



**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](mailto:abach@redhat.com)



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

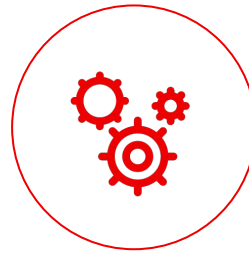
Security

# Benefits of a Kubernetes-native approach to security



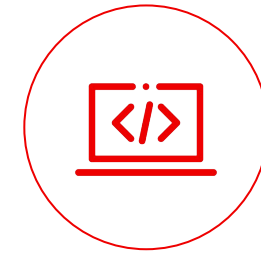
## Lower operational cost

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

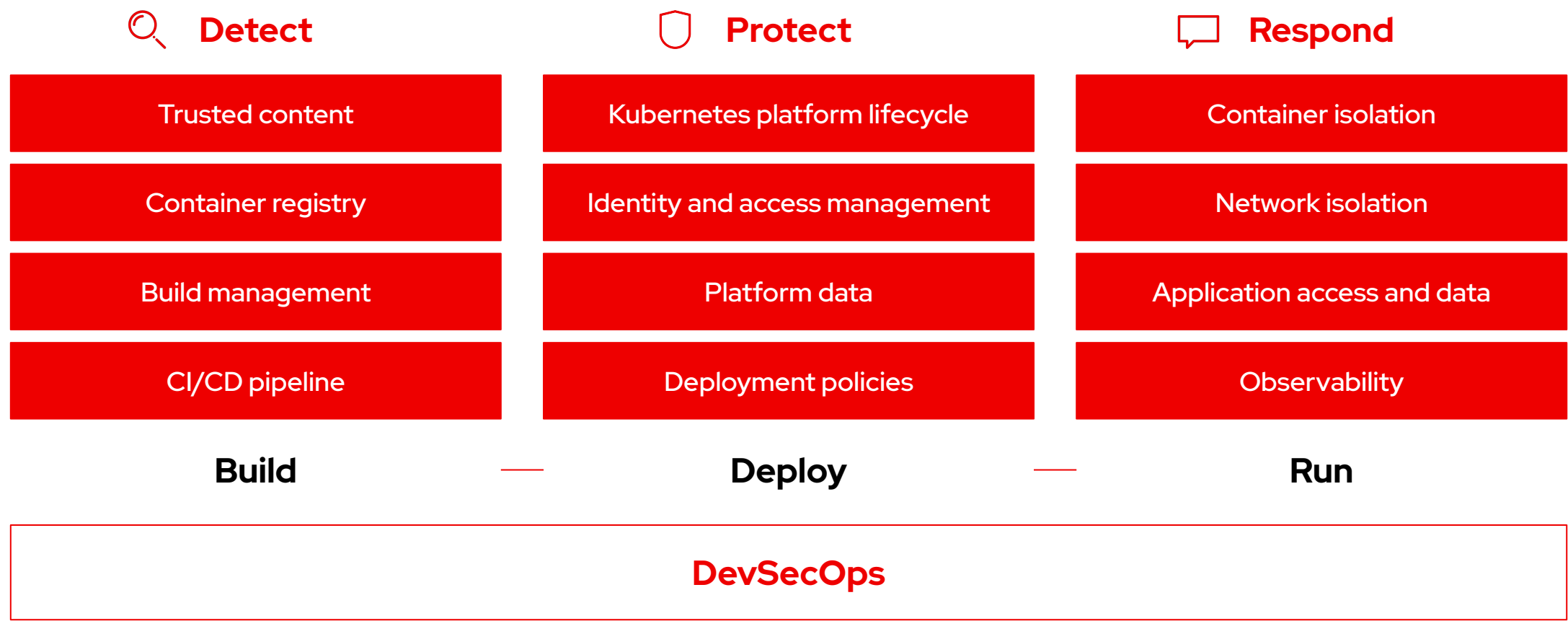
### Secure workloads

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 OpenShift provides a secure foundation



# 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**

# RHACS

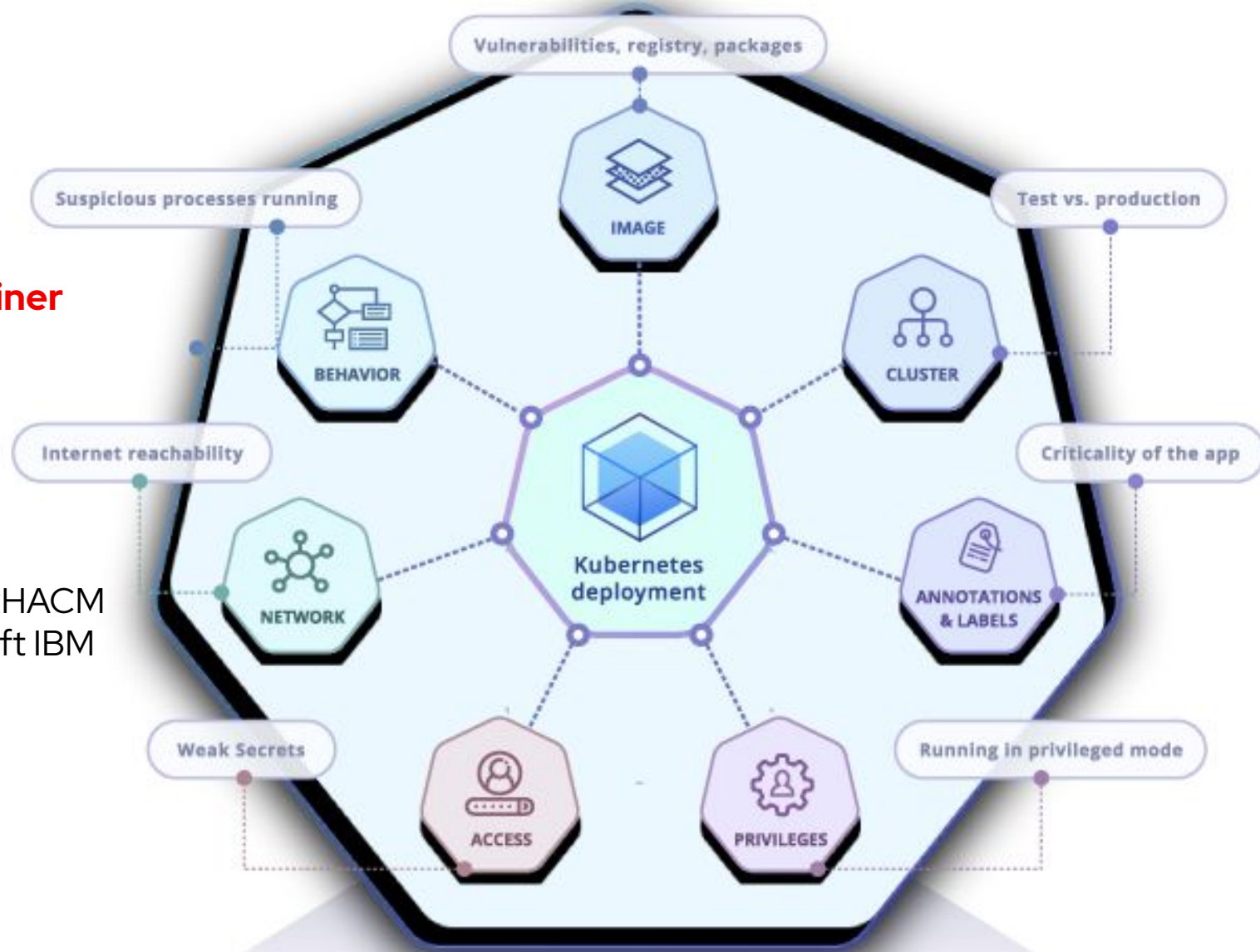
## Securing Kubernetes Deployments

### It's all about the Application in the container

- plus a Registry Scanner.

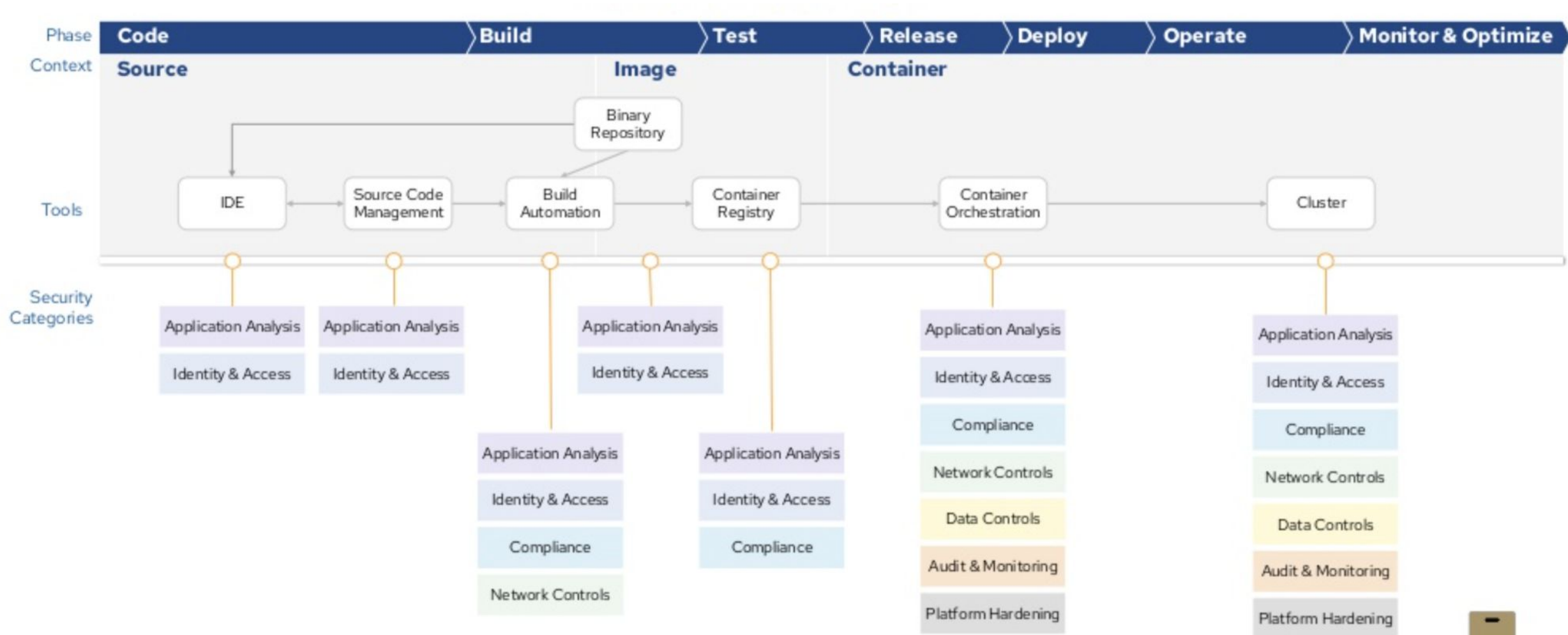
### It's not:

- 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



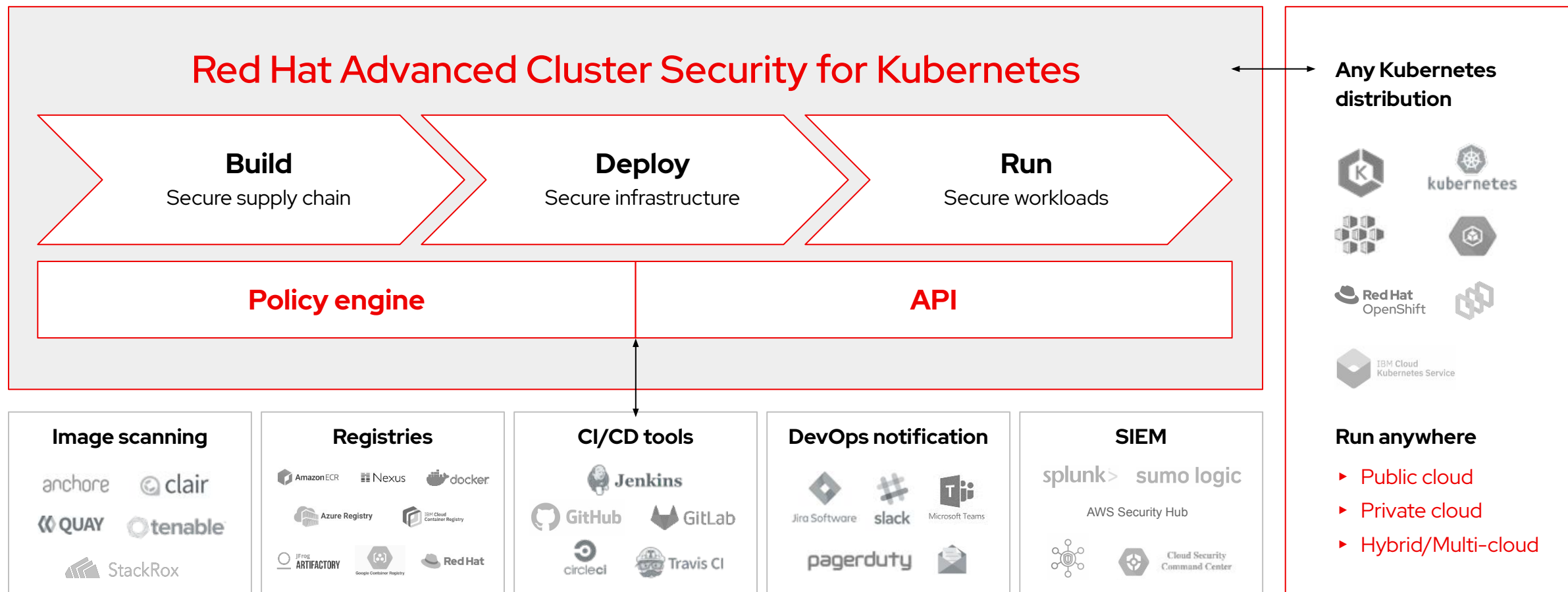
# RHACS

adding security to dev ops for your kubernetes native applications

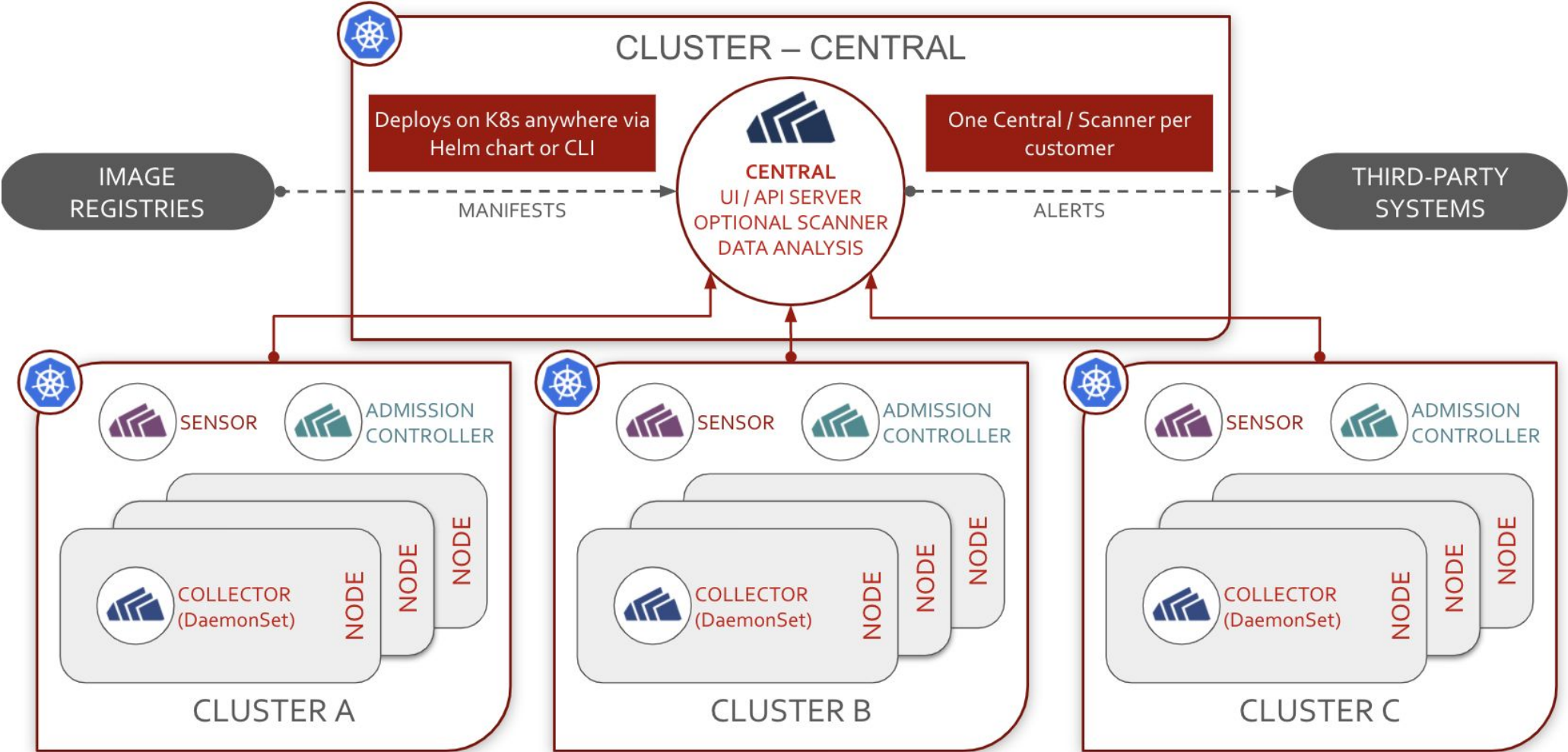




# The first Kubernetes-native security platform



# Architecture





Dashboard

Network Graph

Violations

Compliance

Vulnerability Management

Configuration Management

Risk

Platform Configuration



## DASHBOARD

Default View



Add one or more resource filters



### 202 SYSTEM VIOLATIONS

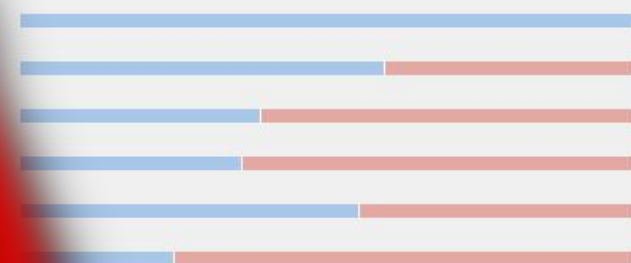


### COMPLIANCE

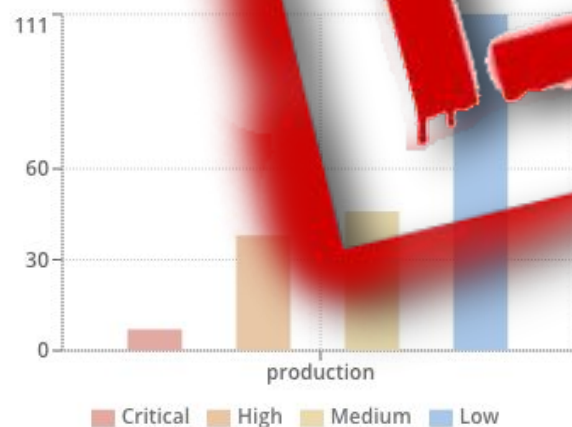
[CIS Docker v1.2.0](#)

[CIS Kubernetes v1.5](#)

[NIST SP 800-190](#)



### VIOLATIONS BY CLUSTER



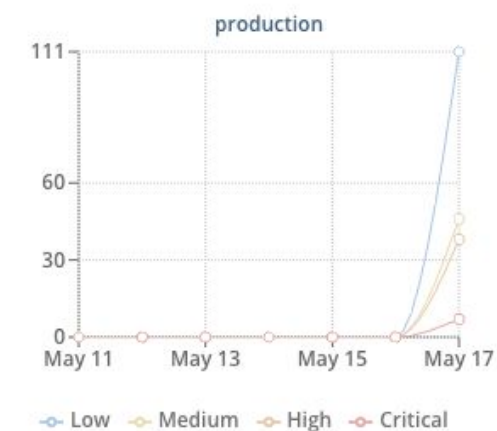
### TOP VIOLATIONS BY CLUSTER

[VIEW ALL](#)

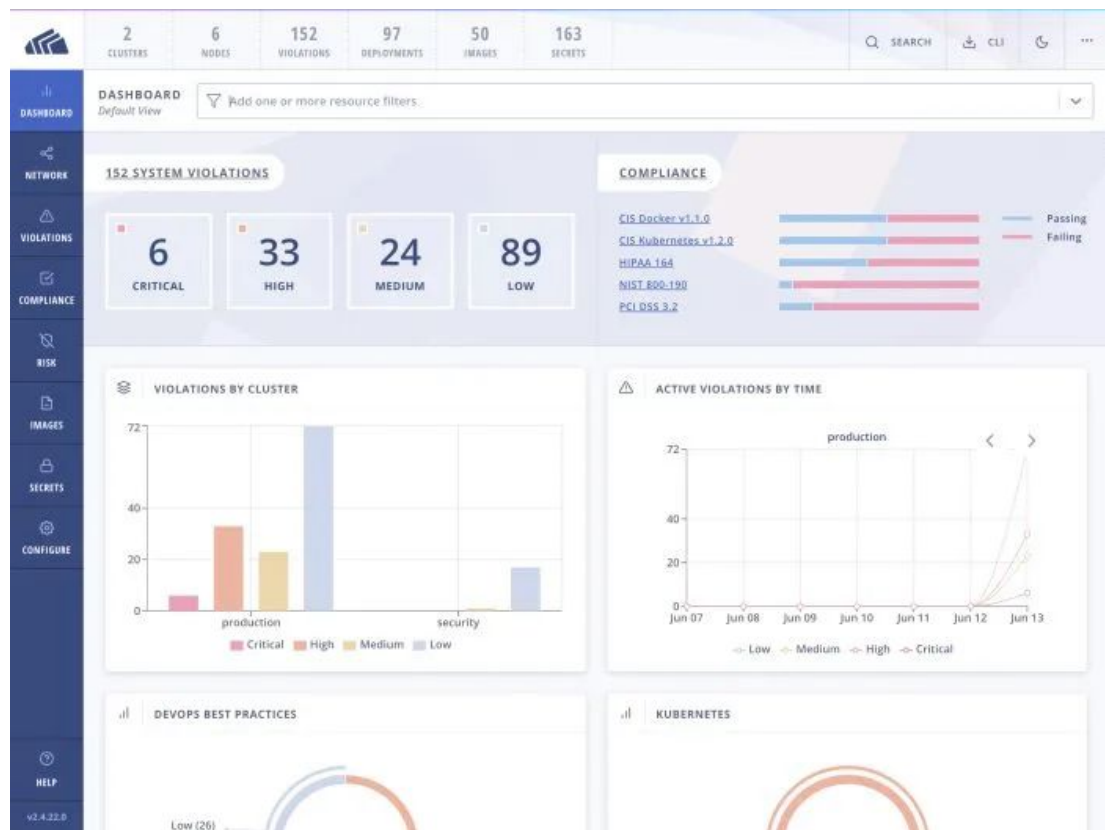
visa-processor	05/17   8:56:37 AM
backend-atlas	05/17   8:56:27 AM
asset-cache	05/17   8:56:29 AM
mastercard-processor	05/17   8:56:37 AM
jump-host	05/17   8:56:34 AM



### ACTIVE VIOLATIONS BY TIME



# 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.

# Vulnerability management

	2	6	152	97	50	163				
	CLUSTERS	NODES	VIOLATIONS	DEPLOYMENTS	IMAGES	SECRETS		Q SEARCH	CLI	...
<b>DASHBOARD</b>	IMAGES Default View Add one or more resource filters									
<b>NETWORK</b>	50 IMAGES Page 1 of 1									
<b>VIOLATIONS</b>										
<b>COMPLIANCE</b>										
<b>RISK</b>										
<b>IMAGES</b>										
<b>SECRETS</b>										
<b>CONFIGURE</b>										
<b>HELP</b>										
vs 4.32.0										

Image	Created at	Components	CVEs ↓	Fixable CVE
us.gcr.io/ultra-current-825/struts-violations/visa-processor:latest	03/29/2019   1:33:22AM	223	428	221
us.gcr.io/ultra-current-825/struts-violations/mastercard-processor:latest	11/07/2018   8:45:33PM	223	428	221
us.gcr.io/ultra-current-825/struts-violations/backend-atlas:latest	03/29/2019   1:35:50AM	223	428	221
us.gcr.io/ultra-current-825/struts-violations/asset-cache:latest	07/12/2017   7:19:16AM	223	428	221
docker.io/library/wordpress:latest	06/12/2019   6:56:42PM	122	413	0
gcr.io/ultra-current-825/srox/monitor:latest	04/23/2019   12:27:14AM	37	256	154
gcr.io/ultra-current-825/srox/jump-host:latest	04/22/2019   11:30:02PM	28	127	47
gcr.io/ultra-current-825/srox/asset-cache:sidecar-latest	06/10/2019   6:18:41PM	32	109	3
gcr.io/ultra-current-825/srox/reporting:latest	04/23/2019   1:32:44PM	23	109	39
gcr.io/ultra-current-825/srox/backend-atlas:sidecar-latest	06/10/2019   6:18:45PM	22	73	3
gcr.io/ultra-current-825/srox/visa-processor:sidecar-latest	06/10/2019   6:20:51PM	22	73	3
docker.io/grafana/grafana:6.0.2	03/19/2019   6:42:21AM	79	59	0
k8s.gcr.io/fluently-gcp-scaler:0.5.1	03/12/2019   3:36:14AM	56	41	0

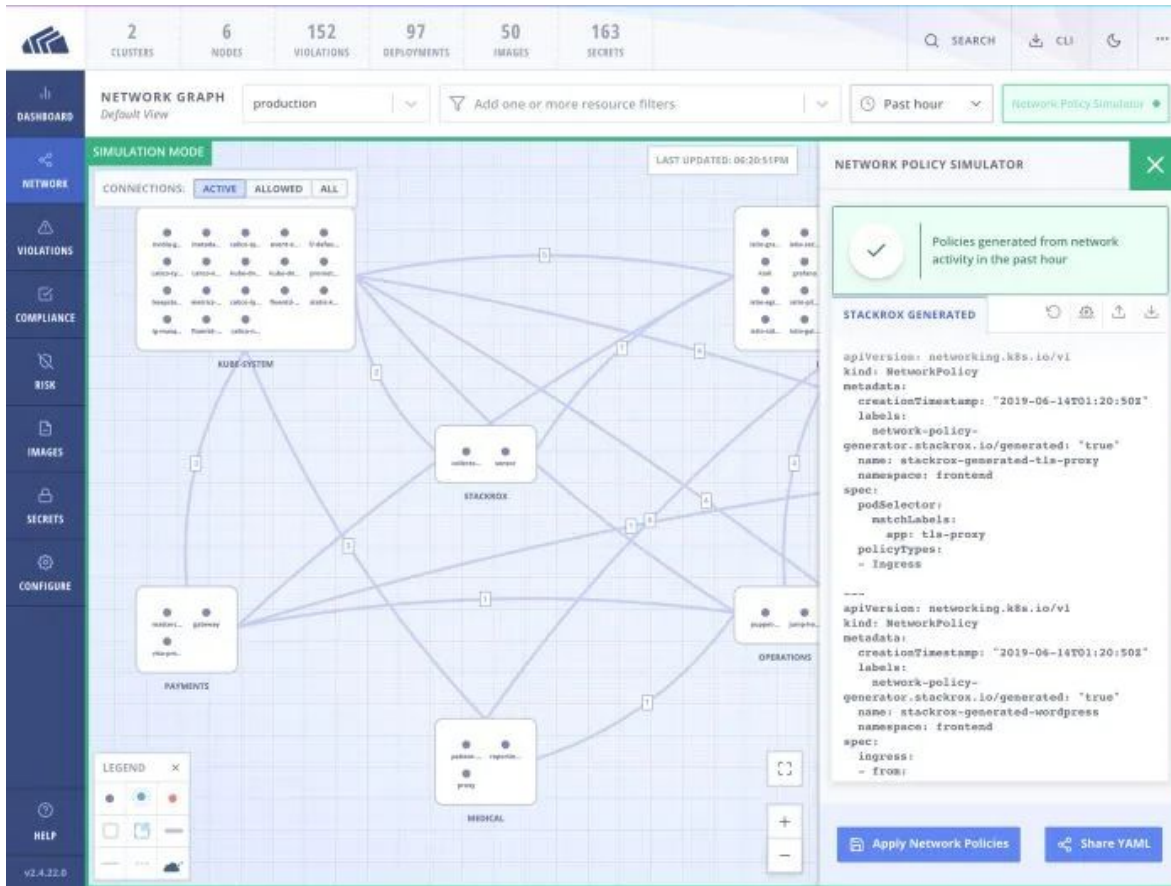
Name ↑	Version	CVEs
openjdk-7	7u131-2.6.9-2-deb8u1	75
struts	2.3.12	33

CVE	CVSS	Fixed
CVE-2016-3082- XSLTResult in Apach...	7.0	
CVE-2012-4316- Apache Struts 2.0.0 ...	7.0	
CVE-2017-5638- The Jakarta MultiPa...	7.0	
CVE-2018-11776- Apache Struts vers...	9.3	
CVE-2013-1956- Apache Struts 2 bef...	9.3	
CVE-2013-1955- Apache Struts Show...	9.3	
CVE-2016-3081- Apache Struts 2.x b...	9.3	
CVE-2012-2251- Apache Struts 2.0.0 ...	9.3	
CVE-2013-2135- Apache Struts 2 bef...	9.3	
CVE-2013-2134- Apache Struts 2 bef...	9.3	
CVE-2012-2115- Apache Struts 2 bef...	9.3	
CVE-2016-0783- Apache Struts 2.x b...	9	
CVE-2016-4461- Apache Struts 2.x b...	9	
CVE-2017-12611- In Apache Struts 2...	7.5	
CVE-2014-0113- CookieInterceptor I...	7.5	
CVE-2014-0112- ParametersIntercep...	7.5	
CVE-2016-4438- Apache Struts 2 bef...	7.5	
CVE-2014-7899- Apache Struts 2.0.0 ...	6.8	
CVE-2017-9805- The REST Plugin in A...	6.8	
CVE-2016-3090- The TextParseUtilTr...	6.5	
CVE-2014-0116- CookieInterceptor I...	5.8	

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.

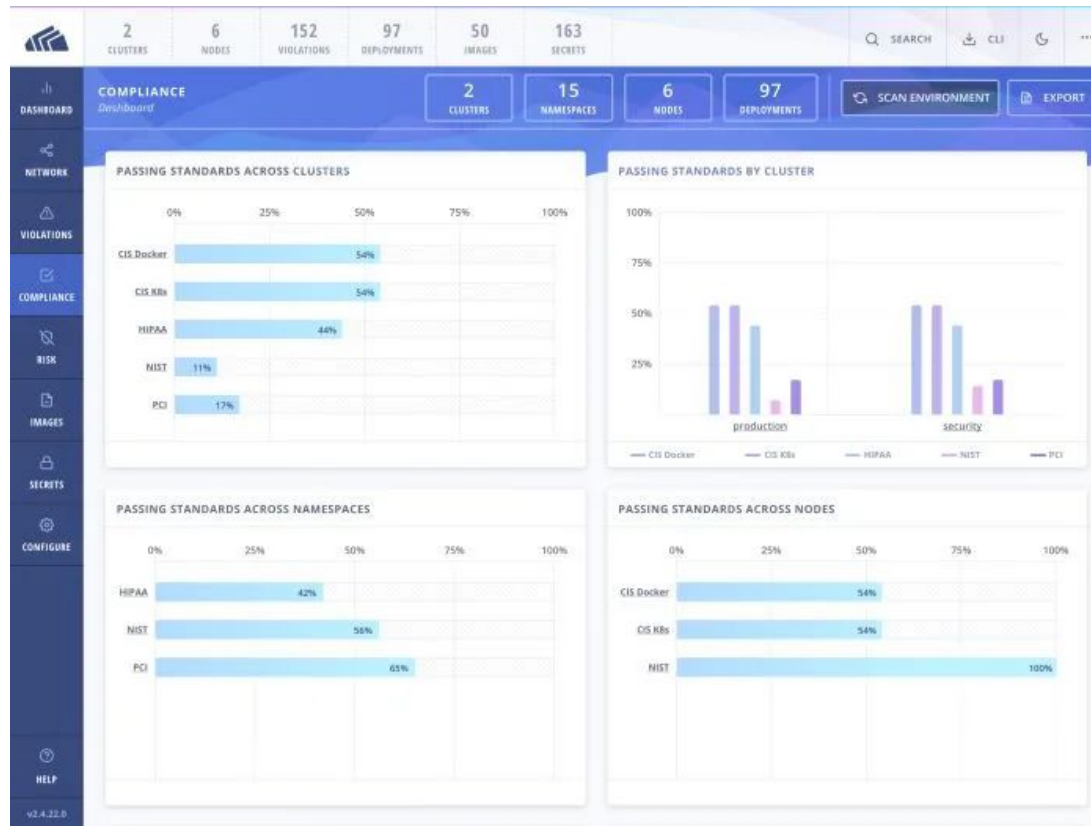


# Network segmentation



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.

# 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.

# Configuration management

The screenshot displays the StackRox Risk dashboard. At the top, a summary bar shows counts for Clusters (2), Nodes (6), Violations (152), Deployments (97), Images (50), and Secrets (163). Below this, a search bar is present. The main content area is titled 'RISK' and shows a 'Filtered View' of '1 DEPLOYMENT MATCHED'. A table lists the deployment details:

Name	Updated	Cluster	Namespace	Priority
mastercard-processor	06/13/2019   11:38:13AM	production	payments	4

To the right of the table, a detailed view for 'MASTERCARD-PROCESSOR' is shown, including sections for 'RISK INDICATORS', 'DEPLOYMENT DETAILS', and 'PROCESS DISCOVERY'. Key findings include:

- Port 15090 is exposed in an unknown manner.**
- Components Useful for Attackers:** Image docker.io/istio/proxyv2:1.1.8 contains components useful for attackers: apt, bash, curl, netcat.
- Number of Components in Image:** Image us.gcr.io/ultra-current-825/struts-violations/mastercard-processor:latest contains 323 components.
- Image Freshness:** Deployment contains an image 217 days old.
- RBAC Configuration:** Deployment is configured to automatically mount a token for service account "default". Service account "default" is configured to mount a token into the deployment by default.

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.



# Runtime detection and response

The screenshot displays the StackRox console interface. At the top, a summary bar shows counts for Clusters (2), Nodes (6), Violations (152), Deployments (97), Images (50), and Secrets (163). Below this, a sidebar on the left contains navigation links for Dashboard, Network, Violations, Compliance, Risk, Images, Secrets, and Configure. The main area is titled 'VIOLATIONS' and shows a list of 152 violations. A table lists violations with columns for Deployment, Cluster, Namespace, Policy, Enforced, and Severity. The table shows various violations such as 'visa-processor', 'asset-cache', 'backend-atlas', and 'monitor' across different namespaces and policies. A detailed view of a specific violation is shown on the right, titled 'VISA-PROCESSOR (42B545BA-8E0A-11E9-...)'. This view includes tabs for Violation, Enforcement, Deployment, and Policy. The Violation tab shows details about the detected execution of 13 binaries with 13 different arguments with UID '0'. It includes information about the first and last occurrence, container ID, user ID, and arguments.

Deployment	Cluster	Namespace	Policy	Enforced	Severity
<input type="checkbox"/> visa-processor	production	payments	Process with UID 0	No	High
<input type="checkbox"/> visa-processor	production	payments	Ubuntu Package Manager Execution	No	Low
<input type="checkbox"/> visa-processor	production	payments	Shell Spawned by Java Application	No	High
<input type="checkbox"/> visa-processor	production	payments	Netcat Execution Detected	No	Medium
<input type="checkbox"/> asset-cache	production	frontend	Ubuntu Package Manager Execution	No	Low
<input type="checkbox"/> asset-cache	production	frontend	Shell Spawned by Java Application	No	High
<input type="checkbox"/> asset-cache	production	frontend	Process with UID 0	No	High
<input type="checkbox"/> backend-atlas	production	backend	Ubuntu Package Manager Execution	No	Low
<input type="checkbox"/> backend-atlas	production	backend	Shell Spawned by Java Application	No	High
<input type="checkbox"/> backend-atlas	production	backend	Process with UID 0	No	High
<input type="checkbox"/> monitor	production	frontend	Process Targeting Kubernetes Service Endpoint	No	High
<input type="checkbox"/> monitor	production	frontend	Process with UID 0	No	High

**VISA-PROCESSOR (42B545BA-8E0A-11E9-...)**

Detected executions of 13 binaries with 13 different arguments with UID '0'

First Occurrence: 06/13/2019 | 11:39:01AM  
Last Occurrence: 06/13/2019 | 5:44:35PM

/usr/local/tomcat/bin/catalina.sh

Container ID: 2311a3319596  
Time: 06/13/2019 | 11:39:01AM  
User ID: 0  
Arguments: /usr/local/tomcat/bin/catalina.sh run

/bin/uname

Container ID: 2311a3319596  
Time: 06/13/2019 | 11:39:01AM  
User ID: 0  
Arguments: /usr/local/tomcat/bin/catalina.sh

/usr/bin/dmname

Container ID: 2311a3319596  
Time: 06/13/2019 | 11:39:01AM  
User ID: 0  
Arguments: /usr/local/tomcat/bin/catalina.sh  
Ancestors: /usr/local/tomcat/bin/catalina.sh

/usr/bin/tty

Container ID: 2311a3319596  
Time: 06/13/2019 | 11:39:01AM

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.

# Risk prioritization at scale

	2	6	152	97	50	163		Q SEARCH	CLJ	...
	CLUSTERS	NODES	VIOLATIONS	DEPLOYMENTS	IMAGES	SECRETS				
DASHBOARD	RISK Default View Add one or more resource filters									
NETWORK	97 DEPLOYMENTS Page 1 of 2									
VIOLATIONS										
COMPLIANCE										
RISK										
IMAGES										
SECRETS										
CONFIGURE										
HELP										
v2.4.22.0										
	Name	Updated	Cluster	Namespace	Priority					
	visa-processor	06/13/2019   11:37:13AM	production	payments	1					
	asset-cache	06/13/2019   11:38:57AM	production	frontend	2					
	backend-atlas	06/13/2019   11:38:49AM	production	backend	3					
	mastercard-processor	06/13/2019   11:38:13AM	production	payments	4					
	jump-host	06/13/2019   11:39:10AM	production	operations	5					
	fluentd-gcp-v3.2.0	06/13/2019   11:30:53AM	production	kube-system	6					
	monitor	06/13/2019   11:38:58AM	production	frontend	7					
	fluentd-gcp-v3.2.0	06/13/2019   11:30:19AM	security	kube-system	8					
	reporting	06/13/2019   11:39:03AM	production	medical	9					
	wordpress	06/13/2019   11:38:57AM	production	frontend	10					
	puppet-master	06/13/2019   11:39:10AM	production	operations	11					
	sensor	06/13/2019   11:36:20AM	production	stackrox	12					
	collector	06/13/2019   11:36:11AM	security	stackrox	13					

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.

# 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

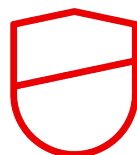
## Relevant use-cases for StackRox you can have a conversation on day 1

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

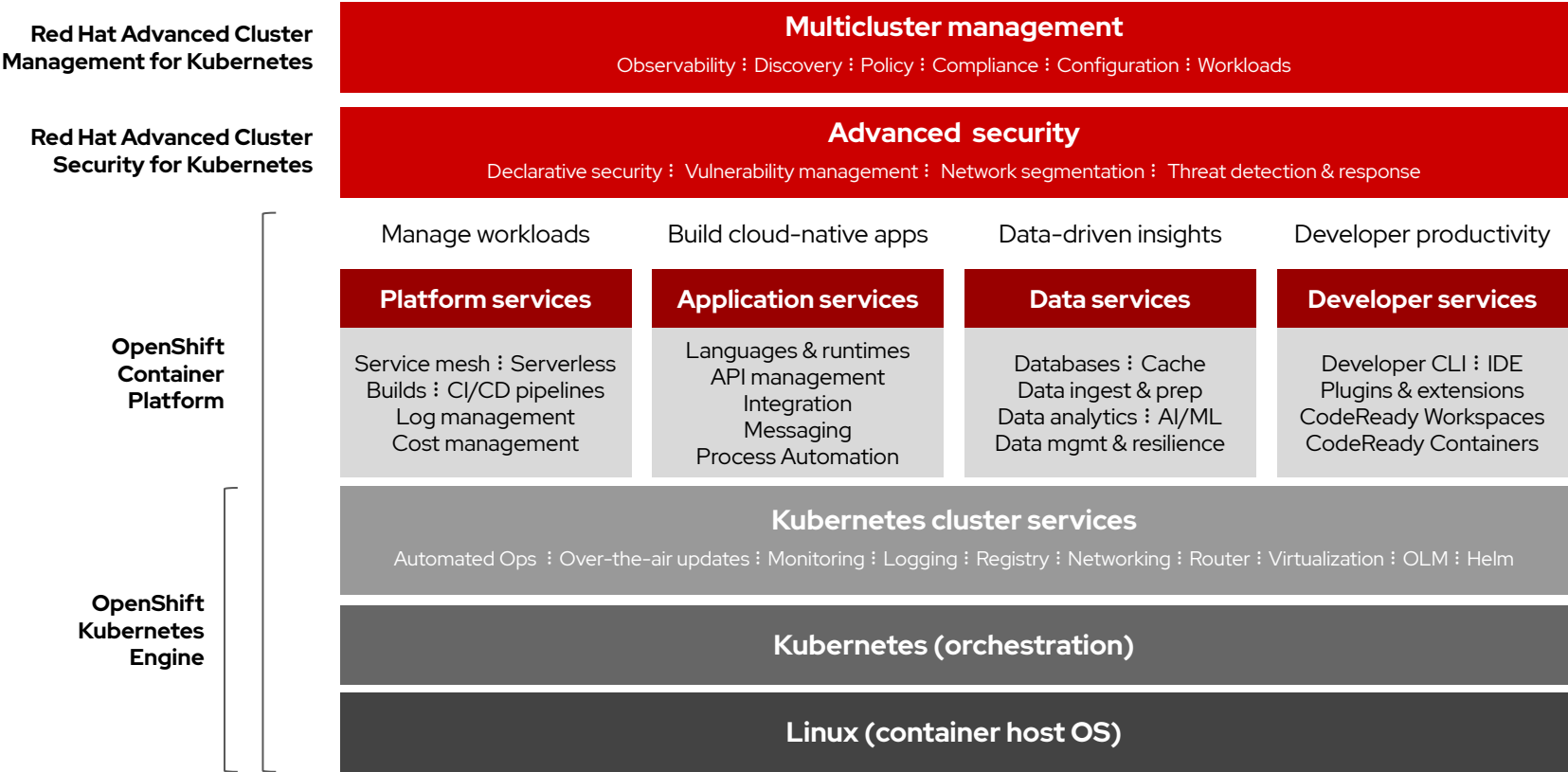
Monitor for and respond to anomalous application behavior. Leverage deep data collection and correlation to identify threats and enable forensic analysis.



---

# RHACS and RHACM

# Enterprise Kubernetes from Red Hat



# 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](https://linkedin.com/company/red-hat)

 [youtube.com/user/RedHatVideos](https://youtube.com/user/RedHatVideos)

 [facebook.com/redhatinc](https://facebook.com/redhatinc)

 [twitter.com/RedHat](https://twitter.com/RedHat)