Red Hat
Advanced Cluster Security
for Kubernetes

StackRox | Red Hat ACS

Alfred Bach

Principal Solution Architect – Cloud, Security & DC– Infrastructure

Partner Enablement Team EMEA

abach@redhat.com

Red Hat

Kubernetes is the standard for application innovation...

▸ Microservices architecture

▸ Declarative definition

▸ Immutable infrastructure

...and Kubernetes-native security is increasingly critical

▸ Secure supply chain

▸ Secure infrastructure

▸ Secure workloads
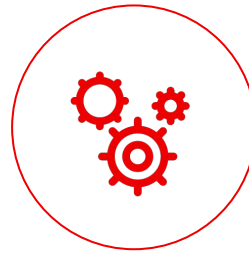
DevOps	DevSecOps	Security

Red Hat

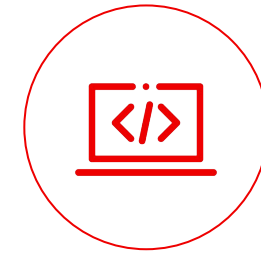# Benefits of a Kubernetes-native approach to security

Lower operational cost

DevOps and Security teams can use a common language and source of truth

Reduce operational risk

Ensure alignment between security and infrastructure to reduce application downtime

Increase developer productivity

Leverage Kubernetes to seamlessly provide guardrails supporting developer velocity

Red Hat

Red Hat Advanced Cluster Security for Kubernetes

A cloud workload protection platform and cloud security posture management to enable you to "shift left"

Shift left	Cloud security posture management (CSPM)	Cloud workload protection (CWPP)
Secure supply chain	Secure infrastructure	Secure workloads
Extend scanning and compliance into development (DevSecOps)	Leverage built-in Kubernetes CSPM to identify and remediate risky configurations	Maintain and enforce a "zero-trust execution" approach to workload protection

Red Hat

Red Hat OpenShift provides a secure foundation

Detect

Trusted content
Container registry
Build management
CI/CD pipeline

Protect

Kubernetes platform lifecycle
Identity and access management
Platform data
Deployment policies

Respond

Container isolation
Network isolation
Application access and data
Observability

Build — **Deploy** — **Run**

DevSecOps

A layered approach to container and Kubernetes security

Red Hat

RHACS delivers security depth to entire application lifecycle

Detect

Trusted content
Container registry
Build management
CI/CD pipeline

Vulnerability analysis
App config analysis
APIs for CI/CD integrations

Protect

Kubernetes platform lifecycle
Identity and access management
Platform data
Deployment policies

Image assurance and policy admission controller
Compliance assessments
Risk profiling

Respond

Container isolation
Network isolation
Application access and data
Observability

Runtime behavioral analysis
Auto-suggest network policies
Threat detection / incident response

**Build** — **Deploy** — **Run**

DevSecOps

Red Hat

RHACS

Securing Kubernetes Deployments

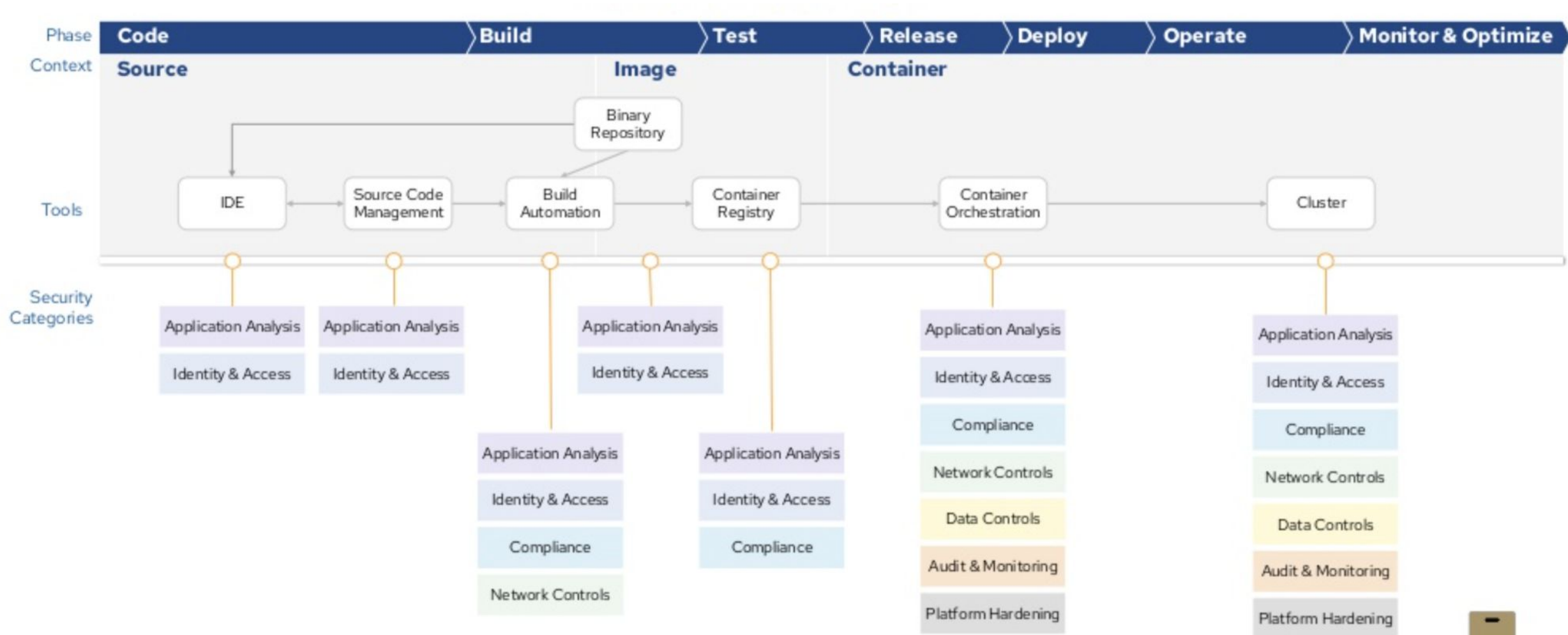**It's all about the Application in the container**
- plus a Registry Scanner.

It's not:

- End 2 End Monitoring -> Dynatrace
- Infrastructure Monitoring - RHACM
- Infrastructure Compliance Monitoring - RHACM
- Access Control / Audit to and in OpenShift IBM QRadar or CyberARC
- SIEM Solution -> Splunk
- Certificate Management - Cert Manager
- API Management - 3scale
- Application Performance Management
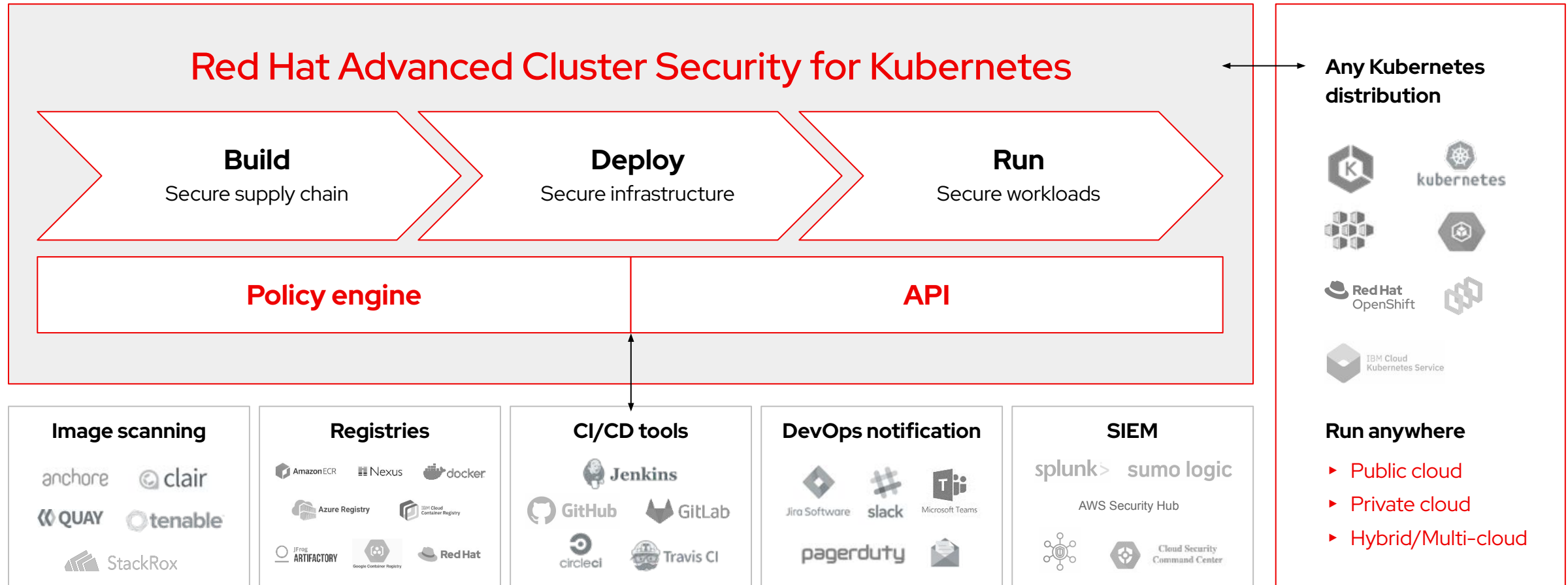- Registry - QUAY
- Service MESH
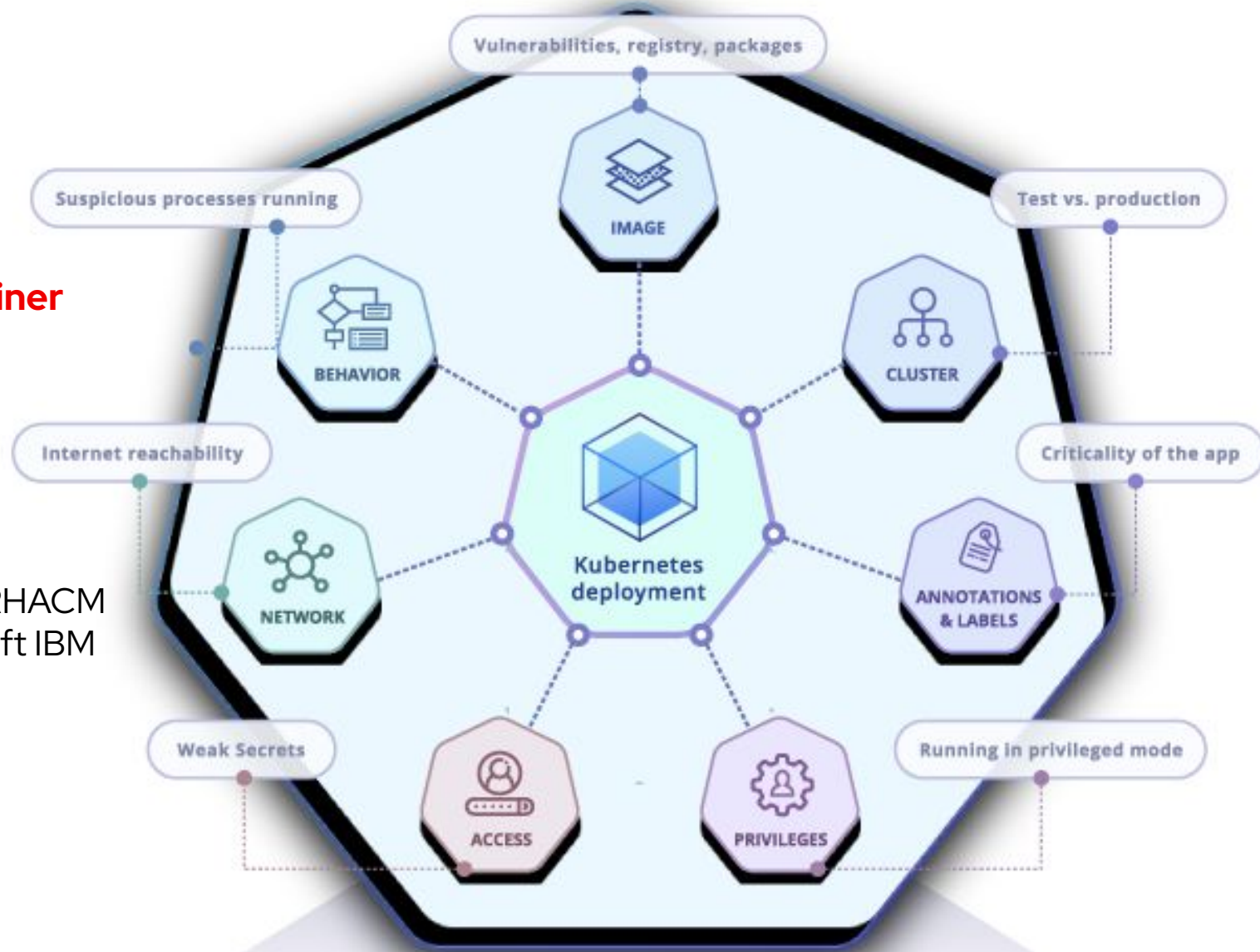
RHACS

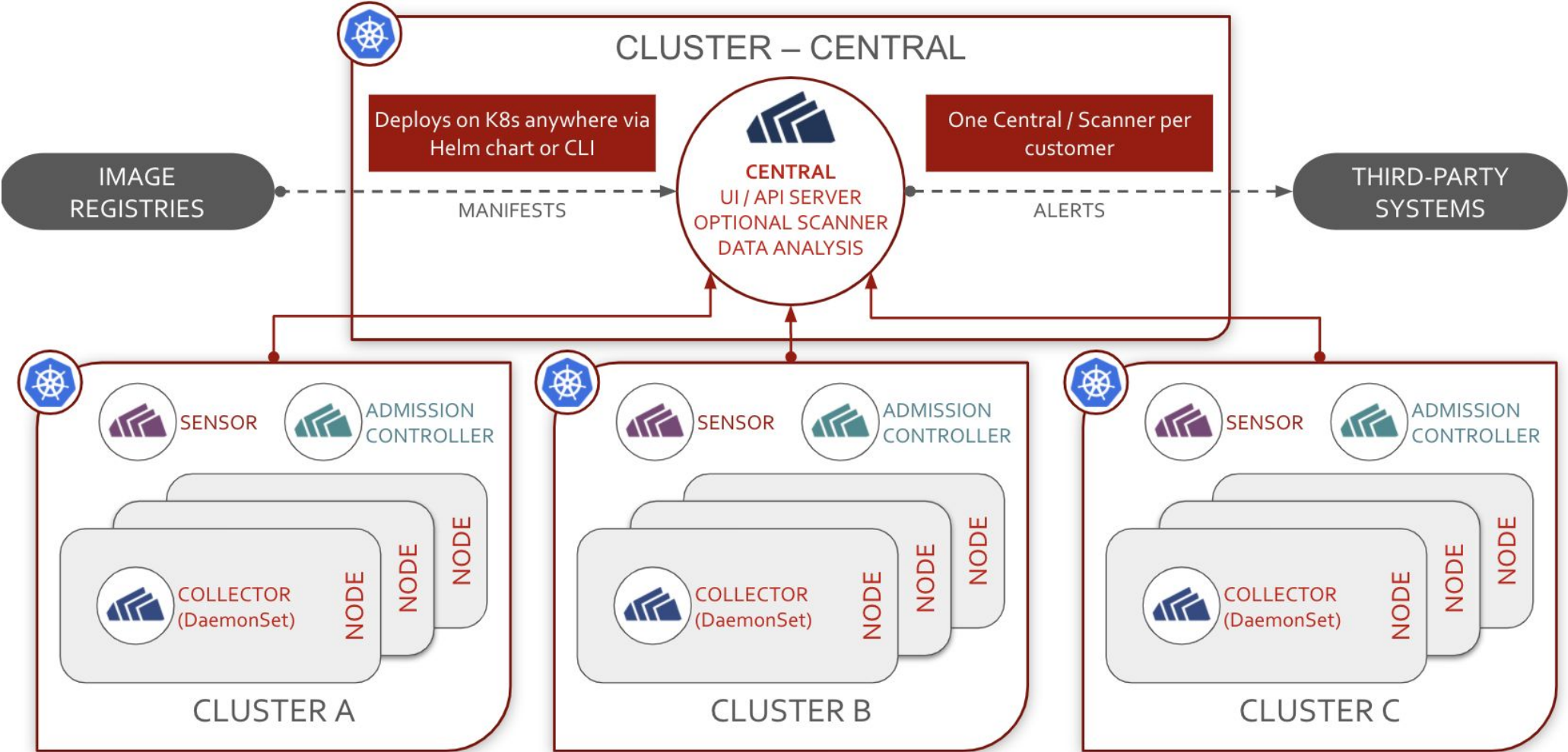adding security to dev ops for your kubernetes native applications

The first Kubernetes-native security platform

Red Hat Advanced Cluster Security for Kubernetes

Any Kubernetes distribution

Build
Secure supply chain

Deploy
Secure infrastructure

Run
Secure workloads

Policy engine

API

Image scanning

anchore   clair
QUAY   tenable
StackRox

Registries

Amazon ECR   Nexus   docker
Azure Registry   IBM Cloud Container Registry
JFrog ARTIFACTORY   Google Container Registry   Red Hat

CI/CD tools

Jenkins
GitHub   GitLab
circleci   Travis CI

DevOps notification

Jira Software   slack   Microsoft Teams
pagerduty

SIEM

splunk>   sumo logic
AWS Security Hub
Cloud Security Command Center

Run anywhere

‣ Public cloud
‣ Private cloud
‣ Hybrid/Multi-cloud

9

Architecture

Who are the buyers?

Budget may come from CISO, DevOps, Platform team

Cloud Native companies

- DevOps teams
- Shift left / DevSecOps
- Influencers: Security Architects

Fortune 500, Global 2,000

- CISO
- IT Ops
- Influencers: Security Architects, DevOps

Red Hat

Relevant use-cases for StackRox you can have a conversation on day 1

Try to focus on these use-cases and give timely & valuable feedback to help shaping our roadmap

Detect

Find and remediate security issues as your applications are built enabling faster delivery. Apply intelligence from runtime analysis to adjust subsequent builds.
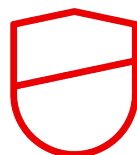
Protect

Protect your infrastructure by securing the Kubernetes platform configuration and automating security-related application deployment policies.

Respond

Monitor for and respond to anomalous application behavior. Leverage deep data collection and correlation to identify threats and enable forensic analysis.

Red Hat

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

Red Hat