

Guide to NIST SP 800-190 compliance in container environments

Understanding the threat landscape for container usage

Organizations are eagerly adopting containers, Kubernetes, and microservices, but security concerns can be an impediment, as our latest [State of Kubernetes Security Report¹](#) reveals. While many are embracing containers in their organizations, some are still learning about containers and Kubernetes themselves—understanding that the security implications of this infrastructure add to the learning curve. It is critical to understand the threat landscape in these environments, assess your risk posture when using containers, and mitigate the security risks associated with container adoption.

One tool to help better understand how to safeguard containers comes from the National Institute of Standards and Technology (NIST). [NIST Special Publication \(SP\) 800-190²](#) 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 this guide to understand the key recommendations of NIST SP 800-190 and gain detailed descriptions of solutions: customers comply with NIST SP 800-190.

Red Hat OpenShift Platform Plus

Red Hat® OpenShift® Platform Plus is a unified platform to build, modernize, and deploy applications at scale. Multicloud security, compliance, application, and data management work across infrastructures to provide consistency throughout the software supply chain. OpenShift Platform Plus helps you optimize and accelerate with a complete set of services for bringing applications to market on your hybrid cloud environment.

- ▶ OpenShift Platform Plus includes:
- ▶ Red Hat OpenShift Container Platform
- ▶ Red Hat Advanced Cluster Security for Kubernetes
- ▶ Red Hat Advanced Cluster Management for Kubernetes
- ▶ Red Hat OpenShift Data Foundation
- ▶ Red Hat Quay

¹ Red Hat report. “Kubernetes adoption, security, and market trends report 2023,” 17 April 2023.

² NIST. “National Institute of Standards and Technology Special Publication 800-190.” accessed 8 May 2024.

Kubernetes security at a glance

The most effective way to secure containerized applications in Kubernetes environments requires embedding security controls into each phase of the container life cycle: Build, deploy, and runtime.

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 life cycle by applying best practices and identifying and eliminating known vulnerabilities early.

Deploy

In the deploy phase, developers configure containerized applications for deployment into production. Context grows beyond information about images to include details about Kubernetes configuration options available for 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 effect of potential compromises.

Runtime

Containers go into production with live data, live users, and exposure to networks, such as an internal or public internet. During the runtime phase, the primary purpose of security is to protect both running applications and the Kubernetes infrastructure by finding and stopping malicious actors in real-time.

In conjunction with protecting containers across their life cycle, you must also safeguard the underlying infrastructure and make sure that 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 and the containerized applications they run.

How OpenShift Platform Plus supports NIST SP 800-190

OpenShift Platform Plus is our unified hybrid platform to build, modernize, and deploy applications at scale. The following details map the features of OpenShift Platform Plus to guidance provided in NIST SP 800-190.

NIST Standard 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 life cycle 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 makes certain only images meeting your policy requirements is allowed to progress.

Solutions

Red Hat Quay:

1. Clair can scan images for vulnerabilities using a number of vulnerability databases to find existing vulnerabilities in images.
2. Clair also reports vulnerability and security information for golang, java, and ruby ecosystems through the open source vulnerability (OSV) database.

Red Hat Advanced Cluster Management:

1. Uses an extensible policy framework for configuration management across multiple clusters.
2. Uses placement rules to bind policies to managed clusters.
3. Supports the integration with the compliance operator.
4. Supports multiple policy engines, including Gatekeeper, Open Policy Agent (OPA), and Kyverno.
5. Supports GitOps deployed policies.
6. Applicable to the entire hardware and software stack.
7. Provides out-of-the-box policies for security, resiliency, and software engineering controls that are not provided by the compliance operator.

Red Hat Advanced Cluster Security:

1. Integration with your continuous integration and continuous delivery (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 and detailed reporting.
3. Out-of-the-box policies with enforcement that makes certain only images that are compliant with your policies progress.

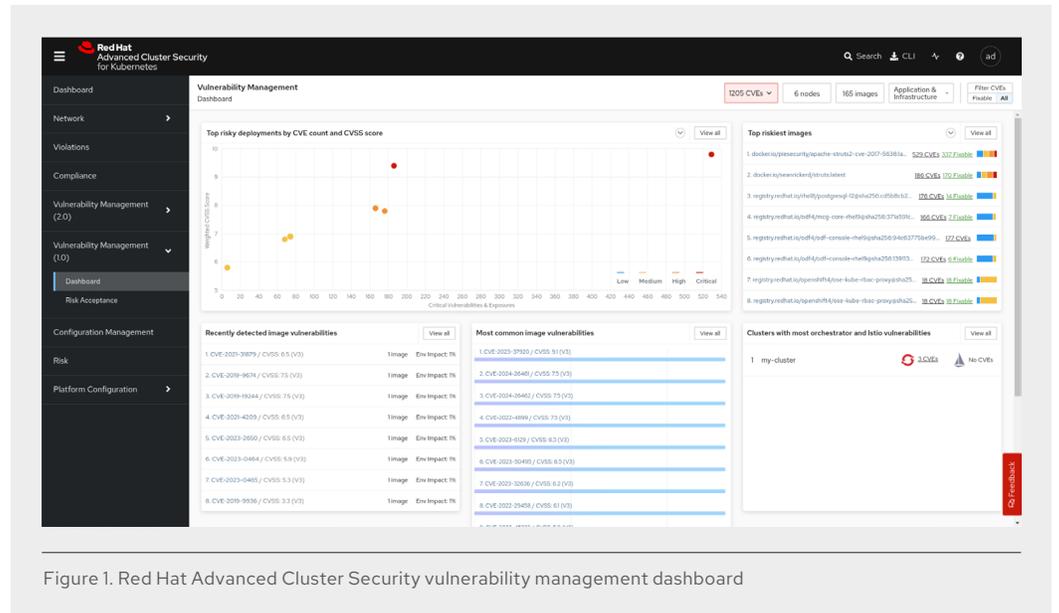


Figure 1. Red Hat Advanced Cluster Security vulnerability management dashboard

4.1.2 - Image configuration defects

Organizations should implement security controls and processes that make sure compliance with security-focused configuration best practices. This includes:

1. The 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.

Solutions

Red Hat Advanced Cluster Security:

1. Supports image scanning natively, but can also integrate with your existing image.
2. 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.
3. Provides real-time and continuous visibility and monitoring of all deployed images to ensure compliance during build and deployment stages as well as runtime. Any images or containers in violation of your policies are prevented from running.
4. Delivers built-in capabilities that identify the use of Secure Shell (SSH) protocol within containers, including policies that alert on the exposure of port 22 and processes that appear to be SSH daemons.

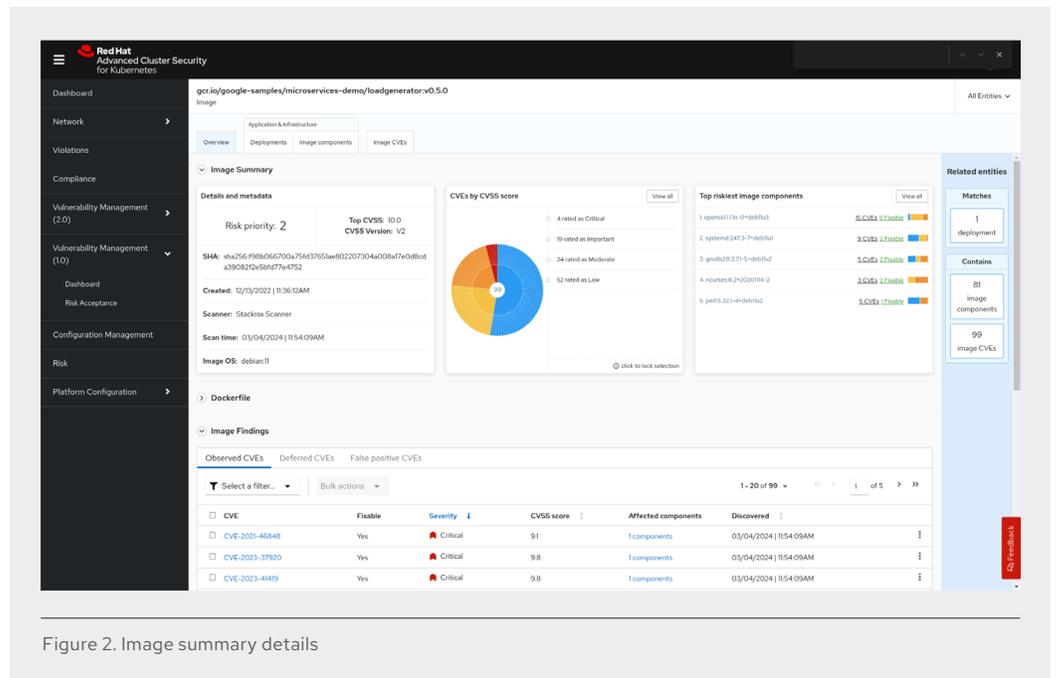


Figure 2. Image summary details

4.1.3 Embedded malware

Organizations should continuously monitor images for embedded malware. The monitoring processes should include the use of malware signature sets and behavioral detection heuristics based largely on actual “in the wild” attacks.

Solutions

OpenShift Container Platform:

1. The file integrity operator continually runs file integrity checks on the cluster nodes.
2. Deploys a daemonset which uses the Advanced Intrusion Detection Environment (AIDE) providing a status object with a log of files that are modified during the initial run of the daemon set pods.

Red Hat Advanced Cluster Security:

1. Detects anomalous activity indicative of malicious intent such as those exhibited by embedded malware.
2. Provides out-of-the-box policies that ensure insecure registries are not used.

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.

Solutions

Red Hat Advanced Advanced Cluster Security:

1. Provides out-of-the-box policies that detect instances where secrets are being delivered in an insecure manner, including in environment variables.
2. Examines the metadata about the secrets configured in monitored clusters, including the deployments configured to reference those secrets.
3. Helps make certain that secrets transmitted via Kubernetes are only accessible to containers that are configured to use them.

4.1.5 - Use of untrusted images

Organizations should maintain a set of trusted images and registries and ensure that only images from this set are allowed to run in their environment, thus mitigating the risk of untrusted or malicious components being deployed.

Solutions

OpenShift Container Platform:

1. Delivers signatures for the images in the Red Hat Container Registries which can be automatically verified when being pulled to OpenShift Container Platform 4 clusters by using the Machine Config Operator (MCO).
2. Allows customers to create and sign their own images using sigstore and verifying those signatures before allowing them to be deployed in their OpenShift Container Platform.
3. Trusted Artifact Signer empowers software developers and consumers to safely sign and verify software artifacts—source code, release files, images, binaries, SBOM, playbook, and more to enhance software supply chain security.

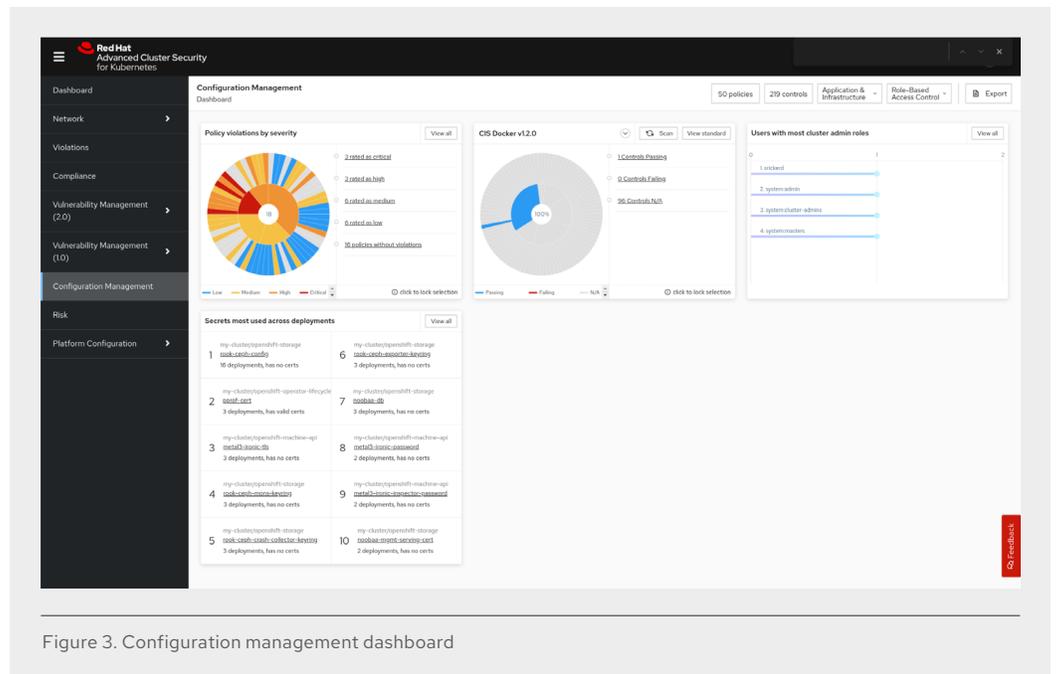


Figure 3. Configuration management dashboard

4.2.1 - Insecure connections to registries

Use a secure or encrypted connection when pushing and pulling from a registry.

Solutions

Red Hat Advanced Cluster Security:

1. By default, the CRI-O engine will not pull from unencrypted registries. However it does provide the option of whitelisting registries where insecure connections are used. Red Hat Advanced Cluster Security analyzes the configuration of your CRI-O engine on cluster nodes and identifies exceptions where an unencrypted registry is being whitelisted.
2. The solution flags images whose tags or references begin with http://.

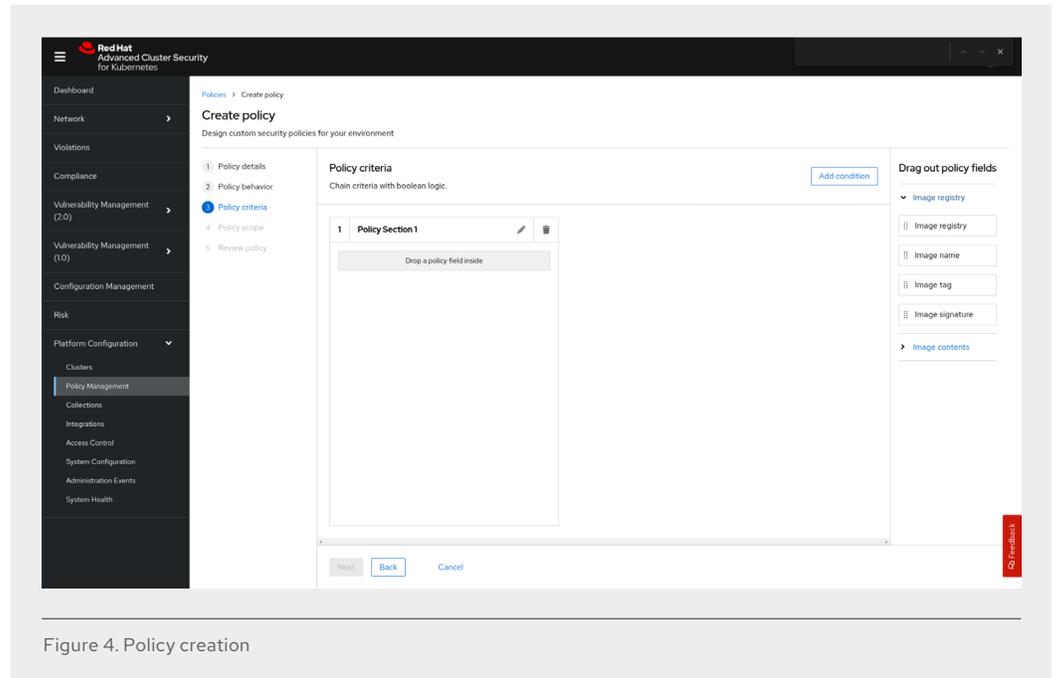


Figure 4. Policy creation

4.2.2 - Stale images in registries

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

Solutions

Red Hat Advanced Cluster Security:

1. The solution has a prebuilt policy intended to discourage the use of the latest tag and instead recommends accessing images using immutable names that include image versions.
2. It also provides an out-of-the-box policy to flag the use of images built more than 90 days ago. Alternatively, you can configure the policy to look for shorter or longer time windows as it fits your specific needs.
3. Lastly, we incorporate image age as one of the risk factors when providing the risk score for each deployment.

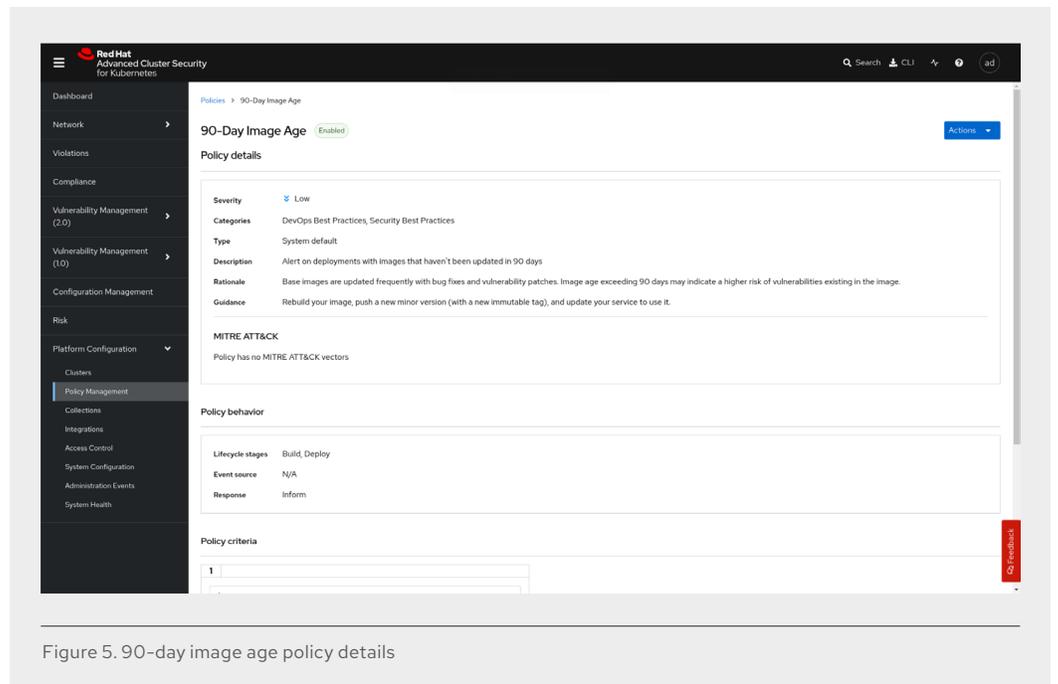


Figure 5. 90-day image age policy details

4.2.3 - Insufficient authentication and authorization restrictions

All access to registries that contain proprietary or sensitive images should require authentication.

Solutions

Red Hat Quay:

1. Supports role-based access control (RBAC) for repositories, allowing for organizations to grant and restrict read, write, and admin access to repositories, thus securing proprietary or sensitive images.
2. Supports the integration of OpenID Connect protocol (OIDC) methods such as Red Hat's single sign-on technology, Google, Github, Microsoft, or others.

4.3.1 - Unbounded administrative access

Orchestrators should use a least privilege access model in which users are only granted the ability to perform the specific actions on the specific hosts, containers, and images their job roles require.

Solutions

OpenShift Container Platform:

1. Requires the cluster administrator to grant more privileged roles to users
2. Allows for segmentation of teams by projects.
3. Allows for RBAC to individual namespaces and projects.

4.3.2 - Unauthorized access

Access to cluster-wide administrative accounts should be tightly controlled as these accounts provide the ability to affect all resources in the environment. Organizations should use strong authentication methods, such as requiring multifactor authentication instead of just a password.

Solutions

OpenShift Platform Plus:

- ▶ Support for OIDC providers such as Red Hat's single sign-on technology across the breadth of the platform.

4.3.3 - Poorly separated inter-container network traffic

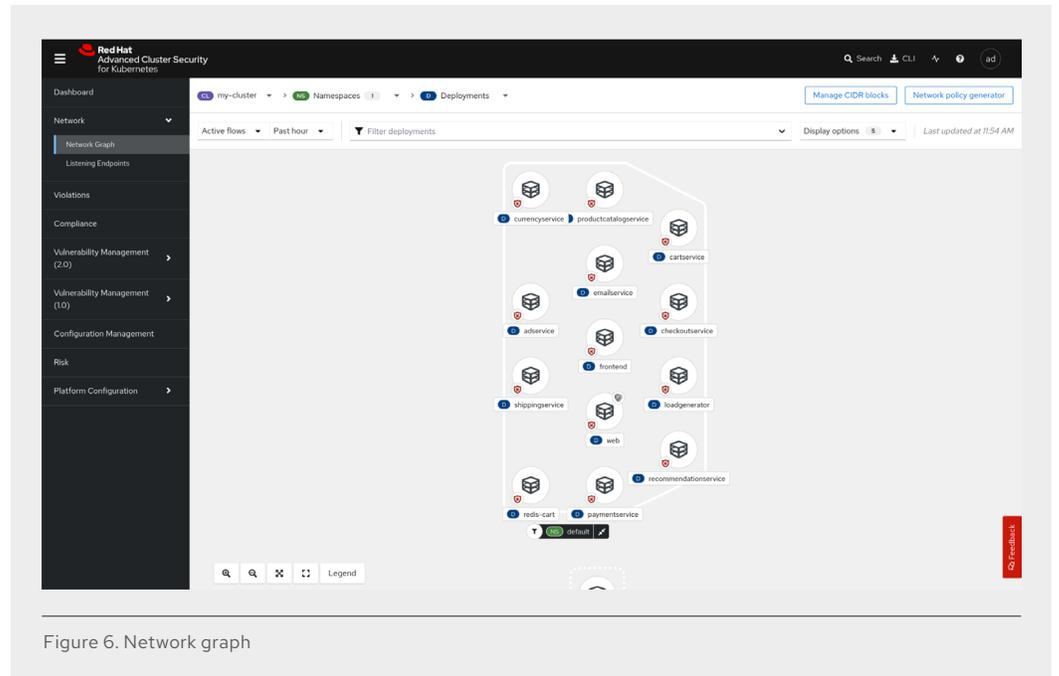
Configure Kubernetes such that you are segmenting network traffic to decrease your risk exposure. As a first step, you should define networks by sensitivity level and ensure separation of sensitive and non-sensitive networks.

For example, applications open to the broader internet can share a virtual network, internal facing applications can use another, and communication between the 2 should occur through a small number of well-defined interfaces.

Solutions

Red Hat Advanced Cluster Security:

1. Runs checks to see if your Kubernetes network segmentation rules are applied to all of your deployments.
2. Provides a visual simulation of your existing network connections to help you understand your network topology. The Network Graph identifies allowed and active connections to help you identify gaps in your inter-application segmentation policies.
3. Generates on-demand network policies (YAML files) and pushes them to your Kubernetes deployment for a better network security posture.



4.3.4 - Mixing of workload sensitivity levels

Orchestrators should be configured to isolate deployments to specific sets of hosts by sensitivity levels.

Solutions

OpenShift Container Platform:

- ▶ Uses taints within the OpenShift Container Platform.

Red Hat Advanced Cluster Security:

- ▶ Allows security policies to be enforced by the host.

Red Hat Advanced Cluster Management:

1. Provides out-of-the-box policies for security, resiliency, and software engineering controls that are not provided by the compliance operator.
2. Supports an active upstream community for collaborative development of policies.

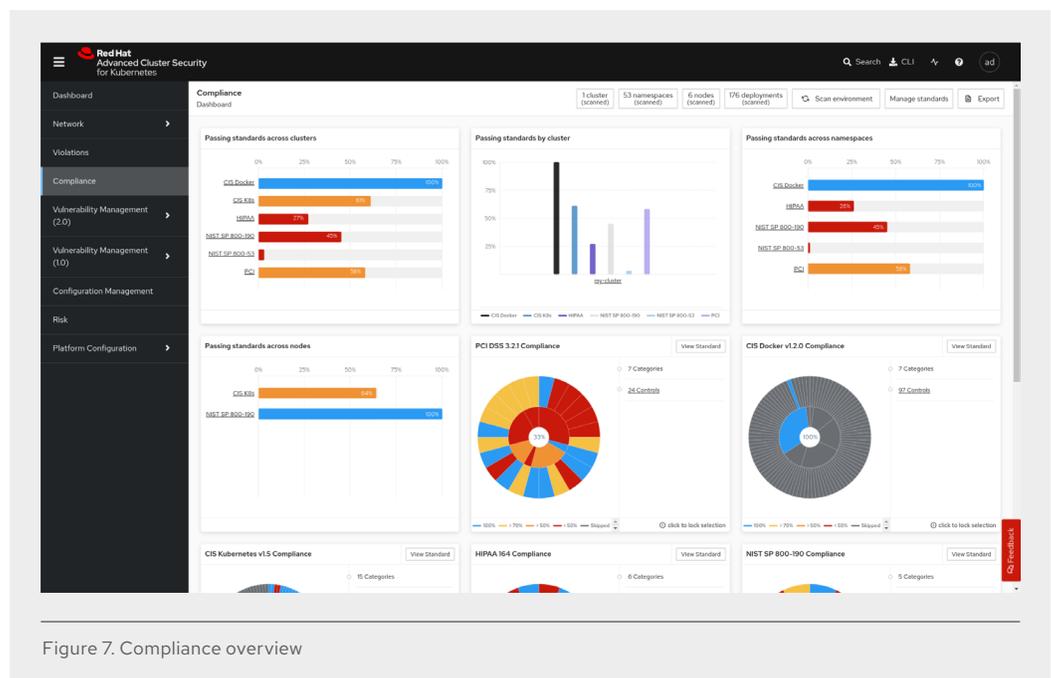
4.3.5 - Orchestrator node trust

Your Kubernetes deployment should safely introduce nodes to the cluster, have a persistent identity throughout their life cycle, 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 affecting overall operations.

Solutions

Red Hat Advanced Cluster Security:

1. Check to see if you have scanned your deployments against the above-mentioned policies.
2. Flag deployments that have not been scanned.
3. Identify policy violations.
4. Present additional opportunities to harden your Kubernetes environment.



4.4.1 - Vulnerabilities within the runtime software

The container runtime must be carefully monitored for vulnerabilities, and when problems are detected, they must be remediated quickly.

Solutions

Red Hat Advanced Cluster Security:

1. Scan Red Hat Enterprise Linux® CoreOS nodes for vulnerabilities and detect potential security threats.
2. Includes the scanning of the runtime software.

OpenShift Container Platform:

- ▶ Dashboard will alert organizations of available upgrades to ensure the entire environment is kept up to date.

Red Hat Advanced Cluster Management:

1. Tag based organization of multicluster to ensure proper isolation of non-compliant clusters.
2. Alert system with multiple integrations to third parties.

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.

Solutions

Red Hat Advanced Cluster Security:

1. Runs checks to see if your Kubernetes network segmentation rules are applied to all of your deployments.
2. Provides a visual simulation of your existing network connections to help you understand your network topology. The Network Graph identifies allowed and active connections to help you identify gaps in your inter-application segmentation policies.
3. Generates on-demand network policies (YAML files) and pushes them to your Kubernetes deployment for a better network security posture.

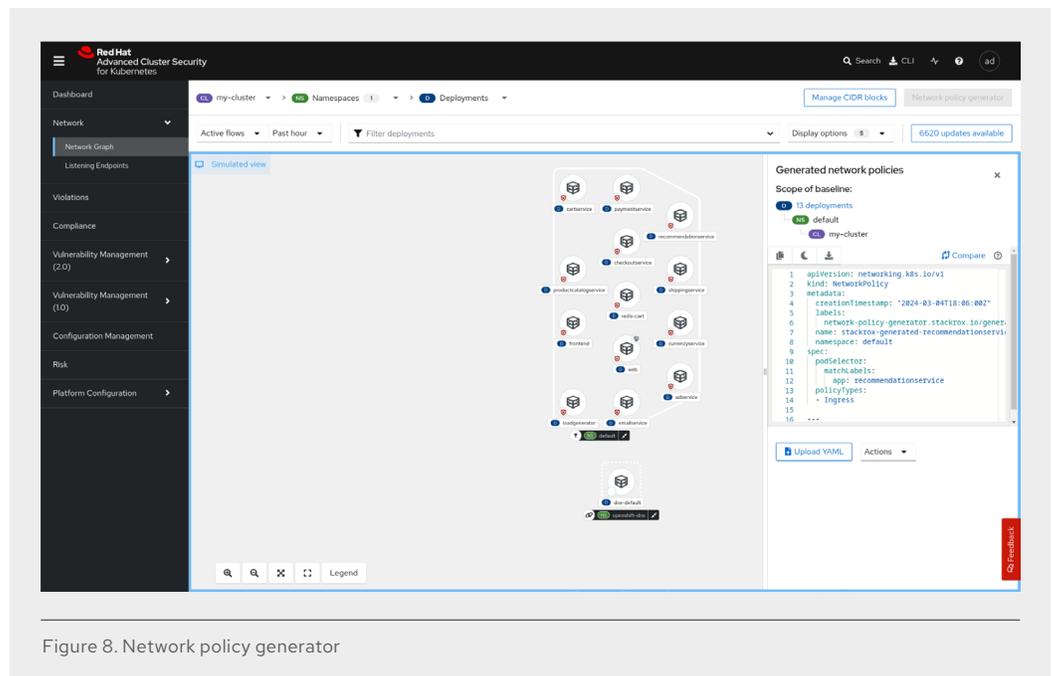


Figure 8. Network policy generator

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.

Solutions

Red Hat Advanced Cluster Security:

- ▶ Scans your environment and runs compliance checks against CIS Docker and Kubernetes Benchmarks to ensure continuous compliance across your container environment.

In addition, there are out-of-the-box compliance policies for:

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

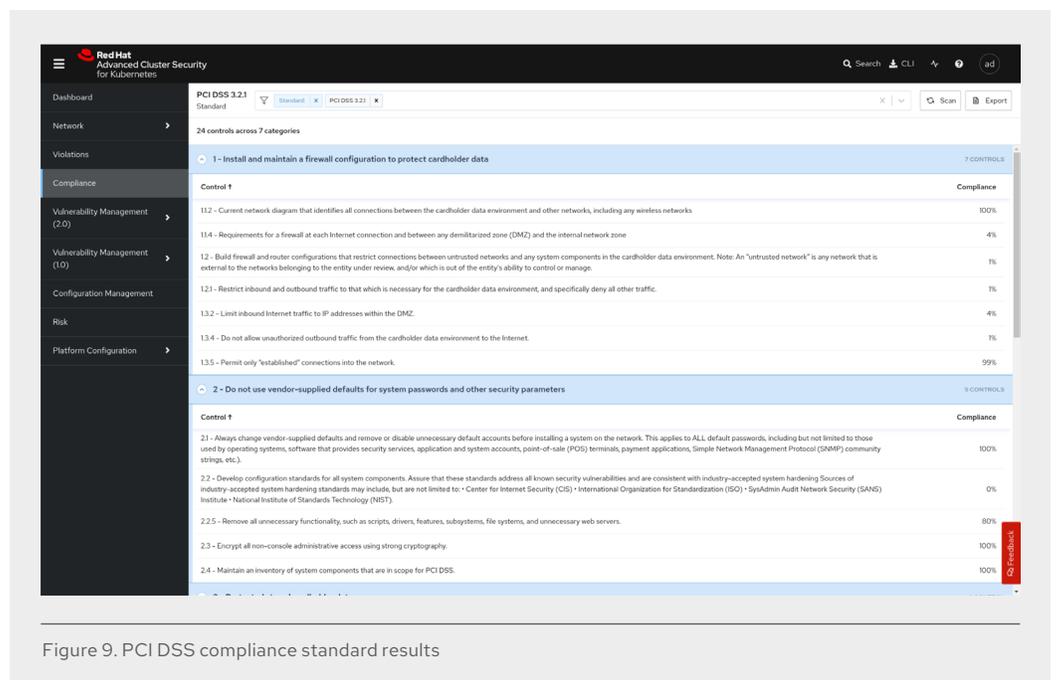


Figure 9. PCI DSS compliance standard results

4.4.4 - Application vulnerabilities

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

Solutions

Red Hat Advanced Cluster Security:

Combines behavioral modeling with rules and allowlisting to detect threats to containers, including unexpected activity. Examples include:

1. Out-of-the-box policies to detect the use of package managers and suspicious process execution based on filenames and paths.
2. On-demand scans to identify risky configurations that could lead to changes on the host, such as changes to important system files.

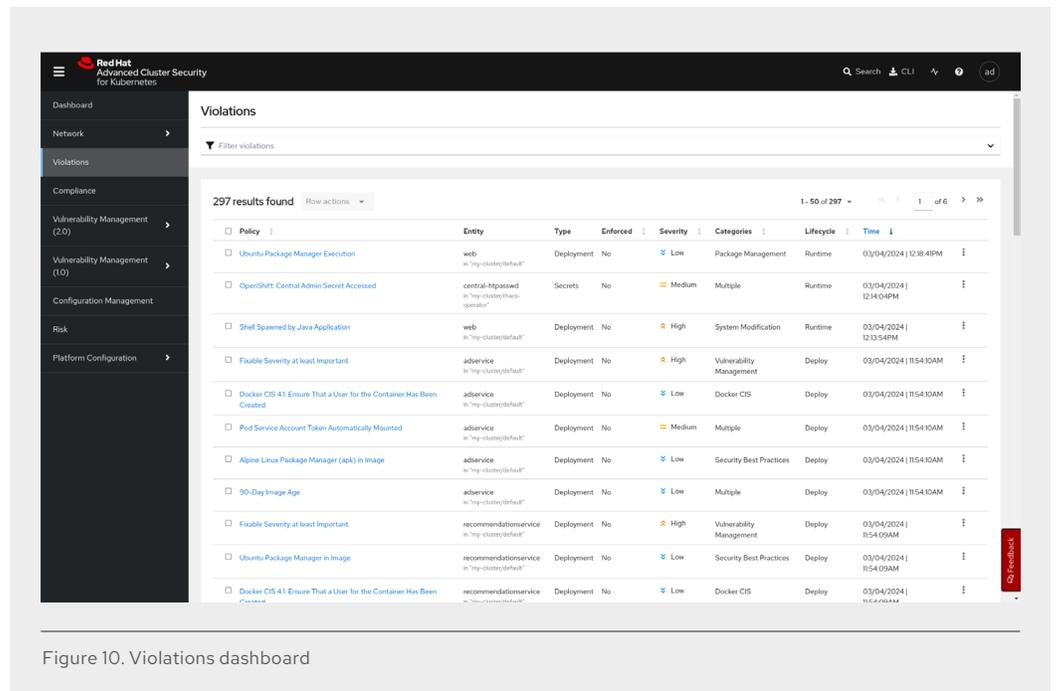


Figure 10. Violations dashboard

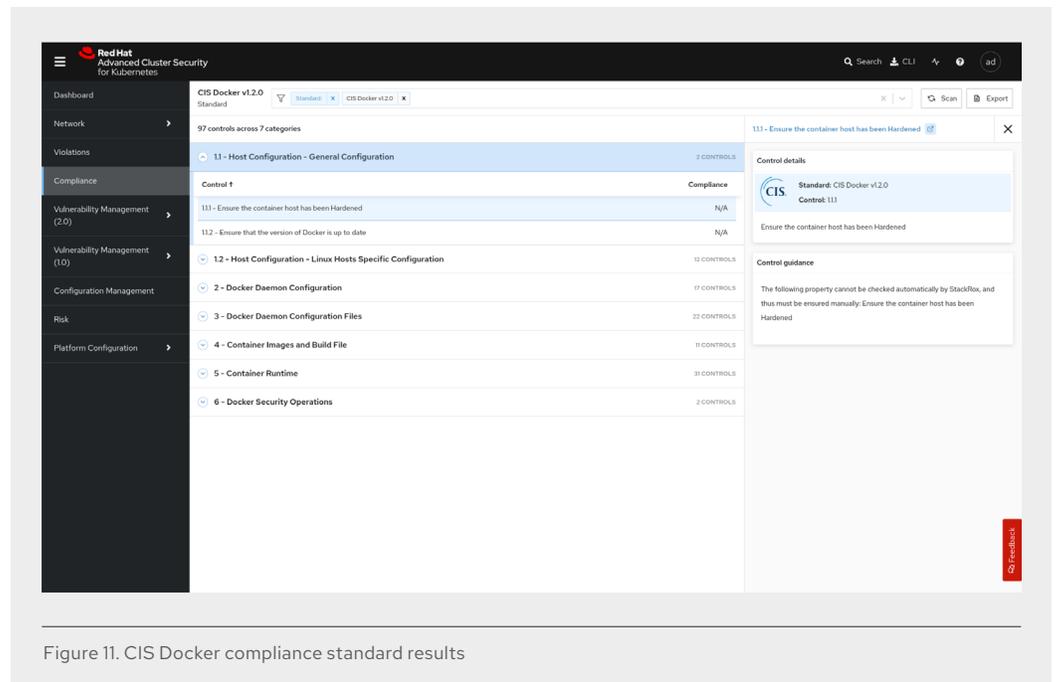
4.5.1 - Large attack surface

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

Solutions

Red hat Advanced Cluster Security:

1. Supports the use of container-specific OS such as CoreOS and Google Container Optimized OS.
2. Identifies the node OS deployed in clusters to verify use of a container-specific OS such as CoreOS or Google Container-Optimized OS as compliance evidence.
3. Allows compliance with CIS General Linux Benchmark to make certain your Linux host is configured with strengthened security.
4. Allows compliance with the CIS Docker and Kubernetes benchmarks to make sure your environment is hardened, in instances where a container-specific OS is not being used.



4.5.2 - Shared kernel

Organizations should not mix containerized and non-containerized workloads on the same host instance.

Solutions

OpenShift Container Platform:

- ▶ The supported installation is one where Red Hat OpenShift is the sole workload on the hosts. To be supportable, other workloads should not be running on the same hosts as OpenShift Container Platform.

4.5.3 - Host OS component vulnerabilities

Organizations should implement management practices and tools to validate the versioning of components provided for base OS management and functionality.

Solutions

Red Hat Advanced Cluster Security:

- ▶ Capable of scanning Red Hat CoreOS nodes for vulnerabilities and detecting potential security threats. Red Hat Advanced Cluster Security scans Red Hat CoreOS RPMs installed on the node host, as part of the Red Hat CoreOS installation, for any known vulnerabilities.

4.5.4 - Improper user access rights

Organizations should still ensure that all authentication to the OS is audited, login anomalies are monitored, and any escalation to perform privileged operations is logged.

Solutions

OpenShift Container Platform:

- ▶ Limits access to the host OS. The recommended method to access the host OS is through the `oc debug` command.

Red Hat Advanced Cluster Security:

- ▶ Can monitor the processes while the debug pod is running. A policy could also be created to monitor any pod that contains annotations such as `privileged=true`.

4.5.5 - Host file system tampering

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

Solutions

Red Hat Advanced Cluster Security:

Analyzes the volumes being mounted in every deployment and detects if a deployment has mounted any files or directories from the underlying host file system, including:

1. Detecting, alerting on, or blocking deployments that mount sensitive host paths.
2. Providing a built-in policy for `/var/run/docker.sock`, `/var/run/crio/crio.sock`, and `/run/crio/crio.sock`, and can be configured to match any other host path.

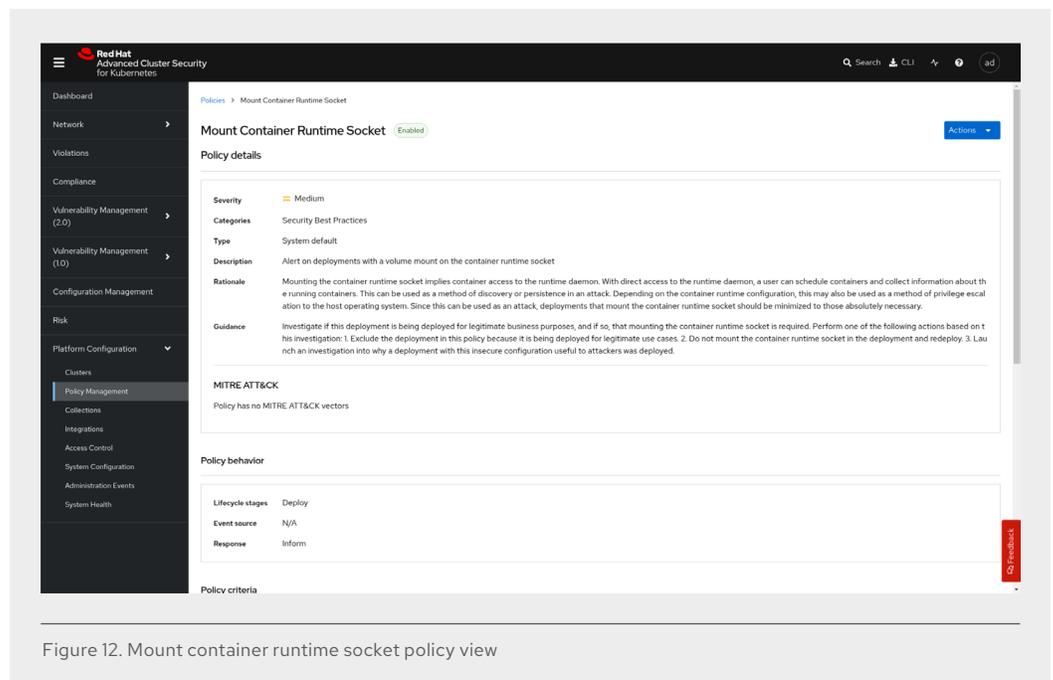


Figure 12. Mount container runtime socket policy view

Summary

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

To help you understand the state of NIST SP 800-190 compliance in your environment, [try out](#) Red Hat Advanced Cluster Security. You will experience:

1. The overall security health of your clusters against NIST SP 800-190 controls.
2. Services deployed with high-risk combinations of vulnerabilities and misconfigurations.
3. CIS benchmark failures that may affect compliance requirements with NIST SP 800-190.
4. Key vulnerabilities across your container attack surface.
5. Configuration best practices for DevOps teams.

For an enterprise deployment, we strongly recommend investing in OpenShift Platform Plus, which includes OpenShift Container Platform, Red Hat Advanced Cluster Security, Red Hat Advanced Cluster Management, Red Hat Data Foundations, and Quay. By using these products, you can adhere to the major risk point of NIST SP 800-190 compliance.

Further reading: Implementing Kubernetes-native security with Red Hat

Security platforms purpose-built to protect Kubernetes offer powerful security and operational advantages. Kubernetes-native security applies controls at the Kubernetes layer, ensuring consistency, automation, and scale. Organizations successfully deploy security as code, providing security that is built-in, not bolted on.

Download this whitepaper, "[Kubernetes-native Security: what is it and why it matters](#)" to find out more about the key features and benefits of Kubernetes-native security, and how it is different from existing container security approaches to deliver protections that are purpose-built for Kubernetes environments.



About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers develop cloud-native applications, integrate existing and new IT applications, and automate and manage complex environments. [A trusted adviser to the Fortune 500](#), Red Hat provides [award-winning](#) support, training, and consulting services that bring the benefits of open innovation to any industry. Red Hat is a connective hub in a global network of enterprises, partners, and communities, helping organizations grow, transform, and prepare for the digital future.

[f facebook.com/redhatinc](https://facebook.com/redhatinc)
[@RedHat](https://twitter.com/RedHat)
[in linkedin.com/company/red-hat](https://linkedin.com/company/red-hat)

North America
 1 888 REDHAT1

**Europe, Middle East,
and Africa**
 00800 7334 2835
europa@redhat.com

Asia Pacific
 +65 6490 4200
apac@redhat.com

Latin America
 +54 11 4329 7300
info-latam@redhat.com