CROWDSTRIKE

Plan para proteger las cargas de trabajo de AWS

La total visibilidad y protección de las cargas de trabajo y los contenedores que ofrece CrowdStrike Falcon Cloud Security, junto con la vista global de las alertas de AWS Security Hub, son las herramientas esenciales para crear arquitecturas seguras en la nube.

aws PARTNER

- Sector público
- Apto para Amazon Linux
- Vendedor de Marketplace
- Competencia en software de seguridad

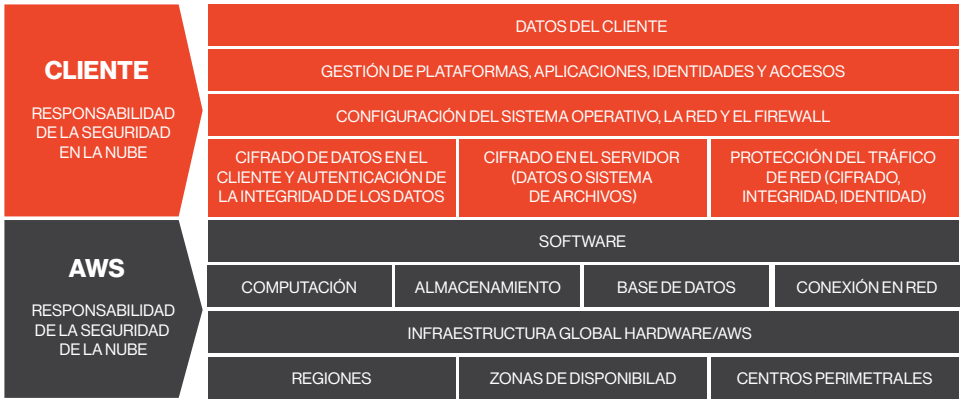
eBook de CrowdStrike

Índice

Los planes obsoletos dejan a las arquitecturas de nube expuestas frente a los ataques

A pesar de que la adopción de la nube se ha disparado, muchas posturas de seguridad siguen ancladas en el pasado. Se ha demostrado que ampliar las herramientas de seguridad locales tradicionales para que funcionen en la nube es inadecuado. Esta forma de proceder deja a los arquitectos de la nube y a los equipos de DevOps sin un plan claro para proteger las aplicaciones, las cargas de trabajo y la infraestructura.

Sienta unas bases de seguridad sólidas con Amazon Web Services (AWS) y CrowdStrike, líder en protección de endpoints y cargas de trabajo en la nube. La combinación de CrowdStrike Falcon y AWS Security Hub te permite gestionar de forma centralizada y automatizada las alertas de amenazas de los servicios de AWS, incluido Amazon GuardDuty. Con CrowdStrike Falcon Cloud Security, puedes reforzar la seguridad de tus cargas de trabajo de AWS y adoptar el modelo de responsabilidad compartida.



CrowdStrike Falcon Cloud Security protege tus cargas de trabajo que se ejecutan en AWS

AWS protege tu infraestructura en la nube

AWS Security Hub ofrece una vista completa de las alertas de seguridad y el cumplimiento normativo

- Agrega datos de alertas de Falcon y servicios AWS nativos como Amazon GuardDuty
- Monitoriza el estado de tu infraestructura AWS con información en pantalla
- Verifica si se cumplen las normativas

CrowdStrike Falcon Cloud Security protege tus cargas de trabajo de AWS con un único agente ligero

- Disfruta de seguridad avanzada para las aplicaciones nativas de la nube, que incluye prevención de brechas, protección de cargas de trabajo y gestión de la postura de seguridad en la nube.
- Simplifica tu modelo de capas de seguridad con un agente único que ocupa poco espacio en los recursos de AWS, lo cual mejora el rendimiento.
- Reduce la arquitectura necesaria para tener total visibilidad de la seguridad y reduce la complejidad para conseguir un mayor rendimiento de tus inversiones en AWS.

Falcon y AWS dotan a tus flujos de trabajo de una protección total

La integración de CrowdStrike con AWS Security Hub te brinda una vista completa y en tiempo real de las alertas de seguridad de mayor prioridad. El enfoque de CrowdStrike centrado en las API combina Falcon Cloud Security y AWS Security Hub, lo que facilita a todo tu equipo — incluidos DevOps, CISO, operaciones y los arquitectos de la nube— la automatización de las tareas de seguridad y aumenta la protección general.

TOTAL VISIBILIDAD

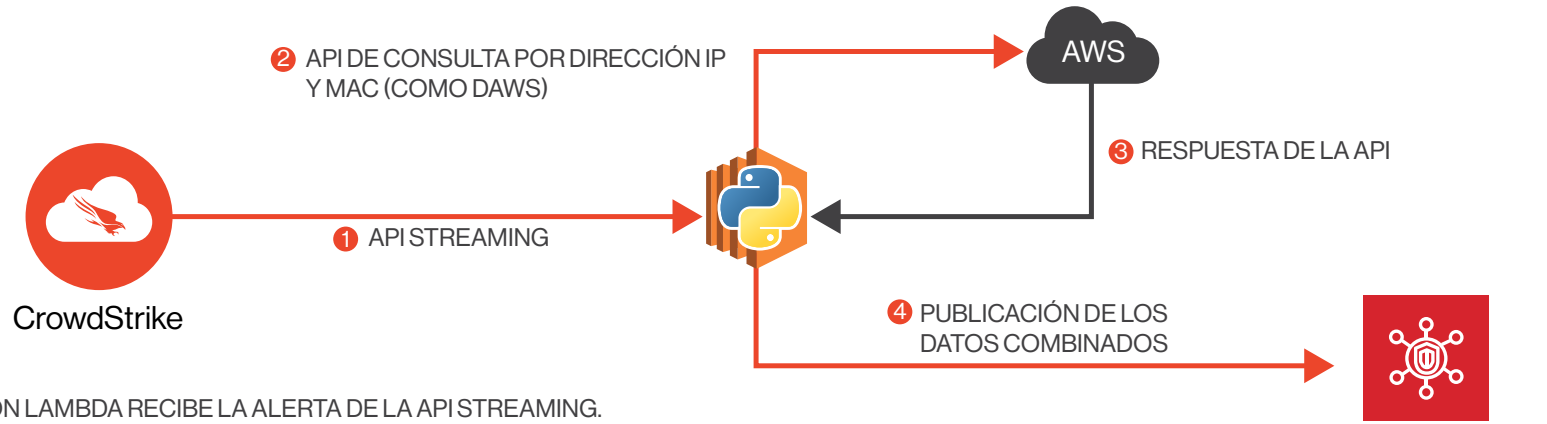
Falcon Cloud Security protege tus cargas de trabajo de AWS a lo largo de todo el ciclo de vida de las amenazas con una combinación de Machine Learning, inteligencia artificial, análisis del comportamiento y Threat Hunting proactivo en una única solución.

MEJOR RENDIMIENTO

Falcon Cloud Security funciona en todos los entornos (instancias de Amazon Elastic Cloud Compute [Amazon EC2], Amazon Elastic Container Service [Amazon ECS] en Amazon EC2 y Amazon Elastic Kubernetes Service [Amazon EKS] en Amazon EC2) y protege los endpoints y las cargas de trabajo aunque estén desconectados.

ARQUITECTURA SIMPLIFICADA

Falcon Cloud Security simplifica las complejas canalizaciones de DevSecOps y aumenta la fiabilidad operativa al emplear arquitecturas en la nube más sencillas. Falcon consolida tus agentes de endpoints y cargas de trabajo con una plataforma ampliable que crece y se adapta a tus necesidades sin añadir complicaciones.



1. LA FUNCIÓN LAMBDA RECIBE LA ALERTA DE LA API STREAMING.
2. LA FUNCIÓN LAMBDA CONSULTA LA API DE AWS PARA OBTENER INFORMACIÓN.
3. SI COINCIDE CON UNA INSTANCIA EC2, SE DEVUELVEN LOS DATOS.
4. LOS DATOS DE EC2 Y CROWDSTRIKE SE COMBINAN, SE LES DA FORMATO Y SE ENVÍAN A AWS SECURITY HUB.

Visibilidad total

Gracias a las alertas de Amazon GuardDuty y Falcon Cloud Security, agregadas mediante AWS Security Hub, tu equipo dispone de una visión de conjunto que ofrece el contexto necesario para tomar decisiones estratégicas en materia de seguridad y recursos. Al automatizar los análisis rutinarios de seguridad, podrás detectar y tratar en menos tiempo los incidentes más acuciantes entre tanto ruido.

Aprovecha la inteligencia de Threat Graph

Identifica posibles amenazas con rapidez y precisión, gracias a la inteligencia de Threat Graph alimentada por IA, con lo que alcanzarás un nivel de protección nunca visto para tus cargas de trabajo de AWS.

Automatiza las tareas de seguridad

Sin Threat Graph, los analistas tendrían que recopilar la telemetría sobre endpoints y cargas de trabajo, añadir fuentes de inteligencia, escribir reglas de correlación y, por último, analizar los datos para determinar las posibles relaciones entre los eventos de seguridad, y todo ello manualmente. Sin embargo, gracias a Falcon Cloud Security, toda la inteligencia, los eventos y sus relaciones se recogen en un único lugar, con lo que los administradores de seguridad pueden automatizar el análisis para disponer de una visibilidad más inteligente y exhaustiva a la hora de investigar posibles brechas.

Integra la seguridad en las canalizaciones de CI/CD

Falcon Cloud Security permite a los equipos de seguridad en la nube adaptarse a las cargas de trabajo de AWS, dinámicas y flexibles por naturaleza. Mediante potentes API y una integración optimizada con AWS Security Hub, implementarás perfectamente los flujos de trabajo de despliegue de CI/CD.

Los equipos de DevOps fomentan la automatización

- Automatiza la entrega de canalizaciones de desarrollo
- Simplifica la implementación y la gestión
- Garantiza la seguridad a la velocidad que se entregan las aplicaciones

Los equipos de seguridad consiguen una visión más exhaustiva

- Añade contexto a tus alertas de seguridad de AWS
- Conoce la gravedad de los incidentes de seguridad
- Simplifica la respuesta a los incidentes
- Identifica la intención de los atacantes según los indicadores de ataque
- Reduce los falsos positivos e incrementa la eficiencia de la seguridad

Más de 7 billones
de eventos a la semana

200K
nuevos IOC publicados cada día

Más de 200
atacantes rastreados

Más de 1,2 millones
de muestras de malware procesadas a diario

Mejor rendimiento

Con CrowdStrike, solo necesitas un sensor para proteger todos tus endpoints y cargas de trabajo, ya sean dispositivos IoT, portátiles o instancias de computación en la nube. Al usar AWS Security Hub como panel de control, puedes agregar y establecer la prioridad de las alertas de seguridad de Falcon Cloud Security y Amazon GuardDuty para proteger las instancias de Amazon EC2 o los contenedores que se ejecutan en Amazon ECS y Amazon EKS.

Mantén el nivel de seguridad y rendimiento de las instancias de Amazon EC2

Falcon Cloud Security utiliza una escala nativa de la nube para proteger las instancias de Amazon EC2 con un impacto mínimo en el rendimiento durante la ejecución, y todo ello sin oleadas de análisis ni actualizaciones de firmas invasivas. La solución protege contra todos los ataques avanzados que eluden las estrategias tradicionales que protegen el perímetro y basadas en firmas.

Protege los contenedores que se ejecutan en Amazon ECS y Amazon EKS

Falcon Cloud Security se ejecuta en el nodo de instancias de Amazon EC2, protegiendo de todo tipo de amenazas —ya sea malware conocido o ataques más sofisticados— todos los contenedores que también se ejecutan en el nodo, incluidos los que gestionan Amazon ECS y Amazon EKS. Para ello, detecta y supervisa las cargas de trabajo, examina parámetros como el identificador único del contenedor y el tipo de configuración, y envía alertas a AWS Security Hub.

Adelanta (shift-left) las comprobaciones de seguridad de los contenedores en las canalizaciones de CI/CD

Si anticipas las tareas de seguridad en el proceso de desarrollo de software, los equipos podrán detectar los fallos antes de que tengan consecuencias graves. Al añadir Falcon Cloud Security a tus flujos de trabajo de implementación de CI/CD, mejorarás la seguridad durante la ejecución de las cargas de trabajo de Amazon ECS y Amazon EKS, y lograrás visibilidad de las aplicaciones que se encuentran en contenedores. Podrás ver y gestionar eventos, como imágenes de contenedores de riesgo, mediante el panel de control de AWS Security Hub.

1
agente ligero

0
reinicios necesarios

Los equipos de DevOps codifican más fácilmente

- Protege contra el malware sin integrar ningún dispositivo tradicional
- Simplifica el código y los scripts con un agente único que se conecta sin problemas

Los equipos de seguridad obtienen más información

- Correlaciona las alertas de AWS con la detección de Falcon Cloud Security para agilizar la clasificación y la remediación de amenazas
- Dota al equipo de operaciones de una plataforma de Threat Hunting

Arquitectura simplificada

Cuando Falcon Cloud Security y AWS Security Hub funcionan en tándem consigues aumentar la eficacia, lo que te ayuda a acortar el tiempo de detección, investigación y remediación para atajar más brechas. Disponer de un servicio integrado de seguridad total supone contar con un equipo más eficiente que dedica menos tiempo a gestionar flujos de trabajo independientes. Optimiza la potencia de AWS Security Hub para agregar eventos aprovechando la inteligencia sobre amenazas y la arquitectura simplificada de CrowdStrike.

Simplifica las arquitecturas de AWS

Otros proveedores de seguridad a menudo requieren un enrutamiento complejo para las aplicaciones tradicionales que debe insertarse en el flujo de paquetes, y multitud de agentes de carga de trabajo para proporcionar sistemas antivirus, EDR y seguridad de contenedores que hay que instalar y gestionar por separado. Todo ello añade complejidad a tus entornos de AWS y prolongar el tiempo de inactividad. Falcon, como agente único, brinda el mismo nivel de seguridad de una manera más económica.

Agiliza los tiempos de respuesta

Priorizar los incidentes en AWS Security Hub ayuda a agilizar la clasificación de amenazas para que tu equipo se ocupe primero de las más peligrosas.

Impulsa la eficiencia para ahorrar aún más

Como Falcon Cloud Security se puede adquirir en AWS Marketplace, puedes aprovechar el valor calculado y la facturación integrada, y al mismo tiempo optimizar el gasto de las cargas de trabajo elásticas.

El equipo de DevOps puede empezar a trabajar más rápidamente

- Incorpora seguridad y remediación con un sensor de endpoints
- Olvídate de la instalación: CrowdStrike se conecta desde una consola SaaS
- Utiliza un único servicio de seguridad para disfrutar de una protección total

Los arquitectos de la nube crean diseños con más eficacia

- Consolida la arquitectura para construir más fácilmente
- Escala a medida que aumentan las cargas de trabajo en la nube sin tener que recurrir a más infraestructuras
- API potentes que automatizan tareas en todas las áreas funcionales para contar con una protección completa

100 000 nodos
al día para su implementación inmediata

75 %
más eficiente

Actúa pensando en la excelencia

La ciberseguridad no es solo un problema de tecnología; para proteger tus cargas de trabajo de AWS también necesitas profesionales y procesos eficaces. Si no se tienen en cuenta las operaciones de seguridad, se pueden ocasionar daños y habrá que realizar tareas de remediación que ralenticen al equipo de DevOps y reduzcan el tiempo de actividad de tus aplicaciones críticas. Sin embargo, puedes evitarlo si configuras correctamente la tecnología de seguridad y la mantienes al día, y si clasificas, investigas y remedias de inmediato las alertas de seguridad que preceden a un incidente.

Son muchas las organizaciones que tienen dificultades para resolver este aspecto operativo de la seguridad porque resulta caro y difícil contratar a los profesionales necesarios para encargarse ininterrumpidamente de la ciberseguridad.

Mejora la eficacia de tu equipo con detección y respuesta gestionadas

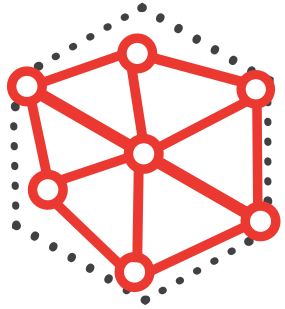
CrowdStrike Falcon Complete es un servicio gestionado de detección y respuesta (MDR) que mejora la eficacia de la plataforma Falcon gracias un equipo especializado de profesionales de la seguridad. Falcon Complete se vuelca en la gestión y monitorización de la seguridad de tus endpoints y tus cargas de trabajo, y responde a las amenazas con rapidez y precisión para que tú no tengas que preocuparte.

Los equipos de DevOps sufren menos interrupciones

- Monitorización constante con remediación quirúrgica que elimina las amenazas rápidamente sin afectar a la carga de trabajo subyacente

Los equipos de seguridad ganan inmediatamente en experiencia y eficacia

- Directivas de seguridad que se ajustan continuamente para lograr la máxima eficacia
- Amenazas identificadas y erradicadas en cuestión de minutos
- Tranquilidad respaldada por una garantía de prevención de brechas de seguridad



El marco 1-10-60 son los tiempos ideales que recomendamos a las empresas que traten de cumplir para ser más rápidas que los atacantes:

<1 minuto
para detectar la amenaza

<10 minutos
para conocer la amenaza

<60 minutos
para eliminar la amenaza

Empieza a usar CrowdStrike en AWS hoy mismo

Para obtener más información sobre las soluciones de CrowdStrike y AWS, visita:

- **CrowdStrike Falcon Cloud Security**
- **CrowdStrike en AWS Marketplace**
- **Conoce mejor tu postura de seguridad con una revisión de riesgos de seguridad en la nube**