

# Proofpoint Threat Response Auto-Pull

## Cuarentena automática del correo electrónico malicioso tras la entrega

### VENTAJAS PRINCIPALES

- Cuarentena automática de los mensajes de correo electrónico maliciosos que consiguen superar las soluciones de seguridad perimetrales
- Reducción exponencial del tiempo que necesitan los equipos de seguridad y mensajería cuando revisan la organización y la respuesta de seguridad del correo
- Empleo de la inteligencia de amenazas de Proofpoint para la clasificación de los mensajes
- Monitorización automática de los buzones de correo malicioso para detectar amenazas
- Cuarentena de los mensajes reenviados a individuos o listas de distribución
- Seguimiento de las campañas de phishing con algunas denuncias y eliminación de la pérdida de tiempo derivado de mensajes denunciados por error

Más del 90 % de las violaciones de seguridad comienzan por un mensaje de correo electrónico, que es el principal vector de ataque. Las amenazas por correo electrónico siguen evolucionando, por lo que las organizaciones estarán expuestas a más mensajes maliciosos. Los mensajes de correo electrónico maliciosos pueden contener enlaces de phishing que se hacen venenosos una vez entregados, o bien usar técnicas de evasión que generan falsos negativos y, por lo tanto, son entregados a los usuarios. Los equipos de seguridad del correo electrónico deben ocuparse con frecuencia del análisis y la limpieza del correo electrónico para reducir la exposición a amenazas y limitar los daños potenciales. Poner en cuarentena un mensaje de correo electrónico puede ser una tarea sencilla, a la que hay que dedicar entre 10 y 15 minutos, pero cuando se trata de diez mensajes o más, la tarea puede complicarse y requerir mucho más tiempo.

### Cuarentena automática del correo electrónico malicioso tras la entrega

Proofpoint Threat Response Auto-Pull (TRAP) permite a sus administradores de mensajería y seguridad simplificar el proceso de respuesta a los incidentes relacionados con el correo electrónico. Cuando se detecta un mensaje malicioso, TRAP analiza automáticamente el correo electrónico y elimina los mensajes maliciosos. Además, coloca en cuarentena los mensajes de correo electrónico no deseados que han llegado a las bandejas de entrada de los usuarios. Con TRAP, dispone de una potente solución que reduce significativamente el tiempo que necesitan sus equipos de seguridad y mensajería para limpiar el correo electrónico.

### Inteligencia sobre amenazas de clase empresarial

La inteligencia de amenazas de Proofpoint cubre muchos vectores de amenaza: el correo electrónico, las redes sociales, los dispositivos móviles, la nube y la red. Por eso nos ofrece una visibilidad única de las últimas amenazas y tácticas empleadas por los atacantes en la actualidad. Con TRAP, puede aprovechar la inteligencia de amenazas de Proofpoint, así como la que aportan otros sistemas, como STIX/TAXII, WHOIS, VirusTotal, Soltra y MaxMind. Todo esto le permite conocer el "quién,

qué y dónde" de los ataques, así como organizar y clasificar por prioridades los eventos entrantes, y librarse de las tareas repetitivas.

Cuando se detecta un mensaje de correo electrónico, la información se completa con la inteligencia de los diversos sistemas mencionados. A continuación, se crean asociaciones entre los destinatarios y las identidades de usuarios, se revelan campañas relacionadas, e incluso se descubren las direcciones IP y dominios del ataque. De esta forma obtiene una clasificación extremadamente precisa de los mensajes, y sus equipos de seguridad pueden centrarse en otras tareas, en lugar de tener que investigar manualmente cada mensaje detectado.

### Identificación y reducción del riesgo de phishing con CLEAR

Un empleado informado puede ser su última línea de defensa frente a un ciberataque. Con Closed-Loop Email Analysis and Response (CLEAR), el ciclo de denuncia, análisis y corrección de mensajes potencialmente maliciosos pasa de durar días a completarse en solo unos minutos. CLEAR, enriquecido con la inteligencia de amenazas de Proofpoint, detiene de raíz los ataques activos con solo un clic. Y su equipo de seguridad puede ahorrar tiempo y esfuerzo, ya que los mensajes maliciosos se ponen en cuarentena automáticamente.

Con CLEAR, dispone de una solución completa que combina las funciones de PhishAlarm, el botón de denuncia del correo electrónico, PhishAlarm Analyzer, que clasifica por categorías y prioridades mediante la inteligencia de amenazas de Proofpoint, y TRAP, para el enriquecimiento de los mensajes y la corrección automática de los mensajes maliciosos.

Los mensajes denunciados se envían a un buzón de correo malicioso para utilizar CLEAR y se supervisan y procesan con TRAP de la misma forma. A continuación, se analizan comparándolos con la inteligencia de amenazas de Proofpoint y otras obtenidas de terceros, con el fin de determinar si hay algo en el contenido que coincida con marcadores maliciosos. Los mensajes se retiran automáticamente de la bandeja de entrada del destinatario.

### Administración del correo electrónico fuera de banda

TRAP también emplea archivos CSV y Proofpoint SmartSearch. Los usuarios pueden cargar los resultados de SmartSearch o archivos CSV, o utilizar incidentes manuales con algunos datos clave para iniciar una acción de cuarentena para uno o miles de mensajes de correo electrónico. Las amenazas de seguridad, así como los mensajes que infringen las directivas, pueden retirarse de los buzones de correo rápidamente. Además, se muestra una lista de actividades que indica quién lee los mensajes y si el intento de retirada del mensaje de correo electrónico ha funcionado.

### Cuarentena automática de mensajes reenviados

Los mensajes de correo electrónico maliciosos y no deseados pueden reenviarse a otras personas, departamentos o listas de distribución. Intentar retirar estos mensajes tras la entrega es siempre una tarea complicada para muchos administradores. TRAP soluciona esta situación con lógica e inteligencia empresarial incorporada que reconoce cuándo se reenvían o envían los mensajes a listas de distribución. A continuación, examina automáticamente y sigue el rastro de los destinatarios para localizar y retirar dichos mensajes. Todo esto le ahorra tiempo y frustración.

## MÁS INFORMACIÓN

Para obtener más información, visite [proofpoint.com/es](https://www.proofpoint.com/es).

#### ACERCA DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) es una compañía líder en ciberseguridad que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentran más de la mitad del Fortune 1000, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en [www.proofpoint.com/es](https://www.proofpoint.com/es).

©Proofpoint, Inc. Proofpoint es una marca comercial de Proofpoint, Inc. en Estados Unidos y en otros países. Todas las marcas comerciales mencionadas en este documento son propiedad exclusiva de sus respectivos propietarios.