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 life cycle, 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 better security and compliance. The policy engine includes hundreds of built-in controls to enforce DevOps and security-focused best 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 using a common language and source of truth—driving down the operational costs of team silos.
  - 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.
- **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 kill then restart instances of breached applications.

- **Increase developer productivity**
  - 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.
  - Accelerate your organization's pace of innovation and provide developers actionable guidance by standardizing on Kubernetes as the common platform for declarative and continuous security across development, security, and operations.

Detailed benefits

Area	Benefits
Visibility	• 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	• Scans images for known vulnerabilities based on specific languages, packages, image layers • Provides a dashboard highlighting riskiest image vulnerabilities and deployments • Verifies image signatures against preconfigured keys for image attestation and integrity • Correlates vulnerabilities to running deployments, not just images • Enforces policies based on vulnerability details—at build time using CI/CD integrations, at deploy time using dynamic admission controls, and at runtime using native Kubernetes controls • Provides risk acceptance customization for enhanced risk-based vulnerability prioritization and false-positive reduction

Area	Benefits
Compliance	• Empowers organizations to run on-demand self-assessments that automates compliance audits • Assesses compliance across hundreds of controls for CIS Benchmarks, payment card industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP), and NIST SP 800-190 and 800-53 • Delivers at-a-glance dashboards of overall compliance across each standard's controls with evidence export to meet auditors' needs • Provides a view of compliance details to pinpoint either clusters, namespaces, nodes, or deployments that don't comply with specific standards and controls
Network segmentation	• Visualizes allowed versus active traffic between namespaces, deployments, and pods, including external exposures • Uses network enforcement capabilities built into Kubernetes to ensure consistent, portable, and scalable segmentation • Baselines network activity and recommends new Kubernetes network policies to remove unnecessary network connections • Simulates network policy changes before they're implemented to minimize operational risk to the environment
Risk profiling	• Heuristically ranks your running deployments according to their overall security risk, through combining Red Hat Advanced Cluster Security data on prioritized vulnerabilities with configuration details and runtime activity • Tracks improvements in your security posture of your Kubernetes deployments to validate the impact of your security team's actions
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

Area	Benefits
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 extended Berkeley Packet Filter (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, sigstore, registries, container runtimes, security integration event management (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

redhat.com
#F31987_0922