CROWDSTRIKE

CrowdStrike Falcon Cloud Security en AWS

aws PARTNER

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

eBook de CrowdStrike

Índice

Introducción

En todo el mundo, organizaciones de todos los tamaños se benefician de la tecnología de la nube, y cada vez más empresas incorporan Amazon Web Services (AWS) a su entorno, ya sea desde la base o posteriormente con un proceso de migración. Movidos por las necesidades empresariales de flexibilidad, innovación y rentabilidad, los CTO y CIO adoptan las tecnologías AWS confiando en que así podrán responder a los cambios de manera rápida y segura, escalar con eficacia e impulsar el crecimiento de su negocio.

A medida que evolucionan las empresas, también deben avanzar las estrategias de seguridad, de manera que siempre vayan un paso por delante de las amenazas. Si quieres estar preparado ante cualquier circunstancia, es fundamental que te anticipes con una estrategia de seguridad en la nube, ya que tanto la tecnología como los ciberataques son cada vez más sofisticados.

Tanto si tu empresa se basa ya en la nube como si está en proceso de adoptarla, debes plantearte una estrategia de seguridad para este entorno. Sea cual sea la fase en la que te encuentres, tu prioridad debe ser siempre proteger tu infraestructura.

En un contexto tecnológico en la nube que cambia continuamente, hay algo de lo que no cabe duda: los ciberdelincuentes conocen los riesgos de seguridad de la nube. ¿Puedes tú decir lo mismo?

52 %

Porcentaje de organizaciones norteamericanas que prevén que, como mínimo, el 41 % de sus cargas de trabajo estarán en la nube en los próximos 24 meses

Protección durante el proceso de migración a la nube

La tecnología de la nube ha permitido a nuevas empresas ponerse en marcha rápidamente y ha ayudado a empresas ya implantadas a crear la base para la innovación. Además, ha dado lugar a un nuevo conjunto de parámetros de seguridad y ha generado nuevas amenazas. Sin embargo, la innovación también conlleva riesgos, como el despliegue y la implementación de directivas de manera descentralizada, las lagunas de visibilidad entre distintas tecnologías y endpoints, y el factor humano, que cada vez entraña un mayor peligro; en otras palabras, los riesgos asociados al shadow IT, una arquitectura mal diseñada y la falta de conocimientos y expertos.

Para las empresas que utilizan la tecnología de la nube para crear su infraestructura y escalarla después según sus necesidades, la seguridad implica proteger un entorno que cambia continuamente. Las aplicaciones y soluciones externalizadas, desarrolladas por terceros con distintos estándares de seguridad y arquitecturas diferentes, pueden generar vacíos de seguridad. Por lo tanto, implementar pronto una estrategia de seguridad es la mejor forma de mantener una visibilidad centralizada de los distintos componentes y servicios en la nube.

Las empresas que migren a la nube a partir de una tecnología tradicional encontrarán riesgos tanto en los sistemas nuevos como en los que ya tenían. Las soluciones híbridas durante una migración son especialmente vulnerables, al igual que los sistemas y bases de datos antiguos que se dan de bajan, si no se desechan convenientemente. La mayoría de las migraciones también obligan a formar de nuevo al personal o a contratar nuevos empleados, además de promover un cambio de cultura en la empresa. Aunque esto crea una buena base para la gestión de futuros cambios tecnológicos, también genera confusión. Por eso, es fundamental mantener una visión integral de la seguridad mientras tiene lugar esta importante transición tecnológica.

El enfoque estratégico de la seguridad de CrowdStrike

Una forma de proteger tus sistemas en la nube es elegir a un partner como CrowdStrike. Con Falcon Cloud Security y la ayuda de un equipo de expertos en ciberseguridad, recibirás protección global; desde el host hasta la nube, además de en los componentes intermedios, las cargas de trabajo y los contenedores en AWS.

La estrategia de CrowdStrike:

- Centrarse en el adversario
- Reducir el nivel de exposición
- Supervisar la superficie de ataque
- Proteger en el momento de la ejecución
- Formar parte de la canalización de CI/CD

Los ciberdelincuentes han adaptado a la nube los ataques habituales en otras tecnologías, como la escalada de permisos, el ransomware y la captura de datos y paquetes (sniffing). Además, probablemente surjan nuevas técnicas de ataque específicas para la nube. Las soluciones de CrowdStrike de seguridad de la nube incluyen alertas y denuncias en tiempo real de más de 200 ciberdelincuentes, de manera que, cuando aparezcan estas nuevas amenazas, estarás preparado para responder.

En lo que respecta a la seguridad de la nube, para reducir el nivel de exposición y limitar la superficie de ataque es preciso segmentar las cargas de trabajo, no dejar cabos sueltos (especialmente los sistemas antiguos que se abandonan) y priorizar la seguridad al utilizar la nube, lo que también se conoce como "shift left" o desplazamiento a la izquierda. Una vez definida la superficie de ataque, contar con un sistema de vigilancia que ofrezca una gran visibilidad es la mejor forma de defenderse contra posibles atacantes. Falcon Cloud Security incluye análisis automatizado, protección durante la ejecución y en reposo, indicadores de ataque (IOA) nativos de la nube, y Machine Learning para realizar las investigaciones más rápidamente.

Falcon Cloud Security para DevSecOps y la supervisión

En el caso de las empresas con una infraestructura en varios entornos, Falcon Cloud Security simplifica la gestión de la seguridad mediante una única fuente de información para todos los recursos en la nube y configuraciones de seguridad. Todo lo que necesitas ver, en un solo lugar. Con protección de IOA y remediación guiada basada en ML, directamente en el plano de control, Falcon Cloud Security ayuda a los equipos a gestionar el cumplimiento de normativas y a desplegar las integraciones de AWS con seguridad y con una mayor eficacia.

Falcon Cloud Security para una prevención integral de las brechas de seguridad

Si vas a crear o sustituir sistemas con tecnología en la nube, Falcon Cloud Security proporciona protección total contra las brechas de seguridad en los entornos de nube privada, pública, híbrida y multinube, lo que permite a los clientes adoptar y proteger rápidamente la tecnología con independencia del tipo de carga de trabajo. Con Falcon Cloud Security puedes crear, ejecutar y proteger aplicaciones rápidamente y de forma segura.

Protección de los contenedores en AWS

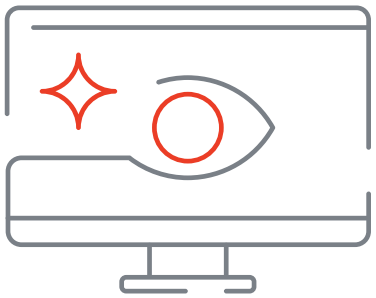
Asegurarte de que tus contenedores estén protegidos es otro componente clave de toda estrategia eficaz de seguridad de la nube. Los contenedores, que por definición están aislados y son independientes, limitan la visibilidad. Con frecuencia se crean y ya no se les presta más atención, por lo que no se piensa en los requisitos de seguridad a largo plazo. Pero incluso cuando se aplican las mejores prácticas de supervisión, los contenedores pueden provocar problemas en los análisis de seguridad, debido a la enorme cantidad de datos que generan cuando se examinan las vulnerabilidades.

Falcon Cloud Security ataja estos problemas de raíz. El agente ligero de CrowdStrike proporciona una visibilidad total de los contenedores, tanto en despliegues locales como en la nube. La continua supervisión y la integración con canalizaciones de IC/EC facilitan la comprobación de los contenedores, así como su restablecimiento en caso necesario. Además, las funciones automatizadas de supervisión y detección continua de amenazas de Falcon Cloud Security proporcionan análisis rápidos de datos de vulnerabilidades mediante IA/ML a una escala enorme, así como protección en tiempo real con alertas inmediatas.

Proteger tus equipos en AWS es fácil y rápido con Falcon

Las organizaciones que emplean AWS conocen las ventajas de la tecnología de la nube para migrar sistemas anticuados y crear aplicaciones modernas. Además, saben lo importante que es aliarse con empresas situadas a la vanguardia en tecnología para reforzar sus sistemas y hacer crecer su negocio.

CrowdStrike Falcon Cloud Security se integra perfectamente con AWS Security Hub, se ha desarrollado con vistas a utilizar servicios AWS, como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS) y Amazon Linux 2, y se despliega mediante AWS Systems Manager. Los clientes de AWS que se alían con CrowdStrike tardan minutos en empezar a funcionar y tienen acceso inmediato a información y análisis de todos sus servicios desde una consola central. Además, CrowdStrike Falcon Cloud Security ocupa muy poco espacio, lo que tienen un impacto nulo en el rendimiento durante la ejecución, incluso durante análisis, búsquedas e investigaciones.



AWS y CrowdStrike juntos

CrowdStrike y los servicios de computación de AWS

- Cargas de trabajode contenedores
- Instancias de Amazon EC2, incluidas las de Graviton
- Amazon WorkSpaces
- Amazon Elastic Kubernetes Service
- Amazon Elastic Container Service
- AWS Fargate
- AWS Outposts

CrowdStrike y las integraciones de servicios de AWS en la nube

- AWS Verified Access
- AWS Account Factory Customization
- AWS Control Tower
- AWS Security Hub
- AWS Systems Manager
- AWS PrivateLink
- Amazon GuardDuty
- AWS Network Firewall
- AWS CloudEndure Disaster Recovery

Ahora es el momento de crear una estrategia de seguridad de la nube

En lo que respecta a la seguridad de la nube, aliarse con un experto que conoce a tus adversarios y sabe lo que buscan y cómo atacan es la mejor forma de defender tu empresa. CrowdStrike, líder del sector en ciberseguridad, ha demostrado su eficacia en la prevención de brechas de seguridad.

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

- **CrowdStrike Falcon for AWS ›**
- **Próximos eventos de CrowdStrike AWS ›**
- **Página de la alianza de CrowdStrike y AWS ›**
- **CrowdStrike en AWS Marketplace ›**