

Proofpoint Impersonation Protection

Proteja las comunicaciones con partners, clientes y proveedores de confianza.



Características principales

- **Proteja las comunicaciones empresariales de confianza frente a las amenazas de suplantación.**
- **Evite la suplantación personal y de su marca.**
- **Descubra dominios parecidos maliciosos y elimínelos.**
- **Detecte y protéjase contra proveedores de riesgo, incluidas las cuentas de proveedores comprometidas.**
- **Proteja el correo electrónico enviado en su nombre por aplicaciones, dispositivos, plataformas SaaS y agentes de IA.**
- **Basado en Nexus[®] AI, aprendizaje automático, LLM y análisis del comportamiento.**

La mayoría de las organizaciones dependen del correo electrónico para llevar a cabo su actividad comercial.

Pero los atacantes han descubierto cómo secuestrar las comunicaciones empresariales de confianza, y la IA generativa ha hecho que estos ataques sean más rápidos, más convincentes y más fáciles de llevar a gran escala. Pueden suplantar la identidad de su organización, su marca o sus partners comerciales y crear mensajes y sitios web creíbles en cuestión de minutos, en lugar de horas.

Según el Servicio IC3 (Internet Crime Complaint Center) del FBI, los ataques Business Email Compromise (BEC) provocan cada año pérdidas de miles de millones de dólares, una cifra que no deja de aumentar. El FBI también ha comenzado a hacer un seguimiento específico de la IA como factor de amenaza y atribuye decenas de millones de dólares en pérdidas por ataques Business Email Compromise (BEC) a casos en los que se ha confirmado el uso de IA. Además, advierte de que esta cifra probablemente subestime la verdadera magnitud del problema.

Estos ataques suelen combinar múltiples tácticas de suplantación de identidad, como dominios suplantados, dominios parecidos (lookalike domains) y cuentas de proveedores comprometidas. En conjunto, ponen en riesgo las comunicaciones con partners, clientes y proveedores de confianza y dificultan que los destinatarios distingan los mensajes legítimos de los fraudulentos.

Proofpoint adopta un enfoque integral y multicapa para proteger a su organización y su marca frente a los ataques de suplantación de identidad. Proporcionamos las herramientas, la tecnología y los recursos necesarios para autenticar el correo electrónico generado por usuarios y aplicaciones, proteger los mensajes enviados en su nombre, identificar cuentas de proveedores comprometidas o potencialmente comprometidas y supervisar la aparición de dominios parecidos maliciosos para facilitar su eliminación.

Proteja su marca de la suplantación de identidad

Una de las tácticas de suplantación de identidad más comunes es el “domain spoofing” (suplantación de dominios), y la IA generativa ha permitido crear mensajes falsificados con mayor rapidez y hacerlos más difíciles de distinguir de los legítimos. Sin los controles de seguridad adecuados, los atacantes pueden secuestrar fácilmente sus dominios de confianza y utilizar la IA para crear mensajes muy convincentes a gran escala. Esto les permite dirigirse a sus clientes, partners e incluso a sus empleados con una rapidez y sofisticación impensables hace tan solo un año. La autenticación del correo electrónico es la manera más eficaz de impedirlo.

Proofpoint Impersonation Protection simplifica la implementación de DMARC, guiándole en cada paso del despliegue y permitiendo autenticar tanto el correo electrónico generado por los usuarios como por las aplicaciones. Nuestros expertos trabajarán con usted para identificar a sus remitentes legítimos. Asimismo, garantizarán que todo su correo electrónico (incluido el de remitentes externos autorizados) se autentique adecuadamente.

La integración con Proofpoint Threat Protection le permite aplicar la autenticación DMARC a los mensajes entrantes con total confianza. Añade una capa de protección frente a los intentos de suplantación de identidad generados mediante IA que falsifican sus dominios de confianza. También le permite pasar por alto las políticas DMARC sin bloquear el correo electrónico legítimo ni comprometer la seguridad con listas seguras. Esta integración le ofrece visibilidad del tráfico de correo electrónico entrante y saliente. Puede ver todos los correos electrónicos enviados que utilizan sus dominios de confianza, incluidos los enviados por terceros y, cada vez más, por agentes de IA que actúan en su nombre.

Proteja frente a cuentas de proveedores comprometidas

Los atacantes explotan cada vez más la cadena de suministro para comprometer las comunicaciones empresariales de confianza. A menudo utilizan cuentas de proveedores comprometidas para secuestrar hilos de correo electrónico entre usted y sus partners. La IA generativa puede ayudarles a estudiar conversaciones anteriores e imitar el estilo de escritura de un proveedor, lo que dificulta la detección de mensajes fraudulentos. Y dado que estos correos electrónicos pueden proceder de cuentas de proveedores legítimos y no contener ninguna payload maliciosa, pueden eludir los controles tradicionales de autenticación y detección. El resultado puede ser una importante pérdida económica, el robo de datos, la extorsión o un ataque de ransomware.

Proofpoint Impersonation Protection ayuda a detectar proveedores de riesgo y a protegerse frente a ellos, incluidas las cuentas de proveedores comprometidas o potencialmente comprometidas. Utiliza IA basada en el comportamiento, aprendizaje automático e inteligencia de amenazas procedente de la amplia cartera de clientes de Proofpoint para detectar indicios de que las cuentas de proveedores pueden estar comprometidas, incluidos ataques en los que se utiliza IA generativa para crear señuelos más convincentes. Los controles adaptativos, como el aislamiento automático de URL, ayudan a reducir la exposición a amenazas procedentes de remitentes comprometidos. La integración con Proofpoint Threat Protection, combinada con el contexto sobre las relaciones entre remitente y destinatario, ayuda a agilizar la respuesta y la investigación de incidentes relacionados con terceros.

Detecte y elimine sitios maliciosos, incluidos los parecidos

Los ciberdelincuentes crean sitios web específicamente diseñados para lanzar ataques. Algunos se hacen pasar por otras organizaciones, marcas o instituciones para engañar a sus empleados, clientes o partners y ganarse su confianza. Otros imitan a su propia organización utilizando dominios y páginas que reproducen fielmente su logotipo, su diseño y la imagen de su marca. La IA generativa ha hecho que ambos tipos de ataques sean más fáciles de crear, más difíciles de detectar y más sencillos de llevar a gran escala. Los ciberdelincuentes utilizan estos sitios para lanzar ataques de phishing de credenciales, Business Email Compromise (BEC), ataques telefónicos o TOAD y otros tipos de ataques cuya eficacia depende de una presencia digital convincente.

Con Proofpoint Impersonation Protection, supervisamos continuamente los dominios recién registrados que

puedan suplantar la identidad de su organización y proporcionamos el contexto necesario para evaluar el riesgo que representan.

La detección es solo el primer paso. Cuando nos notifica un sitio web sospechoso, nuestro equipo de desmantelamiento lo investiga, recopila las pruebas disponibles y trabaja para mitigar la actividad maliciosa y retirar el sitio. Mantenemos relaciones con una amplia red de proveedores de infraestructura de internet y partners de confianza, incluidos registradores, proveedores de alojamiento web, proveedores de servicios de correo electrónico y partners de listas de bloqueo, entre otros.

Nuestro equipo gestiona el proceso de eliminación en su nombre, para que usted no tenga que preocuparse por saber con quién contactar ni qué documentación necesita. Nuestros servicios de eliminación van más allá de los dominios parecidos y también facilitan la mitigación de subdominios y URL maliciosos, así como de dominios que no guardan semejanza con los legítimos.

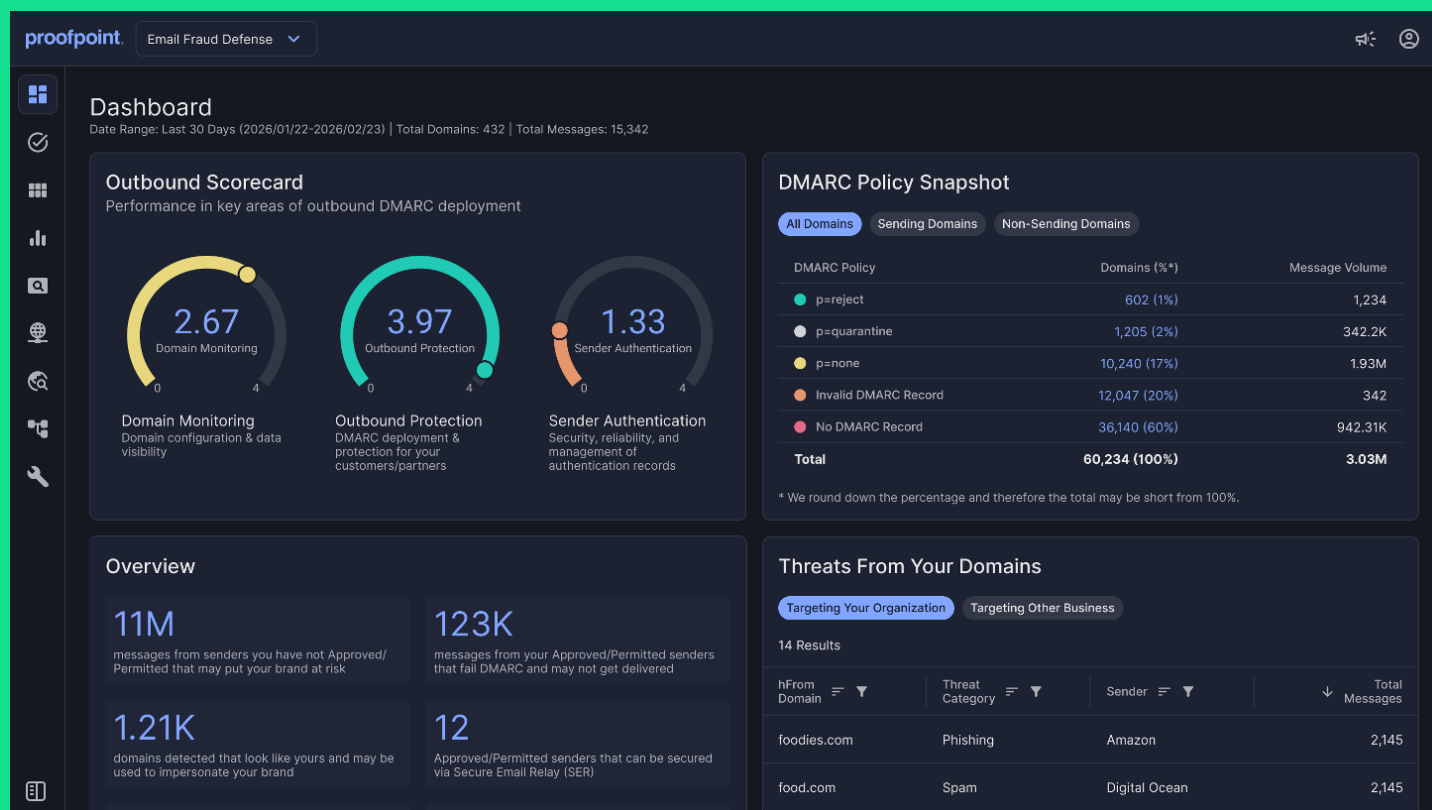


Figura 1. Proofpoint le ofrece visibilidad sobre las amenazas de “domain spoofing” (suplantación de dominios), los dominios parecidos maliciosos y los correos electrónicos enviados utilizando sus dominios de confianza.

Proteja el correo electrónico enviado en su nombre

No todos los correos electrónicos que salen de su dominio los envía una persona. Las plataformas de recursos humanos envían avisos de nómina, las herramientas de CRM envían recibos a los clientes, los dispositivos de oficina envían notificaciones de escaneo a correo electrónico y fax, y los agentes de IA están empezando a generar mensajes en su nombre. Cualquiera de estas fuentes puede aprovecharse con fines maliciosos. Si una aplicación, un dispositivo o un servicio de envío se ve comprometido, los atacantes pueden utilizar ese canal de confianza para enviar correos electrónicos maliciosos que parecen enviados por su organización, superan las comprobaciones de autenticación y, con ayuda de la IA generativa, resultan más convincentes que nunca.

Proofpoint Impersonation Protection cierra esta brecha mediante un relé seguro y dedicado para los remitentes automatizados que utilizan sus dominios, desde aplicaciones internas y dispositivos de oficina hasta plataformas SaaS y agentes de IA. Solo acepta correo de fuentes verificadas y autenticadas, aplica análisis avanzados antispam y antivirus a cada mensaje y aplica una firma DKIM al correo aprobado. Esto ayuda a sus fuentes de correo saliente a mantener la alineación de DMARC y el cumplimiento de SPF sin interrumpir el flujo de correo legítimo. Proofpoint SER también aísla este tráfico mediante direcciones IP dedicadas con una reputación sólida, lo que ayuda a proteger su infraestructura de envío y la reputación de su marca frente a actores malintencionados que, de otro modo, podrían aprovechar la confianza asociada a su dominio.

Obtenga visibilidad, control y apoyo al cumplimiento normativo

Proofpoint Impersonation Protection le ofrece visibilidad y control centralizados sobre los servicios de envío de alto volumen, como Amazon SES. Puede ver qué mensajes se envían de forma masiva desde su dominio y rastrearlos hasta la aplicación, el dispositivo o el agente de IA que los envió. El cifrado opcional y la prevención de la pérdida de datos ayudan a proteger la información sensible, incluida la información de identificación personal (PII) y la información sanitaria protegida (PHI), en los mensajes transaccionales. Estos controles pueden contribuir al cumplimiento de marcos normativos y requisitos como los establecidos por HIPAA, la SEC y FINRA.

Proofpoint Impersonation Protection también le ayuda a cumplir los requisitos de los principales proveedores de servicios de correo electrónico relativos a la identidad del remitente y la integridad de los mensajes enviados de forma masiva. Gracias a la compatibilidad con los encabezados de cancelación de suscripción y a la gestión centralizada de listas, ayuda a que los correos electrónicos legítimos sigan llegando a las bandejas de entrada.

Más información

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

Acerca de Proofpoint, Inc. Proofpoint, Inc. es un líder mundial en ciberseguridad centrada en las personas y los agentes, que protege la forma en que las personas, los datos y los agentes de IA se conectan a través del correo electrónico, la nube y las herramientas de colaboración. Proofpoint es un partner de confianza para más de 80 de las empresas Fortune 100, más de 14 000 grandes empresas y millones de pequeñas organizaciones. Les ayuda a bloquear las amenazas, prevenir la pérdida de datos y reforzar la resiliencia de las personas y los flujos de trabajo de IA. La plataforma de colaboración y seguridad de datos de Proofpoint ayuda a organizaciones de todos los tamaños a proteger y responsabilizar a sus empleados, al tiempo que adoptan la IA de forma segura y con total confianza. Más información en www.proofpoint.com/es

Conecte con Proofpoint: [LinkedIn](#)

Proofpoint, Inc. Proofpoint es una marca comercial de Proofpoint, Inc. en Estados Unidos y en otros países. Todas las demás marcas comerciales contenidas en el presente son propiedad de sus respectivos propietarios.

proofpoint®

