Securing Kubernetes and your Cloud-native Applications
with the industry’s only Kubernetes-native container security

Protecting cloud-native applications requires significant changes in how we approach security – we must apply controls earlier in the application development life cycle, leverage the infrastructure itself to apply controls, and keep up with ever-faster release schedules.

The StackRox Kubernetes Security Platform protects your vital applications across build, deploy, and runtime. Our software deploys in your infrastructure and integrates with your DevOps tooling and workflows to deliver frictionless security and compliance. The StackRox Policy Engine includes hundreds of built-in controls to enforce DevOps and security best practices, industry standards such as CIS Benchmarks and NIST, configuration management of both containers and Kubernetes, and runtime security.

Only StackRox provides a Kubernetes-native architecture for container security, enabling DevOps and InfoSec teams to operationalize security.

Kubernetes-native security gives you:

**Rich context**
StackRox pulls declarative data from Kubernetes to improve every security use case from visibility to configuration management to risk profiling.

**Kubernetes-native controls**
StackRox taps the controls built into Kubernetes to enforce security policies, from admission control to network segmentation to scaling services to zero.

**Scale and portability**
Just as Kubernetes enables portability across all your environments, the StackRox platform ensures you apply security policies consistently.

Get the peace of mind your peers enjoy
Visibility
- Delivers a comprehensive view of your deployments, including images, pods, and configurations
- Discovers and displays network traffic in all clusters spanning namespaces, deployments, and pods
- Captures critical system-level events in each container

Vulnerability management
- Scans images for known vulnerabilities based on specific languages and packages and by image layer
- Correlates vulnerabilities to running deployments, not just images
- Enforces policies based on vulnerability details – at build time using CI/CD integrations, at deploy time using dynamic admission controls, and at runtime using native Kubernetes controls

Compliance
- Assesses compliance across hundreds of controls for CIS Benchmarks, PCI, HIPAA, and NIST SP 800-190
- Delivers at-a-glance dashboards of overall compliance across each standard's controls with evidence export to meet auditors' needs
- Enables drill down into compliance details to pinpoint clusters, nodes, or namespaces that don't comply with specific standards and controls

Network segmentation
- Visualizes allowed vs. active traffic between namespaces, deployments, and pods, including showing external exposures
- Simulates network policy changes before they're implemented to minimize operational risk to the environment
- Baselines network activity and recommends new Kubernetes network policies to remove unnecessary network connections
- Leverages network enforcement capabilities built into Kubernetes to ensure consistent, portable, and scalable segmentation

Risk profiling
- Ranks your running deployments according to their security risk, leveraging Kubernetes data to prioritize vulnerabilities using configuration or deployment details as well as runtime activity
- Tracks improvements in your security posture of your Kubernetes deployments to validate the impact of your security team's actions

Configuration management
- Delivers pre-built DevOps and Security policies to identify configuration violations related to network exposures, privileged containers, processes running as root, and compliance with industry standards
- Analyzes Kubernetes RBAC settings to determine user or service account privileges and misconfigurations
- Tracks secrets and which deployments use them to limit access
- Enforces configuration policies – at build time with CI/CD integration and at deploy time using dynamic admission control

Runtime detection and response
- Monitors system-level events within containers to detect anomalous activity indicative of a threat with automated response using Kubernetes-native controls
- Baselines process activity in containers to automatically whitelist processes, eliminating the need to manually whitelist
- Leverages pre-built policies to detect crypto mining, privilege escalation and various exploits
- Enables flexible system-level data collection using either eBPF or a kernel module across every major Linux distribution

Integrations
- Provides a rich API and pre-built plugins to integrate with DevOps systems, including CI/CD tools, image scanners, registries, container runtimes, SIEMs, and notification tools

Platform Architecture

---

©2020 StackRox, Inc. All rights reserved.