CROWDSTRIKE

FALCON HORIZON (CSPM) GESTIÓN DEL ESTADO DE SEGURIDAD DE LA NUBE

Detenga de raíz las brechas en la nube utilizando visibilidad unificada, detección de amenazas, supervisión continua y cumplimiento normativo en entornos multinube

VER MÁS, CONOCER MÁS, HACER MÁS

La adopción de la nube ha cambiado radicalmente la forma en la que las empresas lanzan al mercado y desarrollan aplicaciones modernas. Actualmente el ciclo de vida del desarrollo de aplicaciones otorga prioridad a la velocidad de lanzamiento, lo que obliga a los equipos de desarrollo a crear aplicaciones nativas en la nube basadas en una infraestructura programable que permita a las empresas cambiar y reconfigurar la infraestructura de la nube sobre la marcha.

Este cambio presenta nuevos retos que complican el trabajo a los equipos de seguridad. El resultado es una visibilidad y control insuficientes de los recursos de la nube, enfoques fragmentados para detectar y prevenir los errores de configuración, un mayor número de incidentes de seguridad y la incapacidad de garantizar un continuo cumplimiento de las normativas.

Falcon Horizon permite gestionar de forma más eficiente permite gestionar de forma más eficiente la seguridad de la nube durante el ciclo de vida del desarrollo de aplicaciones para cualquier nube, con el objetivo de que pueda desarrollar aplicaciones en la nube con seguridad y de forma más rápida y eficaz. La plataforma nativa en la nube CrowdStrike Falcon® proporciona visibilidad de la infraestructura de nube completa, supervisión continua para detectar errores de configuración y detección proactiva de amenazas, lo que permite a los equipos de DevSecOps corregir los problemas más rápidamente y ser más productivos.

VENTAJAS PRINCIPALES

- Ofrece total visibilidad multinube con una sola fuente de información para los recursos de la nube.
- Evita automáticamente los errores de configuración de la nube y las vulnerabilidades de las aplicaciones.
- Evalúa la seguridad de las cuentas de la nube y evita el incumplimiento de normativas.
- Reduce la fatiga de alertas y acelera la respuesta a incidentes.
- Mejora la calidad del código y limita los ciclos de vida de lanzamiento.
- Proporciona protección nativa en la nube sin agentes.

FALCON HORIZON
ADMINISTRACIÓN DEL ESTADO DE SEGURIDAD DE LA NUBE

CARACTERÍSTICAS PRINCIPALES

DESCUBRIMIENTO Y VISIBILIDAD

Unifica visibilidad y mejora de la seguridad de los entornos nube con una única solución nativa en la nube:

- Acceso a una única fuente de información para recursos de la nube y configuraciones de seguridad en distintas cuentas y entornos multinube.
- Descubrimiento automático de recursos y detalles de la nube (errores de configuración, metadatos, redes, seguridad, control de accesos o actividad de cambios) de forma inmediata al desplegarse. Los servicios admitidos incluyen:

AWS		
ACM	EKS	RDS
API Gateway v1	ElastiCache	Redshift
CloudTrail	ELB	Route 53
CloudFront	EMR	S3
CloudFormation	GuardDuty	SES
Config	IAM	SNS
DynamoDB	Kinesis	SQS
EBS	KMS	SSM
EC2	Lambda	VPC
ECR	NLB/ALB	

Azure	
Active Directory (AD)	Kubernetes Service
App Service	Load Balancer
Container Registry	Supervisión
Disk	Network Security Groups
File Service	PostgreSQL
Identity	SQL Server Virtual Machine
Key Vaults	Storage Account

- Gestión simplificada y mejora de las políticas de seguridad de distintas cuentas, proyectos, regiones y redes virtuales desde una sola consola unificada para reducir la superficie de ataque.
- Información de todas las llamadas de API de plano de control y detección de los riesgos de seguridad dentro de clústeres Kubernetes gestionados.
- Identificación de recursos de la nube no protegidos por Falcon Horizon.

GESTIÓN Y SOLUCIÓN DE ERRORES DE CONFIGURACIÓN

Elimina los riesgos para la seguridad y acelera el proceso de entrega:

- Comparación de las configuraciones de aplicaciones en la nube con valores de referencia del sector y las empresas, con el fin de identificar infracciones y poner remedio en tiempo real.
- Corrección de problemas que dejan los recursos de la nube expuestos —como errores de configuración, puertos IP abiertos y modificaciones no autorizadas— con corrección guiada y medidas de seguridad que permiten a los desarrolladores evitar fallos críticos.
- Supervisión del almacenamiento para garantizar que los permisos sean seguros y que no estén accesibles al público.
- Automatización de la detección y corrección de riesgos basados en la identidad en Azure para evitar que los usuarios puedan poner a la empresa en peligro.
- Verificación de que los grupos, usuarios y apps de Azure AD tienen los permisos correctos mediante los nuevos informes de **Identity Analyzer**.
- Solución de problemas más rápida y reducción de la fatiga de alertas con mejor gestión de políticas para cuentas en la nube, regiones o recursos específicos.
- Supervisión de instancias de base de datos y confirmación del uso de recursos de alta disponibilidad, copias de seguridad y cifrado, así como de grupos de seguridad para limitar la exposición.

ELIMINE LOS ÁNGULOS MUERTOS DE LA SEGURIDAD CON FALCON HORIZON

Unifica la visibilidad y el control en entornos multinube: Falcon Horizon ofrece descubrimiento y visibilidad continuos de los recursos nativos en la nube, proporcionando un valioso contexto e información del estado de seguridad general, así como las medidas necesarias para evitar incidentes de seguridad potenciales.

Evita errores de configuración de la nube y el incumplimiento de normativas: Falcon Horizon proporciona supervisión inteligente de los recursos de la nube para detectar de forma proactiva errores de configuración, vulnerabilidades y amenazas para la seguridad, además de una guía de corrección para resolver los riesgos de seguridad y dotar de medidas de seguridad a los desarrolladores con el fin de evitar errores que pueden salir caros y garantizar el cumplimiento normativo en entornos multinube.

Reduce la fatiga de alertas con detección de amenazas selectivas: Falcon Horizon supervisa continuamente para detectar anomalías y actividad sospechosa, y se integra perfectamente con las soluciones SIEM, lo que ofrece a los equipos de seguridad visibilidad y les permite priorizar las amenazas, reducir la fatiga de alertas mediante la eliminación de las que son innecesarias, y responder y corregir los problemas más rápidamente.

FALCON HORIZON
ADMINISTRACIÓN DEL ESTADO DE SEGURIDAD DE LA NUBE

DETECCIÓN DE AMENAZAS EN TIEMPO REAL

Detecta de forma proactiva amenazas durante el ciclo de vida del desarrollo de aplicaciones:

- Eliminación de la saturación de alertas de seguridad en entornos multinube mediante la identificación y administración de amenazas selectivas.
- Drástica reducción del número de alertas, centrándose en las áreas con más probabilidad de ser aprovechadas por los adversarios.
- Priorización de las vulnerabilidades según el entorno y adopción de medidas para evitar que el código vulnerable llegue a producción.
- Supervisión continua para detectar la actividad maliciosa, el comportamiento no autorizado y el acceso a los recursos de la nube, mediante el empleo de detección de amenazas de tiempo real.

SUPERVISIÓN CONTINUA DEL CUMPLIMIENTO NORMATIVO

Evalúa la seguridad de las cuentas de la nube y evita el incumplimiento de normativas:

- Supervisión continua del cumplimiento de normativas de todos sus recursos de la nube desde una sola consola.
- Conformidad con el marco CIS Benchmark que ofrece informes detallados, lo que le permite evaluar la seguridad de las cuentas en la nube en relación con las directrices CIS de Docker y Kubernetes.
- Identificación de las infracciones de políticas y medidas inmediatas activadas por el usuario para solucionarlas.

INTEGRACIÓN CON DEVSECOPS

Gracias a Falcon Horizon, el módulo de CSPM sin agente de Crowdstrike (solución nativa en el nube), es posible eliminar los conflictos y la complejidad de los entornos nube caracterizados por la presencia de múltiples proveedores y cuentas de usuario:

- Visibilidad y control centralizados de todos los recursos de la nube para que los equipos de operaciones de seguridad y de DevOps tengan una fuente única de información.
- Los equipos de seguridad pueden impedir que los recursos comprometidos avancen por el ciclo de vida de la aplicación.
- Con la integración con un SIEM, se simplifica la visibilidad de las operaciones de seguridad y se obtiene información y contexto de los errores de configuración y las infracciones de políticas con el fin de agilizar la respuesta a incidentes.
- Mediante una sola API, es posible integrar de forma rápida Falcon Horizon con las herramientas de DevOps y de colaboración que ya tiene, como el correo electrónico, Slack o PagerDuty, entre otras.
- Los informes y paneles de información predefinidos ofrecen la información de forma unificada y permiten compartir dicha información entre los distintos equipos: operaciones de seguridad, DevOps, infraestructuras, etc....

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 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**