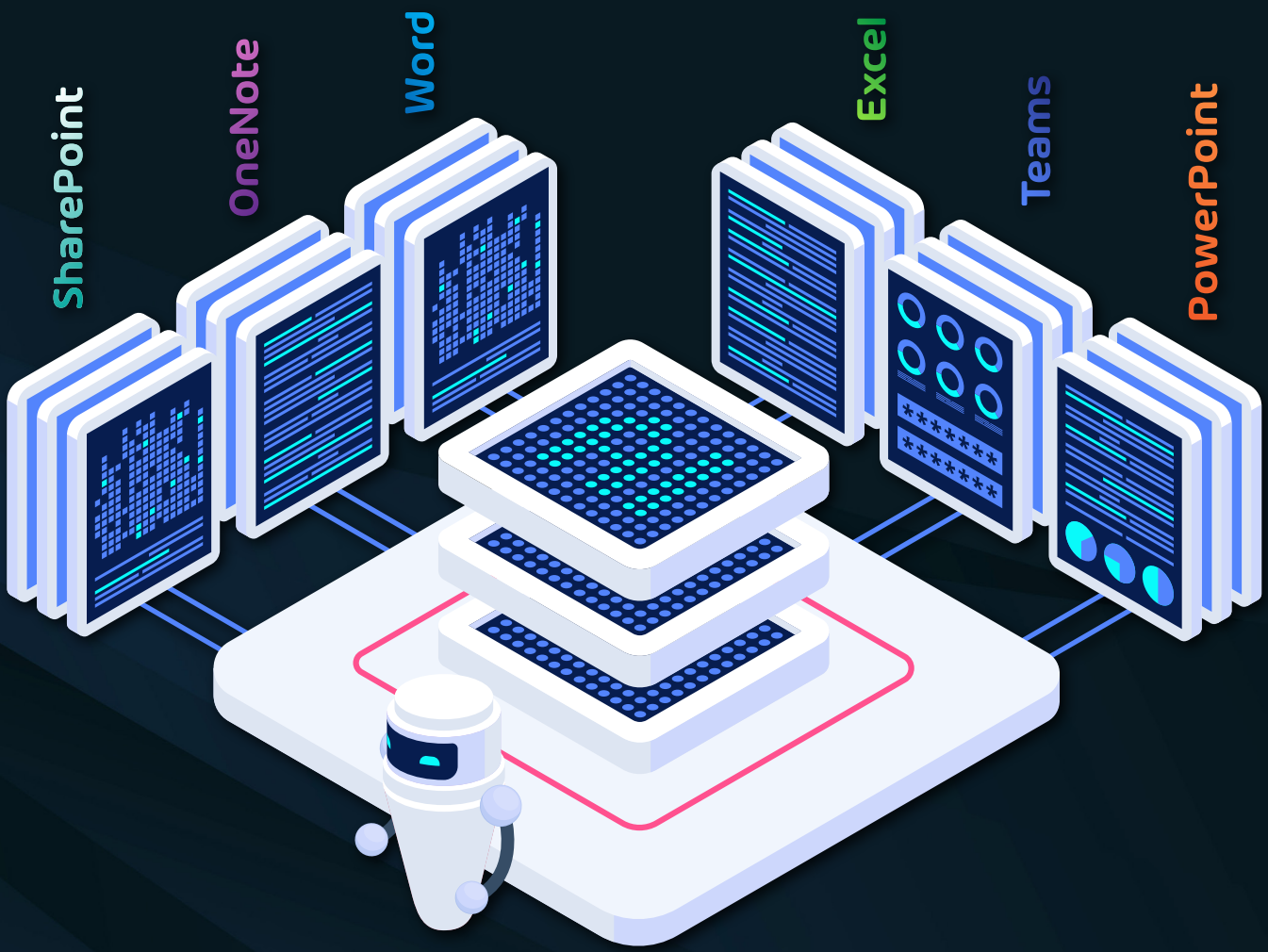
COMMENT PRÉPARER VOTRE ENTREPRISE À MICROSOFT COPILOT



HORNETSECURITY

COMMENT PRÉPARER VOTRE ENTREPRISE À MICROSOFT COPILOT

GÉRER LES AUTORISATIONS MICROSOFT 365 - ÉVITER LES FUITES DE DONNÉES

Microsoft Copilot promet de faciliter le travail quotidien des employés. L'assistant numérique IA peut, par exemple, concevoir des présentations, créer des résumés ou rédiger des e-mails.

Pour ce faire, Copilot accède aux mêmes documents, e-mails et fichiers dans Microsoft 365 SharePoint et OneDrive auxquels l'utilisateur peut accéder pour fournir des résultats individualisés. Ce qui semble à première vue être un excellent moyen de faciliter le travail comporte également un risque majeur : des données sensibles peuvent tomber entre de mauvaises mains ! Un cauchemar pour les RSSI et les administrateurs.

Ce livre blanc examine les risques associés à l'utilisation de Copilot et présente une solution pour mettre en œuvre une gestion efficace des autorisations afin d'éviter la perte de contrôle et garantir la conformité.

Copilot accède à toutes les données de SharePoint pour lesquelles un utilisateur dispose d'une autorisation.

RISQUE DE FUITE DE DONNÉES DÛ À LA RECHERCHE COPILOT DANS ONEDRIVE ET SHAREPOINT

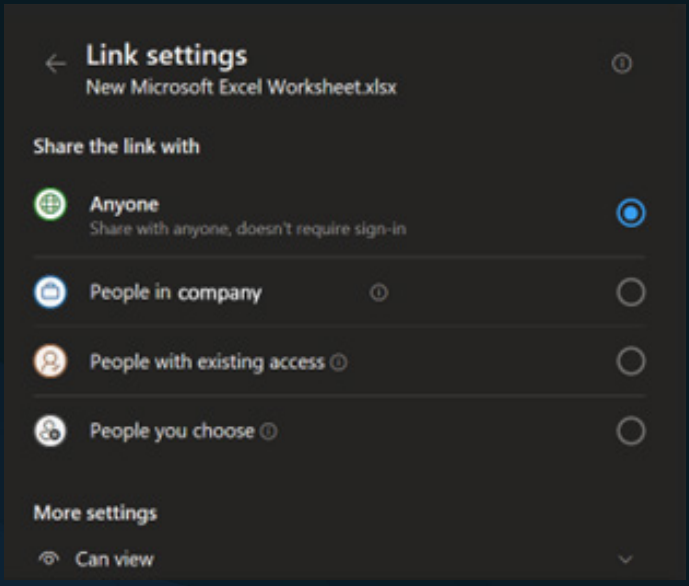
Copilot peut faciliter le travail de plusieurs façons. Par exemple, l'outil peut résumer, modifier ou préparer de manière créative des informations à l'aide de ce que l'on appelle des "invites", c'est-à-dire des commandes écrites par l'utilisateur.

Copilot accède au contenu de toutes les applications Microsoft 365 telles que Word, Excel, PowerPoint, Outlook et Teams pour collecter des informations. L'assistant IA peut compiler des données à partir de documents, de feuilles de calcul Excel, de présentations, etc. stockés dans SharePoint et OneDrive en quelques secondes.

Étant donné que Copilot accède à toutes les données pour lesquelles un utilisateur dispose d'une autorisation lors de la recherche, l'outil peut tomber sur des informations sensibles (données personnelles, informations relatives à la sécurité, chiffres commerciaux, informations salariales, etc.) dans SharePoint ou OneDrive auxquelles l'utilisateur ne devrait pas avoir accès, mais auxquelles il a toujours accès en raison de configurations d'autorisations par défaut inappropriées.

UN EXEMPLE :

un employé partage rapidement et facilement un document Excel contenant des chiffres commerciaux sensibles avec son supérieur via un lien en utilisant la fonction « Partager ». Le problème survient lorsque le paramètre de partage par défaut génère automatiquement un lien d'accès qui accorde l'accès à tous les membres de l'entreprise ou, pire encore, simplement à toute personne disposant de ce lien.



Même si d'autres employés de l'entreprise ne connaissent pas le document et ne reçoivent pas ce lien, Copilot y a désormais accès et peut lire les informations du document et les intégrer dans les résultats de recherches d'autres employés.

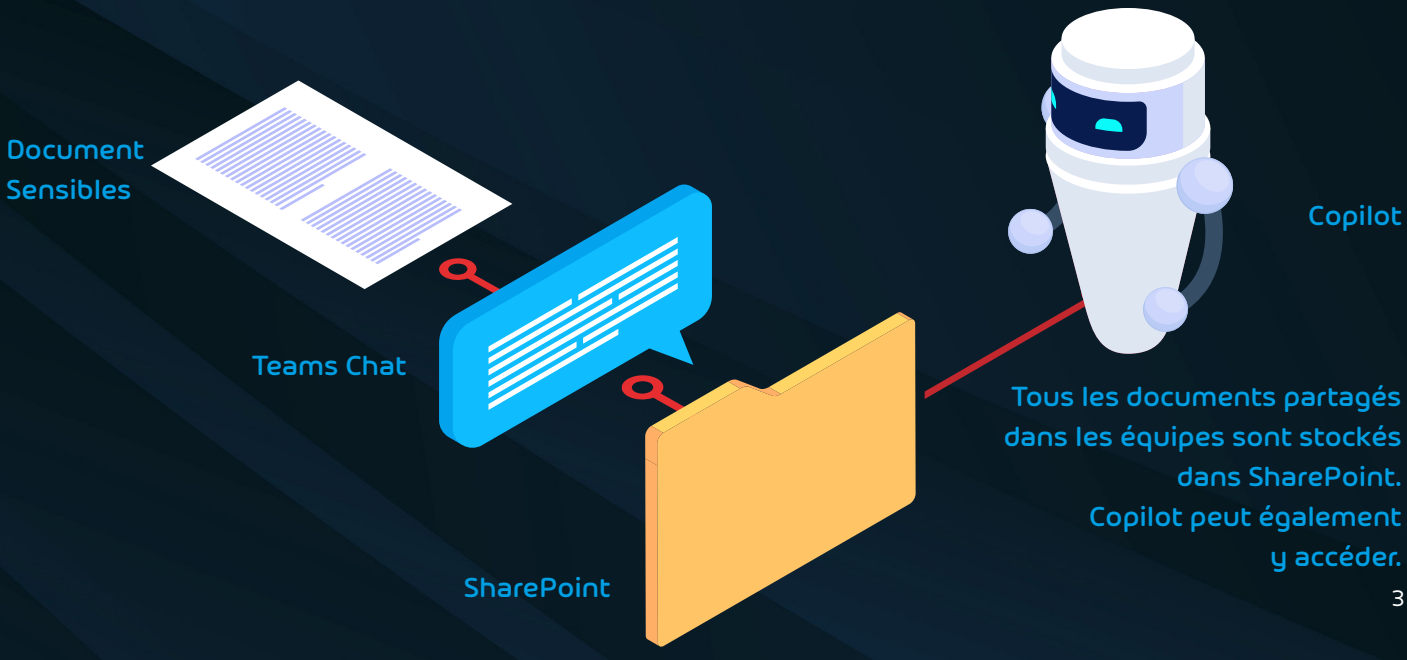
LES DOCUMENTS PARTAGÉS DANS MICROSOFT TEAMS SONT STOCKÉS DANS SHAREPOINT

Le partage de fichiers dans Teams augmente également le risque de fuite de données en lien avec Copilot si les paramètres de partage ne sont pas configurés correctement. Lorsqu'un fichier est partagé dans une conversation Teams, il est enregistré sur le site de l'équipe dans SharePoint, ce que très peu de gens savent.

Les fichiers téléchargés dans une conversation individuelle ou de groupe se retrouvent dans le dossier « Fichiers de conversation Microsoft Teams » dans OneDrive Entreprise. Si vous disposez d'un canal privé, il obtient son propre site SharePoint distinct avec une bibliothèque de documents à laquelle seuls les membres du canal privé ont accès.

Cela signifie que tous les documents sont stockés dans différents sites SharePoint plutôt que directement dans Teams, des sites auxquels Copilot peut également accéder.

Cela devient encore plus problématique lorsque les utilisateurs invités externes de Microsoft 365 utilisent Copilot pour accéder à des informations de l'entreprise vers lesquelles ils n'ont pas de liens d'accès direct. Cela devrait être alarmant pour les RSSI et les administrateurs.



UNE GESTION RIGOUREUSE DES AUTORISATIONS EST REQUISE POUR LES DONNÉES MICROSOFT 365

Copilot peut utiliser et afficher aux utilisateurs toutes les données organisationnelles pour lesquelles les utilisateurs individuels ont au moins des autorisations d'affichage. Il est donc important que l'entreprise applique strictement le principe du "besoin de savoir", c'est-à-dire l'attribution de droits d'accès minimaux dans Microsoft 365.

Cela signifie qu'il ne permet aux utilisateurs d'accéder qu'aux données nécessaires à leur travail et de ne pas accorder d'autorisations supplémentaires. Ces droits d'accès doivent être mis à jour lorsque les rôles des utilisateurs changent au sein de l'entreprise. Une gestion efficace des autorisations est également essentielle en raison des lois et réglementations.

Lorsqu'il s'agit d'accéder aux données de l'entreprise, les exigences légales doivent également être respectées. Celles-ci dépendent de divers facteurs, tels que l'emplacement de l'entreprise et les données concernées.

Depuis l'entrée en vigueur de NIS2, l'affiliation sectorielle a également une influence décisive sur la charge de travail future des administrateurs et des RSSI.

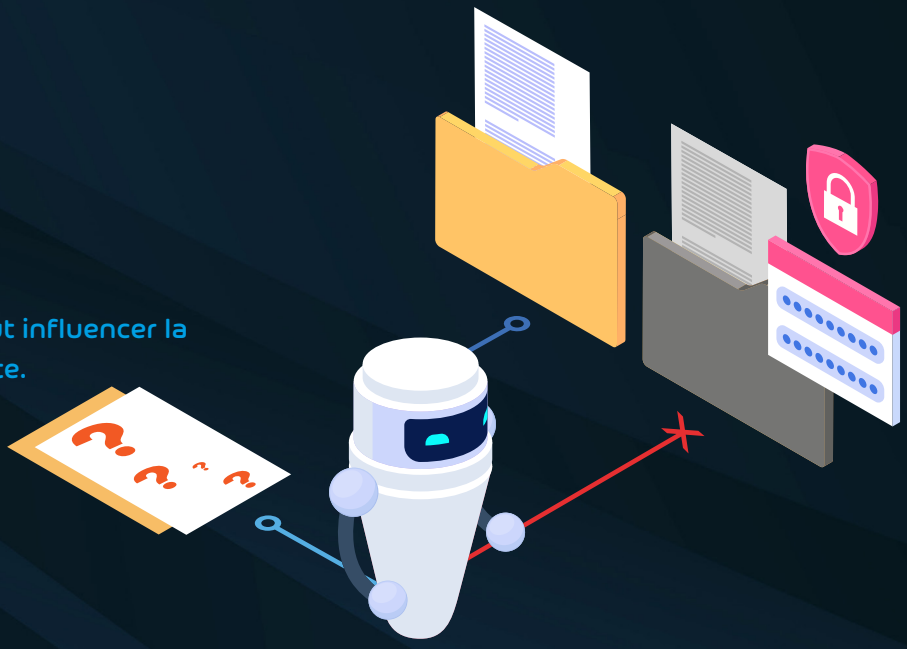
Avec les outils Microsoft existants, il n'est pas possible d'obtenir une vue d'ensemble complète de toutes les autorisations attribuées dans l'entreprise, ni d'appliquer et de surveiller les stratégies d'autorisation à l'échelle du client. En outre, les modifications apportées aux paramètres dans les outils Microsoft n'affectent que les fichiers créés ou partagés à partir du moment de la modification.

Une réaction instinctive est donc souvent de bloquer tout partage de fichiers ou de ne pas autoriser le partage externe et de définir des autorisations strictes par défaut pour le partage interne. Cependant, cela incitera les utilisateurs à chercher un autre moyen de partager des fichiers. Les documents sensibles peuvent ensuite être partagés via un stockage cloud tiers ou via des e-mails grand public, où les RSSI et les administrateurs ont encore moins de visibilité.

LE PARAMÈTRE «RECHERCHE SHAREPOINT RESTREINTE» DE MICROSOFT N'EST PAS LA SOLUTION

Microsoft lui-même a également reconnu que des problèmes peuvent survenir avec les recherches Copilot dans SharePoint. En avril 2024, la société a introduit le paramètre « Recherche SharePoint restreinte » pour les administrateurs en tant qu'aperçu public. Cela permet de limiter les recherches à l'échelle de l'entreprise et les recherches Copilot à certains sites SharePoint.

Restricted SharePoint Search peut influencer la précision des réponses du copilote.



Il s'agit d'une fonctionnalité qui n'offre aucune possibilité de paramètres granulaires. Soit un site SharePoint complet est autorisé, soit il est complètement bloqué.

L'activation de ce paramètre affecte l'expérience de recherche globale, même pour les utilisateurs non Copilot. Copilot dispose de moins d'informations, ce qui peut avoir un impact sur sa capacité à fournir des réponses précises et complètes.

Donc, pour une utilisation optimale de Copilot, cela ne peut pas non plus être la solution.

Pour s'assurer que les fichiers disposent des autorisations correctes en permanence et que seuls les fichiers destinés à l'utilisateur apparaissent dans les recherches Copilot, une solution tierce est nécessaire pour permettre une gestion efficace du cycle de vie des données à grande échelle pour Microsoft 365.

SE PRÉPARER À COPILOT AVEC 365 PERMISSION MANAGER

Ce dont nous avons besoin de toute urgence pour nous conformer aux politiques d'autorisation définies, c'est un outil évolutif qui couvre sans effort même les grands environnements avec des milliers de sites SharePoint.

Avec 365 Permission Manager, il est possible de surveiller et de gérer efficacement les accès et les autorisations. En particulier concernant Copilot, la simplification de la gestion des autorisations empêche la diffusion involontaire d'informations.

Au lieu d'avoir à naviguer dans les différents portails de l'ensemble d'outils natifs de Microsoft, 365 Permission Manager fournit une interface pratique et conviviale permettant aux administrateurs et aux RSSI d'obtenir une vue d'ensemble complète des autorisations dans les environnements M365, de définir des politiques de conformité et de prévenir ou de réviser les violations.

LES AVANTAGES DE 365 PERMISSION MANAGER

Surveillance complète

» 365 Permission Manager fournit une vue d'ensemble complète des autorisations M365 pour SharePoint, OneDrive et Microsoft Teams. Une fonction de filtrage avancée indique les éléments auxquels les utilisateurs externes ou les invités peuvent accéder. En outre, les administrateurs et les RSSI sont avertis lorsque des fichiers, des sites ou des dossiers sont partagés avec des parties prenantes externes.

Personnaliser les stratégies d'autorisations

» 365 Permission Manager vous permet de déterminer des stratégies d'autorisations prédéfinies et de créer des stratégies définies par l'utilisateur. Celles-ci peuvent être appliquées au niveau du site, du dossier et du fichier selon les besoins. Cela le rend fondamentalement différent des outils Microsoft 365, qui fournissent des stratégies standardisées.

Gérer les autorisations à grande échelle

» Des ajustements à grande échelle peuvent être effectués dans le panneau de configuration de 365 Permission Manager. Avec les actions dites "de masse", les autorisations pour un nombre illimité de locataires et de groupes peuvent être ajustées en même temps. Cela permet d'économiser du temps et des efforts et de garantir que les autorisations des employés sont conformes.

Restez au courant à tout moment

» En cas d'infraction, l'administrateur ou le RSSI reçoit un message d'avertissement. Les utilisateurs et les sites, fichiers ou dossiers concernés sont indiqués. Cela permet d'agir immédiatement pour éviter les fuites de données. Les violations peuvent être approuvées ou rejetées au cas par cas ou dans le cadre d'actions de masse.

» Une fonctionnalité particulièrement utile est la liste des tâches : elle répertorie toutes les violations des stratégies appliquées à chaque site SharePoint Online. Ces violations peuvent être corrigées à grande échelle, avec des exceptions définies s'il y a une justification commerciale. Les employés sont également tenus responsables. Ils sont avertis par e-mail des violations de stratégie qui affectent leurs sites OneDrive ou SharePoint dont ils sont propriétaires.

Qu'il s'agisse de se conformer aux politiques d'autorisations, de protéger les informations et les données ou de se préparer à l'utilisation de Copilot dans l'entreprise, 365 Permission Manager est conçu pour répondre à toutes ces exigences et les RSSI et les administrateurs peuvent s'attendre à l'utilisation de Copilot de manière plus sûre et plus conforme.