CROWDSTRIKE

FALCON CLOUD WORKLOAD PROTECTION

Prevención de brechas para contenedores y cargas de trabajo en la nube

PROTECCIÓN DE CARGAS DE TRABAJO EN LA NUBE QUE TRANSFORMA EL MODO DE TRABAJO DE DEVOPS

La necesidad de velocidad y agilidad en las empresas digitales actuales exige cambios en la infraestructura de TI, concretamente una migración a arquitecturas nativas de la nube y la adopción de DevOps (del inglés, desarrollo-operaciones). Este cambio ha llevado a muchas empresas a adoptar el uso de contenedores, microservicios y Kubernetes (K8s) para mejorar la eficiencia y la escalabilidad de los procesos de desarrollo y sentar la base de una infraestructura inmutable de nueva generación.

Además, la integración continua/entrega continua (IC/EC) introduce la automatización y la supervisión permanentes a lo largo del ciclo de vida de las aplicaciones, desde la integración y las pruebas hasta la entrega y el despliegue, lo que redunda en una aceleración de la innovación. Este cambio hacia el modelo de IC/EC no está exento de riesgos, y los equipos de infraestructura, DevOps y seguridad buscan formas de garantizar que los contenedores y microservicios sean seguros y cumplan las normativas, además de eliminar los ángulos muertos de seguridad.

Los contenedores introducen un nuevo entorno y una estructura de administración diferente con Kubernetes, y para los equipos de seguridad es difícil adaptarse al cambio. El resultado es un aumento del riesgo debido a la falta de visibilidad; enfoques fragmentados para detectar y prevenir las amenazas; errores de configuración para las cargas de trabajo y contenedores en la nube y sin servidor; y la incapacidad de garantizar el continuo cumplimiento de las normativas.

Estas son algunas de las dificultades habituales para proteger los contenedores:

- Falta de visibilidad de las cargas de trabajo y contenedores en la nube, y de los entornos Kubernetes
- Una gestión de las vulnerabilidades ineficaz para registros, bibliotecas, hosts e imágenes de contenedores
- Protección de la orquestación de contenedores
- Protección en tiempo real de los contenedores y cargas de trabajo nativas de la nube
- Falta de expertos en seguridad de la nube y una superficie de ataque que va en aumento
- El cumplimiento de las normativas de forma permanente y la implementación de políticas de seguridad

Los procesos manuales y las soluciones tradicionales no están a la altura de los rápidos cambios y los retos especiales a los que se enfrentan ahora las empresas con los contenedores. Las alternativas son complejas plataformas de seguridad de la nube y herramientas aisladas, lo que añade más proveedores y aumenta la complejidad de la seguridad global de la empresa.

VENTAJAS PRINCIPALES

Analiza e identifica continuamente vulnerabilidades, amenazas, secretos incrustados y el incumplimiento de normativas.

Ofrece una visibilidad inigualable con eventos detallados de cargas de trabajo en la nube, contenedores y metadatos.

Identifica las cargas de trabajo en la nube que se ejecutan en su entorno, incluidas las que tienen configuraciones con un riesgo potencial.

Proporciona una protección en tiempo de ejecución continua para todas las cargas de trabajo y contenedores en la nube.

Facilita y acelera la caza de amenazas y la investigación para cualquier carga de trabajo.

Protege inmediatamente, sin sacrificar el rendimiento y al ritmo de DevOps.

Se adapta a la escalabilidad dinámica de las cargas de trabajo y contenedores de la nube en tiempo real.

EL ENFOQUE DE CROWDSTRIKE DE LA PROTECCIÓN DE CONTENEDORES Y CARGAS DE TRABAJO EN LA NUBE

CrowdStrike protege su infraestructura de nube centrándose en adelantarse a los adversarios, reducir de forma implacable su superficie de ataque y obtener una visibilidad total de los eventos que tienen lugar en el entorno. Para detener las brechas en contenedores y cargas de trabajo en la nube, y en entornos Kubernetes mediante datos y análisis a escala de la nube, se requiere una plataforma muy integrada. Cada función desempeña un papel crucial en la identificación anticipada de las vulnerabilidades, la detección de amenazas, la protección en tiempo de ejecución y el cumplimiento de normativas, y todas deben estar diseñadas y creadas para priorizar la velocidad, la escalabilidad y la fiabilidad.

La experiencia de CrowdStrike con una de las nubes de seguridad más grandes del mundo ofrece una visión inigualable de los atacantes y nos permite proporcionar soluciones específicas de CrowdStrike® que crean menos trabajo para los equipos de DevSecOps, protegen frente a las fugas de datos y optimizan los despliegues en la nube.

CARACTERÍSTICAS PRINCIPALES

ANÁLISIS Y GESTIÓN DE VULNERABILIDADES

Consiga una visibilidad total de las cargas de trabajo, contenedores y hosts, ya sean locales o estén en la nube.

- **Mejora de la toma de decisiones:** consiga información y detalles sobre sus cargas de trabajo y contenedores en la nube: imágenes, registros, bibliotecas y datos a partir de esas imágenes.
- **Descubrimiento de amenazas ocultas:** detecte en sus imágenes el malware oculto, los secretos incrustados, problemas de configuración y otros riesgos para reducir así la superficie de ataque.
- **Visibilidad de los entornos de contenedores:** consiga visibilidad total de los contenedores en ejecución para descubrir los detalles de acceso de archivos, comunicaciones de red y actividad de procesos.
- **Identificación de vulnerabilidades más rápida:** ahorre un valioso tiempo con directivas de análisis de imágenes prediseñadas que le permiten detectar las vulnerabilidades y los fallos de configuración, entre otros, rápidamente.
- **Identificación de configuraciones de contenedores de riesgo:** identifique rápidamente los contenedores mal configurados o que presentan riesgos, como los de puntos de montaje no habituales o los enlaces que sugieren la posibilidad de un compromiso.
- **Eliminación de las amenazas antes de producción:** bloquee las vulnerabilidades que se pueden aprovechar, según los indicadores de ataque, antes de la ejecución, eliminando molestias para el equipo de seguridad.
- **Supervisión continua:** identifique nuevas vulnerabilidades en tiempo de ejecución, alerte y tome medidas sin necesidad de volver a analizar las imágenes.

SEGURIDAD DE CANALIZACIONES DE IC/EC

Integre la seguridad como parte de la canalización de IC/EC.

- **Acelere la entrega:** cree directivas de imágenes verificadas para asegurarse de que solo las imágenes aprobadas puedan avanzar por la canalización y ejecutarse en sus hosts o en clústeres Kubernet.

PROTECCIÓN DE CARGAS DE TRABAJO EN LA NUBE OPTIMIZADA PARA DEVOPS

Ofrece una plataforma para todas las cargas de trabajo y contenedores

Protege las cargas de trabajo y contenedores en la nube dondequiera que se ejecuten

Se integra directamente en la canalización de IC/EC para el análisis de imágenes y registros

Operativa desde el primer día: se despliega y se puede utilizar en cuestión de minutos, sin necesidad de reiniciar ni realizar ajustes o complicadas configuraciones

Prioriza los incidentes de forma inteligente según la gravedad y la importancia

Simplifica el proceso de filtrado y automatiza la respuesta

- **Identificación anticipada de las amenazas:** analice las imágenes de contenedores continuamente para identificar vulnerabilidades conocidas, problemas de configuración, secretos/claves y problemas de licencias de OSS.
- **Evaluación del estado de vulnerabilidad de su canalización:** descubra el malware que sus analizadores estáticos no han detectado antes de desplegar los contenedores.
- **Mejora de las operaciones de seguridad:** simplifique la visibilidad de las operaciones de seguridad proporcionando información y contexto para evitar errores de configuración e infracciones de normativas.
- **Integración con cadenas de herramientas de desarrolladores:** integración con Jenkins, Bamboo, GitLab y otras, para agilizar la corrección y la respuesta en los grupos de herramientas de DevOps que ya utiliza.
- **DevSecOps:** los informes y paneles facilitan la coherencia y la posibilidad de compartir conocimiento entre los equipos de operaciones de seguridad, DevOps e infraestructura.

PROTECCIÓN EN TIEMPO DE EJECUCIÓN

Proteja las cargas de trabajo y los contenedores en la nube dondequiera que residan.

- **Protección de hosts y contenedores:** la protección de CrowdStrike Falcon® en tiempo de ejecución defiende los contenedores frente a ataques activos.
- **Mayor compatibilidad de contenedores:** Falcon admite contenedores en Linux y se puede desplegar en entornos Kubernetes, como EKS. Además, admite contenedores como servicio (CaaS), como Fargate, que proporcionan el mismo nivel de protección. Hay versiones Technology Preview para AKS, GKE y Red Hat OpenShift.
- **Utilice tecnologías de protección líderes del mercado:** el aprendizaje automático, la inteligencia artificial (IA), los indicadores de ataque y el bloqueo de hash personalizado defienden automáticamente frente al malware y otras amenazas sofisticadas dirigidas contra los contenedores:
  - **Aprendizaje automático e IA:** Falcon emplea aprendizaje automático e IA para detectar malware conocido y desconocido en contenedores, sin necesidad de análisis ni firmas.
  - **Indicadores de ataque:** Falcon usa indicadores de ataque para identificar amenazas basadas en el comportamiento. Conocer las secuencias de comportamiento permite a Falcon detener los ataques que no se limitan al malware, como los que no utilizan archivos.
- **Detención del comportamiento malicioso:** la identificación de comportamientos permite bloquear actividades que infringen las directivas, sin afectar al funcionamiento legítimo de los contenedores.
- **Investigación más rápida de incidentes de contenedores:** los incidentes se pueden investigar fácilmente cuando se asocian las detecciones con el contenedor concreto, en lugar de agruparlas sin orden con los eventos de host.
- **Todo a la vista:** capte la información de inicio, fin, imagen y tiempo de ejecución de los contenedores, así como todos los eventos generados en su interior, aunque el contenedor solo se ejecute durante unos segundos.
- **Despliegue optimizado con Kubernetes:** realice el despliegue fácilmente y a escala incluyendo Falcon en un clúster de Kubernetes.
- **Mejora de la orquestación de contenedores:** vea los espacios de nombres, metadatos de pod, procesos, archivos y eventos de redes de Kubernetes.

MOTOR DE PREVENCIÓN DE BRECHAS DE THREAT GRAPH

Prevea y evite las amenazas modernas en tiempo real mediante la combinación más completa de la industria de telemetría de endpoints, contenedores y cargas de trabajo en la nube; inteligencia sobre amenazas y análisis basados en inteligencia artificial.

- **Inteligencia sobre amenazas líder del mercado integrada:** Falcon emplea inteligencia sobre amenazas enriquecida, para proporcionar una representación visual de las relaciones entre roles de cuentas, cargas de trabajo y API para conseguir un contexto más detallado que permita ofrecer una respuesta más rápida y más eficaz.
- **Prevención de amenazas automatizada:** el análisis profundo basado en inteligencia artificial y comportamientos identifica en tiempo real las amenazas nuevas y no habituales, y toma las medidas adecuadas, ahorrando un tiempo muy valioso a los equipos de seguridad.
- **Aceleración de la respuesta:** CrowdStrike Threat Graph® pone este conocimiento a disposición del responsable de la respuesta en tiempo real, lo que le permite conocer las amenazas inmediatamente y actuar con decisión.

- **Reducción de la fatiga de alertas:** la estrategia de identificación y gestión de amenazas selectivas destaca lo relevante entre la saturación de avisos de seguridad de los entornos multinube y reduce la fatiga de alertas.
- **Descubrimiento de ataques y mejora de la respuesta:** CrowdScore™ Incident Workbench de CrowdStrike ayuda a desentrañar los ataques y mejorar el tiempo de respuesta, desgranando y correlacionando las alertas de seguridad con los incidentes, filtrándolas automáticamente, y priorizando y destacando las que requieren una atención urgente.

UNA SOLA FUENTE DE VERDAD CON POTENTES API

El hecho de contar con una sola fuente de datos ofrece a los equipos de seguridad un acceso rápido a todo lo que necesitan para responder e investigar.

- **Ventajas de la automatización lista para DevOps:** las potentes API permiten la automatización de la funcionalidad de CrowdStrike Falcon, que incluye detección, administración, respuesta e inteligencia.
- **Optimización del rendimiento empresarial:** aproveche la orquestación y automatización de la seguridad, así como otros flujos de trabajo avanzados para optimizar el rendimiento de su empresa.
- **Integración con canalizaciones de IC/EC:** integraciones con Chef, Puppet y AWS Terraform para facilitar los flujos de trabajo de IC/EC.
- **Protección al ritmo de DevOps:** Falcon protege inmediatamente e iguala la velocidad de DevOps, adaptándose a la escalabilidad dinámica de los contenedores en tiempo real con integración de IC/EC a través de API y scripts prearranque.

SIMPLICIDAD Y RENDIMIENTO

Use una plataforma para todas las cargas de trabajo y contenedores. Funciona en todos los entornos: privados, públicos y de nube híbrida.

- **Simplificación de la adopción de DevSecOps:** reduzca los gastos, conflictos y complejidad asociados a la protección de entornos con cargas de trabajo y contenedores en la nube y sin servidor.
- **Un solo panel:** una única consola proporciona visibilidad centralizada del estado de seguridad de la nube, las cargas de trabajo y los contenedores, independientemente de su ubicación.
- **Flexibilidad total de las directivas:** las directivas se pueden aplicar a cada carga de trabajo, contenedor, grupo o a un nivel superior, y pueden unificarse entre despliegues locales y multinube.
- **Capacidad de escalar a voluntad:** sin necesidad de rediseñar ni añadir infraestructura adicional.
- **Amplia compatibilidad con plataformas:** la plataforma Falcon admite contenedores basados en Open Container Initiative (OCI), como Docker y Kubernetes, y también plataformas de orquestación alojadas y autogestionadas, como GKE (Google Kubernetes Engine), EKS (Amazon Elastic Kubernetes Service), ECS (Amazon Elastic Container Service), AKS (Azure Kubernetes Service) y OpenShift.

ACERCA DE CROWDSTRIKE

CrowdStrike, líder mundial en ciberseguridad, redefine la seguridad en la era de la nube mediante una plataforma de protección de endpoints que ha sido construida desde la base con el objetivo de detener las brechas de la seguridad. La arquitectura de un solo agente ligero de CrowdStrike Falcon® aprovecha la inteligencia artificial a escala de la nube y ofrece protección en tiempo real y visibilidad en toda la empresa, evitando los ataques a los endpoints, estén o no conectados a la red. Gracias a CrowdStrike Threat Graph®, CrowdStrike Falcon correlaciona a la semana, en tiempo real, más de 4 billones de eventos relativos a los endpoints en todo el planeta, alimentando una de las plataformas de datos para seguridad más avanzadas del mundo.

Empezar la prueba gratuita
del antivirus de nueva generación

Más información en **www.crowdstrike.com/es**