Seguridad del correo electrónico en la nube (CES)

Cloudflare, empresa líder en seguridad del correo electrónico reconocida por los analistas, detecta y evita de forma preventiva las amenazas de phishing

Protegerse contra los ataques de phishing selectivo

Bloquea o aísla fácilmente las amenazas que otras soluciones no detectan

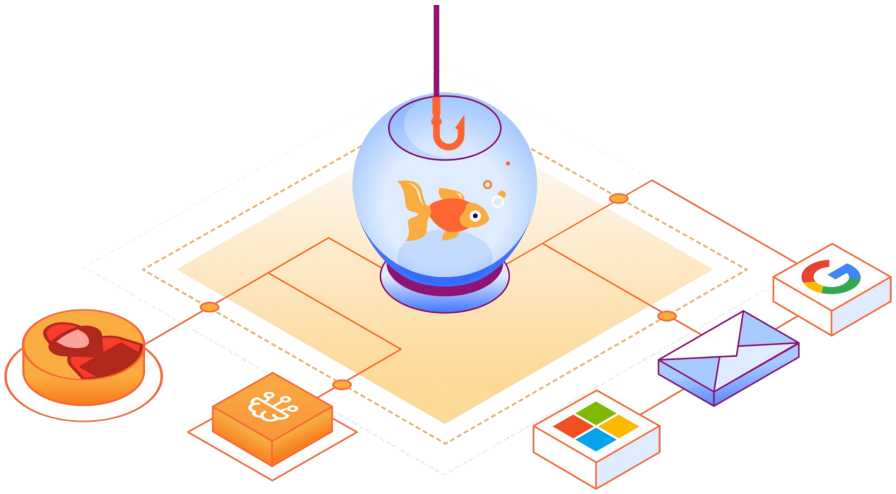
El correo electrónico representa la aplicación empresarial más utilizada y más susceptible a ataques, por lo que es más importante que nunca proteger a los usuarios contra los ataques de phishing que quieren manipular su confianza. A medida que las organizaciones continúan adoptando cada vez más los 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 (denominada Area 1) 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 empiezan con un correo electrónico de phishing[1]

50 000M
en pérdidas como resultado de los ataques BEC 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 entregado mediante enlaces desconocidos o engañosos.

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 continua proliferación de los ataques de phishing, 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 archivado, la prevención de pérdida de datos (DLP) y la encriptación del lado del 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 un alto índice 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.

Aumenta tus controles de seguridad de entrada existentes

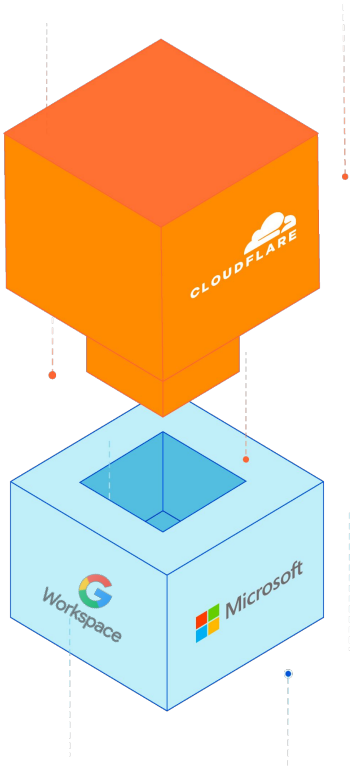
La solución de seguridad del correo electrónico nativa de nube de Cloudflare se puede implementar en cuestión de minutos para mejorar las implementaciones existentes de puerta de enlace de correo electrónico segura o complementar las prestaciones de correo electrónico integradas que proporcionan Microsoft y Google. Con pocos o ningún ajuste necesario, la organización puede conseguir una mayor protección contra el phishing dedicando menos tiempo y esfuerzo a la gestión de la solución de salida.

"Desde que implementamos Cloudflare [sobre M365], hemos observado una reducción del 50 % del número de correos electrónicos maliciosos o sospechosos que nuestros usuarios reciben cada día. Esto libera 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 las horas ahorradas con 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 sofisticados ataques al correo electrónico corporativo

50 000 millones de USD de 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 conversational para hacerse pasar por un empleado o proveedor de confianza.

Extender 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 simplemente el 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 1 billón de solicitudes DNS al día) y los modelos de aprendizaje automático (en constante evolución), deconstruye 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.

Aísla las URL peligrosas y engañosas

Protege a los usuarios contra los enlaces de correo electrónico no fiables

Los ataques de phishing modernos utilizan técnicas de engaño cada vez más perfeccionadas, por lo que incluso las soluciones de seguridad mejor entrenadas tienen dificultades para identificar con precisión los enlaces maliciosos todo el tiempo. Las herramientas para acortar enlaces agravan este problema, ya que permiten los ataques diferidos, donde los enlaces maliciosos se activan después de la entrega. Esto genera:

- **Mayor riesgo** porque se podría hacer clic en enlaces desconocidos.
- **Más interrupciones** porque se podrían bloquear enlaces seguros.
- **Mayores costes** al tener que investigar los enlaces no fiables.

Con el aislamiento adaptable, Cloudflare permite a los usuarios acceder de forma segura a enlaces no fiables neutralizando el malware y otro contenido web malicioso y eliminando la carga de las actualizaciones de políticas y las investigaciones que podrían requerir mucho tiempo.

Evita los ataques de phishing multicanal

El correo electrónico es el principal mecanismo de entrega de enlaces maliciosos. Sin embargo, los atacantes han ampliado sus tácticas más allá del correo electrónico, siendo ahora su objetivo los usuarios del conjunto de aplicaciones que se utilizan para la colaboración diaria. Al ampliar la protección más allá del correo electrónico con la plataforma Zero Trust de Cloudflare, las organizaciones pueden aislar de forma proactiva a los usuarios del contenido web malicioso que llegue a través de:

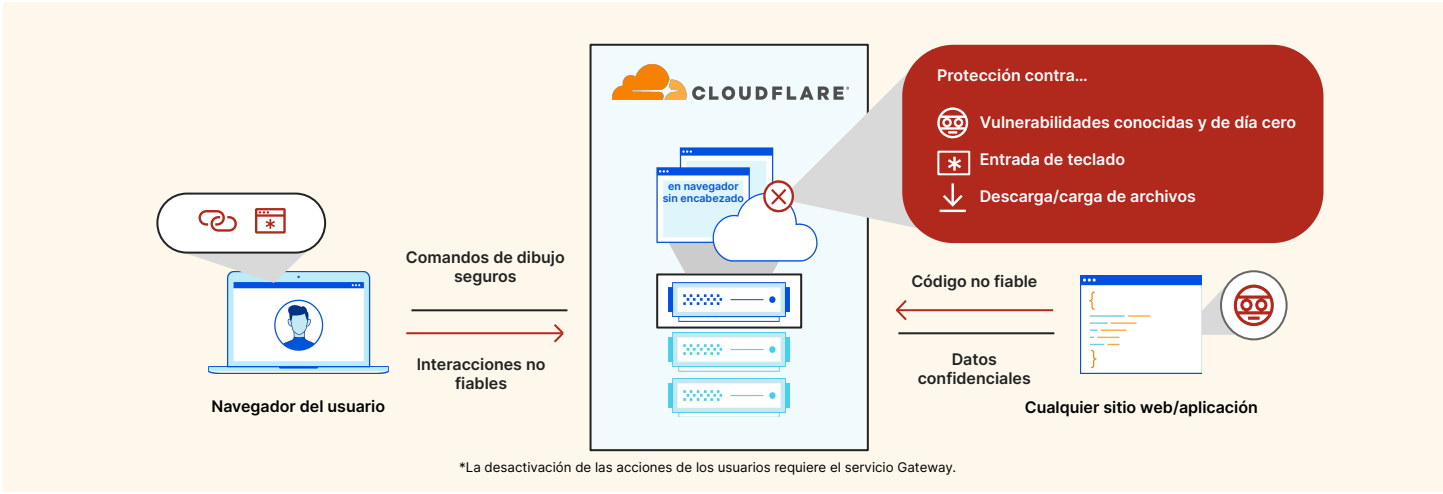


Figura 2: sesión aislada

Reinvención de la seguridad del aislamiento remoto del navegador

El aislamiento de navegador de Cloudflare utiliza nuestra tecnología Network Vector Rendering (NVR) para entregar una solución fluida, segura y escalable para el aislamiento de los enlaces y el contenido web no fiable. NVR transmite comandos de dibujo seguros y ligeros al dispositivo, donde se pueden ejecutar sesiones aisladas del navegador en cualquier servidor, en cualquier centro de datos ubicado en cualquiera de las más de 300 ciudades que abarca la red de Cloudflare. Esto ayuda a eliminar el riesgo de la ejecución de código no fiable en el dispositivo del usuario final, al mismo tiempo que proporciona una experiencia transparente y con baja latencia que es invisible para los usuarios.

Investigación y respuesta rápidas

Gestión de soluciones intuitiva y 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**

Gestión de la detección y la respuesta al phishing

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 y los conocimientos en materia de seguridad 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.

Más de 1100

Horas ahorradas al año 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

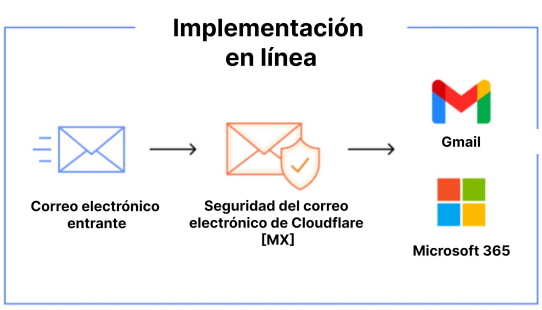
Número total de horas dedicadas en siete años a la configuración de la seguridad del correo electrónico

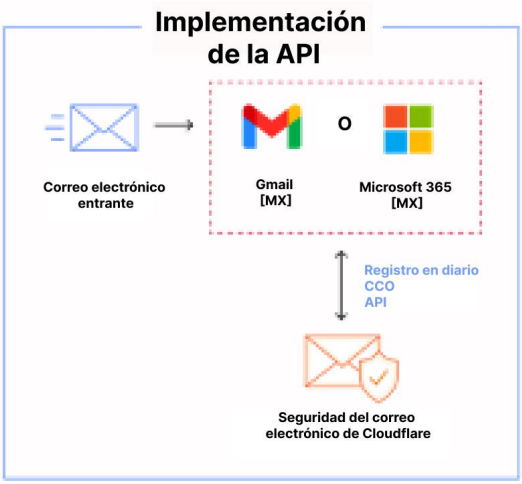
La seguridad del correo electrónico de Cloudflare apenas requiere configuración inicial ni ajustes continuados, y proporciona una gran eficacia de detección lista para su uso.

Protección flexible y de fácil implementación

Tres opciones (en línea, API y modo múltiple) para una implementación rápida y sencilla sin riesgo adicional

La organización puede elegir el método que se adapte mejor a su entorno e implementarlo en cuestión de minutos sin hardware, agentes o dispositivos. A diferencia de los proveedores que solo ofrecen SEG o API, Cloudflare proporciona opciones flexibles que protegen tanto antes como después de la entrega para una resolución continua de las amenazas, al mismo tiempo que se integran perfectamente con los flujos de trabajo de SOC y las plataformas SIEM/SOAR existentes.





FORRESTER

Líder en el informe Forrester Wave™ for **Enterprise Email Security**, 2T 2023

Evalúa y compara

Empieza una evaluación del riesgo de phishing y descubre qué ataques no se están detectando

Evalúa rápidamente tu entorno de correo electrónico y determina qué amenazas de phishing están evadiendo tus defensas actuales. Compara con otros proveedores que no ofrecen ajustes listos para usar para descubrir cómo nuestra solución de seguridad del correo electrónico proporciona la protección más rápida y fácil.

Prueba hoy mismo la protección contra phishing líder del mercado

Solicitar evaluación

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