Red Hat
Advanced Cluster Security
for Kubernetes

# Red Hat Advanced Cluster Security for Kubernetes

## Améliorez la sécurité de Kubernetes et de vos applications cloud-native avec la seule solution de sécurité des conteneurs native pour Kubernetes

La protection des applications cloud-native nécessite des changements importants dans notre approche de la sécurité. Il faut effectuer des contrôles plus tôt dans le cycle de développement des applications, utiliser l'infrastructure elle-même pour effectuer les contrôles et rester en phase avec les calendriers de lancement toujours plus serrés.

La solution Red Hat® Advanced Cluster Security for Kubernetes, basée sur les technologies StackRox, protège vos applications essentielles pendant la création, le déploiement et l'exécution. Notre logiciel se déploie dans votre infrastructure et s'intègre à vos outils et workflows DevOps afin d'améliorer la sécurité et la conformité. Le moteur de politique intègre des centaines de contrôles pour faire appliquer les meilleures pratiques DevOps et de sécurité, les normes du secteur telles que les critères CIS (Center for Internet Security) et les directives du NIST (National Institute of Standards and Technology), ainsi que pour la gestion des configurations des conteneurs et de Kubernetes ainsi que pour la sécurité de l'exploitation.

La solution Red Hat Advanced Cluster Security for Kubernetes offre une architecture native pour Kubernetes qui permet aux équipes DevOps et InfoSec d'assurer la sécurité de vos conteneurs.

### Fonctions et avantages

- Fonctions de sécurité natives pour Kubernetes :
- Renforcement de la protection
- Les zones d'ombre sont effacées, et vous recevez des informations sur les vulnérabilités critiques ainsi que les vecteurs de menaces.
- Réduction des délais et des coûts
- Les délais et les efforts nécessaires pour mettre en œuvre la sécurité et pour simplifier les analyses, investigations et corrections sont réduits grâce au contexte riche apporté par Kubernetes.
- Amélioration de l'évolutivité et de la portabilité
- Kubernetes apporte évolutivité et résilience, en évitant les conflits et la complexité opérationnels qui peuvent découler de contrôles de sécurité hors bande.

Red Hat
Advanced Cluster Security
for Kubernetes

## Les avantages en détail

| Domaine | Avantages |
|---|---|
| Visibilité | • Offre une vision d'ensemble de vos déploiements, notamment de vos images, pods et configurations<br>• Permet la découverte et l'affichage du trafic réseau dans tous les clusters, y compris les espaces de noms, les déploiements et les pods<br>• Collecte les événements critiques au niveau du système, dans chaque conteneur |
| Gestion des vulnérabilités | • Examine les images à la recherche de vulnérabilités connues en se basant sur des langages, paquets et couches d'images spécifiques<br>• Met en corrélation les vulnérabilités avec les déploiements en cours d'exécution et pas seulement avec les images<br>• Applique les politiques en fonction des détails relatifs à la vulnérabilité : au moment de la création par une approche CI/CD, lors du déploiement à l'aide de contrôles d'admission dynamiques et lors de l'exécution via les contrôles natifs pour Kubernetes |
| Conformité | • Évalue la conformité par l'intermédiaire de centaines de contrôles : critères CIS, norme PCI (Payment Card Industry), loi HIPAA (Health Insurance Portability and Accountability Act) et norme NIST 800-190<br>• Propose des tableaux de bord qui présentent l'état global de la conformité à toutes les normes, avec la possibilité d'exporter les données pour répondre aux besoins des responsables d'audits<br>• Fournit une vue détaillée des informations de conformité pour identifier les clusters, nœuds et espaces de noms qui ne répondent pas aux normes spécifiques et ne passent pas les contrôles |
| Segmentation du réseau | • Affiche le trafic existant par rapport au trafic autorisé entre les espaces de noms, les déploiements et les pods, notamment les expositions externes<br>• Simule les modifications des politiques réseau avant leur mise en œuvre pour minimiser les risques liés à l'exploitation de l'environnement<br>• Compare l'activité du réseau à des références et recommande de nouvelles politiques réseau Kubernetes pour supprimer les connexions réseau inutiles<br>• Utilise les capacités de contrôle réseau incluses dans Kubernetes pour assurer une segmentation cohérente, portable et évolutive |
| Établissement d'un profil de risques | • Classe vos déploiements en cours selon le risque de sécurité, et se base sur les données de Kubernetes pour hiérarchiser les vulnérabilités à l'aide des détails de configuration ou de déploiement ainsi que des activités de l'environnement d'exécution<br>• Suit les améliorations apportées à la sécurité de vos déploiements Kubernetes pour valider les effets des mesures prises par vos équipes |

| Domaine | Avantages |
|---|---|
| Gestion des configurations | ▸ Fournit des politiques DevOps et de sécurité pour identifier les violations de configuration liées à l'exposition du réseau, aux conteneurs privilégiés, aux processus qui s'exécutent en tant que root et à la conformité avec les normes du secteur<br>▸ Analyse les paramètres du contrôle d'accès basé sur les rôles de Kubernetes afin de déterminer les privilèges des utilisateurs ou des services et d'identifier les erreurs de configuration<br>▸ Surveille les secrets et détecte les déploiements qui utilisent ces secrets pour limiter l'accès<br>▸ Applique des politiques de configuration, au moment de la création avec une approche CI/CD et lors du déploiement, à l'aide de contrôles d'admission dynamiques |
| Détection et réponse dans l'environnement d'exécution | ▸ Surveille les événements au niveau du système à l'intérieur des conteneurs pour détecter les activités anormales révélatrices de menaces, et prend des mesures de réponse automatisées à l'aide des contrôles natifs pour Kubernetes<br>▸ Compare l'activité des processus à l'intérieur des conteneurs à des références pour placer automatiquement les processus sur liste blanche, évitant ainsi que cette tâche soit faite manuellement<br>▸ Utilise des politiques préconçues pour détecter le minage de cryptomonnaies, la réattribution des privilèges et autres exploits<br>▸ Permet une collecte des données flexible au niveau du système, à l'aide de la technologie eBPF (extended Berkeley Packet Filter) ou d'un module de noyau sur toutes les distributions Linux majeures |
| Intégrations | ▸ Fournit une API riche et des plug-ins préconçus à intégrer aux systèmes DevOps, notamment des outils de CI/CD, des analyseurs d'images, des registres, des environnements d'exécution de conteneurs, des solutions de gestion des informations et des événements de sécurité (SIEM) et des outils de notification |

## À PROPOS DE RED HAT

Premier éditeur mondial de solutions logicielles Open Source pour les entreprises, Red Hat s'appuie sur une approche communautaire pour proposer des technologies Linux, de cloud hybride, de conteneur et Kubernetes fiables et performantes. Red Hat aide ses clients à intégrer des applications nouvelles et existantes, à développer des applications natives pour le cloud, à standardiser leur environnement sur son système d'exploitation leader sur le marché ainsi qu'à automatiser, sécuriser et gérer des environnements complexes. Red Hat propose également des services d'assistance, de formation et de certification primés qui lui ont valu le titre de conseiller de confiance auprès des entreprises du Fortune 500. Partenaire stratégique des prestataires de cloud, intégrateurs système, fournisseurs d'applications, clients et communautés Open Source, Red Hat aide les entreprises à se préparer à un avenir toujours plus numérique.

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

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)
00800 7334 2835
europe@redhat.com

FRANCE
00 33 1 4191 2323
fr.redhat.com

fr.redhat.com
#F27185_0221