The Anatomy of At-Risk Data in Microsoft 365

Understand the hidden risks behind everyday file sharing and how to take control.

eBook

WeActis by Mondata

Think the Data Shared by your Employees is Safe?

Oversharing, outdated links, and sensitive files with incorrect permissions all add up to *at-risk data*.

In this educational guide, we break down what makes a file “at-risk,” why it’s YOUR business (not just IT’s), and how modern collaboration combined with AI is amplifying the risk.

If you Use Collaboration Environments, you Own More Risk than you Think.

Collaboration has never been easier or more risky. Every day, files are uploaded, shared, and forgotten. Employees assume they're doing the right thing. Leaders assume IT has everything under control.

But here's the truth: data security in Microsoft 365 is a shared responsibility, and unmonitored sharing creates invisible risk that no one's managing. That's how sensitive data gets leaked, corrupted, or misused; especially in the age of generative AI.

To address the root causes of risk, we need to accept this truth: data security is no longer only IT responsibility, and if we want employees to own their role, it must be frictionless.

That's why WeActis exists. But before we show how it works, let's unpack the anatomy of a threat you've probably never seen – but that's growing inside your environment: At-risk data.

Chapter 1

What Is “At-Risk Data” in the Era of Collaboration?

At-Risk Data Refers to Files and Folders That:

- Are overexposed to unintended audiences (internal or external)
- Contain sensitive information but lack proper classification or protection
- Are shared through risky permission settings (e.g., editable links with no expiration)
- Remain unmonitored for extended periods, even though they’re still accessible

It’s not about malware or hackers.

It’s about what’s quietly leaking, corrupting, or decaying inside your own ecosystem.

The 4 Key Components of Risk

(What Makes a File At-Risk)

Each file or folder shared in Microsoft 365 carries a unique combination of risk attributes. Here's how WeActis breaks them down:

1

Access Scope: Who Can Reach This File?

The broader the access, the greater the chance of a data breach.

We evaluate the target audience:

- Public (anyone with the link)
- Entire organization
- External collaborators
- Specific users or groups

We also evaluate the type of item shared:

- Files (risk is isolated to one document)
- Folders (risk cascades to every file inside, even sensitive ones)

REAL-WORLD EXAMPLE

An Operations Manager shares a folder with the entire organization to give access to a single policy template.

However, the folder also contains archived supplier contracts and internal audit reports that were never intended to be shared with a broad audience.

No one flagged it because the intention was to help. But now, dozens of sensitive files are accessible to everyone, including new interns, external collaborators added to Teams, and potentially even AI tools integrated with Microsoft 365.

The result: A well-meaning action becomes a silent compliance and confidentiality risk one that could stay unnoticed for months.

HOW WEACTIS HELPS

WeActis notifies the Operations Manager about his at-risk shared folder and guides him on how to revoke the share.

2

Sensitivity: How Confidential Is the Information?

You can't protect what you haven't labeled.

WeActis evaluates:

- Microsoft Sensitivity Labels
- Your organization's risk weighting per label (e.g., Public, Internal, Confidential, Highly Confidential)

If a file has no label, WeActis assumes a Moderate impact which:

- Overstates the risk for a document meant for a larger audience
- Underestimates risk for sensitive documents with no label

BEST PRACTICE

It's better to label *only* sensitive files and leave others unlabelled than to have nothing labeled at all.

REAL-WORLD EXAMPLE

A legal contract with client data shared without a label **would never trigger a warning.**

HOW WEACTIS HELPS

WeActis **classifies** the document as containing moderately sensitive data and **notifies** the user when sharing reaches the acceptable threshold defined by the organization.

3

Permissions Type: What Can People Do with It?

Access is one thing. Control is another.

WeActis analyzes the permission rights:

- Write (can change file without leaving explicit traces)
- Write in revision mode (tracked edits)
- Read
- Read with no download

Different permissions carry different risk types:

- Data Integrity Risk: Editable documents can be overwritten
- Propagation Risk: Downloadable files can be re-shared without control
- AI Poisoning Risk: Deliberately changing content in files so the AI thinks it's the truth and sends the new "modified/ false" information to the users.

REAL-WORLD EXAMPLE

An intern gets "Edit" access to a forecasting spreadsheet. **One formula gets changed.** Results across the company are wrong and no one catches it for months.

HOW WEACTIS HELPS

WeActis **flags** the person who shared the document, indicating who they have given editing access to.

4

Permission Age: How Long Has the Risk Existed?

The longer a door is open, the more likely someone walks through it.

WeActis factors in:

- How long a permission has been in place
- Organization-defined thresholds:
  - Short-term (e.g. less than 30 days)
  - Long-term (e.g. more than 90 days)

A forgotten “anyone with the link” share from a year ago is much more likely to be misused than a file shared yesterday.

REAL-WORLD EXAMPLE

A team leader shares a financial forecast file with a regional manager during budget season. The file includes sensitive revenue projections and business assumptions.

The collaboration ends, but the shared link remains active with edit permissions.

Months go by. The regional manager changes roles. The file remains editable by someone who no longer needs access, and whose replacement may not even be aware that the file exists.

The result:
A high-impact file is exposed longer than necessary, with no oversight.

The issue isn’t just that it’s shared, it’s that no one’s reviewing if the access is still justified.

HOW WEACTIS HELPS

WeActis **notifies the SharePoint owner** where the financial forecast file is stored so he can review and revoke access.

Chapter 2

How WeActis Helps You Detect and Fix At-Risk Data

WeActis takes a proactive, user-centered approach to risk mitigation.

Step 1 – Discovery

- We scan Microsoft 365 (OneDrive, Teams, SharePoint)
- We analyze millions of file-level permission data points
- We generate a real-time inventory of files with “at-risk” status

Step 2 – Attribution

- We identify who created the risky share
- We also identify the owner of the resource (e.g., OneDrive or SharePoint site)

Step 3 – Notification

We send friendly, contextual nudges directly to the relevant users

We guide them to take action – no IT ticket needed

Step 4 – Resolution (with options)

Users can:

- Revoke the risky share
- Adjust permissions
- Share via a team workspace instead of private links

Risk Tolerance: Not One-Size-Fits-All

Every organization has different needs and appetites for risk.

That's why WeActis lets you:

- Customize the risk settings weighting
- Adjust weightings per sensitivity label
- Define your own time thresholds for sharing

Why This Matters for Everyone

For Employees

You're not just collaborators. **You're the gatekeepers of the organization's data.**

WeActis empowers you to do the right thing quickly, directly via Teams without impacting your day-to-day operations.

For Business Leaders

Risk is accumulating – quietly, invisibly.

Every day without visibility is a day of risk exposure. WeActis turns passive risk into **proactive measures** by empowering employees to take concrete action without increasing IT burden or disrupting business efficiency.

For Boards

You can't afford the risk of regulatory or reputational damage due to careless sharing.

WeActis finally provides visibility into all collaboration risks, tracks all actions taken, measures and demonstrates continuous improvement to strengthen the organization's security posture.

Final Thought: Data sharing is the new firewall.

If you don't control how it happens, your crown jewels are at risk and AI makes it worse.
Let WeActis help you turn your people into your strongest line of defense.

About WeActis

WeActis revolutionizes cybersecurity by turning employees into active defenders and making security a shared responsibility rather than an IT burden.

Integrated into Microsoft Teams, it seamlessly embeds security into daily workflows, guiding employees to mitigate risks in under five minutes per week.

By improving data hygiene in Microsoft 365, strengthening governance, and streamlining risk reduction, **WeActis** helps organizations build a Cybersecurity Resilience Culture—enhancing compliance, reducing data exposure, and driving measurable, lasting security improvements.

info@weactis.com
1-833-666-3282
WeActis.com

WeActis
by Mondata