CLOUDFLARE

RESUMEN DE SOLUCIONES

Protege a tus usuarios del phishing multicanal

Protección en capas que no se limita solo a la bandeja de entrada

DESCRIPCIÓN GENERAL

Los ataques de phishing ya no se limitan al correo electrónico

Si bien el el correo electrónico sigue siendo el mecanismo de distribución más persistente y efectivo para las campañas de phishing, los atacantes utilizan tácticas cada vez más inteligentes para apuntar y explotar a los usuarios en múltiples canales (p. ej., aplicaciones) que se utilizan para las comunicaciones y la colaboración diarias. Estos ataques suelen utilizar de manera inteligente enlaces ofuscados para engañar a los usuarios y redireccionarlos a contenido malicioso y entornos inseguros.

Más canales = más maneras de explotar a los empleados

Apuntar a los empleados con enlaces engañosos en el correo electrónico y en otras aplicaciones de colaboración permite a los atacantes eludir los métodos de detección tradicionales y hacer que los usuarios tengan la percepción de que son auténticos. Esto aumenta el riesgo de que un empleado haga clic en contenido web malicioso, divulgue credenciales o que se filtre información confidencial. La seguridad del correo electrónico solo ayuda cuando el ataque se origina a través de las bandejas de entrada, pero se necesita una solución de seguridad más integral para bloquear estos ataques cuando se propagan a otras aplicaciones.

DESAFÍOS

Las amenazas multicanal pueden eludir el filtrado tradicional de correos electrónicos

Los ataques multicanal aprovechan la ofuscación de enlaces complejos y varias aplicaciones de colaboración para hacer que los usuarios hagan clic en contenido malicioso o filtren información confidencial. Este tipo de ataque puede resultar difícil de abordar debido a lo siguiente:

- **Ofuscación de enlaces** (redirecciones/acortadores de URL)
- **URL basadas en imágenes** (códigos QR)
- **Ataques diferidos** (activados después de la distribución)
- **Interacción distribuida** a través de las aplicaciones de trabajo

89 %

de los encargados de tomar decisiones de seguridad están preocupados por las amenazas de phishing multicanal[1]

N.º 1

Los enlaces maliciosos son la principal amenaza de phishing basado en el volumen de detección [2]

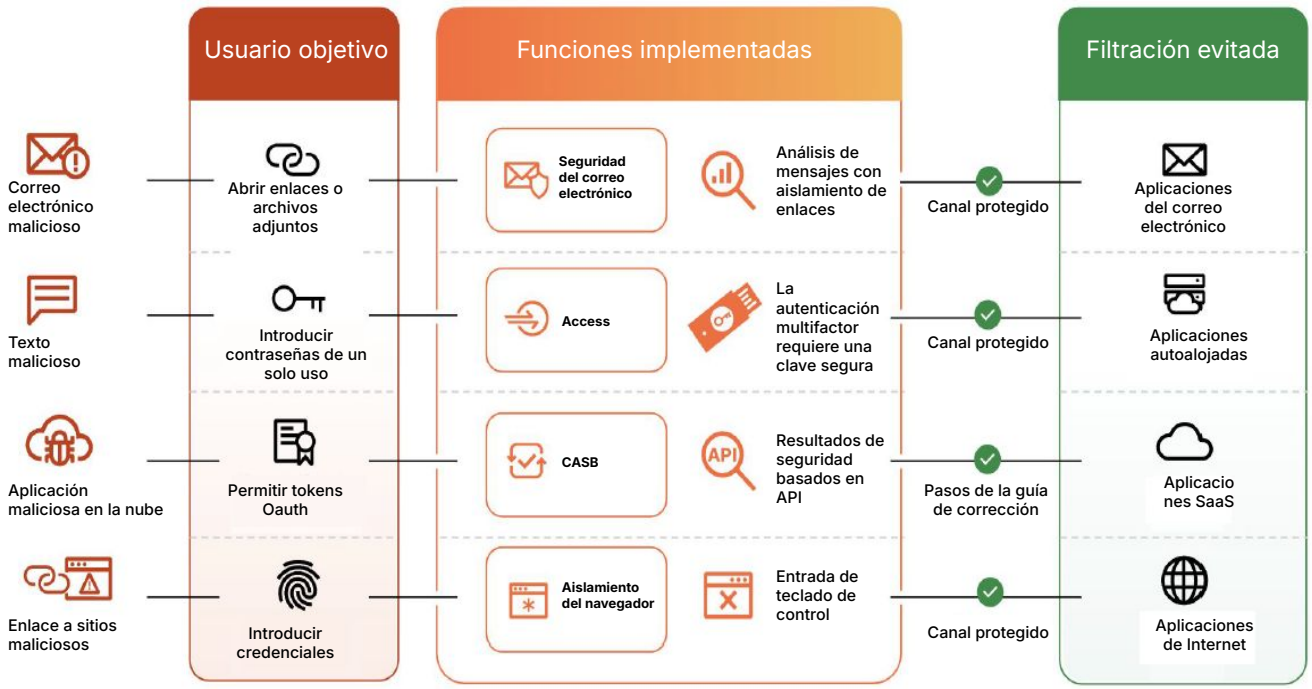
81 %

de las organizaciones han sufrido un ataque multicanal en los últimos 12 meses[1]

SOLUCIÓN

Seguridad unificada en cada punto de exposición al phishing

Para detener los ataques multicanal se necesita una plataforma que aborde la amplia variedad de vulnerabilidades que existen en los flujos de trabajo de los empleados y en las interacciones en las aplicaciones. Por eso, Cloudflare ofrece la solución más completa contra el phishing que se concentra en ofrecer una protección eficaz para empleados y aplicaciones. Con la plataforma Cloudflare One, las organizaciones pueden aprovechar la seguridad de correo electrónico (ES) integrada de manera nativa + los servicios de Zero Trust para implementar la protección en capas para el correo electrónico, las aplicaciones autoalojadas, las aplicaciones SaaS y las aplicaciones de Internet — lo que ofrece una amplia protección para detener pagos fraudulentos y fuga de datos.



Detiene de forma preventiva las amenazas que provienen del correo electrónico

Detecta los ataques al correo electrónico corporativo (BEC), el malware y otras amenazas que se originan en los correos electrónicos con análisis de contenido impulsados por IA/aprendizaje automático para lograr una protección automatizada.

Evita las fugas que generan el robo de credenciales

Evita las fugas con acceso condicional + requisitos de clave segura que actúan como última línea de defensa en caso de que las credenciales sean robadas o vulneradas.

Bloquea y aísla los ataques basados en enlaces

Aísla a los usuarios de los ataques selectivos que engañan a los empleados a través de aplicaciones de mensajería que se utilizan comúnmente a través de enlaces ofuscados de manera inteligente
y que son difíciles de detectar.

Detiene amenazas originadas en el correo electrónico (ES)

El correo electrónico es la aplicación empresarial más utilizada y más susceptible a ataques, por lo tanto, es más importante que nunca proteger a los usuarios contra los ataques de phishing que buscan manipular su confianza a través del correo electrónico. Al aumentar o reemplazar las actuales protecciones de correo electrónico por Cloudflare, las organizaciones pueden mitigar de manera automática sofisticados ataques de phishing que aprovechan enlaces de correos electrónicos integrados, archivos adjuntos y cuentas de suplantación o afectadas para robar información confidencial y cometer fraude financiero.

La solución ligera y nativa en la nube de Cloudflare se puede implementar en cuestión de minutos para mejorar las funciones integradas del correo electrónico que ofrecen Microsoft y Google. Con una mayor automatización y un ajuste mínimo para lograr resultados óptimos, Cloudflare reduce considerablemente el tiempo y el esfuerzo necesarios para la gestión continua.

Compromiso de correo electrónico empresarial (BEC)
El análisis de contenido con IA/aprendizaje automático deconstruye cada mensaje para evaluar el historial de conversación, los patrones de redacción, el sentimiento y otras variables para determinar la autenticidad del remitente.

Archivos adjuntos maliciosos y ransomware
Los modelos de detección de aprendizaje automático de cargas, detecciones sin firma, visión informática, extracción remota y otras formas de análisis se utilizan para identificar cargas malintencionadas cifradas y no cifradas.

Enlaces de correos electrónicos maliciosos
Se combinan técnicas avanzadas para deconstruir e investigar URL complejas con aislamiento adaptable de enlaces para garantizar una experiencia web segura y eficiente para los empleados.

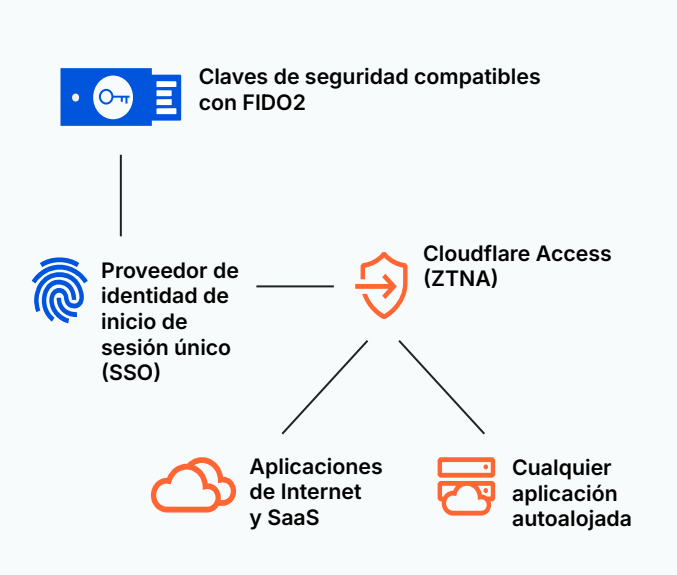
Mitiga los ataques de phishing OAuth (CASB)

El ataque de phishing OAuth aprovecha los proveedores de identidad y los flujos de trabajo legítimos para engañar a los usuarios y hacer que estos otorguen permisos para aplicaciones maliciosas. La plataforma Cloudflare One ofrece la función de detectar estas aplicaciones y brinda orientación para corregir y mitigar rápidamente estas amenazas.

Evita las fugas de credenciales vulneradas (ZTNA)

Si bien muchas organizaciones implementan una gran cantidad de medidas preventivas para evitar que las credenciales de los empleados terminen en las manos equivocadas, la triste realidad es que las medidas preventivas no son 100 % infalibles. En el caso de que las credenciales sean robadas o se filtren accidentalmente, debe haber una última línea de defensa para evitar una fuga general.

Con Cloudflare Access como capa general alrededor de cada recurso, que incluye recursos autoalojados o no web, las organizaciones pueden aplicar sistemáticamente la clave de seguridad compatible con FIDO2 para la autenticación multifactor resistente al phishing. Incluso en el caso de que las credenciales de los empleados se vean vulneradas, las organizaciones aún pueden garantizar que sus datos están protegidos.



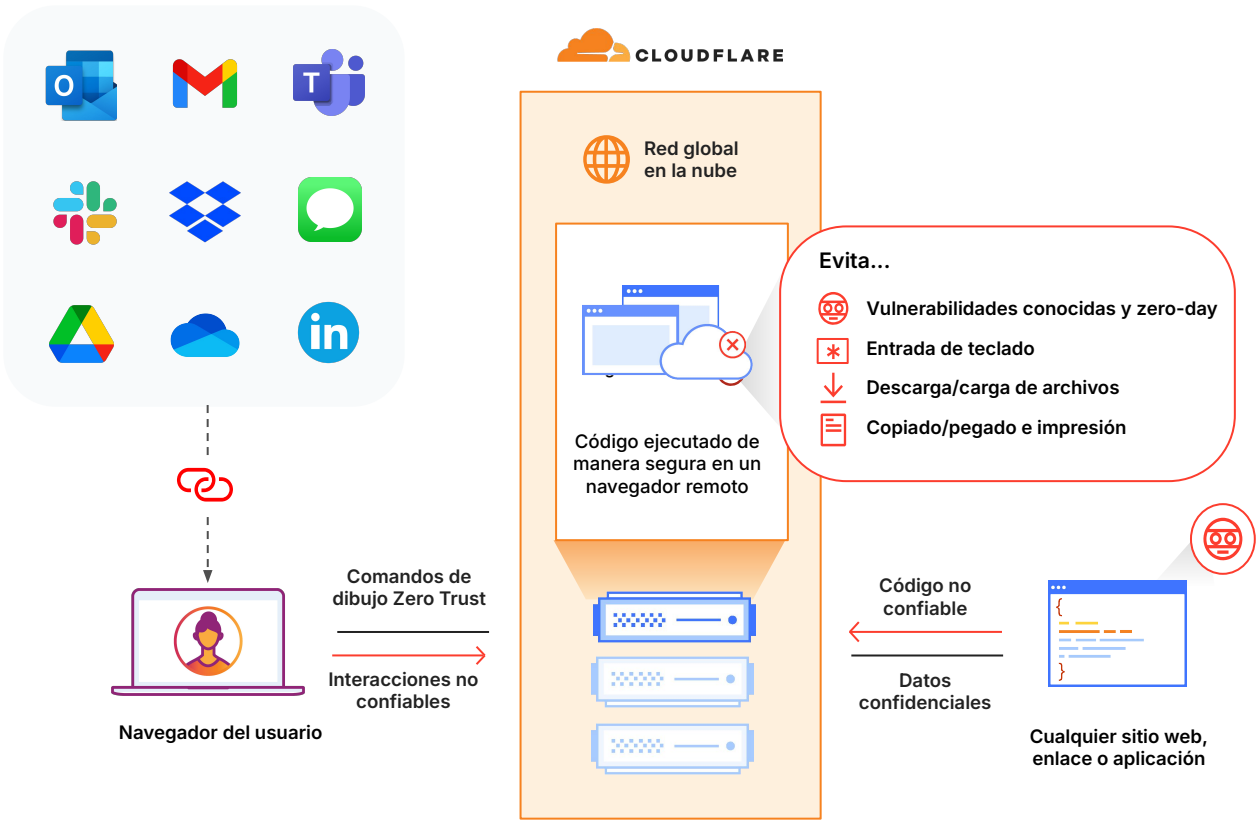
Aislamiento de ataques basados en enlaces (ES + RBI + SWG)

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

El aislamiento del navegador de 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 hacerlo en el dispositivo local del usuario. De esta manera, se mitiga el malware y las vulnerabilidades zero day del navegador, y al mismo tiempo se brinda un control detallado de las acciones del usuario (p. ej. desactivación de las entradas de teclado) para evitar el robo de credenciales y las fugas de datos.

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

La integración de funciones 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 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.



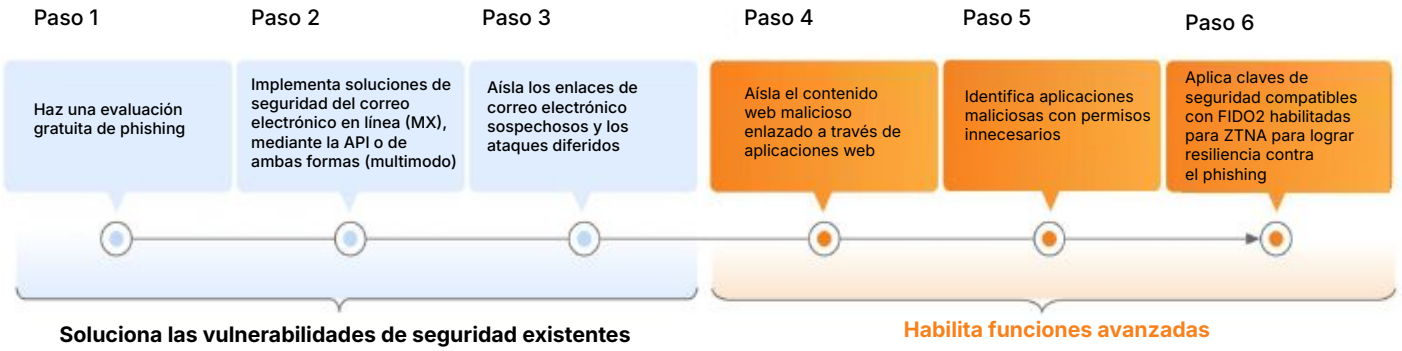
BENEFICIOS

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 brinde de manera rápida y sencilla una protección multicanal completa.

Con la plataforma Cloudflare One, 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 casi sin 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 costo:** Reduce el gasto con una única plataforma totalmente integrada que resuelve todos los casos de uso de phishing.
- **Fácil de implementar y gestionar:** Garantiza una protección inmediata, mientras reduce el tiempo y el esfuerzo necesarios para la gestión continua.



Evalúa y compara

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

Ejecuta un análisis retroactivo gratuito (bandejas de entrada O365) 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 (PRA) para supervisar 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 ofrece la protección más rápida y fácil.

Descubre qué amenazas de phishing están atravesando tu sistema de protección

Ejecutar análisis retroactivo

Solicitar evaluación

CLOUDFLARE

1. 2023 Forrester Opportunity Snapshot: Fuente
2. Informe sobre las amenazas de phishing 2023 Fuente