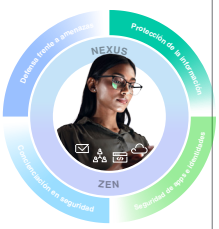
Prevención de la pérdida de datos en fusiones y adquisiciones

Utilice Proofpoint Adaptive Email DLP para detener pérdidas de datos sensibles fusiones y adquisiciones

Ventajas principales

- Prevenga la pérdida de datos accidental o intencionada a través del correo electrónico.
- Evite daños en la reputación de su empresa.
- Mejore la concienciación en seguridad en toda la empresa.
- Consiga una seguridad eficaz del correo electrónico con una administración sencilla y con un impacto mínimo en la actividad de los usuarios.
- Disfrute de una rápida rentabilización, con protección en tan solo 48 horas.

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



Las fusiones y adquisiciones aumentan enormemente el número de personas que comparten información confidencial entre empresas por correo electrónico. Para los equipos de seguridad de la información, también es difícil hacer un seguimiento de todos los empleados y terceros implicados. Estos factores aumentan el riesgo de que se filtren datos sensibles.

Proofpoint Adaptive Email DLP (que significa prevención de la pérdida de datos) resuelve estos problemas. Adaptive Email DLP utiliza inteligencia artificial basada en el comportamiento para analizar los patrones de correo electrónico de sus empleados, sus relaciones de confianza y la manera en que comparten los datos confidenciales. Nuestro producto analiza los mensajes de correo electrónico para detectar comportamientos inusuales y notificarlos a los administradores. Además, alerta a los usuarios en tiempo real, antes de que se filtren datos sensibles.

Por qué las fusiones y adquisiciones aumentan el riesgo

Durante las fusiones o adquisiciones, las empresas deben compartir mucha información altamente confidencial, como datos de los empleados, documentos del consejo de administración, datos sobre capital privado y otros tipos de inteligencia.

Según la investigación de Gartner, estas transacciones aumentan el riesgo de pérdida de datos de las siguientes maneras:

- Podría haber conflictos entre las prácticas de seguridad de ambas empresas.
- La incertidumbre o el secretismo sobre la transacción pueden provocar situaciones de ansiedad. Esto puede llevar a los empleados a actuar de forma inusual o perjudicial.
- A menudo surgen nuevas necesidades técnicas. Por ejemplo, tras el cierre de la transacción, las empresas pueden tener que asegurar tres modos de funcionamiento diferentes: el modo de cierre, el de transición y el de futuro. La superficie de ataque es mucho mayor durante este período.

Cómo protege Adaptive Email DLP los datos confidenciales

La pérdida de datos confidenciales puede dañar la reputación de su empresa y ser costosa de solucionar. Adaptive Email DLP evita este riesgo. Nuestro producto utiliza IA basada en el comportamiento para detectar y detener la pérdida accidental e intencionada de datos a través del correo electrónico. La IA analiza más de 12 meses de datos de correo electrónico para conocer los patrones de correo electrónico de sus empleados, sus relaciones de confianza, y su forma de gestionar los datos confidenciales.

Adaptive Email DLP utiliza este entrenamiento de IA para reconocer el comportamiento anómalo del correo electrónico cuando se produce. Por ejemplo, que un empleado envíe un correo electrónico al destinatario equivocado, envíe datos confidenciales a una cuenta menos segura o no autorizada, o filtre información deliberadamente. Cuando se detectan problemas, Adaptive Email DLP muestra a los usuarios mensajes de advertencia en tiempo real. Los usuarios pueden corregir sus acciones para evitar la pérdida de datos, sin intervención adicional de un administrador.

Para las fusiones y adquisiciones, estas características significan que Adaptive Email DLP evita que los datos confidenciales acaben en manos equivocadas, al tiempo que mantiene el flujo de las comunicaciones críticas.

Impida el envío de mensajes de correo electrónico al destinatario equivocado

Esta situación se produce cuando un usuario envía un mensaje a la persona equivocada. Es una causa frecuente de filtración de datos en las empresas. También son difíciles de bloquear con normas y políticas. Gracias a que aprende los hábitos de correo electrónico de los empleados, Adaptive Email DLP advierte a los usuarios sobre mensajes con el destinatario equivocado antes de que los envíen.

Evite adjuntar archivos equivocados

Esta situación se produce cuando se envía un mensaje de correo electrónico a la persona correcta, pero en el que se adjunta el archivo equivocado. Como en el caso de los mensajes enviados a las personas equivocadas, Adaptive Email DLP utiliza IA para detectar los adjuntos erróneos, y advierte a los usuarios en tiempo real.

Bloquee la filtración por correo electrónico

Las reglas de correo electrónico pueden ser eficaces a la hora de bloquear la pérdida de datos. Sin embargo, solo funcionan para tipos de datos conocidos y predefinidos, como los datos de identificación personal (PII), los del sector de las tarjetas de pago (PCI) y los documentos nacionales de identidad (DNI).

Adaptive Email DLP identifica y clasifica sus datos confidenciales. También conoce las cuentas de correo electrónico personales de los usuarios en función de sus hábitos de uso del correo electrónico. Si un empleado intenta enviar datos confidenciales a sí mismo o a otros, nuestro producto puede bloquear o rastrear sus acciones, en función de su configuración.

Figura 1: Adaptive Email DLP advierte a los usuarios en tiempo real sobre los mensajes dirigidos a los destinatarios equivocados.

Figura 2: El panel de Adaptive Email DLP ofrece a los equipos de seguridad de la información visibilidad completa de las amenazas de correo electrónico.

Forme a los usuarios en tiempo real

La formación en tiempo real ayuda a los usuarios a evitar errores e infracciones de las políticas. Como complemento a la formación para concienciar en materia de seguridad, Adaptive Email DLP enseña en tiempo real a los usuarios los riesgos detectados en sus mensajes de correo electrónico, de esta forma pueden corregir los errores de manera inmediata y evitar así filtraciones de datos.

Conozca las amenazas

El panel de Adaptive Email DLP ofrece a un equipo de seguridad de la información una instantánea de todos los mensajes de correo electrónico que el sistema está comprobando. El panel muestra los mensajes de riesgo detectados y bloqueados (incluidos los enviados a los destinatarios equivocados y los archivos adjuntados erróneamente), así como los intentos de filtración a través del correo electrónico. También muestra las mejoras de seguridad a lo largo del tiempo para los usuarios y para la empresa.

Datos como las principales políticas personalizadas y los usuarios de mayor riesgo ayudan a los analistas a centrarse en lo más importante. Estos detalles permiten acelerar las investigaciones y ayudan a los equipos de seguridad a trabajar con los usuarios para mejorar las prácticas en materia de manipulación de datos.

Administre fácilmente

Adaptive Email DLP requiere un mínimo de configuración. En tan solo 48 horas empieza a prevenir la pérdida de datos por correo electrónico. Además, proporciona intervenciones de seguridad precisas y eficaces, sin interrumpir los flujos de trabajo normales de sus usuarios.

MÁS INFORMACIÓN

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