Proofpoint Email Fraud Defense

Ventajas principales

- Simplificación de la implementación de DMARC, ya que le guía por todos los pasos del despliegue.
- Protección de su marca en ataques de fraude por correo electrónico, sin bloquear los mensajes legítimos.
- Identificación automática de sus proveedores y el riesgo que representan.
- Visibilidad de los dominios parecidos y los mensajes enviados utilizando sus dominios de confianza.
- Integración del gateway de Proofpoint, líder del sector, para implementar DMARC con fiabilidad y flexibilidad.

Proofpoint Email Fraud Defense (EFD) simplifica la implementación de DMARC con flujos de trabajo guiados y apoyo de consultores especializados, protege la reputación de su empresa frente al fraude en el correo electrónico, y le proporciona visibilidad completa de los dominios parecidos y los mensajes enviados utilizando su dominio. Además, reduce los riesgos que presentan sus proveedores, identificándolos automáticamente y detectando los dominios parecidos que han sido registrados por terceros.

Proofpoint Email Fraud Defense le guía a lo largo de todo el proceso de implementación de DMARC. También le ayuda a proteger mejor a sus clientes, partners y empleados, frente a las estafas Business Email Compromise (BEC). Protegemos su marca frente a estafas por correo electrónico y mitigamos el riesgo de amenazas de impostores entrantes. Autenticamos todos los mensajes que entran y salen de su organización. Y lo hacemos sin bloquear el correo legítimo.

Facilidad de uso

Consultores especializados y un flujo de trabajo guiado

Creamos un proyecto para usted, con un flujo de trabajo guiado. Nuestro plan le ayuda a desplegar eficazmente la autenticación del correo electrónico. Nuestros consultores le ayudarán en todos los pasos del despliegue. Trabajamos con usted para identificar a todos sus remitentes legítimos, incluidos los externos, para garantizar su correcta autenticación. Analizamos su entorno específico de correo electrónico para ayudarle a priorizar las tareas según sus necesidades y criterios, como el volumen de correo electrónico y los principales remitentes.

Servicios de autenticación alojados

Proofpoint Email Fraud Defense incluye tanto SPF alojado como DKIM alojado. Esto facilita la configuración y la administración, además de aumentar la seguridad.

SPF alojado

- Ayuda a superar el límite tradicional de consulta de DNS (10).
- Reduce la sobrecarga que implica realizar cambios en el registro de SPF.
- Actualiza los registros en tiempo real.
- Mejora la seguridad de SPF ya que impide el registro excesivo.

DKIM alojado

- Simplifica la configuración y administración de selectores y claves de DKIM.
- Ofrece opciones flexibles de alojamiento de selectores de DKIM (delegado o no delegado).
- Admite el protocolo DNSSEC.
- Crea servicios distribuidos geográficamente y tolerantes a fallos.
- Simplifica la importación de selectores de DKIM y claves públicas.

Protección integral de la marca

Proofpoint Email Fraud Defense evita que se envíen mensajes fraudulentos utilizando sus dominios de confianza. Protegemos su marca y la reputación de su empresa en ataques de fraude por correo electrónico.

Identificación de dominios parecidos al suyo

Proofpoint Email Fraud Defense aprovecha la información obtenida por Proofpoint Domain Discover. Identifica automáticamente los dominios parecidos al suyo. Detectamos dinámicamente nuevos dominios registrados que se hacen pasar por su marca en ataques por correo electrónico o sitios web de phishing. Analizamos millones de dominios y relacionamos sus datos de registro con nuestros propios datos sobre actividad del correo electrónico y ataques activos. De esta forma, ofrecemos una visión completa de los dominios sospechosos. Mostramos cómo los ciberdelincuentes suplantan su marca. Recibe alertas instantáneas cuando los dominios sospechosos pasan de estado inactivo a activo (con carga maliciosa).

Con el complemento (add-on) Virtual Takedown, puede reducir la exposición de particulares, partners y empleados a dominios maliciosos parecidos al suyo. También puede eliminar el dominio con el proveedor de registro o alojamiento. Puede exportar dominios para que se bloqueen en el gateway de correo electrónico de Proofpoint.

Visibilidad total de su ecosistema de correo electrónico completo

Proofpoint Email Fraud Defense le ofrece visibilidad de todos los mensajes enviados utilizando sus dominios de confianza. Esto incluye los destinados a buzones de particulares, gateways de empresas y su propio gateway.

Nuestro completo panel le muestra:

- Cuáles de los atacantes de su dominio han intentado el secuestro de cuentas.
- La tasa de fraudes de cada dominio.
- Sus políticas y sus porcentajes de aprobación de DMARC, SPF y DKIM.
- Los remitentes autorizados y sus correspondientes registros de DMARC.

Proofpoint Email Fraud Defense le ofrece información práctica y recomendaciones. Esto facilita el seguimiento, la gestión y la adopción de medidas en tareas abiertas. Con Proofpoint Email Fraud Defense, no tiene que preocuparse por no aprobar la autenticación DMARC o bloquear mensajes de correo electrónico válidos mientras impide a los atacantes suplantar sus dominios.

Visibilidad de los riesgos de proveedores

Proofpoint Email Fraud Defense no se limita a implementar DMARC, sino que ofrece visibilidad del riesgo que suponen sus proveedores. La función Nexus Supplier Risk Explorer identifica automáticamente a sus proveedores, valida sus registros de DMARC y descubre el riesgo que representan. Esto incluye las amenazas de impostores, el phishing, el malware y el spam. Revelamos el volumen de mensajes y los mensajes entregados desde dominios parecidos a los de sus proveedores. Puede seguir investigando cualquier amenaza potencial. Al clasificar por prioridades el nivel de riesgo del dominio de cada proveedor, le ayudamos a centrarse en los incidentes más críticos.

Integración con el gateway de correo electrónico de Proofpoint

Proporcionamos integración real entre la autenticación del correo electrónico y el gateway de correo electrónico seguro. Cuando se combina con el gateway de correo electrónico de Proofpoint, líder del sector, Proofpoint Email Fraud Defense mitiga el riesgo de amenazas de impostores, implementando DMARC en su tráfico entrante. Le ayudamos a verificar la reputación de DMARC de un dominio concreto, de manera que su gateway no bloquee el correo legítimo que por algún motivo no supera la autenticación DMARC. Además, le ayudamos a crear políticas que se omiten para el correo electrónico válido, sin poner en riesgo su nivel de seguridad.

MÁS INFORMACIÓN

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