proofpoint.

RESUMEN DE LA SOLUCIÓN

Seguridad de los datos para la IA generativa

Garantice el uso seguro de la IA generativa.

Ventajas principales

- Visibilidad del uso no autorizado de herramientas de IA generativa.
- Prevención de la exposición de datos sensibles mediante herramientas empresariales de IA generativa y desarrollo basado en LLM.
- Aplicación de políticas de uso aceptables para la IA generativa en la nube y en los endpoints.
- Vigilancia de las amenazas internas mediante políticas dinámicas para detectar cualquier uso peligroso de la IA.
- Formación de los empleados en el uso aceptable de las herramientas de IA generativa.

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

La IA generativa ofrece un enorme potencial, ya que impulsa la productividad, la innovación y la información sobre los datos. Sin embargo, su adopción también plantea retos, sobre todo en términos de seguridad, confidencialidad y cumplimiento de los datos. Al utilizar herramientas públicas de IA generativa, los usuarios corren el riesgo de exponer datos sensibles y propiedad intelectual. Además, un gobierno deficiente puede dar lugar a un acceso no autorizado a los datos por parte de herramientas empresariales como Microsoft 365 Copilot y a una clasificación incorrecta de los resultados sensibles. Los grandes modelos de lenguaje (LLM) personalizados y entrenados con datos de clientes pueden revelar datos personales, creando riesgos de incumplimiento de normativas como GDPR y HIPAA y CCPA. Sin un gobierno sólido, las empresas se arriesgan a poner en peligro la seguridad y a recibir multas por incumplimiento de normativas.

Proofpoint garantiza un uso aceptable de las herramientas y modelos de IA generativa mediante un enfoque integral centrado en las personas que combina visibilidad, control y formación. Proofpoint Data Loss Prevention (DLP) supervisa el uso de la IA generativa en los endpoints, proporcionando información sobre las interacciones de los usuarios e identificando herramientas no autorizadas. Para prevenir la pérdida de datos, Proofpoint aplica políticas que bloquean la entrada de datos confidenciales o los enmascaran en prompts para IA generativa. Proofpoint Data Security Posture Management (DSPM) evita la exposición de datos a través de herramientas de IA generativa y LLM clasificando los datos sensibles y protegiéndolos de accesos no autorizados. Además, Proofpoint ZenGuide ofrece formación personalizada sobre ciberseguridad para enseñar a los empleados a utilizar la IA generativa de forma segura, fomentando una cultura de uso responsable. Al integrar estas estrategias, Proofpoint protege los datos confidenciales de las organizaciones en el cambiante panorama de la IA generativa.

Obtenga visibilidad sobre el uso no autorizado de herramientas de IA generativa

Proofpoint ayuda a las organizaciones a comprender quién utiliza qué herramientas de IA generativa y si se están exponiendo datos confidenciales a través de estas herramientas o de LLM personalizados. Nuestro informe sobre la seguridad de los datos en el contexto del uso de la IA destaca los tipos de datos sensibles enviados a las herramientas públicas de IA generativa, los usuarios más activos, los principales sitios por actividad, etc. (Figura 1).

Mediante las API cloud, puede identificar los permisos de las aplicaciones de IA de terceros, como OpenAI, y generar alertas relacionadas. También puede identificar despliegues de IA en AWS Bedrock y Azure OpenAI que utilicen datos confidenciales.

Ventajas principales

- Prevención de la exposición de datos sensibles mediante herramientas empresariales de IA generativa y desarrollo basado en LLM.

Evite la exposición de datos sensibles mediante herramientas de IA generativa y LLM

Proofpoint DSPM identifica y clasifica los datos sensibles en los flujos de trabajo de IA, con el fin de evitar cualquier exposición que pudiera llevar a un compromiso. También protege los datos a los que accede Microsoft Copilot aplicando las etiquetas Microsoft Information Protection (MIP), que se utilizan para aplicar políticas de protección como el cifrado y los controles de acceso.

También protege los LLM personalizados y las aplicaciones de IA en plataformas como AWS Bedrock y Azure OpenAI mediante la detección de datos confidenciales que alimentan modelos básicos o personalizados y flujos de trabajo RAG (Retrieval-Augmented Generation).

Proofpoint ofrece API especializadas para la seguridad de los LLM, que permiten analizar en tiempo real la sensibilidad de los datos que pasan por los LLM. Estas API ofrecen un gobierno y visibilidad totales sobre el uso de los datos, gracias a una integración perfecta con los flujos de trabajo de los clientes para un despliegue eficaz.

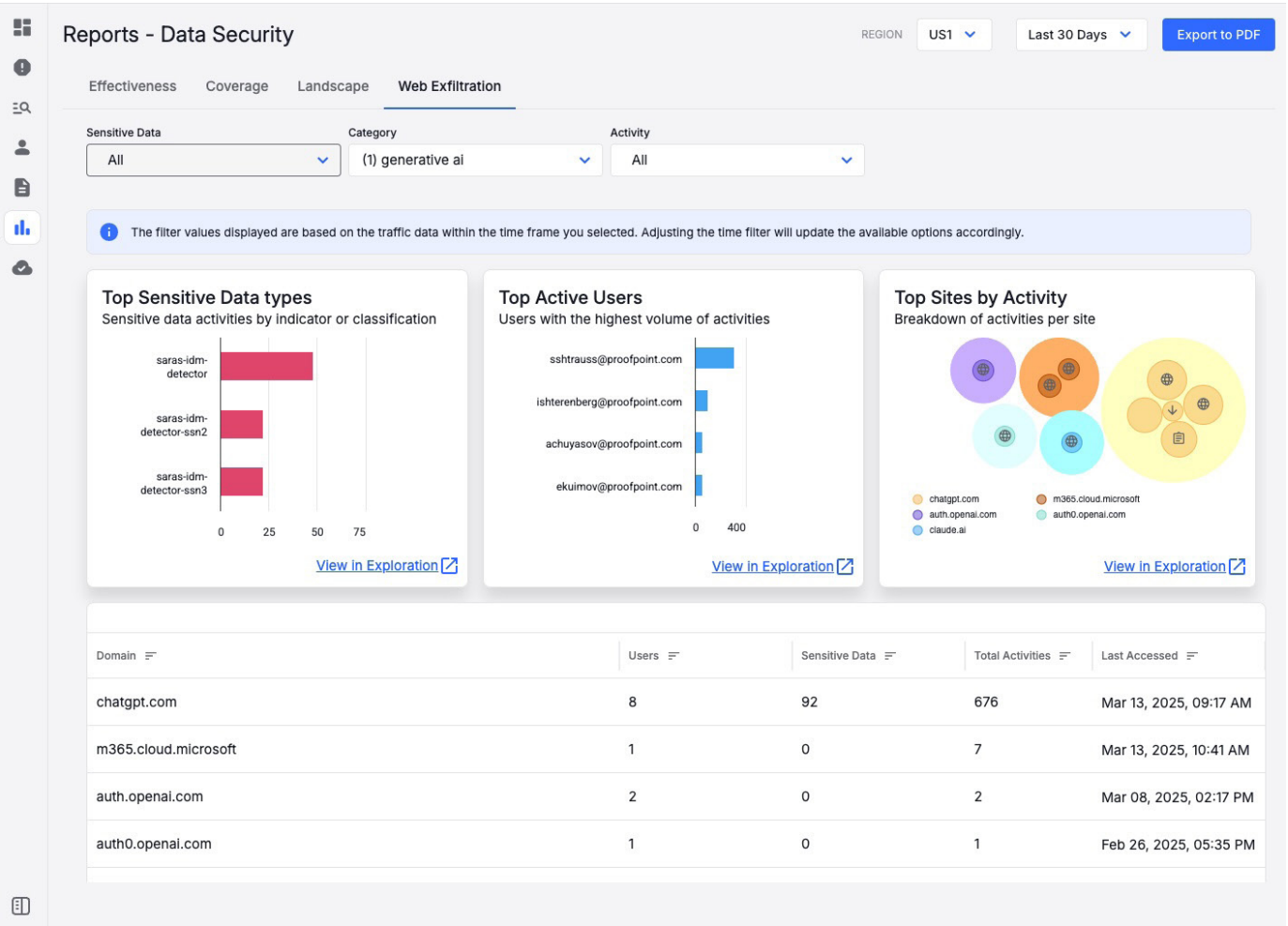

Figura 1: Informe que destaca los principales riesgos de la filtración de datos mediante IA generativa.

Ventajas principales

- Aplicación de políticas de uso aceptables para la IA generativa en la nube y en los endpoints.
- Vigilancia de las amenazas internas mediante políticas dinámicas para detectar cualquier uso peligroso de la IA.
- Formación de los empleados en el uso aceptable de las herramientas de IA generativa.

Prevenga la pérdida de datos y las amenazas internas asociadas al uso de la IA generativa

En los endpoints, puede supervisar a los usuarios que navegan por sitios de IA generativa mediante la categorización web o generar alertas si se instalan aplicaciones de IA no autorizadas. Nuestras políticas dinámicas pueden reforzar la vigilancia de los extremos en el caso de usuarios que muestren comportamientos de riesgo. Por ejemplo, puede capturar metadatos y capturas de pantalla antes y después de que los usuarios envíen contenido sensible a sitios de IA generativa no autorizados. Esto significa que puede dedicar menos tiempo a analizar las interacciones de los usuarios con herramientas de IA generativa.

Con Proofpoint DLP, puede aplicar políticas de DLP a nivel de endpoint para más de 600 herramientas de IA generativa por usuario, grupo o departamento, así como bloquear cargas web a plataformas de IA generativa u ocultar datos confidenciales ingresados en solicitudes. Para mantener la productividad de los usuarios, nuestra solución también puede animarles a respetar las normas de uso de la IA generativa, o pedirles una justificación en lugar de aplicar normas de prevención.

Mediante el uso de API cloud, proporcionamos visibilidad de los archivos excesivamente compartidos expuestos a Microsoft 365 Copilot y alertamos a su equipo de seguridad cuando los usuarios hacen un uso indebido de Copilot para localizar archivos que contienen información confidencial.

Por ejemplo, Proofpoint detecta cuando un usuario interno de alto riesgo utiliza Copilot para acceder a numerosos archivos que contienen datos confidenciales en un breve espacio de tiempo. Nuestra solución también clasifica, etiqueta y protege los contenidos generados por IA en aplicaciones cloud. Además, revoca o bloquea las autorizaciones de aplicaciones de IA de terceros no aprobadas.

Forme a los empleados en el uso aceptable de las herramientas de IA generativa

Proofpoint enseña a los usuarios a utilizar la IA generativa de forma segura en su organización. Proofpoint ZenGuide forma a los usuarios mediante vídeos, pósteres, módulos interactivos y boletines informativos sobre la gestión segura de datos. Le permite aprovechar la información sobre sus usuarios de alto riesgo y automatizar el aprendizaje personalizado basado en el nivel de riesgo para grupos específicos, como los desarrolladores, o para sus usuarios más vulnerables.

Las actividades de formación fomentan el comportamiento positivo mediante evaluaciones, advertencias personalizadas y experiencias de coaching. Estas actividades incluyen evaluaciones de conocimientos, premios de formación, notificaciones y confirmaciones de cumplimiento de las políticas, todo ello diseñado para mejorar la concienciación y fomentar un uso seguro y aceptable de las herramientas de IA generativa.

Impulse su negocio con el uso seguro de la IA generativa

Proofpoint ofrece una solución centrada en las personas para los retos modernos de la seguridad de los datos. Proporcionamos información sobre los riesgos de exposición y pérdida de datos asociados a las herramientas de IA generativa y los LLM.

Con Proofpoint, puede lograr fácilmente el equilibrio adecuado entre la productividad de los usuarios y la seguridad de los datos adoptando políticas que permitan a los usuarios acceder a herramientas y modelos de IA generativa mediante formación, supervisión mejorada y controles de datos adecuados.

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. Organizaciones líderes de todos los tamaños, entre las que se encuentran el 85 % de las empresas Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en las personas y su cumplimiento normativo, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en www.proofpoint.com/es.

Conecte con Proofpoint: LinkedIn

DESCUBRA LA PLATAFORMA DE PROOFPOINT →

0207-017-06-01 03/25