proofpoint.

Proofpoint Threat Protection

Proteja a sus empleados frente a las amenazas modernas actuales

Ventajas principales

- Detenga y bloquee más rápidamente las amenazas avanzadas por correo electrónico.
- Bloquee las amenazas emergentes con mayor precisión con inteligencia artificial continua.
- Obtenga información sobre sus riesgos asociados a las personas y de amenazas.
- Mejore de la eficacia operativa.
- Capacite a sus empleados e impulse un cambio de comportamiento.

El correo electrónico es el principal vector de ciberamenazas, y en la actualidad hay muchas campañas de malware, phishing e ingeniería social dirigidas contra sus empleados. Según el informe de Verizon sobre las investigaciones de fugas de datos de 2023, en el 74 % de las fugas de datos intervino el factor humano[1]. Con Proofpoint Threat Protection, su organización puede proteger a sus empleados frente a las amenazas modernas actuales.

La ciberdelincuencia es un negocio al alza

La ciberdelincuencia es un negocio en expansión por su alta rentabilidad y bajo riesgo. Según Cybersecurity Ventures, se prevé que el coste de la ciberdelincuencia alcance los 10,5 billones de dólares anuales en 2025[2]. Las organizaciones ciberdelictivas se asemejan a las empresas tradicionales en su objetivo principal: obtener beneficios económicos. Los ciberdelincuentes persiguen apoderarse de la información personal y corporativa, robar identidades y lanzar ataques destinados a cometer fraudes financieros a través del correo electrónico. Y dado que el correo electrónico es una piedra angular fundamental de la empresa moderna, es el principal vector de amenazas contra sus empleados. Además, estas amenazas evolucionan constantemente y son difíciles de defender. Por eso, proteger a sus empleados frente a estas amenazas modernas es una tarea de enormes proporciones, incluso para las organizaciones más sofisticadas y complejas. Pero Proofpoint puede ayudarle.

1 Verizon. *2023 Data Breach Investigations Report* (Informe sobre investigaciones de fugas de datos de 2023), 2023.
2 Steve Morgan *(revista sobre ciberdelincuencia)*. "Cybercrime To Cost The World 10.5 Trillion Annually By 2025" (La ciberdelincuencia costará al mundo 10,5 billones de dólares al año hasta 2025), noviembre de 2020.

Este conjunto de soluciones forma parte de la plataforma Human-Centric Security, que mitiga las cuatro principales áreas de riesgo asociado a las personas.

84 %

de las empresas Fortune 100 confían en Proofpoint para proteger a sus empleados frente a las amenazas.

Fuente: Proofpoint, 2023

Detecte y bloquee más rápidamente las amenazas por correo electrónico con detección antes de la entrega

Gracias a nuestra protección antes de la entrega, puede identificar y bloquear amenazas conocidas y desconocidas en toda la empresa. Esto significa que las amenazas sofisticadas se detienen en la puerta de entrada, no después de que lleguen. Estas amenazas son:

- Phishing de credenciales avanzado
- Malware
- Ransomware
- Estafas Business Email Compromise (BEC)
- URL maliciosas
- Códigos QR
- Adjuntos
- Y muchas más

Cuando esto se combina con nuestra detección y corrección automatizadas después de la entrega, su organización puede proteger de forma global a sus empleados con una única solución integral.

Identifique amenazas con detección multicapa basada en IA

Utilizamos un pila de detección multicapa compuesta por inteligencia de amenazas, aprendizaje automático, IA basada en el comportamiento, detección en entorno aislado (sandbox), análisis de contenido y semántico (LLM). Estas funciones trabajan de manera conjunta para detectar varios tipos de amenazas modernas. El resultados es que la pila proporciona una tasa de detección de enorme fiabilidad (99,99 %) con una mejor explicabilidad de amenazas. Y a diferencia de las soluciones de seguridad del correo electrónico de detección en una sola capa, genera menos falsos negativos y menos falsos positivos porque puede detener con mayor precisión los mensajes maliciosos sin bloquear los mensajes fiables y obstaculizar su negocio.

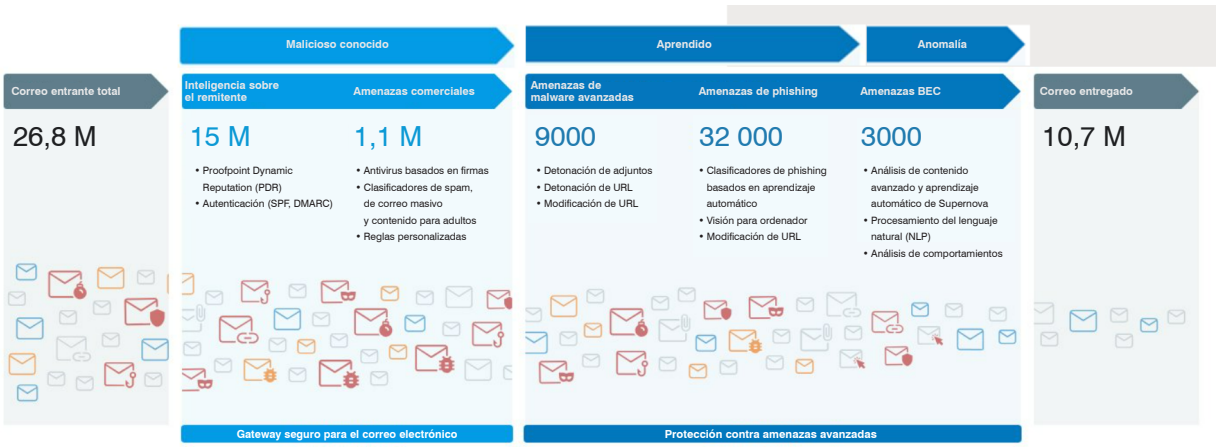

Figura 1. Protección multicapa basada en IA de Proofpoint en acción.

Consiga visibilidad integral de las amenazas y los riesgos asociados a las personas

Con Proofpoint, obtiene información exclusiva sobre sus VAP (Very Attacked People™, o personas muy atacadas) y las amenazas que les afectan específicamente. De este modo, puede implementar controles adaptables específicos, como el aislamiento del navegador, la formación para concienciar en materia de seguridad, la autenticación reforzada y mucho más. Y combinada con nuestra visibilidad del riesgo asociado a las personas, obtendrá una información enormemente valiosa sobre sus empleados: cuántos reciben ataques, su nivel de vulnerabilidad y los privilegios de los que disponen. Además, Proofpoint analiza más de 3 billones de mensajes de correo electrónico al año en nuestro ecosistema de más de 230 000 clientes, partners y proveedores. Nuestra inteligencia de amenazas e investigación le proporcionan datos de alerta temprana sobre nuevas amenazas previamente desconocidas que afectan a tus usuarios.

Mejore la eficacia operativa

Con Proofpoint, puede detectar y corregir automáticamente los mensajes de correo electrónico maliciosos después de su entrega. Esta automatización del proceso de clasificación y eliminación de mensajes que contienen payloads engañosas le ayuda a identificar y resolver las amenazas con mayor rapidez y eficacia. Si estos correos electrónicos no deseados proceden de cuentas comprometidas internamente o han sido reenviados o recibidos por otros usuarios, Proofpoint le proporciona alertas automatizadas, análisis comparativos de amenazas y vistas procesables de las amenazas. Esto reduce el tiempo de corrección. También aligera la carga de trabajo de su equipo, haciéndolo más eficiente. Además, los usuarios pueden denunciar fácilmente los mensajes sospechosos con un solo clic desde una etiqueta de advertencia de correo electrónico o un botón de denuncia de mensajes de phishing. Si un mensaje denunciado por un usuario resulta ser malicioso, este y todas las demás copias se ponen en cuarentena automáticamente. A su vez, los usuarios reciben una notificación por correo electrónico que les informa de que el mensaje era malicioso y se elimina automáticamente. Esta notificación en bucle cerrado ayuda a reforzar el comportamiento futuro para denunciar mensajes similares.

Capacite a sus empleados e impulse un cambio de comportamiento

Proofpoint le ayuda a mitigar aún más los riesgos que corren sus empleados cambiando los comportamientos inseguros y creando hábitos de seguridad sostenibles. Utilizamos nuestra rica inteligencia sobre amenazas para informar a su programa de varias maneras, entre las

Figura 2. Proofpoint ofrece visibilidad de sus VAP (Very Attacked People™ o personas muy atacadas).

que se incluyen el diseño de simulaciones de phishing reales, la formación guiada basada en amenazas que le permite educar a los usuarios más propensos a hacer clic y a los más atacados, y la automatización de la investigación de amenazas del correo electrónico denunciado por los usuarios. Le ayudamos a garantizar la participación de los usuarios ofreciéndole experiencias de aprendizaje personalizadas. Nuestro enfoque adaptable ayuda a sus empleados a retener lo que aprenden y a cultivar hábitos de seguridad positivos y duraderos. Y le permitimos comunicar mejor el riesgo asociado a sus empleados y el impacto del programa a su equipo directivo mediante el seguimiento del cambio de comportamiento en el mundo real y la evaluación comparativa con otras empresas como la suya.

Oferta de servicios gestionados de Proofpoint

Proofpoint proporciona los siguientes servicios gestionados para Proofpoint Threat Protection:

- **Managed Email Threat Protection**: disfrute de experiencia proactiva, continuidad del personal y conocimientos ejecutivos mediante la gestión práctica de su solución de seguridad del correo electrónico. También le proporcionamos comprobaciones operativas diarias y la aplicación proactiva de inteligencia sobre amenazas.
- **Managed Abuse Mailbox:** reduzca la carga de las revisiones manuales de los mensajes de correo electrónico denunciados por los usuarios. Nuestro equipo realiza análisis y asigna resoluciones definitivas a todos los mensajes denunciados no clasificados.
- **Managed Security Awareness:** mejore y adapte su enfoque de la formación en seguridad de los usuarios. Orientamos la estrategia de su programa centrándonos en el cambio de comportamiento y en la creación de una cultura de seguridad más resiliente.

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

MÁS INFORMACIÓN

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

0203-007-06-01 3/24