StackRox

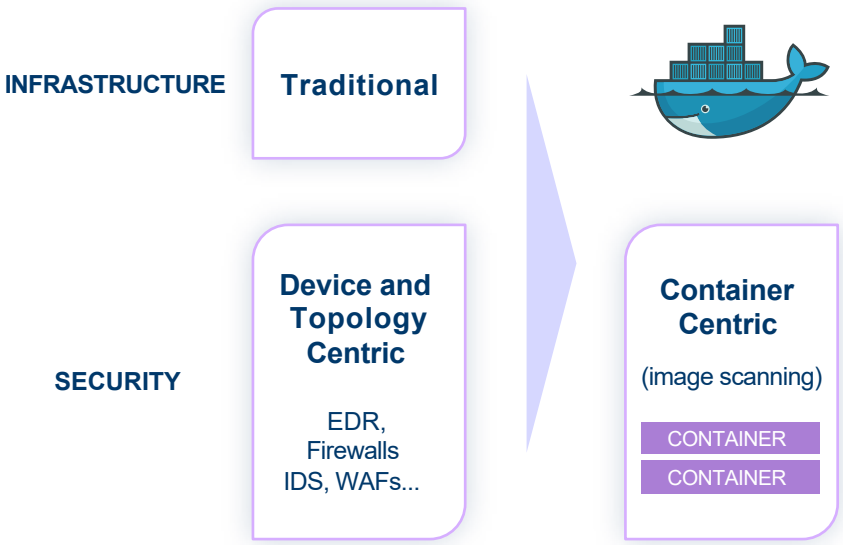
Solution Brief

Cloud-native security for containers and Kubernetes

To accelerate business innovation, companies have rapidly adopted DevOps methodologies and the cloud-native architecture to bring more speed, iteration, and portability to application development. Containers and microservices initiated a seismic shift in application infrastructure, and Kubernetes has emerged as one of the most quickly adopted technologies ever, helping companies automate the management of these application building blocks. This massive change in infrastructure has driven a parallel change in security, as new tooling and processes are needed to apply controls to the cloud-native stack.

Security in containerized environments

Organizations quickly recognized that containers introduce new security risks and attack vectors. Gartner has even listed container security as one of their top 10 security projects of 2019. A generation of container-centric security technologies emerged, providing a container- and image-centric approach, where traditional host vulnerability scanning gave way to container image scanning.



"Security can't be an afterthought. It needs to be embedded in the DevOps process … across the entire life cycle, which includes the build and development process, as well as deployment and run phase of an application."

– Gartner: Best Practices for Running Containers and Kubernetes in Production

Gartner

But the infrastructure has already undergone yet another sea change, therefore the focus on containers alone is no longer sufficient and must shift towards Kubernetes and containers. Kubernetes enhances container operability, automation, and scalability, but it also changes security requirements once again.

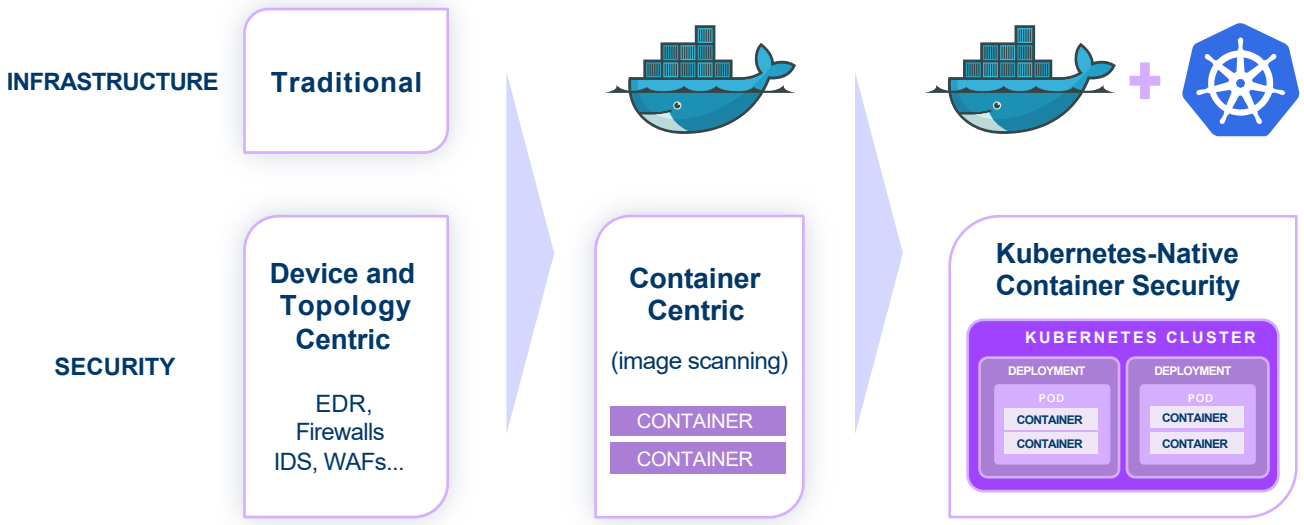
In today's Kubernetes world, it's no longer adequate to secure just your images and containers - you need a security platform that protects your entire Kubernetes environment.

Security in a container and Kubernetes world

The container-centric approach to securing cloud-native infrastructure falls short in three critical areas:

- **Limited visibility:** these solutions can see only images, image components, and running containers; in other words, they have no visibility into information about Kubernetes
- **Lack of context:** container-centric approaches can take action based only on the context provided by images, i.e., vulnerabilities (via vulnerability scanning) and CVE scores
- **Non-scalable policy enforcement:** because containers themselves lack sufficient controls, container-centric solutions require third-party components that create operational risk, and that approach fails to scale at pace with Kubernetes

The StackRox Kubernetes Security Platform was purpose-built for the modern cloud-native stack. We have built multiple deep integrations with Kubernetes into our platform, making your security as portable, scalable, and resilient as your application infrastructure. This Kubernetes-native approach also delivers the most comprehensive set of container AND Kubernetes security capabilities across the full application development life cycle.



Our Kube-native architecture leverages three distinct advantages from Kubernetes:

1. **Richer context:** Kubernetes provides context around your images and containers, pods, deployments, and namespaces across all clusters. This context improves visibility, configuration management, and runtime detection and response. It also improves vulnerability management, since StackRox not only identifies which containers and images have vulnerabilities and their severity score but also shows which deployments are at the greatest risk because of other attributes of the deployment (network configuration, test vs prod, privileges, secrets, etc.). As a result, StackRox prioritizes which deployments need immediate remediation rather than cataloging all image with high-severity CVSS scores.

2. **Native enforcement:** instead of relying on third-party components that introduce operational risk and complexity, StackRox leverages the built-in enforcement capabilities native to Kubernetes itself. Kubernetes supports network policies for firewalling, admission controllers for blocking non-compliant deployments, the ability to scale services to zero to shut down non-compliant deployments, and killing containers found to be running malicious or suspicious processes. Leveraging Kubernetes instead of external controls taps into the scalable, robust, and portable attributes of Kubernetes and enables your DevOps teams to operationalize these security controls.

3. **Continuous hardening across the full life cycle:** StackRox leverages the learnings across all phases of the container life cycle to constantly tune configurations, network settings, and runtime analysis. This approach enables StackRox to continuously improve the security posture of your environments.

These advantages, derived from our tight integrations with Kubernetes, enable a better security outcome for our customers. While many container security providers highlight a common set of use cases, how you deliver those use cases impacts the result. The following discussion of the top container security use cases illustrates the advantages of applying a Kubernetes-native architecture.

VISIBILITY

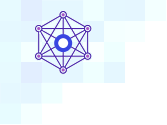
See your entire landscape of images, registries, containers, deployments, and runtime behavior.

VULNERABILITY MANAGEMENT

Identify and fix vulnerabilities in both container images and Kubernetes across the entire software development life cycle.

COMPLIANCE

Audit your systems against CIS Benchmarks, NIST, PCI, and HIPAA, with interactive dashboards and one-click audit reports.



NETWORK SEGMENTATION

Visualize existing connections and enforce tighter segmentation using Kubernetes-native controls to reduce your blast radius.

RISK PROFILING

See all your deployments ranked by risk level, using context from Kubernetes' declarative data, to prioritize remediation.

CONFIGURATION MANAGEMENT

Apply best practices for Docker and Kubernetes to harden your environment for a more secure and stable application.

THREAT DETECTION

Use rules, automated whitelists, and baselining to accurately identify suspicious activity in your running applications.

INCIDENT RESPONSE

Take action, from failing builds and blocking deployments to killing pods and thwarting attacks, using Kubernetes for enforcement.

Key use cases

Visibility

You can't secure what you can't see. As a first step, you must gain visibility into your container and Kubernetes environment. You should know what images you're using, understand their provenance, whether they contain any vulnerabilities and their severity level, and that's just the start. You must also know which pods, namespaces, and deployments are running vulnerable containers and what their attack surface and blast radius are during a breach.

First-generation, container-centric approach	StackRox approach

• Provides visibility into images, containers, and vulnerabilities, with CVE and severity scores	• Provides visibility into images, containers, and vulnerabilities with CVE and severity scores, AND Kubernetes components across clusters including:
	  ◦ pods
	  ◦ deployments
	  ◦ namespaces
	• Enhances visibility with contextual data from Kubernetes such as allowed network paths, runtime process execution, secrets exposure, and other factors

Key StackRox features

- **Deployment-centric data:** StackRox delivers a comprehensive picture of your containerized apps, including their images, pods, configurations, and how they relate to each other.
- **Detailed network visibility:** StackRox discovers and displays network traffic in all Kubernetes clusters, spanning namespaces, deployments, and pods. StackRox supports all CNI plugins and integration with Istio enables visualization of traffic between Istio services.
- **Deep runtime monitoring:** StackRox automatically captures all critical system-level events in each container to quickly hone in on suspicious activity, streamlining investigations for your security and operations teams.
- **Easy image discovery:** Using StackRox, you can easily identify and analyze container images in your environment with native integrations for nearly every image registry.

Vulnerability management

One of the most critical steps in securing containers and Kubernetes is to prevent images or containers with known vulnerabilities from being deployed as well as to identify and stop running containers that have vulnerabilities. You must also run on-demand vulnerability searches across images, running deployments, and clusters to enforce policies at build, deploy, and runtime.

Vulnerability management solution must also integrate with your CI/CD pipeline to fail a build if it contains a vulnerability, while providing the developer details on why the build failed and how to remediate it.

First-generation, container-centric approach	StackRox approach
• Focused on image and container scanning alone • Is limited to providing a list of vulnerabilities and CVE scores without context	• Delivers full life cycle image and container scanning • Combines details about vulnerabilities with Kubernetes data and the life cycle stage that the vulnerability impacts to quantify the security risk that a given vulnerability poses to your environment • Operationalizes vulnerability management by pinpointing which pods, namespaces, deployments, and clusters are impacted by a given vulnerability

Key StackRox features

- **Flexible image scanning:** StackRox provides a built-in image scanner to easily discover vulnerabilities in your container images, with options to identify vulnerabilities based on specific languages and packages and by image layer. You can also choose to integrate output from your existing scanning solutions.
- **Contextual search:** StackRox includes search capabilities for fast enumeration, filtering, and discovery of vulnerabilities across your entire environment, allowing you to find and address vulnerabilities more quickly.
- **Automated policy enforcement:** StackRox can enforce policies across the entire life cycle based on vulnerability information - at build time with CI/CD pipeline integration, at deploy time using dynamic admission control and at runtime using Kubernetes-native enforcement.
- **Runtime vulnerability discovery:** StackRox immediately correlates vulnerabilities to running deployments rather than just images so that you quickly identify actual exposure to streamline remediation.

Compliance

DevOps moves fast and relies on automation for continuous improvement; therefore, organizations need a compliance solution built to complement, not inhibit, DevOps activities. You not only need to adhere to industry compliance requirements but also show proof of continuous adherence. Lastly, you also need to adhere to internal policies for configurations and other best practices to prevent non-compliant builds or deployments from being pushed to production.

First-generation, container-centric approach	StackRox approach
• Provides compliance checks that are limited to CIS benchmarks alone	• Provides pre-built compliance checks for CIS benchmarks for Docker and Kubernetes as well as PCI, HIPAA, and NIST SP 800-190

Key StackRox features

- **Automated compliance checks:** StackRox automatically assesses compliance across hundreds of controls for PCI, HIPAA, NIST SP 800-190, and CIS Benchmarks for Kubernetes and Docker, based on evaluating Kubernetes-specific configurations.
- **Summary dashboards and reporting:** StackRox delivers an at-a-glance view of overall compliance across each standard's controls. Use the interactive dashboard and generate PDF reports to understand your organization's adherence with regulatory and best practice requirements and where it needs to improve.
- **Evidence export:** StackRox exports CSV files with a single click to document all pertinent aspects of each individual control, to meet auditors' needs.
- **Customizable views with data drill down:** StackRox enables users to drill down into compliance details based on multiple dimensions including Kubernetes constructs such as clusters, nodes, or namespaces or based on particular compliance standards and control areas.

Network segmentation

Containers pose a unique networking challenge because containers communicate with each other across nodes and clusters (east-west traffic) and outside endpoints (north-south traffic). As a result, a single container breach has the potential to impact every other container. Therefore it's imperative to limit a container's communication in adherence with least privilege principles without inhibiting your container's functional goals.

First-generation, container-centric approach	StackRox approach
• Injects inline proxy/firewall between containers to enforce networking controls • Introduces scale and reliability risk with a proprietary component in the critical path of application operations	• Leverages Kubernetes' native networking policy enforcement capabilities • Delivers robust and portable network policy enforcement that scales as Kubernetes scales without requiring third-party inline proxies • Ensures that security and DevOps see and act using a single source of truth and consistent information to effectively restrict network access

Key StackRox features

- **Network graph:** StackRox intuitively visualizes both allowed and active network traffic so you can achieve more secure network configurations. View details of network connectivity between namespaces and deployments, including external exposure, alongside pod-level information.
- **Kubernetes network policy simulator:** StackRox lets you quickly simulate, preview, and understand the impact of network policy changes throughout your environment to minimize operational risk to your applications.
- **Kubernetes network policy generator:** StackRox automatically baselines network activity and recommends Kubernetes network policies to remove allowed but unnecessary network connections to harden your environment. Integration with DevOps tools allow your DevOps and security teams to collaborate seamlessly.
- **Kubernetes-native network enforcement:** StackRox leverages the network enforcement capabilities built-in to Kubernetes to ensure consistent, portable, and scalable network segmentation regardless of your CNI plugin or Kubernetes distribution.

Risk profiling

A common customer pain point is being inundated with security alerts and incidents that need investigation without any guidance on prioritization. This approach inevitably leads to instances where high-risk security issues trail low/medium risk issues in remediation simply because teams cannot identify which problems present the highest risk. Or in the worst case scenario, without prioritization, nothing is remediated.

First-generation, container-centric approach	StackRox approach
• Provides a list of image vulnerabilities • Prioritizes risk based only on the CVE and its severity • Lacks the ability to prioritize remediation efforts when multiple images, containers, or deployments contain the same vulnerability • Exacerbates alert fatigue and increases the likelihood of ignoring a high risk issue	• Correlates image vulnerabilities and their severity with rich contextual data derived from deep integration with Kubernetes • Instantly informs you which deployments are affected by any given vulnerability • Provides a numerical risk-based ranking of each deployment based on information across the entire life cycle, including the severity of the vulnerability AND other risk factors such as the container privilege, secrets, network configuration, running processes, and other factors • Empowers you to understand which deployments are in need of immediate remediation so that the highest risk deployments are addressed first

Key StackRox features

- **Contextual risk assessment:** StackRox delivers deeper contextual insights about security risks across your Kubernetes deployments by collecting and synthesizing data derived from your software components, declarative configurations, and runtime activity to enable you to improve your security posture.
- **Risk prioritization and ranking:** StackRox leverages the power of declarative configuration and immutable infrastructure to assess risk in your environment. StackRox ranks your running deployments according to their holistic security risk, leveraging Kubernetes data to prioritize vulnerabilities using configuration or deployment details as well as runtime activity. This approach lets you triage risk fast and identify those environments that need your immediate attention.
- **Continuous feedback:** StackRox tracks improvements in your overall security posture of your Kubernetes deployments over time with continuous risk profiling. StackRox makes it easy to validate the impact of your security team's actions to more effectively reduce risk to your applications and infrastructure.

Configuration management

The configuration options for container and Kubernetes environments run deep and can be difficult to get right. In sprawling container and Kubernetes environments, it's impossible to manually check each security configuration for each asset to assess its risk.

While the CIS Benchmarks for Docker and Kubernetes provide helpful guidance and a useful framework for hardening your environment, they contain hundreds of checks for different configuration settings. Ensuring continuous adherence to the CIS benchmarks and other configuration best practices can be challenging without an automated management layer.

First-generation, container-centric approach	StackRox approach
• Provides visibility into what's inside containers and images but offers no context for how Kubernetes is configuring them for deployment • Lacks visibility into Kubernetes configurations, such as how RBAC is configured, whether secrets are exposed, or other attributes • Lacks enforcement capabilities to correct misconfigurations	• Provides a deployment-centric approach that leverages data from Kubernetes to understand how images, containers, and deployments are configured prior to running to identify missed best practices and recommendation • Leverages native Kubernetes capabilities such as admission controllers to block misconfigured images, containers, and deployments from deploying or running

Key StackRox features

- **Kubernetes RBAC assessment:** StackRox analyzes Kubernetes Role-Based Access Control (RBAC) settings to understand user and service account privileges and applies this context to determine misconfigurations and inform risk assessment.
- **Kubernetes secrets monitoring:** StackRox tracks Kubernetes secrets and which deployments use them, enabling you to proactively limit unnecessary access.
- **Pre-configured policies:** StackRox delivers pre-built DevOps and Security policies that identify configuration violations related to network exposures, privileged containers, processes running as root, and compliance with industry standards.
- **Automated policy enforcement:** StackRox can enforce configuration policies - at build time with CI/CD pipeline integration and at deploy time using dynamic admission control.

Threat detection

Once container images are built and deployed into production, they are exposed to new security challenges and external adversaries. The primary goal of security in the runtime phase is to detect and respond to malicious activity in an automated and scalable way while minimizing false positives and alert fatigue.

First-generation, container-centric approach	StackRox approach
• Relies on explicitly identifying and creating a list of whitelisted processes, leading to operational challenges and high number of false positives and false negatives • Requires established knowledge of acceptible processes beforehand	• Combines automated process discovery and behavioral baselining with automated process whitelisting • Observes runtime behavior and creates a whitelist, resulting in higher-fidelity threat detection with fewer false positives, as opposed to requiring manual creation of process whitelists

Key StackRox features

- **Intelligent runtime analysis:** StackRox monitors, collects, and evaluates system-level events within each container in your Kubernetes environments to enable you to hone in on suspicious activity more quickly.
- **Automated process whitelisting:** StackRox baselines process activity within containers, automatically identifying anomalous processes that operators can selectively whitelist, eliminating the work of having to manually whitelist allowed process executions in advance.
- **Pre-configured threat profiles:** StackRox applies pre-defined policies to detect threats including cryptocurrency mining, privilege escalation, and various exploits.
- **Flexible data collection:** StackRox allows you to choose to collect system-level data using either eBPF or a kernel module across every major distribution of Linux.

Incident response

Your container security solution must fit into DevOps workflows and bridge the gap between DevOps and Security teams. Incident response is therefore a critical use case that must span the full container life cycle and must be tailored to how different teams achieve their day-to-day tasks.

For example, DevOps must be informed of deployment or runtime violations seamlessly and with the necessary contextual details to enable them to fix the issue and ensure future builds don't cause similar violations. Responses should also be tailored to different phases of the container life cycle (build, deploy, runtime) and the environment (production vs. test) and enable tiered response based on the severity of the violation (alert, fail build, block deployment, scale deployment to zero, kill pods, etc.).

First-generation, container-centric approach	StackRox approach
• Responds in a manner that creates operational risk to applications and infrastructure • Unable to leverage built-in Kubernetes controls for incident response and enforcement	• Delivers highly configurable and full life cycle incident response capabilities • Leverages native Kubernetes capabilities for enforcement in response to a violation

Key StackRox features

- **Kubernetes-native runtime enforcement:** StackRox utilizes Kubernetes controls to take action on running deployments, speeding remediation while minimizing operational risk to your applications and infrastructure.
- **Forensics and investigations:** StackRox captures detailed, historical runtime activity to more effectively understand and respond to threats. This information empowers operators to explore and hunt for threats.
- **Native integrations:** StackRox provides native integrations with Splunk, Sumo Logic, PagerDuty, Google Cloud Security Command Center, and other SIEM and incident management solutions. The integrations enable you to view, correlate, and analyze StackRox in the systems your team is already using, enhancing their security insights and enabling more effective incident response.

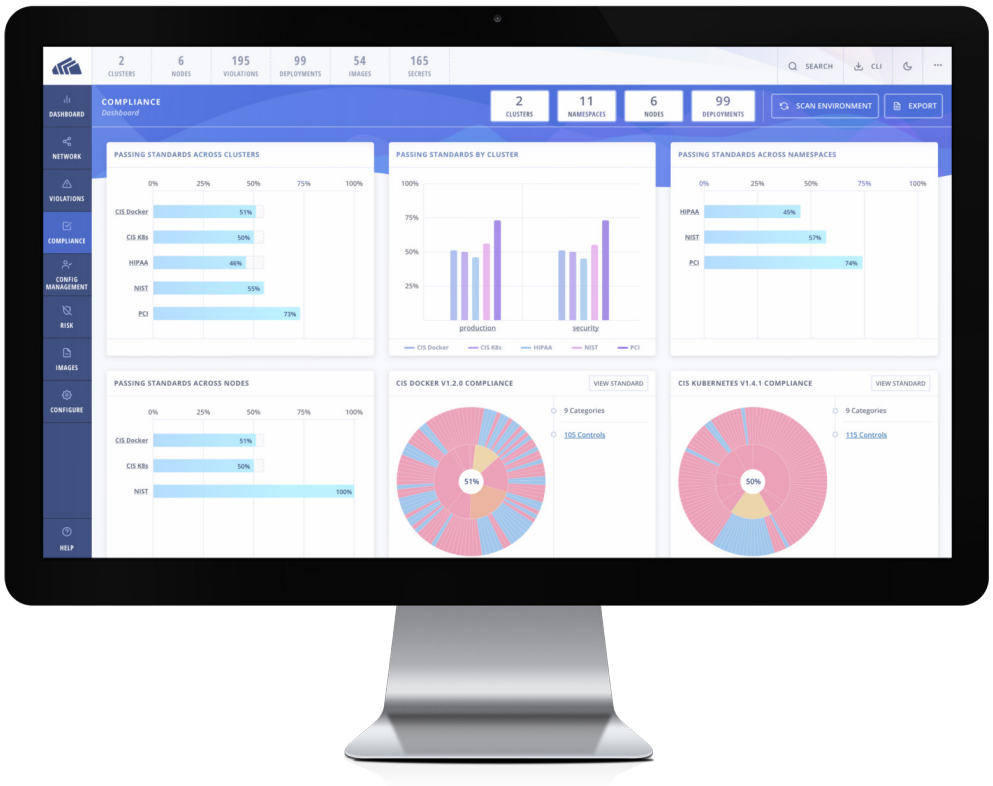
Conclusion

The native controls inherent in containers and Kubernetes offer the potential for building the most secure applications you've ever created. But getting all the knobs and dials set correctly can be daunting. First-generation container security platforms focus on just the container. StackRox delivers the next generation in container security, with a Kubernetes-native architecture that is both container native and Kubernetes native. Leveraging the declarative data and built-in controls of Kubernetes for richer context, native enforcement, and continuous hardening immediately improves your security posture. The StackRox integrations with Kubernetes helps your DevOps and Security teams operationalize container security, simplifying the process of protecting your cloud-native application.

Ready to see StackRox in action?

Get a personalized demo tailored for your business, environment, and needs.

REQUEST DEMO



StackRox

StackRox helps enterprises secure their containers and Kubernetes environments at scale. The StackRox Kubernetes Security Platform enables security and DevOps teams to enforce their compliance and security policies across the entire container life cycle, from build to deploy to runtime. StackRox integrates with existing DevOps and security tools, enabling teams to quickly operationalize container and Kubernetes security. StackRox customers span cloud-native start-ups Global 2000 enterprises, and government agencies.

LET'S GET STARTED

Request a demo today!

info@stackrox.com
+1 (650) 489-6769
www.stackrox.com