BLOG POST

Compartir y Comunicar sin Preocupaciones

PREVENCIÓN DE PÉRDIDA DE DATOS EN LA ERA DE LA IA



Stephen Hearty
Head of Symantec Product Marketing EMEA



Sunil Choudrie
Head of Product Marketing for InfoSec, Broadcom

A medida que la **IA generativa (GenAI)** se incorpora más en las actividades diarias, aumenta la necesidad de las organizaciones de proteger sus datos confidenciales frente a este nuevo vector de pérdida de datos, y de integrar la protección con sus prácticas actuales de seguridad de los datos. Para los responsables de TI y seguridad actuales, el dilema está claro: ¿cómo aprovechar el potencial de la IA para la eficiencia y la innovación a la vez que se mitigan los riesgos de fuga de datos? En este contexto, **la prevención de la pérdida de datos (DLP)** es más importante que nunca. En este blog veremos cómo se está utilizando la IA en el lugar de trabajo, los riesgos de la exposición de datos y cómo una buena solución DLP puede ayudarle a utilizar la IA de forma segura, incorporando casos prácticos de IA en su configuración existente.

El principal desafío que plantea la IA para las organizaciones es que, para ser productivas, deben poder trabajar con cualquier tipo de datos. Dada la gran utilidad de la IA, cada vez se exigirá más de ella, lo que aumenta el riesgo de que se le proporcionen datos confidenciales que, a su vez, podrían difundirse de forma generalizada. Sin una gobernanza de datos adecuada, el riesgo de exposición de los datos es alto, lo que puede provocar pérdidas financieras (por interrupciones operativas o por sanciones) así como daños a la reputación.

Según un reporte reciente de Microsoft y LinkedIn, el 75 % de los trabajadores del conocimiento en todo el mundo utilizan la IA generativa.

Otro estudio reveló que alrededor de la mitad de los empleados utilizan la IA en la sombra, es decir, herramientas no autorizadas por los empleadores.

BUENOS DATOS DE ENTRADA PARA BUENOS RESULTADOS

En un mundo ideal, así es como funcionaría la IA generativa. Un empleado plantea una pregunta y obtiene una respuesta que aumenta la productividad, sin que los datos confidenciales cambien de manos. En realidad, la situación es más compleja, por supuesto. Hoy en día, los empleados utilizan numerosas aplicaciones de IA, tanto públicas como privadas. Y muchas veces usan herramientas que sus empleadores no han autorizado. Esto hace que sea difícil llevar un seguimiento de los riesgos a los que se exponen los datos confidenciales. Sin embargo, como premisa básica para la prevención de la pérdida de datos, disponer de "datos buenos de entrada" es un excelente punto de partida. Aquí, por "bueno" nos referimos a datos no clasificados como privados o confidenciales.

Esta clasificación es algo que una solución DLP debe ofrecer de forma predeterminada, escaneando documentos para detectar la información confidencial basándose en parámetros predefinidos y etiquetando automáticamente los contenidos confidenciales. La clave en este caso es utilizar un enfoque sistemático que se aleje de la clasificación humana subjetiva de lo que un empleado pueda considera sensible o no.

Partiendo del paso anterior, un buen proveedor o partner de DLP debe poder ayudarle a determinar qué información clasificar como confidencial, garantizando que los datos más importantes estén siempre protegidos.

MÁS INFORMACIÓN

LA VISIBILIDAD LO ES TODO

El primer paso en la vía hacia el uso seguro de la IA es saber qué herramientas utilizan sus empleados. Con soluciones como Symantec DLP Cloud, usted puede hacer un inventario completo de las aplicaciones de IA en toda su organización. Ello incluye quién las está usando y cómo, lo que le permite determinar si debe o no restringir el acceso de los empleados. También obtendrá información sobre la forma en que fluyen los datos hacia y desde las herramientas de IA. Y, lo que es más importante, puede bloquear los datos etiquetados como confidenciales para que las aplicaciones de IA no tengan acceso a ellos.

Veamos un ejemplo de cómo funcionaría en la práctica. Un médico de una clínica con mucha actividad utiliza una herramienta de IA para ayudarse con el diagnóstico y el tratamiento. El médico introduce el nombre del paciente, las afecciones médicas y las prescripciones, y pide sugerencias para un posible plan de tratamiento. Afortunadamente, la clínica cuenta con un sistema DLP que está configurado para escanear contenidos en tiempo real. El sistema da aviso del uso de información protegida y automáticamente bloquea la solicitud. Alerta al médico y registra el incidente, mientras prosigue el seguimiento del uso de la herramienta para garantizar el cumplimiento futuro. El médico vuelve a introducir su consulta, esta vez anonimizando los datos, y recibe información valiosa sin poner en riesgo la privacidad de estos.

COPIAR Y PEGAR ES UNA MALA PRÁCTICA

Hay muchos otros ejemplos de cómo los empleados utilizan la IA con el consiguiente riesgo de exposición de los datos. La mayoría de los casos de pérdida de datos se producen al copiar y pegar información sensible perteneciente a archivos confidenciales. El código fuente es el tipo de exposición de datos más frecuente, ya que los desarrolladores utilizan cada vez más la IA para revisar y perfeccionar la codificación, con lo que los datos sensibles pueden reaparecer en el dominio público.

Las soluciones DLP se pueden configurar para supervisar este tipo de acciones, a fin de detectar posibles fugas de datos y evitarlas en tiempo real. Un buen sistema DLP también debe tener en cuenta los grandes volúmenes de contenidos creados por la IA. Los mismos controles y categorización que se aplican a los otros datos también deben funcionar para los nuevos documentos generados por IA. Los sistemas de IA pueden operar a gran escala, por lo que su sistema DLP debe poder responder a ese ritmo de flujo interminable de nuevos contenidos.

MÁS VALE PREVENIR QUE CURAR

Independientemente de las políticas que una empresa decida aplicar, el objetivo final es siempre el mismo: evitar que las aplicaciones de IA utilicen datos confidenciales. Porque una vez que esos datos salen, es casi imposible recuperar su confidencialidad, y pueden aparecer en cualquier momento en respuesta a una consulta aleatoria. Los sistemas de IA privados también están lejos de hallarse libres de riesgos. Si RR. HH. introduce una lista de salarios de empleados en un sistema interno de IA, por ejemplo, hay muchas probabilidades de que empleados no autorizados puedan verla.

En definitiva, la prevención de la pérdida de datos debe estar siempre en el centro de atención, porque subsanar la filtración rara vez, o nunca, es una opción. Y hay cosas que un buen sistema DLP puede hacer para reducir el riesgo. Cuando se detecta que una aplicación de IA intenta acceder a datos confidenciales, Symantec DLP entra en acción. Puede avisar al usuario, bloquear el acceso y alertar a los administradores o equipos de seguridad en tiempo real, lo que permite una respuesta e intervención rápidas para detener posibles fugas de datos. La solución también proporciona pistas de auditoría detalladas para facilitar el rastreo de dónde y cómo se expusieron los datos, ya sea en aplicaciones de IA u otras partes de la red.

LA DLP PARA LA IA NO TIENE POR QUÉ SER DIFÍCIL

Todo esto puede parecer sumamente complejo, pero desde una perspectiva de DLP, la IA es simplemente un caso de posible pérdida de datos, es verdad que complejo y en evolución, pero nada que no se pueda gestionar con una buena solución DLP. Para las empresas que ya han hecho el esfuerzo de establecer una gobernanza y controles de datos eficaces, no hay razón para permitir que la IA pueda saltarse esos controles. Con la IA se aplican las mismas comprobaciones y contrastaciones que protegen a los otros datos. Con la solución y el soporte adecuados, las políticas y protocolos existentes se pueden revisar y adaptar para gestionar los riesgos de IA.

Symantec DLP Cloud ya está configurado para proteger todos sus datos en cualquier lugar, tanto si implican el uso de IA como si no. Con las mismas capacidades de escaneo, detección y supervisión, y una estricta aplicación de políticas, la solución se puede adaptar fácilmente al tráfico de IA.

Si le preocupan los nuevos riesgos que plantea la IA, o si está revisando su sistema de protección de datos, hable con nuestros expertos hoy mismo. Podemos ayudarle a aprovechar el potencial de la IA sin poner en riesgo la seguridad de sus datos.

PROTECCIÓN DE SUS DATOS EN MICROSOFT COPILOT

En teoría, **Microsoft Copilot** es un sueño hecho realidad para las empresas, pero obtener lo mejor de esta solución requiere la implantación de controles sólidos. Integrado en toda la familia 365, Copilot puede acceder potencialmente a todos los datos de su empresa.

Desde SharePoint, pasando por OneDrive, hasta una bandeja de entrada repleta, no es difícil imaginar cómo los datos confidenciales podrían entrar (y salir) de esa potente herramienta de IA.

Symantec DLP ayuda a mantener a Copilot en su lugar, proporcionando controles integrales que protegen sus datos confidenciales sin limitar los beneficios para su negocio.

Obtenga más información en nuestra infografía

DESCARGAR

