Proofpoint Advanced Email Security

Proteja frente a las amenazas avanzadas por correo electrónico, optimice las operaciones y disfrute de una visibilidad procesable de los riesgos asociados a los usuarios y de su panorama de amenazas

Productos

- Proofpoint Email Protection
- Proofpoint TAP
- Proofpoint TRAP
- Proofpoint Email Isolation
- Proofpoint Browser Isolation
- Proofpoint Security Awareness Training
- Proofpoint Email Fraud Defense
- Proofpoint Internal Mail Defense
- Proofpoint Email Encryption
- Proofpoint Email DLP

Ventajas principales

- Bloqueo de los intentos de estafa por correo electrónico y de los mensajes que contienen URL peligrosas, adjuntos maliciosos y ransomware, o que intentan estafas por correo electrónico.
- Neutralización automática de los mensajes denunciados por los usuarios o activados después de la entrega gracias a flujos de trabajo integrados.
- Visibilidad inigualable de sus empleados, las amenazas y los riesgos asociados a los proveedores y a la nube, entre otros.
- Despliegue sencillo de políticas DMARC y aplicación rápida y segura de la autenticación para bloquear los mensajes fraudulentos que falsifican dominios de confianza.
- Formación y capacitación de sus usuarios para convertirlos en una sólida línea de defensa frente a las ciberamenazas.

En la actualidad, el correo electrónico es un elemento fundamental para las empresas, pero también es el principal vector de amenazas. Y los ataques por correo electrónico (phishing, estafas Business Email Compromise o BEC, ataques a la cadena de suministro y compromiso de cuentas de correo electrónico) evolucionan constantemente. Por tanto, proteger eficazmente contra este vector de amenazas ha demostrado ser una tarea abrumadora, incluso para las organizaciones más importantes y complejas. Proofpoint puede ayudarle.

Nuestra solución de protección avanzada del correo electrónico se despliega en un número de organizaciones de las listas Fortune 100, Fortune 1000 y Global 2000 superior al de cualquier otro proveedor. Para hacer frente a este desafío, nuestra solución adopta un enfoque en línea y basado en API. Esto garantiza una protección total de todos los mensajes entrantes y salientes. No solo se centra en los mensajes de correo electrónico que pasan por alto las soluciones de seguridad tradicionales. Nuestro enfoque multicapa integrado reduce el riesgo de ataques que consiguen su objetivo gracias a que detecta las amenazas de manera más rápida y precisa. Nuestras funciones de detección líderes y nuestra plataforma escalable le permiten aumentar su eficacia operativa. Gracias a información procesable, puede comprender mejor los posibles riesgos, anticiparse y responder de manera más rápida y eficaz.

Detección y bloqueo de amenazas avanzadas

Eficacia fiable

La inteligencia de amenazas y las funciones de detección de Proofpoint le ofrecen una defensa sólida contra las amenazas sofisticadas, y le permitirán reducir los falsos positivos.

Utilizamos herramientas de análisis de la reputación, de reescritura de URL y de entorno aislado (sandbox) predictivo y al hacer clic para detectar las amenazas con payload, como las que se distribuyen a través de adjuntos y de URL. La detección de técnicas de evasión y ocultación como los CAPTCHA y los enlaces protegidos mediante contraseñas, de sitios de mucha carga, de redireccionadores y de sitios web para compartir archivos viene integrada.

También utilizamos los modelos de inteligencia artificial (IA) y de aprendizaje automático del gráfico de amenazas Nexus para detectar ataques sin payload (carga maliciosa), como los ataques BEC. Estos modelos evalúan señales como

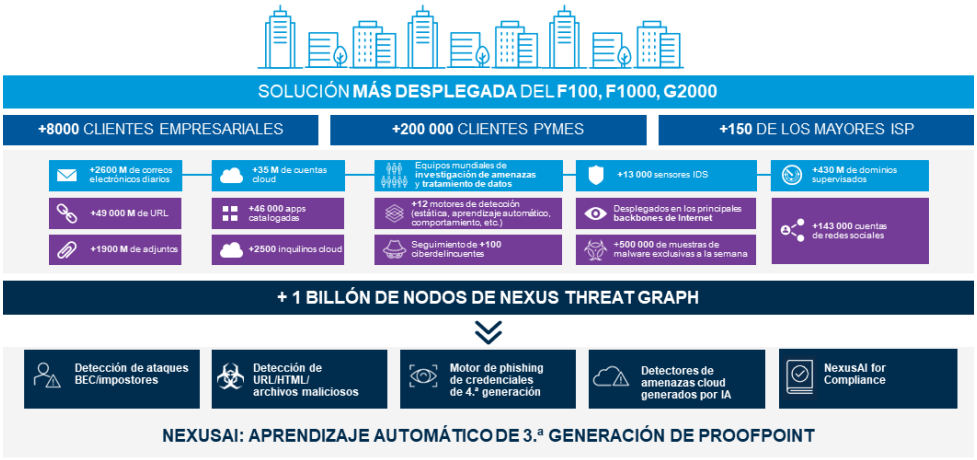

Figura 1: Gráfico de amenazas Nexus.

En el panorama actual de amenazas centradas en las personas, los usuarios son su mayor activo, y también su mayor riesgo.

los riesgos asociados a los proveedores, señales de usuarios de suites de colaboración, el procesamiento de lenguaje natural de contenido, las relaciones remitente/destinatario y las intenciones. Los datos de referencia y contextuales nos permiten detectar mensajes de correo electrónico potencialmente maliciosos. Se complementan perfectamente con nuestra inteligencia de amenazas y otros motores de detección dirigidos, lo que permite minimizar los falsos positivos.

Analizamos los mensajes de correo electrónico con herramientas de análisis de contenido, de análisis de la reputación y de entorno aislado (sandbox). Esto detiene eficazmente las amenazas avanzadas del correo electrónico, como el malware polimórfico y el ransomware, antes de que alcancen a los usuarios. También se proporciona análisis en entorno aislado de las URL, tanto predictivo como al hacer clic, para detectar y bloquear los enlaces maliciosos. La reescritura de URL protege a sus usuarios en cualquier red y dispositivo. También permite detectar si un mensaje se ha modificado con una carga maliciosa después de su entrega.

Clics con total seguridad gracias al aislamiento del correo electrónico y del navegador

Proofpoint Browser Isolation y Proofpoint Email Isolation ofrecen un entorno seguro, que permite a los usuarios acceder a sitios web, al correo web personal y al correo electrónico corporativo con seguridad. Los ciberdelincuentes recurren a distintas tácticas y vectores de amenazas para conseguir acceder a sus sistemas, como el compromiso de las cuentas de proveedores. Por ejemplo, pueden atacar a sus usuarios a través del correo electrónico personal o de canales desprotegidos. El aislamiento le permite desactivar las cargas y descargas. También puede restringir la entrada de datos mientras se analiza un sitio web en tiempo real. Esta operación se realiza en cuestión de segundos. La tecnología añade una capa de protección adicional para impedir el robo de credenciales, el malware o el ransomware. Resulta especialmente útil contra los mensajes de phishing que contienen direcciones URL infectadas una vez entregados.

Prevención de estafas con la autenticación del correo electrónico

La autenticación del correo electrónico añade una capa adicional de protección. Ha demostrado ser una forma eficaz de detener las amenazas de impostores sin malware, como los ataques BEC. Sin embargo, las organizaciones dudan a la hora de adoptar y aplicar estándares de autenticación DMARC por el riesgo de bloqueo del correo electrónico legítimo.

Proofpoint le ayuda a desplegar y aplicar la autenticación DMARC con total confianza, sin bloquear el flujo de correo legítimo. Protege frente al "domain spoofing" (suplantación de dominios) y a los mensajes fraudulentos que utilizan dominios de confianza. Detiene los mensajes de correo electrónico fraudulentos en el gateway de Proofpoint y al mismo tiempo protege la identidad del correo de su empresa.

Y lo que es más importante, puede ver todas las amenazas de impostores, incluidos los "looklike domains" (dominios parecidos) maliciosos, desde un único panel. Dispondrá de esta visibilidad con independencia de la táctica empleada o la víctima elegida. Con nuestro servicio Virtual Takedown, puede impedir proactivamente ataques por correo electrónico de dominios parecidos fraudulentos antes de que se produzcan. Simplificamos su despliegue de la autenticación DMARC con un asesor experto que le guiará por cada paso del proceso. Colaboramos con usted para identificar a todos sus remitentes de confianza, incluidos los externos, para garantizar su correcta autenticación. Proofpoint ha ayudado a más de un tercio de las organizaciones de la lista Fortune 1000 en este proceso. Podemos trabajar con las configuraciones más sofisticadas.

Protección del correo interno y contención rápida de las amenazas

La protección del correo interno es tan crucial como la del entrante. Los atacantes usan cuentas comprometidas para enviar phishing, ataques BEC o malware. Analizamos el correo interno buscando contenido malicioso en forma de URL y adjuntos. Cuando detectamos un mensaje interno malicioso, puede extraerlo y ponerlo en cuarentena automáticamente. Puede hacerlo incluso si otros usuarios ya han recibido el mensaje y lo han reenviado a otros. También ofrecemos informes que indican las cuentas que pueden haber sido comprometidas, lo que le permite actuar rápidamente.

Visibilidad de los ataques y de la superficie de ataque humana

Para reducir mejor los riesgos y su comunicación a los directivos, debe conocer lo siguiente:

- Los usuarios de mayor riesgo y las técnicas de ataques empleadas
- El panorama de amenazas, los objetivos, los ciberdelincuentes y las tendencias
- Otros indicios como los riesgos asociados a los proveedores y a la nube

Proofpoint proporciona todos estos datos y muchos más. Gracias a nuestro enfoque de plataforma, obtiene un conocimiento completo del riesgo asociado a las personas, sin silos de datos. Le ofrecemos las herramientas necesarias para ser más proactivo frente a las amenazas sofisticadas.

Reducción de riesgos con datos basados en las personas

En el panorama actual de amenazas centradas en las personas, los usuarios son su mayor activo, pero también su mayor riesgo. Ofrecemos una visibilidad inigualable de los ataques dirigidos y de la superficie de ataque que constituyen sus empleados.

Le mostramos quién presenta mayor riesgo para su organización y le explicamos por qué. Nuestro informe sobre sus VAP (Very Attacked People™, o personas muy atacadas) indica cuáles son los usuarios que reciben más ataques. Nuestro informe de usuarios más incautos le muestra qué usuarios han hecho clic en mensajes maliciosos reales. Puede introducir y controlar a sus VIP en el panel. Con esos datos, puede implementar controles adaptables para los usuarios de riesgo a fin de darles prioridad y reducir los riesgos. Estos controles pueden incluir información dirigida de concienciación en seguridad, aislamiento del navegador y autenticación multifactor.

Recepción de información centrada en las amenazas para disponer de contexto

Proporcionamos en tiempo real información forense detallada sobre las amenazas y las campañas. Nuestro análisis de amenazas en profundidad le mostrará toda la información necesaria: usuarios atacados, origen del ataque, así como los métodos y su desarrollo. También determinamos el objetivo del ataque. (Podemos averiguar, por ejemplo, si su objetivo era filtrar datos, instalar ransomware, o cometer fraude). Establecemos la relación entre los ataques de correo electrónico y los inicios de sesión sospechosos, con objeto de identificar e impedir más eficazmente el compromiso de cuentas. Nuestra plataforma le permite comparar los tipos de amenazas y los objetivos de los ciberdelincuentes que le atacan, así como los que atacan a empresas como la suya.

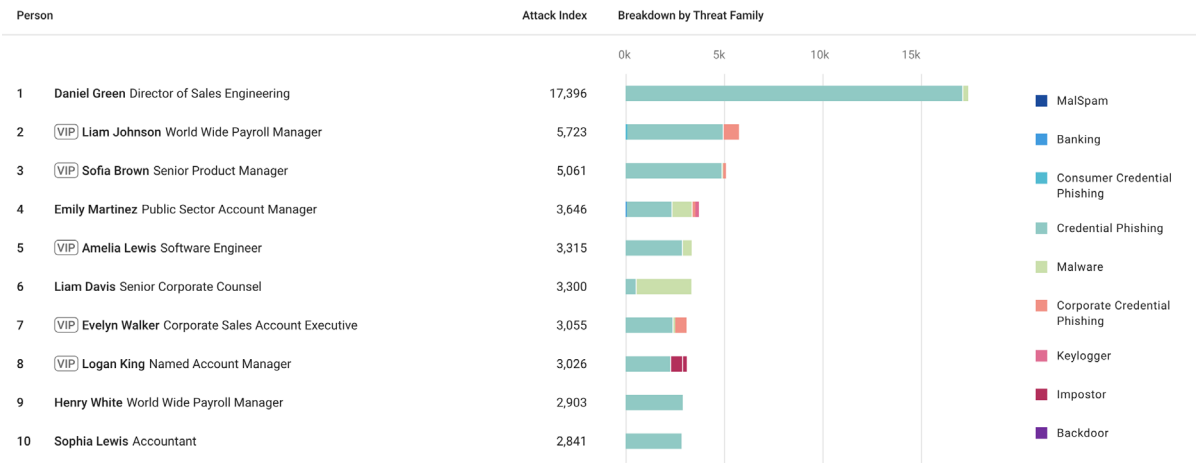

Figura 2: El informe Very Attacked People (VAP) de Proofpoint muestra los usuarios que presentan el mayor riesgo y los tipos de amenazas a las que se enfrentan.

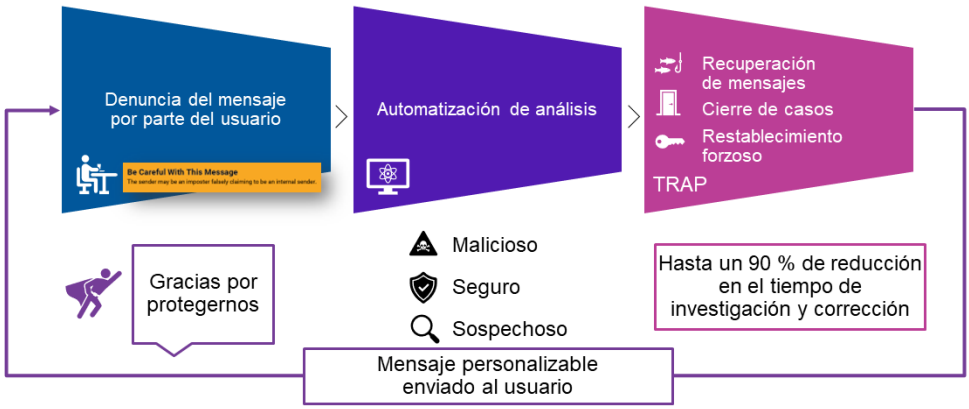

Figura 3: La solución de gestión automatizada del buzón de correo malicioso de Proofpoint Closed-Loop Email Analysis and Response (CLEAR).

Integración de información sobre los riesgos de compromiso de cuentas cloud y los asociados a proveedores

Ofrecemos visibilidad de los riesgos de compromiso de cuentas y de los asociados a proveedores. Esta visibilidad le permite neutralizar completamente los ataques complejos. Nexus Supplier Risk Explorer nos permite identificar automáticamente los proveedores potencialmente comprometidos, así como los dominios que utilizan para enviar correo electrónico a sus usuarios. Y con la función SaaS Defense integrada, puede obtener información sobre los usuarios potencialmente comprometidos, los archivos maliciosos o expuestos y las aplicaciones de terceros en riesgo.

Mejora de la eficacia operativa

Muchas organizaciones sufren carencias de personal en sus equipos de seguridad o bien están sobrecargados. Estos equipos a menudo tienen que gestionar varios proveedores y productos de seguridad, que no siempre se comunican entre sí. Nosotros le ofrecemos una solución integrada que se centra en las amenazas que importan y que automatiza la detección y neutralización de amenazas. Esto ahorra tiempo y dinero, ya que los equipos de seguridad pueden dedicar menos recursos internos a la corrección que si utilizaran soluciones de la competencia.

Extracción automática de los mensajes maliciosos

Nuestra solución permite eliminar las tareas manuales y las conjeturas asociadas a la respuesta a incidentes. Esto ayuda a corregir las amenazas con mayor rapidez y eficacia. Eliminamos mensajes de phishing que contienen URL infectadas una vez entregados. Y podemos eliminar (con un solo clic o automáticamente) todos los mensajes no deseados de las cuentas internas que están comprometidas, incluso si se reenviaron o los recibieron otros usuarios. Además, nuestro gráfico de amenazas Nexus proporciona alertas y recopila y compara automáticamente datos forenses. Esto le ofrece una vista procesable de las amenazas. Gracias a nuestro enfoque podrá reducir el tiempo de corrección de mensajes correo electrónico hasta en un 90 %.

Optimización del proceso del buzón de correo malicioso

Le ayudamos a optimizar el proceso del buzón de correo malicioso y a reducir la carga de trabajo para el personal de TI. Los usuarios pueden denunciar fácilmente los mensajes sospechosos con un solo clic, bien directamente desde una etiqueta de advertencia de correo electrónico o mediante el complemento (add-on) de denuncia de correo electrónico PhishAlarm®. Si el mensaje denunciado se considera malicioso, este y todas sus copias se ponen en cuarentena automáticamente. Y los usuarios reciben un mensaje personalizado en el que se les informa de que el mensaje era malicioso. Esto anima a denunciar mensajes como ese en el futuro. Los administradores pueden obtener informes detallados del comportamiento de los usuarios y comparar la precisión de la denuncia de mensajes maliciosos en comparación con empresas del sector.

Modificación del comportamiento con educación basada en amenazas

Las amenazas modernas del correo electrónico requieren que las personas las activen. Sin embargo, los empleados no tienen por qué ser el eslabón débil de su ciberdefensa. De hecho, con un nivel adecuado de concienciación en seguridad, pueden convertirse en una línea sólida de defensa frente a ciberataques.

Proofpoint le permite tomar medidas respecto a sus VAP o a los usuarios con mayor tendencia a hacer clic. Los datos recopilados sobre ellos se integran automáticamente en nuestra plataforma de concienciación en seguridad. La plataforma utiliza estos datos para elaborar un programa de formación más dirigido y eficaz. Le permite utilizar simulaciones de ataques de phishing realistas a partir de la inteligencia sobre amenazas de Proofpoint para crear experiencias de formación pertinentes. Los usuarios que caen en la trampa de un ataque simulado reciben formación que denominamos "enseñanza a tiempo" (o "just-in-time teaching"). En caso necesario, puede inscribirlos en módulos de formación específicos. También facilitamos a los usuarios etiquetas de advertencias de correo electrónico, que incluyen el botón "Report Suspicious" (Denunciar como sospechoso). Estas etiquetas incluyen descripciones cortas personalizadas y vistas del riesgo asociado a un mensaje determinado, y permiten a los usuarios denunciar los mensajes directamente desde la etiqueta. De esta manera los usuarios pueden tomar decisiones más informadas al respecto. Estas funciones son compatibles con todos los dispositivos y aplicaciones.

Protección frente a la pérdida de datos por correo electrónico

El correo electrónico es el principal vector tanto de entrada de amenazas como de pérdida de datos. Por lo tanto, debe proteger sus datos confidenciales y prevenir su pérdida por correo electrónico. Para prevenir la pérdida de datos accidental o intencionada durante las comunicaciones por correo electrónico, le ofrecemos visibilidad instantánea e imposición de normas. La prevención de la pérdida de datos (DLP) y el cifrado del correo electrónico están estrechamente integrados. Pueden gestionarse de manera centralizada en la plataforma Proofpoint Information and Cloud Security. Con el nuevo administrador de alertas centralizado, puede personalizar las exploraciones listas para utilizar, detectar y denunciar las infracciones de DLP más importantes para usted. Simplifique las operaciones con flujos de trabajo optimizados y funciones de corrección. También se realiza un análisis de la información confidencial que pueda haber en los datos tanto estructurados como sin estructurar, además de ofrecerse políticas perfectamente configuradas y diccionarios predefinidos. De esta forma se identifica automáticamente la información protegida por la legislación oficial y de privacidad de los datos. Asimismo, le ayudan a cumplir diversas normas de protección de datos, como PCI DSS, SOX, HIPAA o RGPD, y reducen el trabajo manual. Si se combinan con cifrado, es posible definir y personalizar políticas propias para cifrar automáticamente los datos confidenciales en el correo electrónico. De esta manera, es fácil gestionar y proteger el intercambio de información confidencial.

Resumen

Proofpoint Advanced Email Security protege eficazmente frente a las amenazas contra el correo electrónico. Además, le ofrece visibilidad práctica de los ataques y de las personas más atacadas. Nuestra solución:

- Bloquea las amenazas avanzadas antes de que se distribuyan.
- Proporciona visibilidad de los riesgos asociados a las personas, las amenazas y otros datos.
- Mejora la eficacia operativa gracias a la respuesta automatizada a las amenazas.
- Forma y contribuye a convertir a los usuarios en una sólida línea de defensa.
- Protege frente a la pérdida de datos por correo electrónico.

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas 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 encuentra el 75 % del Fortune 100, 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**.