

AT&T *Security Day May 2025*

# Secure your data using Microsoft Purview

Jesper Frisgaard Mortensen  
Solution Architect - Security

[linkedin.com/in/jfrisgaard/](https://linkedin.com/in/jfrisgaard/)



# *Data Security Agenda*

- ① Data Security challenges
- ② Microsoft Purview
- ③ Demos – from a user perspective
- ④ AI for Data Defenders

Hvorfor har Data Sikkerhed  
fået fornyet focus ?

# But securing data is complex and multi-faceted



Different types  
of data, users,  
and objectives



AI transformation  
brings new  
data risk



Regulations  
continue  
to evolve

# Fragmented solutions can be challenging

- Unnecessary data transfers

- Duplicate copies of data

- Inconsistent data classification

- Redundant alerts

- Siloed investigations

- Exposure gaps



- Increased implementation complexity

- Longer deployment times

- Greater management burden

- Higher costs

- Worse security outcomes

# Data security incidents can happen anytime, anywhere

Data at risk of misuse if organization has no visibility into their data estate

## External risks

User falls prey to phishing attack, compromises user credentials



**Data compromise**  
by external threat



## Internal risks

User copies file to a USB, then uploads to a personal Dropbox to take to a competitor



**Data theft** by  
malicious insider



User negligently shares sensitive data in generative AI apps



**Data leak** by  
negligent insider



User deletes sensitive information before leaving the organization



**Data sabotage** by  
disgruntled insider



# Generative AI is reshaping the world but there are associated data security risks..

User creates document without proper access controls making it easy for other users to reference it in Copilot



Data overexposure by negligent insider



User asks generative AI to find information on a secret project and leaks it to the press for personal gain



Data leak by disgruntled insider



User negligently shares sensitive data in consumer generative AI apps



Data leak by negligent insider





Integrated solutions to secure & govern your entire data estate

### DATA SECURITY

Secure data across its lifecycle,  
wherever it lives

Data Loss Prevention  
Insider Risk Management  
Information Protection

### DATA GOVERNANCE

Responsibly unlock value  
creation from data

Data Discovery  
Data Quality  
Data Curation  
Data Estate Insights

### DATA COMPLIANCE

Manage critical risks and  
regulatory requirements

Compliance Manager  
eDiscovery and Audit  
Communication Compliance  
Data Lifecycle Management  
Records Management

Unstructured & Structured data

Traditional and AI generated data

Microsoft 365 and Multi-cloud

### Shared platform capabilities

Data Map, Data Classification, Data Labels, Audit, Data Connectors





Integrated solutions to secure & govern your entire data estate

### DATA SECURITY

Secure data across its lifecycle,  
wherever it lives

Data Loss Prevention  
Insider Risk Management  
Information Protection

### DATA GOVERNANCE

Responsibly unlock value  
creation from data

Data Discovery  
Data Quality  
Data Curation  
Data Estate Insights

### DATA COMPLIANCE

Manage critical risks and  
regulatory requirements

Compliance Manager  
eDiscovery and Audit  
Communication Compliance  
Data Lifecycle Management  
Records Management

Unstructured & Structured data

Traditional and AI generated data

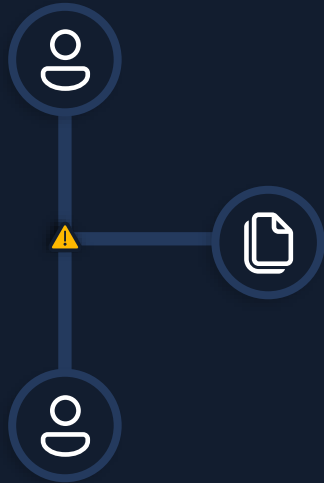
Microsoft 365 and Multi-cloud

### Shared platform capabilities

Data Map, Data Classification, Data Labels, Audit, Data Connectors

# To secure their data, organizations should :

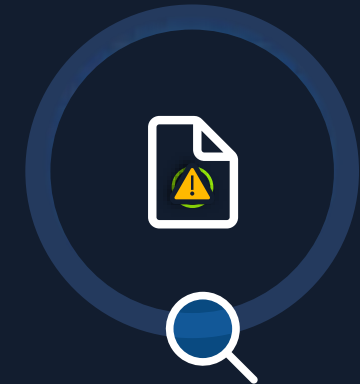
Discover hidden risks  
to data wherever it  
lives or travels



Protect and prevent  
data loss across your  
data estate

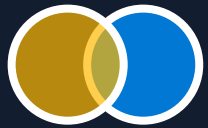


Quickly investigate  
and respond to data  
security incidents



Balance data security and productivity

# Fortify data security with an integrated approach



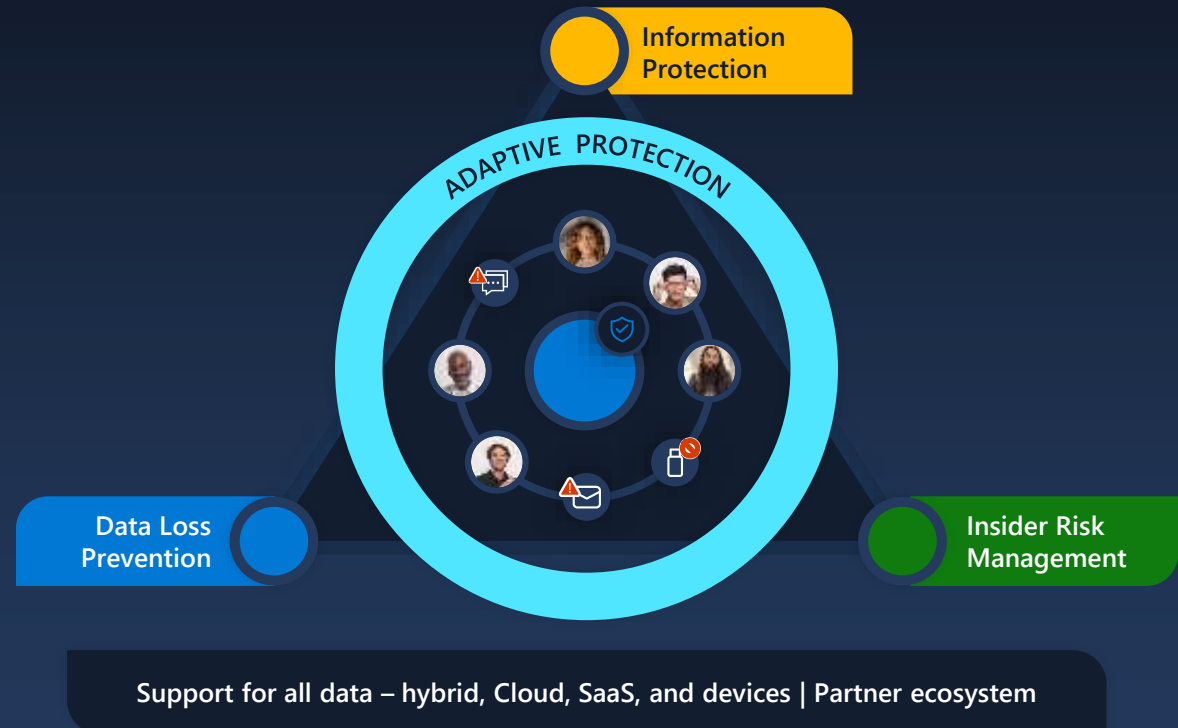
Automatically **discover, classify and label sensitive** data, and **prevent its unauthorized use** across apps, services, and devices.



Understand the **user intent and context around the use of sensitive data** to identify the most critical risks



Enable **Adaptive Protection** to assign high-risk users to appropriate DLP, Data Lifecycle Management, and Entra Conditional Access policies



# Microsoft Purview to help with data discovery

Choose a classifier or a label <

Filter on labels, classifiers, or categories

^ Sensitive info types

All Full Names298

All Medical Terms And Conditions56

Credit Card Number46

Diseases44

EU Debit Card Number43

See all 45

Microsoft 365

Export

Data source ^

Copilot

OneDrive

SharePoint

Teams

Data risk report for unprotected sensitive data

Unprotected sensitive assets across data sources ⓘ

OneDrive

Teams

SharePoint

Exchange

Microsoft 365

Export

4 items Customize columns

Filter set:

Location: Any

Unprotected classifier: Any

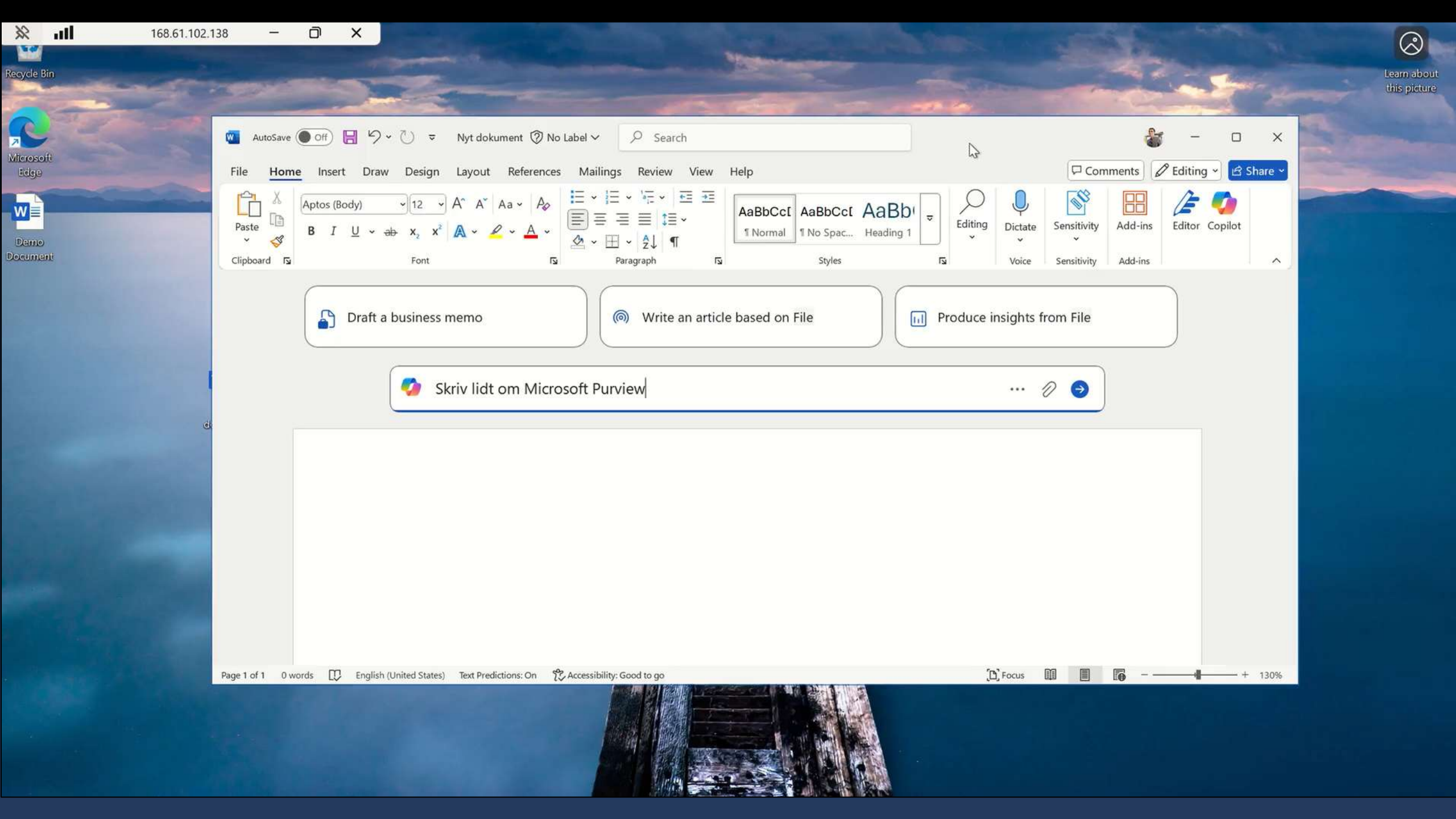
Unprotected label: Any

Add filter

Location	Number of unprotected assets...	Unprotected classifiers ⓘ
Teams	61	All Full Names, All Medical Terms And Conditions, Unauthorized disclosure, Lab Test...
OneDrive	64	All Full Names, Finance, HR, Credit Card Number, U.S. Bank Account Number, EU De...
Exchange	28	Philippines Passport Number, Indonesia Passport Number, New Zealand Social Well...
SharePoint	44	All Full Names, Finance, All Medical Terms And Conditions, Diseases, HR, U.S. Social...

## Demo – user perspective

- ① Auto labeling of Word document
- ② Data Loss Prevention (DLP) in Microsoft Teams
- ③ Data Loss Prevention (DLP) in M365 Copilot



AutoSave Off

Nyt dokument No Label

Search

File Home Insert Draw Design Layout References Mailings Review View Help

Paste

Clipboard

Aptos (Body) 12

B I U

Font

Paragraph

Styles

Editing

Dictate

Sensitivity

Add-ins

Editor Copilot

Draft a business memo

Write an article based on File

Produce insights from File

Skriv lidt om Microsoft Purview

Page 1 of 1

0 words

English (United States)

Text Predictions: On

Accessibility: Good to go

Focus

130%

- Activity
- Chat
- Calendar
- Calls
- OneDrive
- Connections
- ...
- Apps

Chat

... 🔍 📝 ▾

Unread Channels Chats Unmuted ▾

- Discover
- Mentions


Favorites

 Alex Wilber (You)

Chats

 New message

Teams and channels

To:  Megan Bowen X

👁 Show hidden chat history

Type a message

🔗 😊 📎 + ➤





Demo docs

OneDrive > Alex - Contoso > Demo docs

Search Demo docs

New

Sort View

Details

Name	Status	Date modified	Type	Size
No Copilot indexing		3/1/2025 1:10 PM	Microsoft Word Doc...	30 KB
Ok Copilot indexing		3/1/2025 1:09 PM	Microsoft Word Doc...	30 KB

Home

Gallery

Alex - Contoso

Desktop

Downloads

Documents

Pictures

Music

Videos

Demo docs

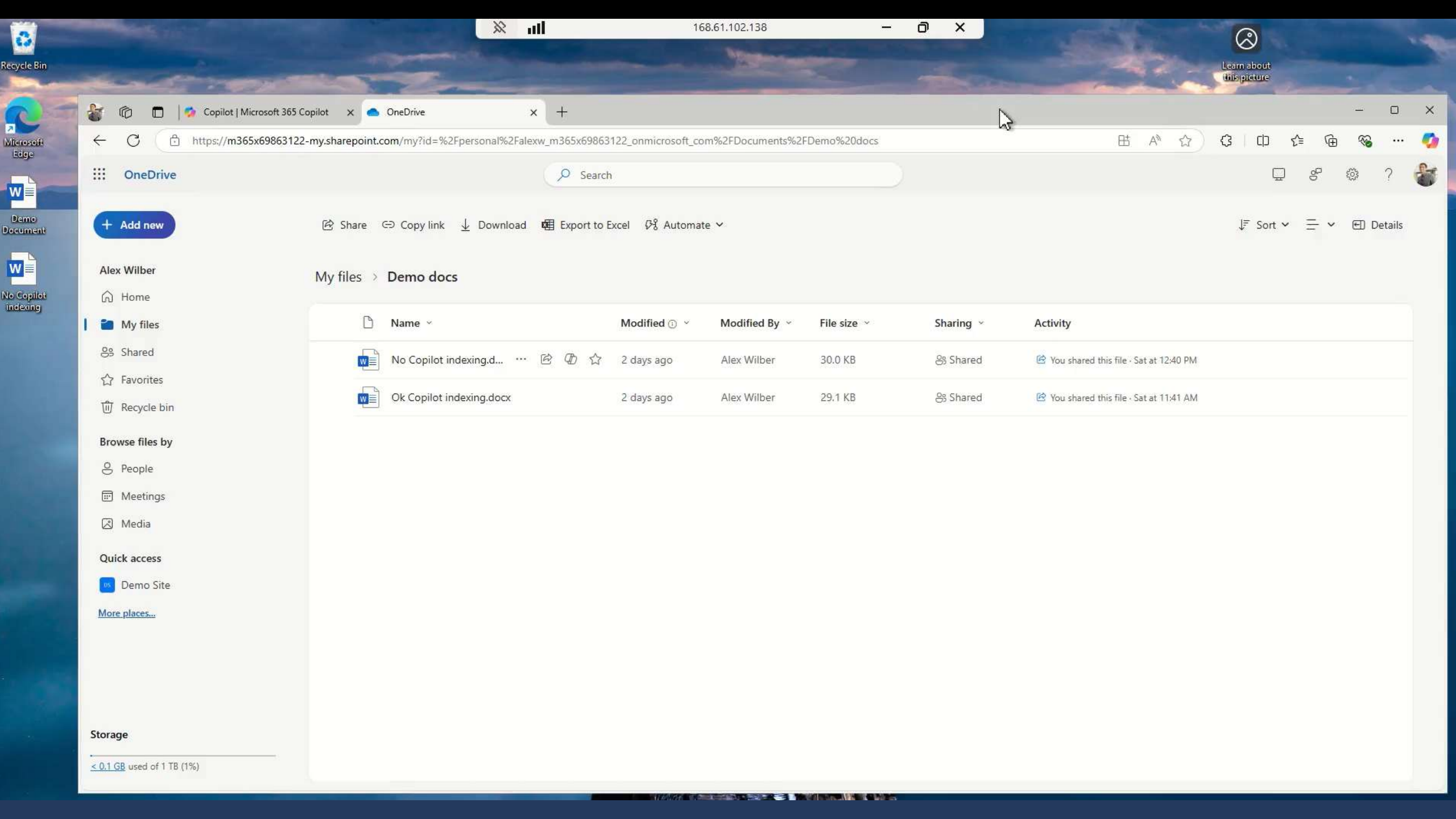
This PC

Windows (C:)

Network

2 items 1 item selected 29.0 KB Available on this device





Copilot | Microsoft 365 Copilot

OneDrive

https://m365x69863122-my.sharepoint.com/my?id=%2Fpersonal%2Falexw\_m365x69863122\_onmicrosoft\_com%2FDocuments%2FDemo%20docs

OneDrive

Search

+ Add new

Share Copy link Download Export to Excel Automate

Sort Details

Alex Wilber

Home

My files

Shared

Favorites

Recycle bin

Browse files by

People

Meetings

Media

Quick access

Demo Site

More places...

Storage

< 0.1 GB used of 1 TB (1%)

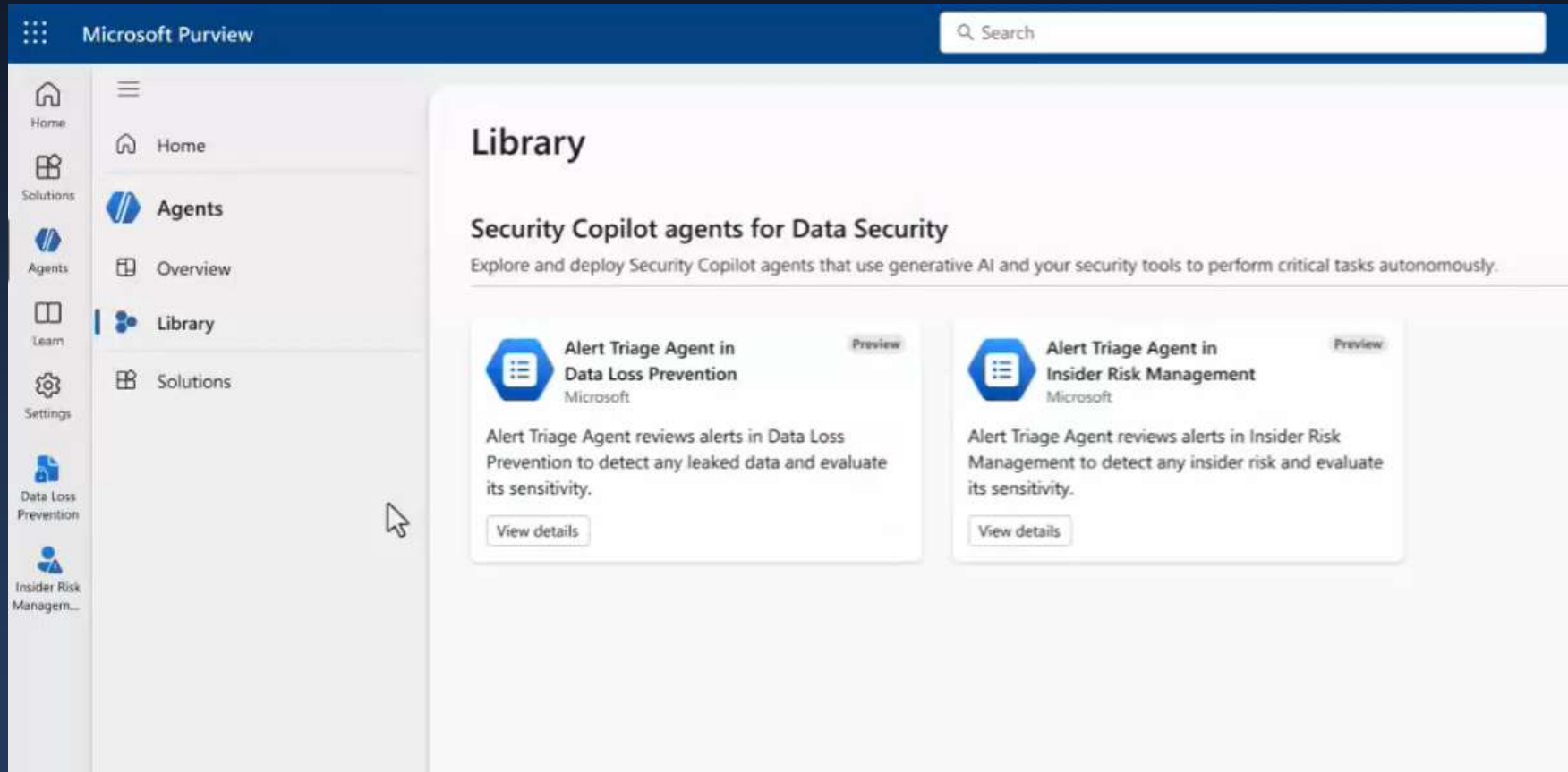
My files > Demo docs

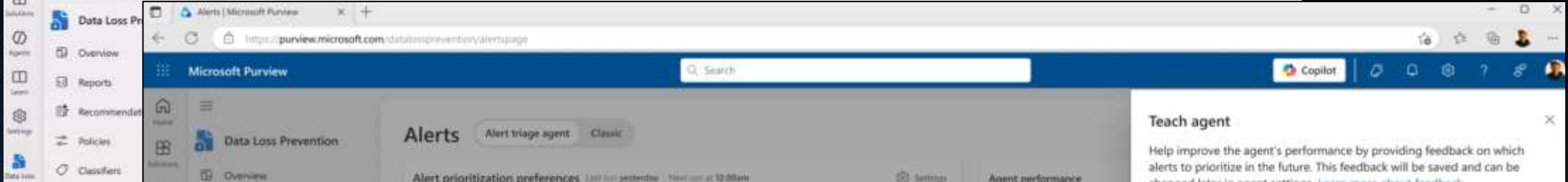
Name	Modified	Modified By	File size	Sharing	Activity
No Copilot indexing.d...	2 days ago	Alex Wilber	30.0 KB	Shared	You shared this file · Sat at 12:40 PM
Ok Copilot indexing.docx	2 days ago	Alex Wilber	29.1 KB	Shared	You shared this file · Sat at 11:41 AM

# AI for Defenders : Microsoft Security Copilot Agents

*Public Preview  
(require Security Copilot SCU's)*

[Automate cybersecurity at scale with Microsoft Security Copilot agents](#)





Alerts	
Alert prioritization preferences: Last run yesterday, Next run at 12:00am	
<div>All (406) Needs attention (6) Less urgent (76) Not triaged (324)</div>	
<input type="checkbox"/> Alert name	Alert categorization ⓘ
<input type="checkbox"/> Oversharing for document 'sales-strategy2023.doc' in Microsoft Copilot Agent: credit card number was accessed on unallowed app by user with high risk score	Needs attention ⓘ
<input type="checkbox"/> DLP policy match for document 'project_obsidian_roadmap.docx' Agent: repeat offenses by this user sending business critical documents to external email	Needs attention ⓘ
<input type="checkbox"/> DLP policy match for document 'employee agreement-2.doc' in SharePoint Agent: user downloaded PII from a SharePoint site, emailed it to themselves, then deleted the file	Needs attention ⓘ
<input type="checkbox"/> DLP policy match for document 'resume_345.doc' in SharePoint Agent: emails sent externally containing data from potential new highly confidential business initiative	Needs attention ⓘ
<input type="checkbox"/> DLP policy match for document 'Q2-Customer Data.xlsx' Agent: downloads of health data by a user that was notified 9 days ago about company policy	Needs attention ⓘ
<input type="checkbox"/> DLP policy match for email with subject '[EXTERNAL] FW: andres pdf' Agent: downloads of health data by a user that was notified 9 days ago about company policy	Needs attention ⓘ

# Microsoft Data Investigations (DSI)

Public Preview  
(require pay-as-you-go)

[Accelerate data security investigations with AI-powered deep content analysis | Microsoft Community Hub](#)

The screenshot displays the Microsoft Purview Data Investigations (DSI) interface. The top navigation bar shows the Microsoft Purview logo and a search bar. The main content area is titled "Investigations > (814fa4da) Data Leak" and shows the "Analysis" tab for "ID 1134731: Multi-stage investigation".

On the left, a sidebar contains filters for "Categories (Default)" and "Categories (AI-generated)". The "Default" categories include Business (1,255), Communications records (0), Credentials and access (546), Customer (1,356), Employee (0), Financial (1,932), Health (909), Incident and investigation (0), Intellectual property (18,376), Marketing (614), Operational (0), Personally identifiable (0), and Regulated data (388). The "AI-generated" categories are also listed.

The main analysis view displays a graph titled "Find high severity credential risks (241 items)". The graph shows a network of data items and their relationships. Key nodes include "Items (241)", "Files (56)", "Users (2)", "IP (2)", "Files (82)", "Users (2)", "Files (103)", and "10.1.44.16".

A pop-up window titled "Find high severity credential risks (241 items)" is overlaid on the right side of the main view. It lists "2 potential high risk users" and provides details on the security risks identified, including high risk files downloaded and potential high risk users. The window also includes a "Mitigate 241 items" button and a "Dismiss" button.

Video

# Get started with actionable insights

## Step 1

One-step insights and agentless deployment



Discover  
sensitive data



Leverage out-of-the-box and custom **Sensitive Information Types** (SITs), trainable classifiers, and more.



Understand  
critical insider risks



Turn on **insider risk analytics** and create a recommended data leak policy. Turn on **Adaptive Protection**.



Understand critical  
exfiltration risks



Turn on **DLP analytics** and create a recommended **DLP policy** in simulation mode.

Integrate seamlessly on a unified platform without dependency

Actionable insights without impact on end users

# Advance your journey with adaptive controls

## Step 2

Advance like a pro with built-in intelligence



### Label and protect data

Define **label taxonomy and label content** by enabling default labels, configuring manual labeling, or scaling with auto-labeling.



### Investigate critical risks

Review and investigate **high-severity insider risk alerts** and finetune policies.



### Prevent sensitive data loss

Fine-tune DLP policies and add **Adaptive Protection** as a condition in your DLP policy. Run DLP policy in **block or block with override** mode.

## ***Data Security** We talked about :*

- ① Data Security challenges
- ② Microsoft Purview
- ③ Demos – from a user perspective
- ④ AI for Data Defenders

Thank you

