Red Hat
Advanced Cluster Security
for Kubernetes

Red Hat Advanced Cluster Security for Kubernetes

Better 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, use the infrastructure itself to apply controls, and keep up with increasingly rapid release schedules.

Red Hat® Advanced Cluster Security for Kubernetes, powered by StackRox technology, 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 better security and compliance. The policy engine includes hundreds of built-in controls to enforce DevOps and security best practices, industry standards such as 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 for Kubernetes provides a Kubernetes-native architecture for container security, enabling DevOps and InfoSec teams to operationalize security.

Features and benefits

- Kubernetes-native security:
- Increases protection.
- Eliminates blind spots, providing staff with insights into critical vulnerabilities and threat vectors.
- Reduces time and costs.
- Reduces the time and effort needed to implement security and streamlines security analysis, investigation, and remediation using the rich context Kubernetes provides.
- Increases scalability and portability.
- Provides scalability and resiliency native to Kubernetes, avoiding operational conflict and complexity that can result from out-of-band security controls.

Detailed benefits

Area	Benefits
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, packages, image layers ▸ Correlates vulnerabilities to running deployments, not just images ▸ Enforces policies based on vulnerability details—at build time using continuous integration/continuous delivery (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, payment card industry (PCI), Health Insurance Portability and Accountability Act (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 ▸ Provides detailed view of 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 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 ▸ Uses network enforcement capabilities built into Kubernetes to ensure consistent, portable, and scalable segmentation
Risk profiling	▸ Ranks your running deployments according to their security risk, taking advantage of 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

Area	Benefits
Configuration management	▸ Delivers prebuilt 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 role-based access control (RBAC) settings to determine user or service account privileges and misconfigurations ▸ Tracks secrets and detects which deployments use the secrets 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 ▸ Uses prebuilt policies to detect crypto mining, privilege escalation, and various exploits ▸ Enables flexible system-level data collection using either external Berkeley Packet Finder (eBPF) or a kernel module across every major Linux distribution
Integrations	▸ Provides a rich application programming interface (API) and prebuilt plugins to integrate with DevOps systems, including CI/CD tools, image scanners, registries, container runtimes, security integration event management (SIEM) solutions , and notification tools

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 integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations 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

redhat.com
#F27185_0221