



BLACK CELL
Protecting critical infrastructures

WHITEPAPER

DIGITAL CHAOS IN SHAREPOINT AND COPILOT

is the best recipe for oversharing

Created by

Márk Fülöp | Cloud Security
April 2026



TABLE OF CONTENTS

ABOUT BLACKCELL	3
OVERVIEW	5
THE PROBLEM	
HOW DID WE GET HERE?	
MEASURES	
SOLUTIONS	8
THOUGHTFUL DEPLOYMENT OF M365 COPILOT	
SHAREPOINT ADVANCED MANAGEMENT	
PURVIEW DATA SECURITY POSTURE MANAGEMENT	
SOURCES	14

ABOUT BLACK CELL

Black Cell is a European cybersecurity company focused on protecting critical infrastructures and the organizations that support them. Our business units cover SOC, Integration, Offensive Security, Cloud Security, Compliance, and ESM (Enterprise Security Monitoring). We take a customer first approach that starts with listening, then shaping solutions to fit the way our clients operate.

Our teams are adaptable and draw on deep knowledge across industries and technologies, from IT and Cloud to ICS/OT. We engage for the long term, providing continual support, service improvement, and measurable outcomes over the lifecycle of the relationship. Clients rely on us to connect regulatory requirements with technology choices and to guide organizational transformation that sticks.

We combine architecture, implementation, and managed operations to close gaps quickly and build sustainable capability. Local presence in Central Europe matters to us, with teams in Budapest and Frankfurt am Main that understand the regional context. This proximity helps us respond faster, coordinate with partners, and keep stakeholders aligned. Above all, we aim to be a trusted partner who strengthens resilience today and prepares you for what comes next.

DISCLAIMER

The information provided in this document is for general guidance only and is used at your own risk. No contractual or advisory relationship is created between Black Cell and any person accessing or using this document or any part of it. Black Cell accepts no liability for any actions, decisions, or consequences arising from the use of this material.

References to third-party sources are included where appropriate. Black Cell is not responsible for the content, accuracy, or availability of external sources, including websites mentioned in this publication.

CONTACT

Béla Droppa

CEO

bela.droppa@blackcell.io

COPYRIGHT NOTICE

© 2026 Black Cell Hungary Zrt. & Black Cell Germany GmbH (hereinafter jointly referred to as Black Cell).

All rights reserved. This publication may be freely distributed in its complete and unaltered form for informational purposes. However, reproduction, modification, or extraction of any part of this document (by any means, including electronic, mechanical, photocopying, or recording) is strictly prohibited without prior written permission from Black Cell.

OVERVIEW

2.1. THE PROBLEM

The rapid development of artificial intelligence presents significant risks. AI doesn't create new problems; it amplifies old ones. For example, with AI, discovery and interpretation of data stored on the company's infrastructure gets significantly easier, meaning unauthorized personnel can find such data more easily. This could root from years of unhealthy sharing habits, incautious access management practices, or oversharing scenarios present on data storage services (such as OneDrive, SharePoint).

The screenshot shows a Microsoft Teams chat interface. At the top, there are tabs for 'Work' and 'Web'. The time is 11:10 AM. A question is asked: 'Are there any ORG changes happening next month'. The AI-generated response is as follows:

Yes, there are some organizational changes happening next month. Here are a few updates:

- BWS Organizational Update:** Kristin Patterson has joined the BWS leadership team to lead the Customer Voice & Health Team. Kadji Bell will transition manager responsibilities to Kristen and take on a critical IC role focused on the execution of the center of excellence, change management, and scaling processes. This change will be effective from August 26 ¹.
- Changes to the BWS Design team:** Mona Kane, Ray Tanaka, and Sarah Evans will move to Sarah Perez's team. Mona will report directly to Sarah, and Ray and Sarah will report to Robyn. Sara Kiani will remain in BWGD and will report to Robin Counts' team. This change is effective immediately ².
- Confidential Q2 CY24 ReOrg:** There are org changes coming up on September 4th based on this report ³ ⁴.

At the bottom of the chat, there are buttons for 'Copy' and 'Share'. Below these buttons, it says '1 of 20 responses' and 'AI-generated content may be incorrect'. There are also thumbs up and thumbs down icons.

If we start rolling out AI (especially Copilot which is closely integrated with Office 365) with these long-standing bad practices, and without appropriate hardening, scenarios such as the one depicted above can unfortunately happen. We can see that the user was able to discover a document which was intended to be confidential but wasn't protected with any of the features present in the product to prevent such scenarios.

Without AI, the user would most likely never (or much harder) have discovered this file. Now, with AI, they have in fact discovered it, and they don't even have to interpret it: Copilot will do it for them, enriched with all the organization-specific knowledge the user has access to.

It's important to note that Copilot can't access information that the interacting user doesn't have access to. The risk is not that Copilot will grant users higher access than they already have, but Copilot is much quicker in search, and it will surface and interpret subtle information much easier.

2.2. HOW DID WE GET HERE?

Before taking a deeper dive in those solutions, let's see what the most common configuration issues are leading to oversharing, and its amplification by AI:

- Site privacy settings that grant access to everyone in the organization.
- Default sharing options set to "everyone," bypassing more secure configurations.
- Broken permission inheritance, where site-level permissions don't align with those at the file or folder level.
- Sharing with the "everyone except external users" domain group
- Sites and files without sensitivity labels that enforce policies around how data can be accessed and shared.

- Unknown, arbitrary shares present on the users' OneDrive accounts or SharePoint sites without the IT Security team's knowledge

2.3. MEASURES

Microsoft is well aware of the risks described above and provides various ways to counter them. By leveraging those solutions provided by Microsoft, including Purview, organizations can implement effective AI governance strategies. This approach helps address the amplified risks associated with AI growth and ensures compliance with regulatory and organizational requirements. It is important to note, when an organisation intends to comply with the EU's AI Act or ISO/IEC 42001:2023, technical compliance is a vital aspect of the assurance process.










SOLUTIONS

3.1. THOUGHTFUL DEPLOYMENT OF M365 COPILOT

This phased approach helps organizations assess risk, act, and build lasting governance practices without slowing innovation. It consists of three phases:

- **Pilot (optional):** Deploy Copilot to a sub-set of users and grant access to up to 100 popular, low-risk sites. Pilots are typically done to validate core Copilot use cases before a larger deployment. This phase helps validate permission controls, surface oversharing issues, and build internal confidence before scaling.
- **Deploy:** Scale Copilot use across the organization while remediating oversharing risks. Use native tools to secure sensitive data, increase site privacy, and enforce labelling policies. By the end of this phase, Copilot is broadly deployed with oversharing guardrails in place.
- **Operate:** Establish ongoing governance with automated policies, regular monitoring, and continuous improvement to further reduce risk, secure sensitive data, and improve Copilot responses. As collaboration grows, AI access will remain aligned with business and security intent.

Address internal oversharing concerns for M365 Copilot deployment

	Pilot (Optional) 	Deploy 	Operate 
Activities	<ul style="list-style-type: none"> Identify most popular sites & assess oversharing Grant Copilot access to popular, low risk sites Turn on proactive audit and protection 	<ul style="list-style-type: none"> Discover oversharing risks Restrict sensitive info from Copilot access and/or processing Increase site privacy 	<ul style="list-style-type: none"> Further reduce risk and simplify oversight Further secure sensitive data Improve Copilot responses
Outcomes	 Deploy copilot to sub-set of users with up to 100 sites	 Copilot fully deployed in your organization	 Continuous improvement of data security practices
Effort*	 2-4 days	 2-4 weeks	 More than one month

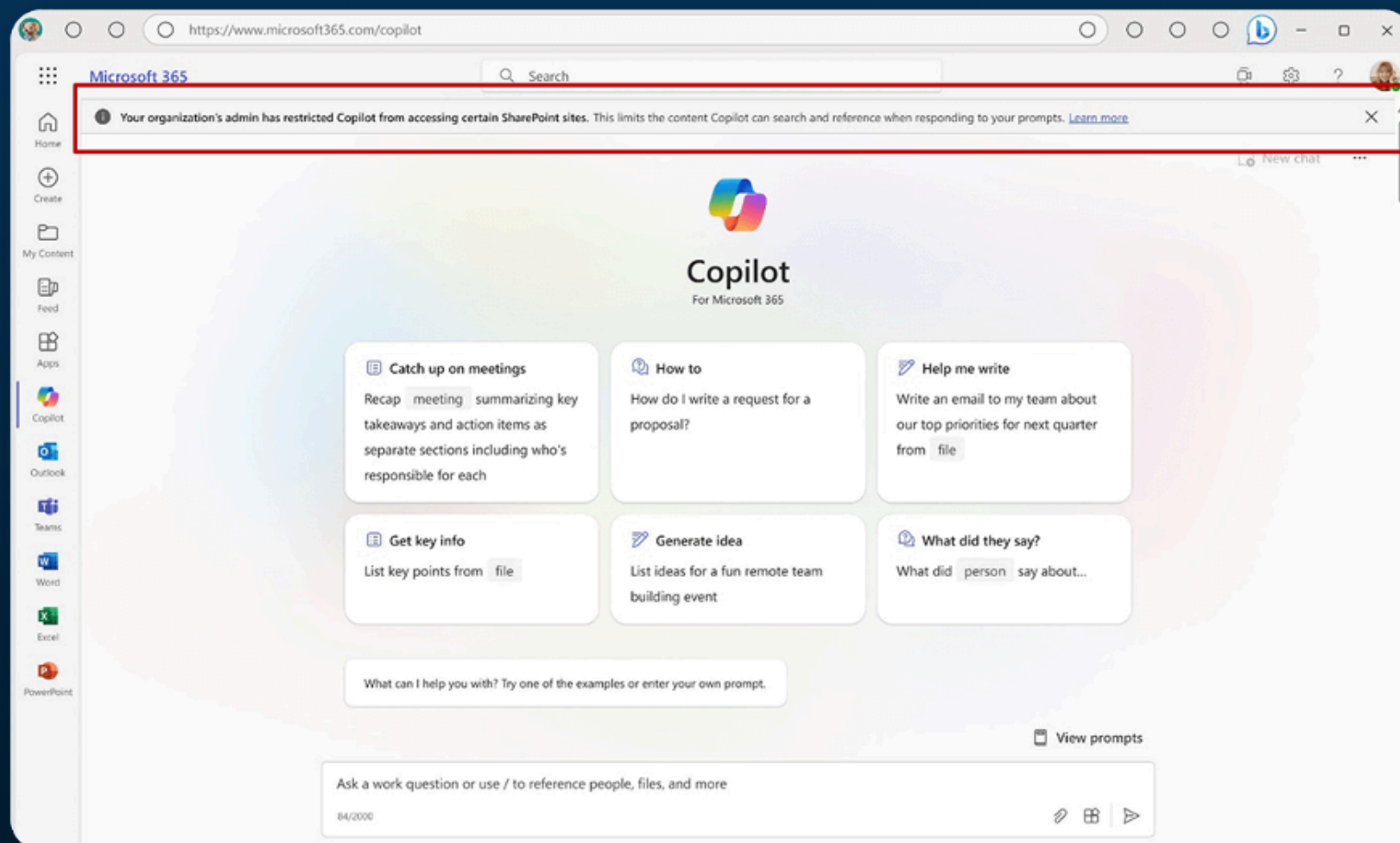
3.2. SHAREPOINT ADVANCED MANAGEMENT

SharePoint Advanced Management (SAM) is an add-on license, which is included with M365 Copilot. It equips IT and security leaders with tools to assess, clean up, or lock down problematic SharePoint sites before Copilot scales.

- **Content Management Assessment:** Provides a guided evaluation of your SharePoint environment, surfacing misconfigurations, inactivity, permission issues, and lifecycle risks across the thousands of sites in your tenant. It packages that data into a single, actionable dashboard, with prescriptive actions for quick resolution. This assessment becomes your baseline for governance.
- **Site Lifecycle Management:** Automatically identifies inactive, ownerless, or uncertified sites and enables scalable remediation actions, such as marking them read-only, archiving them, or prompting owners to take action to maintain access to site content. This tool helps reduce risk by cleaning up content before it can be surfaced by Copilot.

- **Oversharing Control with Permission State Reports:** Provides detailed, customizable reports of site permissions across Microsoft 365 to uncover oversharing risks like broken inheritance, public links, and excessive group access. The report deduplicates group membership to show the true number of users with access, offering clear visibility into who can see what. From there, admins can trigger Site Access Reviews to prompt site owners to clean up permissions or apply controls like Restricted Access and Restricted Content Discovery to contain exposure.
- **Restricted Access Control:** Empowers admins to lock down a site to a specific set of users, ignoring existing permissions and applying a strict allow list. This gives you a rapid-response option to contain risk while implementing risk remediation measures and maintaining business continuity.
- **Restricted Content Discovery (RCD) + Delegation:** When immediate action is needed, RCD offers a fast and effective way to block overshared SharePoint sites from Copilot and agent access. With a single setting, organizations can limit the ability of end users to search for files from specific SharePoint sites. To scale oversight, admins can also delegate RCD authority to site owners, enabling a distributed model with shared responsibility.

For example, with active RCD, Copilot can be completely banned from sensitive or confidential SharePoint sites (such as where organizations store financial, or HR related information):



3.3. PURVIEW DATA SECURITY POSTURE MANAGEMENT (DSPM)

If you are eligible based on your M365 licenses, you can utilise Purview to closely monitor users' AI usage. This requires prior configuration, such as turning on Purview Auditing, or onboarding of devices to Purview for deeper insights.

Purview's DSPM acts as a control centre where you can secure data for AI applications and keep an eye on how AI is being used. It works best with M365 Copilot, but it can also give you certain visibility into 3rd party AI solutions.

After finishing deployment of DSPM, the following assessments will be available, in near real time:

Sensitive interactions per AI app

Sensitive information types shared with Microsoft Copilot, agents, and other AI apps.



Microsoft 365 Copilot



ChatGPT

18

Microsoft Copilot

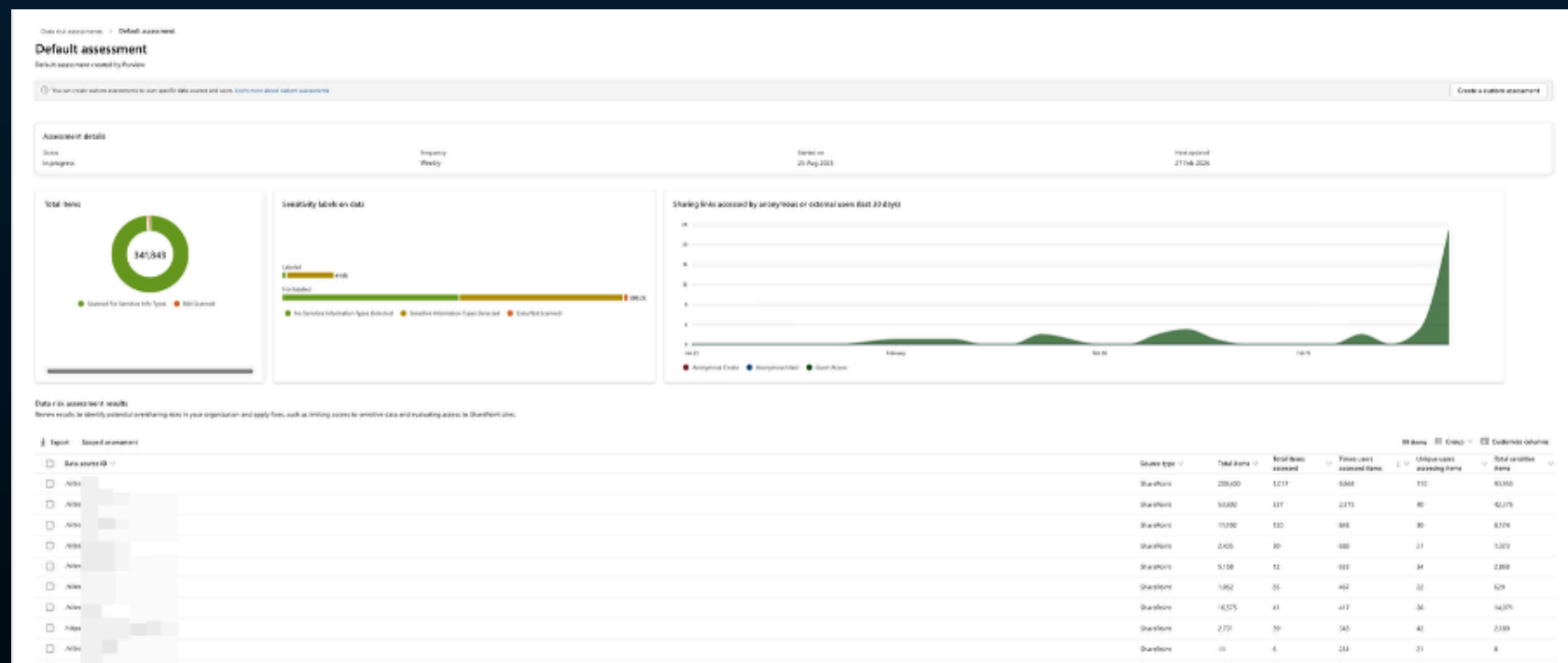
6

Google Gemini

1

● Other ● All Full Names ● All Medical Terms And Conditions 3 more

[View details](#)



For each SharePoint site, there are more details available:

The screenshot displays a user interface for a SharePoint site. At the top, there is a breadcrumb path **/sites/** followed by a redacted area. Below this, a navigation menu includes **Overview** (which is selected), **Identify**, **Protect**, and **Monitor**. The main content area is titled **Data source details** and shows the **Data source type** as **SharePoint** and the **URL** as a redacted string. A horizontal line separates this from the **Data coverage** section. This section reports **Total items in site** as **200,400** and includes a **View site** link. Below the total items, there are two horizontal bar charts. The first, labeled **Labeled**, shows a bar for **28.8k** items. The second, labeled **Not labeled**, shows a bar for **171.6k** items. A legend at the bottom indicates that green represents **No Sensitive Information Types Detected**, yellow represents **Sensitive Information Types Detected**, and orange represents **Data Not Scanned**.

If you require assistance securing your Copilot rollout, or you have already rolled out but are considering governing it more thoroughly, let us know, and we can help with enabling the solutions above and much more.

SOURCES

- <https://techcommunity.microsoft.com/blog/microsoft365copilotblog/mitigate-oversharing-to-govern-microsoft-365-copilot-and-agents/4448744>
- <https://www.syskit.com/governance-handbook/oversharing/microsoft-copilot-oversharing/#pid=1>
- <https://sharegate.com/blog/microsoft-purview-ai-hub-discover-and-protect-activity-in-copilot-and-other-generative-ai-apps>