CLOUDFLARE
AREA 1 SECURITY

RESUMEN DE SOLUCIÓN

Mejora las defensas del correo electrónico de Microsoft 365 con Cloudflare Area 1

Amplía Zero Trust a tu herramienta de comunicación más importante, el correo electrónico en la nube

Protege las bandejas de entrada de Microsoft de las amenazas con una solución de seguridad del correo electrónico preventiva y nativa de la nube

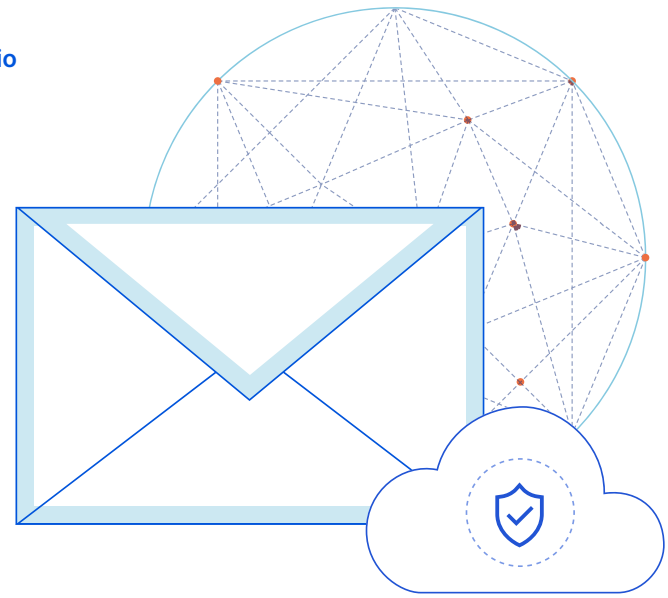
Microsoft 365 proporciona excelente protección contra amenazas de alto volumen de datos, como el correo no deseado y los virus, así como protección adicional para los clientes de Microsoft Advanced Threat Protection (ATP).

Aun así, Gartner® indica que[1], "Con la mejora de la seguridad integrada... los ciberdelincuentes son también cada vez más sofisticados, y a menudo utilizan páginas de inicio de sesión falsas para recopilar credenciales de inicio de sesión. Estas sofisticadas amenazas de correo electrónico incluyen, entre otros, los sitios web en riesgo y los documentos que se utilizan como arma para implementar malware. Muchas bandas de ransomware como servicio utilizan el correo electrónico como el punto de entrada inicial. Además del malware, las amenazas de ataque al correo electrónico corporativo (BEC) y de apropiación de cuenta continúan al alza, con las consiguientes considerables pérdidas financieras".

Las sofisticas amenazas de bajo volumen como las indicadas anteriormente se crean primero con una infraestructura y técnicas de ataque que Cloudflare Area 1 está especialmente capacitada para descubrir en circulación. Mediante la identificación y el bloqueo automático de las campañas en una etapa temprana del ciclo de vida del ataque (de media, 24 días antes del inicio), Area 1 protege las bandejas de entrada de las amenazas.

Como parte de la plataforma Cloudflare Zero Trust, el servicio de seguridad del correo electrónico de Area 1 también:

- **Expone el fraude financiero sin malware**, que a menudo se lleva a cabo en varias conversaciones de correo electrónico con proveedores "de confianza".
- **Bloquea ataques desconocidos en tiempo real**, sin necesidad de "ajustar" una SEG o de esperar actualizaciones de firma/política.
- **Descubre cuentas y dominios en riesgo**, así como dominios nuevos, parecidos y de proximidad que los atacantes utilicen para omitir DMARC/SPF/DKIM.
- **Aisla y bloquea ataques combinados y diferidos** con la integración con Aislamiento del navegador de Cloudflare (beta).



Información general de la solución

En un entorno que prioriza la nube, las puertas de enlace de correo electrónico seguras (SEG) son inflexibles e ineficaces contra las amenazas en continua evolución, como los ataques al correo electrónico empresarial, la suplantación y el ransomware.

Cloudflare Area 1 proporciona seguridad del correo electrónico preventiva y nativa de la nube para detener completamente estos y otros ataques de phishing selectivo.

Las organizaciones que combinan Microsoft 365 con Cloudflare Area 1 obtienen:

- **Protección integral contra phishing** en el correo electrónico interno y externo, la web y el tráfico de red
- **Menor complejidad del entorno informático** y menor tiempo de respuesta a incidentes de phishing
- **Implementación simple en pocos minutos** con un enfoque que prioriza la API
- **Investigaciones más rápidas del centro de operaciones de seguridad** con retracciones de mensajes posteriores a la entrega e integraciones con plataformas SIEM/SOAR

¿Cómo puedes bloquear más amenazas con el enfoque a la seguridad del correo electrónico en la nube de Area 1?

Microsoft 365 proporciona una seguridad excelente para las amenazas del correo electrónico de alto volumen; sin embargo, los ataques de phishing de bajo volumen y muy selectivos, responsables de más del 90 % de las filtraciones de ciberseguridad, siguen sin ser detectados.

¿Cómo deberían las organizaciones que utilizan Microsoft 365 y aún se enfrentan a phishing no detectado gestionar las amenazas modernas?

Aquí es donde entran en juego las soluciones de **seguridad integrada del correo electrónico en la nube** (ICES). Según Gartner®, "Las soluciones que se integran directamente en el correo electrónico en la nube mediante una API, y no mediante una puerta de enlace, facilitan la evaluación y la implementación y mejoran la precisión de la detección, al mismo tiempo que también se benefician de la integración de la mayor parte de la protección contra phishing con la plataforma principal".[2]

"En 2023, al menos un 40 % de todas las organizaciones utilizarán funciones de protección integradas de proveedores de correo electrónico en la nube en lugar de una puerta de enlace de correo electrónico segura (SEG), en contraposición a un 27 % en 2020".

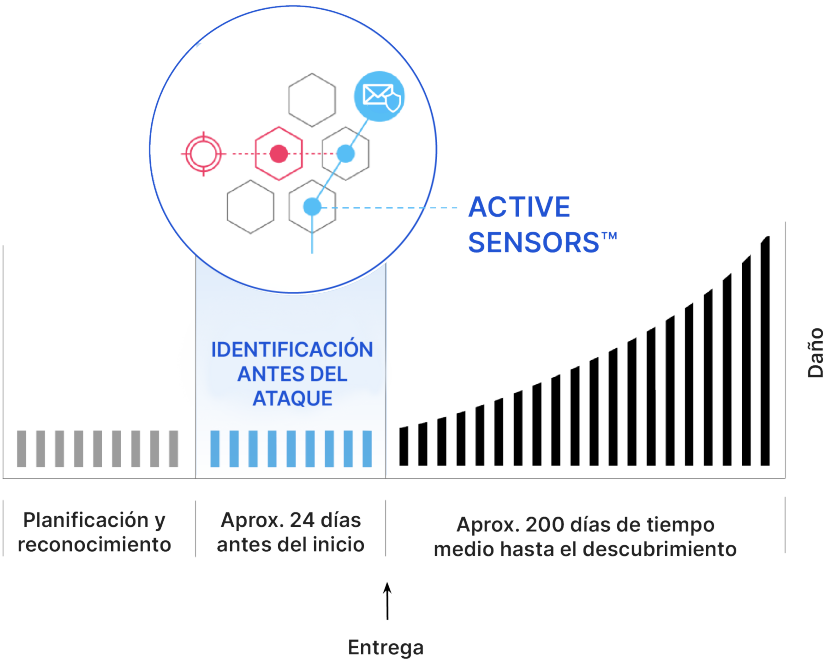
"En 2025, el 20 % de las soluciones contra phishing se proporcionarán mediante la integración de la API con la plataforma de correo electrónico, mientras que hoy estas representan menos de 5 %".

— 2021 Gartner® Market Guide for Email Security

Area 1 Horizon (ahora seguridad del correo electrónico de Cloudflare Area 1) es un proveedor representativo en la categoría de seguridad integrada del correo electrónico en la nube (ICES) en el informe Gartner Market Guide.

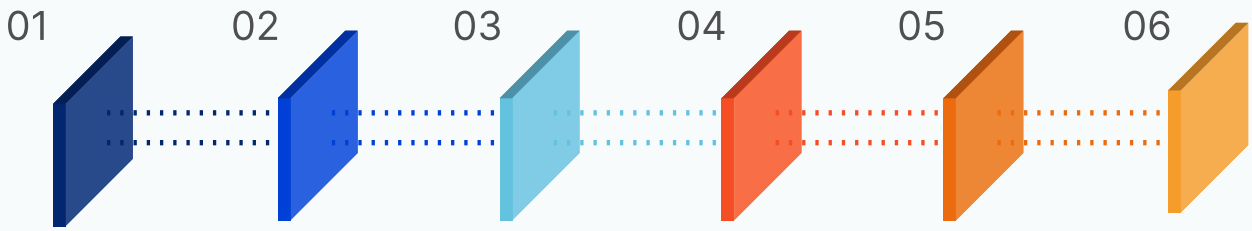
A diferencia de otras soluciones, la solución Area 1 **rastrea la web de manera continua y proactiva** en busca de nuevas campañas de phishing e infraestructuras de atacantes en el entorno. De media, Area 1 detecta preventivamente las cargas útiles y los sitios maliciosos 24 días antes del inicio del ataque.

Figura 1: Detén preventivamente ataques de phishing, antes de que lleguen a tu bandeja de entrada, con Cloudflare Area 1



Area 1 utiliza también una gran variedad de **técnicas de detención más avanzadas**, como NLU, NLP, análisis de gráficos sociales (patrones de comunicación por correo electrónico) y reconocimiento de imágenes, para detectar y detener los ataques más sofisticados, incluidas amenazas completamente nuevas y muy específicas que amenazan a los usuarios individualmente, en contraposición a las que amenazan a muchos usuarios.

Figura 2: Analiza el contenido, el contexto y los gráficos sociales de las comunicaciones por correo electrónico para detener las amenazas modernas como BEC



Análisis estructural
Encabezados, cuerpo, imágenes, enlaces de visión artificial, carga útil

Modelado NLU (Comprensión del lenguaje natural)
Patrones de escritura
Categorías
Expresiones

Análisis de opiniones
Intención, tono, relación, jerarquía

Análisis de cadenas
Conversaciones
Variaciones
Duración

Modelado del sector
Verticales
Lengua franca
Procesos comerciales

Confianza Gráficos
Gráficos sociales de socios, historial de envíos, detección de ATO (apropiación de cuentas), suplantación de socios

Implementaciones simples en pocos minutos

Con un enfoque que prioriza la API y que se integra perfectamente con Microsoft 365, la implementación de Area 1 requiere apenas unos minutos. Detecta y bloquea el phishing con más precisión y eficacia, sin la complejidad del entorno informático necesaria para "ajustar" constantemente una SEG tradicional ineficaz.

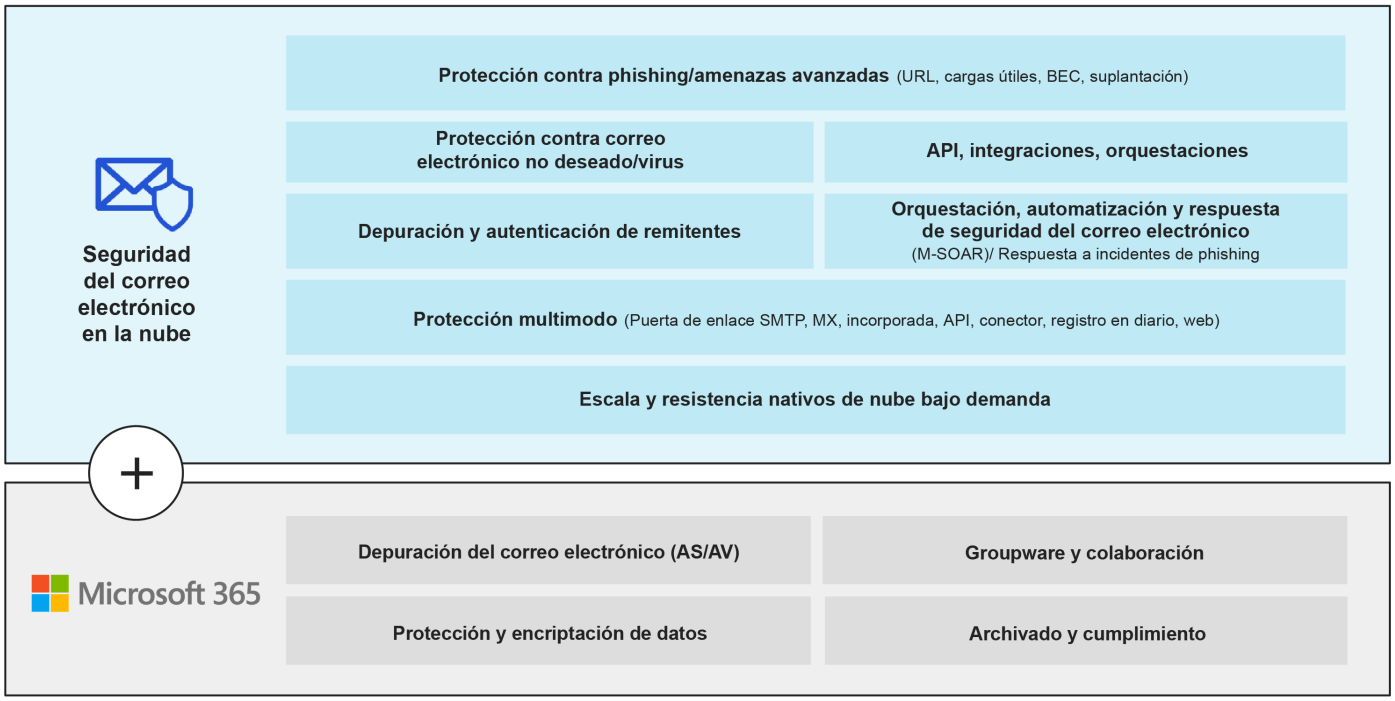
Figura 3: Ejemplo de opción de implementación de la seguridad del correo electrónico de Area 1

Area 1:

- Se puede implementar en menos de 5 minutos, sin necesidad de instalación y sin que afecte a la infraestructura existente;
- Proporciona opciones de implementación más flexibles (incluidos MX/incorporado, conector y API) en comparación con otras soluciones;
- Se integra perfectamente con otras funciones de seguridad del correo electrónico de Microsoft 365 como la protección contra correo no deseado, DLP, encriptación y archivado;
- Puede eliminar con facilidad todos los mensajes maliciosos directamente desde las bandejas de entrada de Microsoft 365 con las funciones integradas de corrección y retracción de mensajes; y
- Es totalmente transparente para los usuarios finales, al mismo tiempo que proporciona detección y corrección de phishing integrales y de un extremo a otro.

Las ventajas de proteger los entornos de correo electrónico de Microsoft 365 con Cloudflare Area 1 incluyen:		
La mejor seguridad del correo electrónico en la nube	**Flujos de trabajo fluidos**	**Mayor eficiencia operativa**
• Amplía las defensas nativas de Microsoft para una protección integral contra las amenazas modernas que incluyen, entre otras, BEC, ataques de correo electrónico en la cadena de suministro, cuentas de proveedor en riesgo y amenazas internas. • Mayor visibilidad de las amenazas y mejora del análisis forense de las investigaciones y los tiempos de respuesta.	• Amplia integración con los entornos, las API y los flujos de trabajo de Microsoft. • Integra con ADFS, envía alertas a Teams y reenvía registros a Azure Sentinel. • Los usuarios finales permanecen en los paneles de control nativos de Microsoft para lograr una productividad continuada y evitar las distracciones.	• Basado en una infraestructura nativa de la nube y dinámicamente escalable para gestionar los picos de tráfico en la nube. • Reemplaza las SEG tradicionales para más seguridad y eficiencia operativa. • Detección avanzada, evaluación y respuesta en una única plataforma para una protección integral.

Protege tus bandejas de entrada de las amenazas con seguridad integrada del correo electrónico en la nube:



Microsoft + Cloudflare: para una nube más segura y privada

Cloudflare ha creado amplias integraciones con Microsoft para ayudar a las organizaciones a ir aún más lejos en su recorrido Zero Trust. Estas integraciones ayudan a las organizaciones a crear implementaciones para los clientes operativamente eficaces al mismo tiempo que proporcionan una experiencia de usuario inmejorable y operaciones a escala.

Además de Area 1, las integraciones de los servicios Cloudflare Zero Trust incluyen:

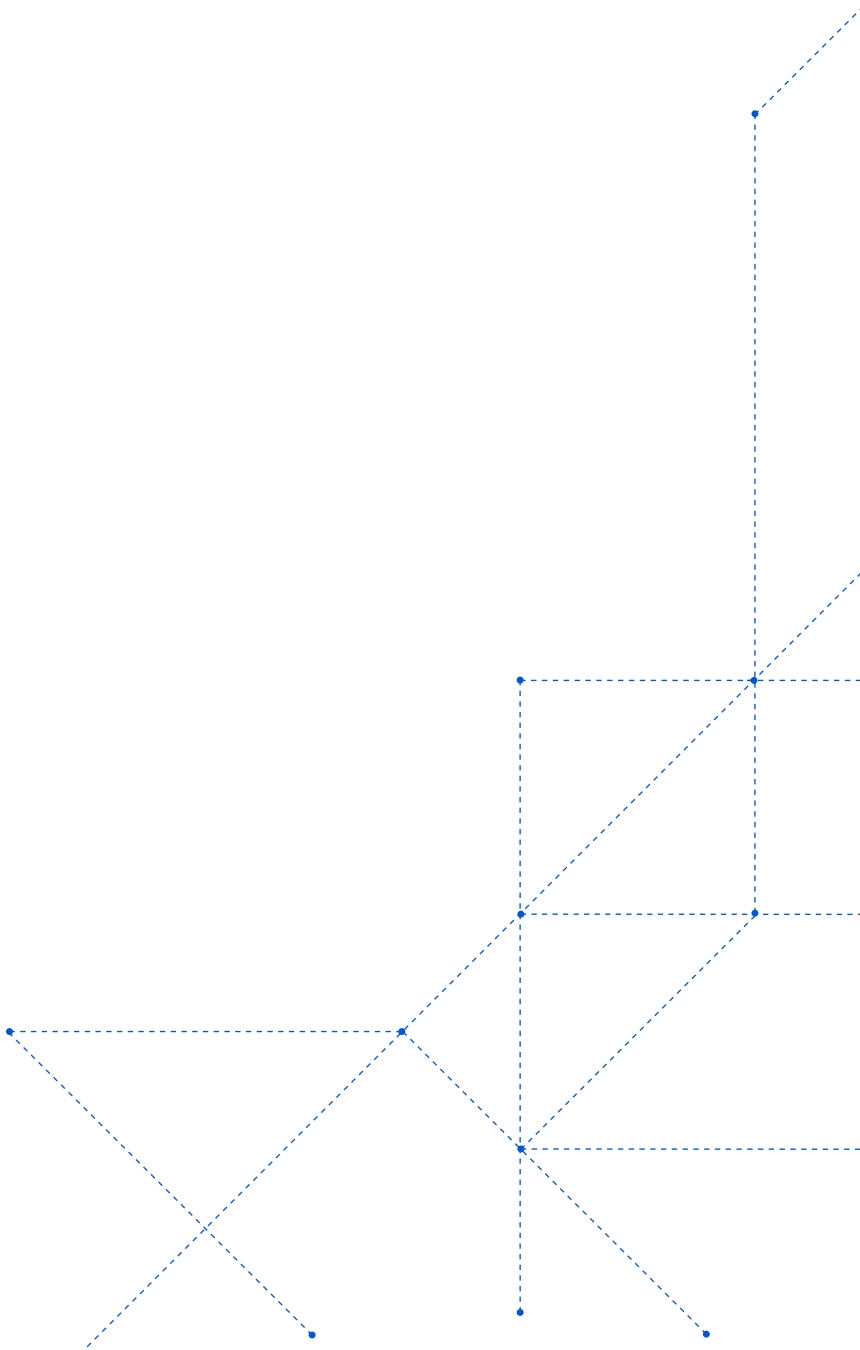
- **Azure Active Directory (AD)**: aprovecha potentes herramientas de autenticación, que incluyen, entre otras, la autenticación multifactor (MFA), políticas de acceso condicional y controles basados en riesgo.
- **Microsoft Cloud App Security (MCAS)**: inicia la integración de M365 para explorar nuevos problemas de seguridad relacionados con los usuarios, datos y servicios en la aplicación de M365 y presentarlos a los clientes.
- **Zero Trust for Azure Apps**: posibilita un acceso seguro a las aplicaciones locales o a las aplicaciones alojadas en Azure, sin necesidad de VPN.
- **Microsoft Endpoint Manager**: evalúa la postura del cliente en el momento del inicio de sesión mediante Microsoft Intune, para que Cloudflare pueda permitir o denegar el acceso según las señales de la postura de seguridad o del dispositivo.
- **Microsoft 365**: proporciona una experiencia de usuario más rápida y segura optimizando la conectividad del usuario a Microsoft 365 mediante Cloudflare y el programa para partners de redes de Microsoft.

Para obtener más información sobre las integraciones de socios de Cloudflare con Microsoft, ponte en contacto con nosotros.

Para ver cómo Cloudflare Area 1 puede mejorar tu protección contra phishing de Microsoft 365, solicita aquí una evaluación personalizada del riesgo.

Referencias

1 y 2 Gartner, "Market Guide for Email Security", 7 de octubre de 2021, Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer



CLOUDFLARE
AREA 1 SECURITY

+34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/

REV:BDES-3778/07SEPT2022