Red Hat
Advanced Cluster Security
for Kubernetes

Red Hat Advanced Cluster Security for Kubernetes

Proteja mejor Kubernetes y las aplicaciones desarrolladas en la nube con la única solución de seguridad para contenedores propia de Kubernetes disponible en el sector.

Es necesario cambiar la forma en la que abordamos la seguridad para proteger las aplicaciones desarrolladas en la nube: debemos aplicar los controles en una fase más temprana del proceso de desarrollo de aplicaciones, utilizando, para ello, la infraestructura, y seguir el ritmo cada vez más rápido de las planificaciones de lanzamiento.

Red Hat® Advanced Cluster Security for Kubernetes es una solución que emplea la tecnología de StackRox para proteger las aplicaciones más importantes durante su diseño, implementación y tiempo de ejecución. El software se implementa en su infraestructura y se integra con las herramientas y los flujos de trabajo de DevOps, por lo que obtiene más seguridad y cumplimiento normativo. El motor de políticas incluye cientos de controles integrados que permiten implementar las prácticas recomendadas de DevOps y de seguridad; los estándares del sector, como los indicadores de CIS y los lineamientos del Instituto Nacional de Estándares y Tecnología (NIST); la gestión de la configuración, tanto de los contenedores como de Kubernetes, y la seguridad durante el tiempo de ejecución.

Red Hat Advanced Cluster Security for Kubernetes ofrece una arquitectura desarrollada en Kubernetes que permite proteger los contenedores mediante medidas de seguridad que ponen en marcha los equipos de DevOps y de seguridad de la información.

Características y ventajas

- La seguridad propia de Kubernetes:
- Aumenta la protección.
- Elimina los puntos ciegos y brinda al personal información acerca de los puntos vulnerables importantes y los vectores de amenaza.
- Reduce el tiempo y los costos.
- Disminuye el tiempo y el esfuerzo necesarios para implementar medidas de seguridad y optimiza el análisis, la investigación y la resolución de problemas de seguridad gracias al contexto abundante que proporciona Kubernetes.
- Aumenta la capacidad de ajuste y la portabilidad.
- Ofrece la capacidad de ajuste y la resistencia propias de Kubernetes, por lo que evita la complejidad y los conflictos en las operaciones que pueden originarse con los controles de seguridad que se realizan fuera de banda.

facebook.com/redhatinc
@RedHatLA
@RedHatIberia
linkedin.com/company/red-hat

Las ventajas en detalle

Sector	Ventajas
Supervisión	▸ Ofrece una visibilidad detallada de las implementaciones, lo que incluye las imágenes, los pods y las configuraciones. ▸ Detecta y revela el tráfico de la red en todos los clústeres, desde los espacios de nombres hasta las implementaciones y los pods. ▸ Identifica los eventos graves en el sistema dentro de cada contenedor.
Gestión de puntos vulnerables	▸ Analiza las imágenes en busca de los puntos vulnerables conocidos en función de los lenguajes, los paquetes y las capas de imagen específicos. ▸ Establece una relación entre los puntos vulnerables y las implementaciones en ejecución, además de las imágenes. ▸ Aplica las políticas en función de la información disponible sobre los puntos vulnerables: en el momento del diseño, mediante integraciones de CI/CD (integración y distribución continuas); en el momento de la implementación, por medio de controles dinámicos de admisión; y durante el tiempo de ejecución, con los controles propios de Kubernetes.
Cumplimiento normativo	▸ Evalúa el cumplimiento normativo de cientos de controles relativos a los indicadores CIS, la Industria de Tarjetas de Pago (PCI), la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA) y la publicación especial 800-190 del NIST. ▸ Ofrece paneles que permiten obtener información a simple vista acerca del cumplimiento normativo de los controles de cada estándar y brinda la posibilidad de exportar la evidencia para satisfacer las necesidades de los auditores. ▸ Otorga una visualización detallada de la información sobre el cumplimiento normativo para identificar los clústeres, los nodos y los espacios de nombres que no cumplen con los estándares y controles específicos.
Segmentación de las redes	▸ Permite visualizar el tráfico en curso entre los espacios de nombres, las implementaciones y los pods y determinar cuánto de este está permitido. En el análisis se incluyen las exposiciones al exterior. ▸ Simula los cambios en la política de red antes de que se implementen, de modo que pueda minimizar el riesgo operativo en el entorno. ▸ Evalúa la actividad de la red según estándares y recomienda políticas nuevas de la red de Kubernetes para eliminar las conexiones que ya no sean necesarias. ▸ Utiliza las funciones de implementación de red integradas en Kubernetes para garantizar la uniformidad, la portabilidad y la capacidad de ajuste de la segmentación.
Creación de perfiles de riesgo	▸ Clasifica las implementaciones en ejecución según su riesgo de seguridad. Además, aprovecha los datos de Kubernetes, la información de configuración o implementación y la actividad del tiempo de ejecución para establecer la prioridad con la que deben atenderse los puntos vulnerables. ▸ Realiza un seguimiento de las mejoras en la estrategia de seguridad que aplica en las implementaciones de Kubernetes para determinar el efecto de las acciones de su equipo de seguridad.

Sector	Ventajas
Gestión de la configuración	▸ Ofrece políticas de DevOps y de seguridad diseñadas previamente que permiten identificar infracciones en la configuración relacionadas a las exposiciones de la red, los contenedores con privilegios, los procesos que se ejecutan como superusuarios y el cumplimiento normativo de los estándares del sector. ▸ Analiza la configuración del control de acceso basado en funciones (RBAC) de Kubernetes para verificar que los privilegios de las cuentas de los usuarios o los servicios sean los adecuados y que no existan configuraciones erróneas. ▸ Realiza un seguimiento de los secretos y detecta las implementaciones que los utilizan para limitar su acceso. ▸ Aplica las políticas de la configuración: en la etapa de diseño, mediante la integración CI/CD y en la de implementación, por medio del control dinámico de admisión.
Detección y respuesta durante el tiempo de ejecución	▸ Supervisa los eventos en el sistema dentro de los contenedores para detectar actividades anómalas que indiquen la presencia de amenazas y brinda respuestas automatizadas por medio de controles propios de Kubernetes. ▸ Evalúa la actividad de los procesos en los contenedores según estándares y elabora listas blancas con ellos de manera automática, para que no deba hacerlo manualmente. ▸ Utiliza políticas diseñadas previamente para detectar la presencia de criptominería, el aumento inapropiado de privilegios, entre otros ataques. ▸ Permite la recopilación flexible de datos del sistema mediante Extended Berkeley Packet Filter (eBPF) o un módulo del kernel en todas las distribuciones principales de Linux.
Integraciones	▸ Brinda una interfaz de programación de aplicaciones (API) amplia y complementos diseñados previamente que pueden integrarse con sistemas de DevOps, como las herramientas de CI/CD, de notificaciones y de análisis de imágenes; los registros; el tiempo de ejecución de los contenedores, y las soluciones de gestión de la información y los eventos de seguridad (SIEM).

Acerca de Red Hat

Red Hat es el proveedor líder mundial de soluciones de software open source para las empresas, que ha adoptado un enfoque impulsado por la comunidad para ofrecer tecnologías confiables y de alto rendimiento de Linux, nube híbrida, contenedores y Kubernetes. Red Hat ayuda a los clientes a integrar las aplicaciones de TI nuevas y actuales; desarrollar aplicaciones nativas de la nube; estandarizar nuestro sistema operativo líder del sector; y automatizar, proteger y gestionar entornos complejos. Sus servicios galardonados de soporte, capacitación y consultoría convierten a Red Hat en asesor de confianza para las empresas de la lista Fortune 500. Como partner estratégico de proveedores de nube, integradores de sistemas, proveedores de aplicaciones, clientes y comunidades open source, Red Hat ayuda a las empresas a prepararse para el futuro del mundo digital.

Argentina
+54 11 4329 7300

Chile
+562 2597 7000

Colombia
+571 508 8631
+52 55 8851 6400

México
+52 55 8851 6400

España
+34 914 148 800

facebook.com/redhatinc
@RedHatLA
@RedHatIberia
linkedin.com/company/red-hat

es.redhat.com
#F27185_0221