Proofpoint Impersonation Protection

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

Ventajas principales

- Proteja las comunicaciones comerciales de confianza frente a las amenazas de suplantación.
- Evite la suplantación personal y de su marca.
- Descubra dominios parecidos maliciosos y ciérrelos.
- Detecte y protéjase contra proveedores de riesgo, incluidas las cuentas de proveedores comprometidas.
- Garantice la seguridad de los mensajes de correo electrónico de sus usuarios y aplicaciones para que sean fiables.

Este conjunto de soluciones forma parte de la plataforma Human-Centric Security, que mitiga las cuatro principales áreas de riesgo asociado a las personas.

La mayoría de las organizaciones dependen del correo electrónico para llevar a cabo su actividad comercial. Sin embargo, los atacantes han encontrado una forma de interceptar sus comunicaciones empresariales de confianza. Ahora son capaces de suplantar su identidad, la de su marca o la de sus partners comerciales. Según el FBI, los ataques de suplantación, como las estafas Business Email Compromise (BEC) han costado a empresas de todo el mundo más de 27 000 millones de dólares. Y el coste de una fuga de datos asociada a un proveedor comprometido ascendió a casi de 5 millones de dólares[1].

En los ataques de suplantación de identidad suelen utilizarse conjuntamente tácticas como la suplantación de dominios, los "lookalike domains" (dominios parecidos) y las cuentas de proveedores comprometidas. Debe proteger sus comunicaciones con partners, clientes y proveedores de confianza contra estas amenazas. Proofpoint puede ayudarle a mitigar el riesgo. Autenticamos el correo electrónico de sus usuarios y aplicaciones y le protegemos frente a cuentas de proveedores comprometidas.

Proofpoint adopta un enfoque holístico multicapa para protegerle a usted y a su marca contra la suplantación de identidad. Le proporcionamos las herramientas, la tecnología y los recursos necesarios para activar la autenticación del correo electrónico, identificar las cuentas de proveedores de riesgo o potencialmente comprometidas, y le ayudamos a descubrir "lookalike domains" (dominios parecidos) maliciosos y a eliminarlos. No solo le protegemos de los mensajes de correo electrónico generados por sus usuarios, sino que además le ofrecemos una solución segura para gestionar los mensajes de correo electrónico de aplicaciones y los mensajes enviados en su nombre por partners SaaS externos.

Evite la suplantación personal y de su marca.

Una de las tácticas más comunes de suplantación es el conocido como "domain spoofing" (suplantación de dominios). Sin los controles adecuados, los atacantes pueden apoderarse fácilmente de sus dominios de confianza. Esto les permite atacar a sus clientes, partners e incluso a sus empleados. La autenticación del correo electrónico es la manera más eficaz de impedirlo.

1 IBM. *Cost of a Data Breach Report* (Informe sobre el coste de una fuga de datos). 2023.

Proofpoint Impersonation Protection implementa el estándar DMARC para ayudarle a autenticar los mensajes de correo electrónico de sus usuarios y aplicaciones. Simplificamos la implementación de DMARC, ya que le guiamos por todos las etapas del despliegue. Nuestros expertos trabajarán con usted para identificar a sus remitentes ilegítimos. 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 seguridad para evitar las amenazas entrantes que suplantan sus dominios de confianza. También le permite pasar por alto las política 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 mensajes de correo electrónico enviados que utilizan sus dominios de confianza, incluidos los enviados por terceros.

Proteja frente a cuentas de proveedores comprometidas

Los ciberdelincuentes han convertido la cadena de suministro en otro vector de amenazas. A menudo utilizan cuentas de proveedores comprometidas para secuestrar las comunicaciones por correo electrónico entre usted y sus partners comerciales. Los mensajes de correo electrónico de proveedores comprometidos no siempre llevan cargas maliciosas y pasan la autenticación. Esto complica enormemente su detección. Y a menudo provocan grandes pérdidas financieras, extorsión de datos o ataques de ransomware.

Proofpoint Impersonation Protection ayuda a detectar y protegerse contra proveedores de riesgo, incluidas las cuentas de proveedores comprometidas. Utiliza IA basada en el comportamiento, aprendizaje automático e inteligencia sobre amenazas obtenida de nuestra amplia cartera de clientes para descubrir de forma proactiva cuentas de proveedores potencialmente comprometidas. Incluye controles adaptables, como el aislamiento automático de URL de cuentas de proveedores comprometidas, para mitigar su exposición. La integración con Proofpoint Threat Protection y el contexto en torno a las relaciones remitente-receptor agilizan la respuesta y la investigación de incidentes por parte de terceros.

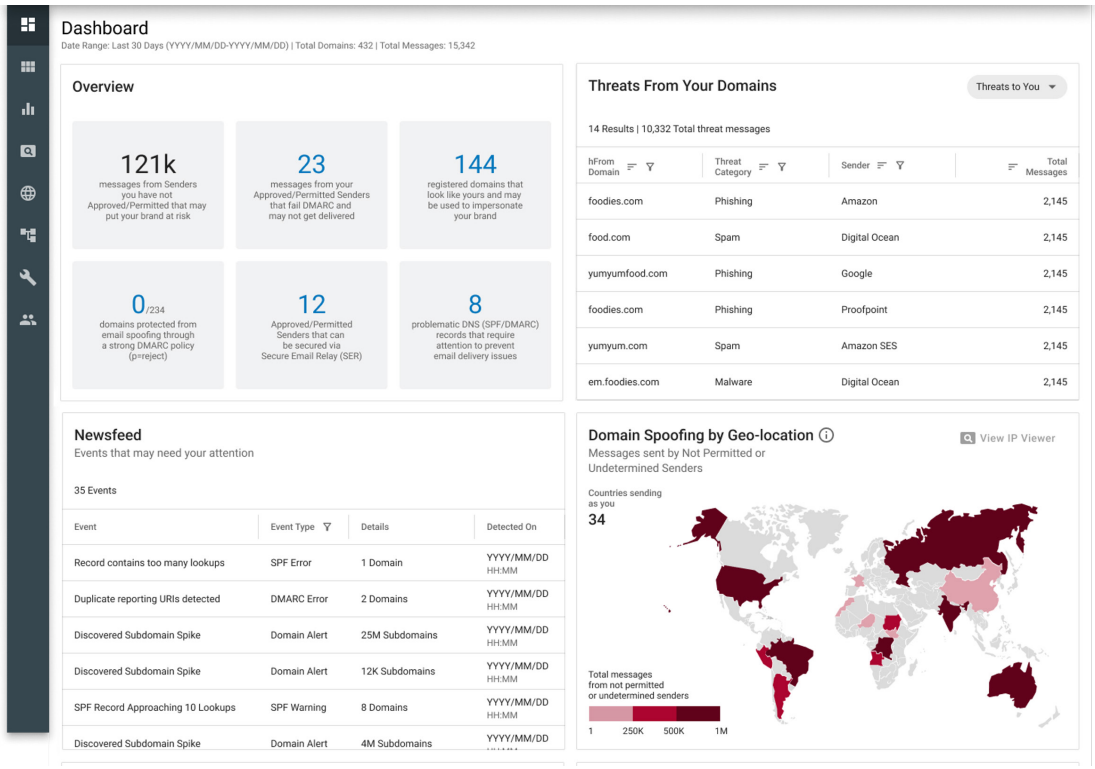

Figura 1: Proofpoint le ofrece visibilidad de las amenazas de falsificación de dominios parecidos maliciosos de sus dominios, así como los mensajes que se envían mediante sus dominios de confianza.

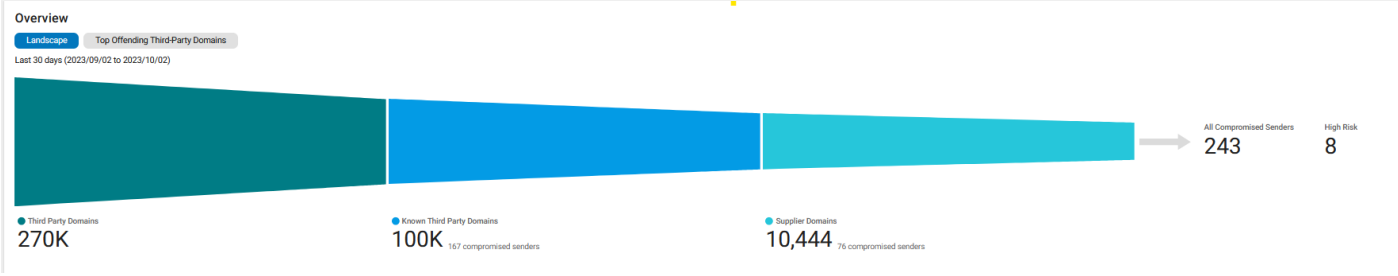

Figura 2: Proofpoint detecta cuentas de terceros potencialmente comprometidas con las que tiene una relación comercial y le proporciona visibilidad sobre los proveedores de alto riesgo.

Detecte y elimine los dominios parecidos maliciosos

Otra táctica habitual es la de engañar a los destinatarios con "lookalike domains" (dominios parecidos). En este caso, los atacantes registran nombres de dominio que se asemejan mucho a una marca o entidad legítima. La falsificación de dominios parecidos se utiliza en ataques como el phishing de credenciales, las estafas BEC e incluso en los ataques por teléfono o TOAD.

Proofpoint le ayuda a identificar dominios parecidos de sus dominios de confianza. Detectamos dinámicamente nuevos dominios registrados que se hacen pasar por su marca en ataques por correo electrónico o sitios web de phishing. Le ofrecemos una vista completa de los dominios sospechosos y le ayudamos a eliminar rápidamente los dominios fraudulentos y los sitios web con cargas maliciosas. No se trata solamente de sus dominios; también le ayudamos a detectar "lookalike domains" (dominios parecidos) de los dominios de sus proveedores. Revelamos el volumen de mensajes y los mensajes entregados desde dominios parecidos a los de sus proveedores, y de esta forma le permitimos gestionar de forma proactiva los proveedores de alto riesgo que puedan ser suplantados.

Proteja los mensajes de aplicaciones enviados en su nombre

Los mensajes de correo electrónico enviados en su nombre pueden provenir de remitentes de aplicaciones externas sobre las que no tiene control. Por ejemplo, las organizaciones utilizan Workday para enviar a sus empleados mensajes relacionados con las nóminas. Y utilizan Salesforce para enviar a sus clientes boletines informativos. Sin ningún control, esto podría dejar vulnerables los mensajes de aplicaciones que utilizan sus dominios de confianza. Una vez comprometida una aplicación de terceros o un partner SaaS, los atacantes pueden inyectar malware en correos electrónicos transaccionales que pueden parecer proceder de usted. Lo peor de todo es que estos mensajes transaccionales contaminados podrían pasar la autenticación de correo electrónico.

Proofpoint Impersonation Protection protege los mensajes de correo electrónico de sus aplicaciones y también los que se envían en su nombre. Aplicamos nuestros controles de seguridad y cumplimiento a los correos electrónicos transaccionales que utilizan sus dominios de confianza. Autenticamos estos mensajes y aplicamos nuestra detección de amenazas líder del sector para identificar malware o amenazas. Esto garantiza que sus clientes, partners comerciales y empleados únicamente reciban de usted mensajes de correo electrónico auténticos y limpios. También le proporciona un control centralizado sobre los correos electrónicos transaccionales de aplicaciones de terceros y partners SaaS. Puede bloquear el tráfico de correo electrónico de aplicaciones maliciosas de partners externos comprometidos que utilicen sus dominios en cualquier momento.

MÁS INFORMACIÓN

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