

RESUMEN DE LA SOLUCIÓN

Proofpoint Prime Threat Protection – Versión para empresas



Ventajas principales

- Bloquee la mayor variedad de amenazas con una precisión del 99,99 %.
- Amplíe la protección del usuario a todas las plataformas, no solo al correo electrónico.
- Refuerce la resiliencia de los usuarios con información y asesoramiento basados en los riesgos.
- Reduzca los tiempos de respuesta en caso de que las cuentas de empleados y proveedores se vean comprometidas.
- Simplifique las operaciones con una detección muy eficaz y un flujo de trabajo automatizado.
- Acelere la rentabilización mediante la consolidación y la integración preconfigurada.

Descripción general

El correo electrónico sigue siendo uno de los principales vectores de ciberamenazas. Sin embargo, en los últimos años, la superficie de ataque se ha ampliado. Ahora los ciberdelincuentes atacan a las personas a través del correo electrónico y otros canales digitales como plataformas de mensajería, herramientas de colaboración, aplicaciones cloud y servicios de intercambio de archivos.

Como respuesta, muchas organizaciones están adoptando un enfoque fragmentado de la seguridad, basado en productos aislados. Sin embargo, esta estrategia crea vulnerabilidades adicionales en sus defensas y pasa por alto muchos riesgos. Además, la gestión e integración de todas estas herramientas es una tarea compleja.

Para defenderse de estas amenazas centradas en las personas y en constante evolución, es necesario adoptar un enfoque global. Proofpoint Prime Threat Protection (Prime) puede ayudarle.

Proofpoint Prime le permite defenderse de ataques multifase y multicanal y proteger sus comunicaciones corporativas. También proporciona asesoramiento basado en riesgos para sus empleados y agiliza sus operaciones de seguridad a todos los niveles.

Proofpoint Prime Threat Protection – Versión para empresas

PROOFPOINT USER PROTECTION

- Concienciación en seguridad y cambio de comportamiento
- Protección frente a la usurpación de cuentas
- Protección de herramientas de colaboración y mensajería

PROOFPOINT IMPERSONATION PROTECTION

- Protección frente al "domain spoofing" (soplantación de dominios)
- Retransmisión segura del correo de aplicaciones
- Protección frente a amenazas asociadas a proveedores
- Servicios de desmantelamiento de dominios maliciosos

PROOFPOINT CORE EMAIL PROTECTION

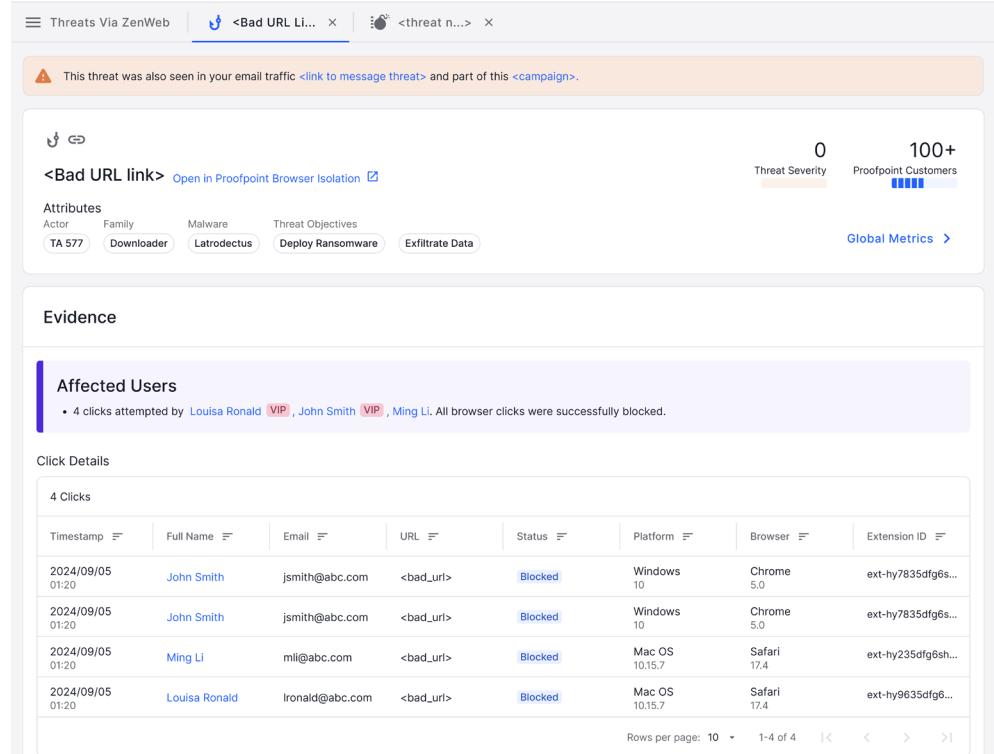
Bloquee las amenazas en el correo electrónico y otros canales digitales

Los empleados nunca se han comunicado y colaborado tan eficazmente como ahora. Trabajan en Microsoft Teams, Slack, aplicaciones cloud, servicios de intercambio de archivos y mucho más. Aunque estas herramientas aumentan la productividad de los empleados, también amplían la superficie de ataque. Los ciberataques centrados en las personas ya no se limitan al correo electrónico, y sus defensas tampoco deberían hacerlo.

Proofpoint Prime protege todo su espacio de trabajo digital. Ya se distribuyan por correo electrónico, mensajes instantáneos, redes sociales o aplicaciones colaborativas, Proofpoint Prime ofrece protección en tiempo real contra una amplia gama de amenazas: estafas Business Email Compromise (BEC), ransomware, phishing selectivo, etc.

Optimizada por la tecnología de IA Proofpoint Nexus®, Proofpoint Prime ofrece una protección inigualable contra las amenazas con una eficacia del 99,99 %. Combina nuestra rica inteligencia sobre amenazas, modelos lingüísticos avanzados, gráficos relacionales, análisis del comportamiento y visión artificial. Todas estas tecnologías trabajan juntas para detectar y bloquear las amenazas antes de que causen daños.

Gracias a su gran alcance y a sus potentes funciones de inteligencia artificial, Proofpoint Prime protege a sus empleados, estén donde estén y con independencia de cómo trabajen.



The screenshot shows a threat detail page for a 'Bad URL link'. The top navigation bar includes 'Threats Via ZenWeb', a search bar with 'Bad URL Li...', and a threat ID 'threat n...'. The main content area displays a warning message: '⚠ This threat was also seen in your email traffic <link to message threat> and part of this <campaign>.' Below this, the threat is identified as '<Bad URL link>' with an 'Open in Proofpoint Browser Isolation' button. The 'Attributes' section lists 'Actor' (TA 577), 'Family' (Downloader), 'Malware' (Latroductus), 'Threat Objectives' (Deploy Ransomware, Exfiltrate Data), and 'Threat Severity' (0). A 'Proofpoint Customers' section shows 100+ customers. The 'Global Metrics' section is partially visible. The 'Evidence' section is expanded, showing the 'Affected Users' section with a note that 4 clicks were attempted by Louisa Ronald, John Smith, and Ming Li, all of whom were successfully blocked. The 'Click Details' table lists four blocked clicks with the following data:

Timestamp	Full Name	Email	URL	Status	Platform	Browser	Extension ID
2024/09/05 01:20	John Smith	jsmith@abc.com	<bad_url>	Blocked	Windows 10	Chrome 5.0	ext-hy7835dfg6...
2024/09/05 01:20	John Smith	jsmith@abc.com	<bad_url>	Blocked	Windows 10	Chrome 5.0	ext-hy7835dfg6...
2024/09/05 01:20	Ming Li	ml@abc.com	<bad_url>	Blocked	Mac OS 10.15.7	Safari 17.4	ext-hy235dfg6...
2024/09/05 01:20	Louisa Ronald	lronald@abc.com	<bad_url>	Blocked	Mac OS 10.15.7	Safari 17.4	ext-hy9635dfg6...

At the bottom, pagination controls show 'Rows per page: 10' and '1-4 of 4'.

Figura 1: Proofpoint amplía la protección contra el phishing más allá del correo electrónico. También bloquea las URL maliciosas compartidas a través de plataformas de mensajería, colaboración y comunicación.

Proteja frente a ataques multifase

Los ciberdelincuentes se apoderan de cuentas de usuarios legítimos utilizando una gran variedad de tácticas: phishing, ataques por fuerza bruta, secuestro de sesiones, ingeniería social, etc. Una vez que una cuenta ha sido comprometida, los ciberdelincuentes suelen elevar los privilegios, acceder a sus datos y establecer una presencia persistente a largo plazo. Aunque haya configurado la autenticación multifactor (MFA), no es inmune a la usurpación cuentas (ATO).

Proofpoint Prime impide los ataques ATO que eluden la MFA. Permite a los equipos de seguridad detectar, analizar y neutralizar rápidamente las cuentas comprometidas en las plataformas más populares, como Microsoft 365, Google Workspace y Okta.

No solo ofrece una visión centralizada de las actividades de los ciberdelincuentes tras un ataque, sino que también admite una serie de respuestas automatizadas. Los equipos pueden suspender automáticamente las cuentas comprometidas, forzar el restablecimiento de contraseñas, deshacer modificaciones no autorizadas y eliminar aplicaciones sospechosas de terceros.

La solución también le protege contra ataques multifase lanzados por ciberdelincuentes que utilizan cuentas de proveedores comprometidas. Proofpoint Prime detecta cuentas de terceros potencialmente comprometidas en todo el ecosistema Proofpoint y alerta a su equipo de seguridad. También permite a su equipo aplicar controles de seguridad adaptables, como aislar URL y mostrar advertencias para correos sospechosos, sin bloquear los mensajes legítimos.

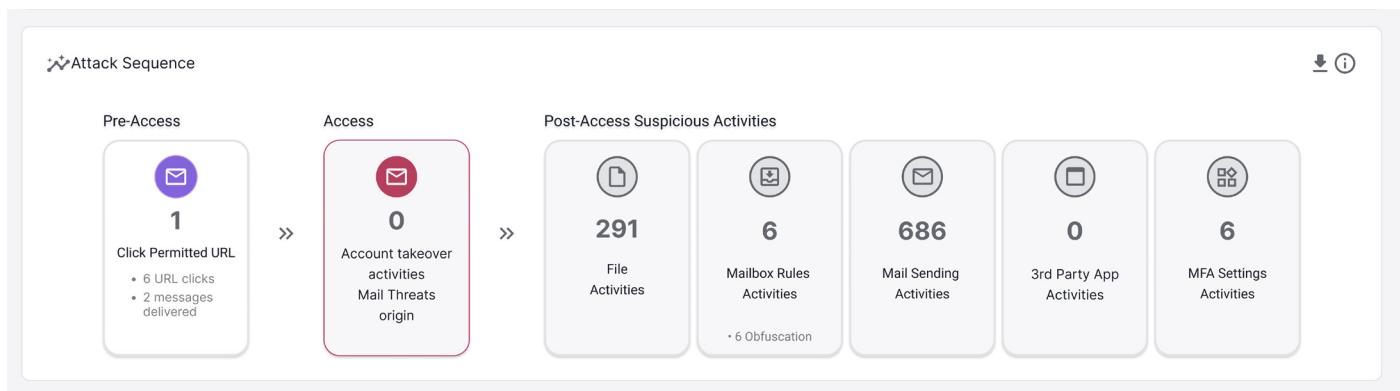


Figura 2: Proofpoint Prime muestra la actividad maliciosa previa y posterior al acceso de las cuentas afectadas.

Proteja sus comunicaciones empresariales de confianza

Los ciberdelincuentes suelen utilizar tácticas de suplantación de la identidad para acceder a comunicaciones corporativas de confianza. La suplantación de la identidad de su organización (ya sea mediante la suplantación directa de dominios o el registro de dominios parecidos) pone en peligro a sus empleados, clientes y partners, y puede ser muy perjudicial para su marca.

Proofpoint Prime puede ayudarle a reducir proactivamente el riesgo de suplantación de la identidad. Le ofrece una visibilidad completa de todos los correos electrónicos salientes que utilizan sus dominios de confianza, incluidos los enviados por terceros. Tendrá acceso a potentes herramientas y consultores expertos que le guiarán en cada etapa de la implementación de la autenticación del correo electrónico.

Esto garantizará el cumplimiento de DMARC y evitará que los ciberdelincuentes suplanten sus dominios. Nuestra protección va más allá de los mensajes de correo electrónico generados por el usuario e incluye un entorno seguro dedicado para retransmitir mensajes generados por aplicaciones y mensajes de correo electrónico enviados por proveedores SaaS externos en su nombre.

Proofpoint Prime también ofrece funciones avanzadas para detectar dominios parecidos ("lookalike domains"). Supervisa dinámicamente Internet en busca de dominios muy similares al suyo y proporciona información detallada sobre su registro y posible uso inadecuado. Y no nos detenemos en la detección: podemos desactivar URL y dominios maliciosos en su nombre gracias a nuestras sólidas relaciones con registradores, hosts y proveedores de dominios de nivel superior. Nuestros profesionales gestionan el proceso de principio a fin, para que sus equipos puedan concentrarse en su actividad principal.

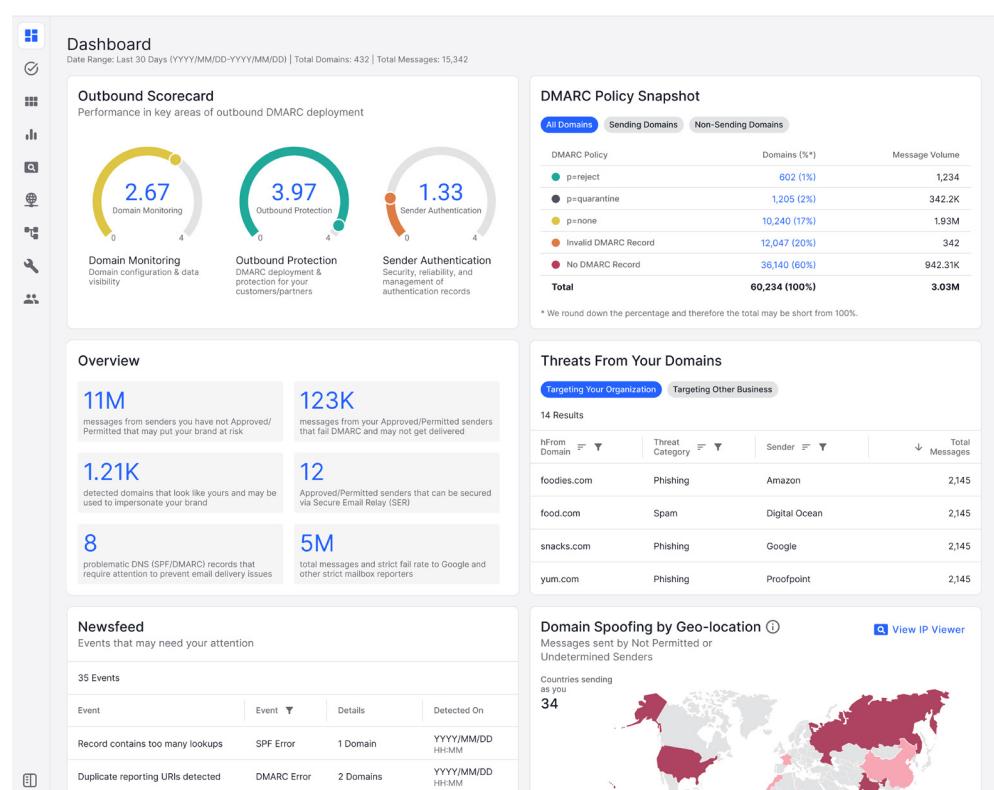


Figura 3: Proofpoint Prime le ofrece visibilidad de las amenazas de suplantación de dominios, dominios maliciosos parecidos a los suyos, así como los mensajes que se envían mediante sus dominios de confianza.

Refuerce la resistencia mediante información y asesoramiento basados en los riesgos

El objetivo de los ciberdelincuentes son las personas. Desafortunadamente, ofrecer formación en ciberseguridad una vez al año no garantiza un nivel de seguridad adecuado frente a tácticas en constante cambio.

Proofpoint Prime proporciona asesoramiento e información sobre los riesgos asociados a los usuarios que fomentan un cambio de comportamiento significativo y una resiliencia humana sostenible a largo plazo. Se basa en un aprendizaje adaptable basado en el riesgo que va más allá de los enfoques tradicionales, lo que lo hace mucho más eficaz que los métodos universales.

Proofpoint Prime ayuda a las empresas a medir el riesgo de los usuarios y a identificar a los empleados de alto riesgo agregando información de todo el ecosistema de Proofpoint. Gracias a la función Pathways, que ofrece un aprendizaje adaptable, Proofpoint permite a los equipos asignar automáticamente experiencias de aprendizaje

personalizadas a los usuarios de riesgo en función de su comportamiento, exposición a amenazas, función, conocimientos de seguridad y privilegios empresariales. Por ejemplo, a un VAP (Very Attacked Person, o persona muy atacada) se le pueden asignar automáticamente tareas específicas (como formación, notificaciones y simulaciones de ataques de phishing) en función de los tipos concretos de amenaza a los que se enfrentan. Esto permite a los equipos de seguridad ofrecer contenidos más pertinentes centrados en las amenazas, lograr una mayor implicación y adaptar las iniciativas de cambio de comportamiento de forma más eficaz en toda la organización.

A medida que sus empleados desarrollan una mayor resiliencia frente a unas amenazas en constante evolución, la exposición global al riesgo disminuye y su plantilla se convierte en una pieza clave de la defensa. Con Proofpoint Prime, puede medir el impacto de su programa de resiliencia humana y evaluar con precisión la reducción de los riesgos asociados a los usuarios. Esto le permitirá demostrar la eficacia de su programa y le facilitará conseguir el apoyo de la dirección y las partes interesadas.

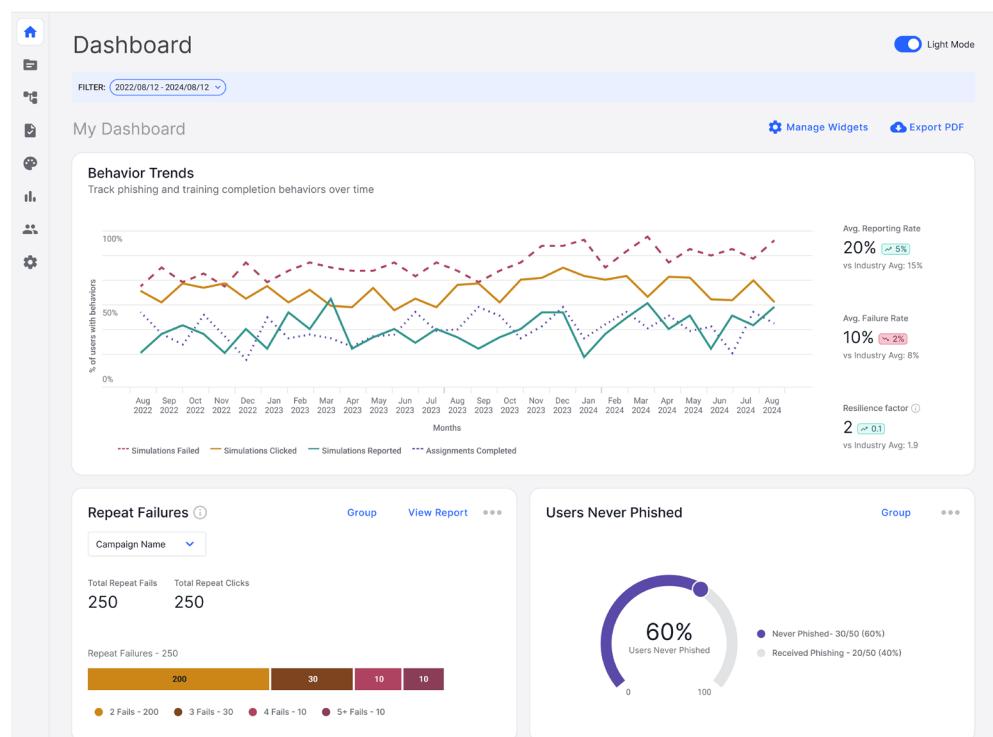


Figura 4: Gracias a la inteligencia global de amenazas de Proofpoint, Prime le ofrece información en tiempo real acerca de un panorama de amenazas en constante cambio. Puede orientar y formar a sus usuarios sobre las nuevas amenazas al tiempo que captura las tendencias de comportamiento a lo largo del tiempo.

Las ventajas de la protección integrada

Proteger los entornos digitales de trabajo frente a las ciberamenazas es cada vez más complejo. Una combinación de productos aislados y compartimentados resulta insuficiente, y muchos riesgos se pasan por alto. Esto genera problemas de integración, una gestión compleja, gastos excesivos y elevados costes operativos.

Proofpoint Prime resuelve estos problemas con un enfoque integral de la defensa frente a amenazas que elimina las vulnerabilidades de seguridad y reduce la complejidad asociada a las soluciones fragmentadas y aisladas. Nuestra protección integrada frente a amenazas permite a su equipo responder con mayor rapidez y eficacia, gracias a flujos de trabajo automatizados, información compartida sobre amenazas e integraciones preconfiguradas. Además, Proofpoint Prime reduce los costes de licencia, lo que le permite reducir sus gastos de explotación y mejorar el rendimiento económico. Por si fuera poco, disfrutará de las ventajas de contar con un partner confianza con un fuerte liderazgo en el sector.



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. Organizaciones líderes de todos los tamaños, entre las que se encuentran el 85 % de las empresas Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en las personas y su cumplimiento normativo, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en www.proofpoint.com/es.

Conecte con Proofpoint: [X](#) | [LinkedIn](#) | [Facebook](#) | [YouTube](#)

Proofpoint es una marca comercial o marca comercial registrada de Proofpoint, Inc. en Estados Unidos y/o en otros países. Todas las demás marcas comerciales son propiedad exclusiva de sus respectivos propietarios. ©Proofpoint, Inc. 2025

DESCUBRA LA PLATAFORMA DE PROOFPOINT →