

# TARGETED ATTACK PROTECTION

## PROTEJA A SUS EMPLEADOS DE LAS AMENAZAS AVANZADAS DEL CORREO ELECTRÓNICO

Los actores de amenazas se aprovechan de las herramientas que sus empleados utilizan para poner en peligro sus extremos, robar sus credenciales y acceder a sus datos. Es por eso que más del 90 % de los ataques dirigidos continúan llegando a sus víctimas mediante el correo electrónico.

Las soluciones de ciberseguridad tradicionales que utilizan técnicas heredadas, como la reputación y las firmas, ya no son suficientes para identificar y detener el correo electrónico mal intencionado. Las técnicas de malware han evolucionado rápidamente a fin de mantenerse al ritmo, y lo mismo debe hacer la tecnología utilizada para protegerse en contra de esas amenazas.

Proofpoint Targeted Attack Protection (TAP) ayuda a detectar, mitigar y bloquear las amenazas avanzadas que se dirigen a las personas por medio del correo electrónico. Detectamos tanto las amenazas conocidas como las nuevas, así como ataques nunca antes vistos que incluyen archivos adjuntos y direcciones URL malintencionados, y que instalan malware en los dispositivos o engañan a los usuarios para que compartan contraseñas u otra información confidencial. TAP no tiene paralelo en la detención de ataques dirigidos que hacen uso de malware polimórfico, documentos envenenados y phishing para acceder a información confidencial o robar dinero.

**TAP brinda la primera línea de defensa en la puerta de enlace del correo electrónico. TAP tiene dos componentes:**

**Attachment Defense:** TAP puede retener los mensajes hasta que se reciba un veredicto tras analizar el archivo adjunto. Los mensajes limpios se entregan en la bandeja de entrada y las amenazas se ponen en cuarentena.

**URL Defense:** Los mensajes que contienen direcciones URL que se sabe que son malintencionadas se colocan en cuarentena de inmediato. TAP reescribe todas las demás direcciones URL a fin de seguir y bloquear los clics. Si los usuarios hacen clic en las direcciones URL reescritas, TAP los redirige, según el veredicto de la inspección, ya sea a la página web original o a una página de bloqueo personalizable que evita el acceso al sitio afectado.

### DETENGA LAS AMENAZAS ANTES DE QUE LLEGUEN A LA BANDEJA DE ENTRADA

TAP se ha diseñado en la plataforma de seguridad del correo electrónico de Proofpoint de siguiente generación, la cual ofrece visibilidad clara de todas las comunicaciones de correo electrónico. Eso significa que TAP cuenta con mayor contexto para extraer inteligencia sobre amenazas, mitigar rápidamente la superficie de ataque mediante el bloqueo de mensajes malintencionados y reducir el riesgo de seguridad.

Otras soluciones de amenazas avanzadas del mercado podrían examinar el tráfico SMTP con la esperanza de detectar las amenazas en la red. Este método carece del contexto para comprender qué usuarios se ven afectados por la amenaza y no tiene la capacidad para inspeccionar

### VENTAJAS CLAVE

- **Detenga las amenazas antes de que lleguen a la bandeja de entrada**
- **Detecte las amenazas conocidas y desconocidas del correo electrónico**
- **Responda con perspectiva de principio a fin**
- **Implemente con rapidez y proteja en cualquier parte**

el tráfico de red cifrado. Por lo tanto, esas soluciones solamente tienen una perspectiva limitada del panorama de amenazas del correo electrónico. Del mismo modo, debido a que no están en el flujo del correo electrónico, no pueden detener las amenazas de día cero antes de que lleguen a las bandejas de entrada de las personas.

### DETECTE LAS AMENAZAS CONOCIDAS Y DESCONOCIDAS MEDIANTE TÉCNICAS SOFISTICADAS Y ADAPTABLES

El panorama de amenazas está en constante cambio. Es por eso que nuestras soluciones de amenazas avanzadas se adaptan continuamente para detectar nuevos patrones de ataque. TAP inspecciona toda la cadena de ataque haciendo uso de técnicas estáticas y dinámicas. Analizamos las posibles amenazas en varias fases, haciendo uso de múltiples métodos para examinar el comportamiento, el código y el protocolo. Debido a que la prevención es crucial, nuestras soluciones se han diseñado para detectar las amenazas lo más pronto posible en la cadena de ataque. TAP hace uso de funciones exclusivas, tal como el análisis predictivo para identificar y aislar las direcciones URL sospechosas antes de que los usuarios hagan clic en ellas.

Sabemos que los atacantes pueden variar sus técnicas para evitar la detección. Además, algunas amenazas, como phishing de credenciales, no dejan rastros obvios. Nuestras tecnologías se han diseñado no solo para detectar las amenazas, sino también para aprender de ellas. Podemos observar los patrones, las tácticas, los comportamientos y las herramientas de cada ataque, lo cual facilita que se capte el siguiente.

## RESPONDA CON UNA PERSPECTIVA DE PRINCIPIO A FIN Y CON INTELIGENCIA SUPERIOR SOBRE SEGURIDAD

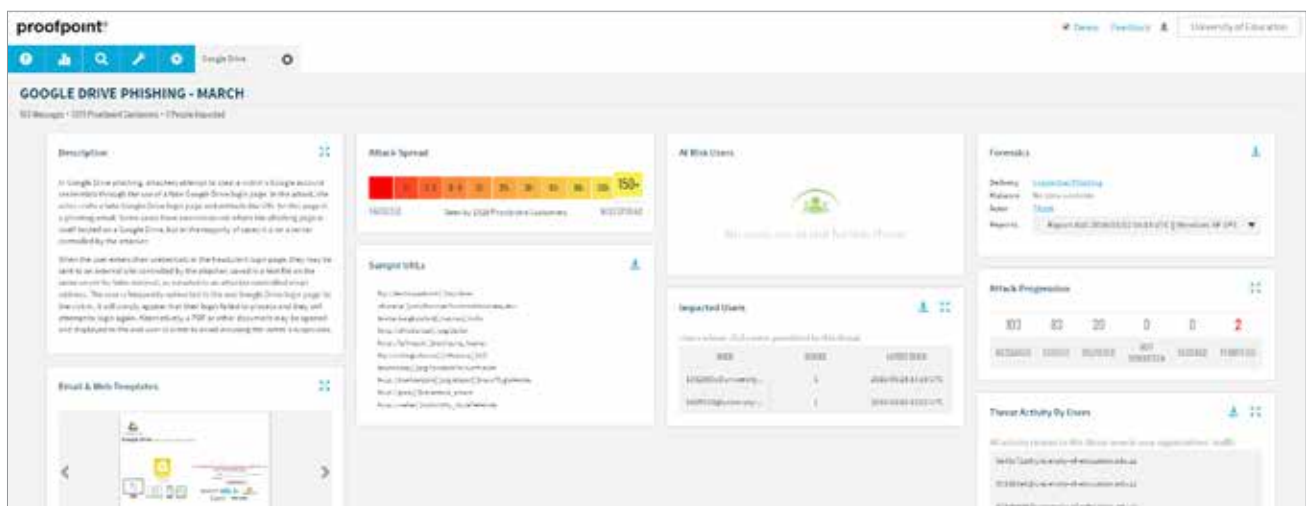
Proofpoint es la única empresa de ciberseguridad con inteligencia sobre amenazas que abarca el correo electrónico, las redes, las aplicaciones móviles y las redes sociales. Nuestro esquema de amenazas con inteligencia basada en la comunidad contiene más de 600 mil millones de puntos de datos que correlacionan campañas de ataques en diversos sectores y lugares. Debido a que podemos atribuir la mayoría del tráfico malintencionado a campañas, usted podrá distinguir fácilmente entre una amplia gama de ataques y amenazas dirigidos a ejecutivos o a otros empleados de alto nivel.

Incorporamos perspectivas procedentes de Proofpoint Emerging Threats (ET) Intelligence, que es la fuente más oportuna y precisa de inteligencia sobre amenazas del mercado. Proofpoint ET Intelligence es el estándar de oro para los investigadores de amenazas que ofrece inteligencia sobre amenazas 100 % verificada, la cual va más allá de los dominios y las direcciones IP.

Proofpoint TAP incluye un panel gráfico en internet que ofrece datos a nivel de organización, amenaza y usuario, lo que le permite priorizar las alertas y tomar medidas. Información forense detallada tanto sobre amenazas individuales como sobre campañas, la cual se brinda en tiempo real.

### Le ayudamos a contestar preguntas críticas como:

- ¿En qué consiste la amenaza? ¿Forma parte de una campaña de ataques?
- ¿A quién se dirige?
- ¿Cuántos mensajes se han bloqueado?
- ¿Qué usuarios han hecho clic?
- ¿Cómo se sabe si se ha afectado un extremo?



## IMPLEMENTE CON RAPIDEZ Y PROTEJA EN CUALQUIER PARTE PARA RECIBIR VALOR INMEDIATO

A fin de proteger a sus empleados, sus datos y su marca, las defensas de hoy deben trabajar donde lo hacen sus empleados y al ritmo de ellos. La arquitectura TAP le permite implementar con rapidez y generar valor de inmediato. Puede proteger cientos de miles de usuarios en días, no en semanas ni meses.

Nuestra solución protege a los usuarios en cualquier red o dispositivo, independientemente de dónde y cómo vean su correo electrónico. Proofpoint TAP se configura con facilidad a modo de módulos de complemento en la plataforma de seguridad de correo electrónico de Proofpoint, la cual se puede implementar a modo de servicio en la nube, aparato virtual o aparato de hardware. Proofpoint también utiliza la nube para actualizar al instante nuestro software cada día a fin de incorporar rápidamente las nuevas funciones y ayudarlo a estar a la delantera de los atacantes.

### ACERCA DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) es una empresa de ciberseguridad de siguiente generación que permite que las organizaciones protejan la manera en que la gente trabaja en la actualidad de las amenazas avanzadas y los riesgos de cumplimiento. Proofpoint ayuda a los profesionales de ciberseguridad a proteger a sus usuarios de los ataques avanzados que se dirigen a ellos (por medio de correo electrónico, aplicaciones móviles y redes sociales), a proteger la información crítica que la gente crea y a equipar a sus grupos con la inteligencia y las herramientas adecuadas para que respondan rápidamente cuando algo vaya mal. Las organizaciones líderes de todos los tamaños, incluyendo más del 50 por ciento de las empresas Fortune 100, confían en las soluciones de Proofpoint, las cuales se han diseñado para los entornos de TI móviles y habilitados para las redes sociales de hoy, y aprovechan tanto la potencia de la nube como una plataforma de análisis centrado en macrodatos para combatir las amenazas avanzadas modernas.