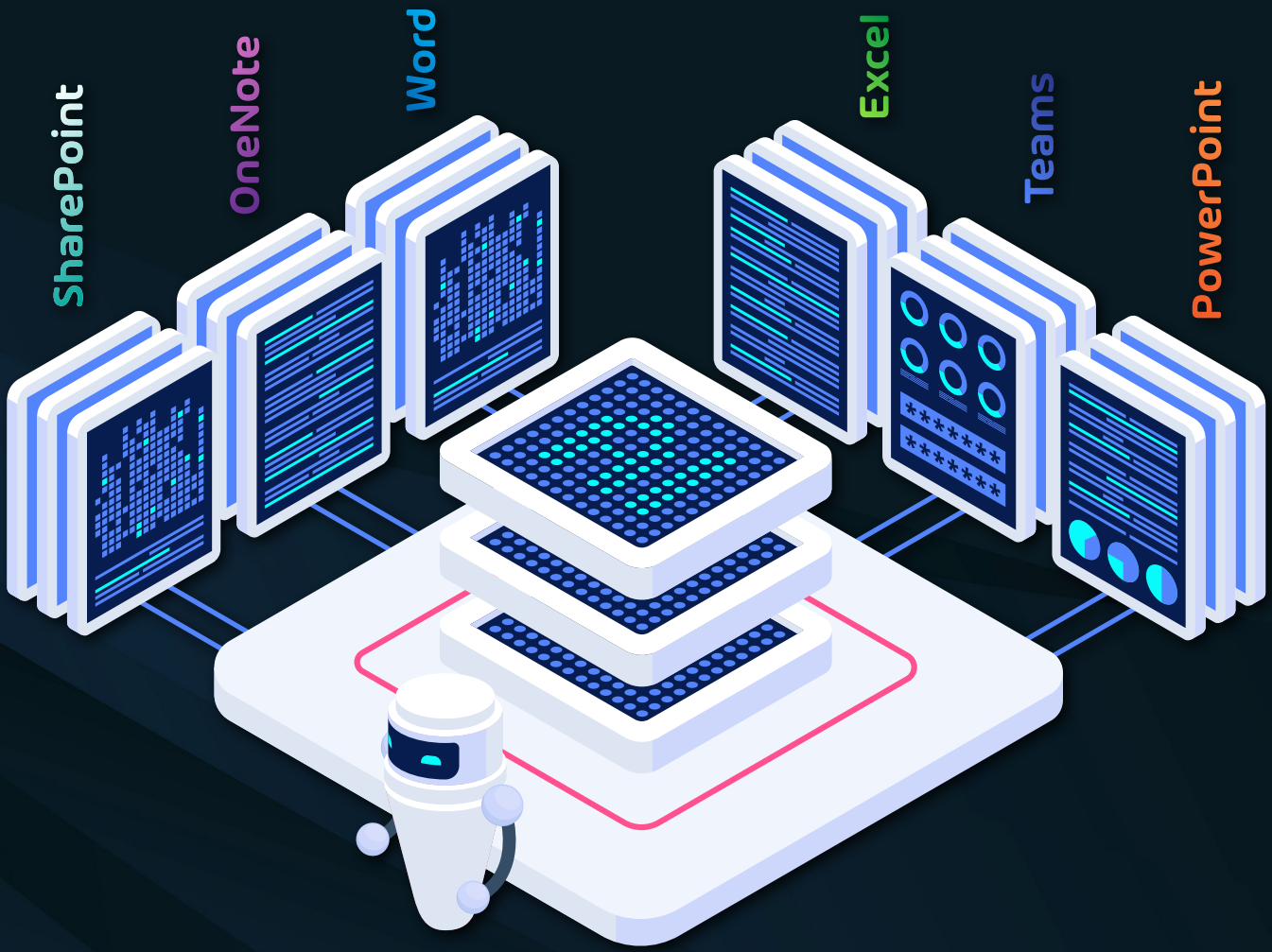
CÓMO HACER QUE TU EMPRESA ESTÉ PREPARADA

MICROSOFT COPILOT



HORNETSECURITY

CÓMO HACER QUE TU EMPRESA ESTÉ PREPARADA PARA **MICROSOFT COPILOT**

ADMINISTRAR LOS PERMISOS DE MICROSOFT 365: EVITAR FUGAS DE DATOS

Microsoft Copilot promete facilitar mucho el trabajo diario de los empleados. El asistente digital de IA puede, por ejemplo, diseñar presentaciones, crear resúmenes o redactar correos electrónicos. Para ello, Copilot accede a los mismos documentos, correos electrónicos y archivos en Microsoft 365 SharePoint y OneDrive a los que puede acceder el usuario para ofrecer resultados individualizados. Lo que a primera vista parece una excelente manera de facilitar el trabajo también alberga un riesgo importante: ¡los datos confidenciales pueden caer en las manos equivocadas! Una pesadilla para los CISO y los administradores.

En este documento técnico se analizan los riesgos asociados con el uso de Copilot y se describe una solución para implementar una gestión eficaz de permisos para evitar la pérdida de control y garantizar el cumplimiento.

Copilot accede a todos los datos de SharePoint para los que un usuario tiene permiso

RIESGO DE FUGA DE DATOS DEBIDO A LA INVESTIGACIÓN DE COPILOT EN ONEDRIVE Y SHAREPOINT

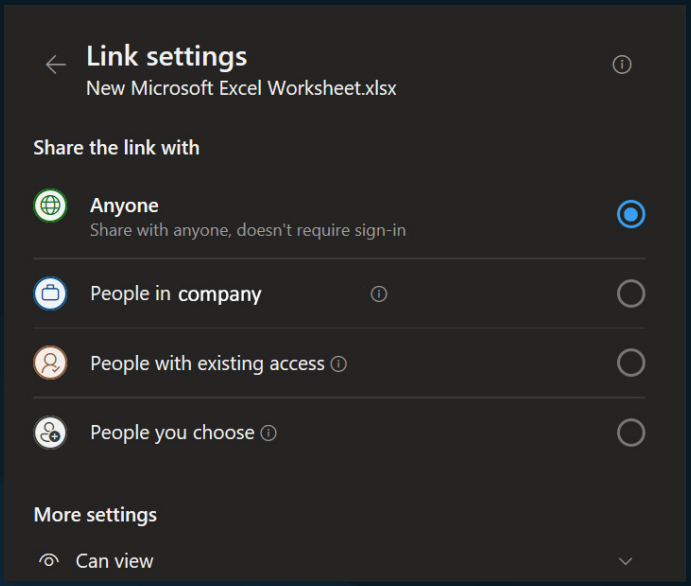
Copilot puede facilitar el trabajo de muchas maneras. Por ejemplo, la herramienta puede resumir, editar o preparar información de forma creativa utilizando los prompts, es decir, comandos escritos por el usuario.

Copilot accede al contenido de todas las aplicaciones de Microsoft 365, como Word, Excel, PowerPoint, Outlook y Teams, para recopilar información. El asistente de IA puede recopilar datos de documentos, hojas de cálculo de Excel, presentaciones, etc. almacenados en SharePoint y OneDrive en cuestión de segundos.

Dado que Copilot accede a todos los datos para los que un usuario tiene autorización durante la búsqueda, la herramienta puede encontrar información confidencial (datos personales, información relevante para la seguridad, cifras comerciales, información salarial, etc.) en SharePoint o OneDrive a la que el usuario no debería tener acceso, pero que aun así tiene, debido a configuraciones de permisos predeterminadas inadecuadas.

UN EJEMPLO:

Un empleado comparte un documento de Excel con cifras comerciales confidenciales con su superior de forma rápida y sencilla a través de un enlace utilizando la función "Compartir". El problema surge cuando la configuración predeterminada de uso compartido genera automáticamente un enlace de acceso que otorga acceso a todos los miembros de la empresa o, peor aún, simplemente a cualquier persona que tenga este vínculo.



Incluso si otros empleados de la empresa no conocen el documento y no reciben este enlace, Copilot ahora tiene acceso a él y puede leer información del documento e incorporarla a los resultados de la investigación de otros empleados.

LOS DOCUMENTOS COMPARTIDOS EN MICROSOFT TEAMS SE ALMACENAN EN SHAREPOINT

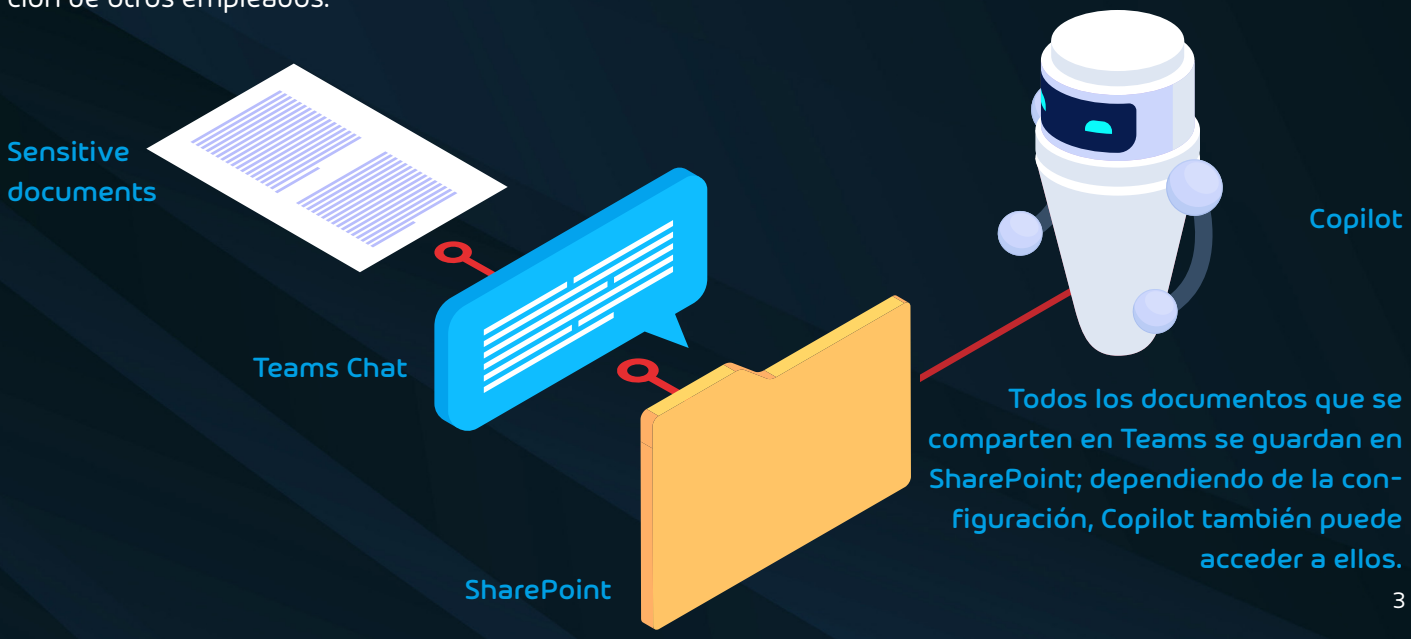
El uso compartido de archivos en Teams también aumenta el riesgo de pérdida de datos en relación con Copilot si la configuración de uso compartido no está configurada correctamente. Cuando se comparte un archivo en un chat de Teams, se guarda en el sitio del equipo en SharePoint, algo de lo que muy pocas personas son conscientes.

Los archivos que se cargan en un chat individual o grupal terminan en la carpeta "Archivos de chat de Microsoft Teams" en OneDrive para la Empresa. Si tiene un canal privado, obtiene su propio sitio de SharePoint, independiente, con una biblioteca de documentos a la que solo tienen acceso los miembros del canal privado.

Esto significa que todos los documentos se almacenan en diferentes sitios de SharePoint en lugar de directamente en Teams, sitios a los que Copilot también puede acceder.

Se vuelve aún más problemático cuando los usuarios invitados externos de Microsoft 365 usan Copilot para acceder a información de la empresa a la que en realidad no tienen vínculos de acceso directo.

Esto debería ser una señal de alarma para los CISO y los administradores.



SE REQUIERE UNA ADMINISTRACIÓN DE PERMISOS SÓLIDA PARA LOS DATOS DE MICROSOFT 365

Copilot puede utilizar y mostrar a los usuarios todos los datos de la organización para los que los usuarios individuales tienen al menos permisos de visualización. Por lo tanto, es importante que la empresa implemente estrictamente el principio de necesidad de saber, es decir, la asignación de derechos de acceso mínimos en Microsoft 365.

Esto significa que solo se concede a los usuarios acceso a los datos necesarios para su trabajo y no se conceden autorizaciones adicionales. Estos derechos de acceso deben actualizarse cuando los roles de usuario cambien dentro de la organización.

La gestión eficiente de las autorizaciones también es esencial debido a las leyes y regulaciones.

A la hora de acceder a los datos de la empresa, también hay que cumplir los requisitos legales. Estos dependen de varios factores, como la ubicación de la empresa y los datos involucrados. Especialmente desde la entrada en vigor de NIS2, la afiliación a la industria también ha tenido una influencia decisiva en la futura carga de trabajo de los administradores y CISO.

Con las herramientas de Microsoft existentes, no es posible obtener una visión completa de todas las autorizaciones asignadas en la empresa, ni aplicar y supervisar las políticas de permisos del tenant. Además, los cambios en la configuración de las herramientas de Microsoft solo afectan a los archivos que se crean o comparten desde el momento del cambio.

Por lo tanto, una reacción instintiva suele ser bloquear todo el intercambio de archivos o no permitir el uso compartido externo y establecer permisos predeterminados estrictos para el uso compartido interno. Sin embargo, esto hará que los usuarios busquen otra forma de compartir archivos. Los documentos confidenciales pueden compartirse a través del almacenamiento en la nube de terceros o los correos electrónicos de los consumidores, donde los CISO y los administradores tienen aún menos visibilidad.

LA CONFIGURACIÓN DE "BÚSQUEDA RESTRINGIDA DE SHAREPOINT" DE MICROSOFT NO ES LA SOLUCIÓN

La propia Microsoft también ha reconocido que pueden surgir problemas con las búsquedas de Copilot en SharePoint. En abril de 2024, la compañía introdujo la configuración "Búsqueda restringida de SharePoint" para los administradores como una versión preliminar pública. Esto permite que las búsquedas en toda la empresa y las búsquedas de Copilot se restrinjan a sitios de SharePoint seleccionados.

La búsqueda restringida en SharePoint puede afectar a la precisión de las respuestas de Copilot.

Se trata de una funcionalidad que no ofrece margen para configuraciones granulares. Se permite un sitio completo de SharePoint o está completamente bloqueado.

La habilitación de esta configuración afecta a la experiencia de búsqueda general, incluso para los usuarios que no son de Copilot. Copilot tiene menos información disponible, lo que puede afectar a su capacidad para proporcionar respuestas precisas y completas.

Por lo tanto, para un uso óptimo de Copilot, esta tampoco puede ser la solución.

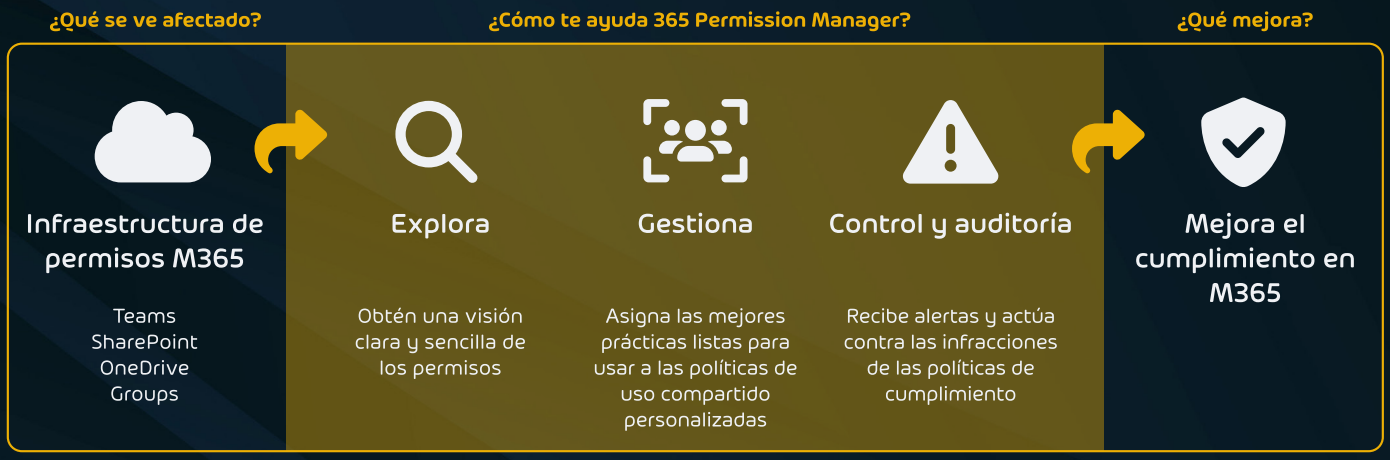
Para asegurarse de que los archivos tienen los permisos correctos de forma continua y que solo los archivos destinados al usuario aparecen en las búsquedas de Copilot, se necesita una solución de terceros que permita una administración eficaz del ciclo de vida de los datos a gran escala para Microsoft 365.

LLEGAR A SER EL COPILOTO CON 365 PERMISSION MANAGER

Lo que se necesita con urgencia para cumplir con las directivas de permisos definidas es una herramienta escalable que cubra sin esfuerzo incluso a grandes tenants con miles de sitios de SharePoint.

Con 365 Permission Manager, es posible supervisar y gestionar eficazmente el acceso y los permisos. Especialmente en lo que respecta a Copilot, la simplificación de la gestión de permisos evita que la información se difunda involuntariamente.

En lugar de tener que navegar a través de los distintos portales del conjunto de herramientas de Microsoft, 365 Permission Manager proporciona una interfaz cómoda y fácil de usar para que los administradores y los CISO obtengan una visión general completa de los permisos en los entornos M365, definan políticas de cumplimiento y eviten o revisen las infracciones.



LAS VENTAJAS DE 365 PERMISSION MANAGER

Seguimiento completo

» 365 Permission Manager proporciona una descripción completa de los permisos de M365 para SharePoint, OneDrive y Microsoft Teams. Una función de filtro avanzada muestra a qué elementos pueden acceder los usuarios externos o invitados. Además, los administradores y los CISO reciben una notificación cuando se comparten archivos, sitios o carpetas con partes interesadas externas.

Personalización de las políticas de permisos

» 365 Permission Manager le permite determinar políticas de permisos predefinidas y crear políticas definidas por el usuario. Estos se pueden aplicar a nivel de sitio, carpeta y archivo según sea necesario. Esto lo hace fundamentalmente diferente de las herramientas 365 de Microsoft, que proporcionan políticas estandarizadas.

Gestión de permisos a gran escala

» Se pueden realizar ajustes a gran escala en el Panel de control de 365 Permission Manager. Con las llamadas acciones masivas, las autorizaciones para cualquier número de inquilinos y grupos se pueden ajustar al mismo tiempo. Esto ahorra tiempo y esfuerzo y garantiza que las autorizaciones de los empleados cumplan con las normas.

Estar al tanto de todo en todo momento

» En caso de infracción, el administrador o CISO recibe un mensaje de advertencia. Se indican los usuarios y los sitios, archivos o carpetas involucrados. Esto permite una acción inmediata para evitar fugas de datos. Las infracciones pueden aprobarse o rechazarse caso por caso o en acciones masivas.

» Una característica útil es la lista de tareas pendientes: enumera las infracciones aplicadas a cada sitio de SharePoint Online. Estas infracciones pueden corregirse a gran escala, con excepciones que se definen si existe una justificación comercial. Los empleados también son responsables. Se les notifica por correo electrónico las infracciones que afectan a sus sitios de OneDrive o SharePoint de los que son propietarios.

Ya sea que se trate de cumplir con las políticas de permisos, proteger la información y los datos, o estar preparado para el uso de Copilot en la empresa, 365 Permission Manager está diseñado para cumplir con todos estos requisitos y los CISO y administradores pueden esperar el uso de Copilot de una manera más segura y compatible.