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?
Trusted Software Supply Chain

- Secure Dependencies
- Secure Containers
- Secure Interfaces
- Inclusive Applications
- Continuous Runtime Security Monitoring
Have you ever delayed or slowed down application deployment into production due to container or Kubernetes security concerns?
State of Kubernetes Security

Most common types of security incidents

Software supply chain directly impacted by misconfigurations and vulnerabilities

- Detected misconfiguration: 53.00%
- Major vulnerability to remediate: 38.00%
- Security incident at runtime: 30.00%
- Failed audit: 22.00%
- None: 7.00%

Source: State of Kubernetes Security 2022
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
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 enables 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.
Architecture

Kubernetes cluster 1
- Scanner
- Admission controller
- Collector

Kubernetes cluster N
- Sensor
- Admission controller
- Collector

Central
- Sensor
- Admission controller

Nodes
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
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.
## 1.1.9 - Ensure that the Container Network Interface file permissions are set to 644 or more restrictive

<table>
<thead>
<tr>
<th>Control</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.9 - Ensure that the Container Network Interface file permissions are set to 644 or more restrictive</td>
<td>0%</td>
</tr>
<tr>
<td>1.1.10 - Ensure that the Container Network Interface file ownership is set to root:root</td>
<td>83%</td>
</tr>
<tr>
<td>1.1.11 - Ensure that the etcd data directory permissions are set to 700 or more restrictive</td>
<td>0%</td>
</tr>
<tr>
<td>1.1.12 - Ensure that the etcd data directory ownership is set to etc:crater</td>
<td>0%</td>
</tr>
<tr>
<td>1.1.13 - Ensure that the admin.conf file permissions are set to 644 or more restrictive</td>
<td>83%</td>
</tr>
<tr>
<td>1.1.14 - Ensure that the admin.conf file ownership is set to root:root</td>
<td>83%</td>
</tr>
</tbody>
</table>

**Control Guidance**

StackRox checks that the permissions of files in the CNI configuration and binary directories are set at most '0644'.
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.
All these activities require support from the Kernel.

What activity do we care about?

- Network Traffic
- File activity
- Running Executables
- Changing privileges
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/
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
Admission Controller

- StackRox works with the k8s admission controller to enforce security policies before Kubernetes creates workloads (for example, deployments, daemon-sets or jobs).
Terminate Log4Shell attack in a fraction of seconds!
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
Questions?

Let’s connect
Twitter, Linkedin