



StackRox | Red Hat ACS

Alfred Bach

Principal Solution Architect - Cloud, Security & DC- Infrastructure

Partner Enablement Team EMEA

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

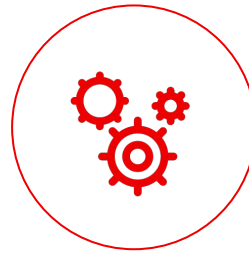
Security

Benefits of a Kubernetes-native approach to security



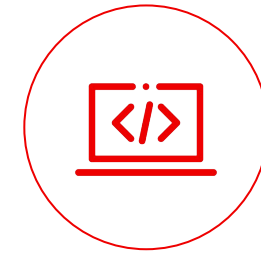
Lower operational cost

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

Extend scanning and compliance into development (DevSecOps)

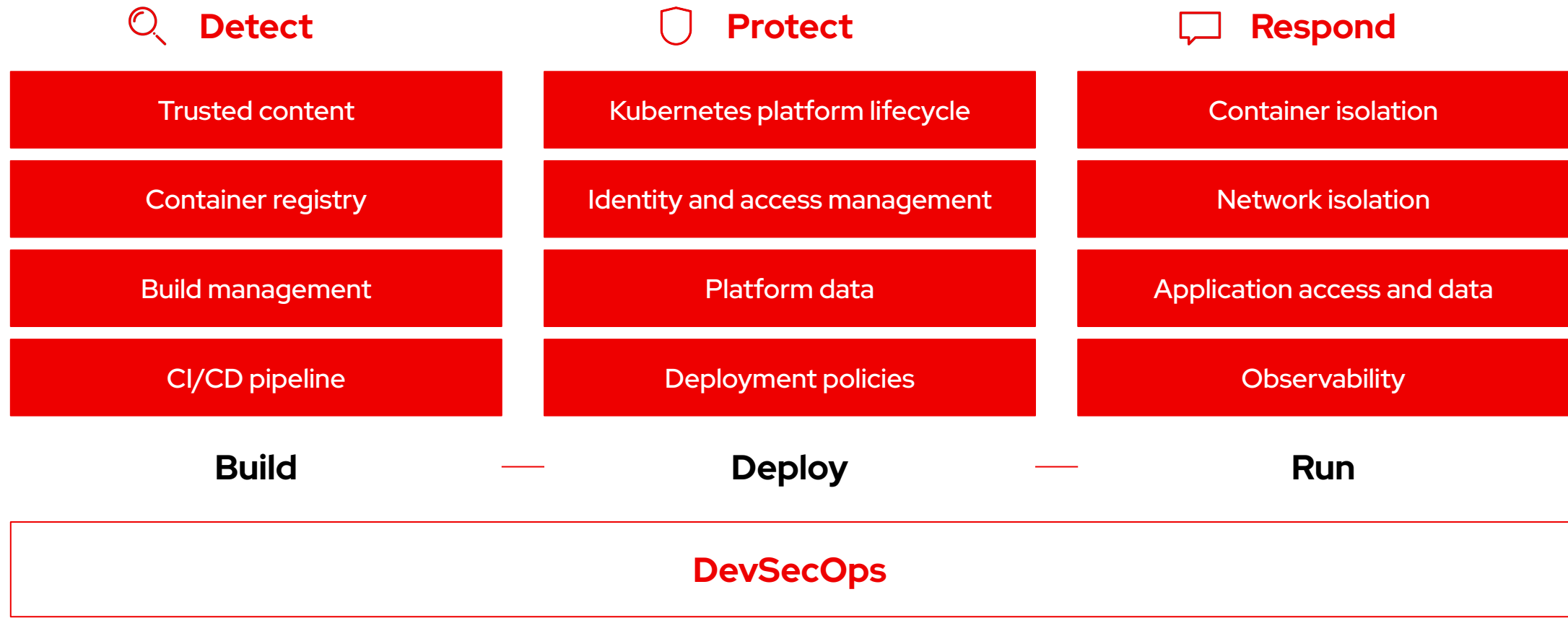
Secure infrastructure

Leverage built-in Kubernetes CSPM to identify and remediate risky configurations

Secure workloads

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

| |
|--------------------|
| 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 |

Vulnerability analysis

App config analysis

APIs for CI/CD integrations

Image assurance and policy admission controller

Compliance assessments

Risk profiling

Runtime behavioral analysis

Auto-suggest network policies

Threat detection / incident response

Build

Deploy

Run

DevSecOps

RHACS

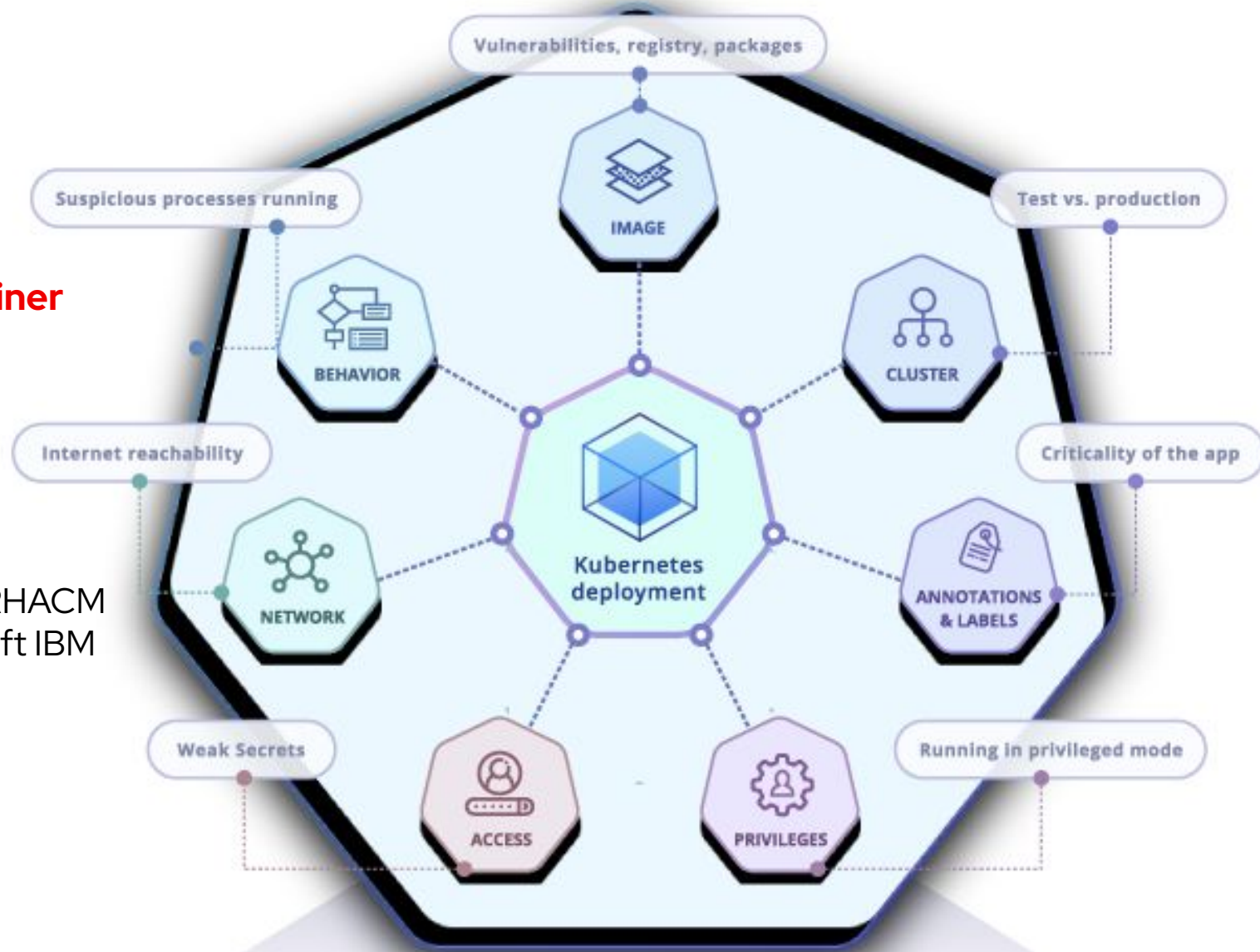
Securing Kubernetes Deployments

It's all about the Application in the container

- plus a Registry Scanner.

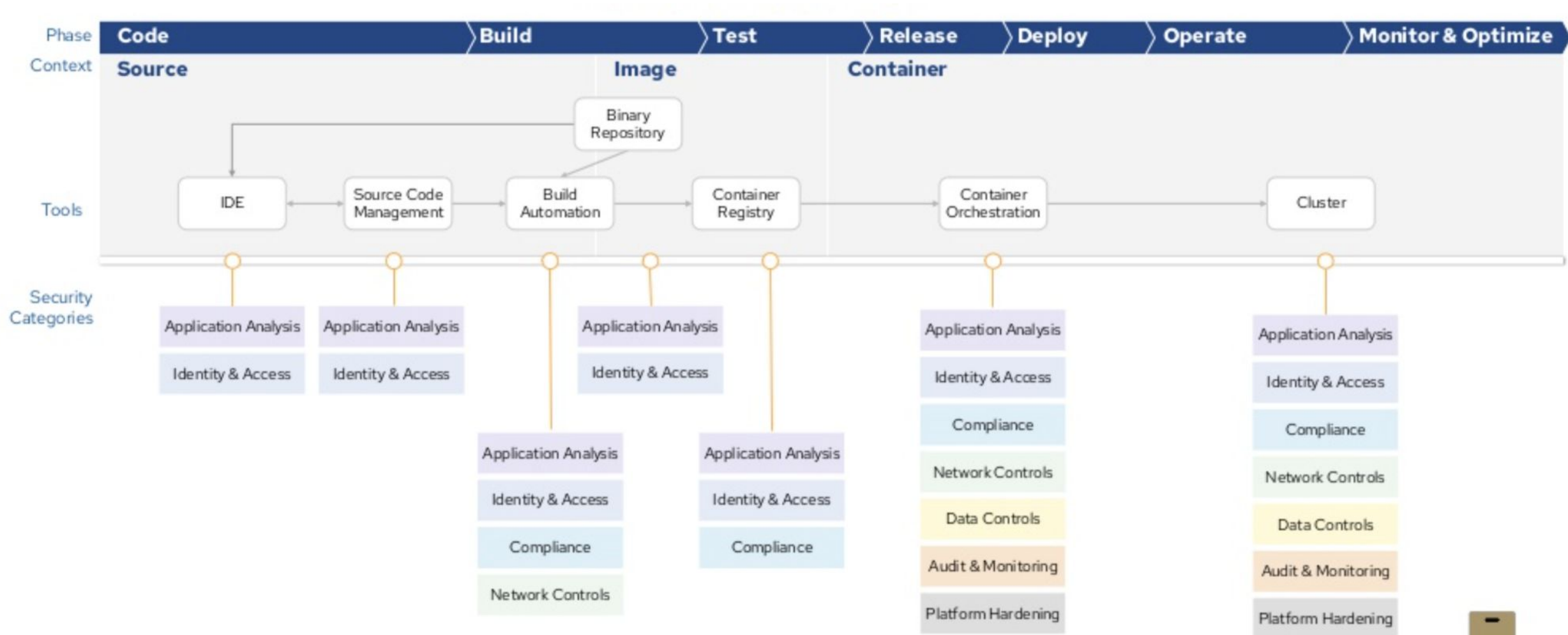
It's not:

- 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

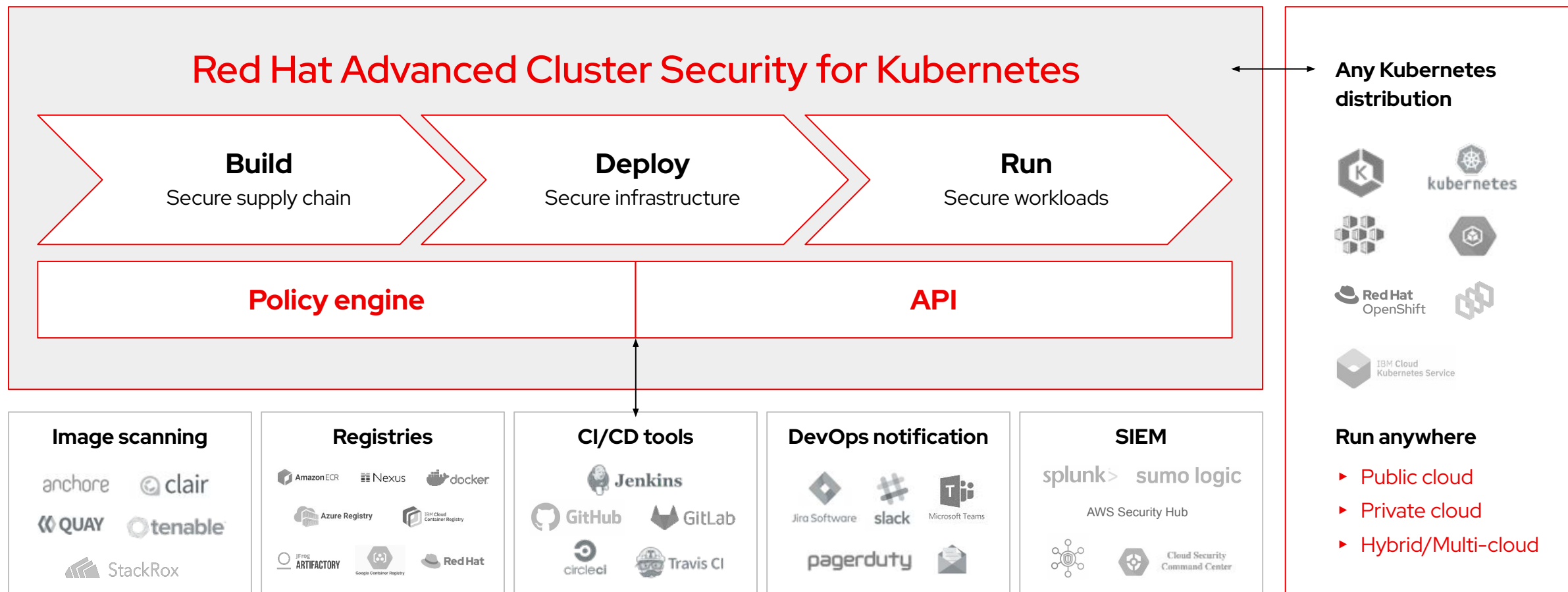


RHACS

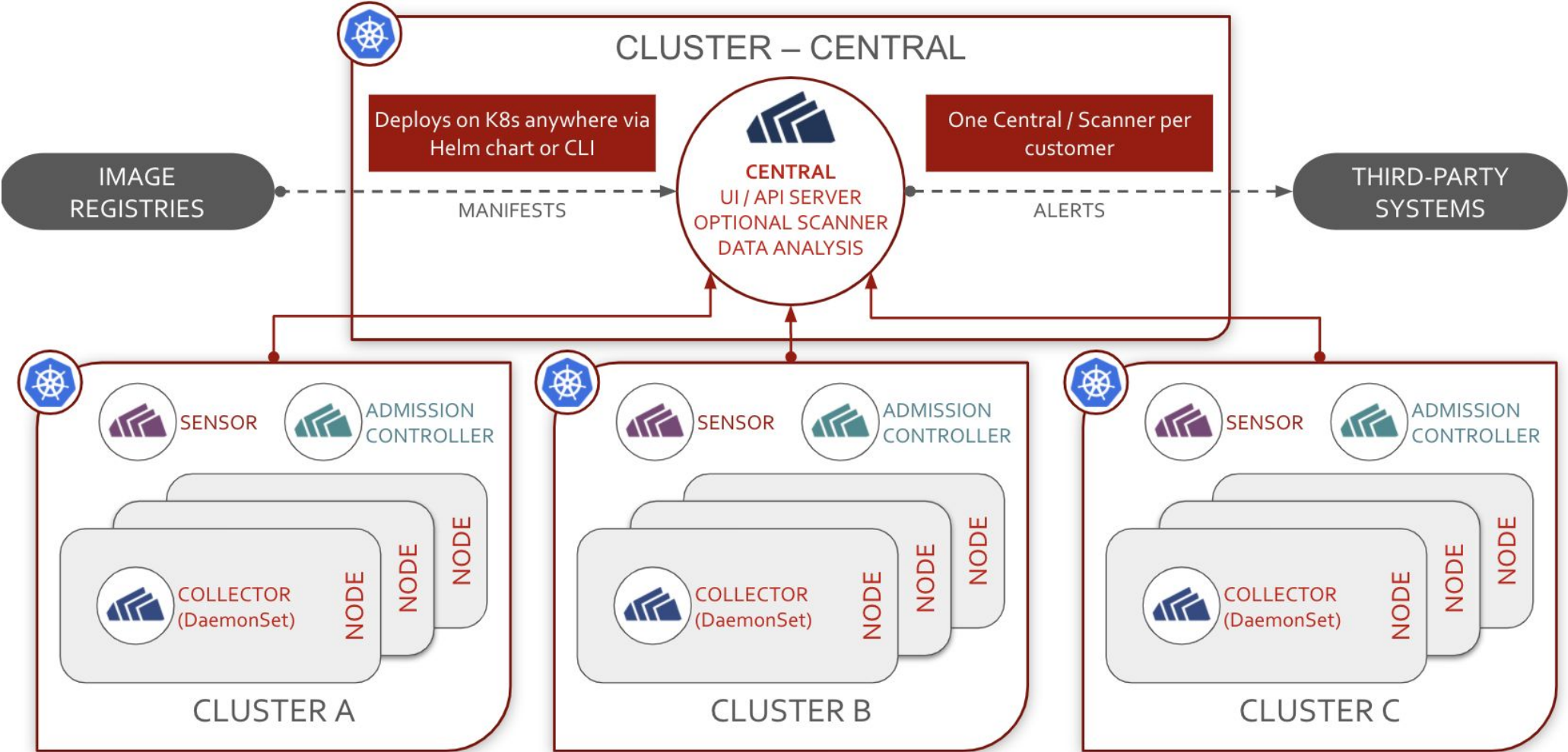
adding security to dev ops for your kubernetes native applications



The first Kubernetes-native security platform



Architecture





Dashboard

Network Graph

Violations

Compliance

Vulnerability Management

Configuration Management

Risk

Platform Configuration



DASHBOARD

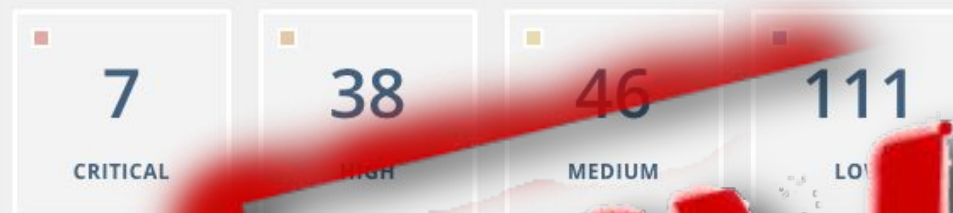
Default View



Add one or more resource filters



202 SYSTEM VIOLATIONS

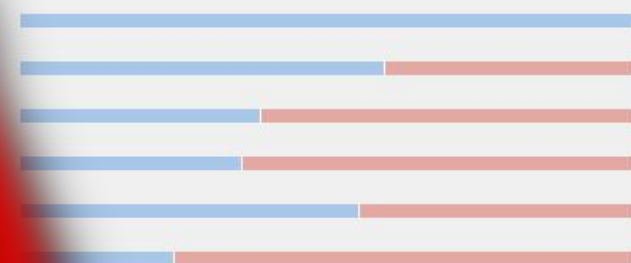


COMPLIANCE

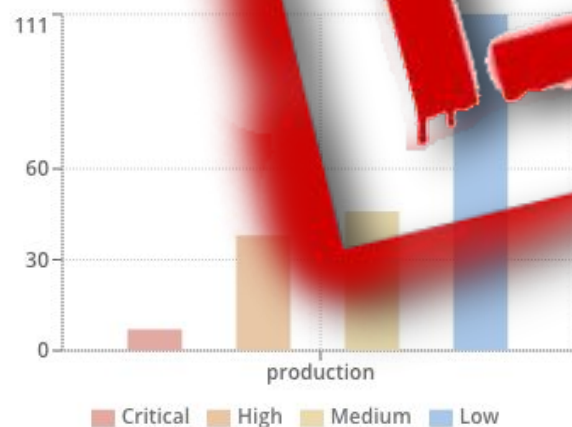
[CIS Docker v1.2.0](#)

[CIS Kubernetes v1.5](#)

[NIST SP 800-190](#)



VIOLATIONS BY CLUSTER



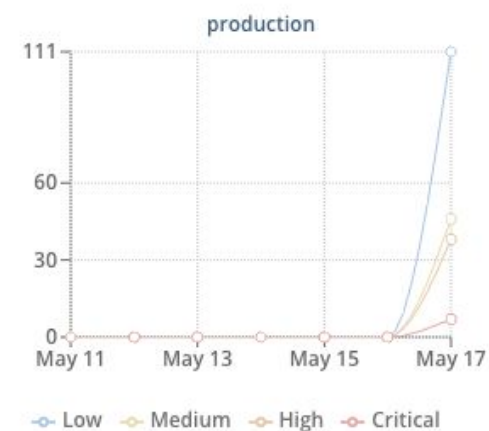
TOP DEPLOYMENTS

[VIEW ALL](#)

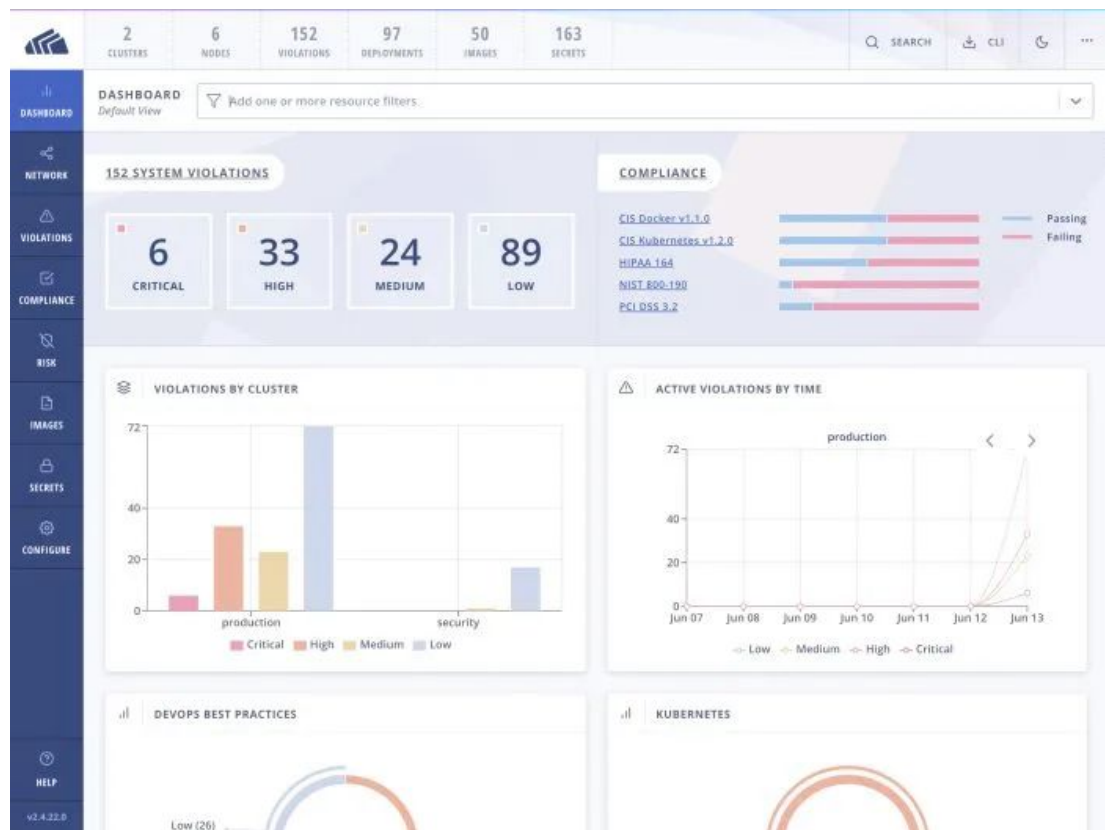
| | |
|----------------------|--------------------|
| visa-processor | 05/17 8:56:37 AM |
| backend-atlas | 05/17 8:56:27 AM |
| asset-cache | 05/17 8:56:29 AM |
| mastercard-processor | 05/17 8:56:37 AM |
| jump-host | 05/17 8:56:34 AM |



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 | Q SEARCH | CLI | ... |
| | CLUSTERS | NODES | VIOLATIONS | DEPLOYMENTS | IMAGES | SECRETS | | | |
| DASHBOARD | IMAGES Default View <input type="text" value="Add one or more resource filters"/> | | | | | | | | |
| NETWORK | 50 IMAGES Page 1 of 1 | | | | | | | | |
| VIOLATIONS | | | | | | | | | |
| COMPLIANCE | | | | | | | | | |
| RISK | | | | | | | | | |
| IMAGES | | | | | | | | | |
| SECRETS | | | | | | | | | |
| CONFIGURE | | | | | | | | | |
| HELP | | | | | | | | | |
| vs. 4.32.0 | | | | | | | | | |

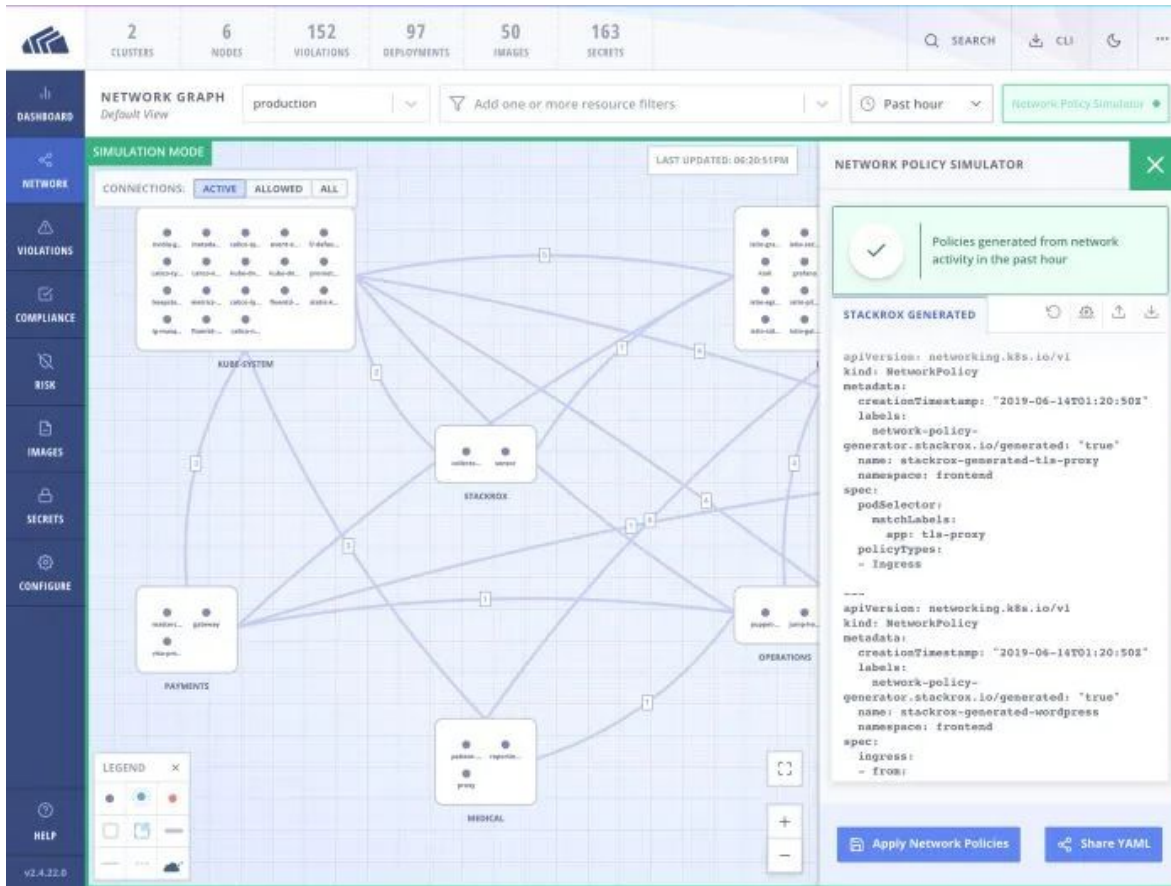
| Image | Created at | Components | CVEs ↓ | Fixable CVE |
|---|-------------------------|------------|--------|-------------|
| us.gcr.io/ultra-current-825/struts-violations/visa-processor:latest | 03/29/2019 1:33:22AM | 223 | 428 | 221 |
| us.gcr.io/ultra-current-825/struts-violations/mastercard-processor:latest | 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/fluentd-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 Apache... | 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 | |

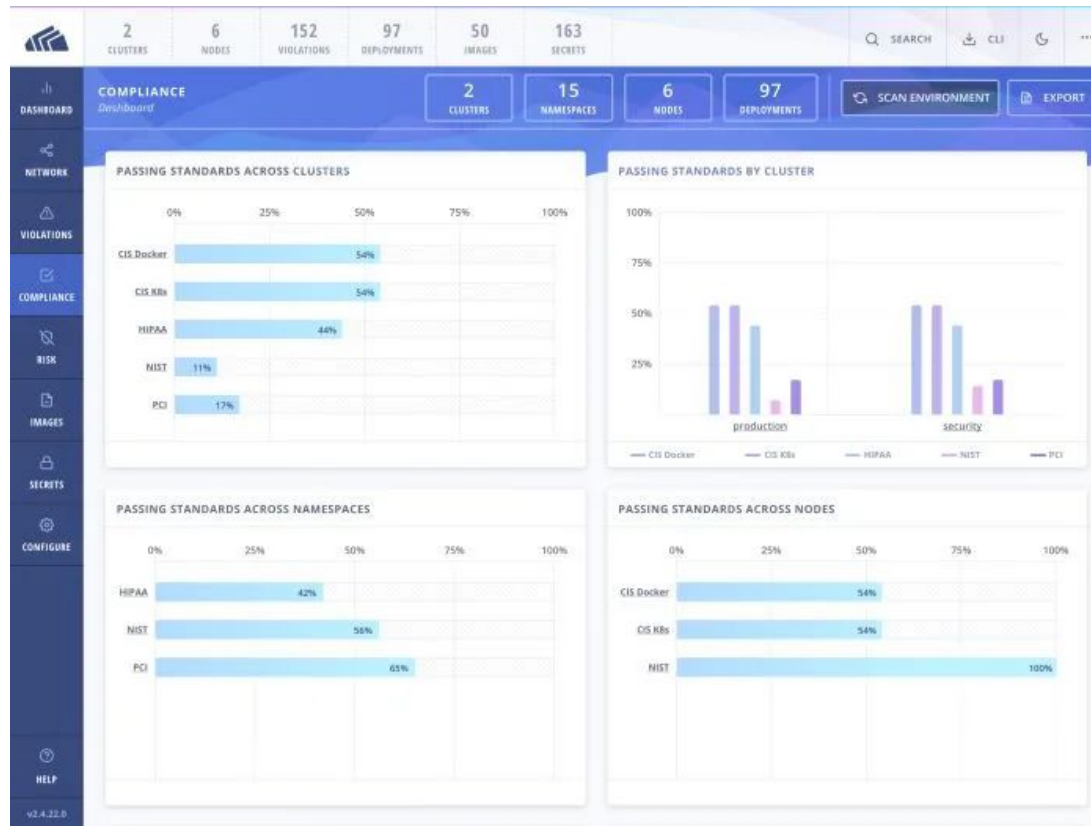
Protect your containers against vulnerabilities from the time images are built until they're deployed and running. StackRox can block vulnerable images from being deployed and integrates with your approved registries, including OpenShift Container Registry (OCR), for granular policy enforcement. StackRox 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 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 (selected), Images, Secrets, Configure, and Help. The main content area is titled 'RISK' and shows a 'Filtered View' for the deployment 'mastercard-processor'. 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' (listing apt, bash, curl, netcat), 'Number of Components in Image' (323 components), 'Image Freshness' (217 days old), and 'RBAC Configuration' (service account 'default' configured).

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

| | | | | | | | | | | | | | | | | | | | | | | |
|---|----------------------------------|-------|------------|-------------|--------|---------|--|----------|-----|---|---|--|--|--|--|--|--|--|--|--|--|--|
| | 2 | 6 | 152 | 97 | 50 | 163 | | Q SEARCH | CLI | 🔄 | ⋮ | | | | | | | | | | | |
| | CLUSTERS | NODES | VIOLATIONS | DEPLOYMENTS | IMAGES | SECRETS | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | | |
| DASHBOARD | VIOLATIONS | | | | | | | | | | | | | | | | | | | | | |
| NETWORK | Default View | | | | | | | | | | | | | | | | | | | | | |
| VIOLATIONS | Add one or more resource filters | | | | | | | | | | | | | | | | | | | | | |
| COMPLIANCE | | | | | | | | | | | | | | | | | | | | | | |
| RISK | | | | | | | | | | | | | | | | | | | | | | |
| IMAGES | | | | | | | | | | | | | | | | | | | | | | |
| SECRETS | | | | | | | | | | | | | | | | | | | | | | |
| CONFIGURE | | | | | | | | | | | | | | | | | | | | | | |
| HELP | | | | | | | | | | | | | | | | | | | | | | |
| v1.4.22.0 | | | | | | | | | | | | | | | | | | | | | | |
| 152 VIOLATIONS | | | | | | | | | | | | | | | | | | | | | | |
| Page 1 of 4 | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |

Risk prioritization at scale

| | | | | | | | | | | | |
|---|---|-------------------------|------------|-------------|----------|---|--------------------|-------------------|-----|---|---|
| | 2 | 6 | 152 | 97 | 50 | 163 | | Q SEARCH | CLJ | ↺ | ⋮ |
| | CLUSTERS | NODES | VIOLATIONS | DEPLOYMENTS | IMAGES | SECRETS | | | | | |
|  | RISK | | | | | | | | | | |
| DASHBOARD | Default View Add one or more resource filters | | | | | | | | | | |
|  | 97 DEPLOYMENTS | | | | | | | | | | |
| NETWORK | Page 1 of 2 | | | | | | | | | | |
|  | Name | Updated | Cluster | Namespace | Priority | VISA-PROCESSOR | | | | | |
| VIOLATIONS | visa-processor | 06/13/2019 11:37:13AM | production | payments | 1 | RISK INDICATORS | DEPLOYMENT DETAILS | PROCESS DISCOVERY | | | |
|  | asset-cache | 06/13/2019 11:38:57AM | production | frontend | 2 | Policy Violations | | | | | |
| COMPLIANCE | backend-atlas | 06/13/2019 11:38:49AM | production | backend | 3 | Apache Struts: CVE-2017-5638 (severity: Critical) | | | | | |
|  | mastercard-processor | 06/13/2019 11:38:13AM | production | payments | 4 | Fixable CVSS >= 6 and Privileged (severity: High) | | | | | |
| RISK | jump-host | 06/13/2019 11:39:10AM | production | operations | 5 | Fixable CVSS >= 7 (severity: High) | | | | | |
|  | fluentd-gcp-v3.2.0 | 06/13/2019 11:30:53AM | production | kube-system | 6 | Process with UID 0 (severity: High) | | | | | |
| IMAGES | monitor | 06/13/2019 11:38:58AM | production | frontend | 7 | Secure Shell (ssh) Port Exposed (severity: High) | | | | | |
|  | reporting | 06/13/2019 11:39:03AM | production | medical | 9 | Shell Spawned by Java Application (severity: High) | | | | | |
| SECRETS | wordpress | 06/13/2019 11:38:57AM | production | frontend | 10 | Netcat Execution Detected (severity: Medium) | | | | | |
|  | puppet-master | 06/13/2019 11:39:10AM | production | operations | 11 | No resource requests or limits specified (severity: Medium) | | | | | |
| CONFIGURE | sensor | 06/13/2019 11:36:20AM | production | stackrox | 12 | Privileged Container (severity: Medium) | | | | | |
|  | collector | 06/13/2019 11:36:11AM | security | stackrox | 13 | Curl in Image (severity: Low) | | | | | |
| HELP | | | | | | Latest tag (severity: Low) | | | | | |
| v2.4.22.0 | | | | | | Ubuntu Package Manager Execution (severity: Low) | | | | | |
| | | | | | | Ubuntu Package Manager in Image (severity: Low) | | | | | |
| | | | | | | Wget in Image (severity: Low) | | | | | |

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

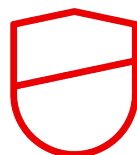
Relevant use-cases for StackRox you can have a conversation on day 1

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.



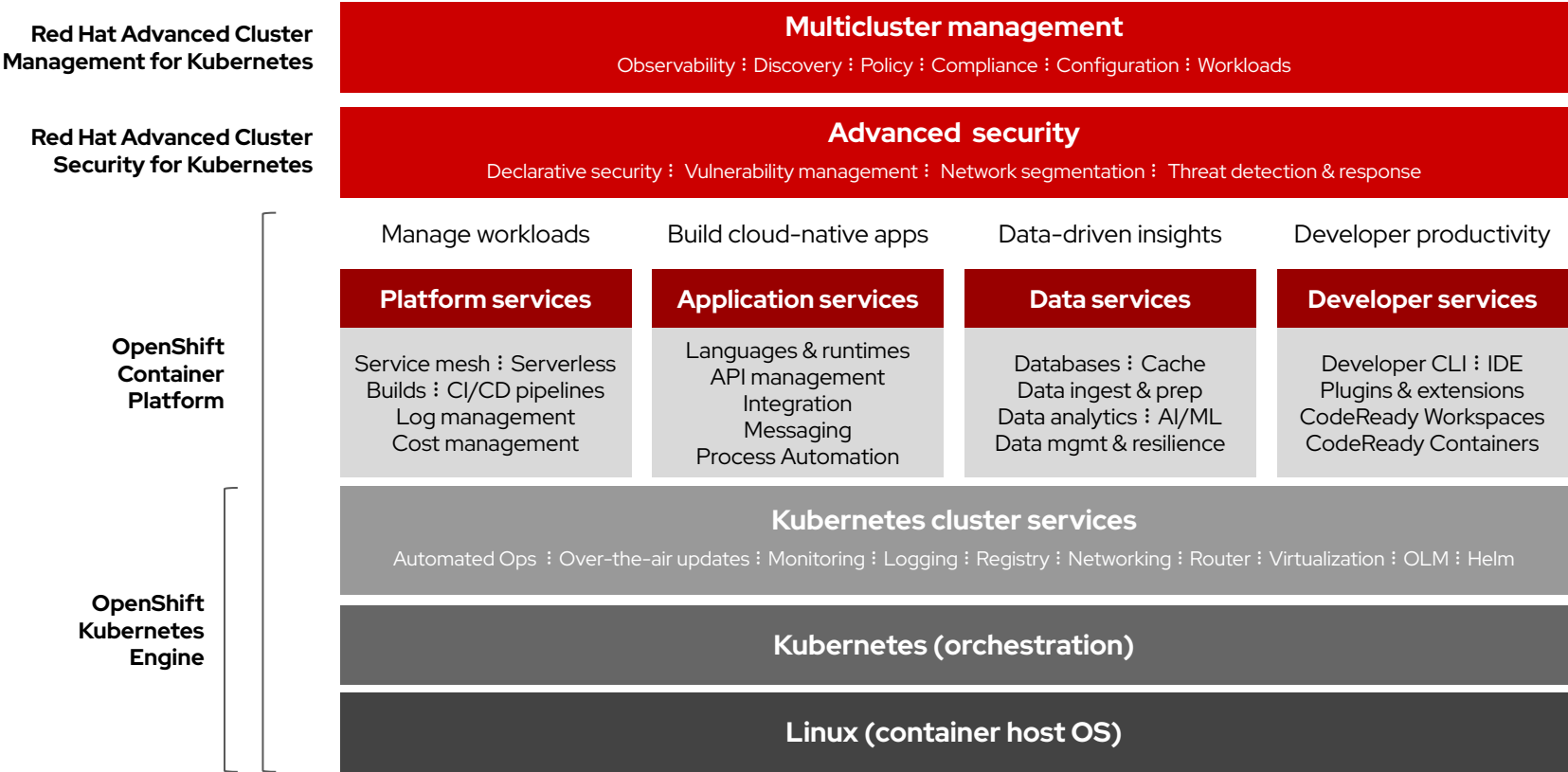
Respond

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

Multicloud 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