Proofpoint Adaptive Email DLP

Impida la pérdida de datos confidenciales mediante el refuerzo de la prevención (DLP) basada en reglas con IA

Ventajas principales

- Prevenga la pérdida de datos accidental o intencionada a través del correo electrónico.
- Mitigue los riesgos reputacionales y pérdida de clientes.
- Reduzca las multas por incumplimiento del RGPD y ley de Privacidad del Consumidor de California (California Consumer Privacy Act, CCPA).
- Mejore la concienciación en materia de seguridad en toda la organización.

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

A pesar de los controles de prevención de pérdida de datos (DLP) por correo electrónico existentes, el tipo de infracción de datos del RGPD más denunciado es "datos enviados por correo electrónico a la persona equivocada". Aunque la DLP basada en reglas desempeña un papel fundamental en la protección de datos sensibles conocidos, como la información de identificación personal (PII), los número de DNI y los datos de tarjetas de pago, hay riesgos que no consigue detectar. Por ejemplo, el envío de datos confidenciales a la persona equivocada o la filtración de datos por parte de los empleados a sí mismos y a otros destinatarios no autorizados.

Adaptive Email DLP utiliza IA basada en el comportamiento para conocer los comportamientos habituales de envío de correo electrónico de sus empleados, sus relaciones de confianza y la forma en que comunican datos confidenciales. A continuación, analiza cada correo electrónico para detectar comportamientos anómalos y notificar a los administradores posibles incidentes de pérdida de datos. Además, advierte al usuario en tiempo real y evita la pérdida de datos confidenciales a través del correo electrónico.

Impida el envío de mensajes de correo electrónico al destinatario equivocado

Esta situación se produce cuando un usuario envía de manera accidental un mensaje a la persona equivocada. Es una causa frecuente de fugas de datos en todas las organizaciones. Además, resulta complicado de evitar con enfoques basados en reglas.

Adaptive Email DLP es capaz de bloquear estas fugas. Utiliza gráficos de relaciones, inspección profunda de contenidos y análisis de comportamiento para comprender el comportamiento típico de los empleados e identificar incidentes de pérdida de datos. Esto significa que los datos confidenciales de su organización están protegidos cuando los correos electrónicos se envían al destinatario equivocado o los empleados comparten el archivo adjunto equivocado.

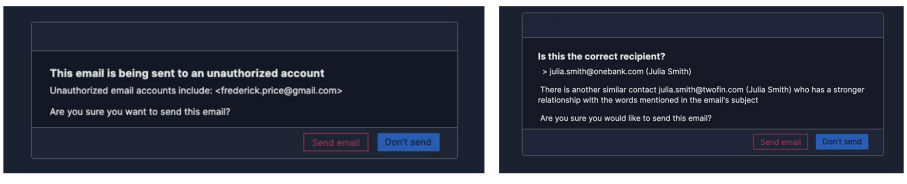

Figura 1: Adaptive Email DLP advierte a los usuarios en tiempo real sobre mensajes que podrían enviarse a las personas equivocadas para evitar la pérdida de datos confidenciales a través del correo electrónico.

Figura 2: Los equipos de seguridad tienen mayor seguridad a la hora de detectar la pérdida de datos a través del correo electrónico.

Evite los archivos adjuntados incorrectamente

Esta situación se produce cuando se envía un mensaje de correo electrónico a la persona correcta, pero en el que adjunta accidentalmente el archivo equivocado.

Cuando la IA basada en el comportamiento detecta un archivo adjunto que parece inusual para un destinatario, Adaptive Email DLP se encarga de resolver el problema. Avisa automáticamente al usuario en tiempo real antes de que se envíe inadvertidamente información sensible a la persona equivocada.

Bloquee la filtración por correo electrónico

La DLP basada en reglas es fundamental para evitar la pérdida de datos confidenciales, pero solamente para riesgos predefinidos, como los de información de identificación personal (PII), tarjetas de crédito (PCI) y documentos de identificación nacional (por ejemplo, DNI). Las fugas de datos siguen produciendo porque los usuarios internos comparten datos confidenciales que no están predefinidos en correos electrónicos personales y otras cuentas no autorizadas.

Adaptive Email DLP bloquea la filtración de datos confidenciales mediante la clasificación automática de este tipo de información. También identifica las cuentas de correo electrónico personales de los usuarios en función de sus hábitos de uso del correo electrónico. Esto permite a la solución bloquear o rastrear automáticamente los intentos de filtración de datos a sí mismo o a otros en función de la configuración.

Forme inmediatamente a los usuarios

La formación en tiempo real de los usuarios puede ayudarles a evitar errores e infracciones de las normas antes de que se produzcan. Como complemento a la formación sobre concienciación en materia de seguridad, Adaptive Email DLP enseña en tiempo real a sus usuarios los riesgos detectados en sus mensajes de correo electrónico. Esto les permite corregir sus errores y evitar incidentes de pérdida de datos sensibles.

MÁS INFORMACIÓN

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