Proofpoint Email DLP y Proofpoint Email Encryption

Protección de los usuarios contra los ataques que les incitan a enviar información sensible a través del correo electrónico

Ventajas principales

- Administración e implementación centralizadas de la prevención de la fuga de datos y del cifrado del correo electrónico en nuestro gateway del correo electrónico líder del sector.
- Integración con la plataforma Proofpoint Information and Cloud Security y gestión integral de todos los casos de pérdida de datos centrada en las personas.
- Análisis y clasificación de la información confidencial en los datos estructurados y no estructurados,
- Experiencia transparente para el usuario y los dispositivos móviles.

Cumplimiento de normativas

- Más de 240 clasificadores integrados
- Norma PCI, ley SOX, ley GLBA, términos relativos al delito de iniciado definidos por la SEC, así como otras plantillas internacionales específicas para cada país
- RGPD, ley británica de protección de datos, directiva europea sobre la protección de datos, ley canadiense sobre la protección e información personal y documentos electrónicos, números de tarjetas de crédito de Japón
- Código PII, ley HIPAA, ICD-9, ICD-10, Código nacional de medicamentos de Estados Unidos, así como otros códigos sanitarios

Proofpoint Email Data Loss Prevention (DLP) y Proofpoint Email Encryption ofrecen un nivel de visibilidad e implementación inigualables, sin la complejidad y los costes asociados a soluciones individuales. Estas soluciones aseguran la clasificación automática de datos y un cifrado transparente, gestionados de forma centralizada en el gateway. Además, mejoran la experiencia de administración con la definición e implementación de políticas en todo el entorno de correo electrónico.

Proofpoint Email DLP y Proofpoint Email Encryption le ofrecen mayor control de sus datos sensibles, y de esta forma le permiten responder mejor a sus requisitos de cumplimiento. Estas soluciones ayudan a proteger a los usuarios de ataques que les incitan a enviar información sensible por correo electrónico. El correo electrónico es el vector número uno de entrada de amenazas, pero también es un vector crítico para la pérdida de datos de salida.

Proofpoint Email DLP — Prevención de fugas de datos potenciales

Proofpoint Email DLP clasifica los datos sensibles con precisión y detecta las filtraciones de datos por correo electrónico. Impide que los datos sensibles salgan de su empresa sin su conocimiento

Coincidencia exacta de datos

Proofpoint Email DLP incluye una función de coincidencia exacta de datos, que detecta los datos sensibles que deben protegerse. Le permite cargar o crear fácilmente diccionarios e identificadores personalizados para detectar información específica de su empresa. Puede, por ejemplo, utilizar números de cuentas de servicios financieros, formularios locales de identificación y números de historias clínicas para analizar los datos del correo electrónico más importantes para su empresa. También puede ampliar los diccionarios existentes para incluir términos y códigos personalizados. Por último, puede utilizar definiciones basadas en direccionamiento con el fin de crear políticas para mensajes entrantes y salientes.

Protección frente al fraude por correo electrónico

Proofpoint Email DLP cuenta con más de 240 clasificadores configurados específicamente. Estos clasificadores pueden identificar, clasificar y bloquear automáticamente los mensajes que normalmente se utilizan como parte de ataques Business Email Compromise (BEC). Reducen enormemente el riesgo de enviar a impostores registros de empleados, formularios fiscales y transferencias bancarias.

Análisis en profundidad y asignación de huellas digitales

Proofpoint Email DLP permite detectar con precisión los datos confidenciales dentro del contenido no estructurado. Con nuestra solución puede:

- Analizar más de 300 tipos de archivos directamente.
- Garantizar que los datos confidenciales en archivos adjuntos, distintos de los estándar de Microsoft Office y PDF, se gestionan de manera adecuada.
- Utilizar nuestro generador de perfiles de tipos de archivos para ampliar la compatibilidad a tipos de archivos nuevos, personalizados y propietarios, como las patentes y las notas de servicio.
- Analizar la huella digital de documentos sensibles, con funciones de coincidencia total y parcial, incluso si los datos residen en formatos de archivos diferentes.

Cumplimiento automatizado de la normativa regulatoria

Proofpoint Email DLP no se limita a la simple coincidencia con expresiones regulares. Descubre rápidamente los datos confidenciales expuestos gracias a los diccionarios predefinidos. Proofpoint Email DLP ofrece las siguientes ventajas:

- Detección extremadamente fiable de las comunicaciones que no cumplen las normativas.
- Verificaciones algorítmicas detalladas integradas en identificadores inteligentes.
- Reducción al mínimo de falsos positivos para los números de tarjetas de crédito y documentos de identificación, así como una amplia variedad de datos confidenciales.
- Análisis avanzados de proximidad y de correlación, para una detección optimizada de múltiples elementos.

Los términos del diccionario se pueden ponderar para incrementar o reducir el valor de la coincidencia de cualquier término o bien permitir excepciones.

Mejora de la eficacia operativa

Integración con la plataforma Information and Cloud Security
Proofpoint Email DLP se integra con la plataforma Proofpoint Information and Cloud Security. Esta integración permite unificar nuestras soluciones DLP líderes del mercado para el correo electrónico, la nube y los endpoints. Nuestra plataforma combina telemetría de contenido, comportamiento y amenazas procedente de estos canales. Esto le permite abordar el espectro completo de casos de pérdida de datos centrados en las personas de manera integral a través de una interfaz de gestión de alertas unificada. Los clasificadores de datos comunes le permiten desplegar políticas de DLP coherentes en distintos canales. De esta forma ahorra tiempo y molestias de administración.

Smart Send
La función Smart Send permite a los remitentes de correo electrónico solucionar sus propias infracciones de políticas en mensajes salientes. Esta potente herramienta es fácil de administrar, ayuda a educar a los usuarios y al mismo tiempo libera recursos de TI para que puedan dedicarse a tareas más estratégicas. También puede definir el direccionamiento en función de políticas, con el fin de redirigir los recursos confidenciales de vuelta al usuario, a Recursos Humanos, a TI o a cualquier otra persona.

Informes en tiempo real
Proofpoint Email DLP proporciona la visibilidad y el flujo de trabajo para ayudarle a tomar decisiones rápidamente y aplicar las medidas oportunas. Esta solución permite ver estadísticas y tendencias en tiempo real, gestionar los incidentes actuales y realizar las acciones adecuadas con los mensajes no conformes, todo ello desde un panel centralizado. Además puede analizar cada incidente de forma detallada, mostrando en una vista colateral las regiones de un mensaje o archivo adjunto para ver las coincidencias respecto al documento de formación o política original. Asimismo puede comentar, realizar el seguimiento y buscar las infracciones en el administrador de incidentes, así como exportar los mensajes correspondientes.

Los informes gráficos muestran las infracciones a lo largo del tiempo. Puede organizarlas por política, usuario, infractores principales, etc. Puede ver las tendencias para identificar las áreas de éxito y las oportunidades de mejora. Los informes se pueden enviar por correo electrónico según un calendario establecido o publicarse en una intranet para ahorrar tiempo.

Proofpoint Email Encryption — Cifrado, visibilidad y controles garantizados

Proofpoint Email Encryption utiliza un motor de DLP basado en políticas. Sus robustos controles ofrecen las siguientes ventajas:

- Posibilidad de definir políticas de cifrado.
- Aplicación dinámica de políticas a nivel mundial, de grupos y usuarios gracias a la integración en LDAP o AD.
- Posibilidad de definir el cifrado en función del destino. Puede, por ejemplo, incluir un partner, un proveedor, los atributos del remitente y del mensaje, como los tipos de adjuntos.

Proofpoint Email Encryption también puede servir como TLS de seguridad, para garantizar un mecanismo de cifrado fiable.

Con Proofpoint Email Encryption, puede:

- Garantizar la seguridad de las comunicaciones empresariales.
- Proteger las comunicaciones entre los grupos o usuarios, ya que ofrece una función de cifrado de comunicaciones internas y elimina la necesidad de redirigir el correo al exterior o desplegar otra solución que puede ser difícil de adoptar.
- Obtener la revocación granular de los mensajes cifrados. La solución permite a los usuarios revocar, hacer que caduque o restaurar el acceso al correo cifrado, sin afectar a otros usuarios u otros mensajes enviados al mismo destinatario.

Administración de claves sin intervención

Puede eliminar la carga administrativa derivada de la administración de claves y centrarse en sus necesidades de cifrado. Las claves se generan, almacenan y gestionan con seguridad. Su gestión a través de nuestra infraestructura en la nube garantiza una alta disponibilidad. Las claves se almacenan aparte del contenido de correo electrónico para garantizar la privacidad y la seguridad.

Mejora de la experiencia del destinatario

Ofreciendo una experiencia de usuario transparente, Proofpoint Email Encryption evita que los empleados puedan sortear las políticas. Proporcionamos múltiples opciones para permitir a los usuarios acceder a los mensajes cifrados. El método predeterminado, que se llama Secure Reader, permite al usuario hacer clic en un adjunto HTML cifrado de un mensaje. A continuación, se dirige al usuario a un portal web en el que puede acceder fácilmente al mensaje cifrado. El otro método, que se conoce como Decrypt Assist, se ha diseñado para el acceso desde dispositivos móviles. El acceso se proporciona a través de un enlace en un mensaje. Cuando los usuarios hacen clic en el enlace, se le dirige a un portal web optimizado para dispositivos móviles que le permite consultar el mensaje cifrado.

Los usuarios pueden acceder y gestionar los mensajes cifrados desde la bandeja de entrada de Secure Reader. Esto les proporciona la experiencia transparente que necesitan con los mensajes cifrados. Además, permite a la organización gestionar con facilidad los mensajes que se reciben. El complemento para Outlook unificado permite a los usuarios enviar y leer fácilmente mensajes cifrados con solo pulsar un botón. Y puede activar el cifrado de mensajes internos para la comunicación confidencial entre empleados.

MÁS INFORMACIÓN

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