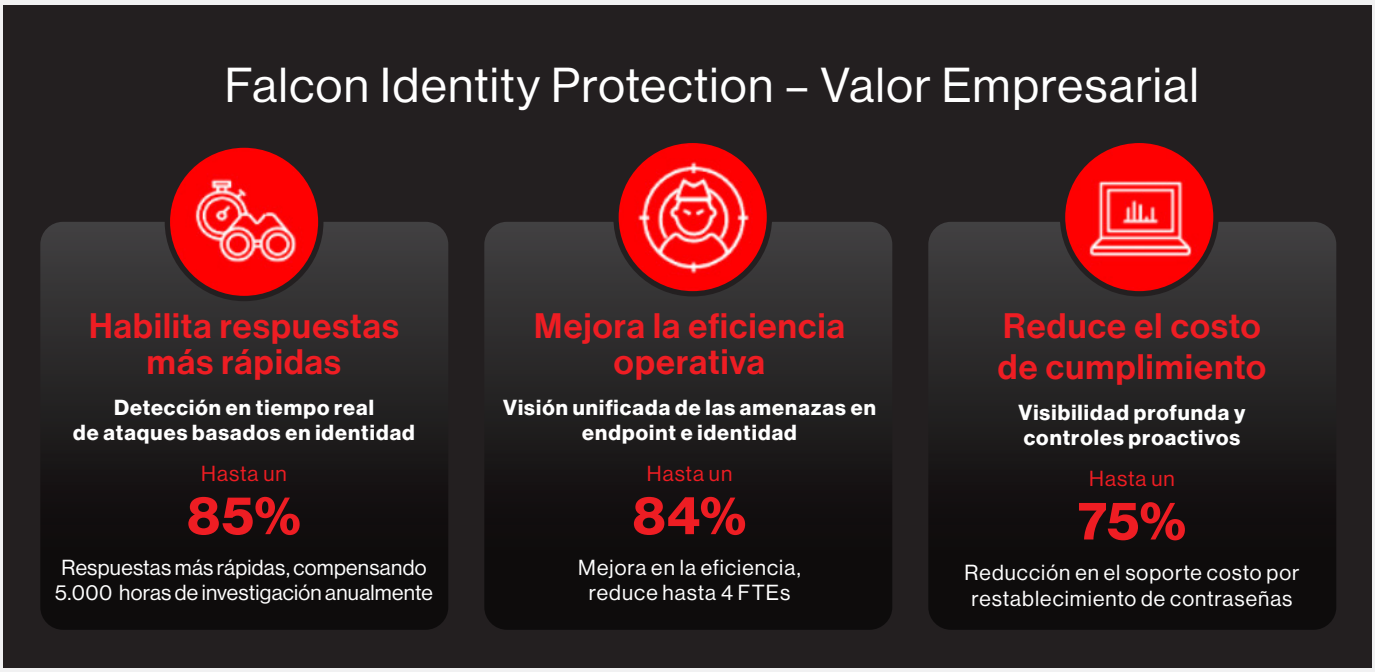
White Paper de CrowdStrike

CROWDSTRIKE

Razones principales para reforzar ya tu defensa cibernética con Falcon Identity Threat Protection

Los ataques basados en la identidad son la principal amenaza de ciberseguridad que enfrentan las organizaciones en la actualidad. De hecho, más del 80% de los incidentes cibernéticos implican el uso indebido de credenciales válidas para acceder a la red de una organización.

CrowdStrike Falcon® Identity Threat Protection, un módulo de la plataforma CrowdStrike Falcon®, detecta y detiene las brechas impulsadas por la identidad en tiempo real en un entorno de identidad híbrido complejo, con un solo sensor y una interfaz de amenazas unificada con correlación de ataques en endpoints, workloads, identidad y datos. Aquí hay cinco beneficios esperados que puedes obtener al agregar la protección de identidad a tu cartera de amenazas de ciberseguridad hoy.*



1. Permite respuestas hasta un 85% más rápidas a las amenazas

Las soluciones tradicionales solo para endpoint pierden amenazas de identidad y el enfoque actual de correlacionar manualmente las amenazas entre endpoint e identidad con múltiples herramientas independientes — herramientas de higiene de AD, Registro de Eventos de Windows, Gestión de Cuentas Privilegiadas (PAM), UEBA, SIEM y más — ralentizan las respuestas del equipo de Centro de Operaciones de Seguridad (SOC). Con la plataforma unificada CrowdStrike Falcon, los clientes de Falcon Identity Threat Protection pueden ver rutas de ataque completas y correlacionar amenazas en una sola consola. Esto puede resultar en **respuestas hasta un 85% más rápidas** y protección en tiempo real, compensando miles de horas de investigación post brecha cada año.

2. Aumenta la eficiencia operativa hasta en un 84%

CrowdStrike Falcon es **una solución nativa de la nube con un solo sensor** que se puede implantar en cualquier lugar del entorno del cliente, simplificando la recopilación de telemetría (desde endpoint o identidad). Un gran distribuidor minorista **consolidó más de 5 herramientas** (típicas de muchas empresas) en una sola para gestionar las amenazas de identidad con Falcon Identity Threat Protection. La consolidación de Centro de Operaciones de Seguridad (SOC) con una plataforma y un sensor, elimina las herramientas y agentes independientes, lo que resulta a modo de ahorro directo de herramientas y costos operativos. Y, al eliminar la necesidad de emplear ingestión de registros dispares, la detección en tiempo real puede reducir las horas totales de mantenimiento y **aumentar la eficiencia operativa hasta en un 84%**, reduciendo el número de personal en aproximadamente cuatro FTEs.

3. Reduce los costos de cumplimiento y soporte hasta en un 75%

La visibilidad profunda de las contraseñas afectadas, las cuentas sobre privilegiadas y el uso indebido de cuentas de servicio permite a los clientes abordar de manera proactiva los asuntos de higiene de Active Directory y establecer controles proactivos, lo que reduce los costos de cumplimiento. En un caso, un CISO informó una **reducción del 75% en los reajustes de la contraseña de soporte y los costos asociados,** un 8% de reducción en la susceptibilidad a la suplantación de identidad y un 32% de reducción en los derechos de acceso innecesarios de los usuarios. Un gran proveedor de telecomunicaciones informó que mejoró la postura de cumplimiento de la Certificación del Modelo de Madurez de Ciberseguridad (CMMC) mediante el uso de Falcon Identity Threat Protection para extender la autenticación multifactor (MFA) en todas partes, incluidas las aplicaciones tradicionales.

4. Reduce el riesgo de robo de credenciales que conducen a una brecha hasta en un 57%

Con ocho de cada 10 ataques que involucran credenciales robadas o afectadas, reducir el riesgo de credenciales robadas tiene un impacto directo en la mejora de la postura de riesgo. La capacidad de Falcon Identity Threat Protection para detectar amenazas específicas de identidad permite a los clientes identificar cuentas de alto riesgo y posibles rutas de ataque en todo su entorno, lo que reduce la superficie de ataque. Recientemente, el CISO para una cadena de hospitalidad compartió cómo Falcon Identity Threat Protection reveló inmediatamente 250.000 posibles rutas de ataque en el entorno de la compañía y cómo el 93% de ellas se podían arreglar con tres cambios de configuración específicos. Las Evaluaciones de Valor Empresarial de CrowdStrike han demostrado una **reducción de hasta un 57% en el riesgo de robo de credenciales** que conduzcan a una brecha. Esto también ha sido demostrado por pruebas de penetración exitosas realizadas por clientes que habían fallado las mismas pruebas antes del despliegue de Falcon Identity Threat Protection.

5. Mejora la ciber asegurabilidad y reduce las primas

A medida que los adversarios continúan el exploit de los controles débiles de seguridad de identidad para lanzar ataques, **las compañías de ciber seguros enfatizan** la necesidad de reforzar los controles para reducir el riesgo cibernético. Dado que el ransomware es uno de los factores clave para el seguro de ciberseguridad, las aseguradoras han reiterado la necesidad de que las organizaciones refuercen la AD, hagan cumplir la autenticación multifactor (MFA) en todas las aplicaciones, incluidas las tradicionales, protejan las cuentas privilegiadas y de servicio e implanten la detección y respuesta de endpoints (EDR) como requisitos previos para la ciber asegurabilidad. Los clientes que han implantado Falcon Identity Threat Protection dicen que ha impactado positivamente en su programa de seguro de ciberseguridad y ha reducido las primas.

Qué dicen los clientes de CrowdStrike

"Después de implementar Falcon Identity Threat Protection, hicimos otra prueba de penetración e inmediatamente vimos los beneficios de la visibilidad mejorada."

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

"Desde que implementamos Falcon Identity Threat Protection, hemos tenido un gran repunte en lo que podemos ver con respecto a las credenciales, las identidades privilegiadas, las diferentes rutas de ataque y cómo podemos mitigarlas."

Steven Townsley
Jefe de Seguridad de Información, Mercedes-AMG Petronas F1 Team (**Ver video**)

"A las dos horas de implementar Falcon Identity Threat Protection, identificamos 10 cuentas privilegiadas con contraseñas afectadas y comenzamos a reiniciarlas de inmediato."

CISO de un condado en el área de Washington, D.C.(**Leer publicación de blog**)

"Obtuvimos el valor de Falcon Identity Threat Protection en el primer minuto, cuando pudimos ver 250.000 posibles rutas de ataque y el 93% de ellas podrían arreglarse con solo tres cambios de configuración."

CISO de una multinacional cadena de hospitalidad

"Es más fácil mantener un panel de vidrio para la mayor parte de tu Centro de Operaciones de Seguridad (SOC) que buscar en 13 consolas y páginas diferentes para analizar y rastrear algo."

CISO de una agro industria y compañía de alimentos

La protección de identidad es esencial, no opcional

El informe sobre amenazas globales de CrowdStrike 2023 muestra que los ataques de identidad van en aumento, con un **crecimiento del 112% en los anuncios de bróker de acceso** en la dark web en 2022. Microsoft Active Directory sigue siendo el suave bajo vientre para que los adversarios lo persigan, con más del 90% de las organizaciones confiando en él .[1] Un reciente análisis de metadatos de millones de cuentas (humanas, de servicio, privilegiadas) realizado por CrowdStrike reveló que un **asombroso 50% de las organizaciones tienen cuentas privilegiadas con contraseña afectada**.

Complicando este problema, las brechas de identidad son notablemente difíciles de detectar, requiriendo un promedio de **alrededor de 250 días para identificar**[2] sin las herramientas adecuadas. Durante ese tiempo, los adversarios pueden moverse lateralmente sin ser detectados en tu entorno y lanzar ataques catastróficos. Con un tiempo de comprometimiento promedio **de 84 minutos en 2022**, según el Informe Global de Amenazas CrowdStrike 2023, las organizaciones no tienen el lujo de esperar a que ocurra una brecha grave de identidad. De hecho, es posible que el adversario ya esté en tu entorno y que no seas consciente de ello.

Podría haber graves consecuencias al ignorar las amenazas impulsadas por la identidad, incluida la afectación total del dominio de tu infraestructura AD, los ataques de ransomware paralizantes y las interrupciones catastróficas del negocio. Según IBM y el Instituto Ponemon, el **costo total promedio global de una brecha de datos es de $4.35 millones de dólares ($9.44 millones de dólares el costo promedio de brecha en los Estados Unidos)**.[3] Con **8 de cada 10 ataques** que involucran credenciales robadas o afectadas, implantar la protección de identidad tendrá un impacto inmediato, potencialmente ahorrándote millones de dólares y protegiendo tu marca y reputación de daños irreversibles.

Recuerda, los adversarios no están esperando que te pongas los guantes antes de lanzar sus golpes. Detén la brecha hoy con Falcon Identity Threat Protection.

Contacta tu representante de cuenta CrowdStrike o solicita tu Análisis de Riesgo del Active Directory gratuito.

[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"

* Los resultados esperados y los resultados reales no están garantizados y pueden variar para cada cliente. Los beneficios esperados 1, 2 y 4 se basan en promedios agregados de más de 100 casos de Evaluación de Valor Empresarial (BVA) y Valor Empresarial Realizado (BVR) realizados con clientes de CrowdStrike Enterprise y completados por el equipo de Valor Empresarial de CrowdStrike desde 2018 a diciembre de 2022. Los BVAs son un análisis de ROI proyectado basado en el valor de CrowdStrike en comparación con la solución actual de los clientes. Los BVRs son un análisis de ROI realizado para clientes implantados durante más de 6 meses usando las entradas de los clientes y la telemetría grabada. El beneficio esperado 3 se basa en los datos compartidos por un cliente directamente con CrowdStrike.

Acerca de CrowdStrike

CrowdStrike (NASDAQ: CRWD) es un líder global en ciberseguridad, que ha redefinido la seguridad moderna con una de las plataformas nativas para la nube más avanzadas del mundo para proteger áreas críticas de riesgo corporativo — endpoints y workloads de nube, identidad y datos.

Impulsado por CrowdStrike Security Cloud™ y una Inteligencia Artificial de clase mundial, la plataforma CrowdStrike Falcon® aprovecha indicadores de ataque en tiempo real, inteligencia sobre amenazas, el tradecraft cambiante de los adversarios y telemetría enriquecida de toda la empresa para ofrecer detecciones hiper precisas, protección y remediación automatizadas, cacería de amenazas de élite y observabilidad priorizada de vulnerabilidades.

Construida para ese fin en la nube con una arquitectura única y liviana de agente, la plataforma Falcon entrega implantación rápida y escalable, protección y desempeño superiores, complejidad reducida y un tiempo de amortización inmediato.

CrowdStrike: **We stop breaches.**

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

Inicia la prueba gratuita

Obtén más información en **www.crowdstrike.com/latam**