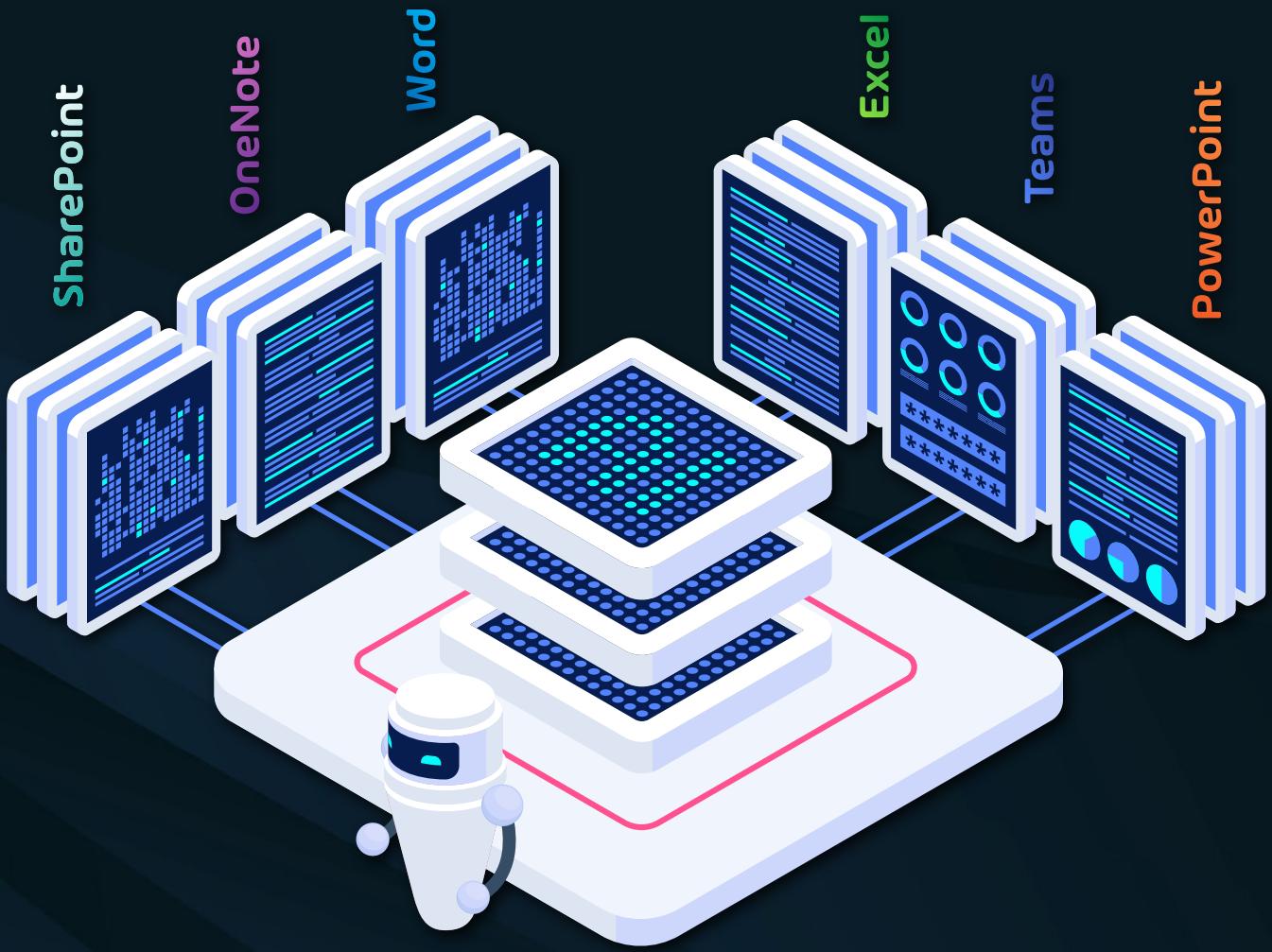
HOW TO MAKE YOUR COMPANY MICROSOFT COPILOT-READY



HORNETSECURITY

HOW TO MAKE YOUR COMPANY **MICROSOFT COPILOT-READY**

MANAGE MICROSOFT 365 PERMISSIONS - AVOID DATA LEAKS

Microsoft Copilot promises to make employees' day-to-day work much easier. The digital AI assistant can, for example, design presentations, create summaries, or draft emails. To do this, Copilot accesses the same documents, emails, and files in Microsoft 365 SharePoint and OneDrive the user can access to deliver individualized results. What at first glance sounds like a great way to make work easier also harbors a major risk: sensitive data can fall into the wrong hands! A nightmare for CISOs and admins.

This whitepaper looks at the risks associated with using Copilot and outlines a solution for implementing effective permission management to prevent loss of control and to ensure compliance.

Copilot accesses all data in SharePoint for which a user has permission.

DATA LEAKAGE RISK DUE TO COPILOT RESEARCH IN ONEDRIVE AND SHAREPOINT

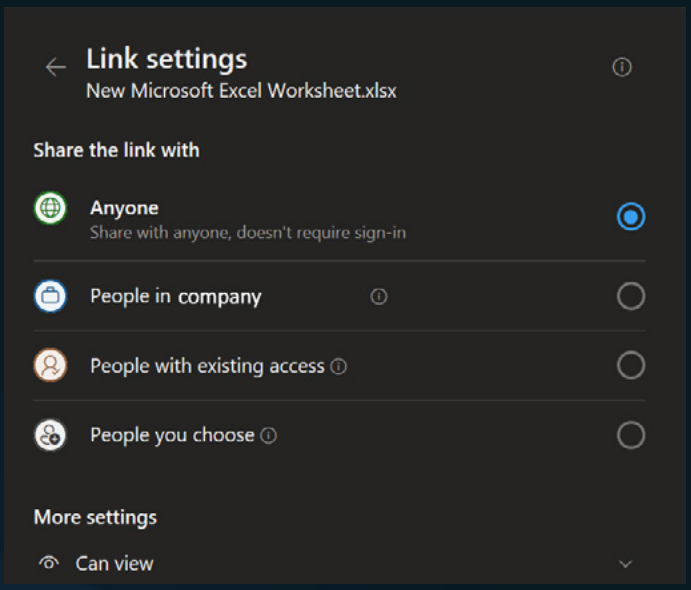
Copilot can make work easier in many ways. For example, the tool can summarize, edit, or creatively prepare information using so-called prompts, i.e. commands written by the user.

Copilot accesses the content of all Microsoft 365 applications such as Word, Excel, PowerPoint, Outlook, and Teams to gather information. The AI assistant can compile data from documents, Excel spreadsheets, presentations, etc. stored in SharePoint and OneDrive in a matter of seconds.

Since Copilot accesses all data for which a user has authorization during the search, the tool may come across sensitive information (personal data, security-relevant information, business figures, salary information, etc.) in SharePoint or OneDrive that the user should not actually have access to but still does due to inappropriate default permission configurations.

AN EXAMPLE:

An employee shares an Excel document with sensitive business figures with his superior quickly and easily via a link using the "Share" function. The problem arises when the default sharing setting automatically generates an access link that grants access to everyone in the company or, even worse, simply to anyone who has this link.



Even if other employees in the company do not know about the document and do not receive this link, Copilot now has access to it and can read information from the document and incorporate it into the research results of other employees.

DOCUMENTS SHARED IN MICROSOFT TEAMS ARE STORED IN SHAREPOINT

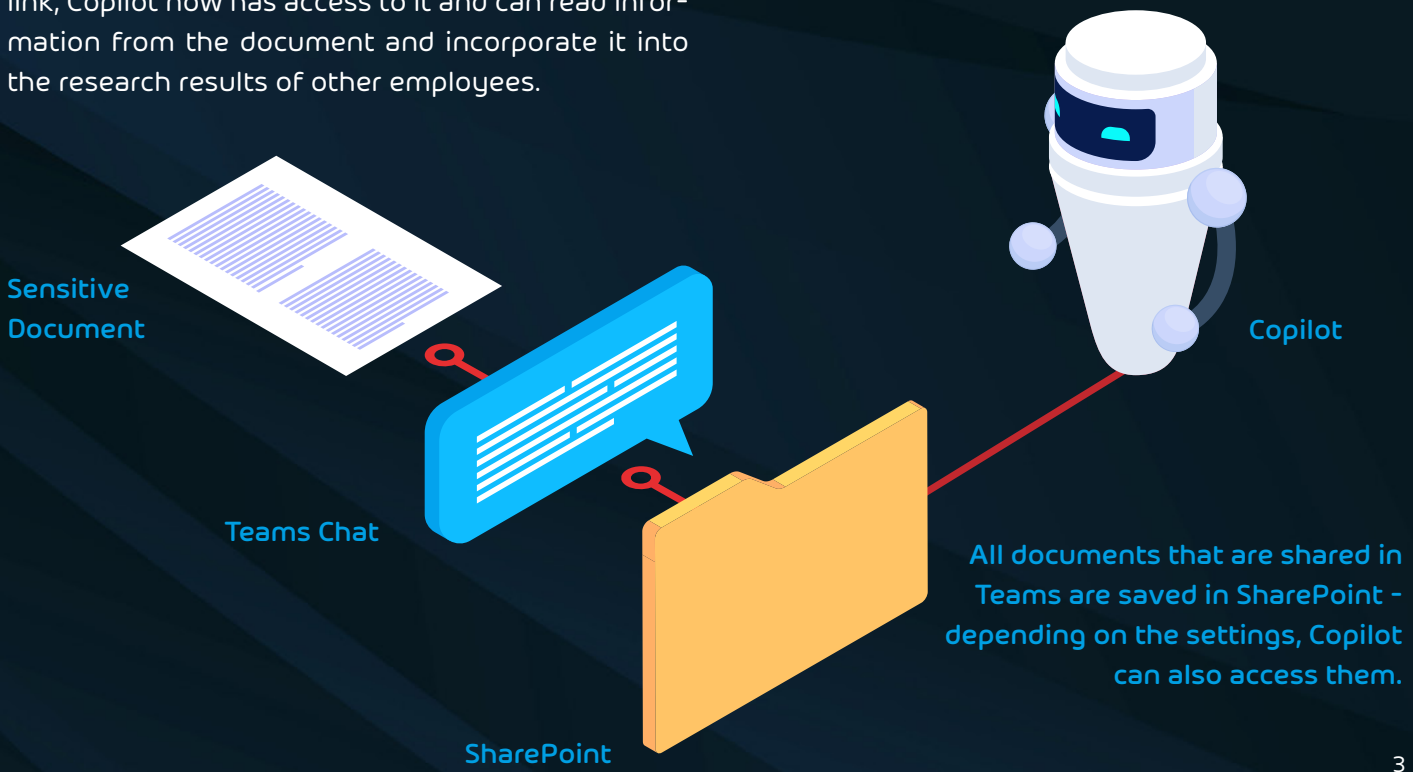
Sharing files in Teams also increases the risk of a data leak in connection with Copilot if the sharing settings are not configured properly. When a file is shared in a Teams chat, it is saved in the Team's site in SharePoint – something very few people are aware of.

Files that are uploaded in an individual or group chat end up in the "Microsoft Teams chat files" folder in OneDrive for Business. If you have a private channel, it gets its own, separate SharePoint site with a document library that only the members of the private channel have access to.

This means that all documents are stored in different SharePoint sites instead of directly in Teams – sites that Copilot can also gain access to.

It becomes even more problematic when external Microsoft 365 guest users use Copilot to access information from the company that they do not actually have direct access links to.

This should be alarming for CISOs and admins.



STRONG PERMISSION MANAGEMENT REQUIRED FOR MICROSOFT 365 DATA

Copilot can use and display all organizational data for which individual users have at least viewing permissions. It is therefore important that the company strictly implements the need-to-know principle, i.e. the assignment of minimum access rights in Microsoft 365.

This means only granting users access to the data required for their work and not granting any additional authorizations. These access rights should be updated when user roles change within the organization.

Efficient authorization management is also essential due to laws and regulations.

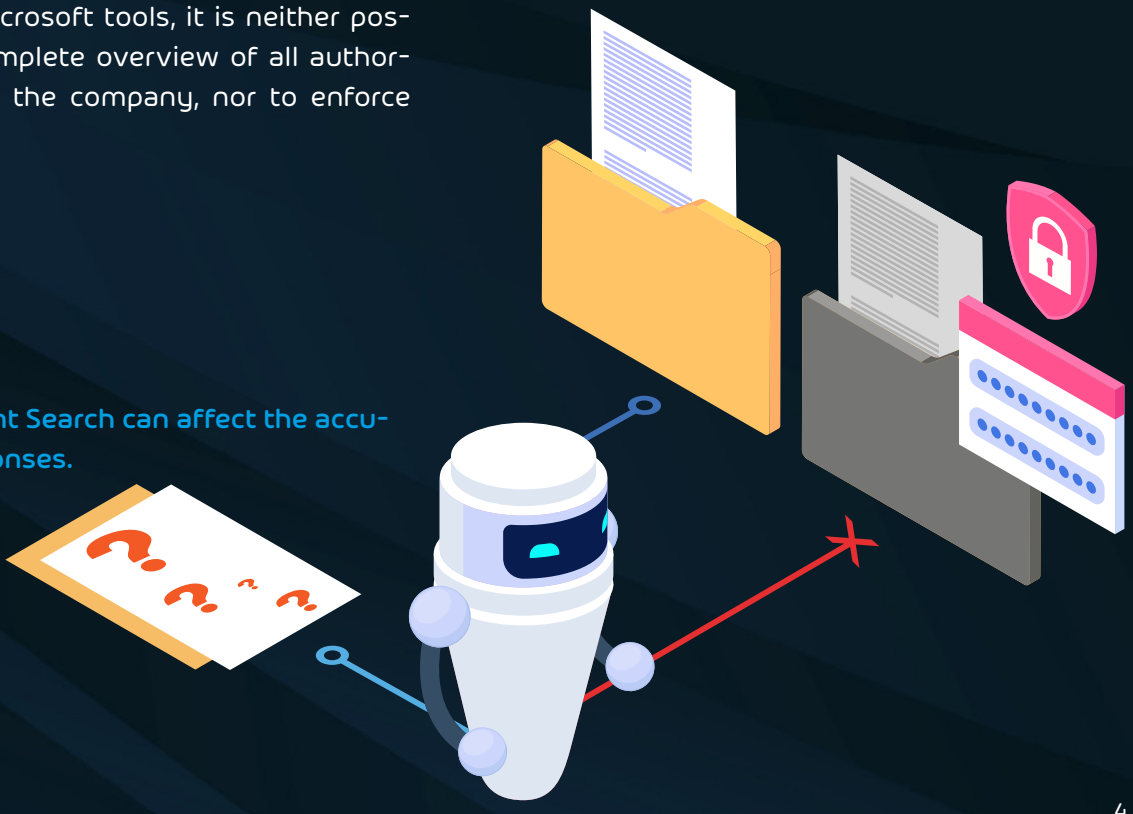
When it comes to accessing company data, legal requirements must also be met. These depend on various factors, such as the company location and what data is involved. Especially since NIS2 came into force, industry affiliation has also had a decisive influence on the future workload for admins and CISOs.

With the existing Microsoft tools, it is neither possible to obtain a complete overview of all authorizations assigned in the company, nor to enforce and monitor tenant-wide permission policies. In addition, changes to the settings within the Microsoft tools only affect files that are created or shared from the time of the change.

A knee-jerk reaction is therefore often to block all file sharing or not allow external sharing and to set strict default permissions for internal sharing. However, this will result in users looking for another way to share files. Sensitive documents may then be shared via third-party cloud storage, or consumer emails, where CISOs and admins have even less visibility.

'RESTRICTED SHAREPOINT SEARCH' SETTING FROM MICROSOFT IS NOT THE SOLUTION

Microsoft itself has also recognized that problems can arise with Copilot searches in SharePoint. In April 2024, the company introduced the "Restricted SharePoint Search" setting for administrators as a public preview. This allows company-wide searches and Copilot searches to be restricted to selected SharePoint sites.



Restricted SharePoint Search can affect the accuracy of Copilot responses.

This is a functionality that offers no scope for granular settings. Either a complete SharePoint site is allowed, or it is completely blocked.

Enabling this setting affects the overall search experience, even for non-Copilot users. Copilot has less information available, which can impact its ability to provide accurate and comprehensive answers.

So, for optimal Copilot use, this cannot be the solution either.

To ensure that files have the correct permissions on an ongoing basis and that only files intended for the user appear in Copilot searches, a third-party solution is needed that enables efficient data lifecycle management on a large scale for Microsoft 365.

BECOMING COPILOT-READY WITH 365 PERMISSION MANAGER

What is urgently needed to comply with defined permission policies is a scalable tool that effortlessly covers even large tenants with thousands of SharePoint sites.

With 365 Permission Manager, it is possible to effectively monitor and manage access and permissions. Particularly regarding Copilot, the simplification of permission management prevents information from spreading unintentionally.

Instead of having to navigate through the various portals in Microsoft's native toolset, 365 Permission Manager provides a convenient and user-friendly interface for admins and CISOs to gain a comprehensive overview of permissions in M365 environments, define compliance policies and prevent or revise violations.

THE ADVANTAGES OF 365 PERMISSION MANAGER

Comprehensive monitoring

» 365 Permission Manager provides a complete overview of M365 permissions for SharePoint, OneDrive and Microsoft Teams. An advanced filter function shows which elements external users or guests can access. Furthermore, admins and CISOs are notified when files, sites or folders are shared with external stakeholders.

Customize permission policies

» 365 Permission Manager allows you to determine predefined permission policies and create user-defined policies. These can be applied at site, folder, and file level as required. This makes it fundamentally different from the 365 Microsoft tools, which provide standardized policies.

Manage permissions on a large scale

» Large-scale adjustments can be made in the Control Panel of 365 Permission Manager. With so-called mass actions, authorizations for any number of tenants and groups can be adjusted at the same time. This saves time and effort and ensures that employees' authorizations are compliant.

Stay on top of things at all times

» In the event of a violation, the admin or CISO receives a warning message. The users and sites, files or folders involved are indicated. This enables immediate action to prevent data leaks. Breaches can be approved or rejected on a case-by-case basis or in mass actions.

» A particularly useful feature is the to-do list: This lists all violations of the policies applied to each SharePoint Online site. These violations can be corrected on a large scale, with exceptions being defined if there is a business justification. Employees are also held accountable. They are notified by email of policy violations that affect their OneDrive or SharePoint sites of which they are site owners.

Whether it's about complying with permission policies, protecting information and data, or being prepared for the use of Copilot in the company, 365 Permission Manager is designed to meet all these requirements and CISOs and admins can look forward to the use of Copilot in a safer and more compliant way.