A large pile of green Brussels sprouts filling the background of the slide.

#CollabDaysBE

Microsoft Purview Information Protection demystified

Albert Hoitingh | @alberthoitingh

CollabDays Belgium 2022 by BIWUG



Thanks to our sponsors!

Platinum



Gold



Silver



European
SharePoint
Office 365 & Azure
Conference

SharePint



Community



Organized by



Albert Hoitingh

Sr. Consultant Microsoft 365 security,
compliance & risk @InSpark



@Alberthoitingh



<https://linkedin.com/in/appieh>

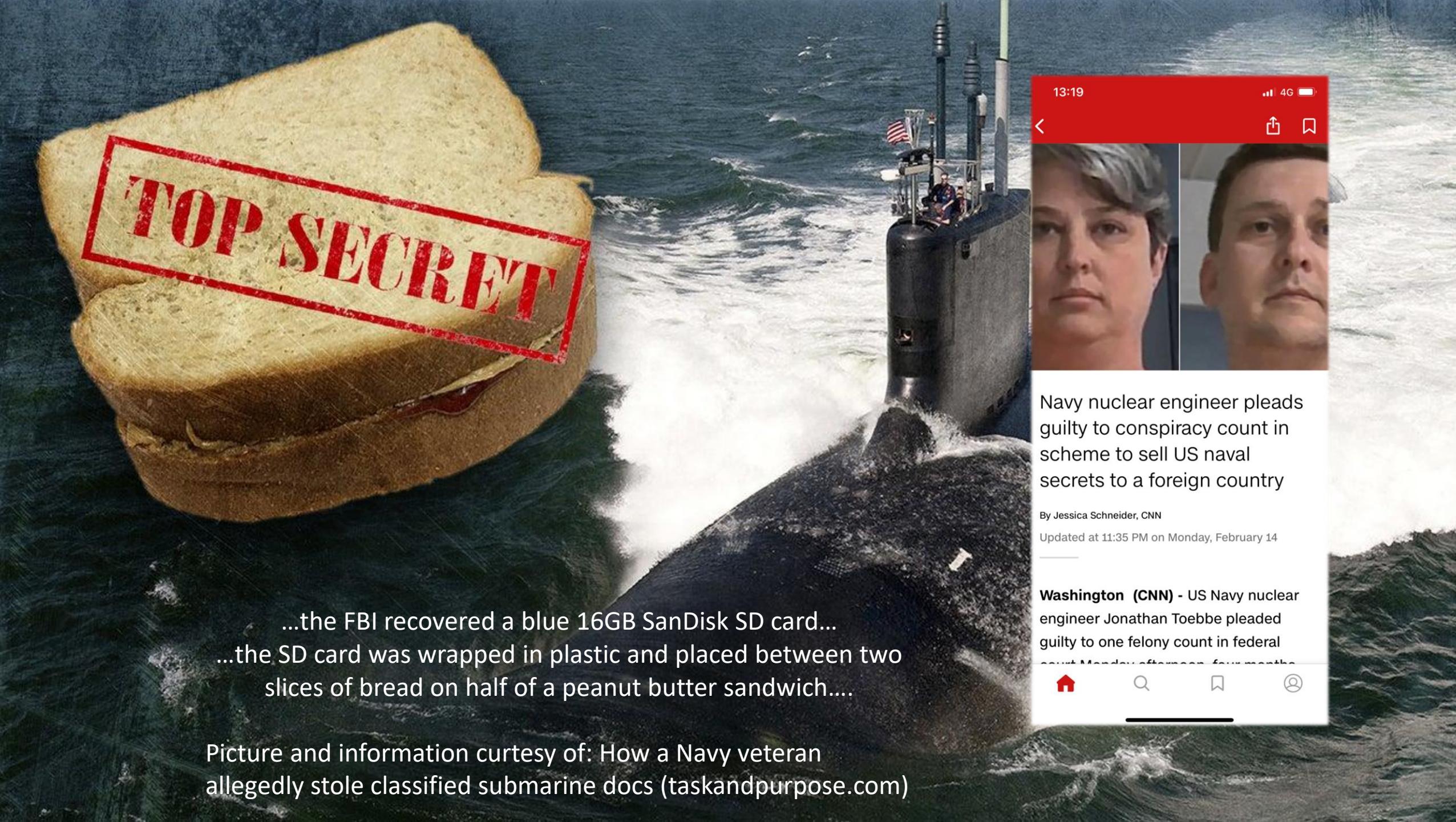


<https://alberthoitingh.com>



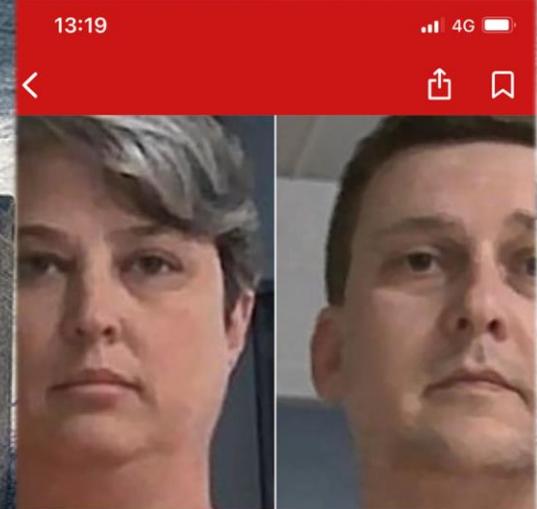
Microsoft Purview Information Protection





...the FBI recovered a blue 16GB SanDisk SD card...
...the SD card was wrapped in plastic and placed between two slices of bread on half of a peanut butter sandwich....

Picture and information courtesy of: How a Navy veteran allegedly stole classified submarine docs (taskandpurpose.com)

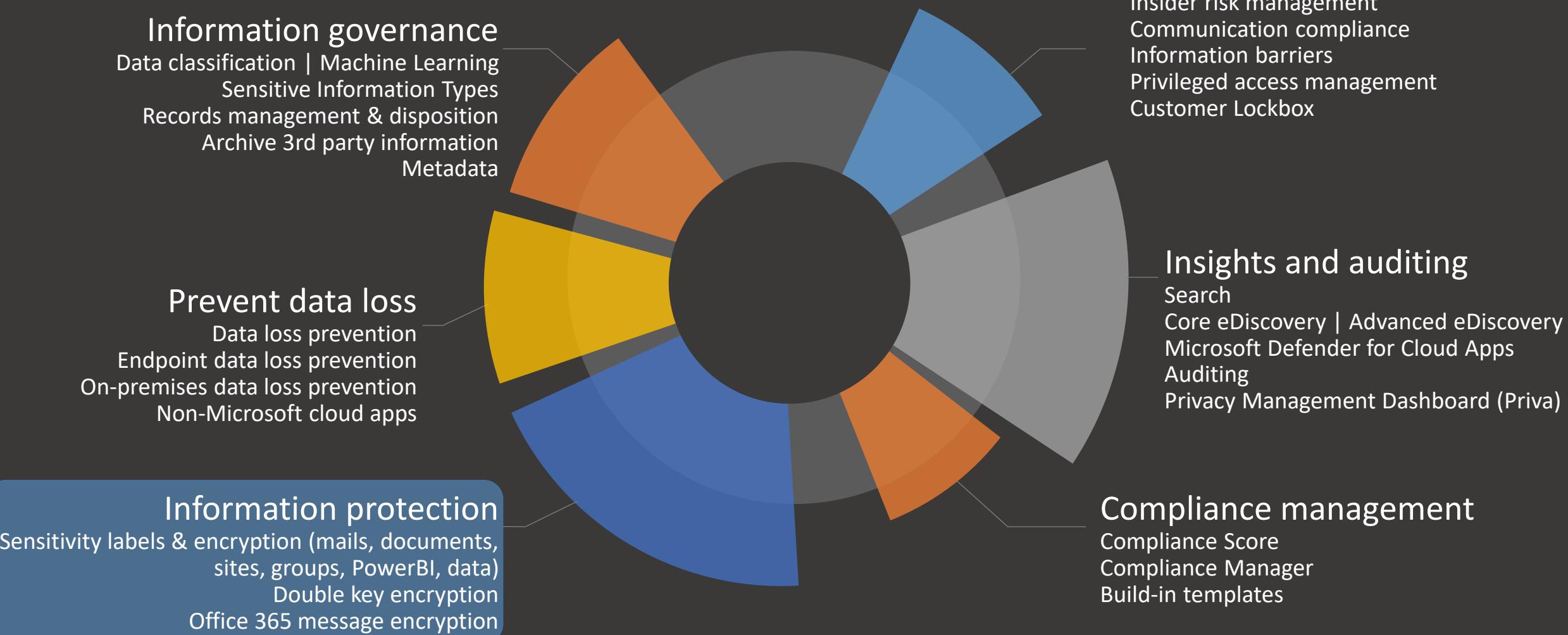


Session Objectives

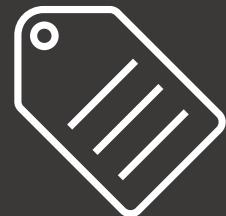
During this session we will:

- Get an overview for Microsoft Purview
- Sensitivity labels
- Different clients
- Auto-labeling
- Tips & tricks (and Ignite 2022)

Microsoft Purview portfolio



Microsoft Purview Information Protection



Discover sensitive information

Classify information

Protect information

Monitor

Platforms

On-premises	Office Apps	SPO EXO Teams PowerBI	Non-Microsoft cloud
Classify and label data in on-premises repositories, including fileshares and SharePoint Server.	Label and protect Office files on Windows, Mac, iOS, Android and web.	Label and protect access to Microsoft Teams, SharePoint Online sites and PowerBI reports and dashboards. Protect e-mails using labels and Office 365 Message Encryption. Label content automatically when at rest.	Use Microsoft Defender for Cloud Apps to extend the labeling to platforms like Box and Google Workspace.
Unified classification, labeling and protection for sensitive information			

London

*Unified
labeling*

*sensitivity
labels*



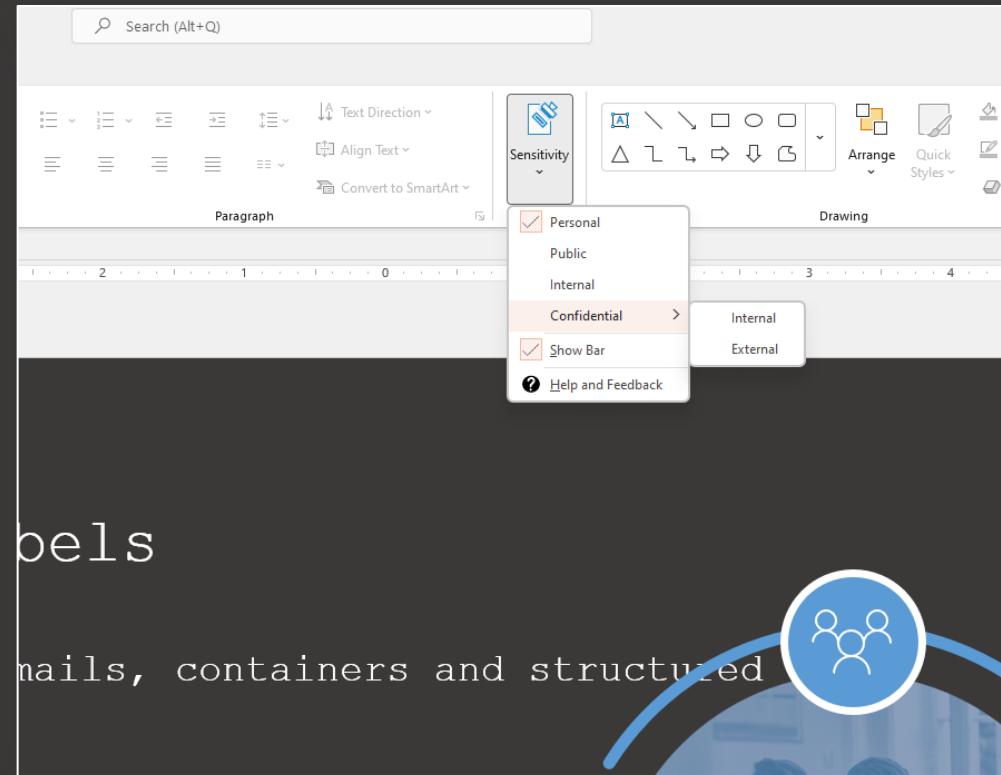
Classify - Sensitivity labels

- Items (documents and e-mails)
- Containers
- Structured data

Different scopes – different functionality – unified across scopes

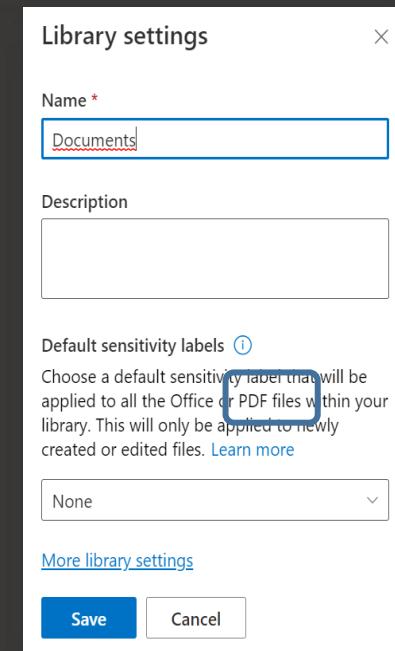
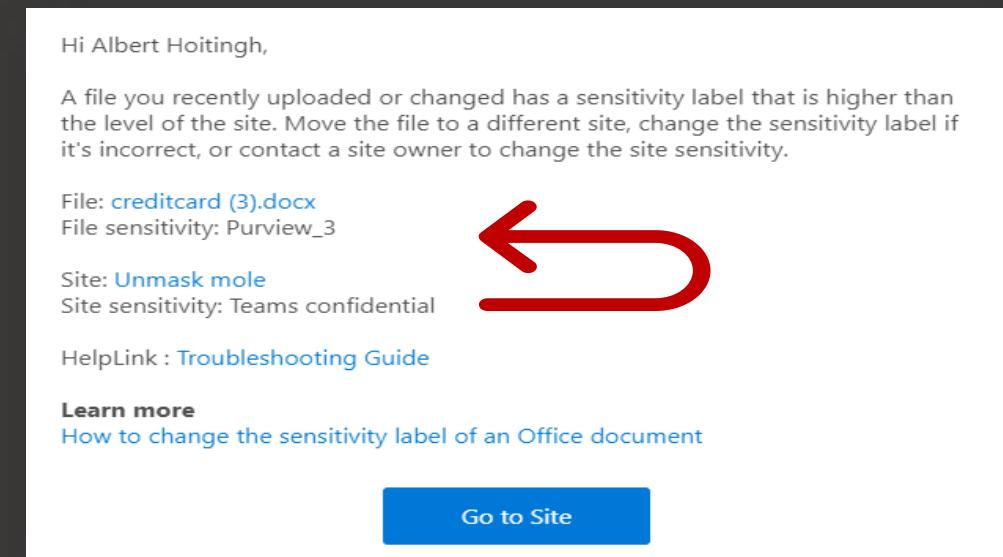
Items

- Label applied to document/e-mail
- Label added as metadata and stays with document
- Can be configured to:
 - Apply visual markings
 - Encrypt the document
 - Allow offline access
 - Work within DLP policies
- Works with a hierarchy, parents and sublabels
- Does not provide retention!



Containers

- Groups and sites
- Microsoft Teams | Microsoft 365 Groups
| SharePoint Online sites
- Privacy | External user access |
- Sharing settings for SharePoint Online
- Azure AD Conditional Access rules
- Default label per library (preview)
- Specific policy option



Schematized data assets

Structured data

- Uses Microsoft Purview Data Governance
- SQL | Azure SQL | Azure Synapse |
Azure Cosmos | Amazon AWS S3
- PowerBI – apply label on download

The screenshot shows a search interface for 'credit card' in Microsoft Purview. The left sidebar includes filters for Asset type (Azure Blob Storage) and Classification (Credit Card Number, EU Debit Card Number). The main pane lists 12 results, with one item highlighted: 'Credit Card-Sensitivity.docx' (Azure Blob Path: https://desktopsdiag755.blob.core.windows.net/purview2/Credit Card-Sensitivity.docx). This item has a 'Label' field containing 'Purview_3'.

The screenshot shows a Power BI workspace titled 'My workspace'. The left sidebar lists Home, Favorites, Recent, Create, Datasets, Apps, Shared with me, Workspaces, and My workspace. The main pane displays a table of data assets:

Name	Type	Owner	Refreshed	Next refresh	Endorsement	Sensitivity
creditcards	Dataset	Albert Hoitingh	1/12/21, 8:19:11 AM	N/A	—	—
creditcards.xlsx	Dashboard	Albert Hoitingh	—	—	—	—
Retail Analysis Sample	Dashboard	Albert Hoitingh	—	—	—	Confidential\IBAN ⓘ
Retail Analysis Sample	Report	Albert Hoitingh	7/2/20, 5:13:37 PM	—	—	Highly Confidential\Fin... ⓘ
Retail Analysis Sample	Dataset	Albert Hoitingh	7/2/20, 5:13:37 PM	N/A	—	Highly Confidential\Fin... ⓘ

Short demonstration – labels in Teams
and Office Online

Encryption



Encryption and labels

- Uses Azure Rights Management and Azure AD accounts
- Microsoft Managed Keys | Bring Your Own Key | Double Key
- RMS Connector for Exchange on-premises

Microsoft Managed (Azure) key details

- Content protection: Symmetric AES 128/256 bit
- Key protection: Asymmetric RSA 2048 bit
- Certificate signing: SHA-256
- Protected document = Encrypted body + signed & encrypted policy

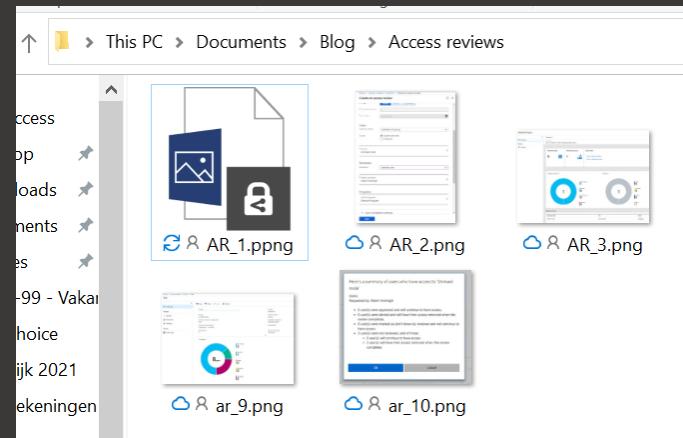
Beware!

- Licensing requirements
- Limitations (Double Key: only Office apps)
- Azure AD accounts (and working with guests)
- Co-authoring and auto-save for Office



File-types are important

- Some types only support labeling (no encryption)
- Opening encrypted files:
- Office and PDF files: native clients and Edge
- Other supported files: AIP Viewer client
- Watch out for the file extension



File types supported for classification only

The following file types can be classified even when they are not protected.

- Adobe Portable Document Format: .pdf
- Microsoft Project: .mpp, .mpt
- Microsoft Publisher: .pub
- Microsoft XPS: .xps .oxps
- Images: jpg, jpe, jpeg, jif, jfif, jfi, png, .tif, .tiff
- Autodesk Design Review 2013: .dwfx
- Adobe Photoshop: .psd
- Digital Negative: .dng
- Microsoft Office: The following file types, including 97-2003 file formats and Office Open XML formats for Word, Excel, and PowerPoint:

.doc	.potx	.vsd	.vstx
.docm	.pps	.vsdm	.xls
.docx	.ppsm	.vsdx	.xlsm
.dot	.ppsx	.vss	.xlt
.dotm	.ppt	.vssm	.xlsm
.dotx	.pptm	.vtm	.xlv

Co-authoring and auto-save

- Not possible in Office apps when encryption is enabled
- Can be enabled using GUI or PowerShell
- Changes labeling metadata

Settings > Co-authoring for files with sensitivity labels

Co-authoring for files with sensitivity labels

This setting allows users in your organization to co-author in Office desktop documents that are encrypted by using sensitivity labels. To support this new capability, all users must have the latest Microsoft 365 Apps for enterprise and label metadata must be upgraded for all labeled documents that aren't encrypted. [Learn more about this one-time setting](#)

Prerequisites

- Sensitivity labels must be enabled for files in OneDrive and SharePoint. If this isn't already done, we'll enable this for you when you turn on co-authoring.
- Minimum versions of apps to support the new labeling metadata.
- Latest Microsoft 365 Apps for enterprise.
- Any labeling apps or solutions you've deployed use the minimum supported version of the MIP SDK.
- Any scripts or tools you're using that read from or write to the labeling metadata for documents are updated to use the new metadata format and location.

[Learn more about these prerequisites](#)

What to expect after turning this on

- When existing labeled and unencrypted documents are opened and saved, the sensitivity label information that's currently stored as a custom property is copied and saved to a new format in a new metadata location.

Turn on co-authoring for files with sensitivity labels

When this was turned on, we also enabled sensitivity labels for files in OneDrive and SharePoint if it wasn't already enabled. [Learn more](#)

⚠️ You can't turn this setting off because this action can result in losing some labeling information. If you accept this risk and still want to turn it off, contact Microsoft Support. [Learn more](#)

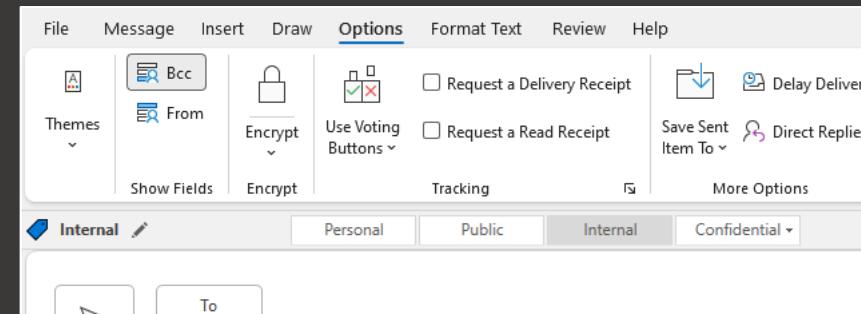
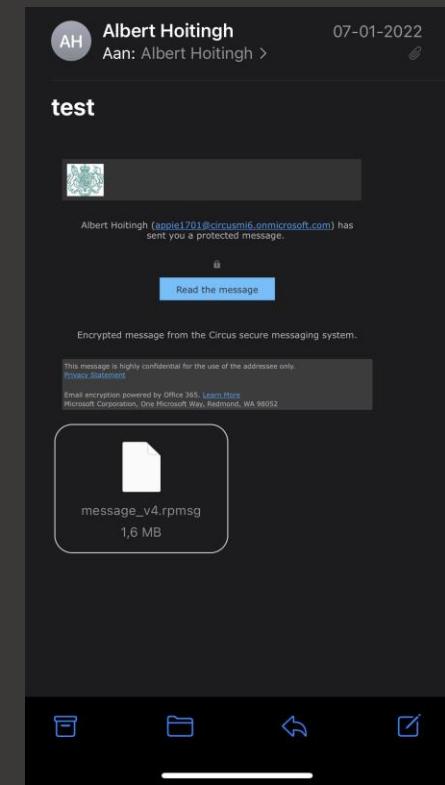
[Apply](#) [Cancel](#)

Labeling, encryption and e-mails

- E-mail can inherit label from attachment
- Office attachment inherit settings from e-mail
- Specific options:
 - Do not forward (or print, save)
 - Encrypt only
- Uses Office 365 Message Encryption

Beware!

- Encrypt only is only available in integrated client
- Do not forward and encrypt can also be set without labels (**Options | Encrypt**)





Office



Xbox



Solitaire



Spotify



Netflix



To Do



News



PicsArt



Twitter



Messenger



Photoshop
Elements



Calculator

Recommended



Get Started
Welcome to Windows

Different clients



ADeltaX



ENG
IT

6:20 PM
Tuesday
6/15/2021



Unified Labeling clients

Client V1.x

Classic client

Deprecated

Client V2.x

Unified Labeling client

Maintenance mode in 2022

Integrated client

Build into Office Apps

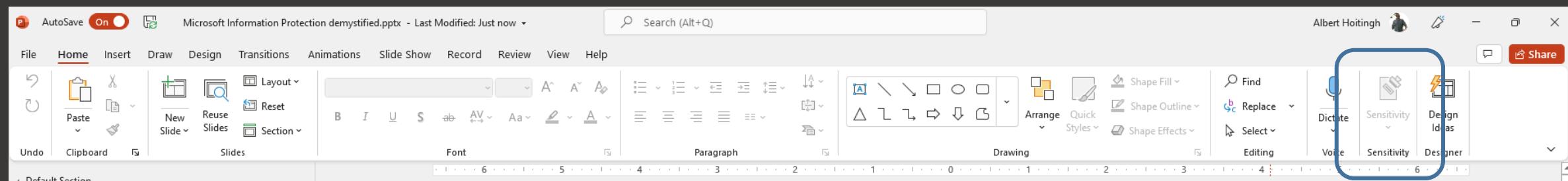
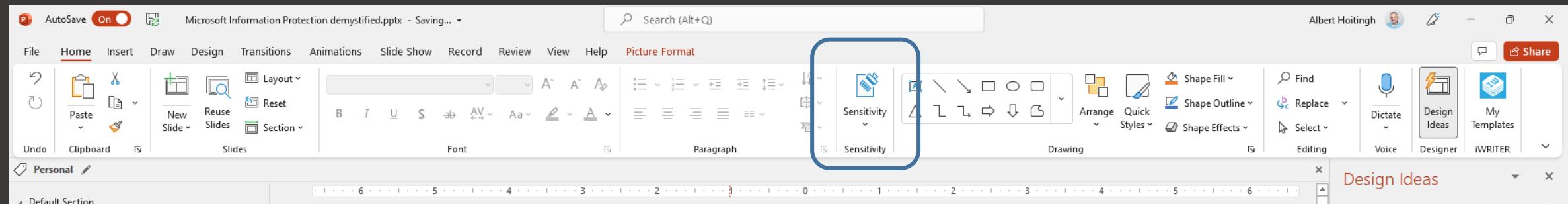
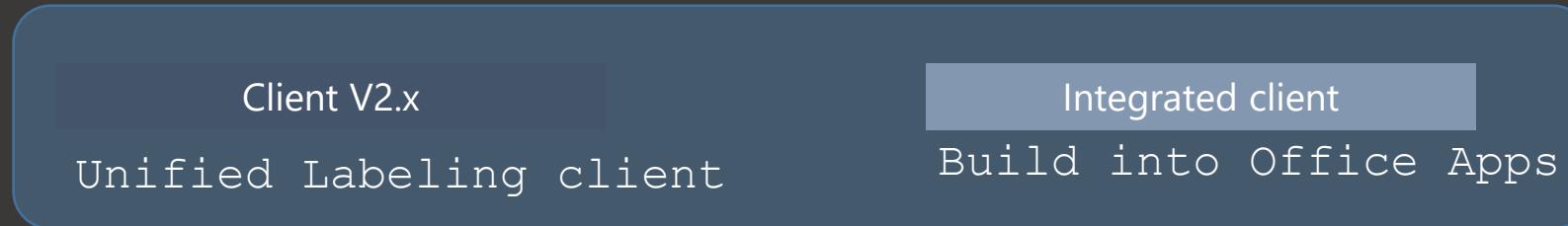
Other clients

Mobile clients

Adobe Acrobat

Autocad

Unified Labeling clients



Beware of the integrated client...

Client V2.x

Unified Labeling client

Integrated client

Build into Office Apps

It does not support

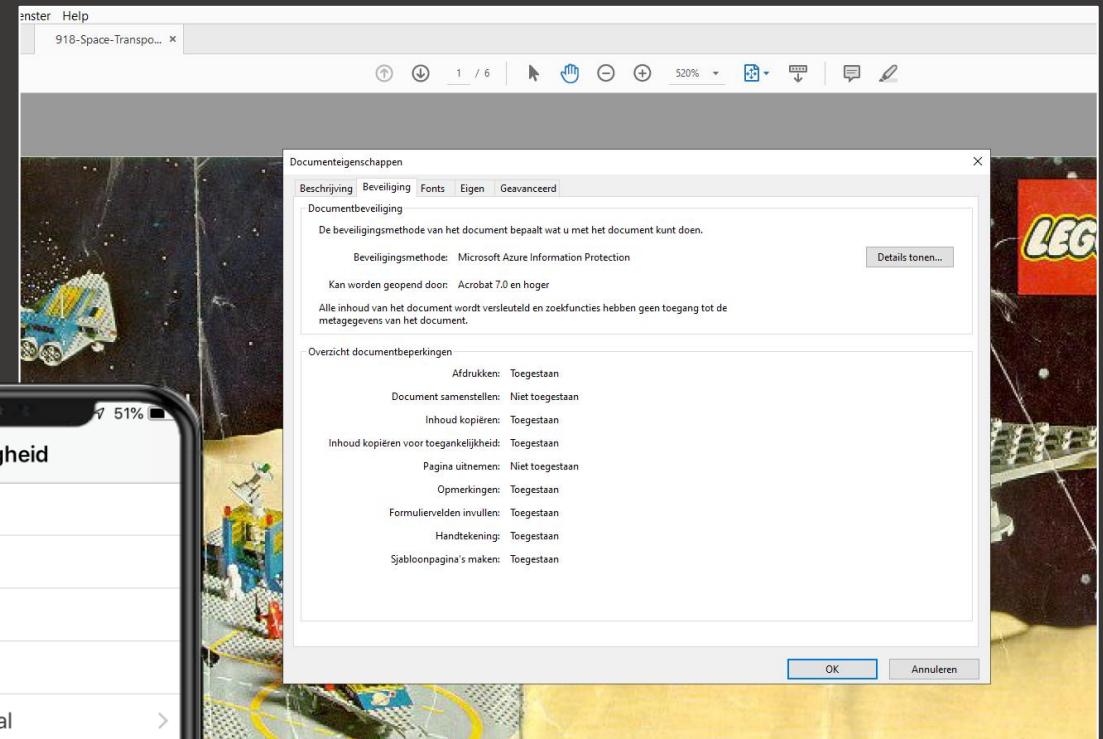
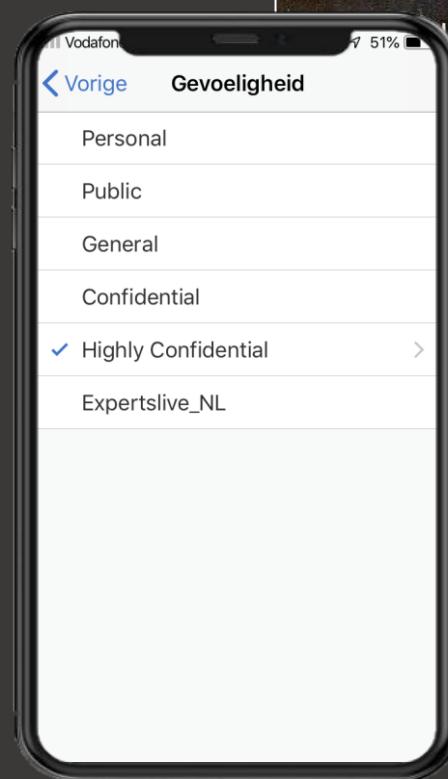
- Label inheritance from e-mail
- On-premises scanner
- Custom permissions independently from label
- Bar in Office
- File explorer integration
- PPDF support
- Powershell labeling cmdlets
- HYOK/Double Key encryption
- Usage logging event viewer
- Do not forward button Outlook
- Document tracking/revoking
- Protection only mode

Unified Labeling clients

Other clients

Office Online (no UDP)
Mobile clients
Adobe Acrobat
Autocad

The screenshot shows the Microsoft Excel ribbon with the Share tab selected. The Share tab includes options for AutoSum, Clear, Sort & Filter, Find & Select, Analyze Data, and Sensitivity. A dropdown menu under the Share tab shows sharing settings for 'All Employees' and 'Confidential'.



*Automatic
detection and
classification*



Auto-classification (E5)



Office apps

**Uses a tooltip within Office apps
(Word, Excel, Outlook and
PowerPoint)**

Data at rest

**Automatic classification for
SharePoint Online, OneDrive for
Business and Exchange Online**

Non-Microsoft Cloud

**Automatic classification using file-
policies in Microsoft Defender for
Cloud Apps**

On-premises

**Automatic classification for on-
premises fileshares, SharePoint
Server en NAS storage**

Auto-classification

Office apps

Either recommend the label or automatically apply it

Works in Office apps and Office Online – beware the differences

Outlook requires an advanced policy setting for matching highest classification

Some differences between Windows, Mac and mobile

Uses sensitive information types and/or trainable classifiers

Auto-labeling for files and emails



Since encryption is turned on, a large amount of content might be automatically encrypted when this label is applied. Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. [Learn more](#)

_DETECT content that matches these conditions

+ Add condition ▾

Recommended labeling and displaying a message to users is supported only for Office apps. This label will be automatically applied to files in Microsoft Purview Data Map, but no message will be displayed.

When content matches these conditions [i](#)

Automatically apply the label

Automatic and recommended labeling works differently for items in Office 365 vs. files stored on Windows devices. [Learn more](#)

Auto-classification

Data at rest

SharePoint Online/OneDrive: Word, Excel, PowerPoint
Exchange Online: PDF attachments

Limitations

List attachments are not supported
Open files cannot be auto-labeled
Maximum of 25,000 files per day
Maximum of 100 policies per tenant, each max 100 sites
Parent labels cannot be used
Existing metadata are not changed
Uses sensitive information types

Choose locations where you want to apply the label

Exchange will automatically apply the label to unlabeled emails, regardless of which device or platform is used to send and receive the email. OneDrive and SharePoint will automatically apply the label to unlabeled Office documents.

Tip Edit the "Auto-labeling" settings for this label to ensure that it's automatically applied to documents when they're saved and emails when they're sent.			
Status	Location	Included	Excluded
<input type="checkbox"/> Off	Exchange		
<input checked="" type="checkbox"/> On	SharePoint sites	1 site Choose sites	None Choose sites
<input type="checkbox"/> Off	OneDrive accounts		

Auto-classification

Non-Microsoft Cloud

Defender for Cloud Apps

Requires integration with MIP

Works with Word, Excel, PowerPoint and PDF documents

Works for Box and Google Workspace - more cloud apps will be supported in future

Microsoft Purview Data Governance

Different cloud and other data sources

For example: Amazon AWS S3

Using sensitivity labels

The screenshot shows the Microsoft Defender for Cloud Apps interface with the title 'Microsoft Defender for Cloud Apps' at the top. On the left, there is a sidebar with icons for 'Cloud', 'Box', and 'Governance actions'. The main area is titled 'Governance actions' and lists various options: Send policy-match digest to file owner, Notify specific users, Remove external users, Remove direct shared link, Set an expiration date on a shared link, Change shared link access level, Put in user quarantine, Put in admin quarantine, Trash, Notify last file editor, Remove a collaborator, and Apply sensitivity label. The 'Apply sensitivity label' option is checked, and a dropdown menu below it shows 'Confidential-IT related information'.

Auto-classification

On-premises

Automatic classification for on-premises fileshares,
SharePoint Server en NAS storage

Uses the Azure Information Protection scanner

Requires the Unified Labeling client

Also used for on-premises DLP

The screenshot shows the 'Repository' settings page in the Azure Information Protection portal. The path '\azureipscanner\scanner_docs*.dwg' is selected in the 'Path' input field. The 'Sensitivity labeling policy' section is expanded, showing the 'Content scan job default' option selected for both 'Enforce' and 'Label files based on content'. The 'Default label' section also shows 'Content scan job default' selected. The 'Relabel files' section has 'Content scan job default' selected.

Dashboard > Azure Information Protection > Omaha >

Repositories ...

+ Add ⬇ Export ⬈ Import 🗑 Delete 🗑 Delete all

Search to filter items...

Path	Default label
\azureipscanner\scanner_docs*.dwg	

Repository

Save Discard Delete

Path
\azureipscanner\scanner_docs*.dwg

Sensitivity labeling policy

Enforce ⓘ
Off On Content scan job default

Label files based on content ⓘ
Off On Content scan job default

Default label ⓘ
None Policy default Custom Content scan job default

Relabel files ⓘ
Off On Content scan job default

Short demonstration
Configuring labels and auto-labeling

*Things to
consider*

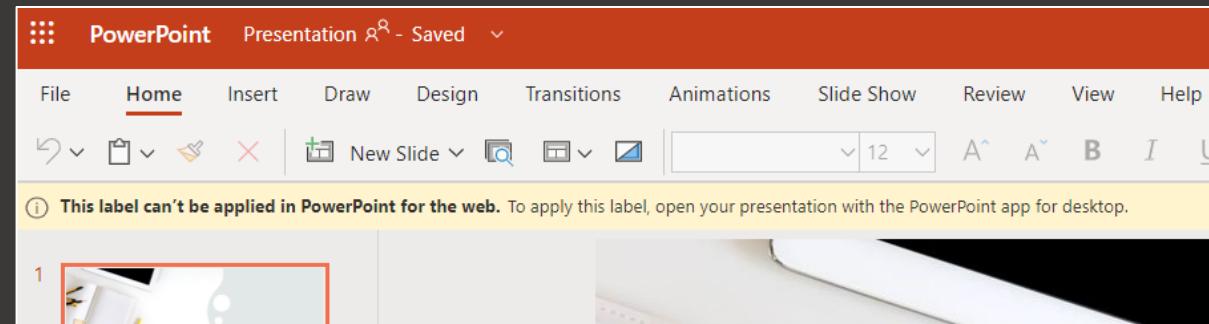


Tips, tricks and some things to think about

- Sharing an encrypted file | working with guests
- Label/encrypt using DLP rules
- Decrypt file in SPO: **Unlock-SensitivityLabelEncryptedFile**
- Metadata change, MSIP_ cannot be used anymore
- Container based - don't affect documents & require AAD CA policies
- Difference in clients
- Custom configuration for UL client

Tips, tricks and some things to think about

- Visual markings per app and restrictions (see screenshot)
- Use Defender for Cloud Apps to block downloads for labeled content or to apply label when downloading a document
- Super User role
- Encrypted PDF's (Adobe Acrobat | Microsoft Edge)



Ignite 2022

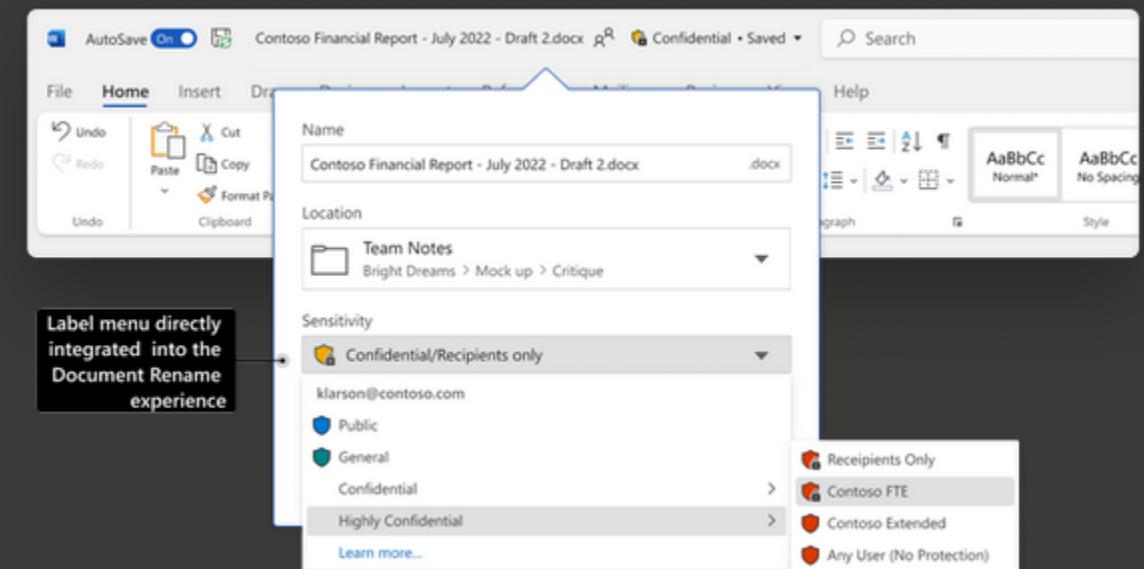
- Teams Premium (secure meetings)
- Adobe Acrobat integration
- Label protection Office to PDF
- AIP Scanner admin-portal
- Enhanced label menu integrated client
- UDP for Office files in SharePoint Online, Teams, OneDrive

The image shows three separate presentation cards from the Microsoft Ignite 2022 conference, all related to Microsoft Purview Data Loss Prevention (DLP). They are arranged in a staggered, overlapping manner against a dark background.

- A simple approach to data protection**
Coming Up | Thursday, October 13 | 9:00 PM - 9:30 PM | Central European Summer Time | Digital
Presentation languages: English, French, German, Japanese, Mandarin, Spanish
Security and compliance teams know that data governance, risk management, and an effective compliance posture are important when maintaining a security strategy. In today's economic climate, maximizing investments, streamlining...
[see more](#)
- Take a unified and comprehensive approach to prevent data exfiltration with Microsoft Purview Data Loss Prevention**
On Demand | Digital
Presentation language: English
Is your data protection program dependent on you managing on-prem infrastructure, and stitching together disparate tools? There is a better way with Microsoft Purview Data Loss Prevention! Microsoft Purview Data Loss Prevention is cloud-...
[see more](#)
- Get started with discovering, protecting, and governing sensitive data**
On Demand | Digital
Presentation language: English
Microsoft Purview Information Protection and Data Lifecycle Management help organizations find, protect, and govern sensitive data in emails, chats, files, in cloud apps or on-premises file shares, on desktop/mobile devices, and more....
[see more](#)

Ignite 2022

- Teams Premium (secure meetings)
- Adobe Acrobat integration
- Label protection Office to PDF
- AIP Scanner admin-portal
- Enhanced label menu integrated client
- UDP for Office files in SharePoint Online, Teams, OneDrive



COMMUNITY

<https://collabdays.be>

Please rate this session and have a
chance to win an awesome prize



#CollabDaysBE

Thank you!



@Alberthoitingh



<https://linkedin.com/in/appieh>



<https://alberthoitingh.com>

```
..  
bin -> usr/bin  
1 boot  
50 dev  
.32 etc  
:52 home  
015 lib -> usr/lib  
2015 lib64 -> usr/lib  
10:01 lost+found  
22:45 mnt  
2015 opt  
p 15:52 private -> /home/encryp  
ep 08:15 proc  
Aug 15:37 root  
Sep 15:50 run  
Sep 2015 sbin -> usr/bin  
Sep 2015 srv  
. Sep 15:51 sys  
. Sep 15:45 usr  
22. Aug 15:39 var  
23. Jul 10:25 ..  
21. Sep 15:53 ..  
21. Sep 15:53 ..
```