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

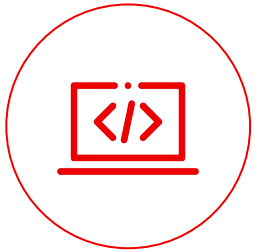
Benefits of a Kubernetes-native approach to security

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 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

RHACS delivers security depth to entire application lifecycle

Detect	Protect	Respond
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
Vulnerability analysis	Image assurance and 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

Build — **Deploy** — **Run**

DevSecOps

Red Hat

RHACS

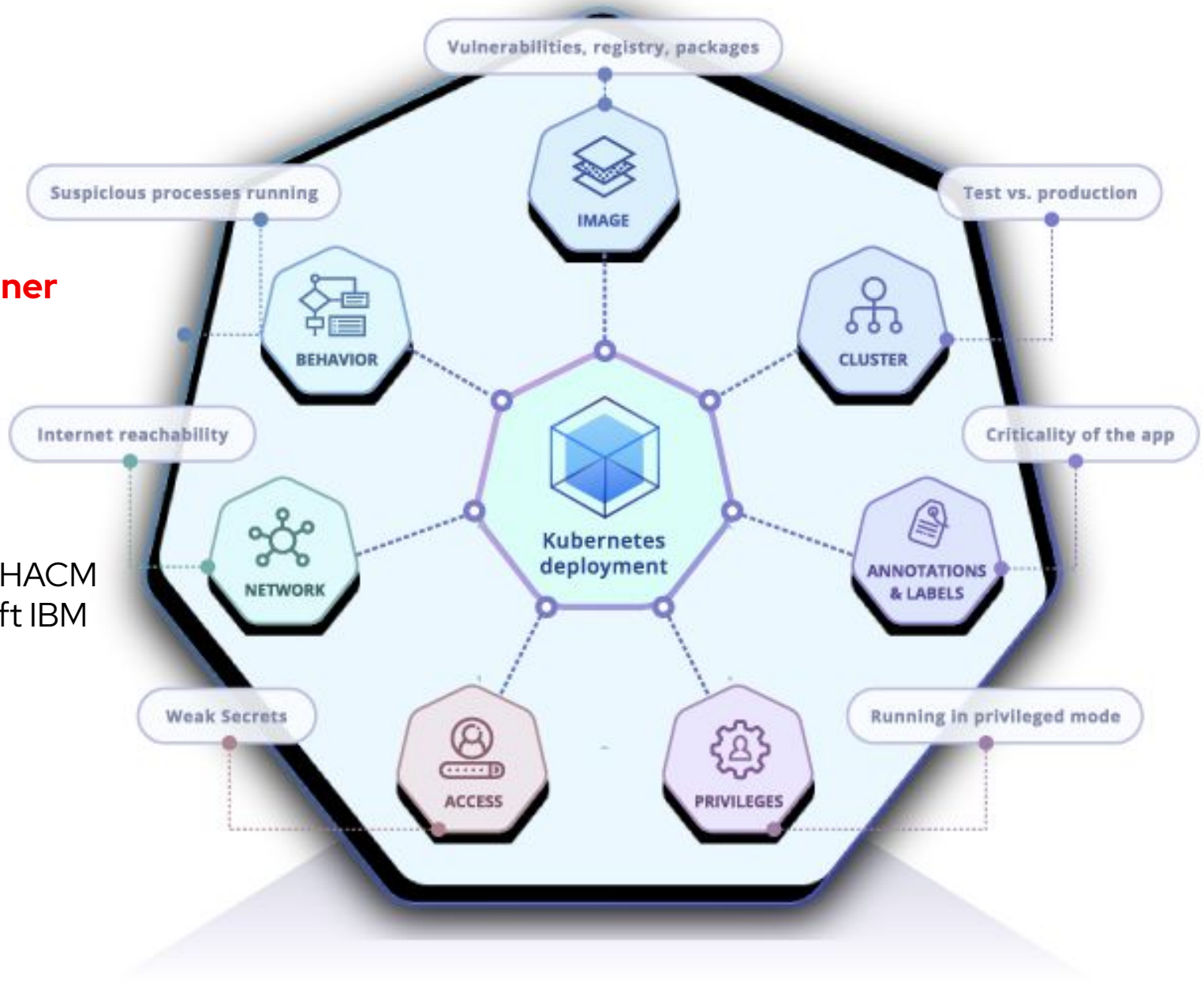
Securing Kubernetes Deployments

It's all about the Application in the container

- plus a Registry Scanner.

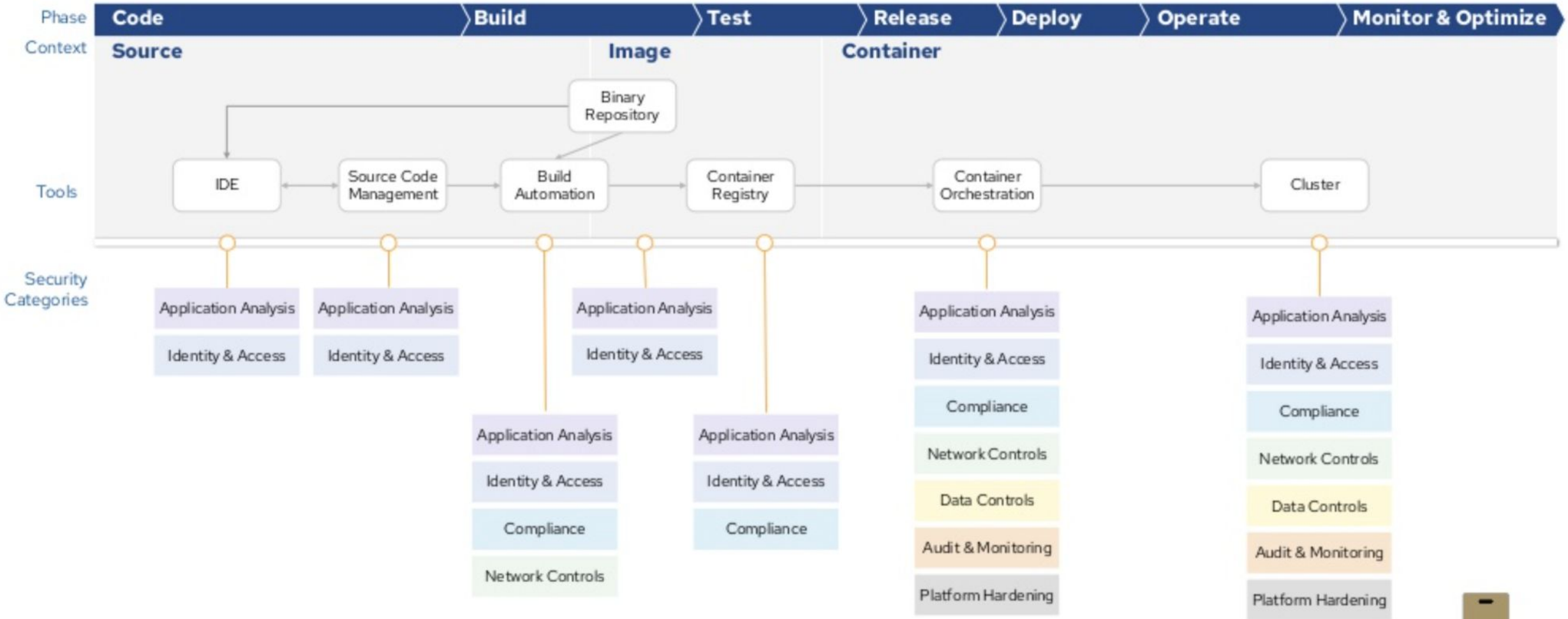
It's not:

- 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

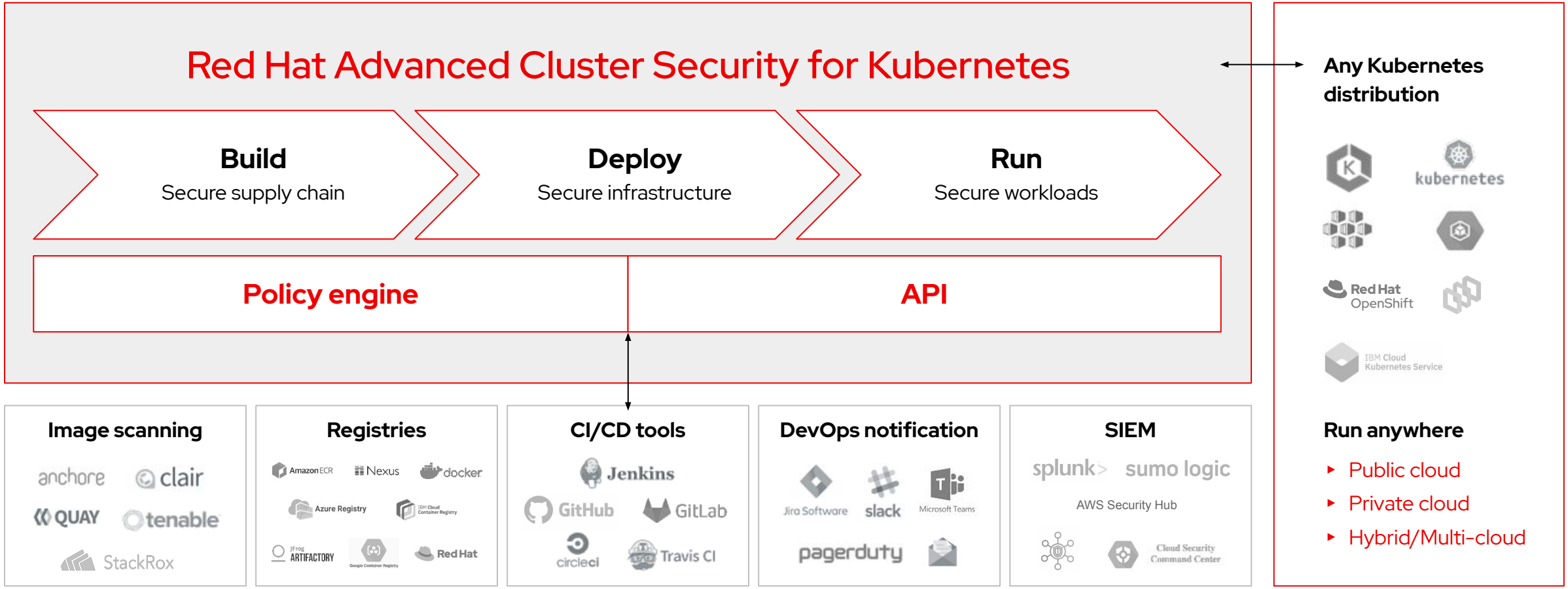


RHACS

adding security to dev ops for your kubernetes native applications

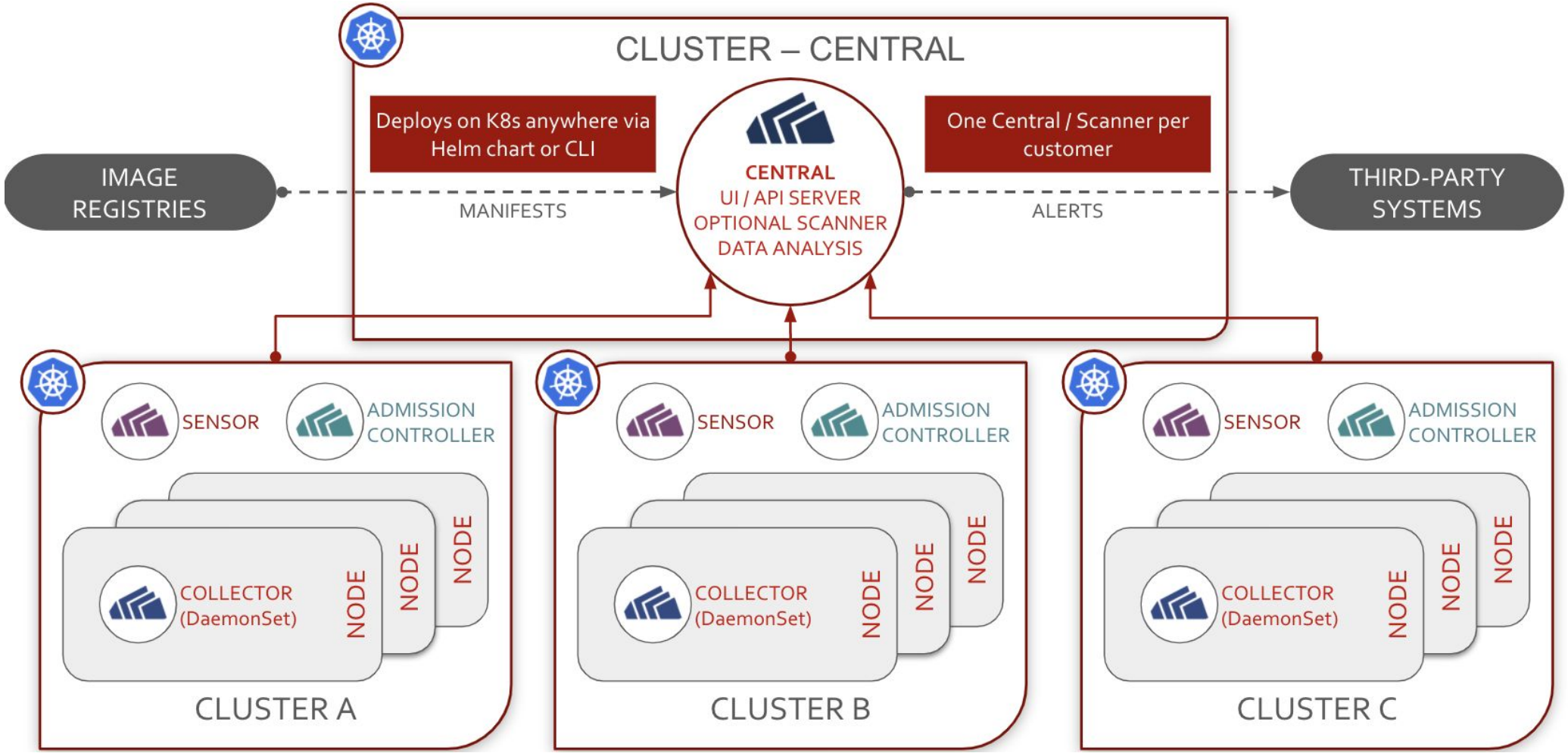


The first Kubernetes-native security platform

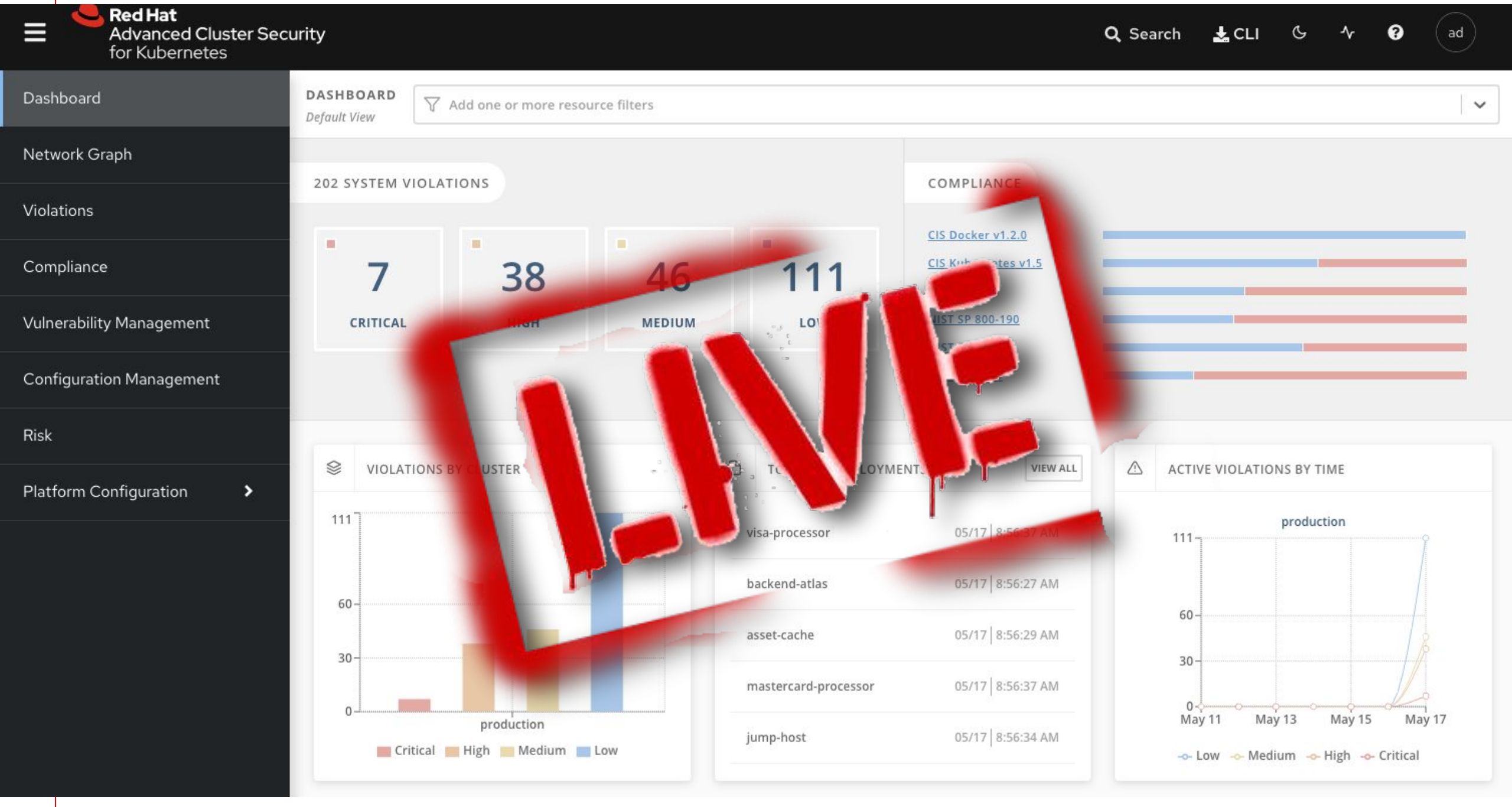


Red Hat

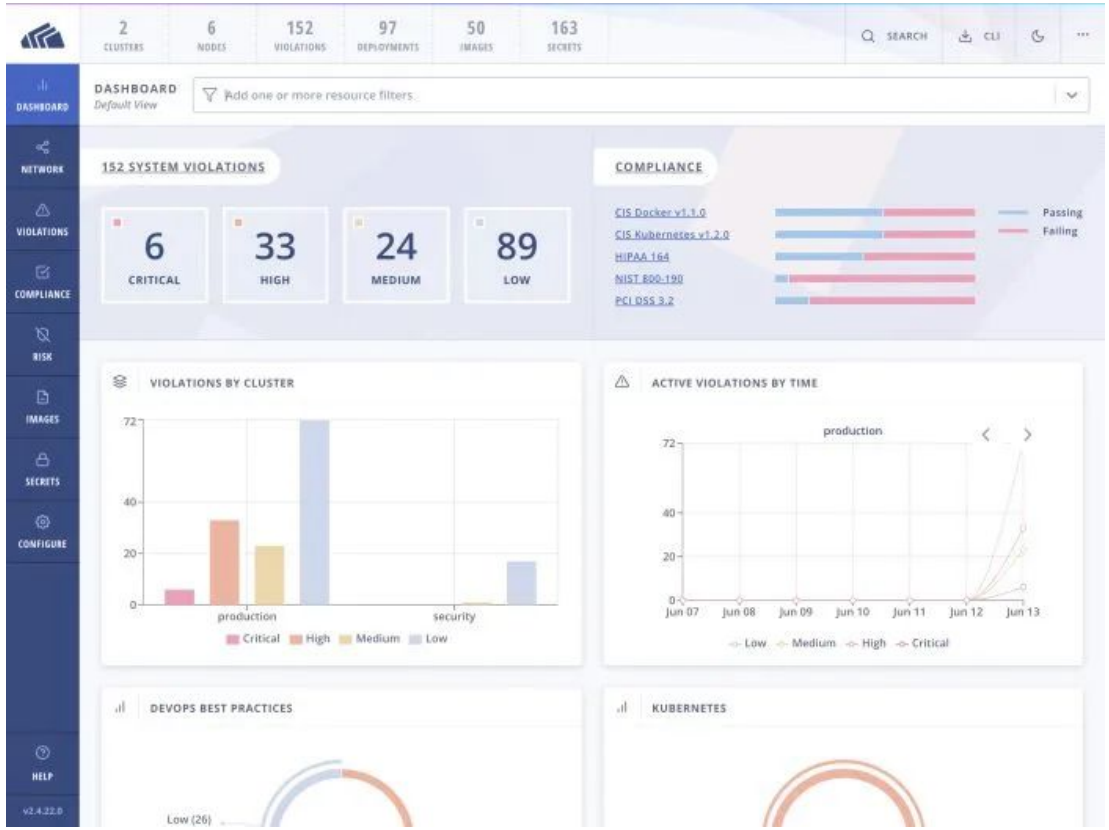
Architecture



Red Hat


Red Hat
Advanced Cluster Security
for Kubernetes
Search
CLI
ad
Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Configuration Management
Risk
Platform Configuration
DASHBOARD
Default View
Add one or more resource filters
202 SYSTEM VIOLATIONS
7
CRITICAL
38
46
MEDIUM
111
COMPLIANCE
CIS Docker v1.2.0
LIVE
VIOLATIONS BY CLUSTER
111
60
30
0
production
Critical
High
Medium
Low
VIEW ALL
visa-processor 05/17 8:56:37 AM
backend-atlas 05/17 8:56:27 AM
asset-cache 05/17 8:56:29 AM
mastercard-processor 05/17 8:56:37 AM
jump-host 05/17 8:56:34 AM
ACTIVE VIOLATIONS BY TIME
production
111
60
30
0
May 11
May 13
May 15
May 17
Low
Medium
High
Critical

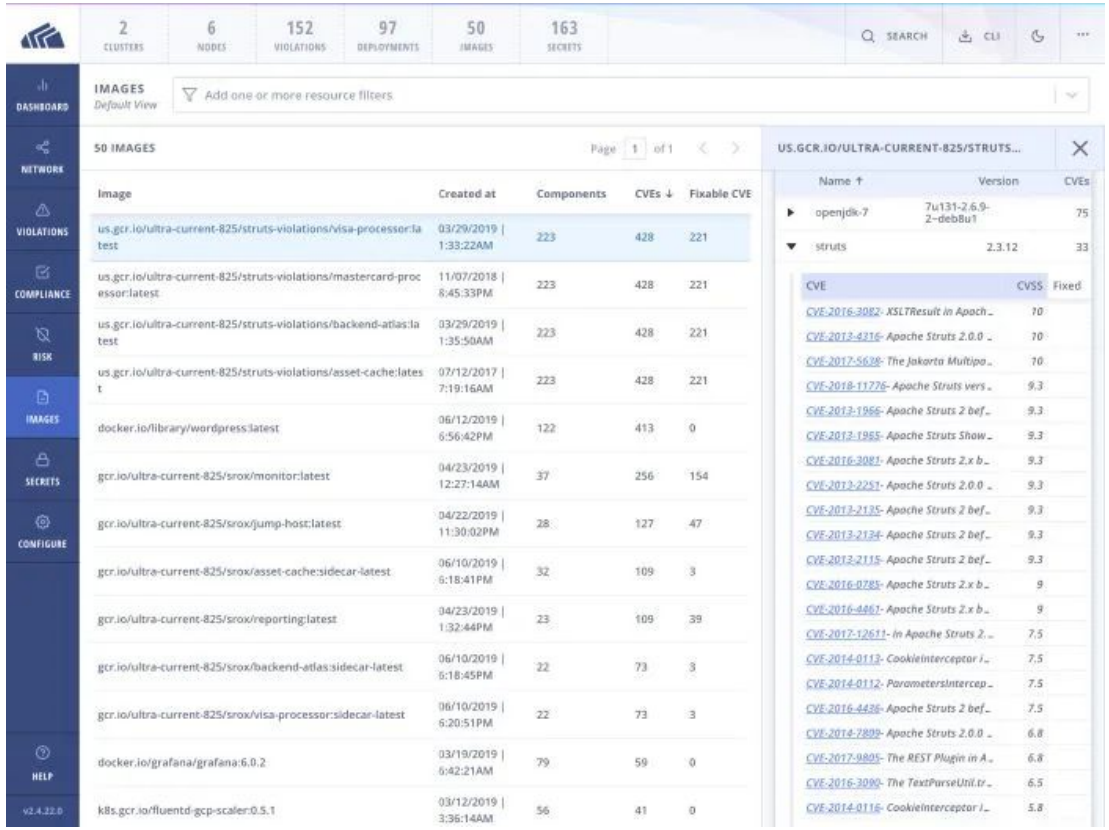
Security for Kubernetes on Red Hat OpenShift



StackRox is available as a Red Hat certified container on the Red Hat Container Catalog. The StackRox platform, with its deep integrations with Kubernetes, provides full life cycle security across build, deploy, and runtime phases for your Kubernetes environments on OpenShift. Customers trust StackRox to protect their cloud-native, on-premises, or hybrid OpenShift environments from vulnerabilities and misconfigurations, ensure compliance with external and internal policies, and detect and stop runtime threats.

Red Hat

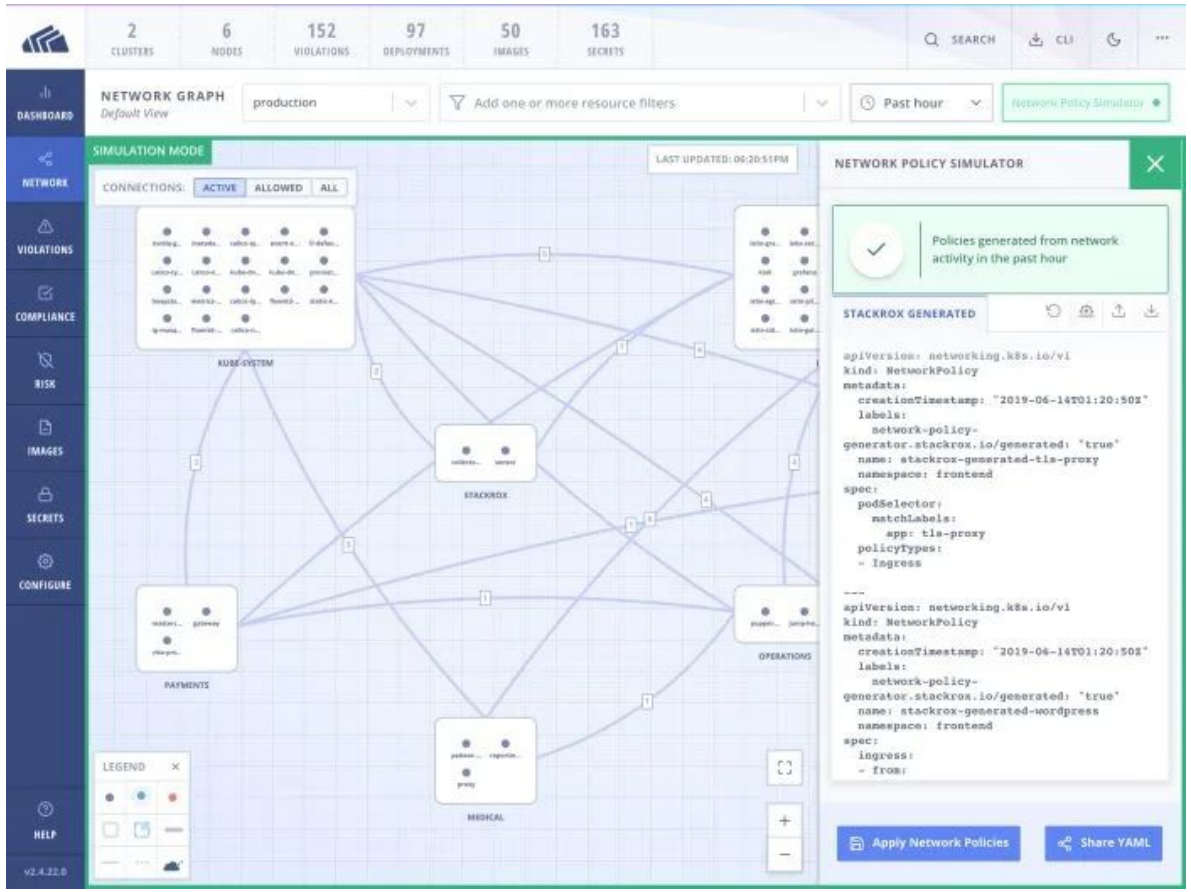
Vulnerability management



Protect your containers against vulnerabilities from the time images are built until they're deployed and running. StackRox can block vulnerable images from being deployed and integrates with your approved registries, including OpenShift Container Registry (OCR), for granular policy enforcement. StackRox also provides extensive support for third-party scanners such as Anchore, Red Hat Quay, Clair, and Tenable to augment your existing image scanning tools.

Red Hat

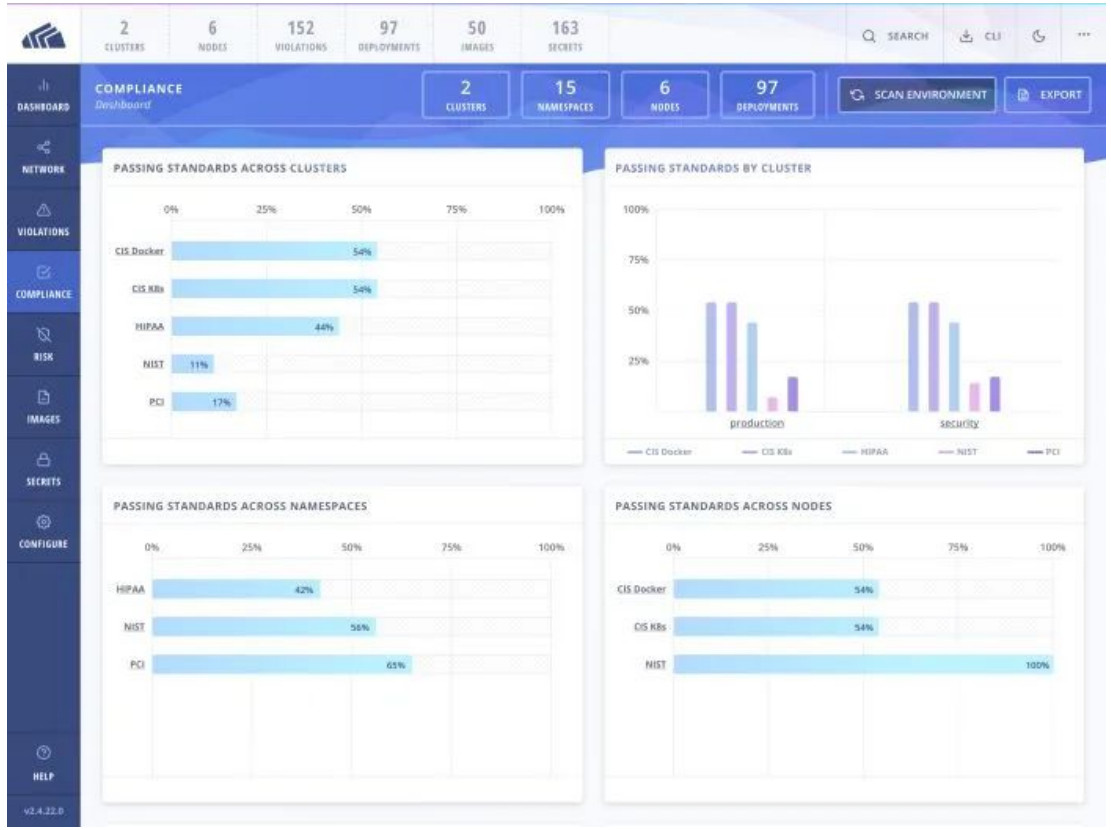
Network segmentation



StackRox provides comprehensive network security for Kubernetes deployments on OpenShift. Leverage our network graph to see your allowed vs. active network traffic across deployments. We integrate with any Container Network Interface to leverage the power of OpenShift for network policy enforcement. Use StackRox to simulate and apply changes to network segmentation policies, and automatically generate updated YAML files based on behavioral modeling of active traffic to tighten overly permissive Kubernetes network policies.

Red Hat

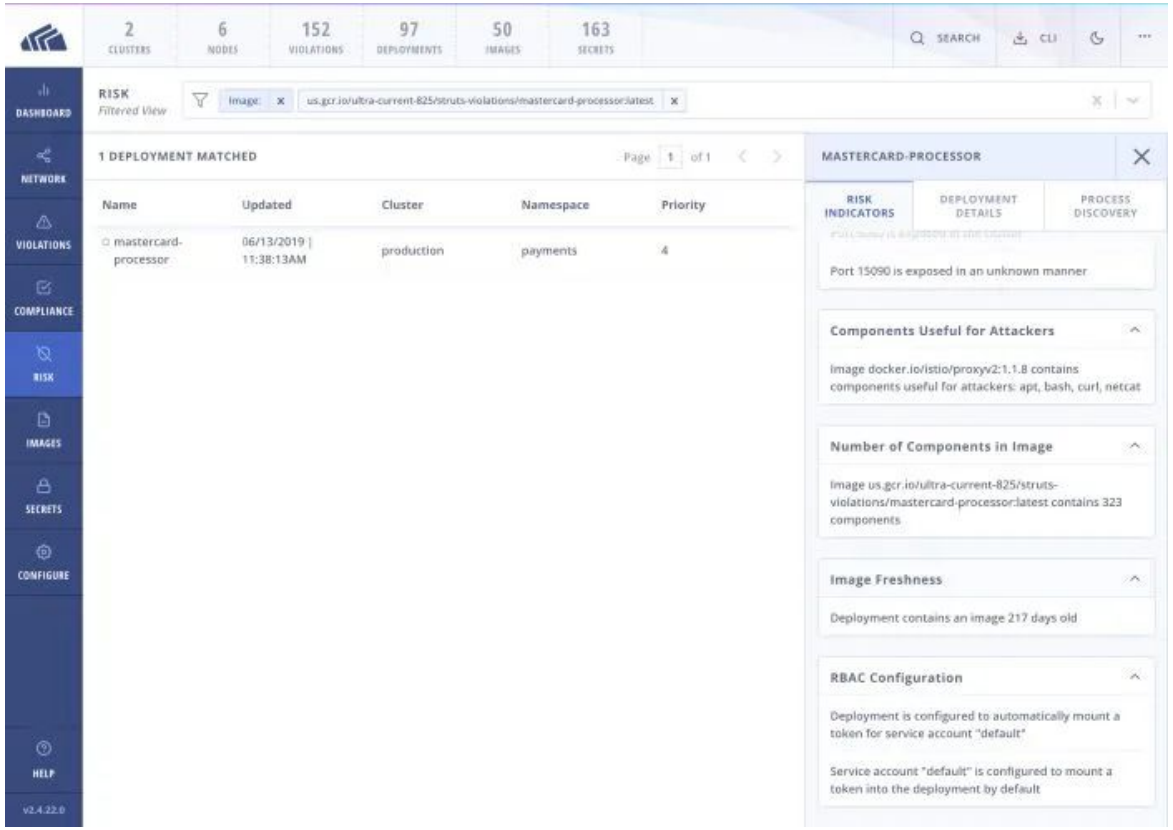
Continuous compliance with CIS benchmarks and beyond



StackRox provides industry-leading compliance capabilities to help ensure adherence to CIS Benchmarks for Docker and Kubernetes as well as NIST, PCI, and HIPAA. Use our policy templates to instantly generate audit reports and effortlessly identify non-compliant clusters, nodes, or namespaces.

Red Hat

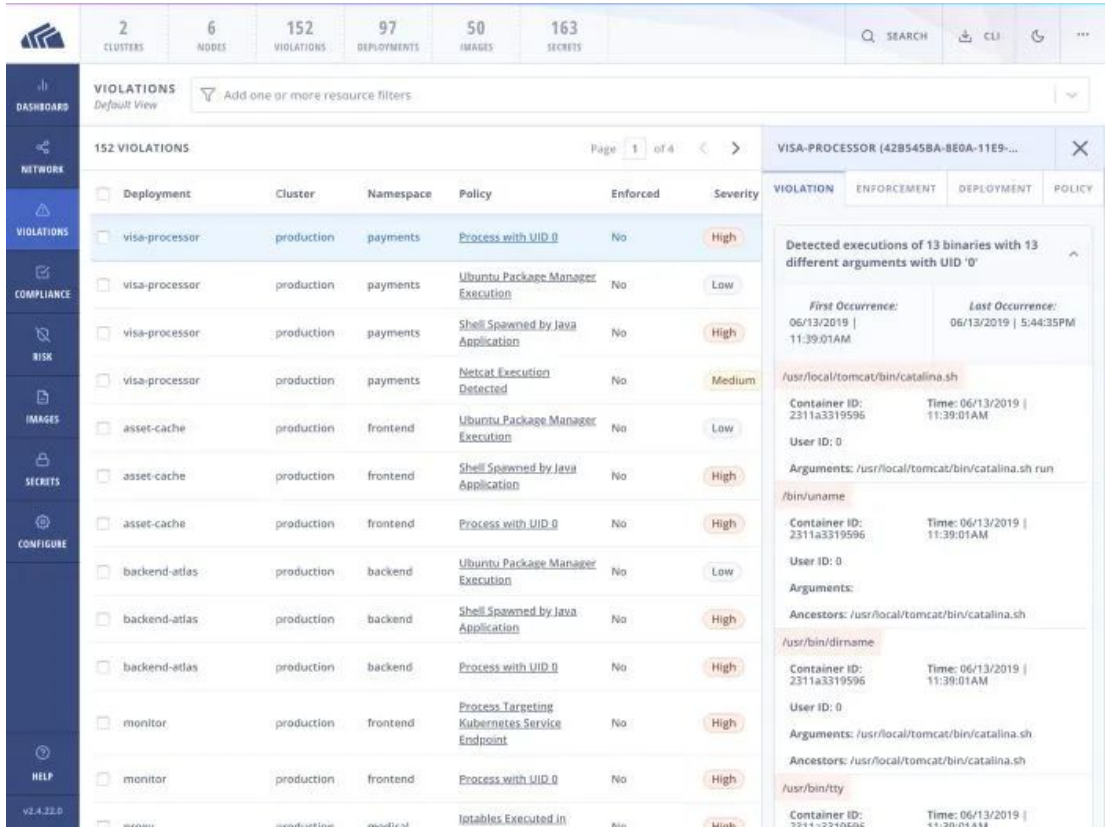
Configuration management



StackRox leverages its Kubernetes-native architecture to apply rich context for configuration management, spanning containers, images, deployments, and OpenShift itself. With StackRox, organizations can identify and remediate misconfigurations such as exposed secrets, excessive privileges, and unnecessary network reachability. Leverage pre-built policy templates or create custom policies to prevent builds or deployments that don't meet your security, compliance, or DevOps best practices requirements.

Red Hat

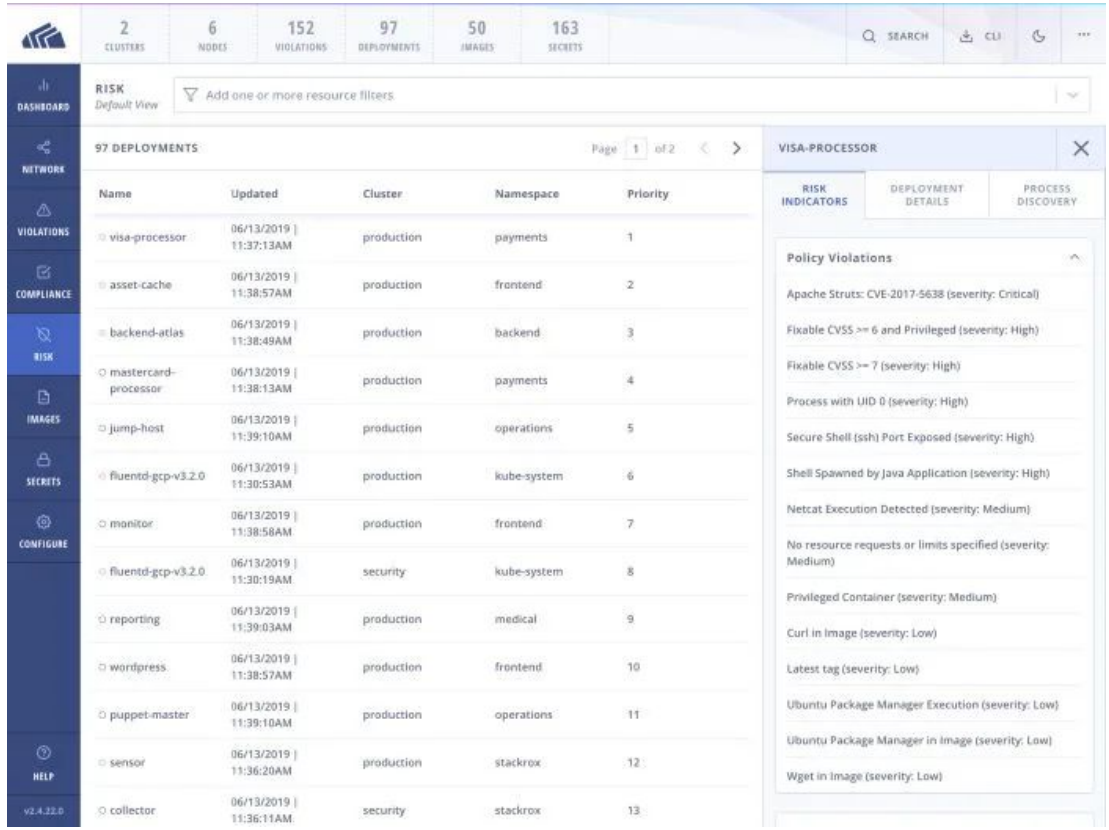
Runtime detection and response



StackRox combines behavioral modeling with rules, allow listing, and baselining to detect and prevent runtime threats on OpenShift platforms. StackRox identifies threats as they occur across several critical areas, including process execution, network connections and flows, and privilege escalation. Use our out-of-the-box policies and automated policy enforcement or build custom policies that combine industry standards with your company's own internal policies.

Red Hat

Risk prioritization at scale



Use StackRox to automatically profile and prioritize risks across every OpenShift deployment. Unlike other security solutions, StackRox goes beyond image scanning to combine CVE details with other risk factors, such as deployment misconfigurations including exposed secrets or overly permission network policies, runtime anomalies, and other contextual information to identify the top issues that need immediate remediation.

Red Hat

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

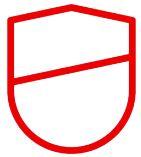
- CISO
- IT Ops
- Influencers: Security Architects, DevOps

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

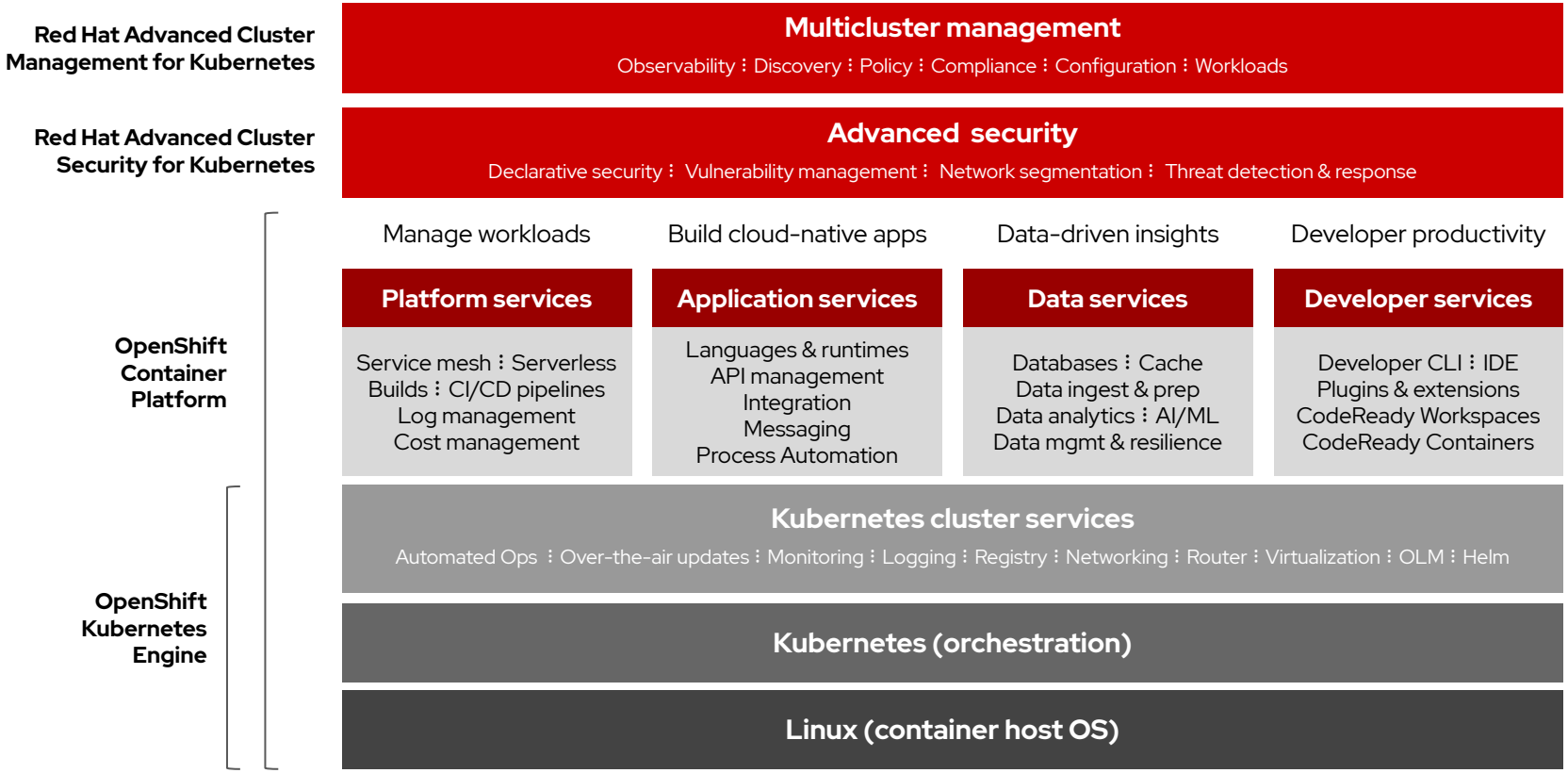
Protect your infrastructure by securing the Kubernetes platform configuration and automating security-related application deployment policies.

Respond

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

RHACS and RHACM

Enterprise Kubernetes from Red Hat



Red Hat

Positioning ACS and ACM

Advanced Cluster Security

Implement and enforce security policies at build, deploy and runtime

- Intrusion detection with runtime behavioral analysis
- Image assurance with vulnerability and config analysis / admission control
- Network policy visibility; auto-suggest network policies; simulate results
- Standards-based compliance with security controls
- Deep data collection and correlation for forensics

Advanced Cluster Management

Multicluster and application lifecycle policy-based management

- Create, update and destroy clusters
- Automate the placement of workloads based on capacity and policy and via GitOps
- Visualize application relationships across clusters and those that span clusters
- Governance & regulatory compliance; OPA Gatekeeper integration
- Centralize health monitoring, metrics and alerts across multiple clusters

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