CLOUDFLARE

RESUMEN DE SOLUCIONES

Protección contra phishing Cloudflare + Microsoft

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

Elimina las puertas de enlace heredadas y actualiza la protección contra el phishing

A principios de la década del 2000, las puertas de enlace de correo electrónico seguro (SEG) comenzaron a tener una mayor necesidad de enrutamiento y filtrado del correo electrónico. Si bien las SEG tuvieron éxito durante varios años, su diseño no les permitió seguir el ritmo del rápido crecimiento de las amenazas de phishing en cuanto al alcance y a la sofisticación.

Una continua actualización de las políticas y los conjuntos de reglas manuales que se crearon originariamente para los servidores locales solo aumenta la cantidad de tiempo y los esfuerzos necesarios para mantener una SEG. Esto ha generado un aumento en los costos y la complejidad y aún no logra evitar las amenazas más peligrosas, como por ejemplo los ataques al correo electrónico corporativo (BEC). El aumento de gastos generales y la reducción de la efectividad se pueden atribuir a lo siguiente:

- **Amenazas zero-day y tácticas de phishing emergentes**: los ataques de phishing modernos utilizan tácticas cada vez más engañosas para evadir filtros estáticos y controles tradicionales. Esto hace que a las SEG les resulte difícil bloquear nuevas amenazas que no presentan indicadores de riesgo conocidos.
- **Implementaciones complejas**: las SEG exigen una configuración minuciosa y un ajuste constante para adaptarse a las nuevas amenazas, y también necesitan varios módulos de complementos para utilizar plenamente sus funciones.
- **Respuestas a incidentes que exigen demasiado tiempo**: cuando las actividades sospechosas o maliciosas omiten los controles implementados de SEG, el proceso de investigación y respuesta puede ser largo y complicado, e implicar un conjunto fragmentado de interfaces y flujos de trabajo.

Implementa una protección altamente eficaz casi sin configuración

A medida que las organizaciones siguen adoptando Microsoft 365 para mejorar la comunicación y la colaboración para su fuerza de trabajo híbrida, es fundamental aprovechar las funciones de seguridad nativas de Microsoft e integrar soluciones complementarias basadas en el aprendizaje automático para bloquear y aislar de manera automática las amenazas más peligrosas. Esta estrategia no solo reduce de manera significativa el riesgo de phishing, sino que también simplifica los flujos de trabajo, lo que minimiza el tiempo y el esfuerzo necesarios para gestionar la seguridad.

91 %

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

Principal

vector de ataque para cometer fraude y obtener acceso[2]

$50 MM

en pérdidas como resultado de los ataques BEC en la última década[3]

$4,88 M

representa el costo promedio de una fuga de datos en 2024[4]

1. 2020 Deloitte research
2. Microsoft SIR Report
3. 2023 FBI IC3 PSA
4. 2024 IBM Cost of a Data Breach

Funciones de seguridad de correo electrónico de Microsoft

Eliminar la superposición de SEG para reducir riesgos y costos

Los analistas afirman que la consolidación de las funciones para minimizar la superposición de funcionalidades está ayudando a las organizaciones a reducir los costos y la complejidad. Sin embargo, también aconsejan a las organizaciones evaluar con cuidado las funciones nativas para garantizar que satisfacen todos los casos de uso.

A medida que Microsoft sigue integrando sus funciones de seguridad esenciales, la creciente superposición con las SEG ha brindado a las organizaciones la oportunidad de optimizar las operaciones de seguridad al aprovechar las funciones ya incluidas en su licencia E3 o E5. Este cambio permite a las organizaciones eliminar las costosas y complejas implementaciones de SEG, destinando una parte del presupuesto a la integración de soluciones ligeras que abordan de manera efectiva las amenazas de phishing más peligrosas.

La seguridad del correo electrónico de Cloudflare brinda una solución integrada y casi sin configuración que optimiza los análisis de amenazas con aprendizaje automático de Microsoft 365 para automatizar la detección de BEC y ataques multicanal.

Áreas que se superponen con la funcionalidad de SEG:

- **Depuración de correo electrónico**
  Políticas basadas en reglas para el correo no deseado y los correos masivos, con detección de firmas para malware desconocido.
- **Protección de archivos adjuntos y URL**
  Reescritura básica para todos los enlaces de correo electrónico y funciones de aislamiento para archivos adjuntos.
- **Investigación y detección de amenazas**
  Búsqueda de correos electrónicos, investigación y correlación de incidentes, detección y corrección.
- **Protección de información**
  Políticas de cifrado, archivado y DLP para correos electrónicos, archivos y puntos finales.
- **Información y capacitación**
  Simulaciones de ataques de phishing y entrenamiento para usuarios finales.

Exchange Online Protection

Se incluye en cada plan y ofrece la depuración de correo electrónico esencial para filtrar correos masivos, correos no deseados y malware.

- Protección contra correo electrónico no deseado
- Protección de malware basada en firmas

Microsoft Purview (DLP)

Reglas y aplicación de reglas para evitar la pérdida de datos configurables. Integrado con Microsoft Information Protection.

- DLP para correos electrónicos y archivos
- DLP para Teams
- DLP para puntos finales

Defender for O365 Plan 1

Controles de seguridad adicionales para una protección básica contra enlaces y archivos adjuntos maliciosos.

- Enlaces seguros (reescritura de URL)
- Archivos adjuntos seguros (espacios aislados)
- Protección interna de correo electrónico

Defender for O365 Plan 2

Incluye todo lo del Plan 1 y funciones para detectar amenazas, investigación, capacitación y respuesta.

- Detección de amenazas
- Correlación de incidentes entre dominios
- Entrenamiento de simulación de ciberataques

Licencia E3

Licencia E3 + cumplimiento normativo

Licencia E3 + cumplimiento normativo + seguridad

Licencia E5

● Completa ● Limitada ○ Ninguna

	SEG	M365	Cloudflare
Prevención de amenazas			
Permitir/Bloquear listas	●	●	●
Remitente malicioso reconocido	●	●	●
URL/archivo adjunto malicioso reconocidos	●	●	●
Filtrado de correos no deseados/masivos	●	●	●
Aprendizaje automático (análisis de contenido)	●	○	●
Malware/Ransomware Zero-Day	●	●	●
Enlaces maliciosos	●	●	●
Reescritura de URL (análisis en el momento del clic)	●	●	●
Aislamiento adaptable de enlaces	○	○	●
Compromiso de correo electrónico empresarial (BEC)	●	●	●
Suplantación de identidad de empleado	●	●	●
Suplantación de identidad de proveedor	●	●	●
Afectación de empleado (ATO)	●	●	●
Afectación de proveedor	●	●	●
DMARC Management	●	●	●
Detección de aplicaciones maliciosas (OAuth Phish)	●	●	●
Seguridad de contenido web	●	●	●
Información y capacitación de seguridad	●	●	●
Respuesta a amenazas			
Interfaz única e intuitiva	○	●	●
Clasificación automatizada de amenazas	○	●	●
Búsqueda e investigación rápidas	●	●	●
Retracción automática	●	●	●
Informes on demand	●	●	●
Detección y servicio de respuesta gestionados	●	○	●
Protección de datos			
Cifrado	●	●	○
Archivado	●	●	○
DLP para correos electrónicos	●	●	●
DLP para nubes (aplicaciones de colaboración)	●	●	●
DLP para redes	●	●	●

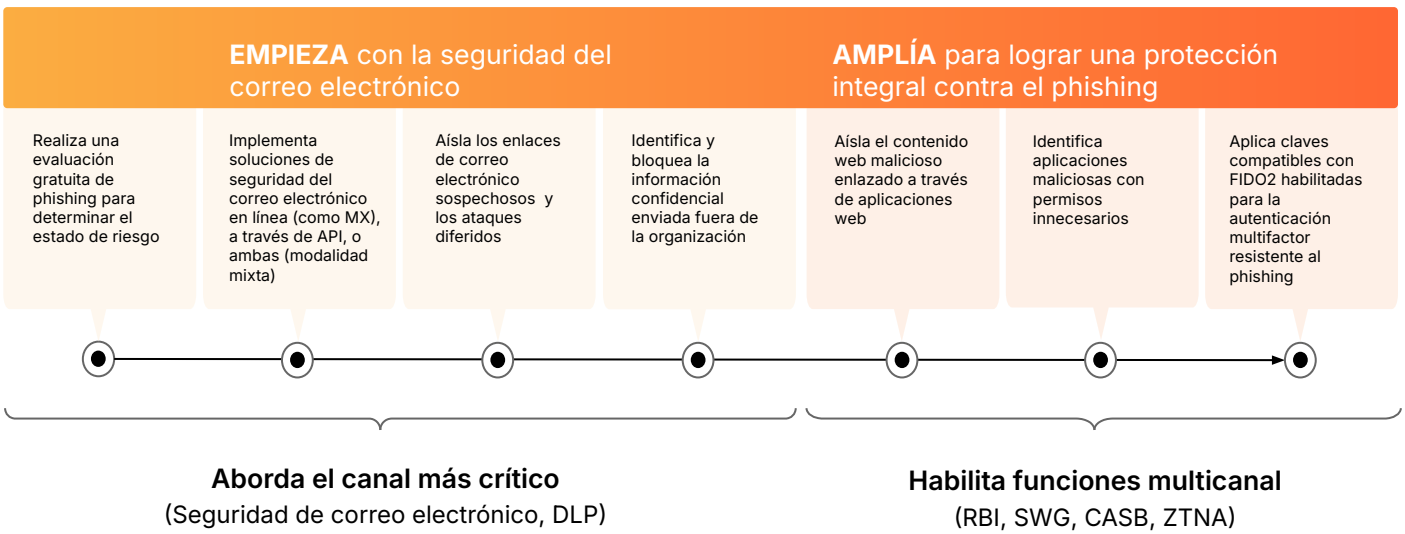
BENEFICIOS

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 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 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 reduces 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 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 supervisar las bandejas de entrada en busca de phishing. Compara con otros proveedores que no ofrecen ajustes listos para usar para descubrir cómo nuestra solución de seguridad del correo electrónico brinda la protección más rápida y fácil.

Ejecutar análisis retroactivo

Solicitar evaluación

