

Proofpoint Targeted Attack Protection

Consiga visibilidad y protección frente a amenazas avanzadas

Ventajas principales

- Detecte, analice y bloquee las amenazas avanzadas antes de que lleguen a la bandeja de entrada.
- Disfrute de información adecuada para identificar sus VAP (Very Attacked People™, o personas muy atacadas) de la empresa TM y los riesgos para la seguridad.
- Aproveche el sistema de inteligencia sobre amenazas de Proofpoint para proteger frente a amenazas y recibir análisis forenses de los ataques.
- Implemente controles de seguridad adaptables mediante funciones de aislamiento de URL y formación para concienciar en materia de seguridad.
- Permita a los VAP navegar con confianza por sitios web desconocidos a través del correo electrónico corporativo, garantizando al mismo tiempo su protección frente a ataques basados en URL y la web. Esta función forma parte de nuestros bundles de soluciones.

Más del 90 % de los ataques comienzan por la recepción de un mensaje de correo electrónico. Además, estas amenazas evolucionan constantemente. Proofpoint Targeted Attack Protection (TAP) ofrece un enfoque innovador para detectar, analizar y bloquear las amenazas avanzadas dirigidas contra los empleados de la empresa. Ofrece además una visibilidad inigualable de estas amenazas, que le permite optimizar la respuesta.

TAP detiene tanto los ataques por correo electrónico conocidos como los emergentes. Detecta y bloquea el malware polimórfico, los documentos con carga maliciosa, el phishing de credenciales y otras técnicas avanzadas. Supervisa la actividad de las apps cloud para identificar inicios de sesión sospechosos, exceso de uso compartido de archivos, aplicaciones de terceros de riesgo, etc. Además, le proporciona la información que necesita para identificar y proteger a las personas más atacadas dentro de su empresa.

Protección frente a amenazas BEC, basadas en la nube y a través de adjuntos y URL

Proofpoint TAP emplea técnicas estáticas y dinámicas para detectar los nuevos patrones de ataque y adaptarse en todo momento. Analizamos las amenazas potenciales mediante distintos métodos que examinan su comportamiento, su código y el protocolo que utilizan. Esto permite detectar los ataques en las primeras etapas de la cadena de ataque, a menudo incluso antes de que se produzcan daños.

Proofpoint TAP protege frente a los ataques BEC y las amenazas de compromiso de cuentas de proveedores. La mayor parte de estos tipos de ataques no tiene payloads maliciosas, por lo que su identificación requiere de técnicas de detección sofisticadas que van más allá del análisis en entorno aislado (sandbox). Proofpoint TAP está optimizado con el gráfico de amenazas Nexus. Recopila, analiza y correlaciona más de un billón de puntos de datos del correo electrónico, nube, red y redes sociales. El motor Advanced BEC Defense está diseñado y entrenado mediante datos de amenazas enriquecidos. Aprende en tiempo real de manera que puede reaccionar rápidamente a cambios en el panorama de amenazas.

Empleamos técnicas de entorno aislado (sandbox) para estudiar una amplia variedad de ataques. Se puede tratar de ataques que utilicen URL y adjuntos maliciosos para instalar malware en los equipos o engañar a los usuarios y conseguir que compartan información sensible. También utilizamos ejecución asistida por analistas para maximizar la detección y la extracción de inteligencia.

Proofpoint TAP detecta las amenazas y los riesgos asociados a las aplicaciones cloud, y las relaciona con ataques para robar credenciales y otros tipos de ataques, para ayudarle a entender los ataques basados en la nube. Nuestra tecnología no solo detecta las amenazas: recurre además al aprendizaje automático para observar las tendencias, los comportamientos y las técnicas empleadas en cada ataque. Una vez que tiene esta información, TAP aprende y se adapta para detectar los próximos ataques más rápidamente.

Proofpoint Advanced BEC Defense

Advanced BEC Defense protege frente a los ataques BEC y las amenazas de compromiso de cuentas de proveedores. Lleva a cabo un análisis completo de cada detalle dentro de un mensaje, como:

- Datos del encabezado
- Dirección IP del remitente
- Relación entre el remitente y el destinatario
- Análisis de la reputación
- Análisis en profundidad del contenido

Advanced BEC Defense también proporciona visibilidad pormenorizada de las técnicas empleadas por los ciberdelincuentes, observaciones sobre las amenazas y muestras de amenazas. Le ayuda a conocer cómo están siendo atacados los usuarios.

Proofpoint TAP URL Defense

Proofpoint TAP URL Defense ofrece protección frente a amenazas del correo electrónico basadas en URL, como el malware y el phishing de credenciales. Proporciona funciones exclusivas de análisis predictivo que se basa en patrones de tráfico de correo electrónico para identificar y aislar las URL sospechosas. Todas las URL que llegan a la bandeja de entrada se reescriben de manera transparente, a fin de proteger a los usuarios en cualquier dispositivo o en la red. Además, cada vez que se hace clic en una URL, se ejecuta en tiempo real en un entorno aislado (sandbox).

Proofpoint TAP Attachment Defense

Proofpoint TAP Attachment Defense ofrece protección contra las amenazas conocidas y desconocidas que llegan a través de archivos adjuntos. Protege frente a amenazas disimuladas en una amplia variedad de tipos de archivos, documentos protegidos con contraseña, archivos adjuntos con URL incrustadas y archivos Zip.

Proofpoint TAP Account Takeover

Proofpoint TAP Account Takeover proporciona visibilidad y defensas en toda la cadena de ataques de usurpación de cuentas de correo electrónico. Su cronología gráfica de secuencias de ataque ayuda a acelerar las investigaciones de cuentas comprometidas y actividades sospechosas. Puede ver qué tipo de amenazas de correo se dirigen a las cuentas. Si un atacante accede a una cuenta, puede tomar medidas correctivas para protegerla. También corrige los cambios malintencionados en las reglas de los buzones de correo, las aplicaciones de terceros mal utilizadas y la filtración de datos en entornos de correo electrónico y en la nube. Proofpoint TAP Account Takeover es compatible con Microsoft 365, Google Workspace u Okta.

Proofpoint TAP SaaS Defense

Proofpoint TAP SaaS Defense detecta la actividad de inicio de sesión sospechosa, concretamente las conexiones desde ubicaciones inusuales y los intentos y errores de inicio de sesión excesivos. También identifica cuando hay demasiadas conexiones de direcciones IP maliciosas conocidas. Le ofrece visibilidad de eventos de intercambio de archivos internos y externos con un riesgo de exposición alto. De esta forma puede determinar si se han podido filtrar datos confidenciales durante los 30 días previos. Asimismo, detecta las aplicaciones de terceros críticas y de alto riesgo que se utilizan en su empresa, y es compatible con Microsoft 365 o Google Workspace.

Proofpoint TAP URL Isolation for VAPS

Proofpoint TAP URL Isolation for VAPs ha sido diseñada para proteger a los VAP (Very Attacked People™ o personas muy atacadas) de su empresa frente a ataques basados en URL y web. Proporciona detección de phishing en tiempo real y permite proteger a los usuarios y los clics autorizados contra las URL desconocidas y de riesgo. Gracias a nuestra solución de aislamiento del navegador, los VAP pueden acceder con confianza a sitios web desde el correo electrónico corporativo, con la tranquilidad de saber que la empresa está segura.

Información detallada y visibilidad de las amenazas y sus objetivos

Proofpoint dispone de una visibilidad que se extiende a múltiples vectores de amenazas, como el correo electrónico, la nube, la red y las redes sociales. Esta visibilidad procede de nuestros más de 115 000 clientes de todo el mundo. Los datos que recopilamos se transmiten al gráfico de amenazas Nexus de Proofpoint. Ahí se correlacionan los unos con los otros para incrementar la visibilidad del panorama de amenazas. Puede consultar fácilmente toda esta información, así como otros detalles importantes en el panel de Threat Insight de Proofpoint TAP, que ofrece información detallada sobre las amenazas y las campañas en tiempo real. Con estos datos podrá entender tanto los ataques de gran envergadura como los dirigidos. Se incluyen datos sobre las amenazas, como los usuarios afectados, capturas de pantalla del ataque y datos forenses detallados.

Personas muy atacadas (VAP)

Proofpoint Attack Index le ayuda a identificar sus VAP para que sus equipos de seguridad puedan determinar quiénes son los principales objetivos en su empresa. Este índice es una calificación compuesta ponderada de todas las amenazas que se envían a una persona dentro de su empresa. Asigna una nota en una escala del 0 al 1000, en función de la sofisticación de la amenaza, la envergadura y el objetivo del ataque, el tipo de ataque y el volumen global del ataque. Con un mejor conocimiento de sus VAP, puede identificar la solución más eficaz y darle prioridad para neutralizar las amenazas.

Attack Index a nivel de empresa

La utilidad Attack Index se puede aplicar también a nivel de empresa y compararse con otros sectores para ofrecerle una comparación del riesgo general de la empresa. Este informe ayuda a sus CISO y a su equipo de seguridad a saber si su empresa sufre más o menos ataques que las empresas comparables de otros sectores. Incluye información detallada sobre la frecuencia de los ataques y los tipos de amenazas. Con esta información, puede priorizar los controles de seguridad en función del panorama de amenazas particular de su empresa.

Información sobre los ciberdelincuentes

Puesto que las personas continúan siendo el objetivo de los ataques, es más importante que nunca que los clientes dispongan de una visión completa de los ciberdelincuentes que llevan a cabo los ataques. Nuestros investigadores sobre amenazas han estado recopilando datos sobre los atacantes durante muchos años, y esta inteligencia se refleja en el panel de TAP. Los clientes pueden ver qué ciberdelincuentes les atacan, quién es objeto de los ataques, las tácticas y técnicas utilizadas y las tendencias que se generan a lo largo del tiempo en torno a los ciberdelincuentes. Esto ayuda a las organizaciones a asignar controles de seguridad y corrección adicionales para proteger mejor a sus empleados.

MÁS INFORMACIÓN

Para obtener más información, visite <http://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.

©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.