

AI RECIPIENT VALIDATION

PROTECCIÓN AUTOMATIZADA DE CORREO ELECTRÓNICO ERRÓNEO PARA MICROSOFT 365

Key Facts:



SELECCIONA SIEMPRE LOS DESTINATARIOS ADECUADOS



PREVEN LAS BRECHAS DE SEGURIDAD DEL CORREO ELECTRÓNICO



EVITA LA PÉRDIDA DE DATOS

¿Por qué necesito AI Recipient Validation?

En algunos sectores críticos, como finanzas, sanidad o servicios públicos, los errores humanos, como los emails mal dirigidos, se encuentran entre las causas más comunes de las brechas de seguridad.*

Las filtraciones de datos causadas por correos electrónicos mal dirigidos pueden ser costosas para las empresas en términos financieros y también suponer una pérdida de reputación y confianza.

Las normativas, incluido el RGPD en Europa, han mostrado su vertiente más exigente cuando se trata de proteger datos sensibles. Como resultado, las empresas no solo necesitan una solución fiable que reduzca las amenazas del correo electrónico causadas por errores humanos, sino que también garantice que una organización pueda cumplir los requisitos normativos.

AI Recipient Validation de Hornetsecurity protege a los usuarios del correo electrónico ayudándoles a seleccionar siempre los destinatarios correctos. Ofrece a los responsables de seguridad y cumplimiento una visibilidad real de cómo sus empleados gestionan y responden los correos electrónicos para prevenir los emails mal dirigidos.

*2023 Data Breach Investigations Report, Un análisis de 16.312 incidentes y 5.199 violaciones de datos confirmadas <https://www.verizon.com/business/resources/reports/dbir/>

AI Recipient Validation es un servicio de autoaprendizaje basado en IA que analiza continuamente los patrones de comunicación por correo electrónico de un usuario en segundo plano. Detecta automáticamente destinatarios potencialmente no deseados, advierte sobre correos electrónicos que contienen datos confidenciales, como información de identificación personal, o redacción inapropiada, y tiene en cuenta el comportamiento y las respuestas del usuario para ajustar automáticamente las alertas y sugerencias emitidas en siguientes comunicaciones.

AI Recipient Validation advierte a los usuarios cuando intentan enviar correos electrónicos en los siguientes casos:

Validación de destinatarios

- Enviar un correo electrónico a destinatarios potencialmente no deseados.
- Falta un destinatario habitual de ese tipo de mensajes.
- Se añade o sustituye un usuario habitual.
- Enviar correos electrónicos a usuarios de diferentes organizaciones o direcciones de correo electrónico personales por primera vez.
- Responder a una gran lista de distribución.
- Envío de un correo electrónico a un destinatario con el que el usuario no tiene ninguna relación previa.
- Sugerir un usuario en función del contexto del correo electrónico.

Controles complementarios

- Envío de un email con información sensible, como datos personales o financieros.
- Envío de un correo electrónico con una redacción inapropiada.



El motor de IA de autoaprendizaje ajusta las instancias de advertencia en función del comportamiento del usuario.

OBTENER UNA VISIÓN CLARA DE LAS INFRACCIONES COMETIDAS POR LOS USUARIOS

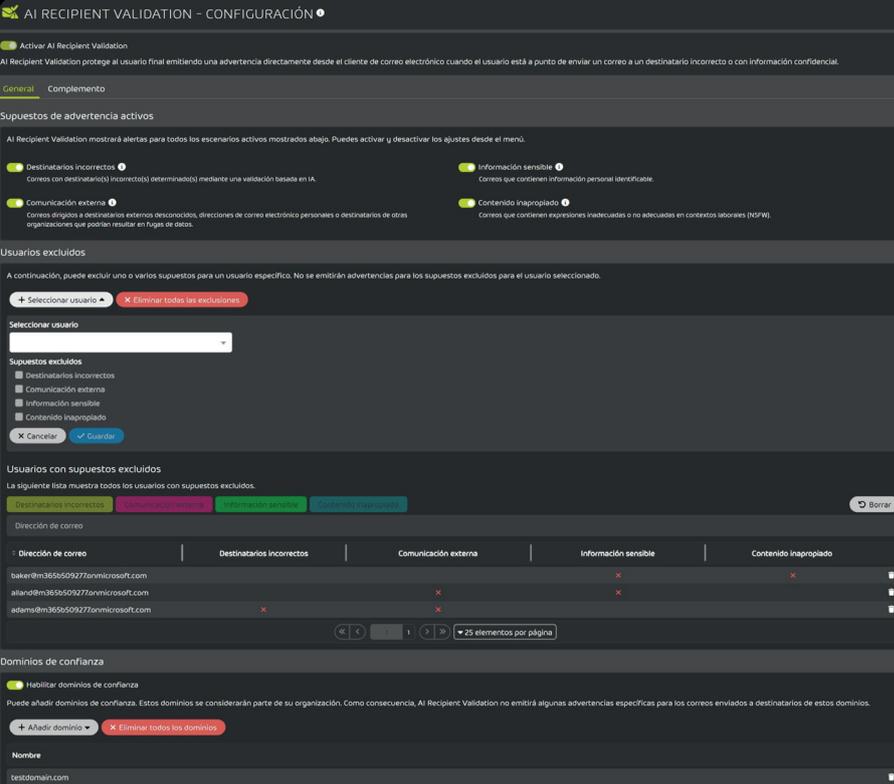
El panel de AI Recipient Validation proporciona a los administradores una visión general de los distintos casos de alertas a los que están expuestos los usuarios. Esto les permite tomar medidas adicionales, como concienciar a los empleados sobre la privacidad de los datos en las comunicaciones por correo electrónico.



CONFIGURAR EL COMPLEMENTO PARA ADAPTARLO A LAS NECESIDADES DE LA EMPRESA

Los administradores pueden configurar AI Recipient Validation para adaptarlo a las necesidades de su empresa, garantizando que las alertas se activen de forma eficaz y productiva:

- Deshabilitando escenarios de advertencia específicos para que no se activen alertas.
- Excluyendo usuarios de escenarios de advertencia específicos.
- Habilitando dominios de confianza para que los dominios externos se traten como internos.



Supuestos de advertencia activos

- Destinatarios incorrectos: Correos con destinatario(s) incorrecto(s) determinado(s) mediante una validación basada en IA.
- Información sensible: Correos que contienen información personal identificable.
- Comunicación externa: Correos dirigidos a destinatarios externos desconocidos, direcciones de correo electrónico personales o destinatarios de otras organizaciones que podrían resultar en fugas de datos.
- Contenido inapropiado: Correos que contienen expresiones inadecuadas o no adecuadas en contextos laborales (NSFW).

Usuarios excluidos

Seleccionar usuario: [Campo de búsqueda]

Supuestos excluidos

- Destinatarios incorrectos
- Comunicación externa
- Información sensible
- Contenido inapropiado

Usuarios con supuestos excluidos

Dirección de correo	Destinatarios incorrectos	Comunicación externa	Información sensible	Contenido inapropiado
baker@m365509277onmicrosoft.com				
alland@m365509277onmicrosoft.com				
adams@m365509277onmicrosoft.com				

Dominios de confianza

Habilitar dominios de confianza

Nombre: testdomin.com

CONFIGURACIÓN RÁPIDA Y SENCILLA CON UNA EXPERIENCIA DE USUARIO AMIGABLE

Nuestro asistente de onboarding hará la instalación en un abrir y cerrar de ojos. Benefíciate al instante de un control adicional que notifica de forma autónoma la posibilidad de una comunicación mal dirigida y protege contra posibles fugas de datos.

AI Recipient Validation se integra a la perfección con la infraestructura de Microsoft 365, sin necesidad de cambiar las configuraciones existentes ni los registros MX. AI Recipient Validation está disponible para los usuarios de Microsoft 365 en las últimas versiones de su cliente de correo Outlook para Windows, Mac y Web.