

A Hitchhikers Guide to Microsoft Information Protection



Peter Schmidt

**aMS Berlin 2022
19. Mai**



Thanks to our SPONSORS

Vielen Dank an unsere Partner!



M365 Kaffeepause
Learning in the flow of work.

logitech®

MARTELL

**DIAMOND
sponsors**

**PLATINUM
sponsor**

Organizing sponsor

Granikos



**Organisatorischer
Partner**

- **Peter Schmidt**
- Cloud Architect @ NeoConsulting
- MVP: Office Apps & Services
- MCM/MCSM: Exchange
- MCT
- Twitter: @petsch
- Blog: www.msdigest.net



Agenda

✓ Introduction to MIP

🏷 Labels

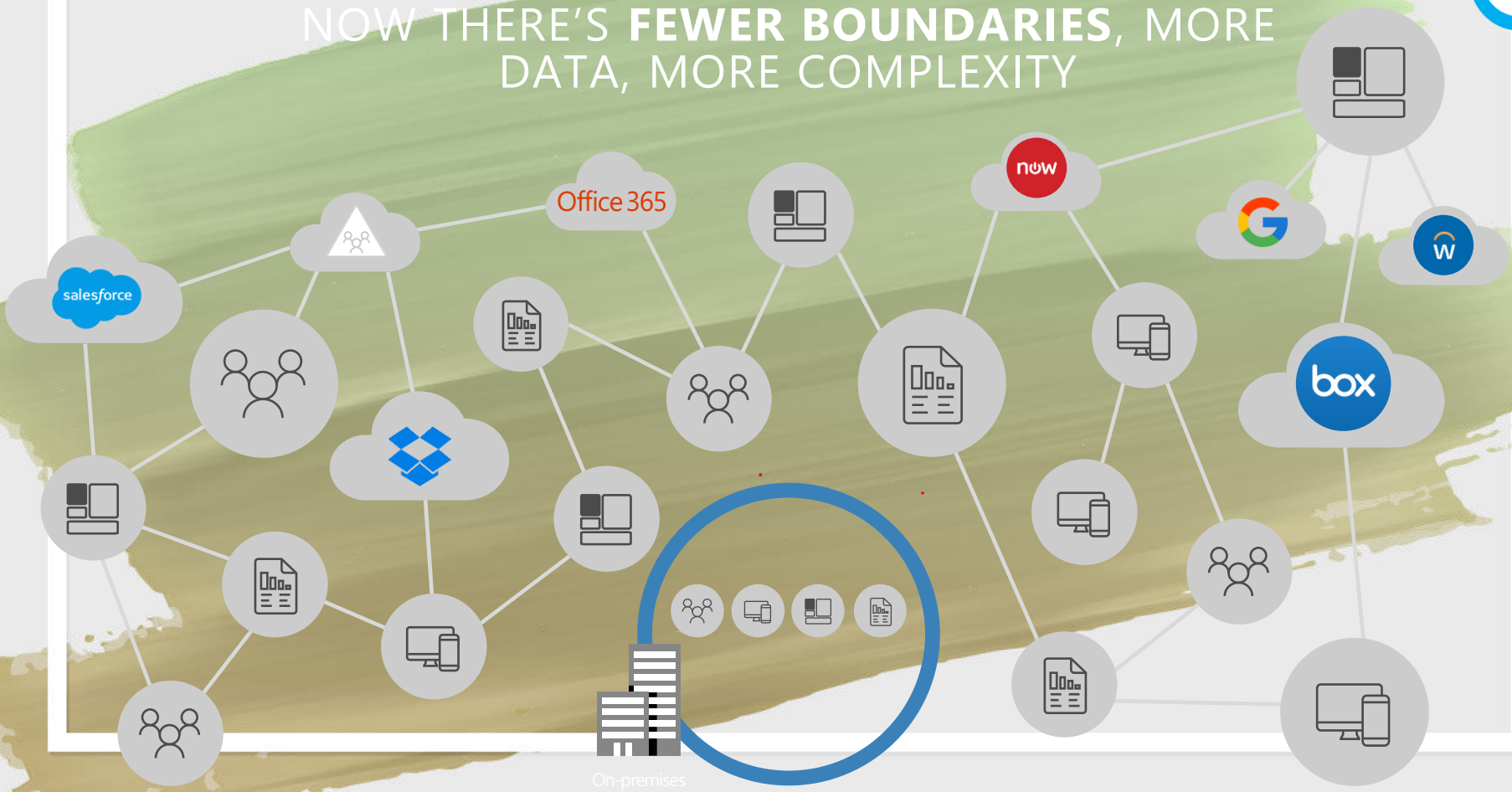
🗄 Data Classification

▶ Demo

🤝 Licensing

📄 Wrap-up

NOW THERE'S **FEWER BOUNDARIES**, MORE DATA, MORE COMPLEXITY



On-premises

Data Protection Scenarios



Sensitive Information
left on Commuter
Train



Sensitive information
Shared with wrong
recipient

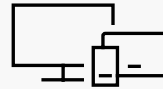


IP Information gets
stolen

Microsoft Information Protection – where are we coming from



**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, 3rd party Apps
& Services, On Premises

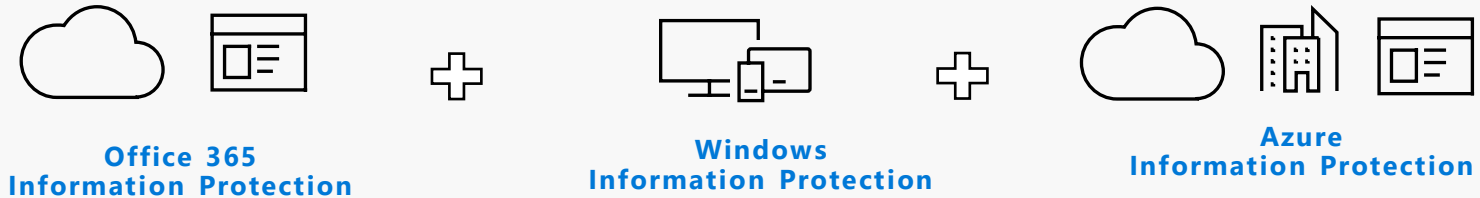
How

Office 365 Security Console

Intune Portal

AIP Portal

Microsoft Information Protection



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

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

How Microsoft 365 Purview (former Compliance) Portal

Microsoft Information Protection

Protect your sensitive data – wherever it lives or travels



Discover



Classify



Protect



Monitor

Across



Devices



Apps



Cloud services



On-premises

Comprehensive set of capabilities

AZURE INFORMATION PROTECTION

Classify, label & protect files – beyond Office 365, including on-premises & hybrid

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 and protect PDFs on Adobe Acrobat Reader



Type of Labels

Azure Information Protection Labels

Sensitivity Labels


Retention Labels


Unified Labels


Sensitivity Labels

- The successor of Azure Information Protection
- Classify and help protect your sensitive content
- Be careful with the encryption option
- Multilingual and colours are configurable through PowerShell only

<https://docs.microsoft.com/en-us/azure/information-protection/rms-client/aip-clientv2>

 Edit label

 Publish label

 Delete label

Name
Confidential

Display name
Confidential

Tooltip
This data includes sensitive business information. Exposing this data to unauthorized users may cause damage to the business. Examples for Confidential information are employee information, individual customer projects or contracts and sales account data.

Description

Encryption
Encryption

Content marking
Watermark: Confidential
Footer: Sensitivity: Confidential

Site and group settings
Public - anyone in the organization can access the site

Endpoint data loss prevention
Endpoint data loss prevention

Auto-labeling for Office apps

Understanding sensitivity labels

✓ Customizable

✓ Persists as container metadata or file metadata

✓ Readable by other systems

✓ Determines DLP policy based on labels

✓ Extensible to partner solutions



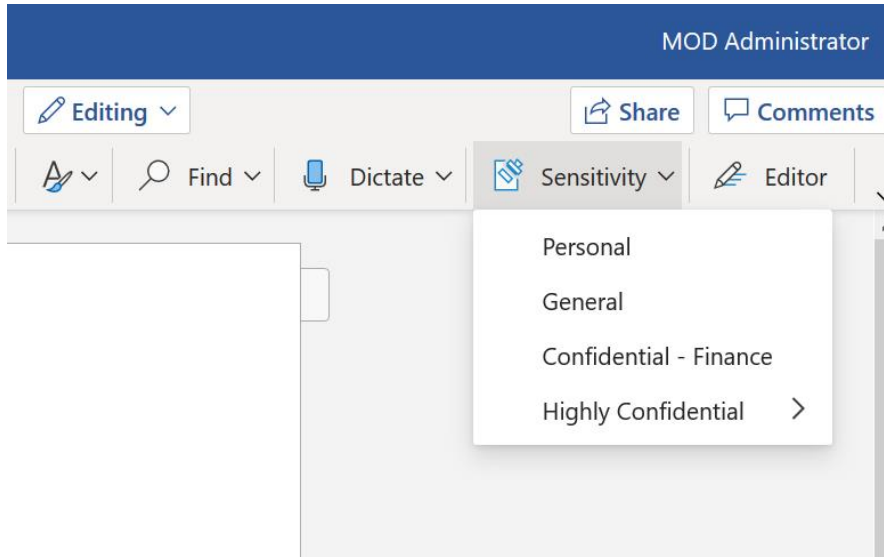
Manual or Automated Labels ✓

Apply to content or containers ✓

Label data at rest, data in use, or data in transit ✓

Enable protection actions based on labels ✓

Seamless end user experience across productivity applications ✓



Sensitivity Labels in Office

Site and group settings



Privacy of Office 365 group-connected team sites

Private - only members can access the site



External users access

☐ Let Office 365 group owners add people outside the organization to the group

Unmanaged devices

☐ Allow full access from desktop apps, mobile apps, and the web

☐ Allow limited, web only access

☒ Block access

Sensitivity Labels
with Teams and
SharePoint

Is the data you care about protected?



GDPR challenges

Personal privacy rights

Must protect data

Mandatory data breach reporting

Big penalties for non-compliance



Personal data

Any information related to an identified or identifiable natural person including direct and indirect identification. Examples include:

- Name
- Identification number (e.g., SSN)
- Location data (e.g., home address)
- Online identifier (e.g., e-mail address, screen names, IP addresses, device IDs)



Sensitive personal data

Personal data afforded enhanced protections:

- Genetic data (e.g., an individual's gene sequence)
- Biometric Data (e.g., fingerprints, facial recognition, retinal scans)
- Sub categories of personal data including:
 - Racial or ethnic origin
 - Political opinions, religious or philosophical beliefs
 - Trade union membership
 - Data concerning health
 - Data concerning a person's sex life or sexual orientation

Getting Start with Data Classification

Classify data according to sensitivity and business impact



Publically available websites, published documents, brochures



Company Intellectual Property (IP), Employee Directory, Purchase Orders



PII (Personally Identifiable Information), Financial reporting data

Data protection & data governance go hand-in-hand

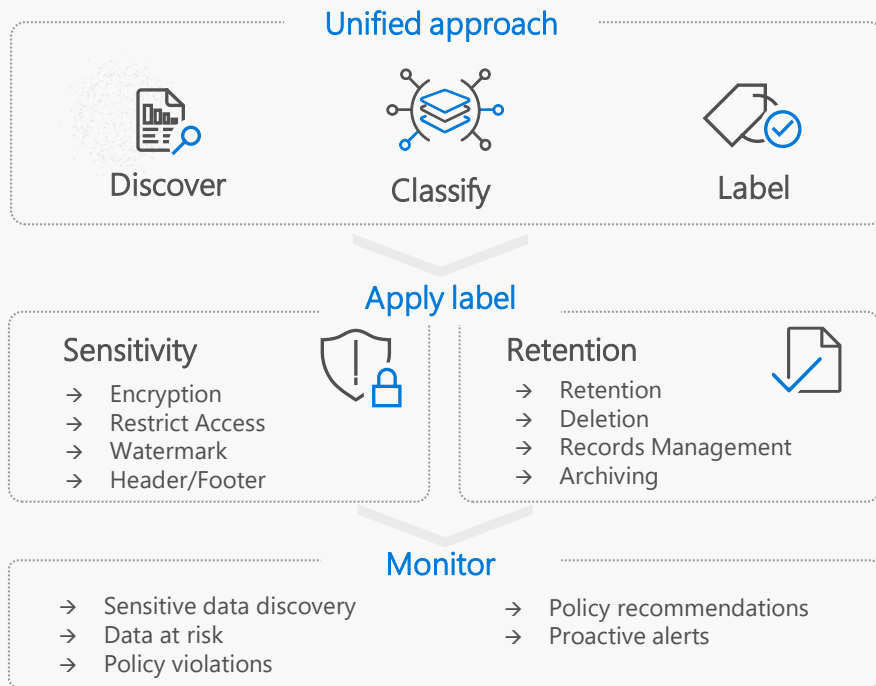
Comprehensive policies to protect and govern your most important data – throughout its lifecycle

Unified approach to discover, classify & label

Automatically apply policy-based actions

Proactive monitoring to identify risks

Broad coverage across locations



A nighttime photograph of the Krakow Barbican, a historic brick fortress with two prominent towers, illuminated by warm lights and reflected in the water. The image has a torn-paper edge effect.

DEMO

Using Sensitivity Labels for Document Protection

Licensing

- E3 (P1)

- Classification and Labelling
- Encryption and Rights Management
- Tracking and Reporting

- E5 (P2)

- Recommendations
- Automation
- AIP Scanner

For native labelling client: Office ProPlus version 1910 or higher



Information Protection in Office 365

- Sensitivity Labels for Teams / SPO / O365 Groups
- PowerBI support for Sensitivity Labels
- Unified Labelling Scanner Network Discovery Feature
- Azure SQL support (Azure Purview)



PowerShell and Files

- **Get-AIPFileStatus** - For a shared folder, identify all files with a specific label.
- **Set-AIPFileClassification** - For a shared folder, inspect the file contents and then automatically label unlabeled files, according to the conditions that you have specified.
- **Set-AIPFileLabel** - For a shared folder, apply a specified label to all files that do not have a label.
- **Set-AIPAuthentication** - Label files non-interactively, for example by using a script that runs on a schedule.
Set-[AIPAuthentication](#) -AppId "<your AppId>" -AppSecret "<your AppSecret>" -
[TenantId](#) "<your TenantId>" -DelegatedUser scanner@contoso.com -OnBehalfOf \$pscreds
- <https://docs.microsoft.com/en-us/azure/information-protection/rms-client/clientv2-admin-guide-powershell>



When you manage sensitive information...

- You can protect your data from leakage
- You can *know* your data is secure
- Users can be more productive
- Users stay in control
- Management can stay on-top



Getting Started

- Define “sensitive data” for your company & establish your label taxonomy
- Customize your protection policies – based on internal objectives and compliance requirements
- Start classifying and labeling content
- Assess and adjust, based on ongoing monitoring of sensitive data, impact on users
- AIP Deployment Guide from Microsoft – aka.ms/AIPDAG & aka.ms/MIPDocs

Q&A

- Time for questions



A low-angle photograph of three skyscrapers reaching towards a dramatic, cloudy sky. The building on the left is covered in scaffolding, suggesting it is under construction. The middle building is a classic brick skyscraper. The building on the right has a curved, modern glass facade. The image has a torn-paper edge effect.

THANK YOU!
Danke Schön!