

Red Hat Advanced Cluster Security for Kubernetes

A Kubernetes-native security solution for cloud-native applications

Introduction

Protecting cloud-native applications requires significant changes in how we approach security. We must apply controls earlier in the application development lifecycle, use the infrastructure itself to apply controls, provide developer-friendly guardrails, and keep up with increasingly rapid release schedules.

Red Hat® Advanced Cluster Security for Kubernetes, powered by StackRox, protects your vital applications across build, deploy, and runtime. Our software deploys in your Kubernetes infrastructure as a self-managed security solution or you can consume it as a fully managed Software-as-a-Service (SaaS). Additionally, it integrates with your existing DevOps tooling and workflows to deliver dependable security and compliance. The policy engine includes hundreds of built-in controls to enforce DevOps and security-focused practices based on industry standards such as Center for Internet Security (CIS), Benchmarks and National Institute of Standards Technology (NIST) guidelines, configuration management of both containers and Kubernetes, and runtime security.

Red Hat Advanced Cluster Security provides a Kubernetes-native architecture for platform and application security, allowing DevOps and InfoSec teams to operationalize security.

Features and benefits

► Lower operational cost

- Guide development, operations and security teams towards a common set of Kubernetes-native security tooling and practices, and providing guardrails for individual users.
- Use Kubernetes-native controls across the build, deploy and runtime phases of the application for better visibility and management of vulnerabilities, policy and configuration violations, and application runtime behavior.
- Reduce the cost of addressing a security issue by catching and fixing it in the development stage (Shift Left).

► Reduce operational risk

- Align security and infrastructure to reduce application downtime using built-in Kubernetes capabilities, such as Kubernetes network policies for segmentation, and admission controller for security policy enforcement.
- Mitigate threats using Kubernetes-native security controls to enforce security policies, minimizing potential impacts to your applications and infrastructure operations. For example, using controls to contain a successful breach by automatically instructing Kubernetes to scale suspicious pods to zero or to delete then restart instances of breached applications.

► Increase developer productivity

- Actively scan for vulnerabilities in repositories, development pipelines and in production.

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

- ▶ Take advantage of Kubernetes and existing continuous integration and continuous delivery (CI/CD) tooling to provide integrated security guardrails supporting developer velocity while still maintaining the desired security posture.
- ▶ Synchronize updates and support with Red Hat OpenShift® releases, ensuring compatibility and up-to-date security features.
- ▶ Use Red Hat certified vulnerability data, ensuring higher accuracy and relevance for Red Hat OpenShift environments.

Detailed benefits

| Area | Benefits |
|--------------------------|--|
| Visibility | <ul style="list-style-type: none">• Delivers a comprehensive view of your Kubernetes environment, including all images, pods, deployments, namespaces, and configurations.• Discovers and displays network traffic in all clusters spanning namespaces, deployments, and pods .• Captures critical system-level events in each container for incident detection. |
| Vulnerability management | <ul style="list-style-type: none">• Detect host-level vulnerabilities and potential security threats in Red Hat Enterprise Linux® CoreOS.• Scan images for known vulnerabilities in specific languages, packages, and image layers.• Highlight the riskiest image vulnerabilities and deployments to prioritize response.• Correlate vulnerabilities to namespaces, running deployments, and images.• Categorize findings by platform, node, workload to simplify tracking and ownership.• Enforce policies based on vulnerability details at build, deploy and runtime.• Integrate ACS with third-party solutions using roxctl and/or the application programming interface (API) to provide vulnerability notifications in the tools teams use everyday (Jira and ServiceNow). |

| Area | Benefits |
|----------------------|---|
| Compliance | <ul style="list-style-type: none">• Assess compliance with technical controls from security and regulatory frameworks, including CIS, payment card industry (PCI), NIST SP 800-53, DISA STIG, and NERC-CIP.• View overall compliance across the controls of each standard with the ability to export evidence for auditors.• Drill-down to detailed views of compliance results to pinpoint clusters, namespaces, nodes, or deployments namespaces that require remediation.• Schedule compliance scans and automate creation of evidence-based reports. |
| Network segmentation | <ul style="list-style-type: none">• Visualize allowed vs. active traffic between namespaces, deployments, and pods, including external exposures at runtime.• Identify running processes listening on ports.• Identify anomalous network traffic and inform and enforce runtime policies.• Alert on policy violations when forbidden traffic is observed.• Generate a connectivity graph and show contextual diff between 2 versions of the application prior to deployment.• Simulate network policy changes in runtime before they are implemented to minimize operational risk to the environment.• Shift-left creation of Kubernetes network policies by analyzing application manifests prior to deployment. |
| Risk profiling | <ul style="list-style-type: none">• Heuristically ranks running deployments according to their overall security risk by combining factors such as vulnerabilities, configuration policy violations, and runtime activity.• Track changes in the security posture of your Kubernetes deployments to validate the effect of your security team's actions.• Search running deployments in all clusters to model threat vectors and uncover risk patterns. |

| Area | Benefits |
|---------------------------------------|--|
| Configuration management | <ul style="list-style-type: none">• Deliver prebuilt DevOps and security policies to identify configuration violations related to network exposures, privileged containers, processes running as root, and compliance with industry standards.• Analyze Kubernetes role-based access control (RBAC) settings to determine user or service account privileges and misconfigurations.• Track secrets and detect which deployments use the secrets to limit access.• Enforce configuration policies—at build time with CI/CD integration and at deploy time using dynamic admission control. |
| Runtime detection and response | <ul style="list-style-type: none">• Monitor events to detect anomalous activity indicative of a threat with correlation to Kubernetes objects.• Implement non-destructive automated response using Kubernetes-native controls with minimal effect on business operations.• Baseline process activity in containers to whitelist processes automatically, eliminating the need to manually whitelist.• Use prebuilt policies to detect crypto mining, privilege escalation, and various exploits.• Monitor Kubernetes admin events and block malicious behavior.• Integrate with external security integration event management (SIEM) and security orchestration, automation, and response (SOAR) solutions to power remediation workflows. |

| Area | Benefits |
|----------------------------|--|
| Security policy guardrails | <ul style="list-style-type: none">• Identify security configuration weaknesses such as network exposures, privileged containers, processes running as root, with out-of-the-box policies that can be applied at build, deploy or runtime.• Create custom policies based on Kubernetes-native constructs, including Kubernetes API, audit logs, namespace resources.• Provide supply chain security by integrating Advanced Cluster Security with CI/CD pipelines to check for known vulnerabilities and misconfigurations prior to deployment.• Verify image signatures for image attestation and integrity.• Analyze Kubernetes role-based access control (RBAC) settings to flag user or service account privileges and misconfigurations.• Track secrets and detect which deployments use the secrets.• Scale management of policies through the use of Kubernetes labels and by managing policies as code. |
| Integrations | <ul style="list-style-type: none">• Provides a rich API and prebuilt plugins to integrate with DevOps systems, including CI/CD tools, image scanners, sigstore, registries, container runtimes, SIEM solutions, and notification tools. |



Ready to see Red Hat Advanced Cluster Security in action?

Start your no-cost trial today



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.

 facebook.com/redhatinc
 @RedHat
 linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

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

Asia Pacific
+65 6490 4200
apac@redhat.com

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