

PROOFPOINT BROWSER ISOLATION

PROTEJA A SUS EMPLEADOS FRENTE A LAS AMENAZAS AVANZADAS DIRIGIDAS A ENTORNOS CORPORATIVOS Y PERSONALES

VENTAJAS PRINCIPALES

- Aísle las direcciones URL maliciosas del correo electrónico corporativo mediante un control adaptable en función del riesgo.
- Aplique navegación aislada cuando haga una navegación de alto riesgo, como en el caso de dominios nuevos o desconocidos.
- Impida el robo y la recopilación de credenciales.
- Despliegue de forma rápida y sencilla desde la nube, sin necesidad de hardware ni de agentes de endpoints.
- Proporcione a sus empleados una experiencia de navegación homogénea.
- Simplifique el cumplimiento del RGPD de la UE.

Proteger a los usuarios frente a los ataques de phishing y el robo de credenciales supone una lucha constante. Para complicar aún más las cosas, los atacantes están tomando rápidamente ventaja mediante el uso de direcciones URL maliciosas en campañas a gran escala. ¿Cómo protegerse frente a estas amenazas crecientes? Con Proofpoint Browser Isolation, puede permitir a sus empleados acceder a Internet de forma segura, mientras les protege frente al malware y la pérdida de datos.

DESCRIPCIÓN DEL PRODUCTO

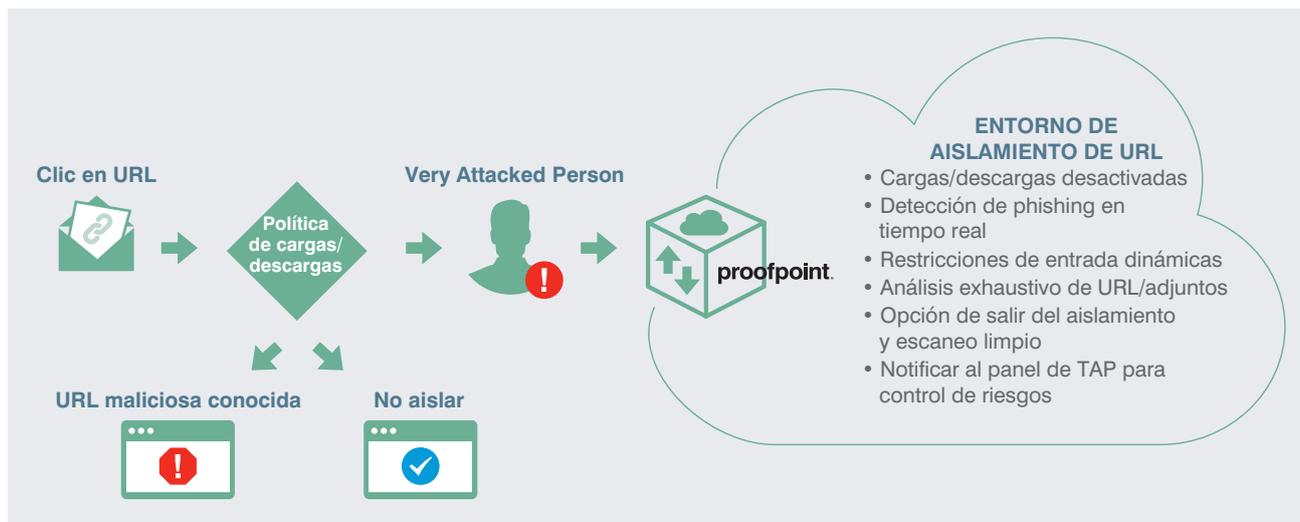
Browser Isolation permite al personal acceder sin riesgos a sitios web, y al correo electrónico personal y corporativo. Y lo hace aislando las sesiones del navegador en un contenedor seguro. Esta solución exclusiva le protege contra el malware y el contenido malicioso, desactiva las subidas y las bajadas de archivos, e impide el robo o la pérdida de datos sensibles. Browser Isolation le ayuda a afrontar los problemas de seguridad, productividad y privacidad que acarrearán los ataques de phishing dirigidos y el uso peligroso de la web. Además, es fácil de desplegar, administrar y mantener.

FUNCIONES Y VENTAJAS

Adapte su seguridad a las direcciones URL peligrosas y a los usuarios que están en el punto de mira

Los ciberdelincuentes actuales dirigen sus mensajes de phishing a personas concretas de su organización. Para proteger a las personas más atacadas, necesita más controles adaptables. Browser Isolation protege a sus empleados del contenido web malicioso en el correo electrónico de la empresa. Con Browser Isolation, se aíslan las sesiones del navegador, en función de las políticas definidas, para garantizar su protección y la de sus empleados frente a las direcciones URL de alto riesgo. Entre ellas, se incluyen las direcciones URL desconocidas, las redes sociales y las aplicaciones cloud online.

La integración con Proofpoint Targeted Attack Prevention (TAP) permite además a los usuarios de TAP aprovechar Browser Isolation para el correo electrónico corporativo. Los controles centrados en las personas en combinación con TAP son una forma eficaz de reducir el riesgo. Puede seleccionar a los usuarios para el entorno de aislamiento en función de los factores de riesgo de su correo electrónico corporativo. La integración con TAP le ofrece funciones de detección y análisis de phishing en tiempo real. Las sesiones de navegador aisladas se comunican al panel de TAP, de manera que puede consultarlas y así controlar el riesgo.



Reduzca la superficie de ataque

Al igual que ocurre en muchas organizaciones, en la suya también se permite a los empleados utilizar el correo web personal o navegar por Internet en el trabajo. Los atacantes lo saben y aprovechan esta situación para lanzar sofisticados ataques. De hecho, un estudio revela que hasta el 60 % de los ataques son consecuencia del uso del correo electrónico web o personal en dispositivos de la empresa. ¿Cómo puede reducir el riesgo sin limitar la libertad de sus empleados a la hora de navegar por Internet y utilizar su correo electrónico personal?

Con Browser Isolation, puede aislar determinados sitios web o aplicaciones en la nube. De esta forma, sus empleados pueden navegar o acceder a su correo web personal sin riesgos y, al mismo tiempo, usted mejora la estrategia de seguridad de su organización. Así, el riesgo para los activos corporativos es nulo. No es necesario inspeccionar los archivos ni supervisar el comportamiento de los usuarios. Además, los archivos o los adjuntos de correo electrónico con payloads o macros maliciosas no se descargan nunca. La solución incluso aísla el contenido de sitios de confianza que han sido comprometidos. Esto le protege contra los ataques de tipo "watering-hole" y los enlaces de correo electrónico a aplicaciones en la nube (como Microsoft SharePoint, Dropbox, etc.) con carga maliciosa. Asimismo, las restricciones dinámicas de entrada permiten reducir el robo de credenciales a través del navegador. Browser Isolation impide además las descargas inadvertidas, y mantiene alejados de sus endpoints otros tipos de contenidos web maliciosos.

Reduzca la carga de trabajo del equipo de IT

Le preocupa conceder permiso a sus empleados para acceder a direcciones URL sin clasificar o desconocidas y a su correo web personal. Es consciente del riesgo que esto conlleva. Pero sus empleados suelen tener buenas razones para navegar por esos sitios. En la mayoría de las soluciones, los equipos de IT deben decidir si permiten o bloquean estos sitios. Si se bloquean todos estos dominios, los equipos de IT reciben multitud de solicitudes para hacer excepciones puntuales de acceso a sitios concretos.

Browser Isolation ofrece algo mejor. Resuelve los desafíos de seguridad, productividad y privacidad asociados al uso de la web por parte de los empleados. Al confinar las sesiones de navegación en un contenedor seguro y aislado, sus empleados pueden acceder libremente al correo web personal y otros sitios. Esto también aporta ventajas a los equipos de IT, que ya no tienen que dedicar tiempo y esfuerzo para hacer las excepciones caso por caso. Además, es sencillo de desplegar, administrar y mantener. Su organización conseguirá un ahorro inmediato, gracias al aumento de la productividad de los equipos de IT. Además, subirá la moral de los empleados al demostrarles su confianza. También evitará violaciones de normativas al preservar la privacidad del correo web de los usuarios. Browser Isolation es fácil de desplegar porque está totalmente alojado en la nube. Y puede integrarlo con su propio filtro web, proxy, gateway y firewall.

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

ACERCA DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) es una compañía de ciberseguridad que protege los activos más importantes y de mayor riesgo para organizaciones y empresas: las personas. Gracias a una suite integrada de soluciones basadas en la nube, 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 de las incluidas en el Fortune 1000, confían en Proofpoint para mitigar los riesgos críticos de seguridad y cumplimiento normativo en sus sistemas de correo electrónico, nube, redes sociales y web. www.proofpoint.com/es

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