data ingest and prep
- Data analytics | AI/ML
- Data management & resilience

Developer productivity

Developer services

- Developer CLI | IDE
- Plugins and extensions
- CodeReady workspaces
- CodeReady containers

Kubernetes cluster services

Install | Over-the-air updates | Networking | Ingress | Storage | Monitoring | Logging | Registry | Authorization | Containers | VMs | Operators | Helm charts

Kubernetes (orchestration)

Red Hat Enterprise Linux

Linux (container host operating system)

Red Hat Enterprise Linux CoreOS

Physical — Virtual — Private cloud — Public cloud — Edge

Red Hat

* Red Hat OpenShift® includes supported runtimes for popular languages/frameworks/databases. Additional capabilities listed are from the Red Hat Application and Data Services portfolio.

Security Partners by Use Case

Partners extend and enhance Red Hat functionality

Application Analysis

SAST, SCA, IAST, DAST, Image Risk

paloalto NETWORKS · SYNOPSYS · aqua · anchore · NeuVector · snyk · sysdig · Red Hat Advanced Cluster Security

Identity & Access Mgmt

Auth, RBAC, Secrets Vault, Provenance, HSM

IBM IAM · CYBERARK · THALES

Compliance

Regulatory Compliance, PCI-DSS, GDPR

aqua · SYNOPSYS · TIGERA · anchore · Red Hat Advanced Cluster Security · NeuVector · sysdig · paloalto NETWORKS

Network Controls

CNI Plugins, Policies, Traffic Controls, Service Mesh

aqua · TIGERA · Red Hat Advanced Cluster Security · sysdig · paloalto NETWORKS

Data Controls

Data Protection and Encryption

IBM Guardium · Zettaset · THALES

Runtime Analysis & Protection

RASP, Production Analysis

aqua · sysdig · paloalto NETWORKS · anchore · NeuVector · Red Hat Advanced Cluster Security

Audit & Monitoring

Logging, Visibility, Forensics

sysdig · NeuVector · Red Hat Advanced Cluster Security · aqua · paloalto NETWORKS

Remediation

SOAR, Automatic resolution

snyk · paloalto NETWORKS · IBM Resilient

Red Hat Platform Security

Secure Host, Container Platform, Namespace Isolation, k8s & Container Hardening

Roadmap*: Identity, Integrity, Observability

Control

Trusted Application Identity

Improve supply chain security with solutions to verify identity of users, images, deployments, config data

Keyless signatures
Tekton CD chains
Encrypted containers
Rootless builds

BUILD

Protect

Platform Integrity

Deliver platform integrity with attestation and verification as a service; Mitigate risk by expanding isolation capabilities

Keylime / IMA
Kube support for user namespaces
Externally managed control planes
Trusted Execution Environment (Intel SGX support)

DEPLOY

Detect & Respond

Observe, Analyze, Remediate

Active recommendations to automate remediation based on deep data collection and analysis

Security Profile operator
Deep network observability
Service Mesh recommendations

RUN

DevSecOps

*Subject to change without notice

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.

in linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

f facebook.com/redhatinc

twitter.com/RedHat

Red Hat