FOSDEM 2023

Demystifying StackRox

Unlock zero trust cloud-native security in Kubernetes

Rutvik Kshirsagar
STSE, Red Hat
(OpenShift | StackRox)

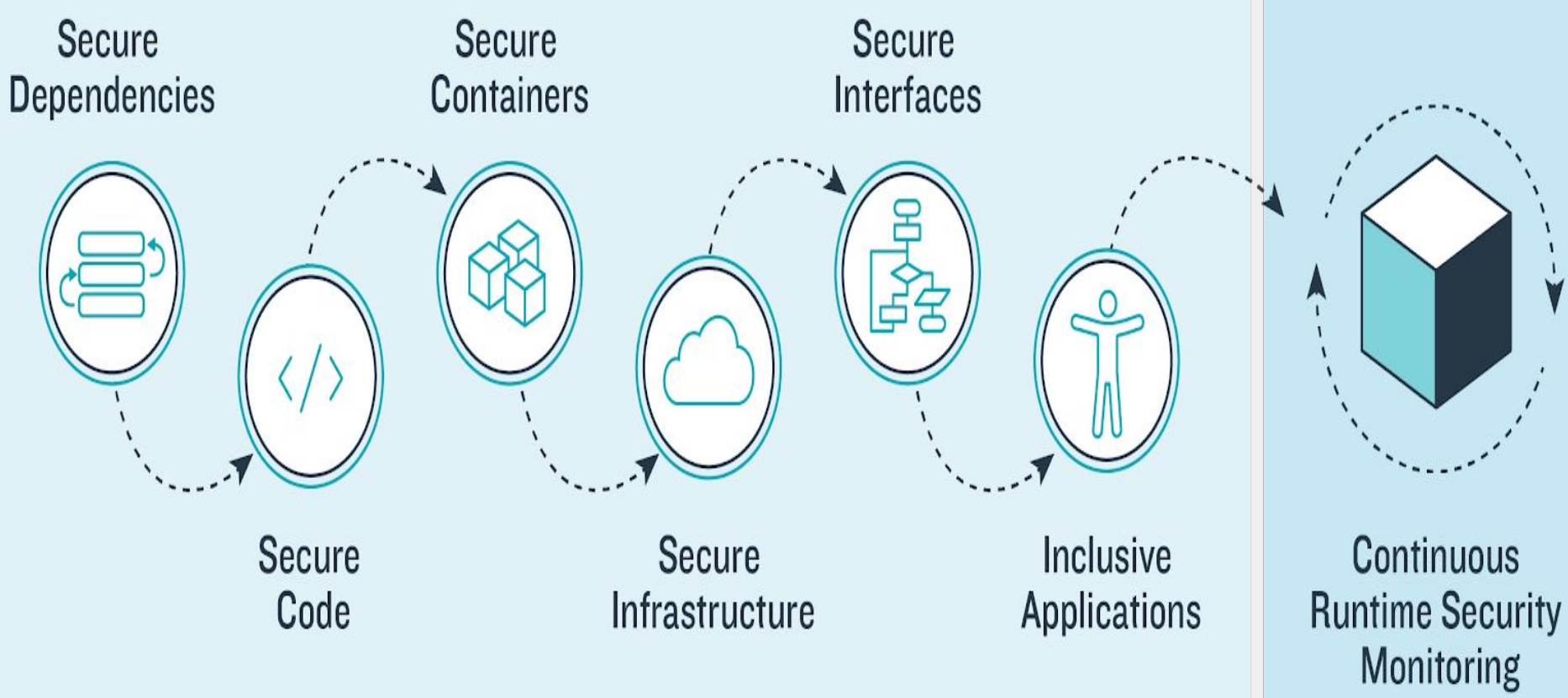
What we'll discuss today

- Trusted Software Supply Chain
- State of Kubernetes Security
- Need of DevSecOps for Containers and K8s
- Kubernetes Security risks and challenges
- Demystifying StackRox
- Scanning Container Images
- Managing Compliance and Hardening
- Using Collector along with eBPF Probes
- Securing Network Policies at Scale
- Integrating Admission Controller
- Demo
- Benefits of a Kubernetes-native approach to security

What is Zero Trust Security in the Kubernetes ecosystem?

Red Hat

Trusted Software Supply Chain



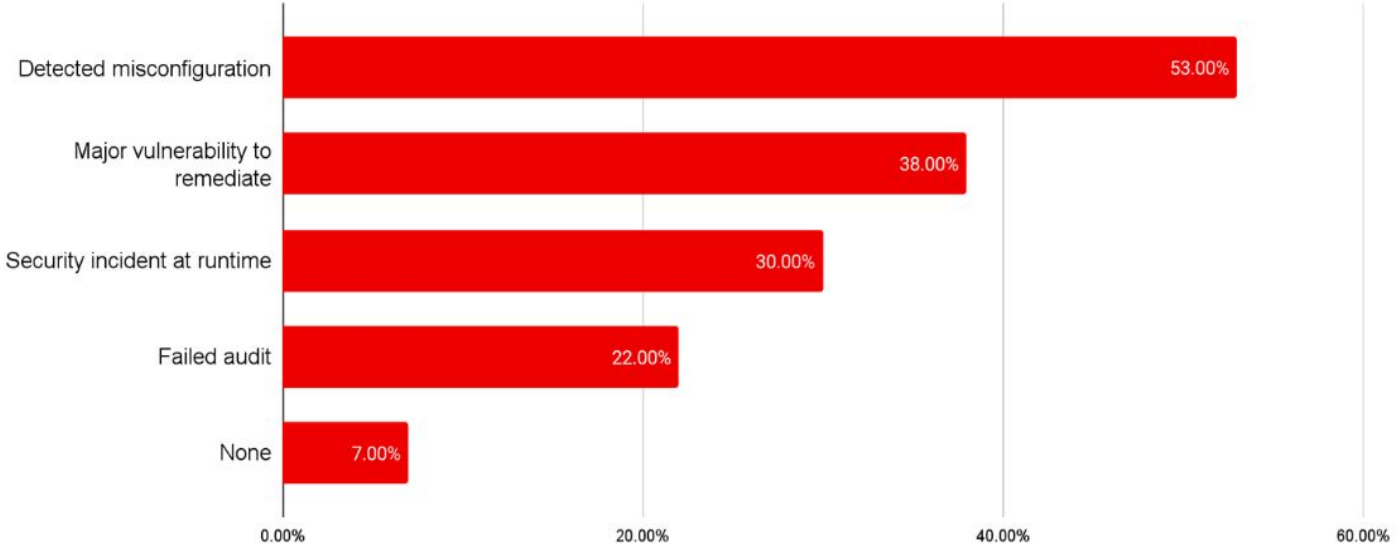
Have you ever delayed or slowed down application deployment into production due to container or Kubernetes security concerns?

Red Hat

State of Kubernetes Security

Most common types of security incidents

Software supply chain directly impacted by misconfigurations and vulnerabilities



Source:
State of Kubernetes Security 2022

Red Hat

Containers and Kubernetes needs DevSecOps

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

Kubernetes security risks and challenges

- Containers are numerous and everywhere, and they may pose compliance challenges
- Images and image registries, when misused, can pose security issues
- Containers talk to each other and to other endpoints
- Kubernetes offers rich configuration options, but defaults are usually the least secure

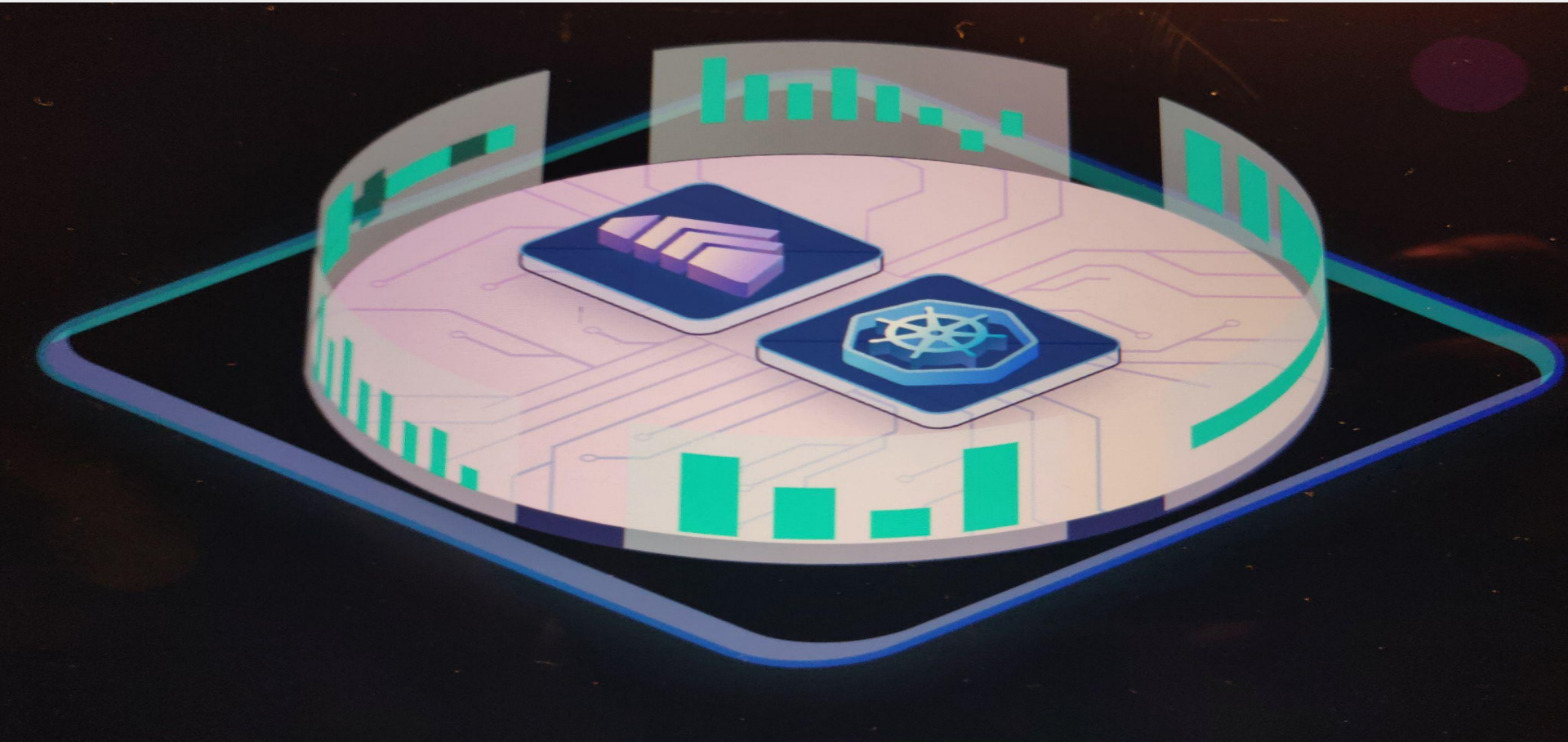
Kubernetes Security Best Practices

- Build Phase
  - Use minimal base images
  - Use an image scanner to identify known vulnerabilities
  - Integrate security into your CI/CD pipeline

- Deploy Phase
  - Use Kubernetes network policies to control traffic between pods and clusters
  - Assess the privileges used by containers
  - Extend your image scanning to deploy phase

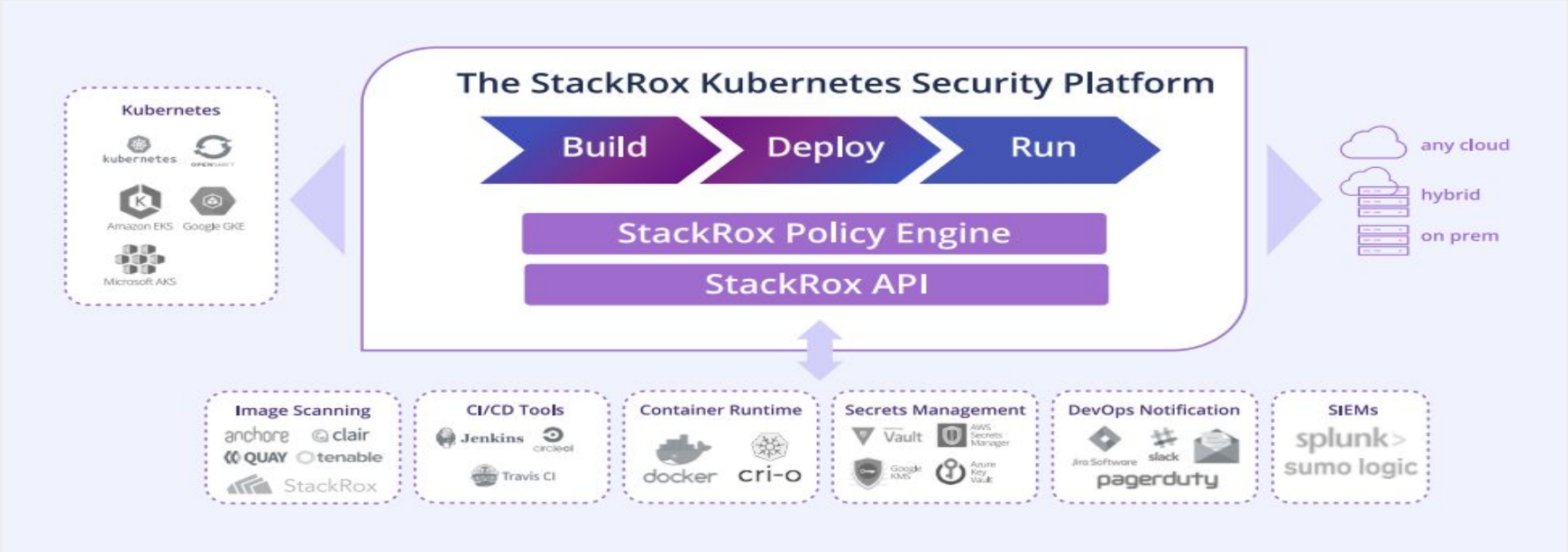
- **Runtime Phase**
  - Extend vulnerability scanning to running deployments
  - Monitor network traffic to limit unnecessary or insecure communication
  - Compare and analyze different runtime activity in pods of the same deployments

Why StackRox is OpenSource?



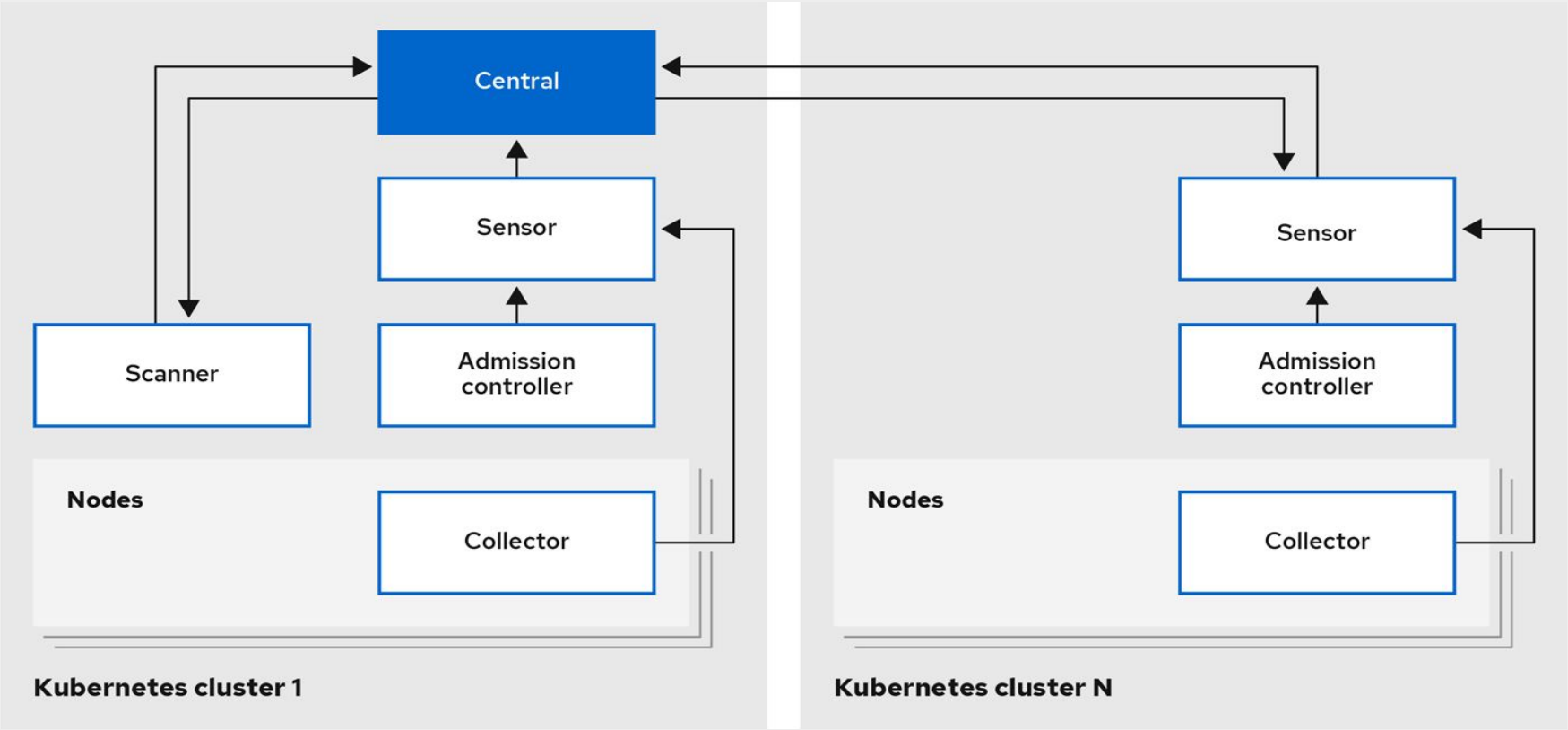
Demystifying StackRox

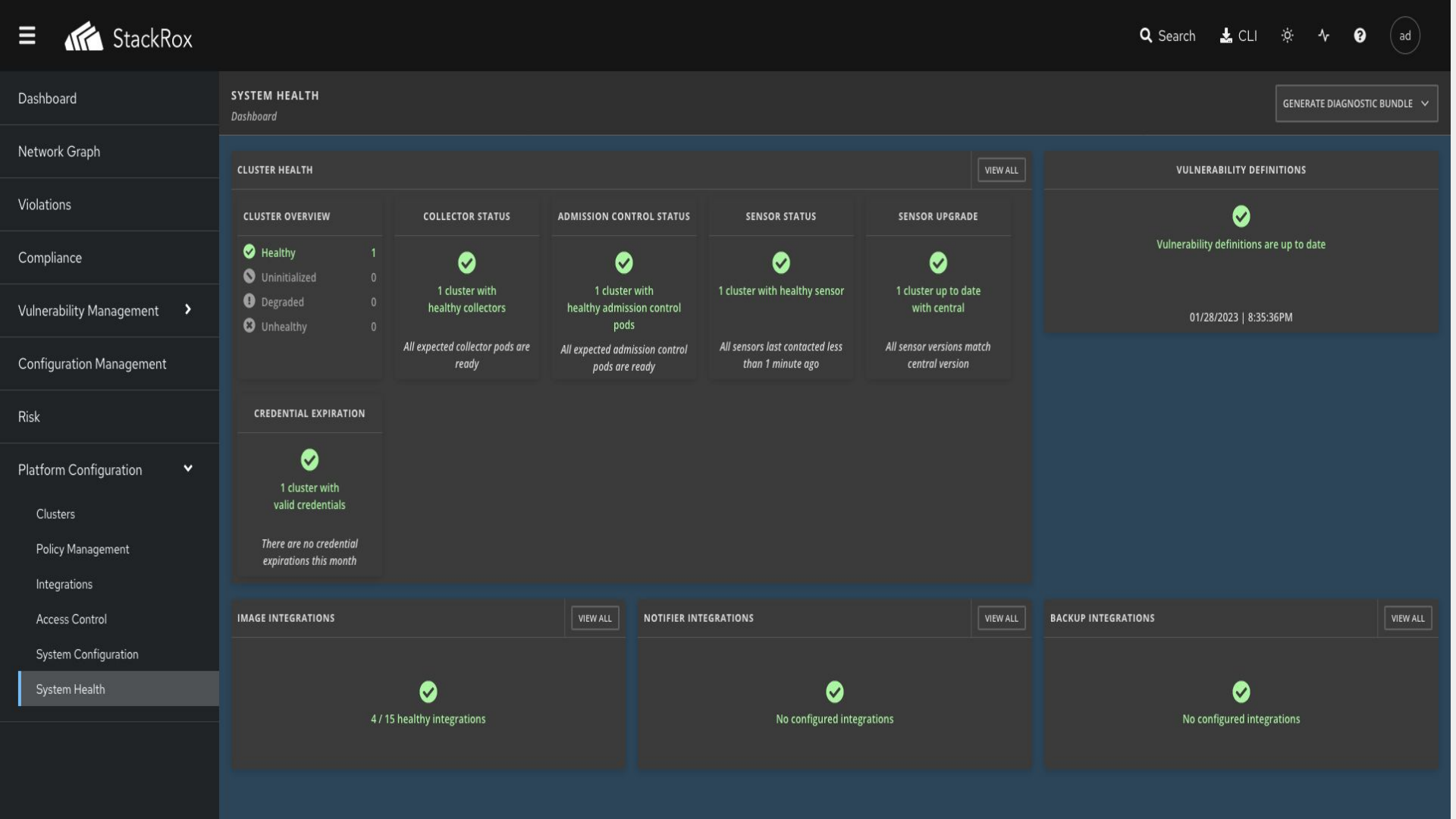
- It enable users to address all significant security use cases across the entire application lifecycle, including visibility, vulnerability management, configuration management, network segmentation, compliance, threat detection, incident response, and risk profiling



Red Hat

Architecture




StackRox
Search
CLI
ad
Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Configuration Management
Risk
Platform Configuration
Clusters
Policy Management
Integrations
Access Control
System Configuration
System Health
SYSTEM HEALTH
Dashboard
GENERATE DIAGNOSTIC BUNDLE
CLUSTER HEALTH
VIEW ALL
CLUSTER OVERVIEW
Healthy 1
Uninitialized 0
Degraded 0
Unhealthy 0
COLLECTOR STATUS
1 cluster with healthy collectors
All expected collector pods are ready
ADMISSION CONTROL STATUS
1 cluster with healthy admission control pods
All expected admission control pods are ready
SENSOR STATUS
1 cluster with healthy sensor
All sensors last contacted less than 1 minute ago
SENSOR UPGRADE
1 cluster up to date with central
All sensor versions match central version
CREDENTIAL EXPIRATION
1 cluster with valid credentials
There are no credential expirations this month
VULNERABILITY DEFINITIONS
Vulnerability definitions are up to date
01/28/2023 | 8:35:36PM
IMAGE INTEGRATIONS
VIEW ALL
4 / 15 healthy integrations
NOTIFIER INTEGRATIONS
VIEW ALL
No configured integrations
BACKUP INTEGRATIONS
VIEW ALL
No configured integrations

Problem Statements

1. Will the container content compromise my infrastructure?
2. Are there known vulnerabilities in the application layer?
3. Are the runtime and OS layers in the container up to date?
4. Is my Kubernetes Cluster Compliant with Industry Certified Security Benchmarks?

Scanning Container Images for Vulnerabilities

StackRox Scanner identifies the vulnerabilities in the:

- Base image operating system
- Packages that are installed by the package managers
- Programming language specific dependencies
- Programming runtimes and frameworks

Supported package formats:

- yum
- microdnf
- apt
- apk
- dpkg
- RPM

Supported operating systems:

- Alpine Linux
- Amazon Linux
- Centos
- Ubuntu
- Debian
- Red Hat Enterprise Linux

Red Hat

Managing Compliance

You can run out-of-the-box compliance scans based on industry standards including:

- CIS Benchmarks (Center for Internet Security) for Docker and Kubernetes
- HIPAA (Health Insurance Portability and Accountability Act)
- NIST Special Publication 800-190 and 800-53 (National Institute of Standards and Technology)
- PCI DSS (Payment Card Industry Data Security Standard)

By scanning your environment based on these standards you can:

- Evaluate your infrastructure for regulatory compliance.
- Harden your Docker Engine and Kubernetes orchestrator.
- Understand and manage the overall security posture of your environment.
- Get a detailed view of compliance status for clusters, namespaces, and nodes.

Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Configuration Management
Risk
Platform Configuration

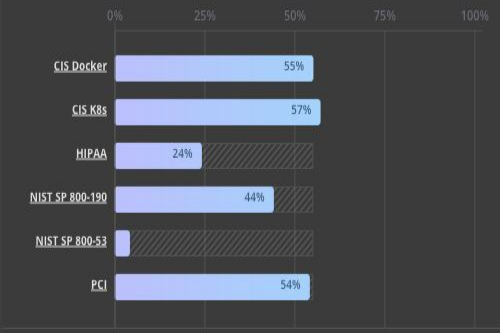
COMPLIANCE

Dashboard

1 CLUSTER (Scanned) | 48 NAMESPACES (Scanned) | 6 NODES (Scanned) | 118 DEPLOYMENTS (Scanned)

SCAN ENVIRONMENT | EXPORT

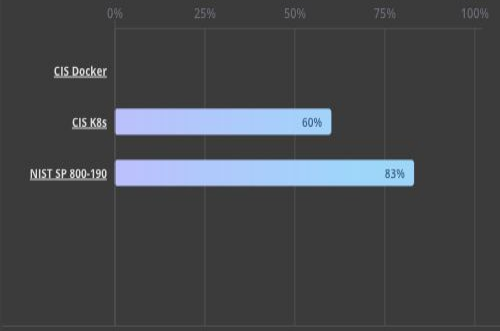
PASSING STANDARDS ACROSS CLUSTERS



PASSING STANDARDS BY CLUSTER

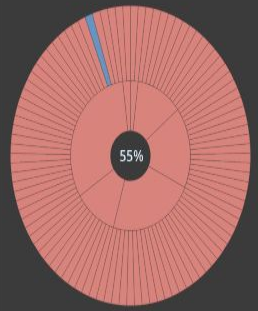
PASSING STANDARDS ACROSS NAMESPACES

PASSING STANDARDS ACROSS NODES



CIS DOCKER V1.2.0 COMPLIANCE

VIEW STANDARD

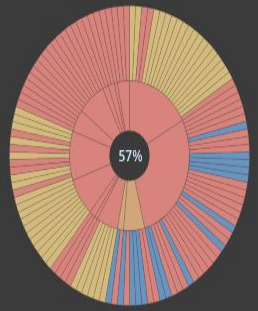


7 Categories

97 Controls

CIS KUBERNETES V1.5 COMPLIANCE

VIEW STANDARD



15 Categories

122 Controls

Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Configuration Management
Risk
Platform Configuration

CIS KUBERNETES V1.5
Standard

Standard: X | CIS Kubernetes v1.5 X

SCAN | EXPORT

122 CONTROLS ACROSS 1 CLUSTER

my-secured-cluster — 122 CONTROLS

Control ↑	Compliance
1.1.1 - Ensure that the API server pod specification file permissions are set to 644 or more restrictive	83%
1.1.2 - Ensure that the API server pod specification file ownership is set to root:root	83%
1.1.3 - Ensure that the controller manager pod specification file permissions are set to 644 or more restrictive	83%
1.1.4 - Ensure that the controller manager pod specification file ownership is set to root:root	83%
1.1.5 - Ensure that the scheduler pod specification file permissions are set to 644 or more restrictive	83%
1.1.6 - Ensure that the scheduler pod specification file ownership is set to root:root	83%
1.1.7 - Ensure that the etcd pod specification file permissions are set to 644 or more restrictive	83%
1.1.8 - Ensure that the etcd pod specification file ownership is set to root:root	83%
1.1.9 - Ensure that the Container Network Interface file permissions are set to 644 or more restrictive	0%
1.1.10 - Ensure that the Container Network Interface file ownership is set to root:root	83%
1.1.11 - Ensure that the etcd data directory permissions are set to 700 or more restrictive	0%
1.1.12 - Ensure that the etcd data directory ownership is set to etcd:etcd	0%
1.1.13 - Ensure that the admin.conf file permissions are set to 644 or more restrictive	83%
1.1.14 - Ensure that the admin.conf file ownership is set to root:root	83%

1.1.9 - ENSURE THAT THE CONTAINER NETWORK INTERFACE FILE PERMISSIONS ARE SET TO 644 OR MORE RESTRICTIVE

CONTROL DETAILS

Standard: CIS Kubernetes v1.5
Control: 1.1.9

Ensure that the Container Network Interface file permissions are set to 644 or more restrictive

CONTROL GUIDANCE

StackRox checks that the permissions of files in the CNI configuration and binary directories are set to at most '0644'

1 RELATED CLUSTER

VIEW ALL

my-secured-cluster

6 RELATED NODES

VIEW ALL

my-secured-cluster/master-1.rktes...	my-secured-cluster/master-0.rktes...
my-secured-cluster/worker-0.rktes...	my-secured-cluster/master-2.rktes...
my-secured-cluster/worker-1.rktes...	my-secured-cluster/worker-2.rktes...

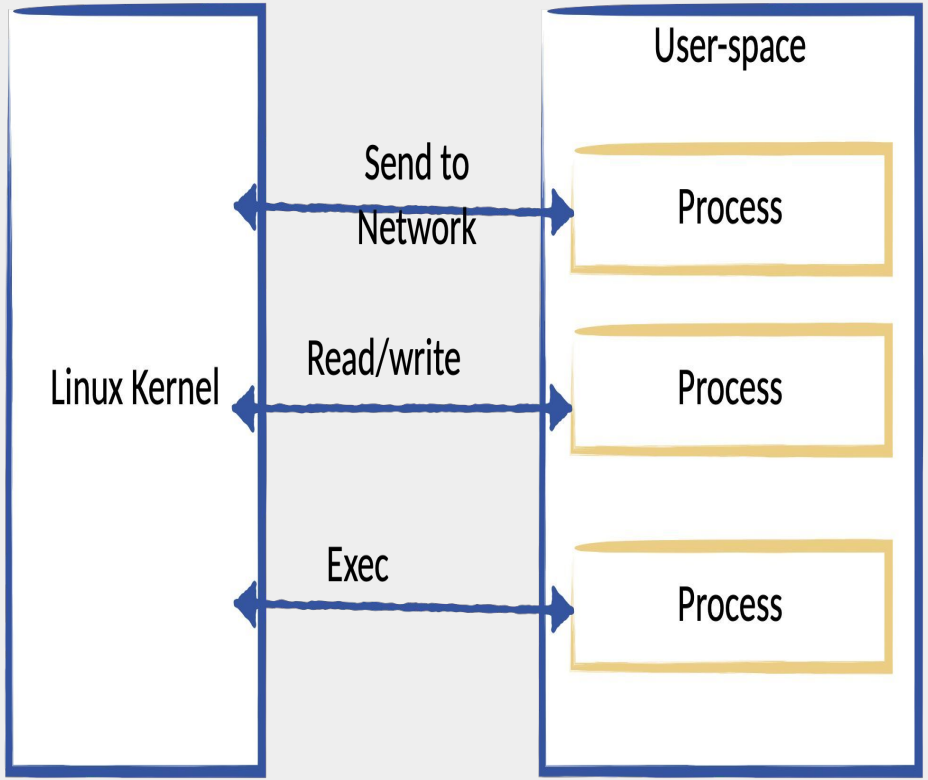
Collector

- It is an agent that runs on every node under strict performance limitations and gathers the data via kernel modules or eBPF probes (the default collection mode nowadays).
- Collector analyzes and monitors container activity on cluster nodes.
- It collects information about container runtime and network activity and sends the collected data to Sensor.
- To implement eBPF probes and collect data, the project leverages the Falco libraries via a custom fork.

What activity do we care about?

- Network Traffic
- File activity
- Running Executables
- Changing privileges

All these activities require support from the Kernel



Significance of eBPF Probes

What is eBPF?

Extended Berkeley Packet Filter

What can eBPF do?

- Networking
- Tracing & Profiling
- Observability & Monitoring
- Security

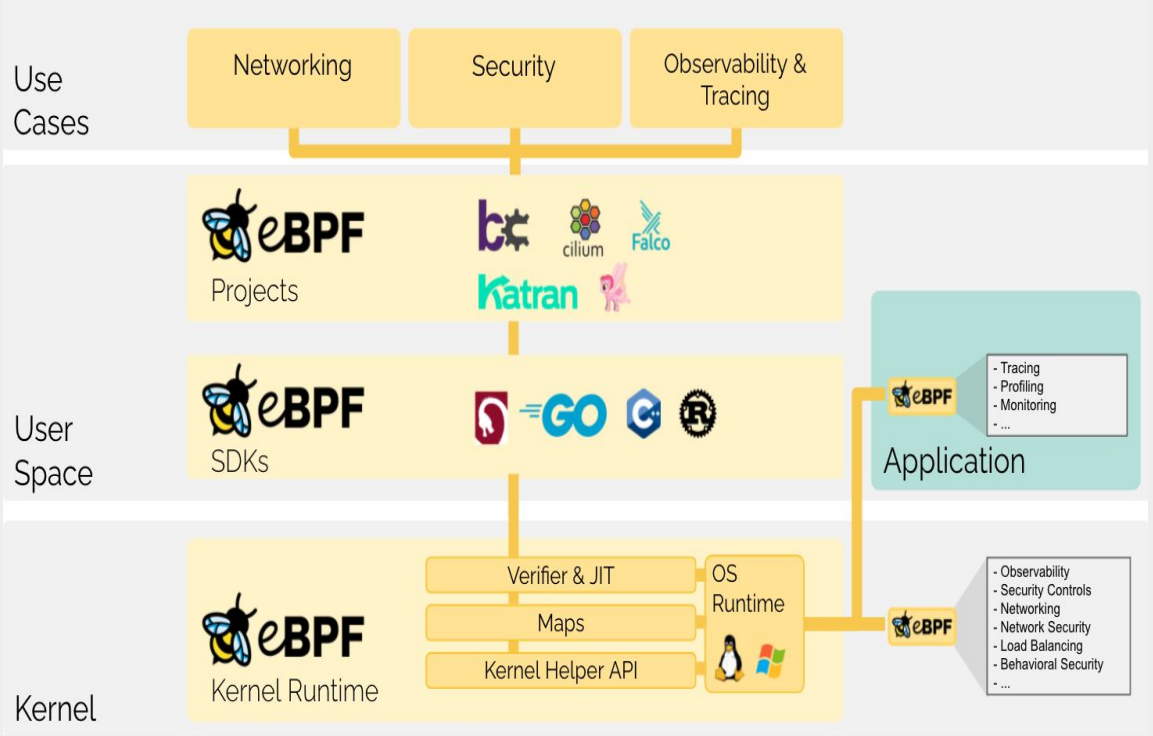


Image source: https://ebpf.io/what-is-ebpf/

Red Hat

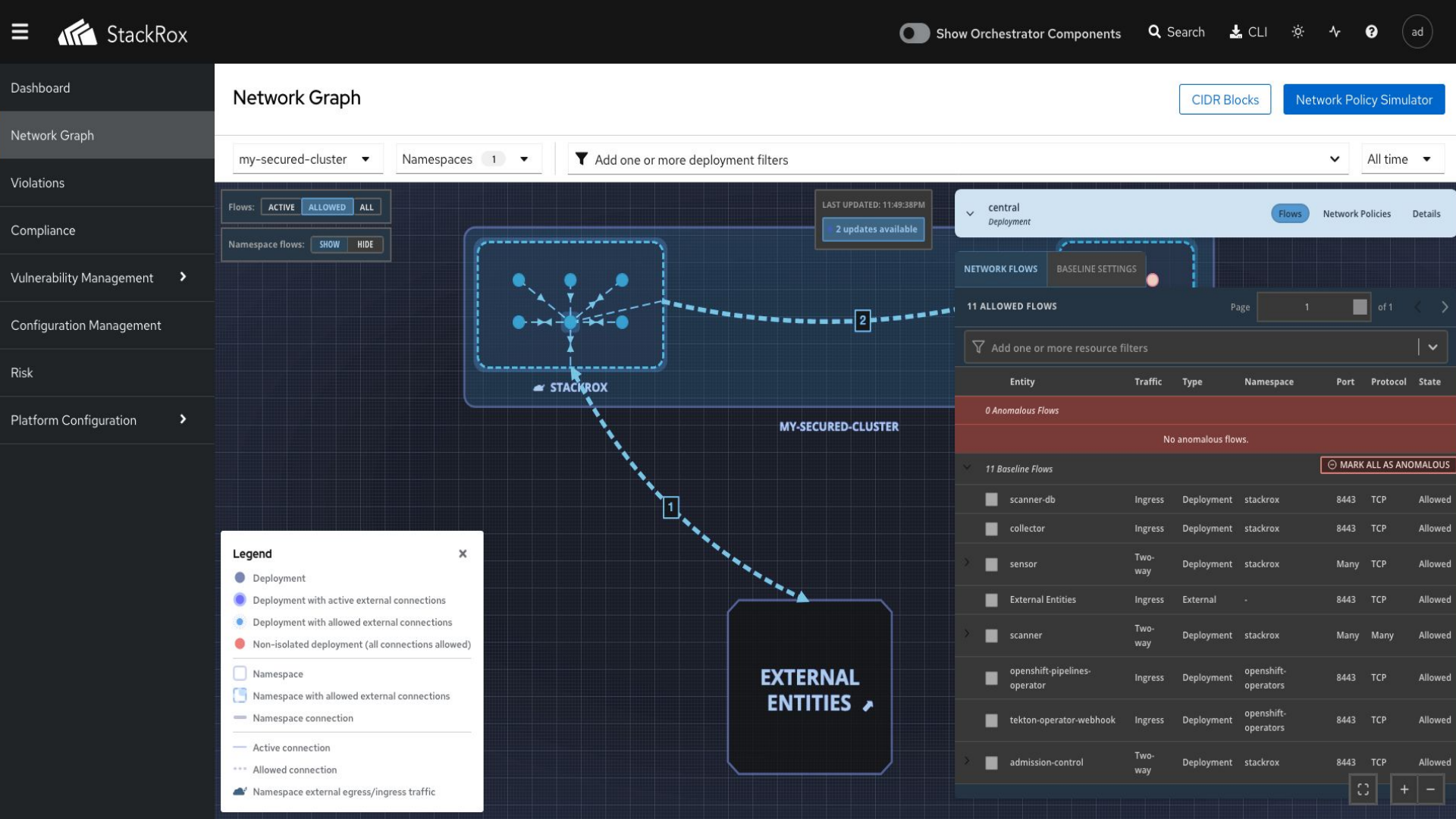
Securing Network Policies at Scale

- Network policies in Kubernetes are configured as YAML files.
- By looking at these files alone, it is often hard to identify whether the applied network policies achieve the desired network topology.
- StackRox gathers all defined network policies from your orchestrator and provides functionality to make these policies easier to use.

To support network policy enforcement, StackRox provides:

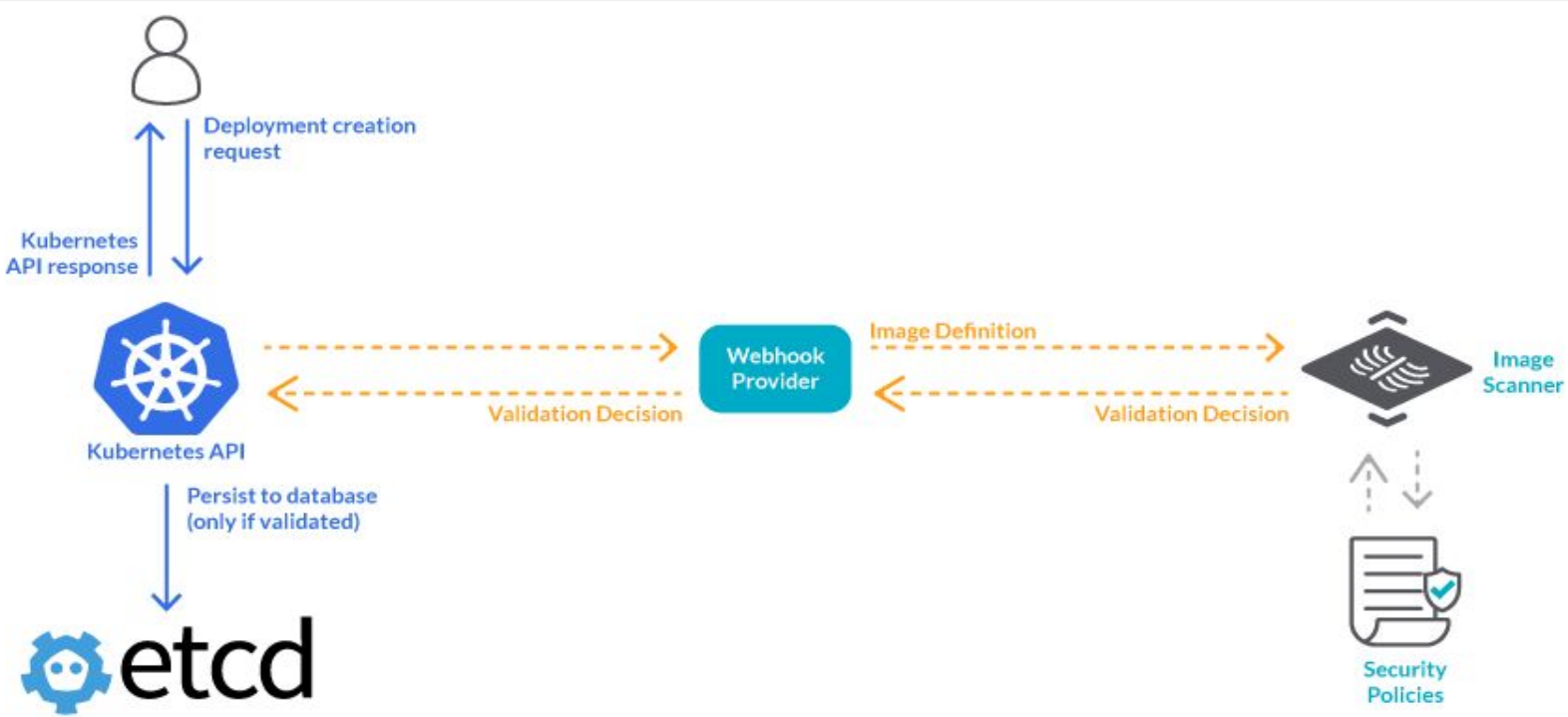
- Network segmentation
- Network graph
- Network policy simulator
- Network policy generator
- Build-time network policy generator

Red Hat


StackRox
Show Orchestrator Components
Search
CLI
ad
Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Configuration Management
Risk
Platform Configuration
Network Graph
CIDR Blocks
Network Policy Simulator
my-secured-cluster
Namespaces 1
Add one or more deployment filters
All time
Flows: ACTIVE ALLOWED ALL
Namespace flows: SHOW HIDE
LAST UPDATED: 11:49:38PM
2 updates available
central
Deployment
Flows
Network Policies
Details
NETWORK FLOWS
BASELINE SETTINGS
11 ALLOWED FLOWS
Page 1 of 1
Add one or more resource filters
Entity
Traffic
Type
Namespace
Port
Protocol
State
0 Anomalous Flows
No anomalous flows.
11 Baseline Flows
MARK ALL AS ANOMALOUS
scanner-db Ingress Deployment stackrox 8443 TCP Allowed
collector Ingress Deployment stackrox 8443 TCP Allowed
sensor Two-way Deployment stackrox Many TCP Allowed
External Entities Ingress External - 8443 TCP Allowed
scanner Two-way Deployment stackrox Many Many Allowed
openshift-pipelines-operator Ingress Deployment openshift-operators 8443 TCP Allowed
tekton-operator-webhook Ingress Deployment openshift-operators 8443 TCP Allowed
admission-control Two-way Deployment stackrox 8443 TCP Allowed
STACKROX
MY-SECURED-CLUSTER
EXTERNAL ENTITIES
1
2
Legend
Deployment
Deployment with active external connections
Deployment with allowed external connections
Non-isolated deployment (all connections allowed)
Namespace
Namespace with allowed external connections
Namespace connection
Active connection
Allowed connection
Namespace external egress/ingress traffic

Admission Controller

- StackRox works with the k8s admission controller to enforce security policies before Kubernetes creates workloads (for example, deployments, daemon-sets or jobs).



Demo

Terminate Log4Shell attack in a fraction of seconds!

Demo

Shift Left Security using Tekton (Cloud Native CI/CD) with StackRox

Image source: https://tekton.dev/

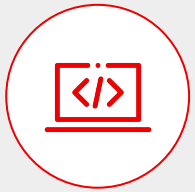
Benefits of a Kubernetes-native approach to Security

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

Step up with StackRox and Secure your kubernetes world!

How to get started?

- https://github.com/stackrox/stackrox#deploying-stackrox
- https://www.stackrox.io/docs/

Get involved with StackRox community:

- https://github.com/stackrox/stackrox#community
- Stay tuned for latest updates via StackRox Community Office Hours
- https://www.stackrox.io/slack/

References:

- What is eBPF?
- What is DevSecOps?
- Get Started with OpenSource StackRox Project
- A Guide to Kubernetes Admission Controllers
- StackRox Community Contribution
- 2022 state of Kubernetes security report

Red Hat

Questions?

Let’s connect
Twitter , Linkedin

Red Hat