

Pon las aplicaciones en contenedores Elimina las amenazas

Octubre de 2024

Kaspersky Container Security

Parte de

kaspersky preparados para el futuro



**Kaspersky
Cloud Workload
Security**



Contenedorización

La contenedorización es una de las principales tendencias del desarrollo de software global. Esta tecnología permite acelerar el diseño de aplicaciones y el proceso de entrega. Sin embargo, las soluciones de seguridad tradicionales no son adecuadas para las funciones de arquitectura de los entornos contenedorizados.

Proteger los entornos contenedorizados y aumentar la seguridad de la infraestructura híbrida de tu organización

Kaspersky Container Security es una solución que protege cada etapa del ciclo de vida de una aplicación contenerizada, desde el desarrollo hasta el funcionamiento. Protege los procesos comerciales de la organización, de acuerdo con los estándares y las regulaciones de seguridad, y admite la implementación de un enfoque DevSecOps.

Kaspersky Container Security ofrece una protección integral frente a las últimas ciberamenazas y automatiza tus auditorías de cumplimiento, liberando los recursos del equipo de seguridad de la información para ocuparse de otras tareas y reduciendo el plazo de lanzamiento.

Kaspersky Container Security se ha desarrollado de manera específica para los entornos contenedorizados locales y en la nube, a fin de garantizar la protección en los diferentes niveles, desde la imagen del contenedor hasta el sistema operativo host.

Kaspersky Container Security forma parte de la solución de Kaspersky Cloud Workload Security. Proporciona una protección integral frente a los ataques y proporciona mayor rapidez en la detección y respuesta ante las amenazas en entornos en la nube.

85 %

de las empresas sufrieron >1 incidente en Kubernetes dentro de los últimos 12 meses*

39 %

de las empresas observaron una filtración de datos confidenciales debido a problemas de seguridad de contenedores*

38 %

de las empresas perdió ingresos en los últimos 12 meses debido a problemas de seguridad del contenedor*

Características principales



Integración en el proceso de desarrollo

- Integración con registros de imágenes y plataformas CI/CD
- Integración con sistemas de notificaciones y seguridad



Auditoría de cumplimiento regulatorio

- Análisis de vulnerabilidades sobre la base de datos NIST
- Auditorías de buenas prácticas



Protección para el orquestador

- Garantiza la seguridad del contenedor en el tiempo de ejecución
- Integración con plataformas de orquestación
- Supervisión de procesos y eventos en el clúster

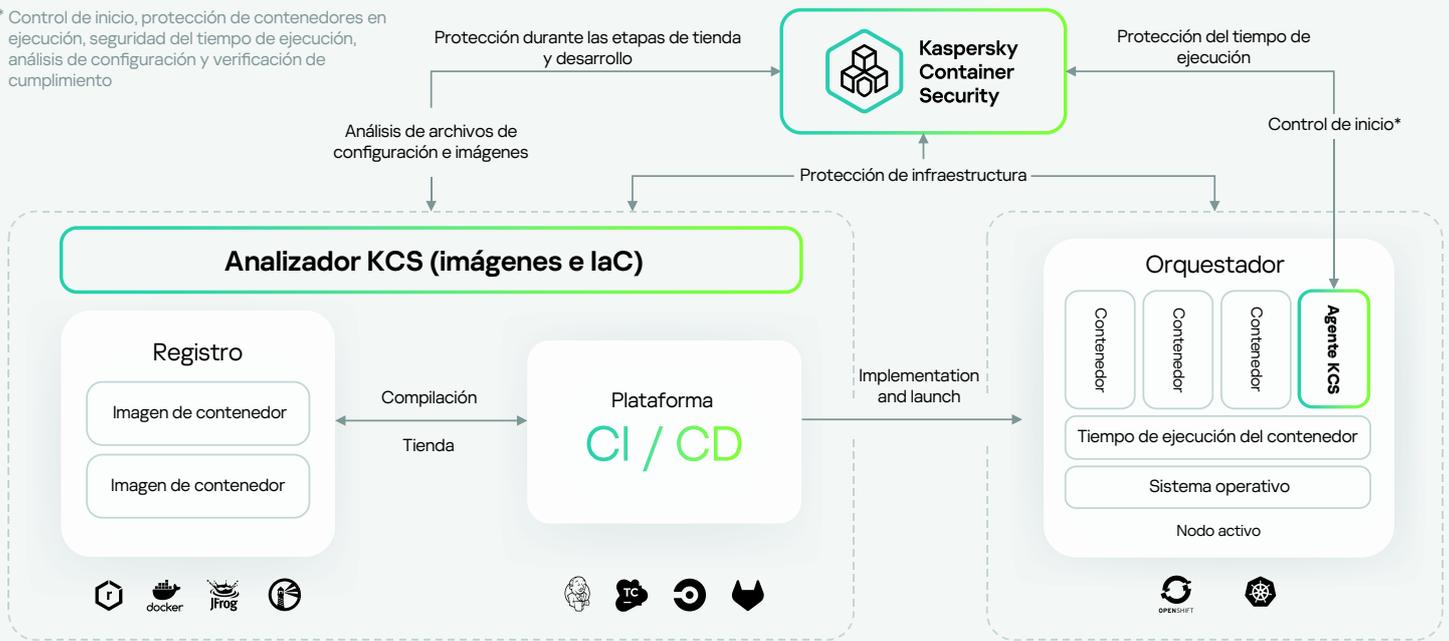


Visualización e inventario de recursos del clúster

- Widgets completamente personalizados para revelar datos transversales
- Inventario transparente de recursos

Arquitectura Kaspersky Container Security

* Control de inicio, protección de contenedores en ejecución, seguridad del tiempo de ejecución, análisis de configuración y verificación de cumplimiento



Kaspersky Container Security (KCS) permite la protección de cada etapa del diseño y la operación de la aplicación. Tiene tres componentes: **Agente KCS, Analizador KCS y Servidor de control KCS.**

Agente KCS

Detecta vulnerabilidades en los niveles del contenedor, el clúster y el orquestador, garantizando la seguridad en el tiempo de ejecución. Se instala en el clúster como un contenedor individual en cada nodo.

Analizador KCS de imágenes e infraestructura

Verifica el registro de imágenes según relevancia y seguridad. El analizador también verifica imágenes como parte del proceso de CI y, de esta forma, reduce los riesgos en la etapa de desarrollo. Se instala en el clúster con los componentes del servidor del orquestador.

Servidor de control KCS

Responsable por la supervisión del estado de los componentes de la solución y la interacción entre ellos, así como por la recopilación de información acerca de los eventos detectados. Se instala en el clúster con los componentes del servidor del orquestador.

Integración en el proceso de desarrollo

Registro y sistema de control de versiones

sobre ataques dirigidos

- Analiza IaC y Dockerfile en busca de secretos y errores en la configuración
- Verifica las imágenes del registro

Herramientas de CI

Diseño y evaluación

- Analiza imágenes en busca de vulnerabilidades, malware y secretos

Orquestador

Ejecución

- Control y supervisión de inicio de contenedores, de acuerdo con las políticas de seguridad
- Análisis de comportamiento de contenedores

Herramientas de CD

Entrega e implementación

- Control de entrega de imágenes y auditoría de cumplimiento de las políticas de seguridad

Ventajas para empresas



Seguridad reconocida en todo el mundo

Las funciones y capacidades de Kaspersky Container Security están alineadas con las mejores prácticas globales para la seguridad de los contenedores.

Protección galardonada y reconocida a nivel internacional.



Cumplimiento de las normativas

Auditorías de buenas prácticas.

Sistema transparente de generación de informes.



Operación sencilla; protección fiable

Visualización de amenazas en tiempo real.

Reduce la necesidad de involucrar al equipo de seguridad de la información, mientras se mejora la calidad y la velocidad de las verificaciones de seguridad.



Protección integral para entornos contenedorizados

Protección en diferentes niveles de la arquitectura del entorno contenedorizado.

Seguridad de aplicaciones para cada etapa del ciclo de vida.

Niveles y objetos de licencia



Kaspersky Container Security

Estándar

Brinda protección para imágenes del contenedor, integración con registros de imágenes, orquestadores, plataformas CI/CD y soluciones SIEM.



Kaspersky Container Security

Protección

Garantiza la protección de los contenedores en el entorno de ejecución, proporciona mayores capacidades de supervisión y herramientas para verificaciones de cumplimiento.

1 licencia



1 nodo con contenedores*

* Se tiene en cuenta la cantidad de nodos en los que se despliega el agente KSC

Parte de Kaspersky Cloud Workload Security

Kaspersky Container Security, en combinación con Kaspersky Hybrid Cloud Security, forma una solución integral de seguridad de cargas de trabajo en la nube para ofrecer una protección fiable y de primera clase frente a los ataques, junto con tiempos de detección de amenazas y de respuesta más cortos en entornos de nube. La solución de Kaspersky Cloud Workload Security garantiza una protección integral de tus infraestructuras híbridas y en la nube: máquinas virtuales/clústeres de contenedores.



Soluciones compatibles



Kaspersky Hybrid Cloud Security



Kaspersky Container Security

Nubes públicas



Orquestadores



Nubes privadas



Registros de imágenes



Plataformas de VDI



Plataformas CI/CD





Kaspersky Container Security

Más información

www.kaspersky.es

© 2024 AO Kaspersky Lab.
Las marcas registradas y logos son propiedad
de sus respectivos dueños.

#kaspersky
#bringonthefuture