proofpoint.

Guía de compra de soluciones de prevención de la pérdida de datos

Esta guía de compra destaca las características más importantes de una solución moderna de protección de la información. Resume los conocimientos adquiridos por Proofpoint en el desarrollo de programas eficaces de prevención de la pérdida de datos (DLP) para organizaciones de todos los tamaños en todo el mundo y en todos los sectores. Esta guía práctica le ayudará, tanto si acaba de empezar su trayecto de prevención de pérdida de datos como si desea modernizar sus sistemas de DLP existentes.

Seguridad centrada en las personas

Para proteger los datos contra las amenazas comunes y únicas, necesita una plataforma que admita un modelo de seguridad centrado en las personas, o lo que es lo mismo, una plataforma que ofrece una visibilidad completa de las interacciones de los usuarios con los datos sensibles y la supervisión de los comportamientos de riesgo. Esto le proporciona información contextual importante sobre sus intenciones en el momento de la pérdida o robo de datos, o su comportamiento aparentemente sospechoso.

Gracias a una solución centrada en las personas, puede evaluar rápidamente los riesgos de pérdida de datos a través del correo electrónico, los endpoints y aplicaciones cloud como Microsoft 365, Google Workspace y Salesforce. Esta información le permite intervenir rápidamente y tomar las medidas necesarias para evitar cualquier pérdida de datos.

Elementos clave de una solución DLP moderna

Si desea gestionar las pérdidas de datos y bloquear las amenazas internas, debe ser capaz de detectar, analizar, prevenir y neutralizar los incidentes. Para limitar sus riesgos, es necesario coordinar todas estas operaciones.

Supervisión

Para proteger los datos, no puede centrarse únicamente en el contenido. Necesita visibilidad de las interacciones de los usuarios de usuarios con los datos. Cuando supervisa las actividades de datos de todos los usuarios a través de los endpoints, el correo electrónico, la nube y la web, obtiene una visión global e información contextualizada.

85 %

de las organizaciones denunciaron uno o varios incidentes de pérdida de datos el año pasado.

50 %

Porcentaje de empleados que han cambiado de empleo en el transcurso de los últimos dos años y que admitieron haberse llevado con ellos datos de la empresa

Detección

Necesita una solución capaz de detectar, en tiempo real o casi real, las acciones peligrosas de un usuario o la posible exposición de los datos, aunque no se transforme en un verdadero incidente. Las funciones de detección deben encontrar el mejor compromiso entre alertas oportunas y procesables y el riesgo de reducir la vigilancia debido al creciente número de alertas.

Análisis

Es la capacidad de analizar tendencias en el comportamiento de los usuarios y buscar amenazas, lo que solo es posible si la solución de DLP combina la actividad de los usuarios en varios canales. Esto le permitirá detectar cualquier comportamiento de riesgo de los usuarios. Aunque este proceso puede automatizarse, es esencial recurrir a analistas que puedan inspeccionar los datos en profundidad.

Respuesta

Es importante poder investigar y responder a los incidentes con rapidez y eficacia. Cuanto más tiempo persista una amenaza interna, más daño puede hacer a su reputación y a su cuenta de resultados. Una solución DLP moderna puede aplicar automáticamente reglas y neutralizar las amenazas. La automatización le ayudará a proteger sus datos más valiosos y a aumentar la eficacia de su equipo de seguridad.

Prevención

Se trata de la capacidad de impedir que un usuario infrinja, intencionadamente o no, las políticas de seguridad de su empresa. Para ello, debe formar a los usuarios, enviar recordatorios en tiempo real y bloquear las actividades de determinados usuarios si es necesario.

3 principales casos de uso

He aquí tres escenarios habituales de pérdida de datos. Todos son atribuibles a la intervención humana. Una plataforma de protección de la información centrada en las personas debe ser capaz de identificar:

- Los usuarios negligentes, que son descuidados con los datos sensibles.
- Los usuarios negligentes que exponen datos sensibles utilizando aplicaciones de IA generativa.
- Los usuarios internos maliciosos, que quieren hacer daño a la empresa.

1: usuarios negligentes y errores comunes

Los usuarios negligentes fueron la causa principal de pérdida de datos, según el informe de Proofpoint Data Loss Landscape en 2024. Estos usuarios no tienen intención de provocar una pérdida de datos. Simplemente quieren hacer su trabajo de la forma más eficaz posible. Sin embargo, sus errores pueden tener graves consecuencias: interrupción de la actividad, daños a la reputación, debilitamiento de la posición competitiva, incumplimientos normativos y multas, acciones legales, etc.

3500 M$ es el gasto total en DLP previsto a nivel mundial en 2025[1].

77 DÍAS se tarda en resolver las amenazas internas[2].

85 % de las organizaciones son objetivo de los ataques en la nube[3].

56 % de los incidentes se deben a la negligencia de los usuarios[4].

Veamos algunos ejemplos de acciones de riesgo de los usuarios:

- Enviar mensajes de correo electrónico al destinatario equivocado, con o sin archivos adjuntos.
- Visitar sitios de phishing.
- Instalar software no autorizado.
- Compartir públicamente datos y archivos confidenciales.
- Enviar por correo electrónico datos de identificación personal (PII) a una cuenta de correo personal.
- Guardar datos corporativos sensibles en dispositivos personales.

Protección frente a comportamientos negligentes

Un sistema de protección de la información eficaz y centrado en las personas bloquea las actividades de riesgo. También ofrece a los usuarios negligentes apoyo para ayudarles a identificar y cambiar su comportamiento de riesgo.

Elementos indispensables:

- **Clasificación.** Compruebe que el mensaje, los datos y el contenido se supervisan continuamente, tanto manualmente como mediante inteligencia artificial (IA), para identificar y clasificar a los usuarios de riesgo. Cuando un usuario se considera de alto riesgo, el sistema le asigna una puntuación de riesgo para proteger los datos en consecuencia.
- **Detección.** El sistema debe supervisar el correo electrónico, los documentos y los datos, evaluando constantemente los riesgos de incumplimiento. A medida que el contenido se mueve a través de múltiples canales (endpoints, correo electrónico, nube y web), es necesario analizarlo para garantizar que este movimiento o intercambio no infringe las políticas de su organización. En cuanto se detecte una infracción a través del correo electrónico, el sistema debe permitir a los equipos de seguridad bloquear el correo electrónico o rastrearlo para investigarlo más a fondo.
- **Prevención.** Hay que impedir que los usuarios filtren datos sensibles a través de todos los canales y dispositivos: mensajes de correo electrónico enviados al destinatario equivocado con o sin archivos adjuntos, memorias USB, cargas web, sincronización en la nube, impresión, etc. Si comete un error, deben recibir al instante un mensaje de advertencia contextual que les permita corregirlo y evitar la pérdida de datos en tiempo real sin necesidad de que intervenga el administrador. En caso necesario, los usuarios pueden justificar el acceso a los datos. El equipo de seguridad podrá entonces autorizar o rechazar la solicitud.

1 The Radicati Group. "Data loss prevention (DLP) market revenue forecast worldwide from 2019 to 2025" (Previsión de ingresos en el mercado de prevención de pérdida de datos entre 2019 y 2025), mayo de 2022.
2 Ponemon Institute. "2022 Cost of Insider Threats Global Report" (Informe de 2022 sobre el coste de las amenazas internas a nivel mundial), febrero de 2022.
3 Assaf Friedman y Itir Clarke (Proofpoint) "How Attackers Use Compromised Accounts to Create and Distribute Malicious OAuth Apps" (Cómo utilizan los ciberdelincuentes las cuentas comprometidas para crear y distribuir aplicaciones OAuth), mayo de 2021.
4 Ponemon Institute. "2022 Cost of Insider Threats Global Report" (Informe de 2022 sobre el coste de las amenazas internas a nivel mundial), febrero de 2022.

2: usuarios negligentes y aplicaciones de IA generativa

Cuando utilizan ChatGPT y otras herramientas de IA generativa, los usuarios pueden aumentar de manera importante su productividad. Sin embargo, a menudo están en el origen de pérdidas de datos. Para evitar las pérdidas de datos sin comprometer la productividad, debe implementar medidas sólidas de protección de datos. El problema es que no se pueden aplicar correctamente las políticas de uso aceptable de IA generativa si no se conoce bien el contenido y cómo interactúan con él los empleados.

Protección contra el uso negligente de la IA generativa

Para evitar la filtración de datos a través de herramientas de inteligencia artificial generativa, es necesario poner en práctica medidas sólidas de protección de datos. No puede limitarse a bloquear por completo el acceso a estas herramientas. Es importante encontrar la manera de permitir el acceso a los usuarios ya que estas herramientas aumentan la productividad e impulsan la innovación.

Si quiere que los empleados utilicen herramientas de IA generativa sin poner en peligro la seguridad de sus datos, debe adoptar un enfoque de le prevención de la pérdida de datos centrado las personas. Una solución basada en este enfoque autoriza e impide de forma muy precisa que los empleados utilicen las herramientas de IA generativa en función de su comportamiento y sus contribuciones, incluso si los datos han sido manipulados y han pasado por varios canales.

Elementos indispensables:

- **Identificación de contenido sensible.** Un sistema capaz de identificar el contenido que debe protegerse puede bloquear las pérdidas de datos con mayor eficacia. Adopte métodos avanzados de identificación y clasificación de contenido, como el reconocimiento óptico de caracteres, la correspondencia de datos exacta y la correspondencia de documentos indexados.
- **Supervisión de usuarios.** Necesita saber quién utiliza herramientas de IA generativa en su entorno y qué métodos emplean. El sistema debe ser capaz de detectar, bloquear y notificar diferentes tipos de acciones de los usuarios. Esto incluye la carga de archivos de código fuente y el pegado de propiedad intelectual corporativa.
- **Gestión de riesgos proactiva.** Mediante la creación y el registro de exploraciones personalizadas, sus equipos pueden realizar un seguimiento regular de la filtración de datos y otras actividades de riesgo asociadas a las herramientas de IA generativa.

3: usuarios maliciosos

Los usuarios maliciosos son peligrosos porque están en la mejor posición para robar datos confidenciales. Los empleados que abandonan la empresa son el tipo de usuarios internos de mayor riesgo. Durante un período de nueve meses en 2023, 87 % de las filtraciones de archivos anormales entre los inquilinos cloud que utilizan la plataforma Proofpoint Information Protection fueron causadas por empleados que abandonaron la empresa. Estos usuarios a menudo consideran que tienen derecho a conservar la información dado el tiempo que han dedicado a sus proyectos.

La razón por la que los usuarios internos maliciosos son tan peligrosos es que pueden esperar su momento y aprovechar su acceso privilegiado para hacerse con datos valiosos y explotar vulnerabilidades de seguridad. Es más, las empresas empeoran las cosas al permitir que sus empleados consulten y almacenen datos en sus dispositivos personales, lo que facilita el robo de datos sensibles.

Un sistema centrado en las personas supervisa a algunos usuarios más de cerca que a otros, aplica controles de acceso más estrictos a los usuarios de mayor riesgo

Protección frente a usuarios maliciosos

Un sistema centrado en las personas supervisa a algunos usuarios más de cerca que a otros, aplica controles de acceso más estrictos a los usuarios de mayor riesgo y bloquea proactivamente la actividad maliciosa basándose en factores de riesgo como la dimisión o el despido.

Elementos indispensables:

- **Visibilidad.** La visibilidad de endpoints, el correo electrónico, la nube y la web proporciona una visión holística e información contextualizada sobre la actividad de un usuario. Telemetría sobre sus interacciones con datos y sistemas, como cuando cambian el nombre de un archivo confidencial o lo suben a un sitio web no autorizado o a una carpeta de sincronización en la nube. Si un usuario instala o ejecuta aplicaciones no autorizadas, estas actividades también se supervisan. El equipo de seguridad debe ser capaz de identificar en tiempo real a la persona que activó la alarma.
- **Investigaciones.** Necesita una biblioteca de alertas de amenazas para los casos de uso más comunes (fraude horario, filtración de datos, elusión de controles de seguridad). Esto le permitirá ponerse en marcha rápidamente. Las alertas para el equipo de seguridad deben incluir metadatos detallados y capturas de pantalla de las actividades de los usuarios. Una cronología contextualizada de los acontecimientos ayuda a los equipos de investigación a comprender los pormenores ("quién, qué, cuándo, dónde") de las actividades de los usuarios.
- **Arquitectura moderna.** Una plataforma nativa para la nube puede ampliarse para cientos de miles de usuarios. Con funciones como los controles de acceso basados en atributos, el enmascaramiento y la anonimización de datos y la compatibilidad con centros de datos multirregionales, le permitirá cumplir los requisitos de privacidad y residencia de datos. Del mismo modo, un sistema moderno complementará su sistema de seguridad por la facilidad con la que puede integrarse en una serie de herramientas:
  - Organización, automatización y respuesta a incidentes de seguridad (SOAR)
  - Sistemas de administración de información y eventos de seguridad (SIEM)
  - Respuesta a incidentes
  - Gestión de incidentes

Funciones principales

Ahora que ya sabe lo que los modernos sistemas DLP centrados en las personas pueden hacer para protegerle, echemos un vistazo más de cerca a las características esenciales. Existen tres categorías:

- Detección y prevención del riesgo de pérdida de datos
- Análisis y respuesta a incidentes
- Despliegue e implementación

Detección y prevención del riesgo de pérdida de datos

Cuando los equipos de seguridad disponen de información sobre el comportamiento de los usuarios y el contenido sensible, pueden gestionar los riesgos relacionados con los datos de forma adecuada y precisa.

NECESIDADES DE LOS CLIENTES	FUNCIONES REQUERIDAS
Detección de contenido sensible	Detección y análisis de los datos sensibles en el correo electrónico, los endpoints, la nube y la web.
	Funcionalidad integrada para clasificar los datos sensibles según el contexto empresarial
	Clasificación de datos optimizada por IA mediante grandes modelos de lenguaje (LLM).
	Métodos avanzados de identificación: • Reconocimiento óptico de caracteres (OCR) • Coincidencia exacta de datos (EDM) • Correspondencia de documentos indexados (IDM)
	Políticas predefinidas para detectar los datos sensibles, como: • PII • Norma PCI, ley SOX, ley GLBA, términos relativos al delito de iniciado definidos por la SEC • Código PHI, ley HIPAA, ICD-9, ICD-11 Código nacional de medicamentos de Estados Unidos • RGPD, UK-DPA, EU-DEPD, PIPEDA
	Capacidad para definir políticas de lectura y aplicación de las etiquetas de confidencialidad de Microsoft Information Protection (MIP) para identificar los datos empresariales críticos.

NECESIDADES DE LOS CLIENTES	FUNCIONES REQUERIDAS
Supervisión del comportamiento de los usuarios	Enfoque centrado en las personas que permite a los analistas intervenir rápidamente con la siguiente información: • Intención de los usuarios • Patrones de acceso a los datos • Patrones de acceso a las aplicaciones
	Capacidad para supervisar las interacciones de los usuarios con los datos en los endpoints gestionados y en la nube, como: • Cambio de nombre de archivos • Modificación de las extensiones de los archivos • Subidas y bajadas web • Copia a una llave USB • Sincronización de recursos compartidos en la nube • Apertura de documentos • Actividad sospechosa en los archivos
	Supervisión del uso de sitios web y aplicaciones: • Carga, pegado o introducción de contenido en sitios de IA generativa • Descargas e instalaciones de herramientas de copia de seguridad de datos o de hacking)
	Supervisión del comportamiento de los usuarios internos de mayor riesgo para determinar sus intenciones y limitar los riesgos, como la manipulación del Registro de Windows para eliminar controles
	Supervisión proactiva de los usuarios de riesgo mediante simples capturas de pantalla cuando se activa una alerta, para garantizar la privacidad
	Apoyar a los usuarios y pedirles que justifiquen el acceso a datos sensibles en lugar de bloquear accesos que podrían afectar a su productividad (correo electrónico, endpoints, nube, Web)
Prevención de la pérdida de datos	Formación de concienciación en materia de seguridad para cambiar el comportamiento de los usuarios explicándoles cómo evitar los riesgos de ciberseguridad y proteger los datos sensibles
	Prevención de filtraciones de datos sensibles desde des endpoints gestionado, como: • Copia no autorizada de archivos en una memoria USB • Subida de archivos a una carpeta personal en la nube • Impresión de documentos sensibles • Pegado de contenido sensible desde el Portapapeles • Recursos compartidos de red
	Control del uso compartido generalizado de archivos en aplicaciones cloud y limitación automática de las autorizaciones para compartir archivos
	Acceso seguro a archivos confidenciales en aplicaciones cloud aprobadas por TI desde endpoints no gestionados
	Detección y prevención automáticas del envío de mensajes de correo electrónico a destinatarios equivocados, con o sin archivos adjuntos
	Detección y prevención automáticas de correos electrónicos enviados al destinatario correcto, pero con un archivo adjunto incorrecto
	Prevención del uso compartido de datos sensibles aún no predefinidos con cuentas de correo electrónico personales y otras cuentas no autorizadas

Análisis y respuesta a incidentes

Es importante que los equipos de seguridad respondan rápidamente a los incidentes en todos los canales. El objetivo es limitar la exposición de los datos y garantizar la privacidad.

NECESIDADES DE LOS CLIENTES	FUNCIONES REQUERIDAS
Resolución de incidentes en todos los canales	Consola unificada que cubre todos los canales (correo electrónico, endpoints y la nube) y realiza las siguientes operaciones: • Triaje de alertas • Investigaciones • Exploraciones personalizadas • Respuesta
	Análisis que abarcan todos los canales y muestran: • Las actividades de los usuarios a lo largo del tiempo • Las actividades relacionadas con los archivos a lo largo del tiempo (creación, modificación, uso compartido)
	Capacidades de exploración proactiva que proporcionan visibilidad en tiempo real del comportamiento de los usuarios de riesgo
	Integración con la plataforma SIEM de su empresa para ordenar los flujos de trabajo con sus herramientas existentes
	Capacidad para detectar y neutralizar automáticamente el riesgo de pérdida de datos de usuarios comprometidos por: • Terminación de sesiones • Restablecimiento de contraseñas • Corrección de riesgos • Identificación del impacto
Privacidad	La flexibilidad de los controles de acceso que asegura que los analistas solo vean los datos absolutamente necesarios
	Anonimización de la información de identificación del usuario y enmascaramiento del contenido sensible para proteger los datos y eliminar el sesgo de los analistas.

Despliegue e implementación

Una vez que haya elegido la solución de DLP más adecuada para su empresa, deberá desplegarla. Para garantizar un proceso de implementación sin contratiempos, debe elegir a los partners adecuados para que le apoyen durante todo el despliegue de su estrategia de DLP.

NECESIDADES DE LOS CLIENTES	FUNCIONES REQUERIDAS
Despliegue	Solución nativa para la nube que pueda desplegarse rápidamente
	Solución altamente escalable que pueda ampliarse fácilmente a cientos de miles de usuarios por inquilino
	Solución fácil de gestionar que requiera un mantenimiento y una energía mínimos gracias a una comunicación clara sobre las actualizaciones y la asistencia del proveedor cuando sea necesario
	Políticas y administración centralizadas para cumplir los requisitos de residencia de datos multirregional
	Plataforma flexible que se integra con su ecosistema de seguridad, como: • Microsoft • Okta y Sailpoint • CrowdStrike • Splunk y ServiceNow • Zscaler y Citrix ShareFile
	Agente de endpoint en modo de usuario que: • Aumenta la visibilidad de las posibles amenazas internas • Mejora la productividad de los usuarios • Elimina los problemas de estabilidad • No entra en conflicto con otras soluciones
Implementación	Servicios profesionales que puedan ayudarle a acelerar la implementación con un equipo de expertos experimentados que puedan adaptar su sistema a sus necesidades. La implementación de una solución de DLP implica varias etapas: • Recopilación de requisitos • Diseño • Personalización de la solución • Pruebas y ajustes • Formación de administradores y usuarios • Documentación
DLP gestionada	Sea cual sea el tamaño de su empresa, debería considerar una oferta de DLP gestionada. Con los servicios gestionados, se beneficiará del apoyo de expertos experimentados que estarán siempre a su disposición para diseñar, desplegar y administrar con usted su programa.

MÁS INFORMACIÓN

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

1207-013-06-01 7/24