CLOUDFLARE

Descripción general del producto

Seguridad del correo electrónico de Cloudflare

Protección autónoma y multicanal para una comunicación segura en el espacio de trabajo

Protección contra los ataques de phishing selectivo

Bloquea y aísla fácilmente las amenazas que otras soluciones no detectan

El correo electrónico es la aplicación empresarial más utilizada y más susceptible a ataques, por lo que es más importante que nunca proteger a los usuarios contra los ataques de phishing que quieren manipular su confianza.
A medida que las organizaciones continúan adoptando cada vez más los servicios de correo electrónico en la nube mediante Microsoft 365 y Google Workspace para facilitar el trabajo híbrido, los ciberdelincuentes han empezado a utilizar ataques más selectivos de bajo volumen que pueden evadir las puertas de enlace de correo electrónico seguras (SEG) tradicionales como Proofpoint y Mimecast.

Por este motivo, la solución de seguridad del correo electrónico en la nube de Cloudflare se ha diseñado específicamente para utilizar la información preventiva de campañas, el análisis de contenido basado en el aprendizaje automático y una plataforma Zero Trust unificada a fin de detener las amenazas de phishing antes de que lleguen a tus usuarios.

91 %

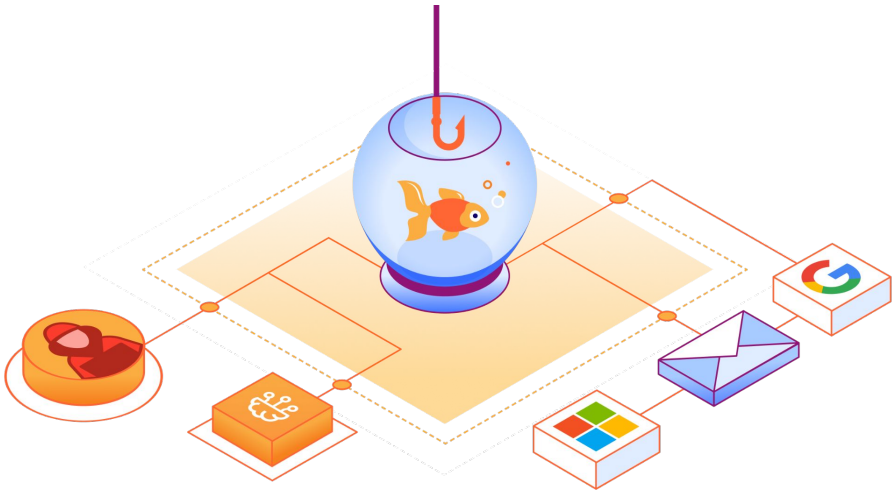
de todos los ciberataques comienzan con un correo electrónico de phishing[1]

50 MM

en pérdidas como resultado de los ataques al correo electrónico corporativo en la última década[2]

81 %

de las organizaciones han sufrido un ataque multicanal en los últimos 12 meses[3]



Evita las amenazas al correo electrónico corporativo (BEC)

Detecta las cuentas suplantadas y en riesgo con el análisis contextual por capas y basado en el aprendizaje automático.

Aísla los ataques diferidos y multicanal

Aísla a los usuarios del contenido web malicioso que se envía a través de enlaces desconocidos y ofuscados.

Bloquea el ransomware y los archivos adjuntos maliciosos

Evita que los intentos de extorsión y el código malicioso pongan en riesgo tu organización.

Mayor protección y simplicidad

Implementa la seguridad por capas que ofrece mayor protección con un coste mínimo

Con la proliferación de los ataques de phishing, que sigue en aumento, Microsoft y Google han continuado desarrollando una funcionalidad nativa que permite prestaciones básicas de protección de los datos y del correo electrónico, entre ellas, la autenticación, el almacenamiento, y la encriptación del lado cliente. Sin embargo, las tácticas de los ciberdelincuentes han evolucionado y ahora ejecutan ataques más selectivos y evasivos que a menudo los controles de seguridad nativos no detectan y que logran una elevada tasa de éxito.

Con la seguridad por capas de Cloudflare, las organizaciones pueden bloquear o aislar automáticamente los ataques de phishing selectivos que utilizan los enlaces maliciosos, los archivos adjuntos y las cuentas en riesgo para intentar robar información confidencial y cometer fraudes financieros.

Complementa tus controles actuales de seguridad del correo electrónico

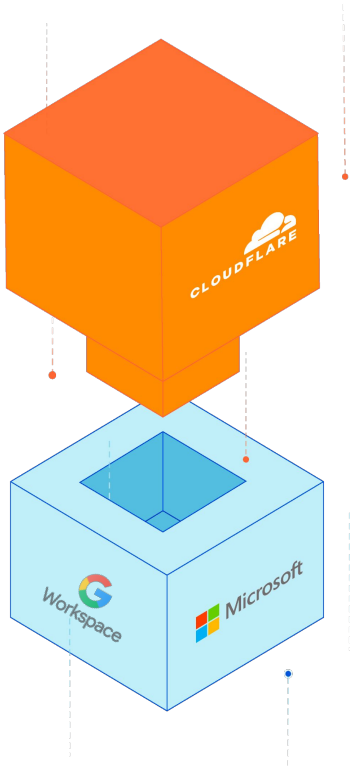
La solución de seguridad del correo electrónico nativa de nube de Cloudflare se puede implementar en cuestión de minutos para mejorar las implementaciones existentes de puerta de enlace de correo electrónico segura, o para complementar las prestaciones de correo electrónico integradas que proporcionan Microsoft y Google. Sin apenas necesidad de ajustes, las organizaciones pueden conseguir una mayor protección contra el phishing, y dedicar menos tiempo y esfuerzo a la gestión continua de la seguridad.

"Desde que implementamos Cloudflare [además de M365], el número de correos electrónicos maliciosos o sospechosos que nuestros usuarios reciben cada día se ha reducido un 50 %. Esta ventaja supone un ahorro de muchas horas, que podemos reinvertir en otros objetivos".

Werner Enterprises
(Fortune 1000)

Seguridad del correo electrónico: protección contra los ataques al correo electrónico corporativo y el phishing selectivo

Proveedor de correo electrónico: prestaciones básicas de datos y de correo electrónico



Reinversión de horas ahorradas gracias a una mayor automatización

La solución automatizada y ligera de Cloudflare ofrece una perfecta integración con los flujos de trabajo de Microsoft y Google al mismo tiempo que proporciona una única e intuitiva interfaz de usuario para las actividades de los analistas.

Eficacia de detección del 99,997 %

La combinación de las prestaciones nativas del proveedor de correo electrónico con la protección contra phishing y los ataques al correo electrónico corporativo de Cloudflare garantiza a las empresas una cobertura completa para minimizar el riesgo.

Más valor con menos costes

La sustitución de las implementaciones obsoletas, costosas y complejas por la solución de Cloudflare, sin apenas configuración, puede reducir los costes, las funciones redundantes y los ajustes innecesarios.

Evita los ataques sofisticados al correo electrónico corporativo

50 000 millones de dólares en pérdidas (y en aumento)

Los ataques al correo electrónico corporativo han sido responsables de una cifra astronómica de pérdidas durante la última década, por lo que es sorprendente que algunas organizaciones aún no hayan priorizado la búsqueda de una solución a ese efectivo método de fraude financiero. Aunque los ataques al correo electrónico corporativo representan un porcentaje mucho más pequeño de las amenazas de phishing, las puertas de enlace de correo electrónico seguras y los proveedores de correo electrónico en la nube a menudo no los detectan, lo que genera mayores pérdidas financieras. Estos ataques selectivos son difíciles de detectar porque se aprovechan de las cuentas suplantadas o en riesgo y del contexto conversacional para hacerse pasar por un empleado o proveedor de confianza.

Amplía los principios de Zero Trust al correo electrónico

Cuando los atacantes utilizan una cuenta de correo electrónico en riesgo de un empleado o proveedor, pueden evadir los controles de seguridad tradicionales que solo intentan confirmar la legitimidad de la cuenta del remitente. Cloudflare va un paso más allá, ya que analiza una gran variedad de atributos del comportamiento, patrones de escritura, indicadores de sentimiento y el historial de conversaciones a fin de determinar la autenticidad del remitente. La información de los modelos de amenazas basados en el aprendizaje automático y de la extensa red de Cloudflare ofrece la herramienta más eficaz contra las cuentas en riesgo utilizadas para extraer pagos fraudulentos.

Figura 1: análisis de mensajes

Detección de los ataques al correo electrónico corporativo con el análisis contextual basado en el aprendizaje automático

Una identificación precisa de los ataques al correo electrónico corporativo requiere algo más que un simple análisis estructural de un mensaje. Una correcta detección también implica comprender detalladamente las variaciones del estilo conversacional y la intención. El motor de análisis de patrones pequeños, basado en la telemetría de la amplia red de Cloudflare (más de 3 billones de solicitudes DNS al día) y los modelos de aprendizaje automático (en constante evolución), descompone cada uno de los aspectos de un mensaje de correo electrónico a fin de evaluar los patrones de escritura, el sentimiento, el contexto histórico y una gran variedad de otras variables que ayudan a revelar la autenticidad del remitente.

Aislamiento de ataques basados en enlaces

Los ataques basados en enlaces se han convertido en el método preferido para robar credenciales, cargar malware/ransomware y extraer información confidencial. La utilización de una combinación de correo electrónico, chat, SMS, redes sociales y otras aplicaciones para enviar estos enlaces complica aún más el proceso de garantizar que tanto los usuarios como los datos están protegidos de los ataques de phishing selectivos.

Cloudflare resuelve los ataques de phishing basados en enlaces representando todo el código web de forma remota en nuestra red global en la nube en lugar de en el dispositivo local del usuario. De esta manera, se mitiga el malware y las vulnerabilidades de día cero del navegador, a la vez que se proporciona un control granular sobre las acciones del usuario (p. ej. desactivar las entradas de teclado) para evitar la recolección de credenciales y las fugas de datos.

Eliminación del riesgo de phishing sin ralentizar el trabajo de los equipos

La integración de capacidades de aislamiento de navegadores de última generación basadas en nuestra exclusiva tecnología Network Vector Rendering (NVR) permite a Cloudflare ofrecer una solución eficaz, segura y escalable para aislar enlaces potencialmente peligrosos. A diferencia de las técnicas que consumen mucho ancho de banda, NVR transmite comandos de dibujo seguros al dispositivo. De esta manera, se elimina el riesgo de contenido web malicioso sin afectar a la experiencia del usuario final. Gracias a NVR y a la red de baja latencia de Cloudflare, las organizaciones pueden aislar las amenazas multicanal, y garantizar una productividad sin interrupciones para sus usuarios.

Investigación y resolución rápidas

Gestión de la seguridad intuitiva sin apenas configuración

Con una mayor automatización y una configuración mínima para lograr unos resultados óptimos, Cloudflare reduce considerablemente el tiempo y el esfuerzo necesarios para la gestión continuada de la seguridad del correo electrónico. Los equipos de seguridad pueden beneficiarse inmediatamente de una vista integral de todas las métricas y tendencias de primera línea en el panel de control, y hacer clic en los mensajes señalados para ver información más detallada. Profundizar en la información de las tendencias permite descubrir rápidamente los tipos de ataque frecuentes, a qué ejecutivos se dirigen ataques, los ataques diferidos mitigados y otros datos críticos.

Todos los análisis, la telemetría, la información acerca de amenazas observadas y los indicadores de riesgo (IOC) están disponibles mediante una exhaustiva API para poder integrarlos fácilmente con las herramientas existentes de orquestación y los flujos de trabajo de los analistas.

> "A menudo explico a mis compañeros lo sencillo y fácil que es utilizar Cloudflare como una solución SaaS en la nube y lo satisfecho que estoy con su alto nivel de precisión".
>
> **Japan Airlines**

Detección y respuesta gestionadas (PhishGuard)

El servicio de seguridad gestionada del correo electrónico de Cloudflare, PhishGuard, complementa tu equipo de SOC existente para liberar ciclos de investigación de seguridad y proporcionar valiosa información sobre amenazas. PhishGuard puede ayudarte a neutralizar las campañas de phishing con investigaciones, evaluaciones de amenazas internas, eliminación de fraudes activos y complejas necesidades de corrección. PhishGuard amplía los recursos de seguridad y los conocimientos para notificarte proactivamente sobre posibles fraudes y amenazas internas, al mismo tiempo que se ocupa de la detección de amenazas por correo electrónico.

Funciones y ventajas de PhishGuard:

- Gestión de los envíos de phishing y la respuesta a incidentes para acelerar su resolución.
- Notificaciones proactivas acerca de fraudes y ataques al correo electrónico corporativo para que las organizaciones puedan responder en una fase temprana del ciclo de vida del ataque.
- Recursos dedicados para la supervisión en tiempo real, las revisiones periódicas de las cuentas y la evaluación continua de las amenazas.
- Firmas de bloqueo personalizadas basadas en un análisis de amenazas del entorno gestionado.

+1100

Horas ahorradas anualmente gracias a la automatización de la clasificación manual

La solución automatizada de Cloudflare elimina las tareas manuales y que pueden requerir mucho tiempo a fin de mejorar los tiempos de respuesta y liberar ciclos adicionales.

50 %

Reducción de los correos electrónicos maliciosos o sospechosos recibidos (sobre M365)

La implementación de la seguridad de Cloudflare sobre Microsoft 365 permite a las organizaciones detectar ataques selectivos y reducir el número global de correos electrónicos maliciosos.

40

Número total de horas dedicadas en siete años a la configuración de la seguridad del correo electrónico

La seguridad del correo electrónico de Cloudflare apenas requiere configuración inicial ni ajustes continuados, y proporciona una gran eficacia de detección lista para su uso.

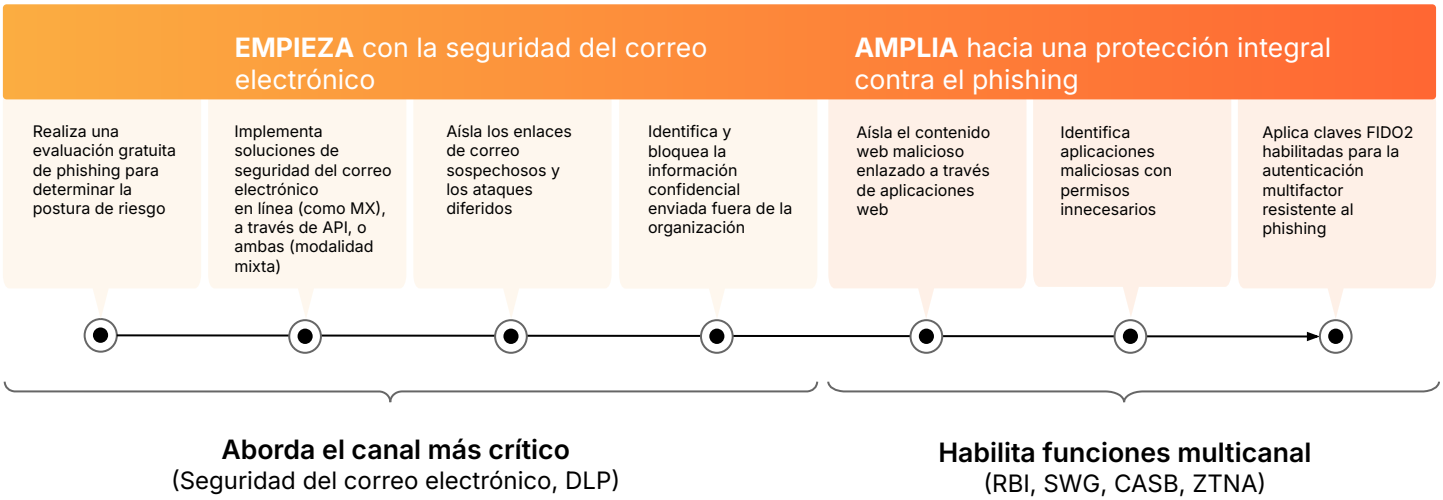
BENEFICIOS

Protección multicanal completa

Más allá del correo electrónico, la rápida evolución de las campañas de phishing pone de manifiesto más que nunca la urgente necesidad de que las organizaciones implementen una solución de phishing que proporcione un camino rápido y sencillo hacia una protección multicanal completa.

Con la plataforma de seguridad unificada de Cloudflare, las organizaciones pueden implementar en primer lugar una solución de seguridad de correo electrónico líder en el sector para abordar rápidamente el canal de phishing más crítico. A continuación, pueden activar de manera muy fácil los servicios Zero Trust para ampliar la protección a todos los canales, y detener de manera eficaz las amenazas de phishing conocidas y emergentes.

- **Protección sin apenas configuración y muy eficaz:** Minimiza el riesgo de phishing con una detección eficaz líder en el sector que requiere una configuración mínima.
- **Mayor consolidación, menor coste:** Reduce el gasto con una única plataforma totalmente integrada que resuelve todos los casos de uso de phishing.
- **Rápida implementación, fácil gestión:** Garantiza una protección inmediata, mientras reduces el tiempo y el esfuerzo necesarios para la gestión continua.



Evalúa y compara

Evalúa tus soluciones actuales de protección del correo electrónico y comprueba qué amenazas no se están detectando

Ejecuta un análisis retroactivo gratuito en minutos para ver qué amenazas de phishing no se han detectado en los últimos 14 días o solicita una evaluación del riesgo de phishing para monitorizar las bandejas de entrada en busca de phishing. Compara con otros proveedores que no ofrecen ajustes listos para usar, y descubre cómo nuestra solución de seguridad del correo electrónico proporciona la protección más rápida y fácil.

Ejecutar análisis retroactivo | Solicitar evaluación

1. Investigación de Deloitte de 2020: Fuente
2. 2023 FBI IC3 PSA: Fuente
3. 2023 Forrester Opportunity Snapshot: Fuente

