Proofpoint Secure Email Relay

Una mejor solución para controlar y proteger los mensajes de correo electrónico transaccionales de aplicaciones y partners SaaS

Ventajas principales

- Protege el correo electrónico transaccional procedente de aplicaciones internas, así como de proveedores SaaS, como Salesforce, ServiceNow y Workday.
- Acelera la implementación de la autenticación DMARC permitiendo las firmas con DKIM de los mensajes de todas las fuentes antes del envío.
- Protege su dominio de confianza frente a fraudes relacionados con remitentes comprometidos y proveedores de correo electrónico vulnerables cuyas direcciones IP se encuentran en sus registros SPF.
- Protege los datos sensibles en mensajes de correo procedentes de aplicaciones, como la información de identificación personal (PII) y la información sanitaria (PHI), aplicando cifrado de payload y prevención de la pérdida de datos.
- Sustituye las transmisiones locales por una alternativa segura basada en la nube.
- Evita interrupciones del correo electrónico de los usuarios, aislándolo del correo de la aplicación.

Proofpoint Secure Email Relay (SER) consolida y protege el correo electrónico transaccional. Impide que remitentes externos comprometidos envíen mensajes de correo maliciosos empleando sus dominios y permite la firma con DKIM para cumplir la autenticación DMARC. Como solución alojada, Proofpoint SER le ayuda a hacer realidad sus iniciativas de migración a la nube.

Las aplicaciones se están trasladando de los sistemas locales a la nube. Esta migración puede suponer una ampliación de la superficie de ataque de su organización. Los mensajes de correo electrónico enviados en su nombre pueden provenir de remitentes de aplicaciones externas sobre las que no tiene control. Esto hace que las identidades de correo electrónico sean vulnerables a la suplantación de identidad. Sin la implantación de controles adecuados, los atacantes pueden robar fácilmente la identidad de su empresa. A partir de ahí pueden hacer un uso ilícito de los entornos cloud de los remitentes autorizados. Posteriormente, pueden enviar correo electrónico malicioso en su nombre. Estos mensajes pasarían los protocolos SPF, DKIM y DMARC, y se pueden enviar directamente a sus clientes, partners y empleados.

Proofpoint SER aplica nuestros controles de seguridad y cumplimiento para los mensajes de correo electrónico transaccionales que emplean su identidad. Estos mensajes de correo electrónico se originan en aplicaciones internas o en partners SaaS externos, como como Salesforce, ServiceNow y Workday. Esto incluye facturas, códigos de autenticación, confirmaciones, etc. Puede que estén aislados del correo generado por los usuarios, pero Proofpoint SER les ofrece los mismos niveles de protección.

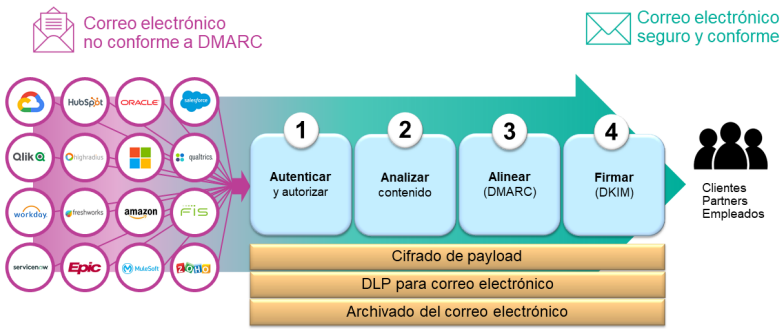

Figura 1: Proofpoint Secure Email Relay protege las aplicaciones cloud que envían correo electrónico transaccional en su nombre, y le permite aplicar controles de seguridad, como el cifrado y la prevención de la pérdida de datos (DLP), a su correo electrónico de aplicaciones.

Otros ejemplos de mensajes de correo electrónico transaccionales son:

- Notificaciones de extractos
- Notificaciones de entrega de paquetes
- Confirmaciones de pedidos
- Recibos de ventas electrónicas
- Presupuestos de seguros
- Solicitudes de comentarios o experiencia
- Notificaciones de tareas
- Notificaciones de alarmas de IoT o dispositivos
- Gestión de emergencias y alertas

Proofpoint SER hace que la autenticación DMARC resulte más sencilla al aplicar en todo el correo electrónico firmas de DKIM. Evalúa los mensajes de correo electrónico mediante tecnologías antispam y antivirus. Además, reduce los riesgos a los que se exponen los datos confidenciales aplicando cifrado de payloads y prevención de pérdida de datos del correo electrónico. Con Proofpoint SER tiene el control de la identidad de su correo electrónico. Esta solución garantiza que sus clientes, partners y empleados reciban únicamente correo electrónico auténtico de su parte.

Protección del correo electrónico de entornos vulnerables

Puede haber proveedores de servicios de correo electrónico y aplicaciones de correo electrónico con autorización para enviar correo electrónico utilizando sus dominios, sin embargo, a veces no cumplen las prácticas de seguridad recomendadas. Esto podría provocar el compromiso de cuentas o un uso ilícito de las plataformas. En ambos casos, los ciberdelincuentes pueden usar sus dominios de confianza para enviar correo electrónico malicioso que supera la autenticación del correo electrónico.

Proofpoint SER adopta un sistema cerrado que permite únicamente a las entidades empresariales verificadas utilizar nuestro servicio de transmisión de correo electrónico. Un usuario cualquiera no se puede registrar para tener una cuenta gratuita en nuestra plataforma. Esto reduce en gran medida el riesgo que suponen los proveedores de servicios de correo electrónico que son vulnerables o están comprometidos.

Proofpoint SER también acepta con seguridad el correo electrónico procedente de sus aplicaciones autorizadas, a través de la autenticación SMTP y TLS (STARTTLS). Aplica medidas antispam y antivirus de Proofpoint a cada mensaje. Proofpoint SER bloquea todo mensaje de correo electrónico que intente enviar contenido autorizado, pero malicioso, en su nombre. Además, puede consolidar el correo electrónico mediante direcciones IP de confianza y acreditadas. De esta forma, puede ocultar ante los ciberdelincuentes a los remitentes que envían correo electrónico en su nombre.

Aceleración de la implementación de la autenticación DMARC

Algunos proveedores de aplicaciones o de servicios SaaS no admiten las firmas con DKIM. Puede usar autenticación DMARC de un solo paso, que solo incluya el protocolo SPF, sin embargo, sin el protocolo DKIM, su correo electrónico legítimo carece de la redundancia de autenticación necesaria. Esto complica el reenvío de mensajes, por ejemplo. Proofpoint SER permite que estos mensajes transaccionales cumplan plenamente la autenticación DMARC mediante las firmas con DKIM de los mensajes antes del envío. De esta manera, se consiguen reglas DMARC de rechazo en sus dominios de forma más rápida para que los ciberdelincuentes no puedan suplantarlos.

Cumplimiento de normativas para correo electrónico de aplicaciones

Las aplicaciones se están migrando a la nube, y esto limita enormemente para las organizaciones las opciones de correo electrónico que cumplen los requisitos normativos. Algunas dirigen el correo electrónico de aplicaciones a través de sistemas locales, pero eso las deja desprotegidas ante entornos externos vulnerables. Otras optan por una combinación de soluciones cloud individuales, sin embargo, estas no suelen ofrecer una vista consolidada de las actividades.

Proofpoint SER le permite cumplir los estándares de las normativas con su aplicación de correo electrónico. En el correo electrónico de aplicaciones con acceso a información de identificación personal y datos sanitarios se puede cifrar el contenido o la conexión. Proofpoint SER también le permite aplicar soluciones de archivado y prevención de la pérdida de datos a su correo electrónico de aplicaciones, de modo que cumpla las normativas de SEC y FINRA.

MÁS INFORMACIÓN

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

ACERCA DE 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. Compañías líderes de todos los tamaños, entre las que se encuentra el 75 % del Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.