

2025-07-21



HORNETSECURITY

ADVANCED THREAT PROTECTION:
MANUAL PARA PARTNERS

www.hornetsecurity.com

THE CLOUD SECURITY PIONEER

Contents

Convenciones lingüísticas y símbolos en la documentación.....	3
Estructura y funcionamiento de ATP.....	5
Descripción de los motores de ATP.....	7
Notificaciones en tiempo real.....	11
Ex Post Alert.....	12
Ex Post Deletion.....	12
Configuración por defecto.....	14
Activar ATP.....	14
Añadir destinatarios de notificaciones.....	15
Eliminar destinatarios de notificaciones.....	17
Activar Secure Links.....	18
Dominios de Secure Links.....	20
Permitir los dominios de Secure Links en Microsoft Defender.....	20
Permitir los dominios de Secure Links enviándolos a Microsoft.....	26
Descodificador de enlaces.....	29
Descodificar enlaces de Secure Links.....	30
Activar Targeted Fraud Forensics Filter.....	31
Añadir un grupo a la lista de grupos de TFFF.....	32
Retirar un grupo de la lista de grupos de TFFF.....	34
Activar Ex Post Deletion.....	34
Escaneo ATP.....	38
Iniciar el escaneo ATP.....	38
Informe ATP.....	41
Índice.....	44



Convenciones lingüísticas y símbolos en la documentación

Aclaración sobre el género empleado

Para mejorar la legibilidad, en esta documentación se emplea el masculino genérico. Cabe señalar aquí que el uso exclusivo de la forma masculina debe entenderse como independiente del género.

Símbolos utilizados

Los siguientes símbolos se utilizan para identificar mejor los pasos relevantes dentro de los capítulos dedicados a instrucciones:

SÍMBOLO	DESCRIPCIÓN	EXPLICACIÓN
	Requisito	Condición que debe cumplirse antes del siguiente paso.
	Resultado intermedio	Resultado alcanzado provisionalmente tras un paso concreto.
	Resultado final	Resultado alcanzado una vez finalizada la secuencia de pasos de un capítulo de instrucciones.

Advertencias e indicaciones de seguridad

Las advertencias e indicaciones de seguridad se emplean para informar al usuario sobre riesgos residuales y peligros, así como sobre el procedimiento a emplear para evitarlos. En esta documentación se emplean las siguientes advertencias e indicaciones de seguridad:

SÍMBOLO	DESCRIPCIÓN	EXPLICACIÓN
	NOTA	Información adicional dentro de determinado párrafo, relevante para la realización de pasos posteriores.
	CONSEJO	Indicación sobre opciones de configuración.



SÍMBOLO	DESCRIPCIÓN	EXPLICACIÓN
	IMPORTANTE	Advertencias con información sobre limitaciones u opciones de configuración importantes del servicio.
	ATENCIÓN	Advertencia sobre costes adicionales que pueden surgir al contratar servicios.
	ADVERTENCIA	Advertencia sobre una posible pérdida de datos.
	PELIGRO	Advertencia sobre una posible infección de un sistema con malware.



Estructura y funcionamiento de ATP

Advanced Threat Protection (ATP) protege a las empresas frente a ataques selectivos e individuales.

Advanced Threat Protection (ATP) protege a las empresas frente a ataques selectivos e individuales. Unos innovadores motores de análisis forense se encargan de impedir los ataques al momento. Al mismo tiempo, esta solución proporciona datos detallados sobre ataques contra empresas.

ATP se compone de los siguientes motores de análisis (véase [Descripción de los motores de ATP](#) en la página 7):

- Motor de sandbox
- Secure Links
- URL Scanning
- Congelación
- Targeted Fraud Forensics

Los correos captados por ATP se clasifican como **AdvThreat** y se ponen en cuarentena. Pueden ser entregados manualmente por usuarios con derechos administrativos (véase [Roles](#)).

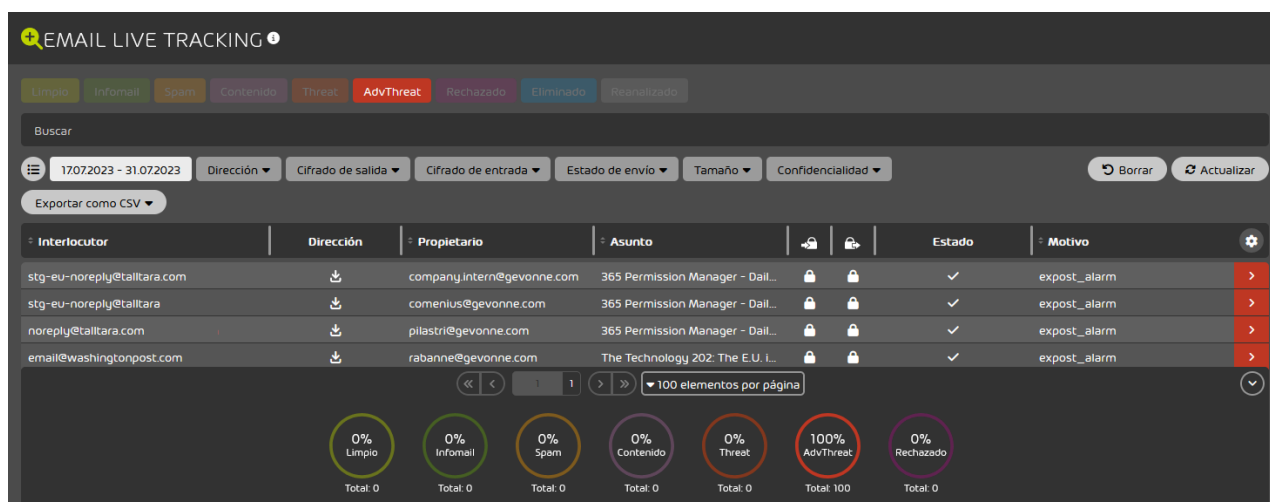


Figura 1: Categoría AdvThreat

ATP informa a los responsables de seguridad de las empresas sobre eventos relevantes para la seguridad en dos momentos:



- Inmediatamente tras la recepción de los correos que provoquen una respuesta de Real-Time Alert (véase [Notificaciones en tiempo real](#) en la página 11).
- Inmediatamente tras la detección de nuevas amenazas en correos ya entregados, mediante la función Ex Post Alert (véase [Ex Post Alert](#) en la página 12). Si la función Ex Post Deletion (véase [Ex Post Deletion](#) en la página 12) está activada para el cliente, los correos peligrosos en buzones de Microsoft 365 se eliminan automáticamente. Pero los correos peligrosos en otros buzones de correo se marcan como **Threat**. En las notificaciones de Ex Post Alert se muestran tanto los correos eliminados como los correos marcados.

El siguiente diagrama muestra el papel de ATP en el procesamiento de correos mediante nuestra infraestructura.

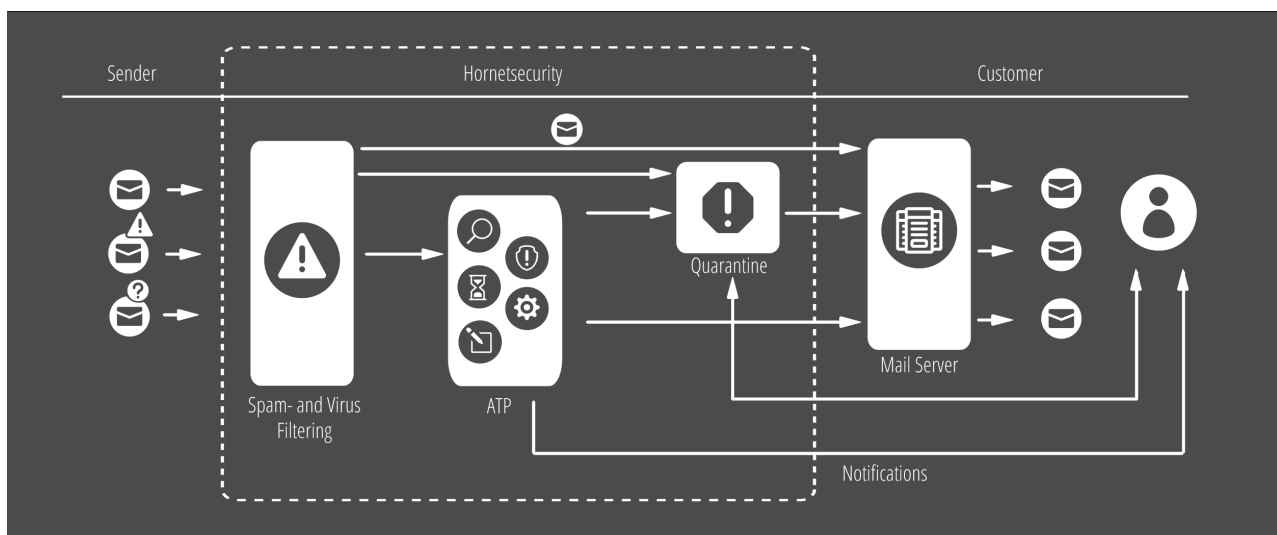


Figura 2: Funcionamiento de ATP

Con la función Ex Post Deletion (véase [Ex Post Deletion](#) en la página 12), los administradores pueden eliminar correos ya entregados de los buzones de correo de Microsoft 365 (véase [Tipos de buzón de correo](#)) de sus usuarios, y los usuarios correos de sus propios buzones de Microsoft 365, desde el módulo **Email Live Tracking** (véase [Email Live Tracking](#)). Además, los correos ya entregados a buzones de Microsoft 365 que Ex Post Alert haya identificado con posterioridad como amenazas se eliminan automáticamente. Para más información sobre cómo activar Ex Post Deletion, véase [Activar Ex Post Deletion](#) en la página 34.



Nota:

Ex Post Deletion solo está disponible para los clientes de 365 Total Protection Enterprise.



Además del análisis automático de los correos, tanto a su llegada como posteriormente en el contexto de la función Ex Post Alert, ATP ofrece la posibilidad de efectuar análisis manuales de correos con archivos adjuntos ejecutables. Con los denominados escaneos ATP (véase [Escaneo ATP](#) en la página 38), el usuario, además de aumentar su seguridad, obtiene información detallada sobre los correos en cuestión en forma de informes ATP (véase [Informe ATP](#) en la página 41).

Para que un cliente pueda emplear Advanced Threat Protection, un administrador debe activar el servicio (véase [Activar ATP](#) en la página 14). A continuación es posible administrar los destinatarios de notificaciones en tiempo real de Real-Time Alert y Ex Post Alert (véanse [Añadir destinatarios de notificaciones](#) en la página 15 y [Eliminar destinatarios de notificaciones](#) en la página 17). El motor Secure Links y el motor Targeted Fraud Forensics Filter, así como la función Ex Post Deletion, deben activarse individualmente (véanse [Activar Ex Post Deletion](#) en la página 34, [Activar Secure Links](#) en la página 18 y [Activar Targeted Fraud Forensics Filter](#) en la página 31). Además, los administradores pueden decidir a qué grupos de usuarios se aplicará el motor Targeted Fraud Forensics Filter (véanse [Añadir un grupo a la lista de grupos de TFFF](#) en la página 32 y [Retirar un grupo de la lista de grupos de TFFF](#) en la página 34).

Descripción de los motores de ATP

Advanced Threat Protection emplea diversos motores para detectar y rechazar ataques.

Tabla 1: Motores de ATP

HORNETSECURITY MOTORES DE ATP	MODO DE FUNCIONAMIENTO Y VENTAJAS
Motor de sandbox	Los archivos adjuntos se ejecutan en numerosos entornos para analizar su comportamiento. Si resulta tratarse de malware, se lo notificamos. Protege frente a ransomware y ataques combinados.



HORNETSECURITY

MOTORES DE ATP

MODO DE FUNCIONAMIENTO Y VENTAJAS

Secure Links

Secure Links impide que los enlaces incluidos en correos electrónicos lleven a los usuarios a páginas web maliciosas. Si Secure Links está activado para un cliente, los enlaces incluidos en los correos entrantes de los usuarios se reescriben al recibirse éstos en nuestra infraestructura. Cada uno de los enlaces reescritos utiliza uno de los varios dominios de Secure Links (véase [Dominios de Secure Links](#) en la página 20). Esta reescritura permite que Secure Links compruebe las páginas web con posterioridad.

**Nota:**

Los administradores pueden decodificar los enlaces reescritos en cualquier momento (véase [Descodificar enlaces de Secure Links](#) en la página 30) mediante el decodificador de enlaces (véase [Descodificador de enlaces](#) en la página 29). Los usuarios solo pueden decodificar los enlaces reescritos por sí mismos (véase [Roles](#)) si un administrador ha habilitado el decodificador de enlaces para ellos (véase [Modificar los módulos mostrados en User Panel](#)).

Cuando un usuario hace clic en un enlace reescrito de un correo, Secure Links analiza la página web correspondiente utilizando las bases de datos de inteligencia de dominios y direcciones URL de Hornetsecurity. Estas bases de datos contienen miles de millones de registros de phishing y malware y se amplían continuamente. Durante las pruebas, se muestran consejos de seguridad al usuario



HORNETSECURITY

MOTORES DE ATP

MODO DE FUNCIONAMIENTO Y VENTAJAS

URL Scanning

Los documentos adjuntos a un correo (p. ej., archivos PDF o de Microsoft) pueden contener enlaces. Sin embargo, no es posible sustituir los enlaces sin dañar la integridad del documento. El motor URL Scanning de Hornetsecurity deja el documento intacto y se limita a comprobar el destino de los enlaces.

QR Code Analyzer

Las imágenes adjuntas a un correo (p. ej., en formato PNG, JPEG, GIF and BMP) pueden contener códigos QR. QR Code Analyzer comprueba el destino del código QR y bloquea el correo si éste conduce a una página web peligrosa.

Congelación

Los correos electrónicos que no pueden ser asignados de inmediato y de manera concluyente a una categoría pero parecen sospechosos, son retenidos temporalmente mediante el proceso de Congelación. A continuación se efectúa un nuevo análisis con firmas actualizadas. Protege frente a ransomware, ataques combinados y suplantación de identidad.



HORNETSECURITY

MOTORES DE ATP

MODO DE FUNCIONAMIENTO Y VENTAJAS

Targeted Fraud Forensics Filter

Targeted Fraud Forensics Filter detecta ataques personalizados sin malware o enlaces. Incluye los siguientes mecanismos de detección:

- Intention Recognition System: Alerta en caso de patrones de contenido que indiquen malas intenciones.
- Fraud Attempt Analysis: Comprueba la autenticidad y la integridad de los metadatos y contenidos de los correos.
- Identity Spoofing Recognition: Detección y bloqueo de identidades falsas de remitentes.
- Spy-Out Detection: Protección antiespionaje de ataques para la obtención de información sensible.
- Feign Facts Identification: Análisis de mensajes en cuanto a falsas apariencias.
- Targeted Attack Detection: Detección de ataques selectivos contra personas concretas.

Este motor debe activarse por separado (véase [Activar Targeted Fraud Forensics Filter](#) en la página 31). Targeted Fraud Forensics Filter se aplica a grupos de usuarios seleccionados que se administran mediante una lista de grupos (véanse [Añadir un grupo a la lista de grupos de TFFF](#) en la página 32 y [Retirar un grupo de la lista de grupos de TFFF](#) en la página 34).



Notificaciones en tiempo real

Real-Time Alert es una función de notificación de Advanced Threat Protection que informa acerca de las razones por las que se ha detenido un correo.

Tan pronto Advanced Threat Protection detecta un ataque, se envía una notificación a la empresa del cliente informándola sobre una posible amenaza. Las notificaciones incluyen información sobre el tipo y el objetivo del ataque, el remitente y el motivo por el que se ha detenido el correo.

Se envían notificaciones en los siguientes casos:

- El motor de sandbox ha detectado código malicioso (véase [Motor de sandbox](#)).
- Secure Links ha bloqueado una página web o una descarga (véase [Secure Links](#)).
- URL Scanning ha detectado un URL malicioso (véase [URL Scanning](#)).
- Targeted Fraud Forensics Filter ha filtrado correos (véase [Targeted Fraud Forensics Filter](#)).

Los destinatarios de las notificaciones pueden añadirse (véase [Añadir destinatarios de notificaciones](#) en la página 15) o eliminarse (véase [Eliminar destinatarios de notificaciones](#) en la página 17) mediante **Email Security > Advanced Threat Protection**.



Hornetsecurity Advanced Threat Protection - Real Time Alert

The Hornetsecurity Advanced Threat Protection Service has just detected the following email attack:

Classification:	Hornet-ATP03
User:	accounting@yourcompany.com
Date:	09/22/2016 12:09 PM CEST
Sender:	hacker@maliciousdomain.com, ceo@yourcompany.com
Server Address:	123.123.123.123, mail.hackedserver1237.com
Reason:	ATP Sandbox
Attachment:	payment_sheet.js

Figura 3: Notificación a tiempo real de Hornetsecurity

Figura 4: Notificación a tiempo real



Ex Post Alert

Mediante Ex Post Alert, los equipos de seguridad informática de las empresas reciben notificaciones cuando correos ya entregados se clasifican como dañinos a posteriori.

**Nota:**

Si la función Ex Post Deletion (véase [Ex Post Deletion](#) en la página 12) está activada para el cliente, los correos peligrosos en buzones de Microsoft 365 se eliminan. Pero los correos peligrosos en otros buzones de correo se marcan como **Threat**. En las notificaciones de Ex Post Alert se muestran tanto los correos eliminados como los correos marcados.

Una notificación de Ex Post Alert solo se envía cuando se han clasificado aproximadamente 100 correos como dañinos a posteriori.

Los destinatarios de Ex Post Alert reciben una evaluación detallada del ataque de modo que puedan tomar inmediatamente medidas tales como comprobar sus sistemas o concienciar a sus empleados.

Los destinatarios de las notificaciones pueden añadirse (véase [Añadir destinatarios de notificaciones](#) en la página 15) o eliminarse (véase [Eliminar destinatarios de notificaciones](#) en la página 17) mediante **Email Security > Advanced Threat Protection**.

**Nota:**

Ex Post Alert se activa para todos los buzones de correo de un cliente al activarse Advanced Threat Protection.

Ex Post Deletion

**Nota:**

Ex Post Deletion solo está disponible para los clientes de 365 Total Protection Enterprise.

Mediante Ex Post Deletion, los clientes de 365 Total Protection pueden eliminar posteriormente correos ya entregados de los buzones de correo de Microsoft 365 (véase [Tipos de buzón de correo](#)) de sus usuarios. Además, los correos ya entregados a buzones de Microsoft 365 que Ex



Post Alert (véase [Ex Post Alert](#) en la página 12) haya identificado con posterioridad como una amenaza se eliminan.



Nota:

Con Ex Post Deletion, los correos solo se eliminan de sus buzones de correo de Microsoft 365 correspondientes. Los correos archivados permanecen en el archivo (véase [Archiving](#)).

Antes de su primer uso, Ex Post Deletion debe activarse en el módulo (véase [Activar Ex Post Deletion](#) en la página 34). A continuación, es posible eliminar correos de buzones de correo en el módulo **Email Live Tracking** (véase [Acciones para correos](#)).



Configuración por defecto

Activar ATP

 Ha activado Spam and Malware Protection.

Puede activar Advanced Threat Protection para proteger a su empresa en tiempo real frente a ciberataques selectivos e individualizados.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee activar Advanced Threat Protection.
3. Vaya a **Email Security > Advanced Threat Protection**.
4. Accione el interruptor **Activar Advanced Threat Protection**.

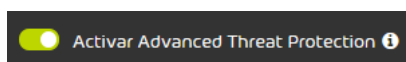


Figura 5: Activar Advanced Threat Protection

 Se muestra una ventana de confirmación.

5.



ATENCIÓN:

Una vez activado Advanced Threat Protection, comenzará un periodo de prueba gratuito de 30 días. Al finalizar el periodo de prueba, el servicio se volverá de pago.

Haga clic en .

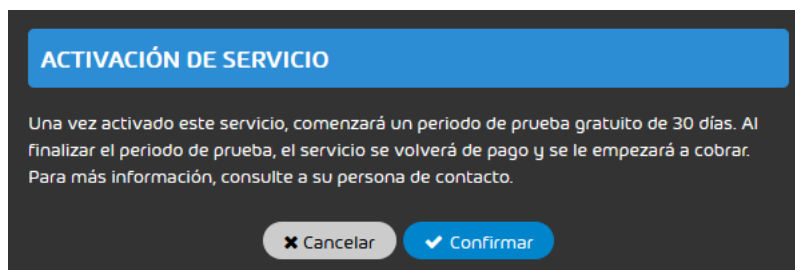


Figura 6: Confirmar



Advanced Threat Protection se ha activado para el dominio.

**IMPORTANTE:**

Con su activación, se activan también todos los motores ATP (véase [Descripción de los motores de ATP](#) en la página 7) salvo Secure Links y Targeted Fraud Forensics Filter para el dominio. Secure Links y Targeted Fraud Forensics Filter deben activarse por separado.

A continuación puede administrar los destinatarios de notificaciones de Advanced Threat Protection (véanse [Añadir destinatarios de notificaciones](#) en la página 15 y [Eliminar destinatarios de notificaciones](#) en la página 17). También puede activar la función Ex Post Deletion y el motor Secure Links y el motor Targeted Fraud Forensics Filter (véase [Activar Ex Post Deletion](#) en la página 34, [Activar Secure Links](#) en la página 18 y [Activar Targeted Fraud Forensics Filter](#) en la página 31).

Añadir destinatarios de notificaciones



Ha activado Advanced Threat Protection (véase [Activar ATP](#) en la página 14).

En el módulo **Email Security > Advanced Threat Protection** puede añadir las direcciones de correo de los usuarios que han de recibir notificaciones de Real-Time Alert (véase [Notificaciones en tiempo real](#) en la página 11) y Ex Post Alert (véase [Ex Post Alert](#) en la página 12).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee activar añadir destinatarios de notificaciones.
3. Vaya a **Email Security > Advanced Threat Protection**.
4. Haga clic en **Añadir destinatario**.

**Nota:**

Es recomendable registrar a los responsables de seguridad de su empresa como destinatarios.

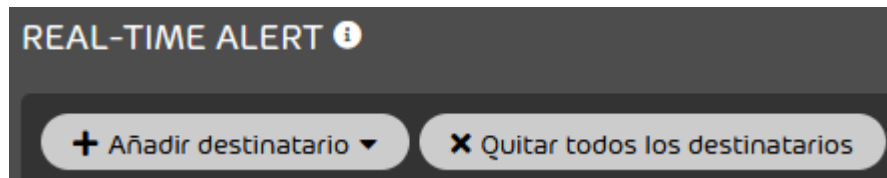


Figura 7: Añadir un destinatario

➔ Se abre una vista avanzada.

5. Introduzca la dirección de correo electrónico deseada en el campo de introducción de datos.

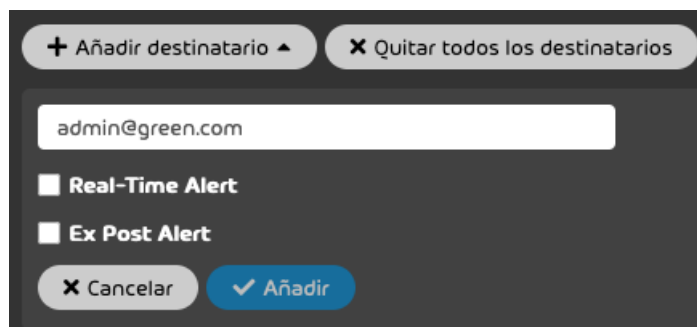


Figura 8: Introducir una dirección de correo electrónico

6. Marque las casillas de los tipos de notificaciones que el destinatario ha de recibir. Tiene las siguientes opciones.
 - Real-Time Alert (véase [Notificaciones en tiempo real](#) en la página 11)
 - Ex Post Alert (véase [Ex Post Alert](#) en la página 12)

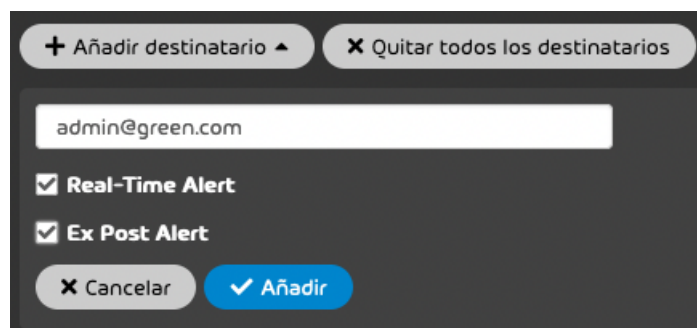


Figura 9: Seleccionar tipos de notificaciones

7. Haga clic en **Añadir**.



- ➔ La dirección de correo se añade a la lista **Destinatarios de notificaciones**. Las marcas en las columnas **Ex Post Alert** y **Real-Time Alert** indican que el destinatario recibe notificaciones de este tipo.

Destinatarios de notificaciones	Real-Time Alert	Ex Post Alert	
expost@green.com	✓	-	✕
admin@green.com	✓	✓	✕

Figura 10: Destinatario añadido

- ✓ Se ha añadido una dirección de correo electrónico para la recepción de notificaciones de Real-Time Alert y/o Ex Post Alert.

Eliminar destinatarios de notificaciones

- ✓ Ha activado Advanced Threat Protection (véase [Activar ATP](#) en la página 14) y añadido destinatarios de notificaciones (véase [Añadir destinatarios de notificaciones](#) en la página 15).

En el módulo **Email Security > Advanced Threat Protection** puede eliminar direcciones de correo electrónico de la lista de destinatarios de notificaciones de Advanced Threat Protection (véase [Estructura y funcionamiento de ATP](#) en la página 5). Puede elegir entre eliminar direcciones de correo seleccionadas o eliminarlas todas a la vez.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio al que pertenezca el destinatario que desee eliminar de Advanced Threat Protection.
3. Vaya a **Email Security > Advanced Threat Protection**.
4. Para eliminar un único destinatario, proceda del siguiente modo:
 - a) Seleccione en la lista **Destinatarios de notificaciones** la dirección de correo que desee eliminar.

Destinatarios de notificaciones	Real-Time Alert	Ex Post Alert	
expost@green.com	✓	-	✕
admin@green.com	✓	✓	✕

Figura 11: Seleccionar una dirección de correo



b) Haga clic en la cruz de la fila de la dirección de correo que desee eliminar.

➔ La dirección de correo se elimina de la lista.

5. Para eliminar todos los destinatarios al mismo tiempo, proceda del siguiente modo:

a) Haga clic en **Quitar todos los destinatarios**.

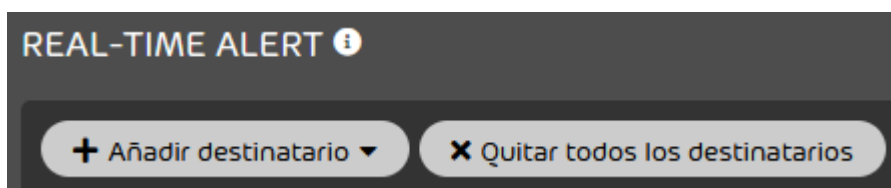


Figura 12: Eliminar todos los destinatarios

➔ Aparece una ventana de confirmación.

b) Haga clic en .

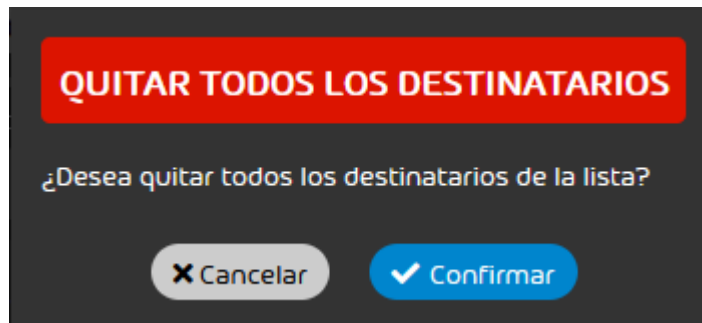


Figura 13: Confirmar

➔ Todas las direcciones de correo se eliminan de la lista.

✓ Se han eliminado algunas o todas las direcciones de correo de la lista de destinatarios de notificaciones de Advanced Threat Protection.

Activar Secure Links

✓ Ha activado Advanced Threat Protection (véase [Activar ATP](#) en la página 14). Ha permitido los dominios de Secure Links (véase [Dominios de Secure Links](#) en la página 20) en la infraestructura del cliente.



En el módulo **Email Security > Advanced Threat Protection** puede activar el motor de ATP Secure Links (véase [Descripción de los motores de ATP](#) en la página 7). Secure Links se activa por defecto para todos los usuarios de sus dominios principal y alias.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee activar Secure Links.
3. En Control Panel, vaya a **Email Security > Advanced Threat Protection**.
4. Accione el interruptor **SECURE LINKS** de **Activar Secure Links**.



Figura 14: Activar Secure Links

- ➔ El interruptor se pone verde y se abre una ventana de confirmación.



Nota:

Secure Links se activa por defecto para todos los buzones de correo de sus dominios principal y alias. Si no desea activar Secure Links para todos los dominios, póngase en contacto con el soporte técnico e indíquele qué dominios desea excluir de la activación antes de hacerlo. No es posible excluir de Secure Links a usuarios individuales de un dominio.

5. Haga clic en **Confirmar**.

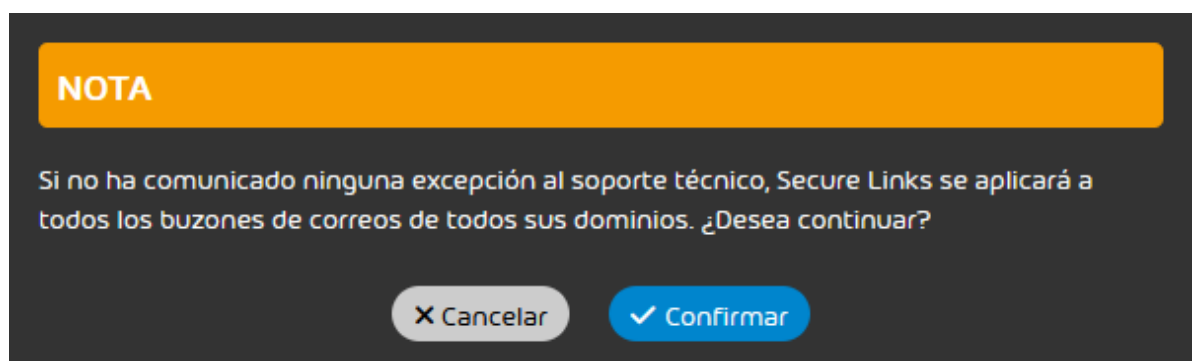


Figura 15: Confirmar



Secure Links se ha activado para todos los buzones de correo de sus dominios principal y alias no definidos como excepciones.

Dominios de Secure Links

La función Secure Links (véase [Descripción de los motores de ATP](#) en la página 7) del servicio Advanced Threat Protection (véase [Estructura y funcionamiento de ATP](#) en la página 5) reescribe los enlaces en correos. Los enlaces reescritos pertenecen a uno de los siguientes dominios:

- atpscan.global.hornetsecurity.com
- seclinks.cloud-security.net
- securelinks.cloud-security.net

Para que los usuarios puedan acceder a los enlaces reescritos, los clientes que utilicen la función Secure Links deben permitir los dominios en su infraestructura. El proceso depende de la infraestructura del cliente. Los clientes que utilicen Office 365 Premium o Microsoft 365 E5 con Microsoft Defender deben permitir los dominios en Microsoft Defender (véase [Permitir los dominios de Secure Links en Microsoft Defender](#) en la página 20). Los clientes que utilicen Office 365 Basic, en el que no se incluye Microsoft Defender, deben permitir los dominios utilizando envíos en Microsoft 365 (véase [Permitir los dominios de Secure Links enviándolos a Microsoft](#) en la página 26).

Permitir los dominios de Secure Links en Microsoft Defender



Su organización utiliza Office 365 Premium o E5. Activará la función Secure Links del servicio Advanced Threat Protection (véase [Activar Secure Links](#) en la página 18).

Para permitir que sus usuarios accedan a enlaces reescritos por la función Secure Links (véase [Descripción de los motores de ATP](#) en la página 7) del servicio Advanced Threat Protection (véase [Estructura y funcionamiento de ATP](#) en la página 5), debe permitir los dominios de Secure Links (véase [Dominios de Secure Links](#) en la página 20) en Microsoft Defender.

1. Abra la página web <https://security.microsoft.com>.
2. Inicie sesión con sus datos de acceso de administrador.
3. Vaya a **Reglas y directivas**.

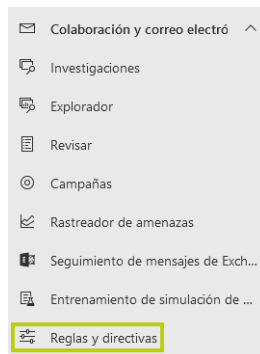


Figura 16: Abrir directivas y reglas

4. Haga clic en **Directivas de amenazas**.

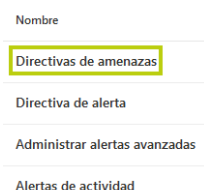


Figura 17: Abrir directivas sobre amenazas

5. En **Directivas**, haga clic en **Vínculos seguros**.

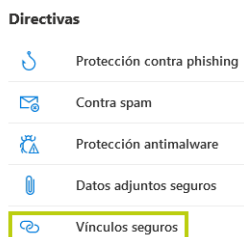


Figura 18: Abrir vínculos seguros

- ➔ Se muestra la página **Vínculos seguros**.

6. Para crear una nueva directiva, haga clic en **Crear**.

i **Nota:**

En lugar de crear una nueva directiva, también puede editar una directiva existente. Para editar una directiva existente, haga clic en la misma en la lista de directivas.

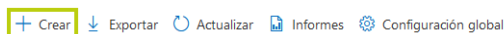


Figura 19: Crear una directiva

- ➔ Se abre la página **Asigne un nombre a la directiva**.
- 7. Introduzca el nombre de la directiva en el campo **Nombre**.

**Nota:**Recomendamos llamar a la directiva **Bypass SafeLinks Secure Links**.**Nombre ***

Bypass SafeLinks Secure Links

Figura 20: Introducir el nombre de la directiva

- 8. Opcional: Introduzca una descripción de la directiva en el campo **Descripción**.
- 9. Haga clic en **Siguiente**.
- ➔ Se muestra la página **Usuarios y dominios**.
- 10. Introduzca el dominio al que pertenecen los usuarios de Secure Links en el campo **Dominios** y haga clic en el dominio mostrado.

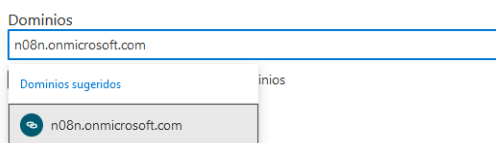


Figura 21: Introducir el dominio

- ➔ El dominio se añade.

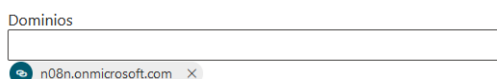


Figura 22: Dominio añadido

- 11. Repita el paso 10 en la página 22 hasta que haya añadido todos los dominios.
- 12. Haga clic en **Siguiente**.



- ➔ Se muestra la página **Configuración de protección de direcciones URL y clics**.

13. Realice los ajustes que desee.

**Nota:**

Los ajustes mostrados en la captura de pantalla son meros ejemplos. Los clientes pueden realizar otros ajustes si lo desean.

Correo electrónico

- ☒ Activado: Vínculos seguros comprueba una lista de vínculos malintencionados conocidos cuando los usuarios hacen clic en vínculos en el correo electrónico. Las direcciones URL se reescriben de forma predeterminada.
- ☒ Aplicar vínculos seguros a los mensajes de correo electrónico enviados dentro de la organización
- ☒ Aplicar un análisis de URL en tiempo real para vínculos sospechosos y vínculos que apuntan a archivos
 - ☐ Espere a que el análisis de URL se complete antes de entregar el mensaje.
 - ☐ No vuelva a escribir las direcciones URL: realice las comprobaciones solo a través de la API de vínculos seguros.

No vuelva a escribir las siguientes URL en el correo electrónico (0)

[Administrar 0 dirección URL](#)

Teams

- ☒ Activado: Vínculos seguros comprueba una lista de vínculos malintencionados conocidos cuando los usuarios hacen clic en vínculos en Microsoft Teams. Las direcciones URL no se reescriben.

Aplicaciones de Office 365

- ☒ Activado: Vínculos seguros comprueba una lista de vínculos malintencionados conocidos cuando los usuarios hacen clic en vínculos en aplicaciones de Microsoft Office. Las direcciones URL no se reescriben.

Configuración de protección de clics

- ☒ Realizar un seguimiento de los clics de usuario
 - ☒ Permitir que los usuarios hagan clic en la dirección URL original
 - ☐ Mostrar la personalización de marca de la organización en las notificaciones y las páginas de advertencia

Figura 23: Configurar la protección de direcciones URL y clics

14. Haga clic en **Administrar dirección URL**.

No vuelva a escribir las siguientes URL en el correo electrónico (0)

[Administrar 0 dirección URL](#)

Figura 24: Administrar URLs

- ➔ Al lado derecho se muestra la página **Administrar las direcciones URL que no se deben reescribir**.

15. Haga clic en **Agregar direcciones URL**.



Figura 25: Añadir URLs

- ➔ Se muestra la página **Agregar direcciones URL**.
16. Introduzca consecutivamente los siguientes dominios en el campo de introducción de datos **URL** y haga clic en el dominio mostrado.
- **atpscan.global.hornetsecurity.com**
 - **seclinks.cloud-security.net**
 - **securelinks.cloud-security.net**
 - **atpscan.global.hornetsecurity.com/***
 - **seclinks.cloud-security.net/***
 - **securelinks.cloud-security.net/***



Figura 26: Introducir el dominio

- ➔ El dominio se añade.



Figura 27: Dominio añadido

17. Haga clic en **Guardar**.
- ➔ La página **Agregar direcciones URL** se cierra. Vuelve a mostrarse la página **Administrar las direcciones URL** que no se deben reescribir. En la página se muestran todos los dominios añadidos.
18. Haga clic en **Listo**.



- ➔ La página **Administrar las direcciones URL que no se deben reescribir** se cierra. Vuelve a mostrarse la página **Configuración de protección de direcciones URL y clics**.
- 19. Haga clic en **Siguiente**.
- ➔ Se muestra la página **Notificación**.
- 20. Realice los ajustes que desee.

Notificación

¿Cómo quiere que sus usuarios reciban las notificaciones?

☒ Utilizar el texto de notificación predeterminado

☐ Usar texto de notificación personalizado

Figura 28: Configurar la notificación

- 21. Haga clic en **Siguiente**.
- ➔ Se muestra un resumen de la configuración de la directiva.
- 22. Haga clic en **Enviar**.
- ➔ Se muestra un mensaje de confirmación.
- 23. Haga clic en **Enviar**.
- ➔ La directiva se crea. La creación de la directiva puede tardar un momento. Una vez creada la directiva se muestra un mensaje de éxito.

Nueva directiva de ✓ Vínculos seguros creada

Se creó la directiva Vínculos seguros **Bypass SafeLinks Secure Links**. Entrará en vigor inmediatamente.

Figura 29: Mensaje de éxito

- 24. Haga clic en **Listo**.
- ➔ La página se cierra.



✓ Los dominios de Secure Links se han permitido en Microsoft Defender.

A continuación puede activar Secure Links (véase [Activar Secure Links](#) en la página 18).

Permitir los dominios de Secure Links enviándolos a Microsoft

✓ Su organización utiliza Office 365 Basic. Activará la función Secure Links del servicio Advanced Threat Protection (véase [Activar Secure Links](#) en la página 18).

Para permitir que sus usuarios accedan a enlaces reescritos por la función Secure Links (véase [Descripción de los motores de ATP](#) en la página 7) del servicio Advanced Threat Protection (véase [Estructura y funcionamiento de ATP](#) en la página 5), debe permitir los dominios de Secure Links (véase [Dominios de Secure Links](#) en la página 20) enviándolos a Microsoft.

1. Abra la página web <https://security.microsoft.com>.
2. Inicie sesión con sus datos de acceso de administrador del inquilino de Microsoft 365.
3. Vaya a **Investigación y respuesta** > **Acciones y envíos** > **Entregas**.

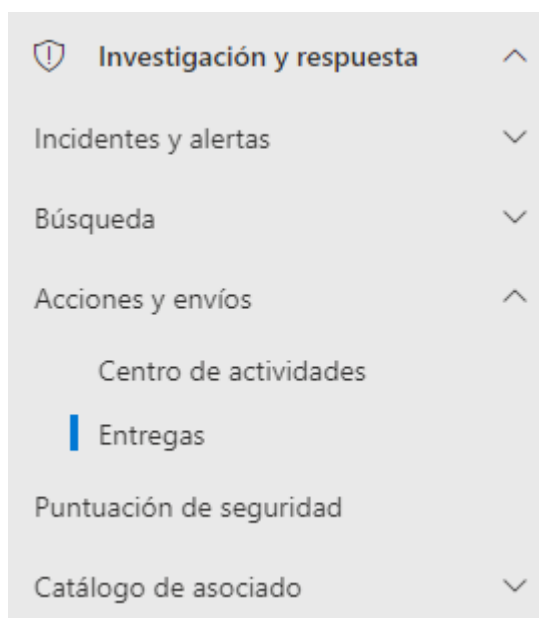


Figura 30: Vaya a Entregas.

4. Seleccione la pestaña **Direcciones URL**.
5. Haga clic en **Enviar a Microsoft para ser analizado**.



+ Enviar a Microsoft para ser analizado ↓ Exportar ↻ Actualizar

Figura 31: Enviar a Microsoft para ser analizado

- ➔ Al lado derecho se muestra la página **Enviar a Microsoft para ser analizado**.
- 6. En el menú desplegable **Seleccione el tipo de envío**, seleccione **URL**.

Seleccione el tipo de envío

Seleccione el tipo de envío *

URL

- 7. Introduzca consecutivamente los siguientes dominios en el campo de introducción de datos **URL** y haga clic en el dominio mostrado.
- **atpscan.global.hornetsecurity.com**
- **seclinks.cloud-security.net**
- **securelinks.cloud-security.net**

URL *

securelinks.cloud-security.net

securelinks.cloud-security.net

URL a Microsoft? *

Figura 32: Introducir el dominio

- ➔ El dominio se añade.

URL *

securelinks.cloud-security.net X

Figura 33: Dominio añadido

- 8. Seleccione **¿Por qué quiere enviarle esta dirección URL a Microsoft?** en **He confirmado que no se trata de una amenaza**.



¿Por qué quiere enviarle esta dirección URL a Microsoft? *

- ☒ He confirmado que no se trata de una amenaza
- ☐ No me parece sospechoso
- ☐ Me parece sospechoso
- ☐ He confirmado que se trata de una amenaza

Figura 34: Especificar el motivo del envío

9. Haga clic en **Siguiente**.

10. Deje sin marcar la casilla **Permitir esta dirección URL**.

☐ Permitir esta dirección URL

Figura 35: Permitir la dirección URL

➔ Los dominios se enviarán a Microsoft para que se permitan de forma permanente.

11. Haga clic en **Enviar**.

➔ Se muestra un mensaje de éxito.

✔ Elementos enviados

Gracias por enviarnos esta información. Nos pondremos en comunicación con usted en cuanto se analice su envío. Las actualizaciones se mostrarán en la página Envíos.

Figura 36: Mensaje de éxito

Los dominios pueden tardar varias horas en permitirse.



Nota:

Recomendamos que el cliente supervise sus colas de cuarentena durante las próximas 24 horas para asegurarse de que Microsoft clasifique los correos correctamente. Para más información, consulte la [documentación de Microsoft](#).



12. Haga clic en **Listo**.



La página **Enviar a Microsoft para ser analizado** se cierra. Los dominios se muestran en la lista de envíos.



Los dominios de Secure Links se han enviado a Microsoft para que se permitan de forma permanente.

A continuación puede activar Secure Links (véase [Activar Secure Links](#) en la página 18).

Descodificador de enlaces

Los administradores pueden utilizar el descodificador de enlaces en el módulo **Configuración de seguridad** > (véase [Estructura y funcionamiento de ATP](#) en la página 5) para volver a convertir los enlaces reescritos por el motor de ATP Secure Links (véase [Descripción de los motores de ATP](#) en la página 7) en los enlaces originales.



Nota:

El descodificador de enlaces también se puede utilizar para los enlaces reescritos por la función Time-of-Click.

Si el motor de ATP Secure Links está activado (véase [Activar Secure Links](#) en la página 18), los enlaces incluidos en los correos enviados a los usuarios de un cliente se reescriben. La reescritura garantiza que se realice un análisis de seguridad en el momento en que un usuario hace clic en el enlace. En caso de peligro, se bloquea el acceso a la página web. Sin embargo, en casos excepcionales, los administradores pueden necesitar el enlace original. Por ejemplo, el enlace original permite a los administradores seguir evaluando una página web bloqueada bajo su propio riesgo.



PELIGRO:

Los enlaces originales evitan el análisis de seguridad que se incluye en los enlaces reescritos. Al abrir un enlace original, podría acceder a una página web maliciosa. Trate los enlaces originales con la máxima precaución.

Para descodificar un enlace reescrito de un correo, los administradores pueden proceder del siguiente modo (véase [Descodificar enlaces de Secure Links](#) en la página 30).



Descodificar enlaces de Secure Links



Ha activado Secure Links (véase [Activar Secure Links](#) en la página 18).

Puede utilizar el descodificador de enlaces en el módulo **Email Security > Advanced Threat Protection** (véase [Estructura y funcionamiento de ATP](#) en la página 5) para volver a convertir los enlaces reescritos por el motor de ATP Secure Links (véase [Descripción de los motores de ATP](#) en la página 7) en los enlaces originales.



Nota:

Para más información sobre el descodificador de enlaces, véase [Descodificador de enlaces](#) en la página 29.



Nota:

El descodificador de enlaces también se puede utilizar para los enlaces reescritos por la función Time-of-Click.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee descodificar un enlace.
3. Vaya a **Email Security > Advanced Threat Protection**.
4. Pegue el enlace reescrito en el campo de introducción de datos en **Descodificador de enlaces** y haga clic en **Descodificar enlace**.

Descodificador De Enlaces ⓘ

Pegue un enlace seguro codificado.

Descodificar enlace

Figura 37: Descodificar el enlace



El enlace se descodifica. El enlace original se muestra en el campo de introducción de datos. El enlace se puede copiar en el portapapeles para su uso posterior.

**PELIGRO:**

Los enlaces originales evitan el análisis de seguridad que se incluye en los enlaces reescritos. Al abrir un enlace original, podría acceder a una página web maliciosa. Trate los enlaces originales con la máxima precaución.



Un enlace reescrito se ha descodificado.

Activar Targeted Fraud Forensics Filter



Ha activado Advanced Threat Protection (véase [Activar ATP](#) en la página 14) y creado grupos de usuarios (véase [Grupos](#)). Ha activado la comprobación SPF (véase [Activar la comprobación SPF](#)).

En el módulo **Email Security > Advanced Threat Protection** puede activar el motor de ATP Targeted Fraud Forensics Filter (véase [Descripción de los motores de ATP](#) en la página 7) para los grupos de usuarios seleccionados.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee activar Targeted Fraud Forensics Filter.
3. En Control Panel, vaya a **Email Security > Advanced Threat Protection**.
4. Accione el interruptor **TARGETED FRAUD FORENSICS FILTER** de **Activar Targeted Fraud Forensics Filter**.

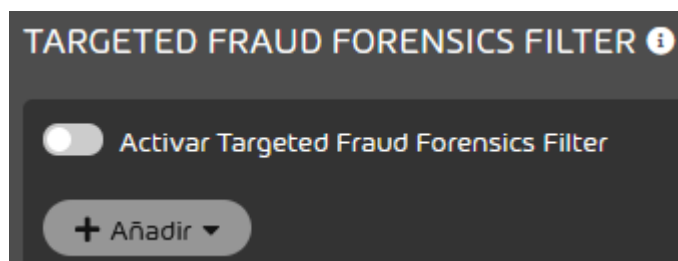


Figura 38: Activar Targeted Fraud Forensics Filter



El interruptor se pone verde. Targeted Fraud Forensics Filter se activa, pero aún no se aplica a ningún grupo de usuarios. El botón **Añadir** se habilita y se muestra un mensaje.

5. Haga clic en **Confirmar**.

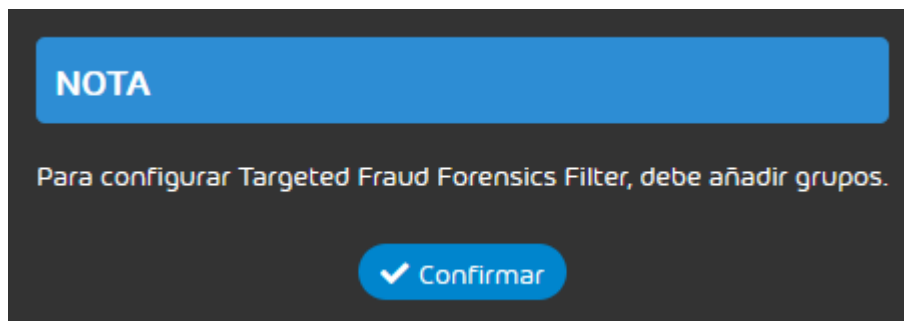


Figura 39: Confirmar

6. Añada los grupos de usuarios deseados a la lista de grupos (véase [Añadir un grupo a la lista de grupos de TFFF](#) en la página 32).

➔ Targeted Fraud Forensics Filter se aplica a todos los grupos de usuarios añadidos.

✓ El motor de ATP Targeted Fraud Forensics Filter se ha activado.

A continuación, puede añadir grupos a Targeted Fraud Forensics Filter (véase [Añadir un grupo a la lista de grupos de TFFF](#) en la página 32) o eliminarlos de allí (véase [Retirar un grupo de la lista de grupos de TFFF](#) en la página 34).

Añadir un grupo a la lista de grupos de TFFF

✓ Ha activado Targeted Fraud Forensics Filter (véase [Activar Targeted Fraud Forensics Filter](#) en la página 31) y ha creado grupos de usuarios o los ha sincronizado con LDAP (véase [Grupos](#)).

Targeted Fraud Forensics Filter no se aplica a dominios, sino a grupos de usuarios. Para aplicar Targeted Fraud Forensics Filter a un grupo, debe incluirlo en la lista de grupos del Targeted Fraud Forensics Filter.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio al que pertenezca el grupo que desee añadir a Targeted Fraud Forensics Filter.
3. En Control Panel, vaya a **Email Security > Advanced Threat Protection**.
4. En el apartado **TARGETED FRAUD FORENSICS FILTER**, haga clic en **Añadir**.

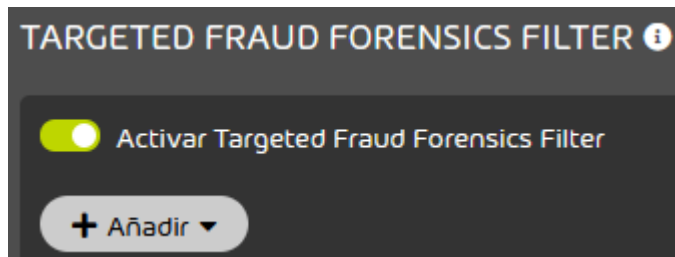


Figura 40: Añadir grupos

- ➔ Se abre una vista avanzada.

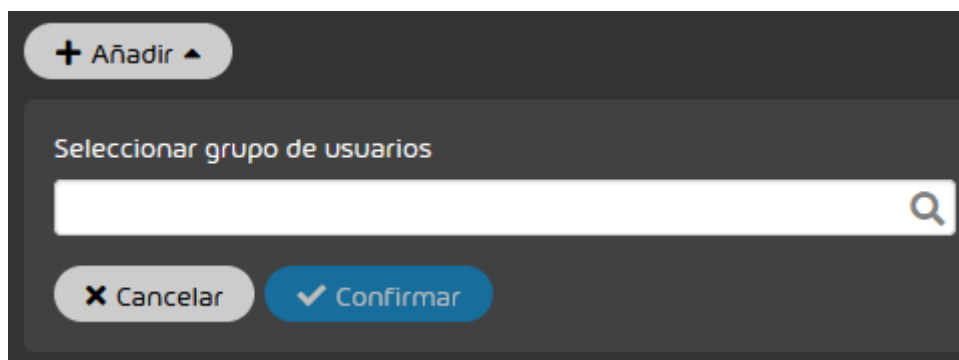


Figura 41: Vista avanzada

- Introduzca el nombre del grupo deseado en el campo de búsqueda.
- ➔ Se despliega un menú desplegable con los resultados de la búsqueda.
- Seleccione el grupo de usuarios.
- Haga clic en **Confirmar**.



Figura 42: Confirmar

- ➔ El grupo se ha añadido a la lista de grupos. Targeted Fraud Forensics Filter se aplica inmediatamente a todos los buzones de correo de este grupo.
- ✓ Se ha añadido un grupo a la lista de grupos de Targeted Fraud Forensics Filter.

A continuación puede eliminar el grupo de la lista de grupos de Targeted Fraud Forensics Filter (véase [Retirar un grupo de la lista de grupos de TFFF](#) en la página 34).



Retirar un grupo de la lista de grupos de TFFF



Ha activado Targeted Fraud Forensics Filter (véase [Activar ATP](#) en la página 14) y ha añadido grupos de usuarios a la lista de grupos (véase [Añadir un grupo a la lista de grupos de TFFF](#) en la página 32).

Targeted Fraud Forensics Filter se aplica a grupos de usuarios. Para dejar de aplicar Targeted Fraud Forensics Filter a un grupo, debe retirarlo de la lista de grupos del Targeted Fraud Forensics Filter.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio al que pertenezca el grupo que desee eliminar de Targeted Fraud Forensics Filter.
3. Vaya a **Email Security > Advanced Threat Protection**.
4. Seleccione el grupo deseado en la lista de usuarios de la sección **TARGETED FRAUD FORENSICS FILTER**.

Grupo	
Administration	×
Marketing	×
Sales	×

Figura 43: Seleccionar un grupo

5. Haga clic en la cruz junto al grupo que desee eliminar.
- ➡ El grupo se ha retirado de la lista de grupos. Targeted Fraud Forensics Filter ya no se aplicará a los buzones de correo de este grupo.



Se ha eliminado un grupo de la lista de grupos de Targeted Fraud Forensics Filter.

Activar Ex Post Deletion



Tiene 365 Total Protection Enterprise y ha activado Advanced Threat Protection (véase [Activar ATP](#) en la página 14).

Con la función Ex Post Deletion, los administradores pueden eliminar de los buzones de correo de Microsoft 365 (véase [Tipos de buzón de correo](#)) de sus usuarios correos ya entregados desde el módulo **Email Live Tracking** (véase [Email Live Tracking](#)). Los usuarios también pueden eliminar correos electrónicos de sus propios buzones de correo de Microsoft 365. Además, los



correos en buzones de Microsoft 365 que Ex Post Alert (véase [Ex Post Alert](#) en la página 12) haya identificado con posterioridad como una amenaza se eliminan automáticamente.

**Nota:**

Con Ex Post Deletion, los correos solo se eliminan de sus buzones de correo de Microsoft 365 correspondientes. Los correos archivados permanecen en el archivo (véase [Archiving](#)).

**Nota:**

Ex Post Deletion solo está disponible para los clientes de 365 Total Protection Enterprise.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee activar Ex Post Deletion.
3. Vaya a **Email Security > Advanced Threat Protection**.
4. Accione el interruptor **Activar Ex Post Deletion**.

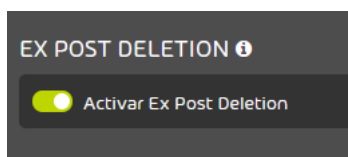


Figura 44: Activar Ex Post Deletion



El interruptor se pone verde. Se muestra una ventana de confirmación.

5. Haga clic en **Confirmar**.

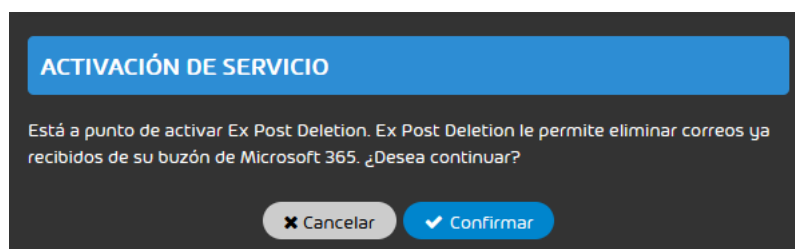


Figura 45: Confirmar la activación



Se abre la página de inicio de sesión de Microsoft.



6. Inicie sesión en Microsoft 365 con sus datos de acceso de administrador del dominio.

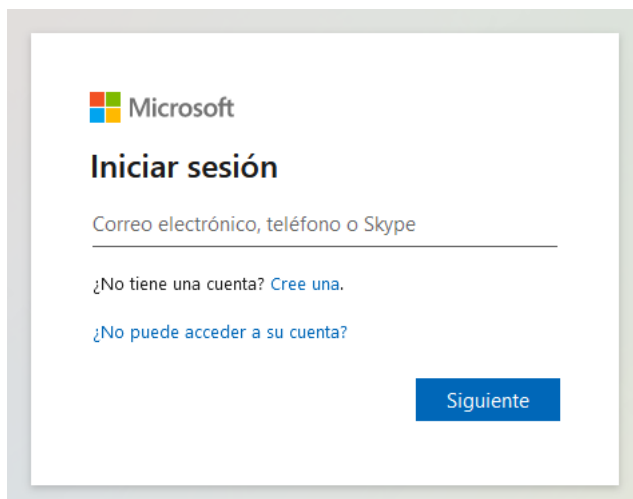


Figura 46: Iniciar sesión en Microsoft

- ➔ Se muestra una ventana con permisos.
7. Conceda los permisos necesarios para conectar Ex Post Deletion con Microsoft.

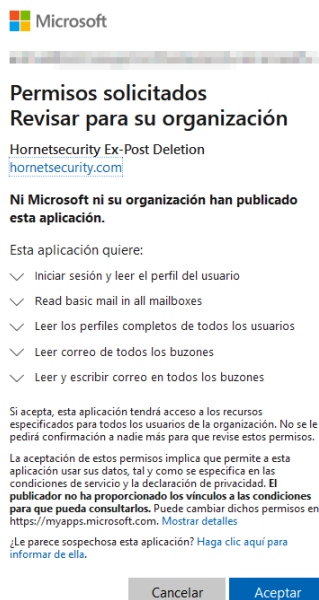


Figura 47: Conceder los permisos



➔ Control Panel vuelve a mostrarse.

✔ Ex Post Deletion se ha activado para un dominio.

A continuación, puede eliminar correos de buzones de correo de Microsoft 365 de sus usuarios en el módulo **Email Live Tracking** (véase [Acciones para correos](#)).



Escaneo ATP

Con el escaneo ATP, los administradores puede analizar adicionalmente correos. El escaneo ATP se efectúa manualmente (véase [Iniciar el escaneo ATP](#) en la página 38) y comprueba correos con archivos adjuntos ejecutables en cuanto a contenido malicioso. En el proceso, el motor de sandbox analiza el correo seleccionado y elabora un informe detallado al respecto, el informe ATP (véase [Informe ATP](#) en la página 41).

El escaneo ATP también está disponible para clientes que no hayan contratado ATP. Sin embargo, el número de análisis mensuales está limitado para este tipo de clientes.

Como los correos de clientes de ATP ya se analizan automáticamente mediante el motor de sandbox (véase [Descripción de los motores de ATP](#) en la página 7), el escaneo ATP es para ellos, principalmente, una medida de seguridad adicional (p. ej., antes de la entrega manual de correos clasificados como **AdvThreat**). Además, con el informe ATP, los clientes de ATP obtienen información adicional.

Iniciar el escaneo ATP



Ha activado Advanced Threat Protection (véase [Activar ATP](#) en la página 14).

Con el escaneo ATP (véase [Escaneo ATP](#)) puede comprobar manualmente correos con archivos adjuntos ejecutables en cuanto a contenidos perjudiciales en el módulo **Email Security > Email Live Tracking** (véase [Email Live Tracking](#)).



Nota:

El escaneo ATP solo está disponible para correos con archivos adjuntos ejecutables (p. ej., archivos .exe). Los correos limpios ya entregados solo se pueden analizar con el escaneo ATP si los servicios Archiving o Continuity Service se encuentran activados.



ATENCIÓN:

Si no ha contratado Advanced Threat Protection (siehe [Estructura y funcionamiento de ATP](#)), podrá realizar dos escaneos ATP gratuitos al mes. Solo podrá efectuar más escaneos ATP después de contratar el servicio de pago de ATP.

1. Inicie sesión en Control Panel con sus datos de acceso.



2. Si, en lugar de sus propios correos, desea ver los correos de los usuarios de un dominio, seleccione el dominio en la selección de ámbitos.
3. Vaya al módulo **Email Security > Email Live Tracking**.
4. Haga clic en la flecha a la derecha de la fila del correo deseado.

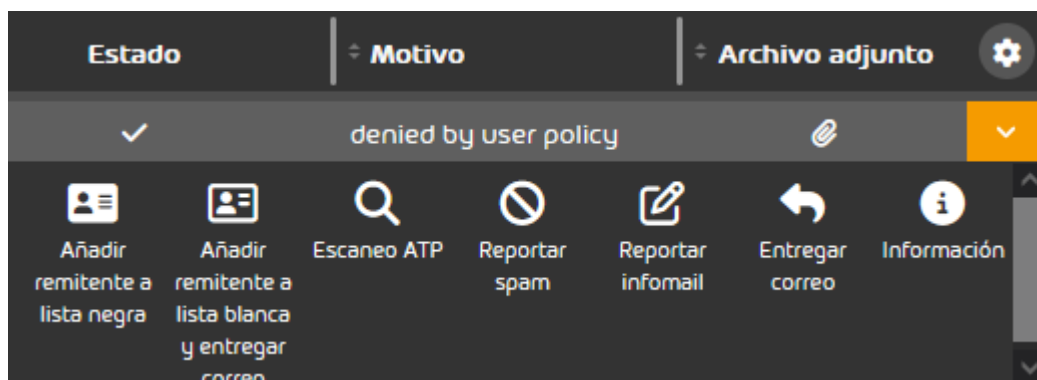


Figura 48: Análisis ATP en Email Live Tracking

- ➔ La vista de opciones avanzadas se abre.
5. Haga clic en **Escaneo ATP** para iniciar el escaneo.

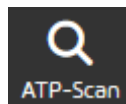


Figura 49: Iniciar el escaneo ATP

- ✓ Se ha iniciado el escaneo ATP para el correo.

Tan pronto como finalice el escaneo ATP, podrá consultar el informe ATP en la vista de opciones avanzadas del correo (véase [Informe ATP](#) en la página 41) desde **Escaneo ATP**.

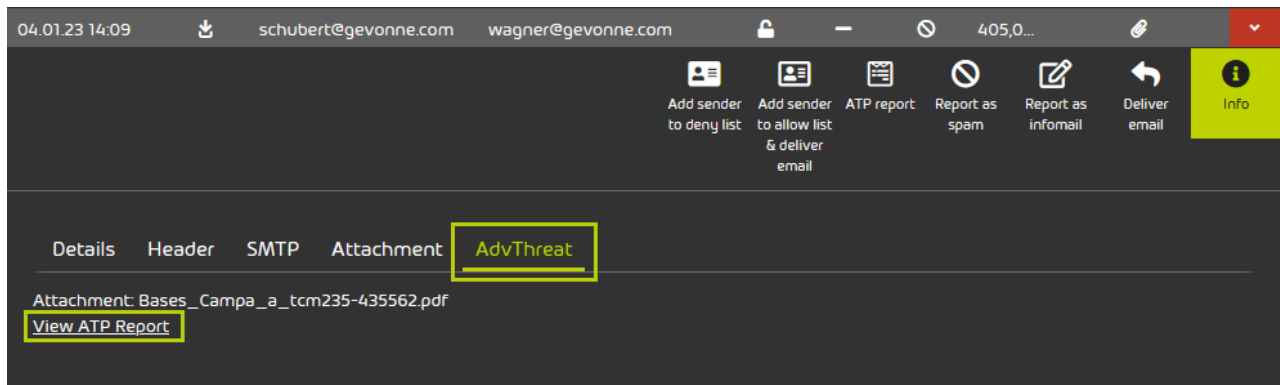


Figura 50: Consultar el informe ATP



Informe ATP

El informe ATP es un informe detallado que se genera tras analizarse un correo con el escaneo ATP (véase [Escaneo ATP](#) y [Iniciar el escaneo ATP](#) en la página 38). El informe ATP informa acerca del correo analizado. Los informes ATP están disponibles para los correos analizados en el módulo **Email Security > Email Live Tracking** (véase [#unique_23](#)). El informe ATP de un correo puede consultarse desde el punto de menú **Informe ATP** o **Información** de la pestaña **AdvThreat**.

El informe ATP se divide en cuatro ventanas principales:

Resumen

Aquí se muestra un resumen del archivo analizado. También se asigna al archivo una puntuación (**Score**) de 0 a 10. 0 significa que el archivo no comporta ningún riesgo, mientras que 10 es el nivel de riesgo más alto.

En la sección **Signatures** (firmas), el archivo se asigna a una de las siguientes categorías en función de su comportamiento:

- Información (verde)
- Atención (amarillo)
- Advertencia (rojo)

Si hace clic en una firma, se le mostrará información avanzada sobre el proceso.

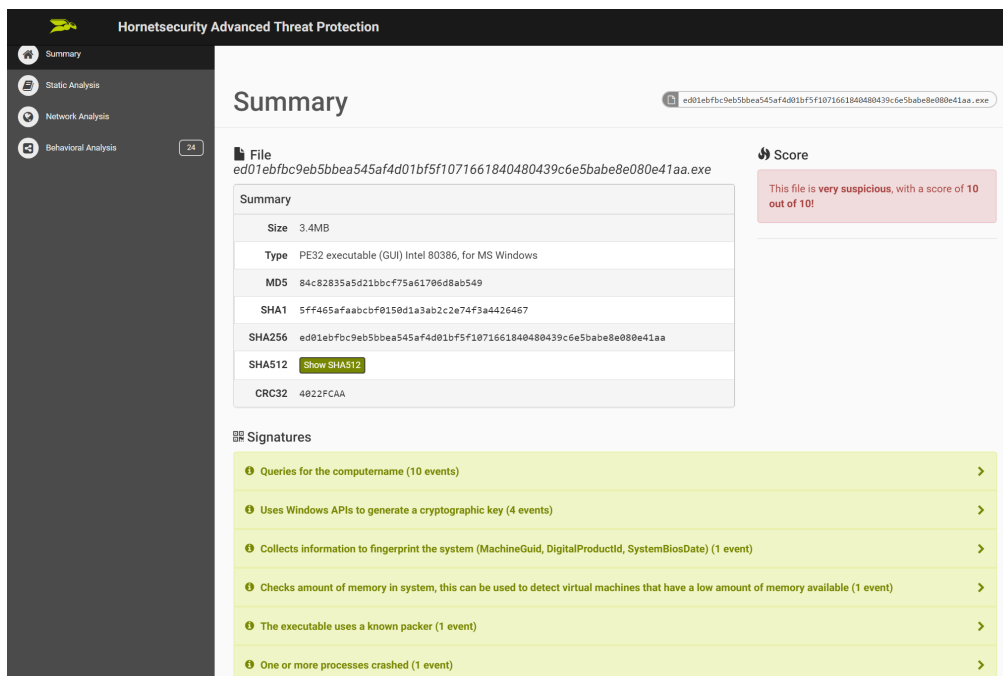


Figura 51: Resumen del informe ATP

Static Analysis

El análisis estadístico se divide, a su vez, en tres subcategorías:

- Static Analysis – Análisis estadístico del archivo. Depende del formato del archivo.
- Strings – Reproducción de las cadenas de caracteres del archivo.
- Antivirus – Análisis del archivo mediante diversos antivirus.

Network Analysis

En este análisis de red se analiza todo el tráfico de la red y se enumera por protocolos (p. ej., HTTP, TCP, UDP).

Behavioral Analysis

En el análisis de comportamiento se analiza el archivo en tiempo de ejecución.

Se muestran todas las llamadas a APIs y recursos del sistema registrados durante un análisis dinámico en sandbox.

Los resultados se dividen en dos secciones:



- Process Tree – Aquí se muestran los procesos en sucesión jerárquica.
- Process Contents – Si selecciona un proceso del "Process Tree", se le mostrarán aquí las llamadas a APIs ejecutadas en orden cronológico.

Índice

A

- activar
 - ATP [14](#)
 - Ex Post Deletion [34](#)
 - Secure Links [18](#)
- Advanced Threat Protection
 - explicación [5](#)
 - Ver también* ATP
- advertencias
 - explicación [3](#)
- añadir
 - destinatarios de notificaciones (ATP) [15](#)
- ATP [14](#)
 - activar [14](#)
 - explicación, *Ver* Advanced Threat Protection explicación

D

- descodificador
 - Secure Links [18](#)
- descodificador de enlaces
 - explicación [29](#)
- descodificar
 - enlace [30](#)
- destinatarios de notificaciones (ATP)
 - añadir [15](#)
 - eliminar [17](#)
- documentación
 - indicaciones [3](#)
 - símbolos [3](#)
- dominios
 - permitir ~ para Secure Links en Microsoft Defender, *Ver* Secure Links permitir dominios en Microsoft Defender
 - permitir ~ para Secure Links enviándolos a Microsoft, *Ver* Secure Links permitir dominios enviándolos a Microsoft
 - Secure Links, *Ver* Secure Links dominios

E

- eliminar
 - destinatarios de notificaciones (ATP) [17](#)
 - grupos de lista de grupos de TFFF [34](#)
- enlace
 - descodificar, *Ver* descodificar enlace
- enviar
 - dominios de Secure Links a Microsoft, *Ver* Secure Links permitir dominios enviándolos a Microsoft
- escaneo ATP
 - explicación [38](#)
 - iniciar [38](#)
- Ex Post Alert [12](#)
- Ex Post Deletion [12](#)
 - activar [34](#)

- explicación
 - advertencias [3](#)
 - descodificador de enlaces, *Ver* descodificador de enlaces explicación
 - indicaciones de seguridad [3](#)

G

- grupos
 - eliminar de la lista de grupos de TFFF [34](#)

I

- indicaciones
 - documentación [3](#)
- indicaciones de seguridad
 - explicación [3](#)
- informe ATP
 - explicación [41](#)
 - ver [38](#)
- iniciar
 - escaneo ATP [38](#)

M

- Microsoft Defender
 - permitir los dominios de Secure Links, *Ver* Secure Links permitir dominios en Microsoft Defender
- motores de ATP
 - funcionamiento [7](#)

N

- notificación [11](#)

S

- Secure Links
 - activar [18](#)
 - descodificador [18](#)
 - descodificador de enlaces, *Ver* descodificador de enlaces explicación
 - descodificar un enlace, *Ver* descodificar enlace
 - dominios [20](#)
 - permitir dominios en Microsoft Defender [20](#)
 - permitir dominios enviándolos a Microsoft [26](#)
- símbolos
 - documentación [3](#)

V

- ver
 - informe ATP [38](#)



HORNETSECURITY

Hornetsecurity GmbH
Am Listholze 78 | 30177 Hannover | Germany
Phone: +49 511 515 464-0 | info@hornetsecurity.com
www.hornetsecurity.com