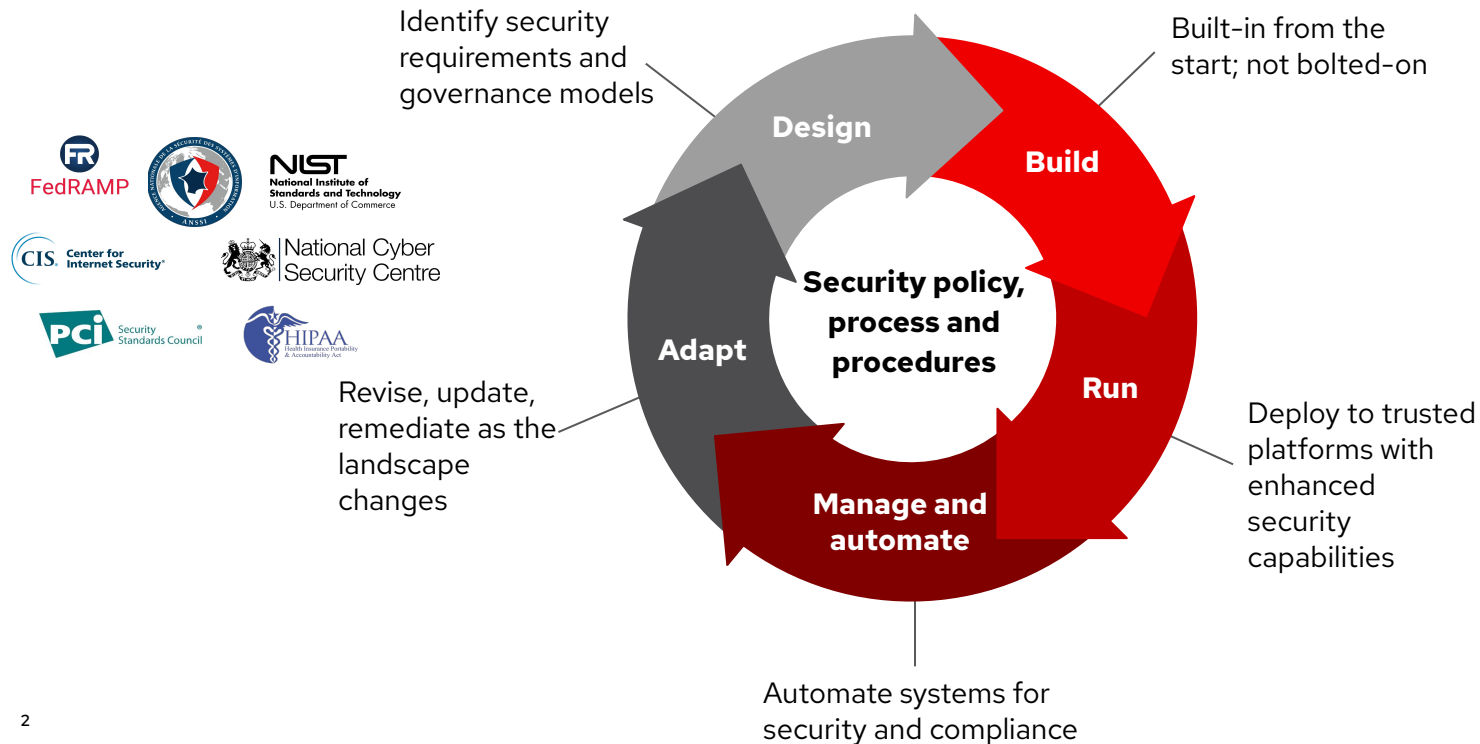


SECURING CONTAINERS

OpenShift Security Workshop

Alfred Bach
Principal Solution Architect
Red Hat EMEA

Security must be continuous and holistic



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

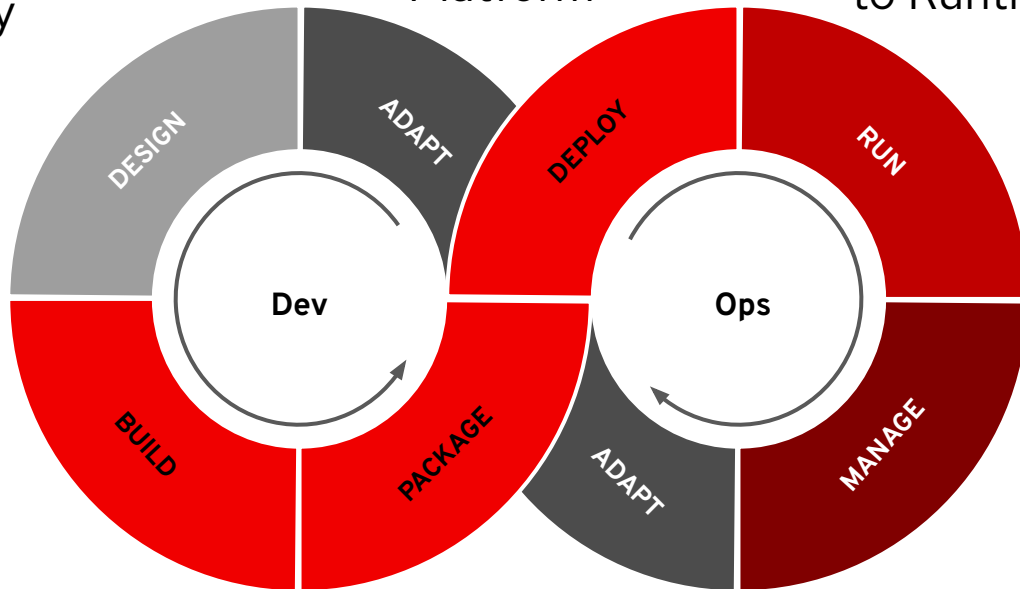


Containers and Kubernetes need DevSecOps


Control
Application
Security

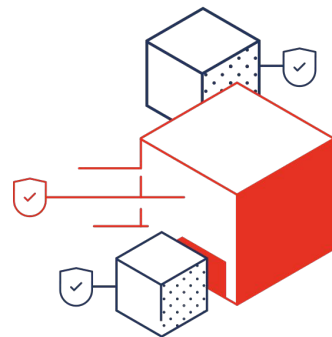

Protect the
Platform


Detect & Respond
to Runtime Threats



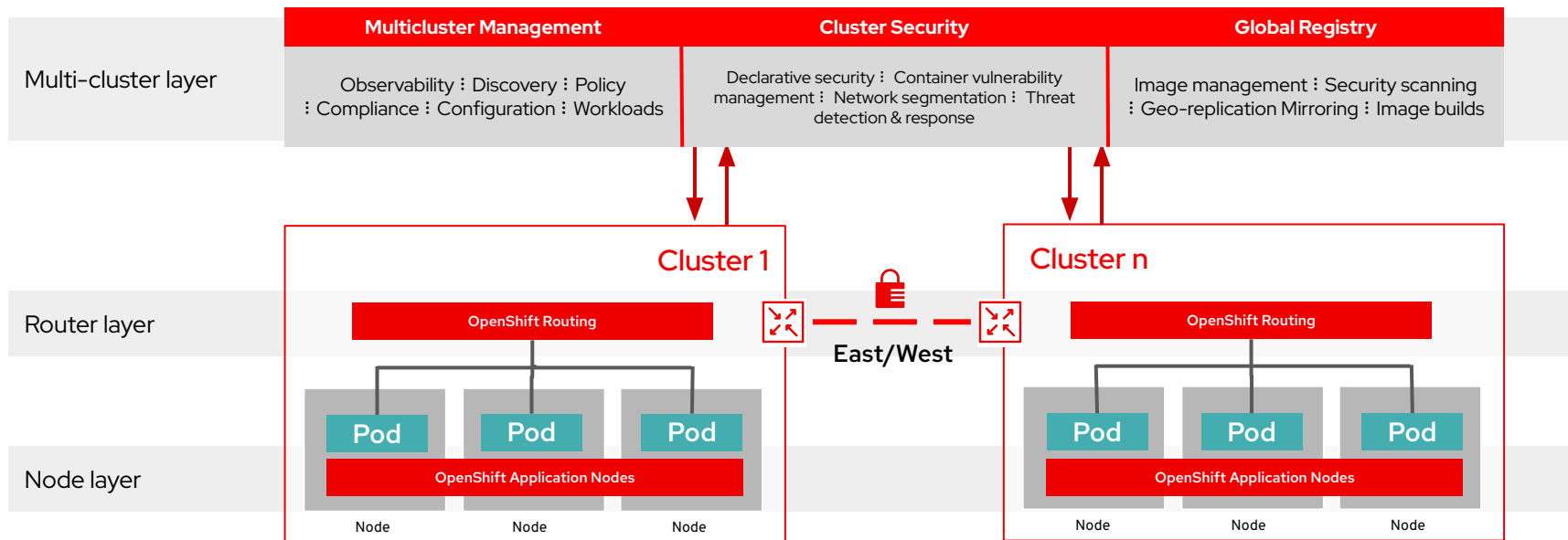
The OpenShift platform vision:

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



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 |



OPENSIFT

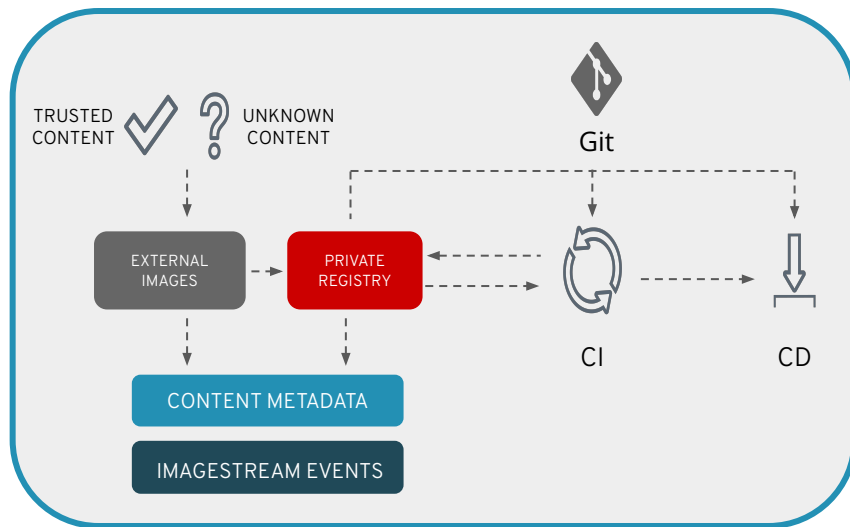


Build: Control application security

Shift Security left

Best practices

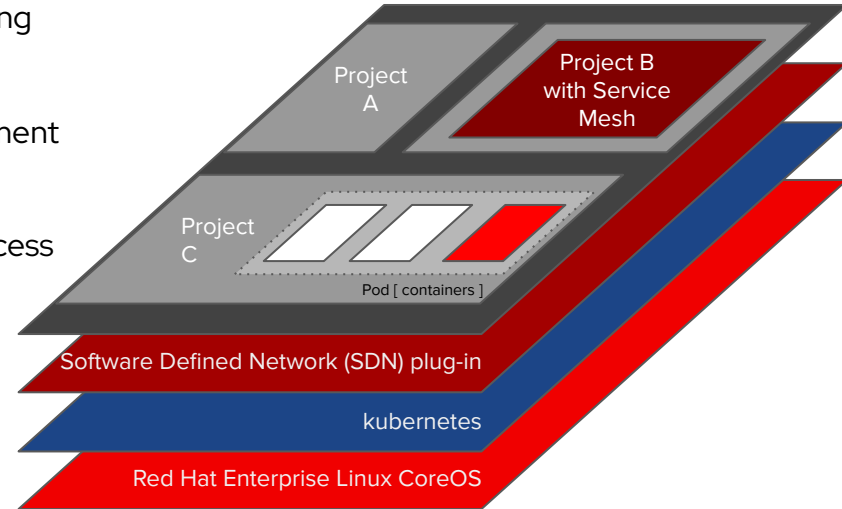
- Red Hat UBI
 - ▶ Use trusted sources for external content such as base images
- Quay
 - ▶ Use a trusted private registry to manage supply chain risk
- OCP Pipelines
 - ▶ Automate your CI/CD pipeline to enable rapid updates
- Quay scanner (registry)
Code Ready (IDE)
ACS scanner (CI)
KubeLint (CI)
 - ▶ 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)



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



Run: Securing the container runtime

Best practices

- ▶ Minimize the impact of an attack by isolating running applications with

- SELinux & Security Context Constraints
- Kubernetes namespaces (Projects), RBAC
- Network Policies for microsegmentation

- ▶ Use resource quotas to prevent resource exhaustion

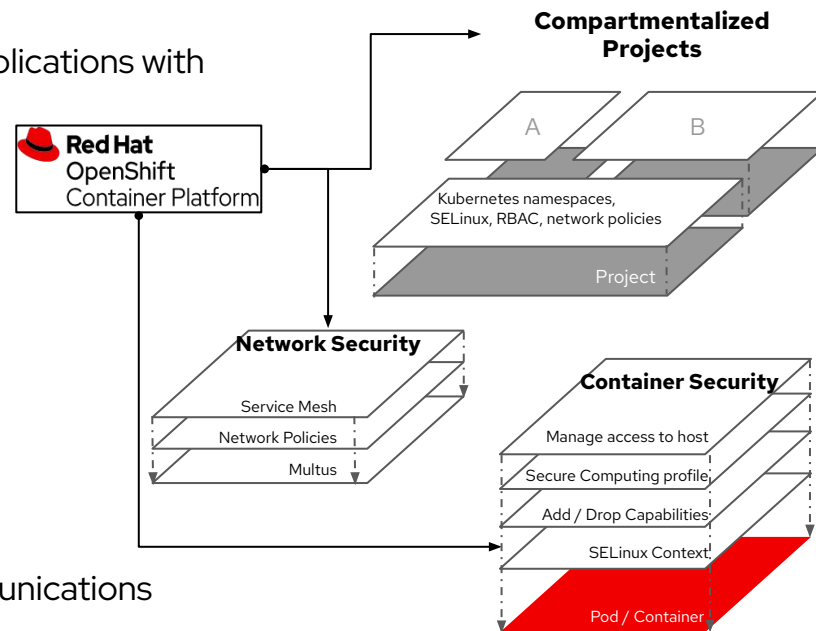
- ▶ Manage application access and protect application data

- 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

- ▶ Monitor application metrics, logging and network communications

- ▶ 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

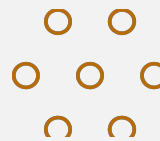
Deploy, upgrade, and manage applications with consistency across multiple clouds

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



Multicloud
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

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

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

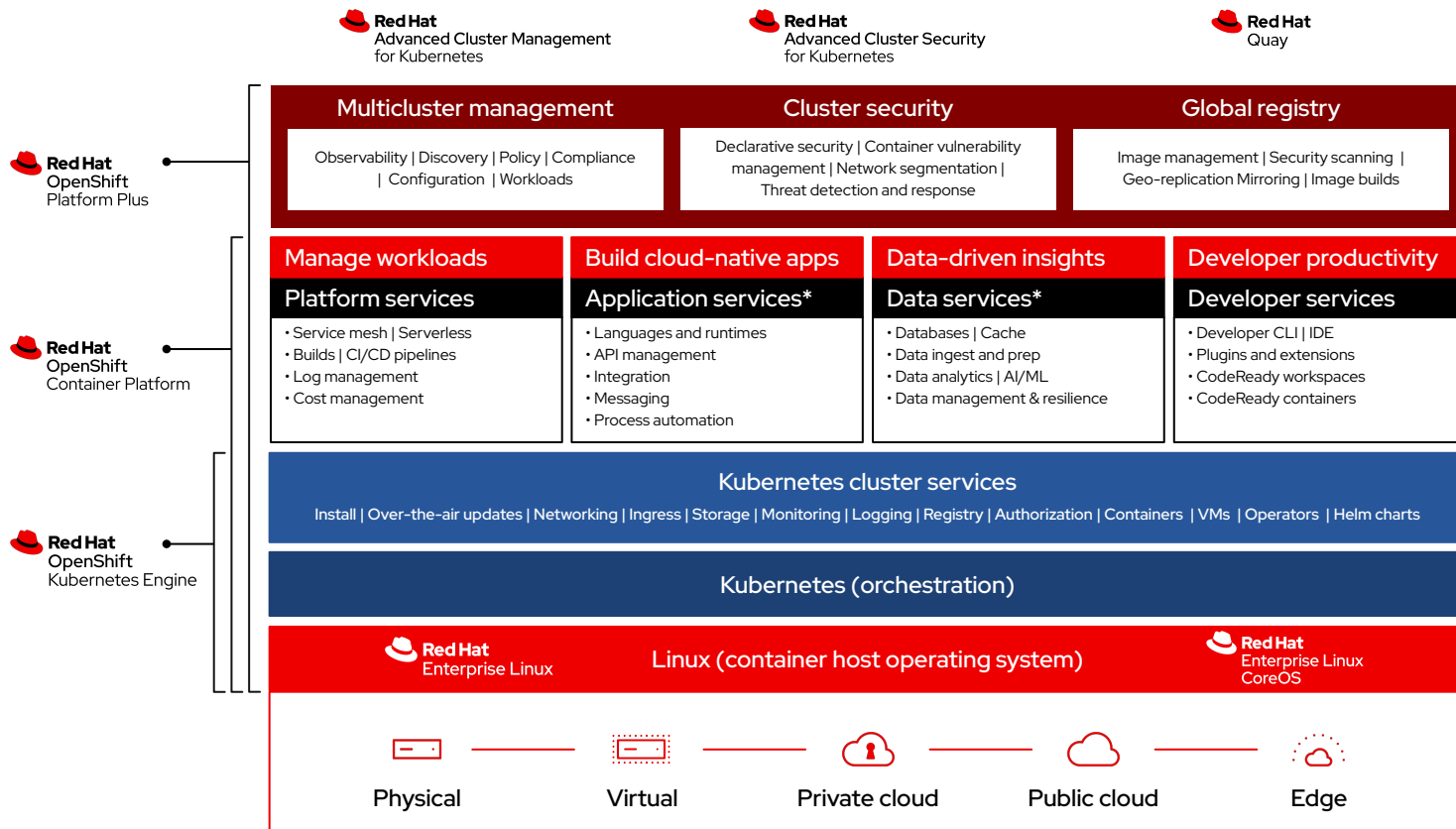
BUILD

DEPLOY

RUN

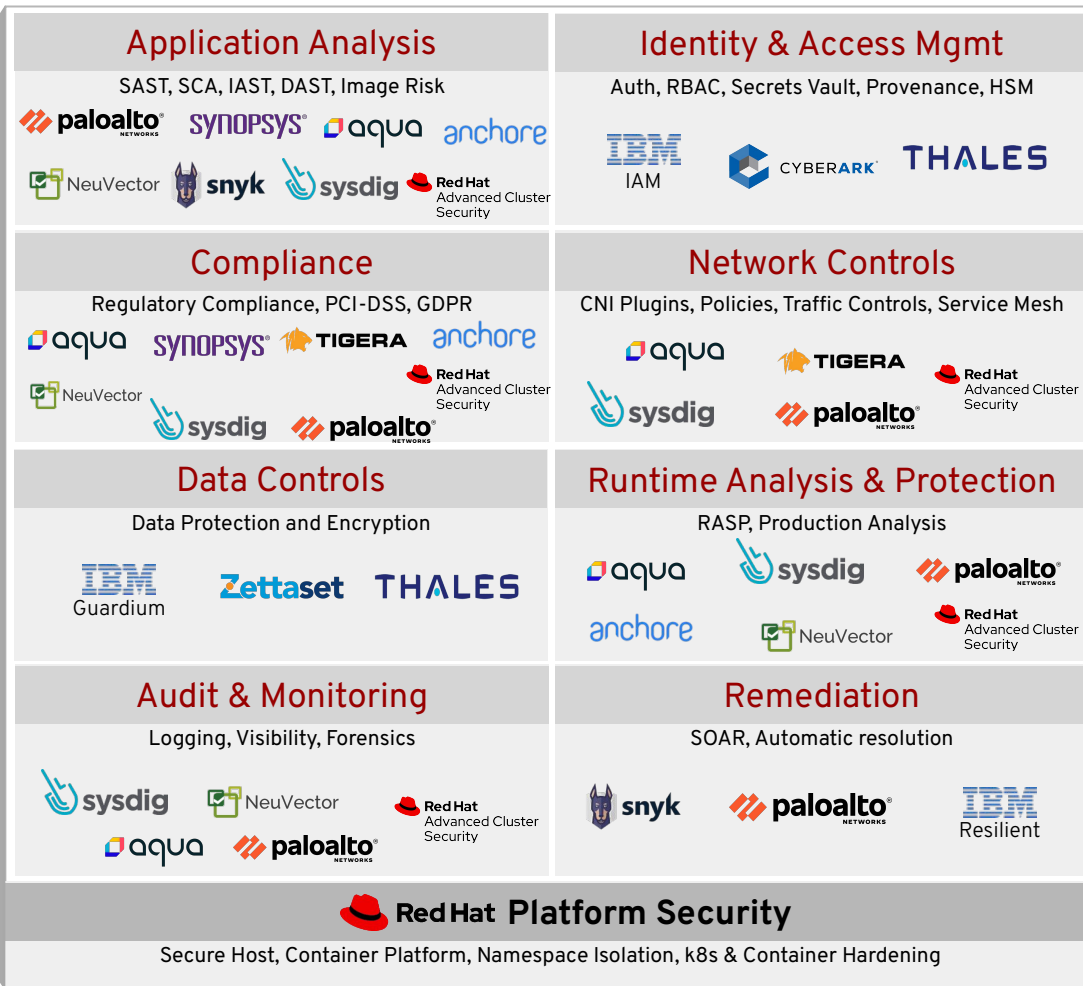
DevSecOps

OpenShift Platform Plus



Security Partners by Use Case

Partners extend and enhance Red Hat functionality



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

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



youtube.com/user/RedHatVideos



facebook.com/redhatinc



twitter.com/RedHat