Proofpoint Email Data Loss Prevention e Email Encryption

VENTAJAS PRINCIPALES

- Administración e implementación centralizadas de cifrado y DLP del correo electrónico en nuestro gateway del correo electrónico, líder del sector.
- Integración con Proofpoint Enterprise DLP y gestión integral de todos los casos de pérdida de datos, centrados en las personas.
- Análisis y clasificación de la información confidencial, tanto en los datos estructurados como sin estructurar.
- Experiencia transparente para el usuario y los dispositivos móviles.

CUMPLIMIENTO DE NORMATIVAS

- Más de 80 políticas predefinidas
- Normas PCI, SOX, GLBA, términos relativos al delito de iniciado definidos por la SEC, así como otras plantillas internacionales específicas para cada país
- Las directivas de protección de datos RGPD, UK-DPA del Reino Unido, EU-DPD de Europa y PIPEDA de Canadá, el número de seguro social de Reino Unido, los números de tarjetas de crédito de Japón
- PII, HIPAA, ICD-9, ICD-10, el código nacional de medicamentos de Estados Unidos, así como otros códigos sanitarios

Proofpoint Email DLP e Email Encryption ofrecen un nivel de visibilidad e implementación inigualable, sin la complejidad y los costes que implican las soluciones individuales. Estas soluciones proporcionan clasificación de datos automática y 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.

El correo electrónico es el vector número uno de entrada de amenazas. También es un vector crítico para la pérdida de datos que salen de la organización. Con Email DLP e Email Encryption, puede incrementar el control de sus datos confidenciales. De esta forma, cumplirá los requisitos normativos. Además, contará con una capa fundamental de protección frente a ataques que engañan a sus empleados para que envíen información confidencial a través del correo electrónico.

Prevención de fugas de datos potenciales

Email DLP detecta los datos sensibles y la información confidencial, y evita que se filtren fuera de la organización a través del correo electrónico. Esta herramienta clasifica la información confidencial y detecta las fugas de datos por correo electrónico. Además, impide que los datos críticos salgan de la organización.

Coincidencia exacta de datos

La función de coincidencia exacta de datos de Email DLP le permite cargar o crear fácilmente diccionarios o identificadores personalizados, especiales para su organización. Por ejemplo, emplea números de cuentas de servicios financieros, formularios locales de identificación y números de historias clínicas, para analizar los datos del correo electrónico que le interesan. Puede ampliar los diccionarios existentes para incluir términos y códigos que sean específicos para la organización. La coincidencia exacta de datos detecta la información confidencial relevante para su organización que debe protegerse. También puede utilizar definiciones basadas en direccionamiento con el fin de crear políticas para mensajes entrantes y salientes.

Protección frente al fraude por correo electrónico

Email DLP cuenta con más de 80 políticas configuradas que localizan, clasifican y bloquean los mensajes de forma automática. Es habitual que estos mensajes se utilicen como parte de ataques BEC (o de fraude del CEO). Estas políticas reducen enormemente el riesgo de enviar a impostores registros de empleados, formularios fiscales y transferencias bancarias.

Huellas digitales y análisis en profundidad

Email DLP detecta con precisión los datos confidenciales en el contenido no estructurado. Con Email DLP puede:

- Analizar más de 300 tipos de archivos directamente.
- Garantizar que los datos confidenciales en archivos adjuntos, distintos de los estándar de Office y PDF, se gestionan de manera adecuada.
- Ampliar la compatibilidad a tipos de archivos nuevos, personalizados o de marca registrada, como patentes y memorándums con el identificador de tipos de archivos.
- Analizar la huella digital de documentos sensibles, con funciones de coincidencia total y parcial, incluso si los datos residen en formatos de archivo diferentes.

Cumplimiento automatizado de la normativa regulatoria

Email DLP descubre rápidamente los datos confidenciales expuestos gracias a los diccionarios predefinidos. No se limita a la simple coincidencia con expresiones regulares. Ofrece:

- Detección extremadamente fiable de las comunicaciones que no cumplen las normativas.
- Verificaciones algorítmicas detalladas integradas en identificadores inteligentes.
- Minimización de falsos positivos para los números de tarjetas de crédito y documentos de identificación, así como una amplia variedad de datos confidenciales.
- Análisis avanzado de proximidad y correlación para mejorar la detección de varios 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 Enterprise DLP

Email DLP se integra con Proofpoint Enterprise DLP. Así se reúnen nuestras soluciones de DLP líderes del mercado para el correo electrónico, la nube y los endpoints. Enterprise DLP combina telemetría de contenido, comportamiento y amenazas procedente de estos canales. Esto le permite abordar el espectro completo de casos de pérdida de datos centrada en las personas de manera integral a través de una interfaz de gestión de incidentes unificada. Puede, por ejemplo, aplicar fácilmente una clasificación común para varios canales. Así, 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 avanzada herramienta de sencillo uso 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 redireccionamiento en función de políticas, con el fin de devolver los mensajes confidenciales al usuario, a recursos humanos, a TI o a cualquier otra persona.

Informes en tiempo real

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 por política, usuario, infractores principales por política, y otros datos, a lo largo del tiempo. Vea las tendencias para identificar las áreas de éxito y las oportunidades. Se pueden enviar mensajes según una planificación o bien publicarlos en una intranet para ahorrar tiempo.

Cifrado, visibilidad y controles garantizados

Email Encryption utiliza un motor de DLP basado en políticas. Sus robustos controles:

- Le permiten definir políticas de cifrado para satisfacer las exigencias de su negocio.
- Aplican políticas a nivel global, de grupo y de usuario, con integración en LDAP o AD.
- Le permiten definir el cifrado basado en el destino, por ejemplo, puede incluir atributos de partner o proveedor, destinatario y mensaje, como tipos de archivos adjuntos.

Email Encryption también puede servir como respaldo TLS para garantizar un mecanismo de cifrado a prueba de fallos.

Con 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. Nuestra infraestructura cloud garantiza su elevada disponibilidad. Las claves se guardan aparte del contenido de correo electrónico para garantizar la privacidad y la seguridad.

Mejora de la experiencia del destinatario

Para las soluciones Email DLP e Email Encryption es fundamental ofrecer al usuario una experiencia transparente, con el fin de evitar que los empleados puedan sortear las políticas que se han implementado. Proofpoint proporciona al usuario varias opciones de acceso a un mensaje cifrado. El método de predeterminado, que emplea Secure Reader, permite a un usuario hacer clic desde el mensaje en un archivo html adjunto cifrado. A continuación, se dirige al usuario a un portal web en el que puede acceder fácilmente al mensaje cifrado. El otro método se basa en la funcionalidad Decrypt Assist, que se ha diseñado específicamente para el acceso desde dispositivos móviles. Se proporciona un enlace en el mensaje para que el usuario haga clic. Desde ahí, se abre el portal web optimizado para móviles que permite acceder al 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. Una organización puede activar el cifrado de mensajes internos para la comunicación confidencial entre empleados.

MÁS INFORMACIÓN

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

ACERCA DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) 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 encuentran más de la mitad del Fortune 1000, 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**.