Documento técnico de CrowdStrike

CROWDSTRIKE

Principales razones para añadir ya Falcon Identity Threat Protection a tu cartera de ciberdefensa

Los ataques basados en la identidad son la ciberamenaza número uno para las empresas actualmente. De hecho, más del 80 % de los incidentes de ciberseguridad están relacionados con el uso ilegítimo de credenciales válidas para obtener acceso a la red de una organización.

CrowdStrike Falcon® Identity Threat Protection, un módulo de la plataforma CrowdStrike Falcon®, detecta y detiene en tiempo real las brechas basadas en la identidad, en un panorama híbrido y complejo, con un solo sensor y con una interfaz unificada de defensa contra amenazas que facilita la correlación de los ataques entre los endpoints, las cargas de trabajo, las identidades y los datos. Estas son las cinco ventajas previstas que puedes obtener si añades la protección de identidades a tu cartera de ciberseguridad hoy mismo.*

1. Respuestas a las amenazas un 85 % más rápidas

Las soluciones tradicionales solo para endpoints no detectan las amenazas para la identidad y, además, la estrategia actual de correlacionar manualmente las amenazas entre endpoints e identidades mediante varias herramientas independientes, como las de higiene de AD, registros de eventos de Windows, PAM, UEBA o SIEM, entre otras, ralentiza las respuestas del equipo del SOC. Con la plataforma unificada CrowdStrike Falcon, los clientes de Falcon Identity Threat Protection pueden ver las rutas de ataque completas y correlacionar las amenazas en una sola consola. De esta forma, las **respuestas son un 85 % más rápidas** y se obtiene protección en tiempo real, lo que ahorra al año miles de horas de investigación tras las brechas.

2. Incremento de hasta el 84 % de la eficiencia operativa

CrowdStrike Falcon es **una solución nativa de la nube con un solo sensor** que puede desplegarse en cualquier lugar en el entorno del cliente, lo que simplifica la recopilación de telemetría (del endpoint o la identidad). Un gran distribuidor minorista **consolidó más de 5 herramientas** (las típicas de varias empresas) en una sola para hacer frente a las amenazas para la identidad con Falcon Identity Threat Protection. La consolidación del SOC con una plataforma y un sensor elimina las herramientas y agentes independientes, con el consiguiente ahorro de costes en infraestructura y operaciones. Además, al no tener que emplear datos procedentes de diferentes registros, la detección en tiempo real permite recortar el total de horas de mantenimiento e **incrementar la eficiencia operativa hasta un 84 %**, reduciendo el personal necesario aproximadamente en cuatro EJC.

3. Reducción de hasta un 75 % de los costes de cumplimiento y soporte

Gracias a la amplia visibilidad de las contraseñas vulneradas, las cuentas con exceso de privilegios y el uso indebido de cuentas de servicio, los clientes pueden anticiparse a los problemas de higiene del Directivo Activo y establecer controles proactivos, lo que reduce los costes derivados del incumplimiento normativo. En un caso, un CISO comunicó que **los restablecimientos de contraseñas, y los correspondientes costes de soporte asociados, habían descendido un 75 %,** el nivel de vulnerabilidad ante el phishing había bajado un 8 % y los casos de derechos de acceso de usuario innecesarios se habían reducido un 32 %. Una granempresa de telecomunicaciones indicó que el empleo de Falcon Identity Threat Protection para llevar la autenticación multifactor (MFA) a todas las áreas (incluidas las aplicaciones tradicionales) le había permitido mejorar su postura en cuanto a la Certificación del Modelo de Madurez de Ciberseguridad (Cybersecurity Maturity Model Certification, CMMC).

4. Reducción de hasta el 57 % del riesgo de robo de credenciales que facilita una brecha

En ocho de cada diez ataques se produce un robo o una vulneración de credenciales, por lo que reducir este riesgo tiene un impacto directo en la mejora de la postura de seguridad. La capacidad de Falcon Identity Threat Protection para detectar amenazas específicas para la identidad permite a los clientes identificar las cuentas de alto riesgo y las posibles rutas de ataque en todo el entorno, lo que disminuye la superficie de ataque. El CISO de una cadena hotelera ha revelado recientemente cómo Falcon Identity Threat Protection descubrió 250 000 rutas de ataque posibles en el entorno de la empresa y cómo el 93 % de ellas pudieron cerrarse mediante tres cambios de configuración concretos. Las evaluaciones del valor comercial de CrowdStrike muestran una **disminución de hasta el 57 % del riesgo de robo de credenciales**, que es la antesala a una brecha. Esto se pone también de manifiesto en el éxito obtenido en las pruebas de penetración por clientes que antes de desplegar Falcon Identity Threat Protection habían obtenido malos resultados en las mismas pruebas.

5. Mejora de condiciones de los ciberseguros y reducción del precio de las primas

Mientras los atacantes continúan sacando partido de la insuficiencia de controles de seguridad de la identidad para lanzar sus ataques, **las compañías ciberaseguradoras insisten en** la necesidad de reforzar los controles para reducir el ciberriesgo. El ransomware es uno de los factores clave de un ciberseguro, por lo que las compañías reiteran la necesidad de que las empresas protejan AD, implementen MFA en todas las aplicaciones, incluidas las tradicionales, protejan las cuentas con privilegios y de servicios, e implementen sistemas de detección y respuesta para endpoints (EDR). Los clientes que han desplegado Falcon Identity Threat Protection afirman que observan un impacto positivo en su ciberseguro y una reducción de las primas.

La opinión de los clientes de CrowdStrike

"Tras desplegar Falcon Identity Threat Protection, realizamos otra prueba de penetración e inmediatamente observamos las ventajas del aumento de visibilidad".

Ryan Melle
SVP, CISO, Berkshire Bank
(**Leer el caso de estudio**)

"Desde que desplegamos Falcon Identity Threat Protection, hemos experimentado una enorme mejora en lo que detectamos en cuanto a credenciales, identidades con privilegios y distintas rutas de ataque, y en la mitigación de estos ataques".

Steven Townsley
Head of Information Security,
Mercedes-AMG Petronas F1 Team
(**Ver el vídeo**)

"Solo dos horas después de desplegar Falcon Identity Threat Protection, habíamos identificado 10 cuentas con privilegios con contraseñas vulneradas y comenzamos a restablecer estas contraseñas inmediatamente".

CISO de un condado de Washington, D.C.
(**Leer el artículo del blog**)

"Empezamos a apreciar la utilidad de Falcon Identity Threat Protection desde el minuto uno, cuando pudimos ver 250 000 rutas de ataque posibles y corregir el 93 % de ellas con solo tres cambios de configuración".

CISO de una cadena hotelera multinacional

"Básicamente es más sencillo tener un solo panel para la mayoría de los SOC, en lugar de tener que consultar 13 consolas y páginas diferentes para analizar y localizar la información".

CISO de un agronegocio y empresa del sector alimentario

La protección de las identidades es esencial y no puede cuestionarse

Según indica el informe Global Threat Report 2023 de CrowdStrike, los ataques contra la identidad van en aumento, con un **incremento del 112 % de anuncios de intermediarios de acceso** en la dark web en 2022. El Directorio Activo de Microsoft, tecnología empleada por más del 90 % de las empresas, sigue siendo el punto débil preferido por los atacantes.[1] Según un reciente análisis de metadatos de millones de cuentas (humanas, de servicios y con privilegios) elaborado por CrowdStrike, un **50 % de las empresas tienen cuentas con privilegios que han sufrido una vulneración de la contraseña**.

A este problema se suma la conocida dificultad para detectar las brechas basadas en la identidad, que requieren de media **unos 250 días para su identificación**[2] si no se cuenta con las herramientas adecuadas. Durante ese período, los atacantes pueden moverse lateralmente a su antojo por el entorno y lanzar ataques de consecuencias catastróficas. Según el informe Global Threat Report 2023 de CrowdStrike, el tiempo de propagación medio **ha descendido hasta los 84 minutos en 2022**, por lo que las empresas no se pueden permitir el lujo de sentarse a esperar la llegada de una brecha para la identidad grave. De hecho, es posible que ya haya un ciberdelincuente infiltrado en tu entorno sin que lo hayas advertido.

Las consecuencias de ignorar las amenazas basadas en la identidad pueden ser graves e incluyen el compromiso total de dominios de la infraestructura de AD, ataques de ransomware que paralizan las operaciones y las devastadoras interrupciones de la actividad empresarial. Según IBM y el Ponemon Institute, **el coste total medio de una brecha a nivel mundial es de 4,35 millones de USD (9,44 millones de dólares en Estados Unidos)**.[3] En **8 de cada 10 ataques** se utilizan credenciales robadas o vulneradas, por lo que el despliegue de protección de la identidad tendrá un impacto inmediato, y puede implicar un ahorro de millones de dólares y la protección de tu marca y tu reputación para evitar daños irreversibles.

Recuerda, los ciberdelincuentes no esperarán a que te cubras antes de asestar el primer golpe. Frena la brecha ya con Falcon Identity Threat Protection.

Ponte en contacto con tu representante de CrowdStrike o solicita tu Evaluación de riesgos del Directorio Activo gratuita.

[1]Frost & Sullivan, "Active Directory Holds the Keys to your Kingdom, but is it Secure?"

[2]IBM y Ponemon Institute, "Cost of a Data Breach Report 2022"

[3]IBM y Ponemon Institute, "Cost of a Data Breach Report 2022"

*No se garantizan los resultados previstos y las consecuencias efectivas, que pueden variar según el cliente. Las ventajas previstas 1, 2 y 4 se basan en medias acumuladas de más de 100 casos de evaluaciones de valor comercial (Business Value Assessment, BVA) y valor comercial realizado (Business Value Realized, BVR) efectuadas con clientes de CrowdStrike Enterprise y el equipo Business Value de CrowdStrike entre 2018 y diciembre de 2022. Las BVA son análisis de la rentabilidad de la inversión prevista basados en el valor de CrowdStrike comparado con la solución que poseen los clientes. Los valores de BVR corresponden al análisis de la rentabilidad de la inversión para los clientes que llevan más de 6 meses con nuestra solución desplegada y se basa en las opiniones de los clientes y la telemetría registrada. La ventaja prevista número 3 se basa en datos aportados a CrowdStrike directamente por un cliente.

Acerca de CrowdStrike

CrowdStrike (Nasdaq: CRWD), líder mundial en ciberseguridad, ha redefinido la seguridad moderna con la plataforma nativa en la nube más avanzada del mundo, para proteger aspectos fundamentales del riesgo empresarial: las cargas de trabajo, la identidad y los datos, tanto en los endpoints como en la nube.

Gracias a CrowdStrike Security Cloud y una inteligencia artificial de talla mundial, la plataforma CrowdStrike Falcon® se nutre de indicadores en tiempo real, inteligencia sobre amenazas, información de las herramientas evolutivas de los adversarios y telemetría enriquecida con datos de toda la empresa, para facilitar detecciones hiperprecisas, protección y remediación automatizadas, Threat Hunting de élite y observación de vulnerabilidades por prioridades.

Desarrollada expresamente en la nube con una arquitectura de agente ligero único, la plataforma Falcon ofrece un despliegue rápido y escalable, protección y rendimiento superiores, menor complejidad y rentabilidad inmediata.

CrowdStrike: **We stop breaches.**

Síguenos: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Empezar una prueba gratuita

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