

Proofpoint Email DLP and Encryption

Identifique los datos sensibles en los mensajes de correo electrónico para prevenir la pérdida y automatizar el cumplimiento

Ventajas principales

- Administración e implementación centralizadas de la prevención de la pérdida de datos y del cifrado del correo electrónico en nuestro gateway del correo electrónico líder del sector.
- Detección y análisis de los datos sensibles en mensajes y adjuntos de correo electrónico.
- Integración con Proofpoint Information Protection para una gestión integral de todos los casos de pérdida de datos centrada en las personas.

Cumplimiento

- Cientos de Identificadores de datos 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
- PII, HIPAA, ICD, ICD-10, ICD-11, el código ICD -11 nacional de medicamentos de Estados Unidos, así como otros códigos sanitarios

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



El correo electrónico es un vector crítico de pérdida de datos en mensajes salientes. Por ello, una de las principales prioridades de los equipos de seguridad debe ser reducir el riesgo de que los datos confidenciales salgan de una organización. Para satisfacer los requisitos de cumplimiento, deben ser capaces de detectar y controlar los datos en los mensajes de correo electrónico. Proofpoint Email DLP and Encryption reduce el riesgo de fuga de datos a través del correo electrónico y de los adjuntos. También permite definir y aplicar dinámicamente políticas de cifrado granular para proteger el correo electrónico entre usuarios internos y partners comerciales externos.

Los datos no se pierden por arte de magia. Son los usuarios quienes los pierden. Según el informe DBIR 2023 de Verizon sobre fugas de datos¹, el 74 % de los incidentes que terminan con la exposición de datos a terceros no autorizados es atribuible al factor humano. La mayoría de los analistas señalan que los usuarios corporativos suelen perder datos. La causa subyacente en estos casos suele ser un simple descuido, siendo los usuarios negligentes las fuentes más importante de pérdida de datos a través del correo electrónico.

Proofpoint Email DLP and Encryption identifica de forma precisa la información confidencial. Detecta la filtración de datos a través del correo electrónico y detiene la pérdida de datos críticos. También le ofrece un mayor control sobre sus datos confidenciales para ayudarle a satisfacer las obligaciones de cumplimiento.

Identifique los datos específicos de su organización

Proofpoint Email DLP and Encryption identifica datos únicos de su organización. Incluye cientos de identificadores y diccionarios de datos predefinidos de eficacia probada. Esto incluye números de cuentas de servicios financieros, formularios locales de identificación y números de historias clínicas. También puede cargar o crear fácilmente diccionarios o identificadores personalizados que sean exclusivos de su organización, así como ajustar la intensidad de coincidencia de los términos del diccionario y las excepciones. Esto le permite analizar los datos de correo electrónico más relevantes para su organización.

1 Verizon. "2023 Data Breach Investigations Report" (Informe sobre las investigaciones de fugas de datos de 2022), junio de 2023.

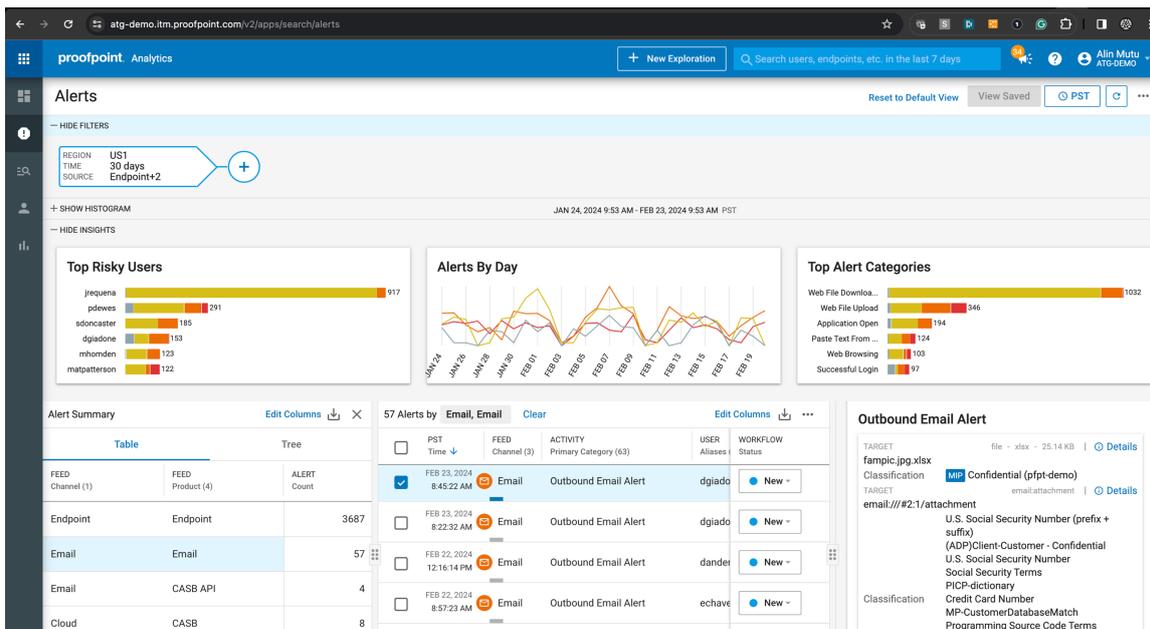


Figura 1: Proofpoint Email DLP and Encryption le permite abordar todo el espectro de escenarios de pérdida de datos centrados en las personas a través de un sistema unificado de gestión de alertas.

Análisis en profundidad y asignación de huellas digitales

Proofpoint Email DLP and Encryption permite detectar con precisión los datos confidenciales dentro del contenido no estructurado. La solución puede analizar más de 300 tipos de archivos de manera inmediata. Garantiza que los datos confidenciales en archivos adjuntos, distintos de los estándares de Microsoft 365 y PDF, se gestionen de manera adecuada. Puede utilizar nuestro generador de perfiles de tipos de archivos para ampliar la compatibilidad a tipos de archivos nuevos, personalizados y propietarios, como patentes y memorandos.

Asignación de huella digital a documentos sensibles, con funciones de coincidencia total y parcial, incluso si los datos residen en formatos de archivo diferentes. También puede emplear métodos avanzados de comparación de contenidos y extracción de texto de imágenes. Esto incluye la correspondencia de documentos indexados, la correspondencia exacta de datos y el reconocimiento óptico de caracteres (OCR).

Automatice el cumplimiento de normativas

Proofpoint Email DLP and Encryption permite buscar automáticamente todas las formas estándar de contenido restringido. Detecta rápidamente los datos confidenciales expuestos gracias a diccionarios predefinidos. Las verificaciones algorítmicas detalladas integradas en identificadores inteligentes minimizan los falsos positivos para los números de tarjetas de crédito y una amplia variedad de datos confidenciales. Análisis avanzado de proximidad y correlación para mejorar el análisis de la detección. La solución le permite respetar, entre otras, las normativas y legislaciones PCI, SOX, PII, HIPAA y RGPD.

Informes en tiempo real

Proofpoint Email DLP and Encryption proporciona la visibilidad y el flujo de trabajo para ayudarle a tomar decisiones rápidamente y aplicar las medidas oportunas. 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 o política original. Puede comentar, realizar el seguimiento y buscar las infracciones en el administrador de incidentes, así como exportar los mensajes correspondientes.

Mejore de la eficacia operativa

La prevención de la pérdida de datos a través del correo electrónico es parte de nuestro enfoque Enterprise DLP. Esto le permite encontrar, rastrear y proteger los datos mientras los usuarios trabajan en el correo electrónico, las aplicaciones cloud y los endpoints. Combina el contenido, el comportamiento y la telemetría de amenazas de estos canales, lo que le permite abordar todo el espectro de escenarios de pérdida de datos centrados en las personas a través de un sistema unificado de gestión de alertas. Puede, por ejemplo, aplicar fácilmente detectores de datos comunes para desplegar políticas de DLP coherentes en todos los canales, y ahorrar así un tiempo precioso y evitar las molestias asociadas a la administración.

Políticas de enrutamiento como Smart Send facilitan el trabajo de los analistas de DLP. Los mensajes de correo electrónico pueden devolverse al remitente para la autocorrección de las infracciones de las políticas en mensajes salientes, o enrutarse a otro destinatario, como el departamento de RR. HH., TI o el propietario de la empresa, como parte del flujo de trabajo.

Cifrado, visibilidad y controles garantizados

Proofpoint Email DLP and Encryption garantiza la seguridad de las comunicaciones empresariales. Protege las comunicaciones externas e internas con un sólido conjunto de controles y administración de claves sin intervención. Gracias a un motor de DLP basado en políticas, la solución le permite definir y aplicar dinámicamente políticas de cifrado granular a nivel mundial, de grupos y usuarios gracias a la integración en LDAP y Active Directory

Puede automatizar el cifrado en función del destino (por ejemplo, un partner, un proveedor), los atributos del remitente o del mensaje como los tipos de adjuntos. O pueden permitir a los usuarios que apliquen el cifrado de forma selectiva. El cifrado del correo electrónico también sirve como respaldo TLS para garantizar de cifrado a prueba de fallos. Los destinatarios disponen de opciones flexibles para acceder a los mensajes cifrados, como un portal web, un navegador móvil o un cliente de Outlook.

Para una comunicación fluida y segura con partners comerciales que también utilizan Proofpoint Email DLP and Encryption, nuestra función Trusted Partner Encryption proporciona a sus usuarios una experiencia transparente. Los mensajes se cifran mediante el gateway de envío. Y el gateway de Proofpoint para partners comerciales los descifra automáticamente antes de que se entreguen a la infraestructura de correo interna.

Mejora de la experiencia del destinatario

Ofreciendo una experiencia de usuario transparente, Proofpoint Email DLP and Encryption evita que los empleados puedan sortear las políticas. La solución proporciona múltiples opciones para permitir a los usuarios acceder a los mensajes cifrados, concretamente:

- **Secure Reader:** permite a los usuarios hacer clic en un adjunto HTML cifrado de un mensaje o en un enlace de un mensaje de correo electrónico. A continuación, dirige al usuario a un portal web en el que puede acceder fácilmente al mensaje cifrado.
- **Bandeja de entrada de Secure Reader:** proporciona a los usuarios una experiencia transparente a la hora de gestionar los mensajes cifrados. Además, permite a la organización gestionar con facilidad los mensajes.
- **Complemento (add-on) para Microsoft Outlook:** permite a los usuarios enviar y leer fácilmente mensajes cifrados con solo pulsar un botón.
- **Cifrado interno:** permite la comunicación confidencial entre empleados.

Experiencia que reduce el plazo de rentabilización

La prevención de la pérdida de datos es una tarea complicada que requiere algo más que conocimientos técnicos y del producto. También requiere un profundo conocimiento de los objetivos del programa, la gobernanza de datos y la custodia de datos. Podemos ser un partner de confianza en sus esfuerzos para garantizar el éxito de su programa de DLP. Nuestro servicio gestionado le ofrece una experiencia que le ayuda a optimizar su inversión en tecnología, facilitar la continuidad de sus operaciones y madurar su estrategia de protección de datos.

MÁS INFORMACIÓN

Para obtener más información, visite [proofpoint.com/es](https://www.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 85 % 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.

©Proofpoint, Inc. Proofpoint es una marca comercial de Proofpoint, Inc. en Estados Unidos y en otros países. Todas las marcas comerciales mencionadas en este documento son propiedad exclusiva de sus respectivos propietarios.