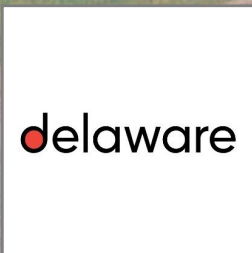


# Office 365 Unified Labels

## Designing a secure collaboration solution

Bram de Jager  
Lead Architect, delaware Netherlands | MVP | MCM



# Agenda

Information Protection basics

Demo

What's next

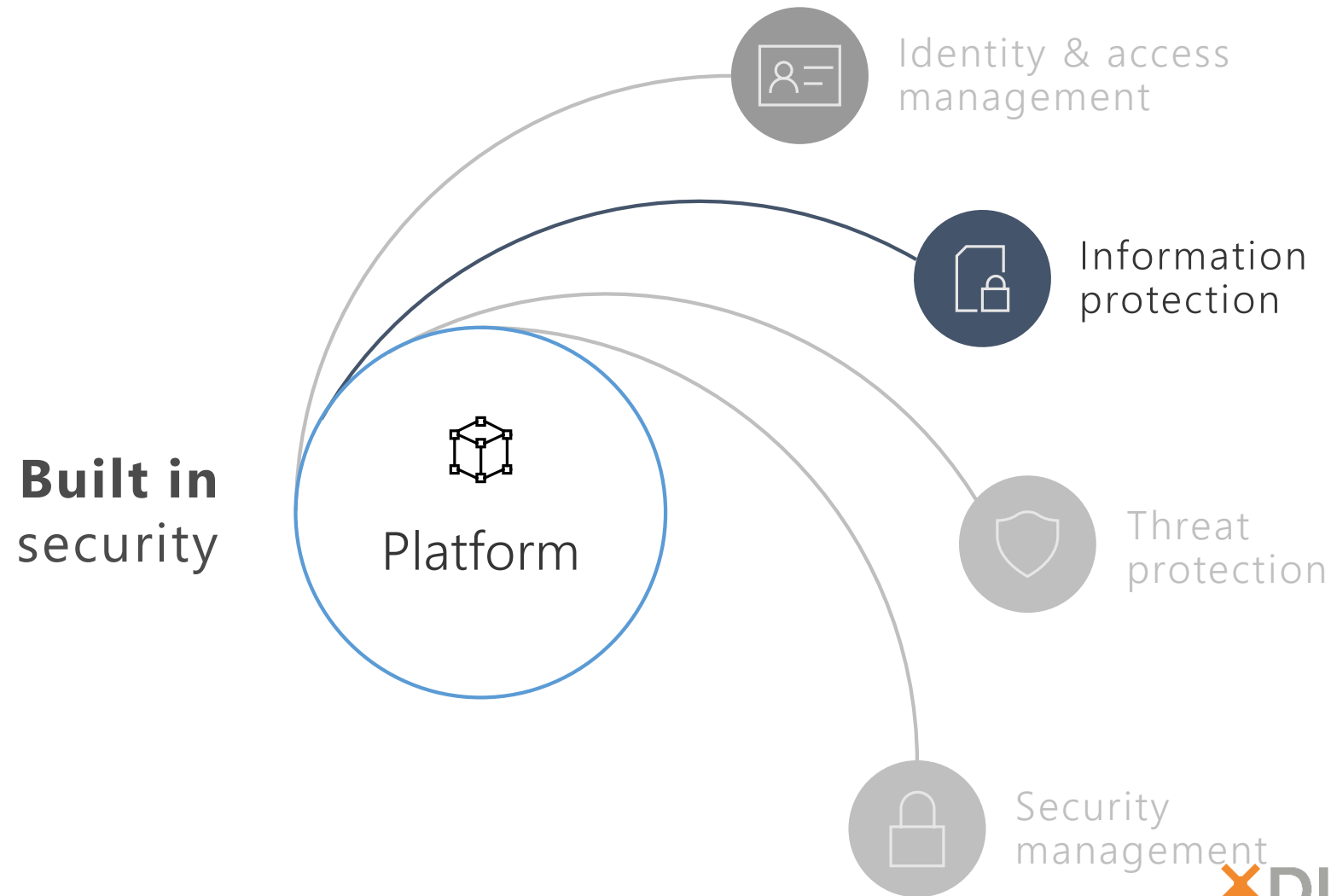
Wrap-up



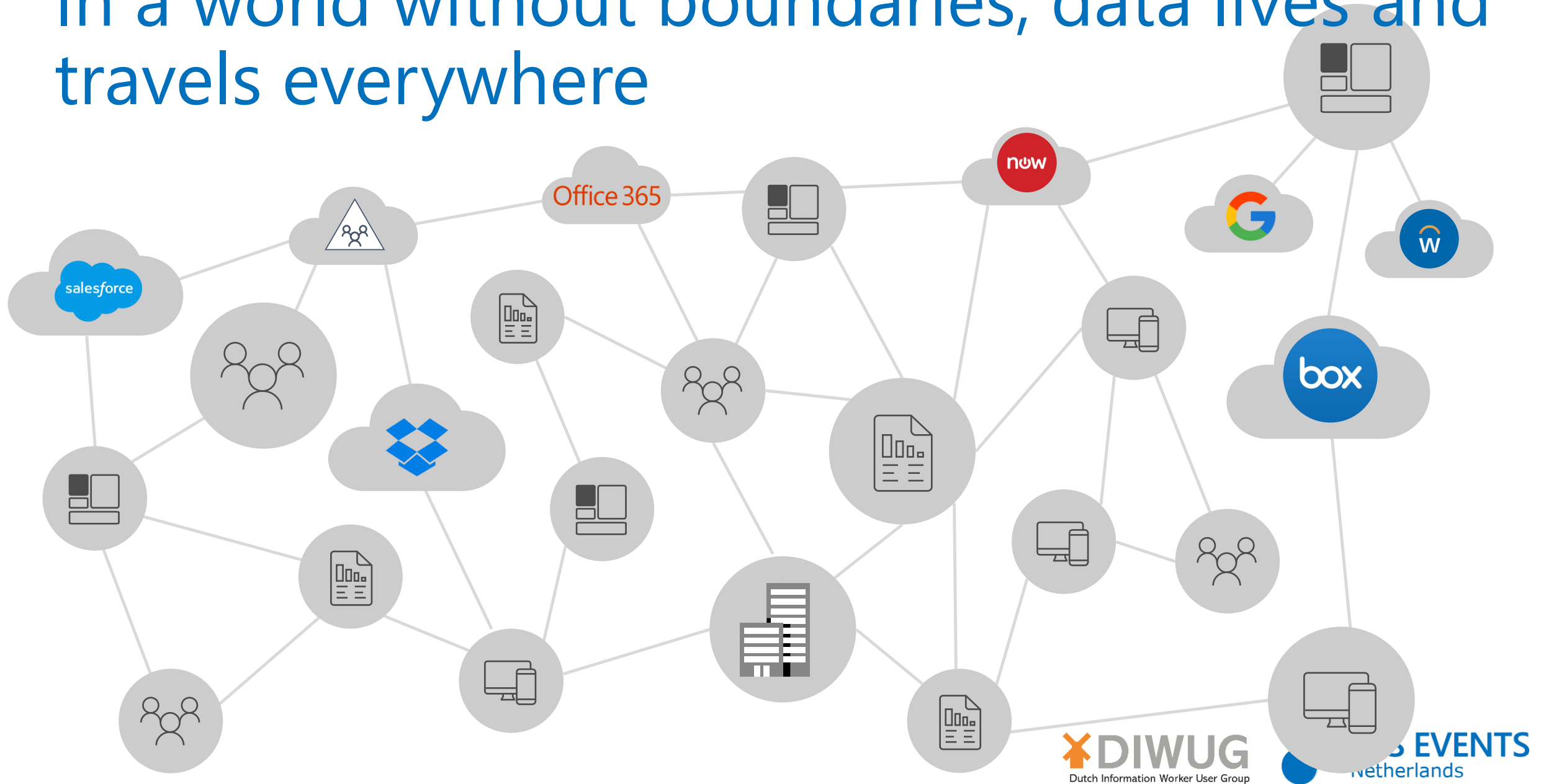
# Information Protection basics

The Microsoft Security Platform with Information Protection as key element

# Microsoft Security Platform



# In a world without boundaries, data lives and travels everywhere



# Do you have a strategy to protect your most valuable data?

Do you know where your sensitive data resides?

Are you using multiple solutions to discover, classify, label, and protect sensitive data?

Do you have control of your data as it travels inside and outside of your organization?



# Sensitive data is at risk

**80 %** of employees use non-approved SaaS apps at work

**85 %** of enterprise organizations keep sensitive information in the cloud

**88 %** of organizations no longer have confidence to detect and prevent loss of sensitive data

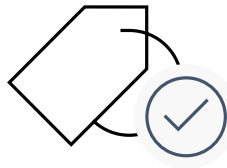
**58 %** Have accidentally sent sensitive information to the wrong person



# Microsoft Information Protection



Discover



Classify

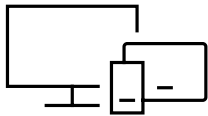


Protect

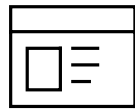


Monitor

Across



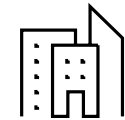
Devices



Apps



Cloud services



On-premises



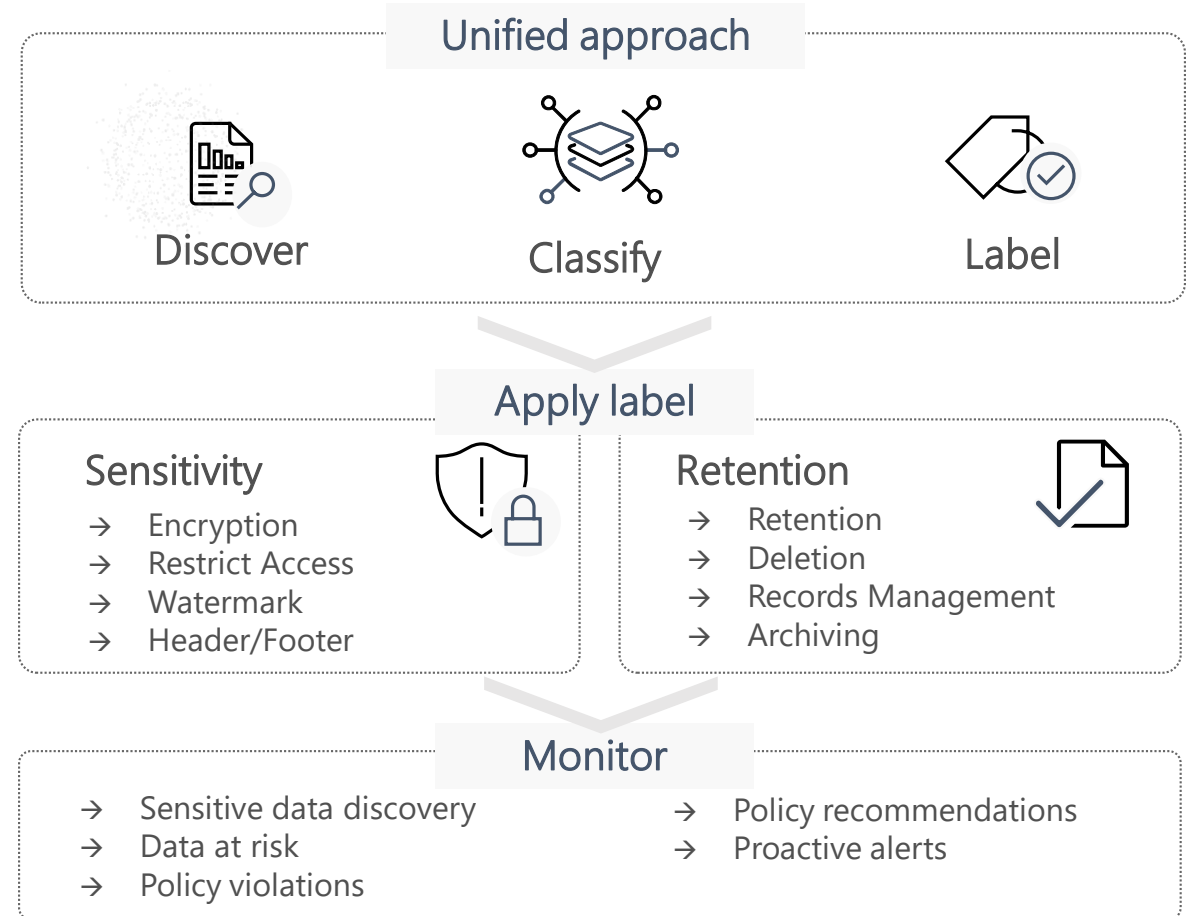
# Data protection & data governance go hand-in-hand

Unified approach to discover, classify & label

Automatically apply policy-based actions

Proactive monitoring to identify risks

Broad coverage across locations

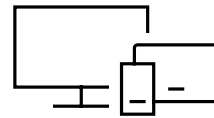


# Microsoft Information Protection

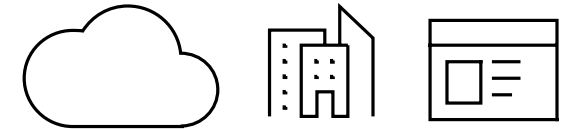
## The way it was



**Office 365  
Information Protection**



**Windows  
Information Protection**



**Azure  
Information Protection**

What

Preserve or remediate emails & documents

Protect files and documents

Classify & Protect  
emails & documents

Where

Office 365 Apps & Services

Windows Clients & Devices

Office Clients, 3<sup>rd</sup> party Apps  
& Services, On Premises

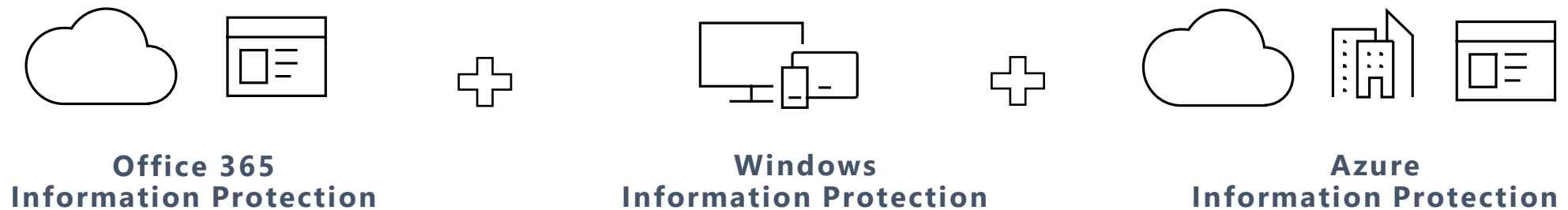
How

Office 365 Security Console

Intune Portal

AIP Portal

# Microsoft Information Protection Going forward



What Consistent content detection and classification to protect and preserve sensitive data

Where Office 365 apps & services, Windows clients & desktops, mobile, on premises + 3<sup>rd</sup> party apps and services

How Microsoft 365 Security and Compliance Center

# What is a sensitivity label?

**Tag** that is customizable,  
readable by other systems,  
and persistent.

It becomes the basis for applying and enforcing  
data protection policies.



In files and emails, the label is persisted  
as document metadata



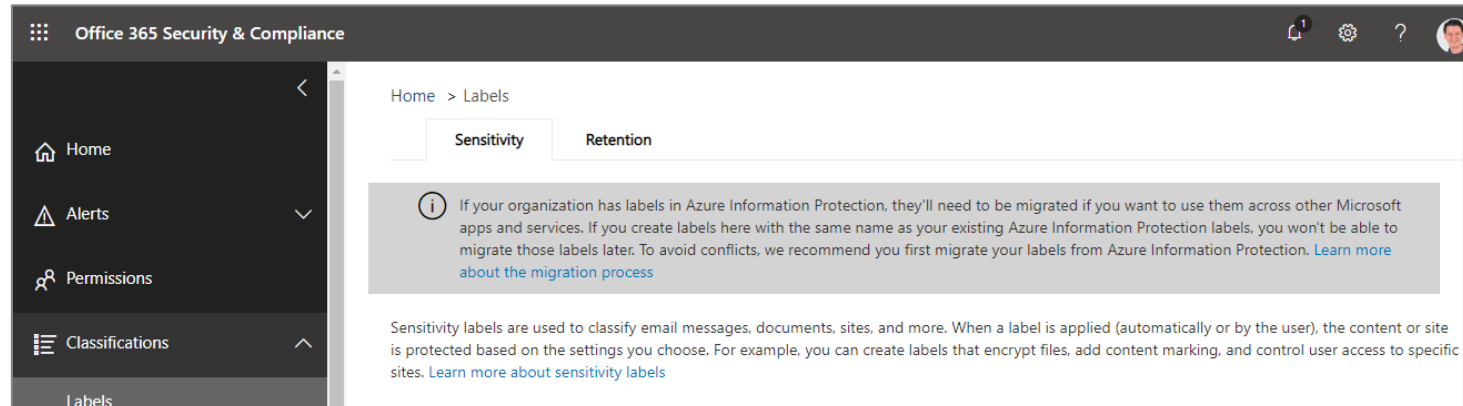
In SharePoint Online, the label is  
persisted as container metadata



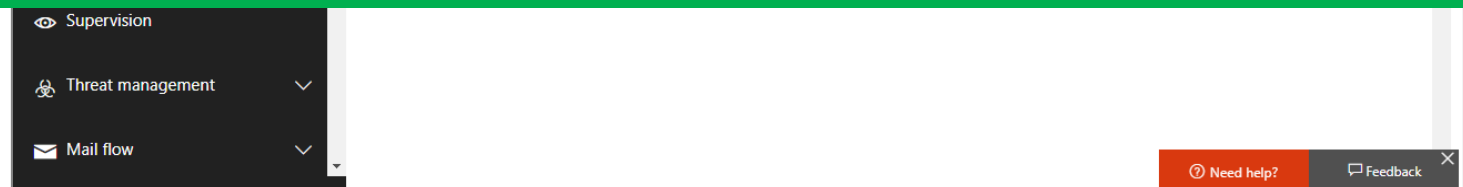
# Demo Information Protection

Azure Information Protection and Unified Labels in practice

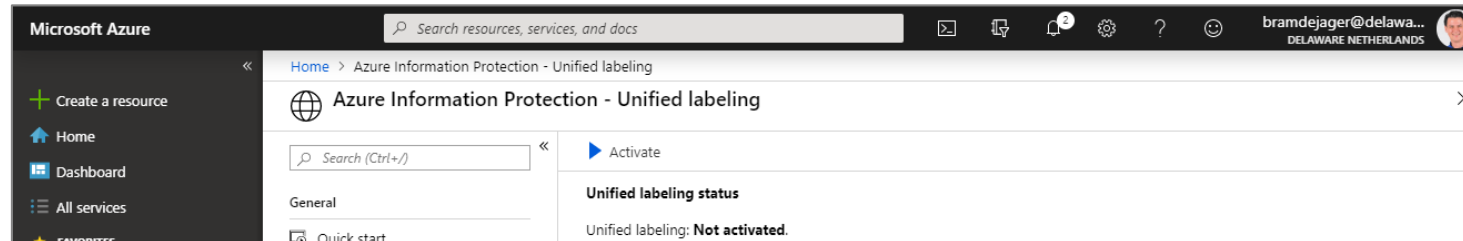
# Before you start, a note on migrate first!



**i** If your organization has labels in Azure Information Protection, they'll need to be migrated if you want to use them across other Microsoft apps and services. If you create labels here with the same name as your existing Azure Information Protection labels, you won't be able to migrate those labels later. To avoid conflicts, we recommend you first migrate your labels from Azure Information Protection. [Learn more about the migration process](#)



# Before you start, Unified Labeling not activated



▶ Activate

## Unified labeling status

Unified labeling: **Not activated.**

Unified labeling is not activated for this tenant. In this state, your Azure Information Protection labels can be used only by the Azure Information Protection client. To make your labels available in the [Office 365 Security & Compliance Center](#), the Microsoft 365 security center and the Microsoft compliance center, and to clients and services that support unified labeling, select **Activate**.

Before you activate unified labeling, check that in the named admin centers, you don't have labels that have the same name or display name as your labels in Azure Information Protection. If this is the case and you activate unified labeling, your Azure Information Protection labels will be automatically renamed so that migration can succeed. Then, to avoid confusion for your end users, you will have to change the display names of these migrated labels.

[Learn more](#) about the migration process.

**Note:** you cannot deactivate unified labeling for your tenant.

# Where the Unified Label feature is available today?

Platform	Application	Availability
Mac	Word, Excel, PowerPoint, Outlook	Version 16.21.0+
Android	Word, Excel, PowerPoint	Version 16.0.11231+
	Outlook	Coming in the first half of calendar year 2019
iOS	Word, Excel, PowerPoint	Version 2.21+
	Outlook	Coming in the first half of calendar year 2019
Windows	Word, Excel, PowerPoint, Outlook	Coming soon to the <a href="#">Office Insider program</a>
Web	Word, Excel, PowerPoint	To be announced
	Outlook Web Access	To be announced



# What's next?

Why would an organization want move to Unified Labels?

# Sensitivity Site and Group settings

The screenshot shows the Microsoft 365 compliance center interface. The left sidebar contains navigation options: Home, Alerts, Monitoring & reports, Classification, Labels (selected), Label policies, Sensitive info types, Label analytics, Classification assistant, Policies, Information barriers, Solutions, Data governance, and eDiscovery. The 'Labels' section is expanded, showing options: Edit a label to help users classify their content, Name, Encryption, Content marking, Endpoint data loss prevention, Site and group settings (highlighted), and Auto labeling. The main content area is titled 'Editing Site and group settings' and includes a close button (X). Below the title, there is a note: 'Select the settings you want to take effect when this label is applied to an Office 365 group or SharePoint site. Note that the settings aren't applied to files, so they don't impact downloaded copies of files. [Learn more about site and group protection](#)'. The 'Site and group settings' section has a toggle switch set to 'On'. Below this, there are three settings: 'Privacy of Office 365 group-connected team sites' with a dropdown menu set to 'Private - only members can access the site'; 'External users access' with a checkbox 'Let Office 365 group owners add people outside the organization to the group' which is unchecked; and 'Unmanaged devices' with a text description and two radio button options: 'Allow full access from desktop apps, mobile apps, and the web' (selected) and 'Allow limited, web only access'. At the bottom of the settings panel are 'Save' and 'Cancel' buttons. The browser's address bar shows the URL: <https://protection.office.com/labels?viewid=sensitivity&flight=EnableM365ComplianceCenter>. The Windows taskbar at the bottom shows the search bar and various application icons. The system clock in the bottom right corner indicates 9:33 AM on 5/21/2019.

# During site creation or afterward change sensitivity

The screenshot shows the SharePoint Admin Center interface for 'Contoso Electronics'. The left sidebar contains navigation links: North America, Home, Sites (with sub-links for Active sites and Deleted sites), Policies, Sharing, Access control, Settings, Advanced (with sub-links for Geo locations and API management), Classic SharePoint admin center, OneDrive admin center, and Data migration. The main content area is titled 'Active sites' and displays a table of sites. A yellow arrow points to the 'Email' icon in the top toolbar. The table lists sites with columns for Site name, Sensitivity, Storage used (MiB), Primary admin, and Hub site association. The 'Sales compete collateral' site is selected, and a yellow arrow points to its 'Sensitivity' setting. A right-hand pane shows the configuration for the selected site, including Storage used (2.61%), Storage limit (2 GB), Primary admin (Emily Braun), Admins, External sharing, and Sensitivity (General). A 'Change' link is next to the Sensitivity setting.

Site name	Sensitivity	Storage used (MiB)	Primary admin	Hub site association
Big Wins	General	61	System Administrator	Sales
Leads	-	39	System Administrator	Sales
North American Sales	General	104	Group owners	Sales
Sales @Contoso Hub	General	23	Group owners	Sales (Hub site)
<b>Sales compete collateral</b>	General	53	Emily Braun	Sales
Sales Leadership Team	General	106	Group owners	Sales

**Sensitivity settings for 'Sales compete collateral':**

- Storage used: 2.61%
- Storage limit: 2 GB
- Primary admin: Emily Braun
- Admins: Add or remove admins
- External sharing: Files and folders on this site can be shared with anyone
- Sensitivity: General

# During site creation or afterward change sensitivity

The screenshot displays the Microsoft 365 Admin center interface. On the left is a navigation pane with options like North America, Home, Sites, Policies, Sharing, Access control, Settings, Advanced, OneDrive admin center, and Data migration. The main area shows the 'Active sites' list with columns for Site name, Hub site association, Template, and External sharing. The 'Product Patents 2018' site is selected. On the right, the 'Sensitivity' settings panel is open, showing five options: Top Secret, General, Contoso Energy SLT Only, Corporate SLT Only, and Confidential. The 'Confidential' option is currently selected.

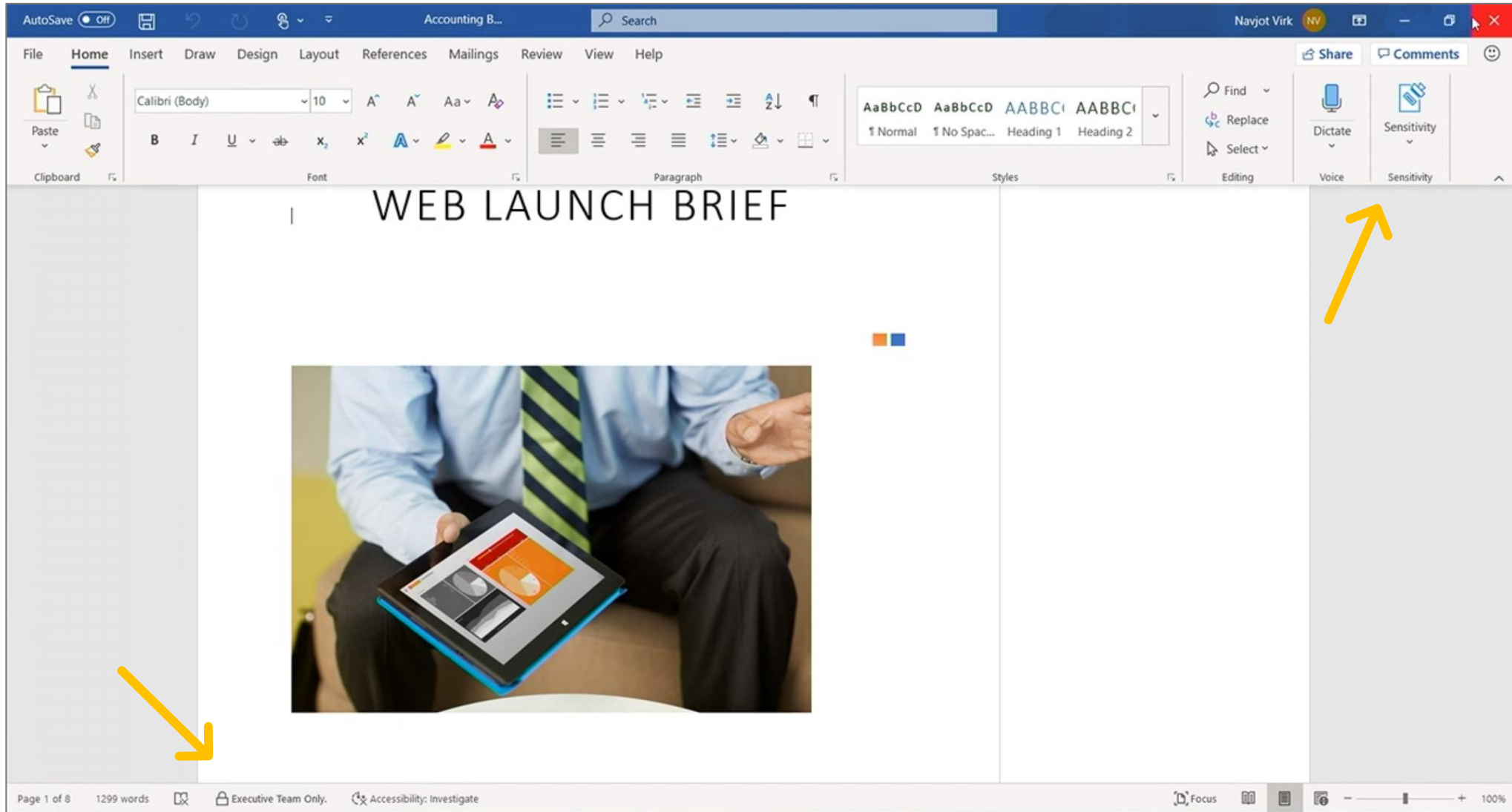
Site name	Hub site association	Template	External sharing
Leads	Sales @ Contoso Hub	Communication site	Off
Marketing	Marketing (Hub site)	Team site	On
Mergers	-	Team site	On
Mergers and Acquisitions	-	Team site	On
Mergers2019	-	Team site	On
News from HR	-	Communication site	On
North America Sales	Sales @ Contoso Hub	Team site	On
Northwest Sales	-	Team site	Off
Northwest Sales	-	Team site	Off
Petroleum Reporting Group	-	Team site	On
Pipelines	-	Communication site	On
Poll Team	-	Team site	Off
Poll Team	-	Team site	Off
Product Patents 2018	-	Team site	On
Project Spectrum	-	Communication site	On
Sales	-	Team site	On
Sales @ Contoso EUR	-	Communication site	Off
Sales @ Contoso Hub	Sales @ Contoso Hub (Hub site)	Communication site	On

**Sensitivity**

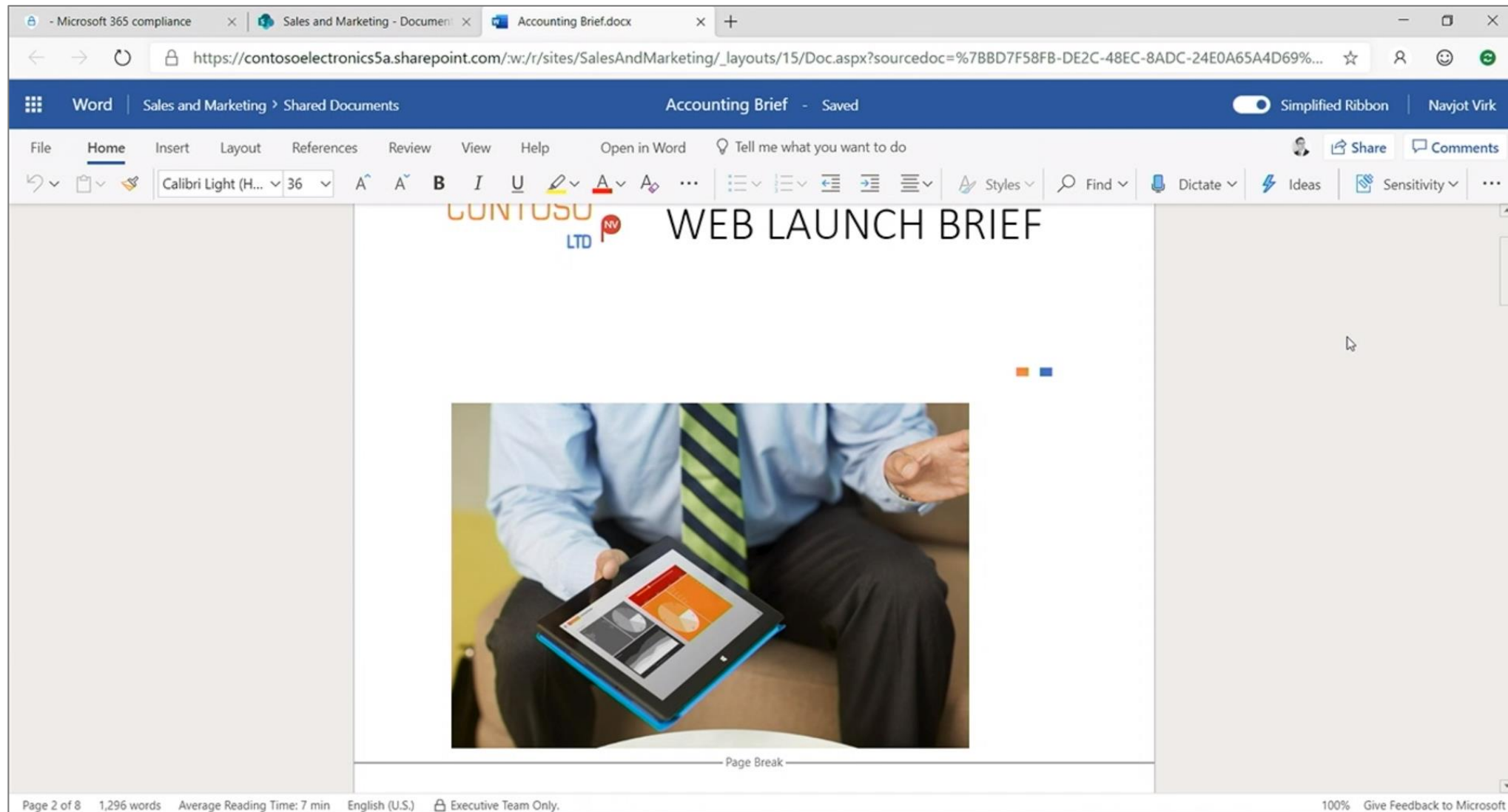
Select the sensitivity level you want to apply to this site. For more info about these labels, or to create a new one, go to the Security Center.

- ☐ **Top Secret**  
1. Apply to Highly confidential documents 2. Documents and emails will be watermarked and have must have headers and footers 3. Office documents will be encrypted 3. Sites will be marked as "no access" while accessing from "un-managed" devices 4. O365 Groups are marked as private
- ☐ **General**  
1. General label. Apply it for non-sensitive data. 2. Documents and emails will be watermarked and have must have headers and footers. 3. O365 Groups are marked as public.
- ☐ **Contoso Energy SLT Only**  
Apply this label to the documents that only SLT can access
- ☐ **Corporate SLT Only**  
Apply this label to the document that only corporate SLT can access
- ☒ **Confidential**  
Apply to confidential documents. Documents and emails will be watermarked and will have headers and footers. Sites will be in limited access mode (i.e. no print sync download) while

# Office client native support Sensitivity



# Native support for Office Online



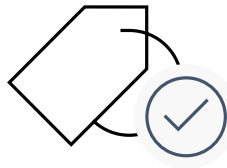
# Wrap-up

Where getting close to saying Goodbye!

# Microsoft Information Protection



Discover



Classify

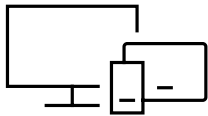


Protect

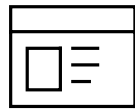


Monitor

Across



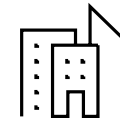
Devices



Apps



Cloud services



On-premises



# Comprehensive set of capabilities

**AZURE ADVANCED THREAT PROTECTION**  
Identify advanced data related attacks and insider threats

**MICROSOFT CLOUD APP SECURITY**  
Visibility into 15k+ cloud apps, data access & usage,  
potential abuse

**OFFICE 365 DATA LOSS PREVENTION**  
Prevent data loss across Exchange Online, SharePoint Online,  
OneDrive for Business

**OFFICE 365 MESSAGE ENCRYPTION**  
Send encrypted emails in Office 365 to anyone  
inside or outside of the company

**WINDOWS INFORMATION PROTECTION**  
Separate personal vs. work data on Windows 10 devices,  
prevent work data from traveling to non-work locations

**OFFICE 365 ADVANCED DATA GOVERNANCE**  
Apply retention and deletion policies to sensitive and  
important data in Office 365

## MICROSOFT INFORMATION PROTECTION

Discover | Classify | Protect | Monitor

### CONDITIONAL ACCESS

Control access to files based on policy, such as identity, machine  
configuration, geo location

### OFFICE APPS

Protect sensitive information while working in Excel, Word,  
PowerPoint, Outlook

### SHAREPOINT & GROUPS

Protect files in libraries and lists

### AZURE SECURITY CENTER INFORMATION PROTECTION

Classify & label sensitive structured data in Azure SQL, SQL  
Server and other Azure repositories

### SDK FOR PARTNER ECOSYSTEM & ISVs

Enable ISVs to consume labels, apply protection

### ADOBE PDFs

Natively view labeled and protected PDFs on Adobe Acrobat  
Reader

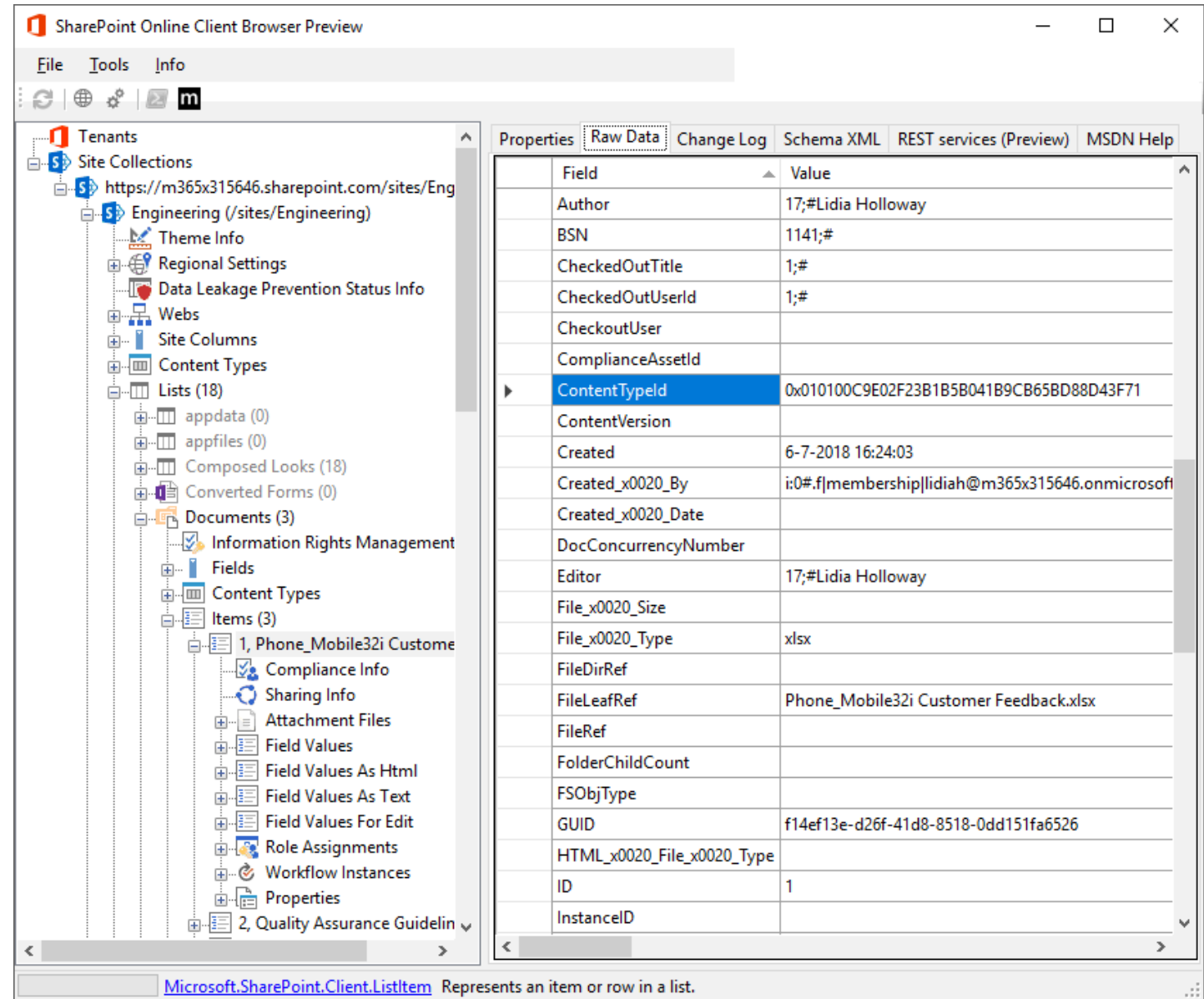
# Private preview Security and Compliance program

Want an early start with these new and upcoming security and compliance capabilities?

Nominate your business for our private previews at <https://aka.ms/spc19SecurityPreviews>.

# SharePoint Client Browser

- Must have SharePoint community tool!
- Provides insights into your SharePoint site or tenant
- Uses the CSOM to connect to SharePoint 2010/2013/2016/2019 and SharePoint Online
- <https://github.com/bramdejaer/spcb>





delaware



**Microsoft**  
**CERTIFIED**  
*Solutions Master*

# Thanks for attending



[bram.dejager@delaware.pro](mailto:bram.dejager@delaware.pro)



[@bramdejager](https://twitter.com/bramdejager)



[bramdejager.wordpress.com](http://bramdejager.wordpress.com)

**DIWUG**  
Dutch Information Worker User Group

**SPS EVENTS**  
Netherlands