StackRox

Guide to NIST SP 800-190 Compliance in Container Environments

Table of Contents

Introduction

Organizations are eager to adopt containers and microservices, but security concerns can be an impediment. People are still learning about containers and Kubernetes themselves - understanding the security implications of this infrastructure adds to the learning curve. You need to understand the threat landscape in these environments, assess your risk posture when using containers, and know how to mitigate the security risks associated with container adoption.

One tool to leverage to understand how to secure containers comes from the National Institute of Standards and Technology (NIST). NIST Special Publication (SP) 800-190 outlines some of the security concerns related to container technologies and offers practical recommendations for securing your containerized applications and related infrastructure components.

You can use the following guide to understand the key recommendations of NIST SP 800-190 and gain detailed descriptions of how the StackRox Kubernetes Security Platform helps customers comply with NIST SP 800-190.

Container Security at a Glance

The most effective way to secure containerized applications requires embedding security controls into each phase of the container lifecycle: Build, Deploy, and Run.

Build
This phase centers on what ends up inside of the container images developers create. In the build phase, security efforts are typically focused on reducing business risk later in the container lifecycle by applying best practices and identifying and eliminating known vulnerabilities early.

Deploy
In this phase, developers configure containerized applications for deployment into production. Context grows beyond information about images to include details about configuration options available for orchestrated services. Security efforts in this phase often center around complying with operational best practices, applying least-privilege

principles, and identifying misconfigurations to reduce the likelihood and impact of potential compromises.

Runtime
Containers go into production with live data, live users, and exposure to networks - internal or the public Internet. The primary purpose of security during the runtime phase is protecting both running applications and the container infrastructure by finding and stopping malicious actors in real time.

In conjunction with protecting containers across their life cycle, you must also secure the underlying infrastructure and ensure it is properly configured. Containers can help organizations implement finer-grained workload-level security, but they also introduce new infrastructure components and unfamiliar attack surfaces. As a result, you must secure your cluster infrastructure and Kubernetes orchestrator as well as the containerized applications they run.

Securing Containers and Kubernetes with StackRox

The StackRox Kubernetes Security Platform protects your applications across the entire container life cycle. The platform discovers your full container environment; ensures assets comply with industry regulations, best practices, and security policies; and identifies and stops malicious actors.

StackRox leverages its Kubernetes-centric architecture to derive rich context about your deployments. We then apply multi-factor risk profiling to build a complete picture of your container risk, including image vulnerabilities, service exposure level, privilege level, and other factors. StackRox provides unique capabilities to help make a container environment NIST SP 800-190 compliant.

- Full lifecycle (build, deploy, runtime) vulnerability scanning/management that's automated to support CI/CD
- Real-time network diagram indicating authorized and unauthorized data flows between containers with ability to enforce more secure network policies
- Automated response capabilities to shut down containers that are violating policy

- Support for only one function per container. StackRox's multi-factor risk profiling is designed to uncover risky behaviors such as running multiple functions per container or orchestrator deployment
- Minimizing functionality and flagging new container functionality. StackRox uses introspection technology to identify new functionality, providing actionable guidance to security operators to quickly detect any unnecessary processes, files, and packages
- Going beyond AV and anti-malware. StackRox uses machine learning, advanced risk profiling, and attack detection (i.e., foothold, persistence, privilege escalation, movement, and objectives) with corresponding response to detect malicious activity

How StackRox Supports NIST SP 800-190

The following details map the features of the StackRox Kubernetes Security Platform to guidance provided in NIST SP 800-190.

4.1.1 - Image Vulnerabilities

Organizations should use image vulnerability tools purpose-built for containers. Key aspects of effective tools and processes include:

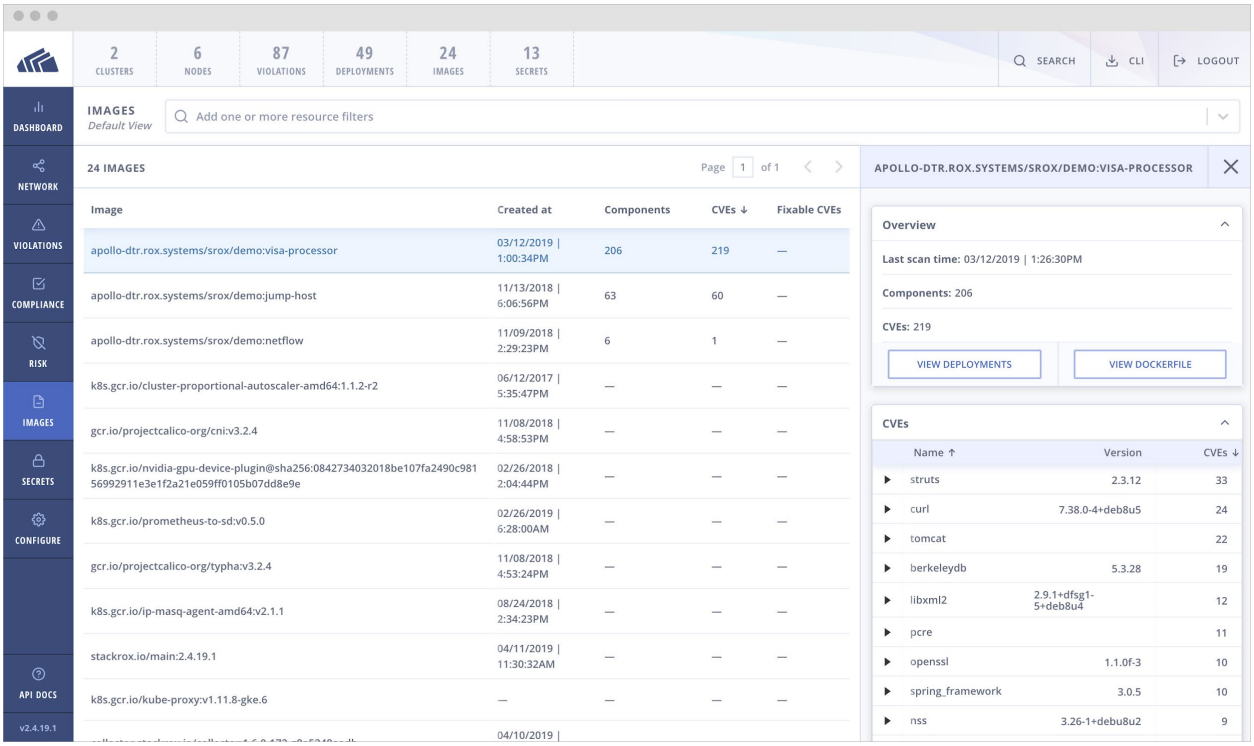
1. Integration with the entire lifecycle of images
2. Centralized visibility into vulnerabilities at all layers of the image across the organization, with flexible reporting and monitoring views aligned with organizations' business processes.
3. Policy-driven enforcement that ensures that only images meeting your policy requirements are allowed to progress.

How StackRox helps

StackRox provides full lifecycle container security that includes:

1. Integration with your CI/CD pipeline to scan and detect vulnerabilities in images at any stage of the development cycle.

2. Introspection of images at all layers, not just the base layer, with executive-level summary views as well as more detailed reporting.
3. Out-of-the-box policies with enforcement that ensures only images that are compliant with your policies are able to progress.



4.1.2 - Image Configuration Defects

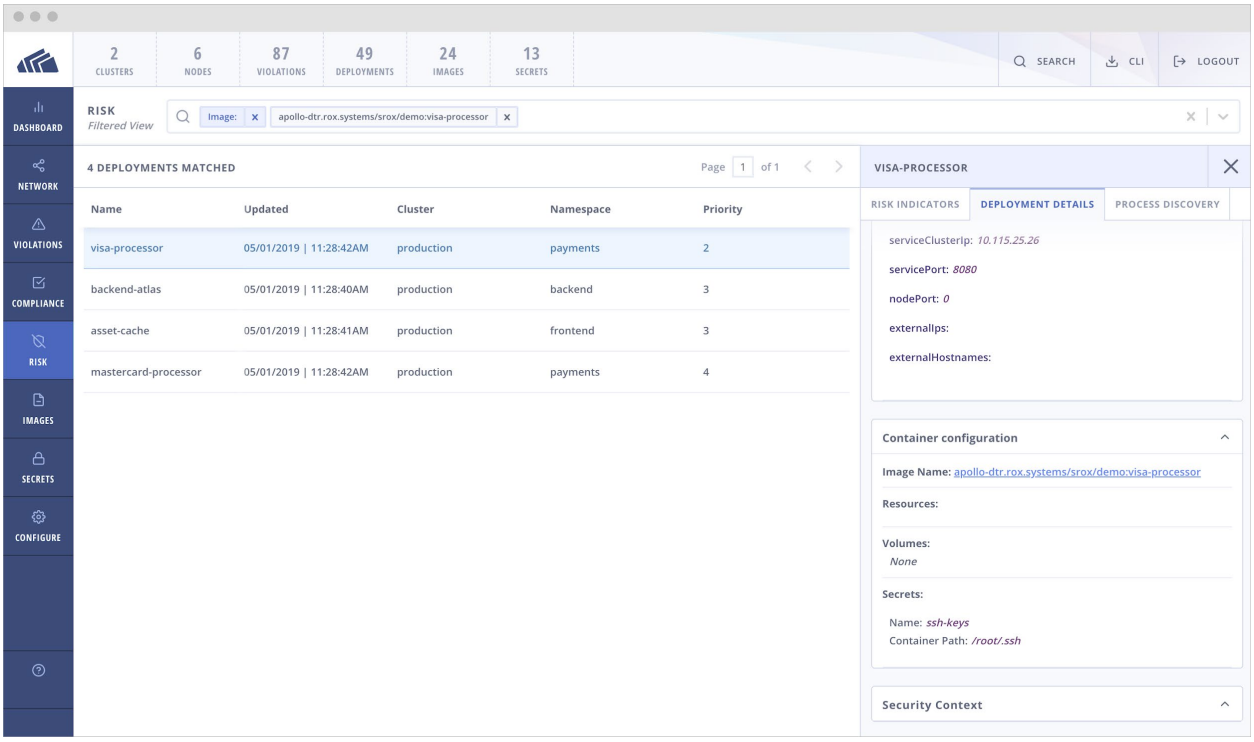
Organizations should implement security controls and processes that ensure compliance with secure configuration best practices. This includes:

1. Ability to audit image configuration settings
2. Real-time and continuous reporting and monitoring of image compliance state
3. Policy enforcement that prevents non-compliant images from running.

How StackRox helps

The StackRox Kubernetes Security Platform is a comprehensive solution that detects and prevents image misconfigurations at all stages of your development cycle.

- StackRox supports image scanning natively but can also integrate with your existing image scanners.
- StackRox audits your image and container configuration and provides out-of-the-box policies to detect misconfigurations, including instances of privileged containers or images deployed as root user. Alternatively, you can configure custom policies and enforcement actions unique to your organizational needs to ensure images meet all of your security requirements.
- StackRox provides real-time and continuous visibility and monitoring of all deployed images to ensure compliance during build/deployment stages as well as runtime. Any images or containers in violation of your policies are prevented from running.
- Lastly, StackRox delivers built-in capabilities that identify the use of SSH within containers, including policies that alert on the exposure of port 22 and processes that appear to be SSH daemons.



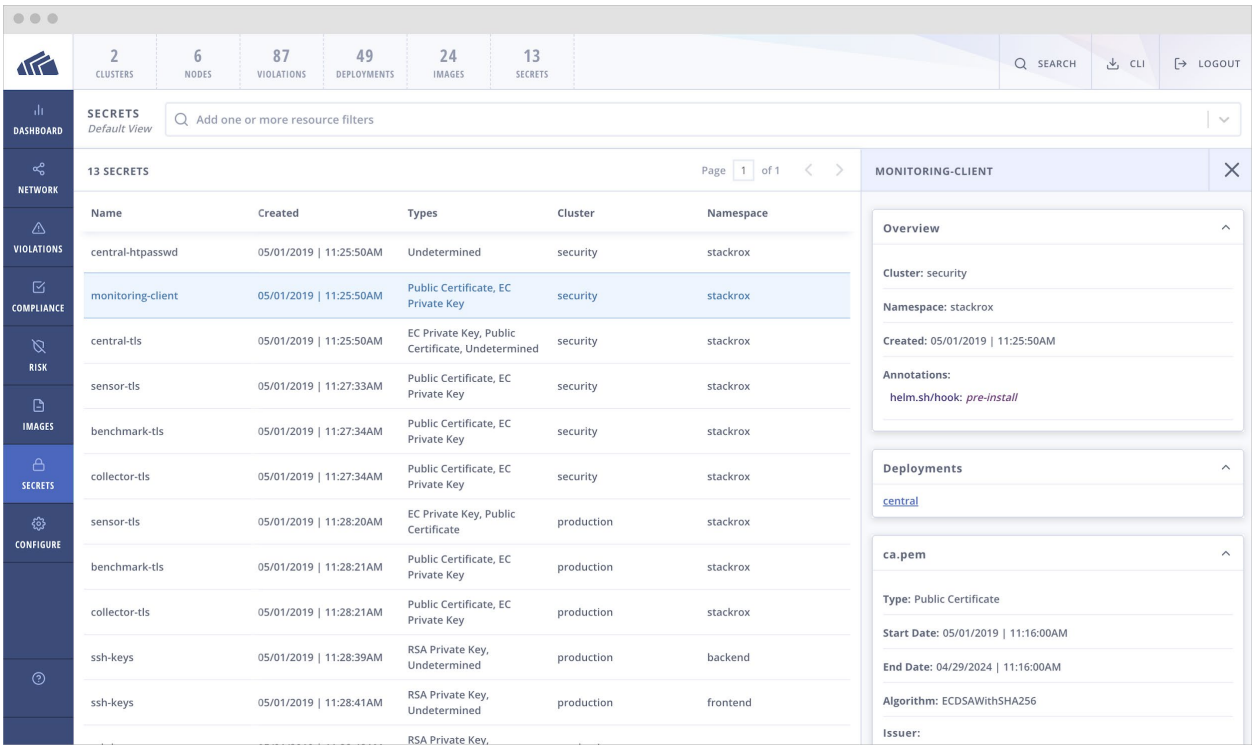
4.1.4 - Embedded clear text secrets

Organizations must protect secrets by storing it outside of images and only make them accessible dynamically at runtime. Organizations should use Kubernetes for secrets management and ensure that secrets are provided only to a particular container that requires it and are encrypted at rest and in transit at all times.

How StackRox helps

StackRox protects secrets in several ways.

- StackRox provides out-of-the-box policies that detect instances where secrets are being provided in an insecure manner, including in environment variables.
- In addition, StackRox examines the metadata about the secrets configured in monitored clusters, including the deployments configured to reference those secrets and ensures secrets transmitted via Kubernetes are only accessible to containers that are configured to use them.



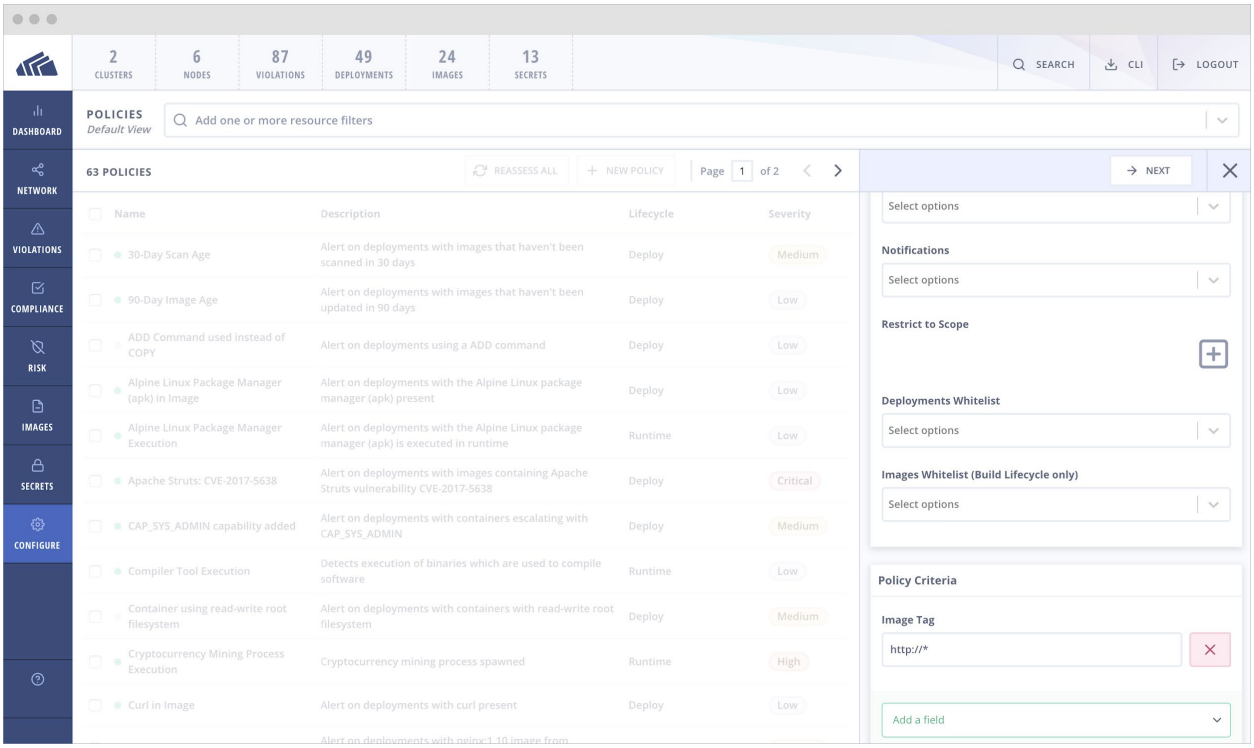
4.2.1 - Insecure connections to registries

Use a secure/encrypted connection when pushing/pulling from a registry.

How StackRox helps

StackRox can help ensure that all communication between you and the registry is done through an encrypted channel.

- By default, the Docker engine will not pull from unencrypted registries. However it does provide the option of whitelisting registries where insecure connections are used. StackRox analyzes the configuration of your Docker engine on cluster nodes and identifies exceptions where an unencrypted registry is being whitelisted.
- StackRox also flags images whose tags/references begin with http://



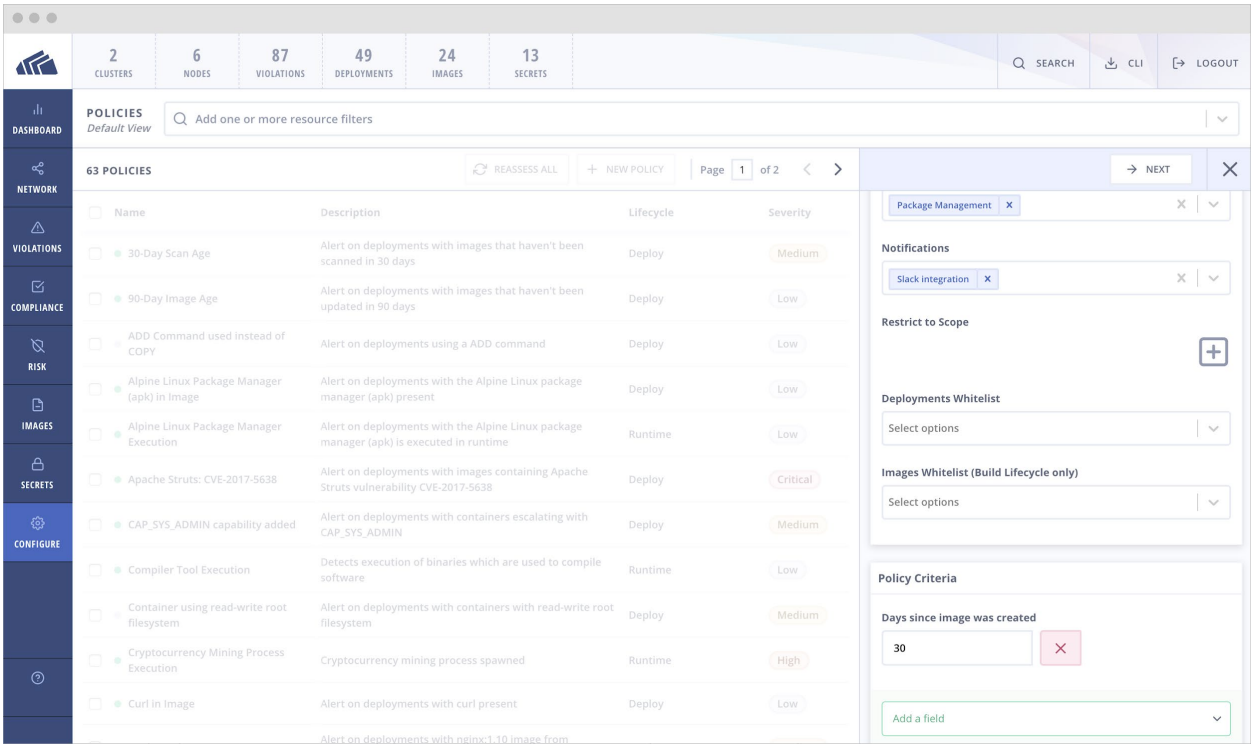
4.2.2 - Stale images in registries

Organizations must implement processes and controls to ensure that the latest versions of images are being used.

How StackRox helps

StackRox takes a multi-pronged approach to identifying and mitigating the use of stale and potentially risky images.

- The StackRox Kubernetes Platform has a pre-built policy intended to discourage the use of the latest tag and instead recommends accessing images using immutable names that includes image versions.
- StackRox provides out-of-the-box policy to flag use of images built more than 90 days. Alternatively, you can configure the policy to look for shorter or longer time windows as it fits your specific needs.
- Lastly, StackRox incorporates image age as one of the risk factors when providing the risk score for each deployment.



4.3.3 - Poorly separated inter-container network traffic

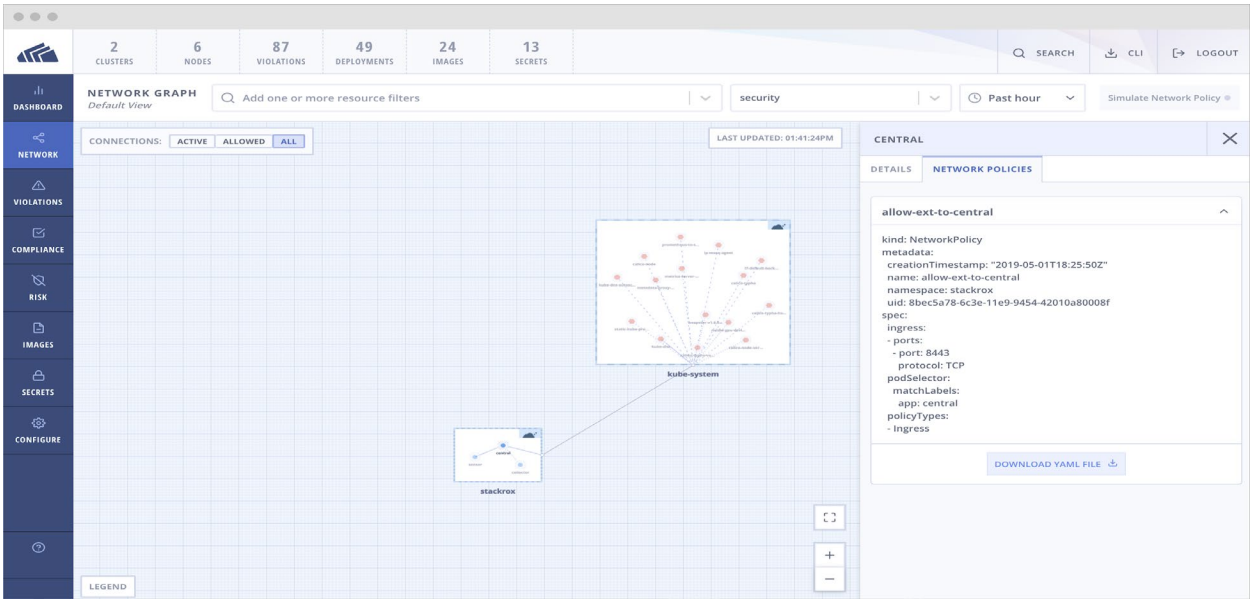
Configure Kubernetes such that you are segmenting network traffic to decrease your risk exposure. As a first step, you should define networks by sensitivity level and ensure separation of sensitive and non-sensitive networks.

For example, apps open to the broader internet can share a virtual network, internal facing apps can use another, and communication between the two should occur through a small number of well-defined interfaces.

How StackRox helps

StackRox helps ensure that networks are segmented in a secure manner in the following ways:

- StackRox runs checks to see if your Kubernetes network segmentation rules are applied to all of your deployments.
- We provide a visual simulation of your existing network connections, the StackRox Network Graph, to help you understand your network topology. The Network Graph identifies allowed and active connections to help you identify gaps in your inter-app segmentation policies.
- You can leverage the StackRox Kubernetes Security Platform to generate new network policies (YAML files) and push them to your Kubernetes deployment for a better network security posture.



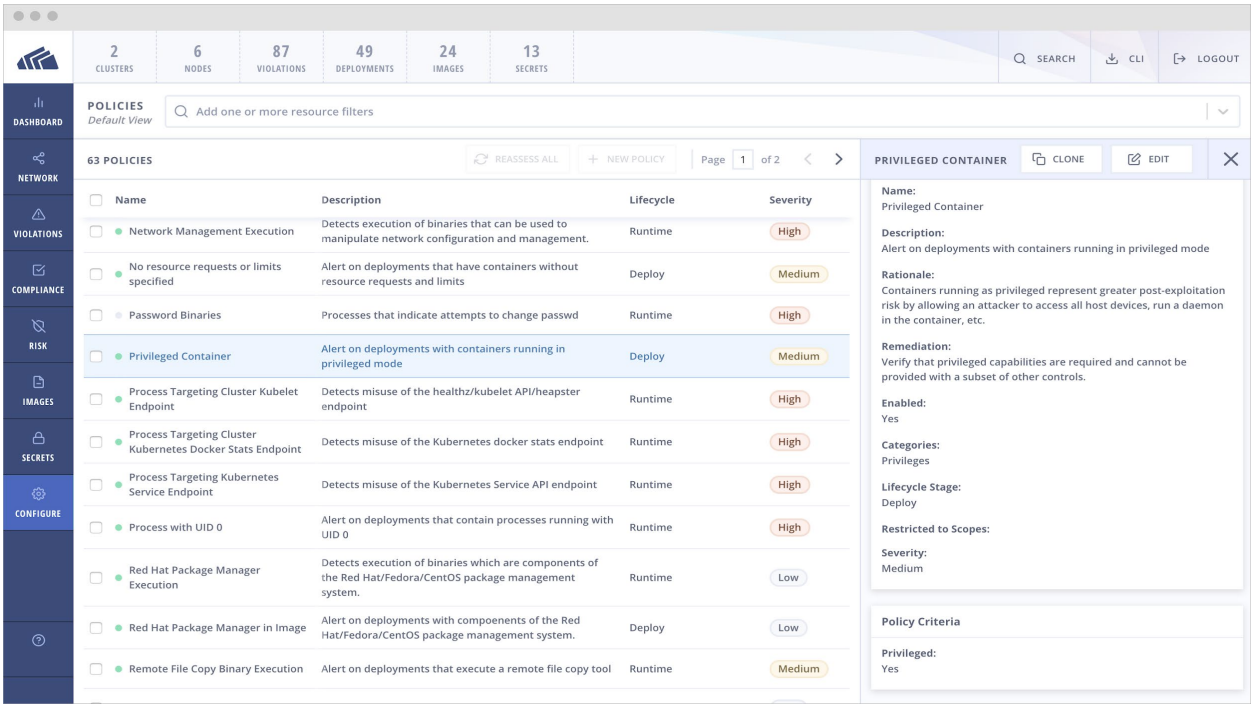
4.3.5 - Orchestrator node trust

Your Kubernetes deployment should securely introduce nodes to the cluster, have a persistent identity throughout their lifecycle, and display an accurate inventory of nodes and their connectivity states. Configure Kubernetes to be resilient to compromise of individual nodes without compromising the overall security of the cluster. Isolate and remove a compromised node without negatively impacting overall operations.

How StackRox helps

The StackRox Kubernetes Security Platform provides hundreds of out-of-the-box policies specifically designed to ensure that you are hardening your Kubernetes environment, including:

- Check to see if you've scanned your deployments against the above-mentioned policies
- Flag deployments that haven't been scanned
- Identify policy violations
- Present additional opportunities to harden your Kubernetes environment



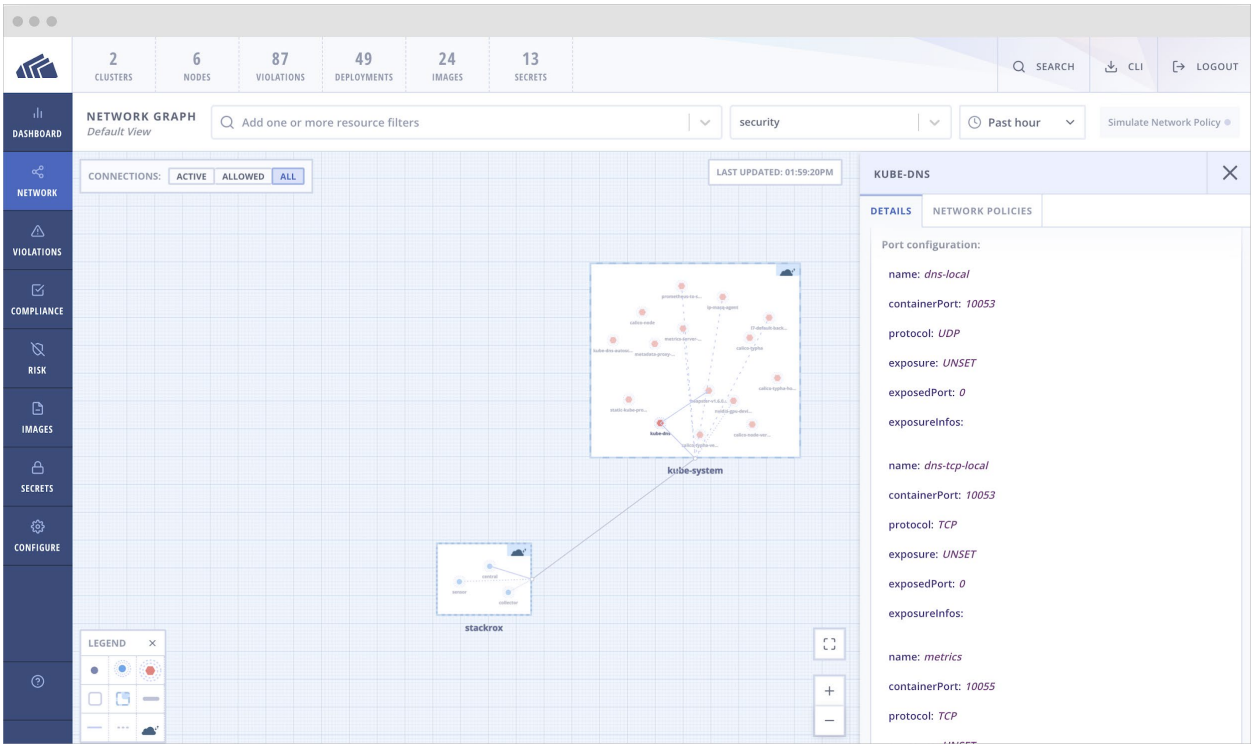
4.4.2 - Unbounded network access from containers

Implement controls for outbound network traffic from containers. Prevent traffic from being sent across networks of varying sensitivity levels.

How StackRox helps

StackRox helps implement controls for outbound network traffic in the following ways:

- StackRox runs checks to see if your Kubernetes network segmentation rules are applied to all of your deployments.
- We provide a visual simulation of your existing network connections, the StackRox Network Graph, to help you understand your network topology. The Network Graph identifies allowed and active connections to help you identify gaps in your inter-app segmentation policies.
- You can leverage the StackRox Kubernetes Security Platform to generate new network policies (YAML files) and push them to your Kubernetes deployment for a better network security posture.



4.4.3 - Insecure container runtime configurations

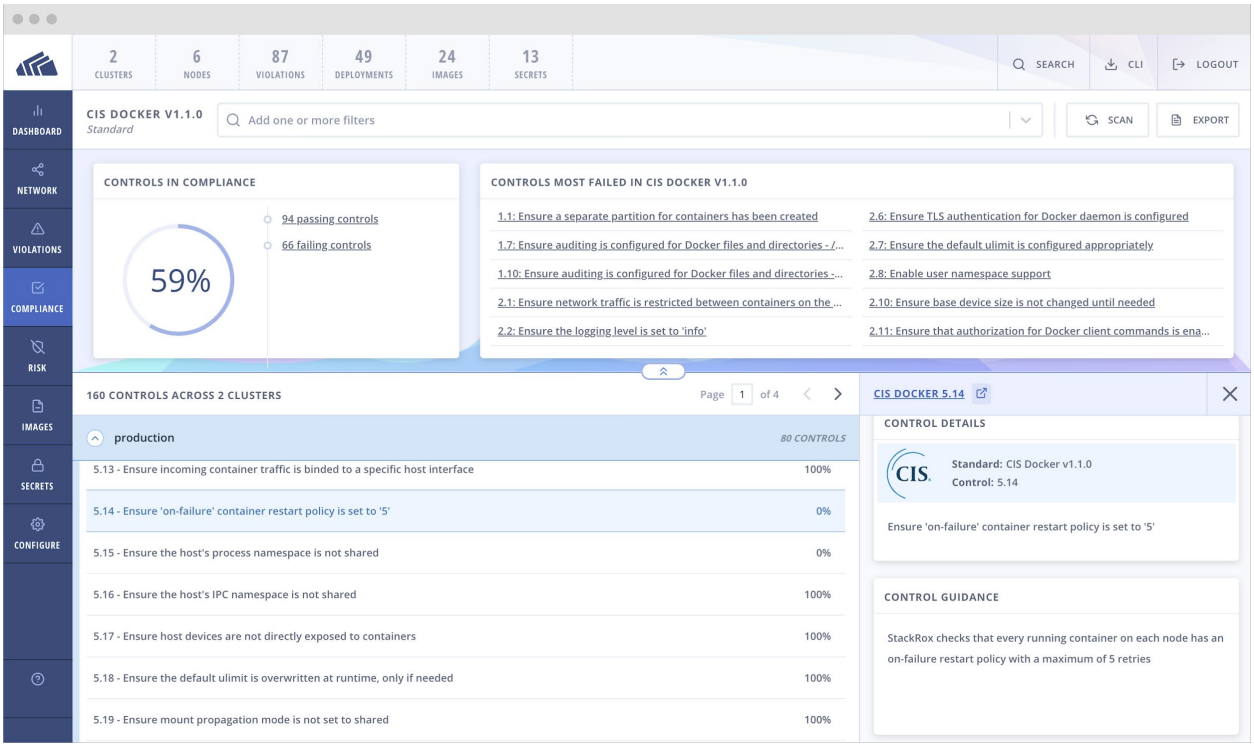
Automate compliance with container runtime configuration standards such as the Center for Internet Security (CIS) Docker Benchmark and continuously assess configuration settings across the environment.

How StackRox helps

The StackRox Kubernetes Security Platform scans your environment and runs compliance checks against CIS Docker and Kubernetes Benchmarks to ensure continous compliance across your container environment.

In addition, StackRox also delivers out-of-the-box compliance policies for:

- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA).



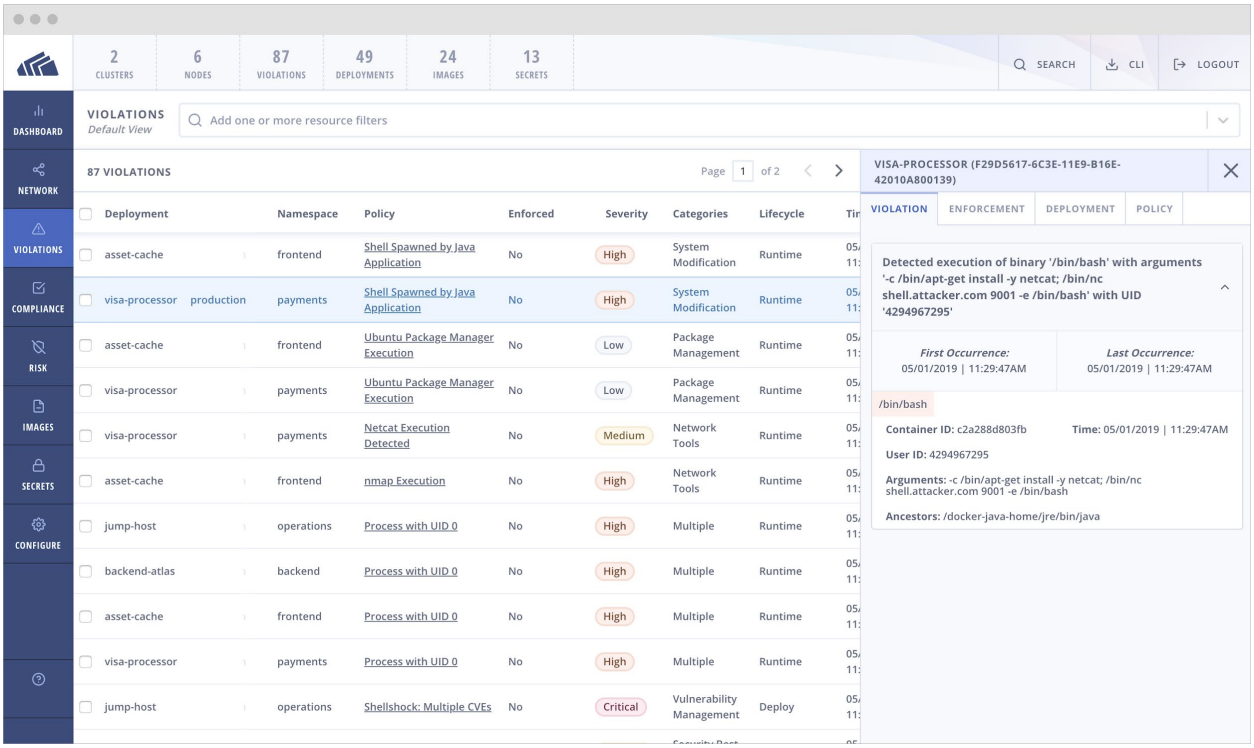
4.4.4 - App vulnerabilities

Implement security controls purpose-built to detect threats, such as intrusions, to containers and container infrastructure.

How StackRox helps

The StackRox Kubernetes Security Platform combines behavioral modeling with rules and whitelisting to detect threats to containers, including unexpected activity. Examples include:

- StackRox delivers out-of-the-box policies for the use of package managers and identifies suspicious process execution based on filenames and paths.
- StackRox identifies risky configurations that could lead to changes on the host, such as changes to important system files.



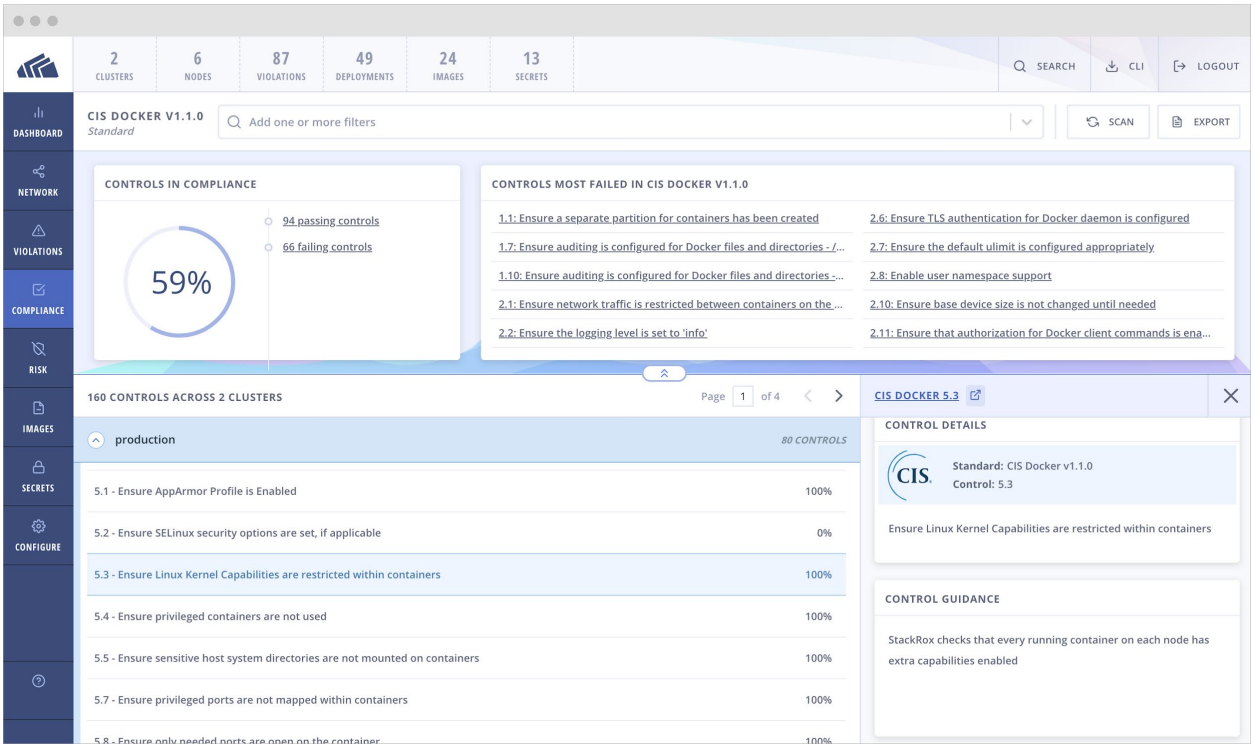
4.5.1 - Large attack surface

When possible, use a container-specific OS because OSs that are specifically designed to host containers are usually hardened by default. When you can't use a container-specific OS, harden the host OS to reduce your attack surface.

How StackRox helps

StackRox helps ensure compliance with this recommendation in several ways

- StackRox supports the use of CoreOS and Google Container-Optimized OS
- StackRox identifies the node OS deployed in clusters to verify use of CoreOS or Google Container-Optimized OS as compliance evidence.
- StackRox can assess compliance with CIS General Linux Benchmark to ensure your Linux host is securely configured.
- In instances where a container-specific OS isn't being used, StackRox automatically assess compliance with the CIS Docker and Kubernetes benchmarks to ensure your environment is hardened.



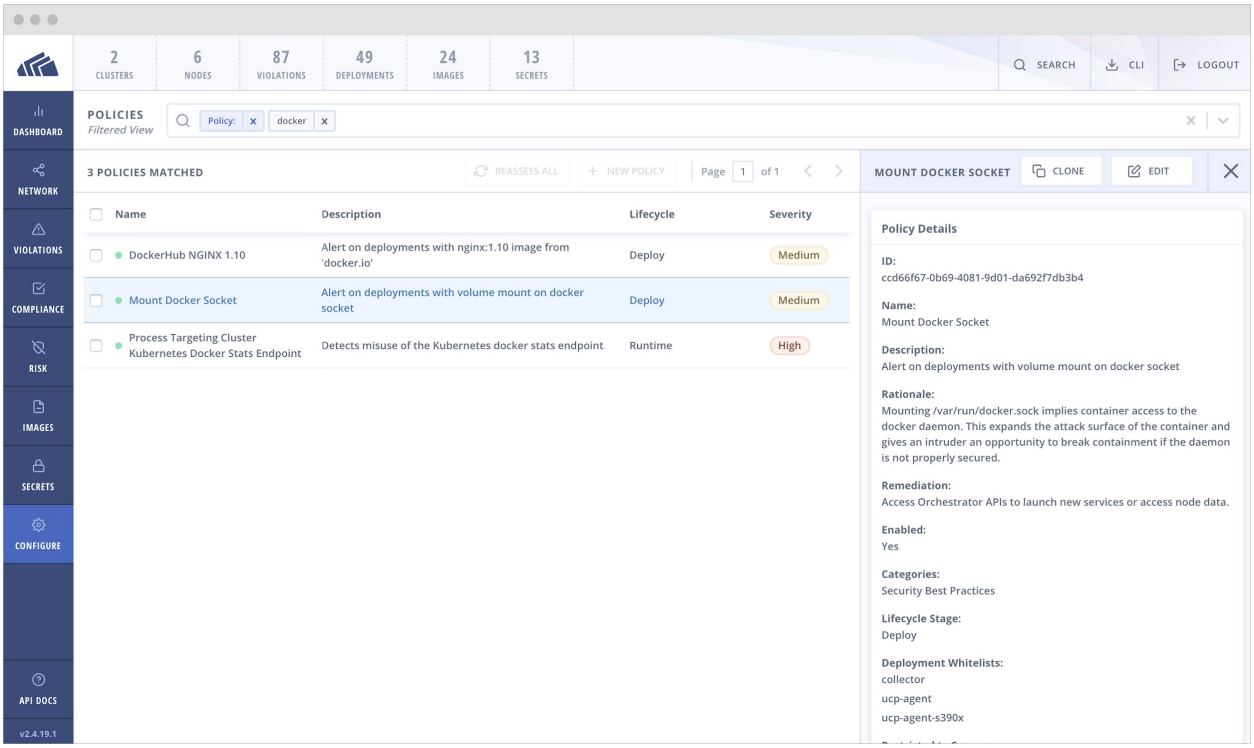
4.5.5 - Host file system tampering

Ensure that containers are running with the minimal set of file system permissions required.

How StackRox helps

StackRox analyzes the volumes being mounted in every deployment and can detect if a deployment has mounted any files or directories from the underlying host file system.

- StackRox can detect, alert on, or block deployments that mount sensitive host paths.
- StackRox ships with a built-in policy for /var/run/docker.sock and can be configured to match any other host path.



Summary and FREE Assessment

Changes in the infrastructure of the cloud-native development stack, including containers and orchestrators such as Kubernetes, are changing the security landscape and, as a result, are driving the need to employ security best practices and standards such as NIST SP 800-190.

To help you understand the state of NIST SP 800-190 compliance in your environment, StackRox offers a FREE container risk assessment.

StackRox synthesizes information across your various container platforms and tool sets and transforms them into actionable security insights. The comprehensive report you'll get from this assessment will show you:

- the overall security health of your clusters
- services deployed with high-risk combinations of vulnerabilities and misconfigurations
- CIS benchmark failures that may affect compliance requirements with NIST SP 800-190
- key vulnerabilities across your container attack surface
- configuration best practices for DevOps teams

AUDIT YOUR CONTAINER SECURITY AT:
https://www.stackrox.com/assessment/

LET'S GET STARTED

Request a demo today!
info@stackrox.com
+1 (650) 489-6769
www.stackrox.com