Be the Information Protection Hero of Your Organization

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

NORDIC — VIRTUAL SUMMIT —

Be the Information Protection Hero of Your Organization

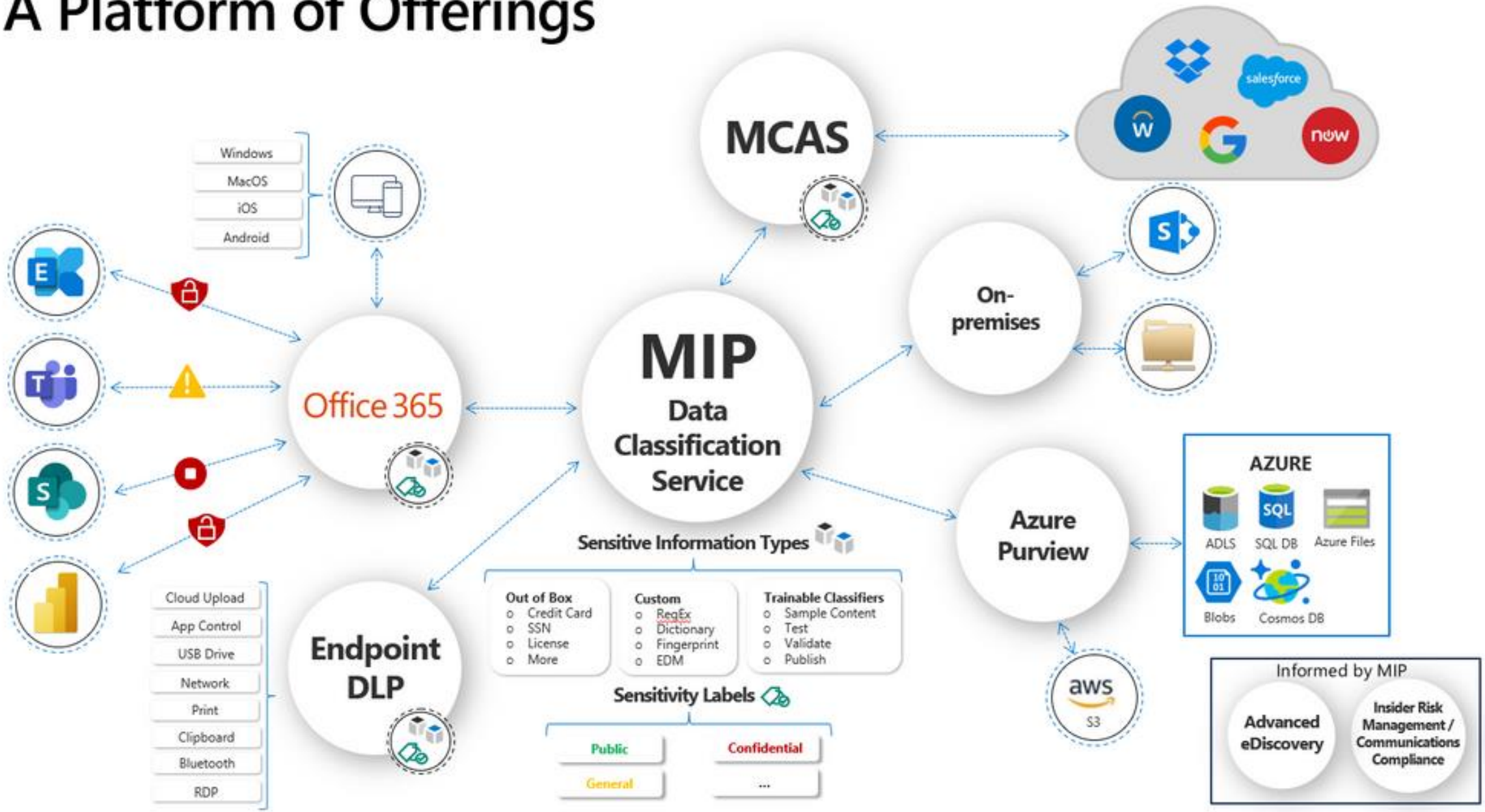
- Morten Thomsen
- Cloud Security Architect, APENTO
- Twitter: @Thomsen79
- Mail: mth@apento.com
- Cerfitified: Enterprise Administrator expert
- MCT

NORDIC — VIRTUAL SUMMIT —

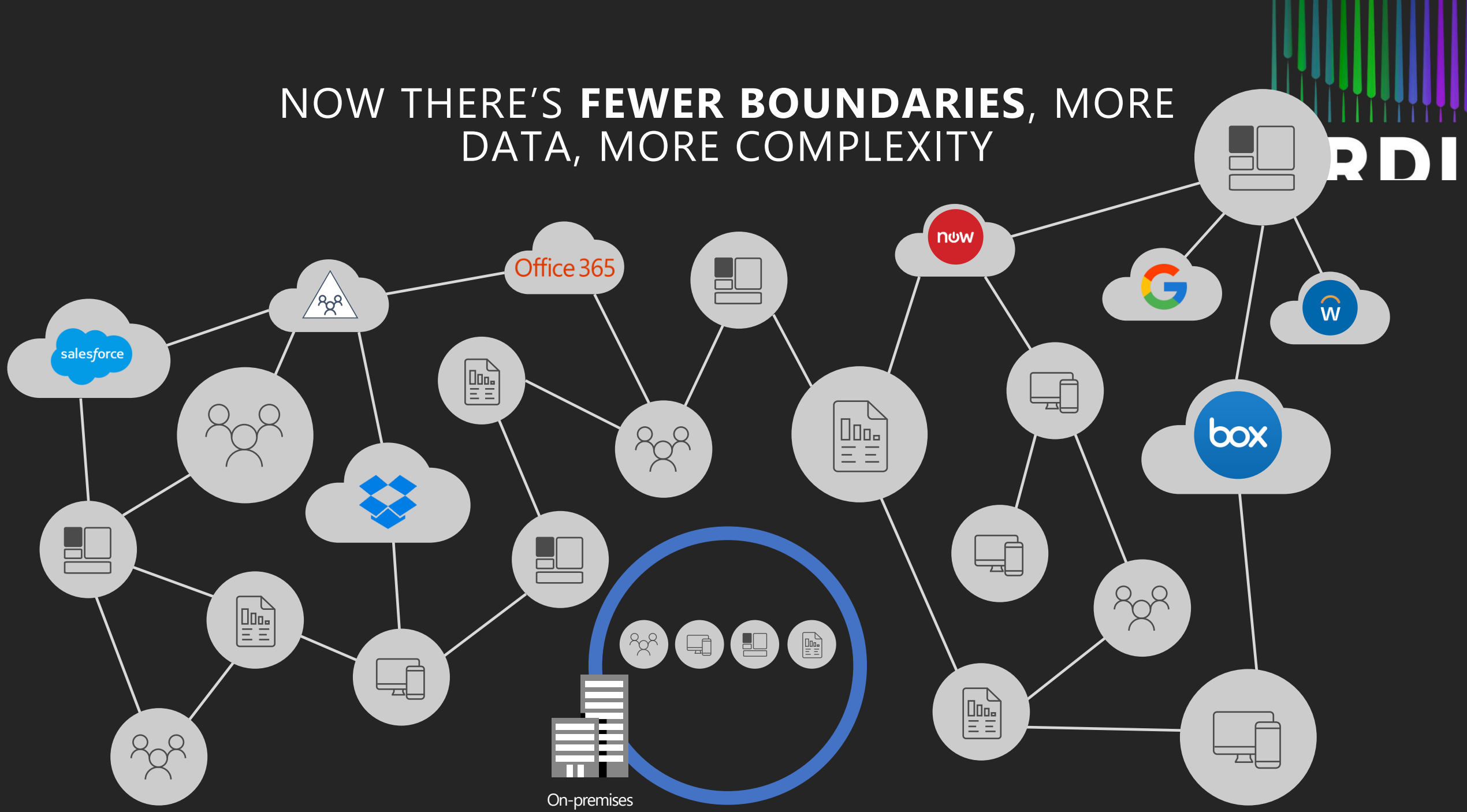
Agenda

- Introduction to MIP
- Labels
- Data Classification
- Demo
- Licensing
- Wrap-up

A Platform of Offerings



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



Data Protection Scenarios

Sensitive Information left on Commuter Train

Sensitive information Shared with wrong recipient

IP Information gets stolen

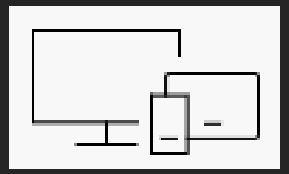
The Journey!

- Remember all the stakeholders in the entire Organization
- The Information protection journey contains:
  - 5-10% legal, risk & compliance to get the classification right
  - 5-10% Technology implementation
  - 80-90% is User Adoption
- To succeed you need the business with you!
- And User adoption, user adoption and user adoption

MICROSOFT INFORMATION PROTECTION

Office 365 Information Protection

+



Windows Information Protection

+

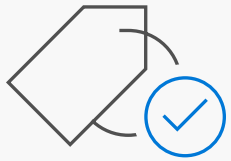
Azure Information Protection

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 Compliance Center

Microsoft Information Protection

Protect your sensitive data – wherever it lives or travels

Discover



Classify

Protect

Monitor

Across

Devices

Apps

Cloud services

On-premises

Labels

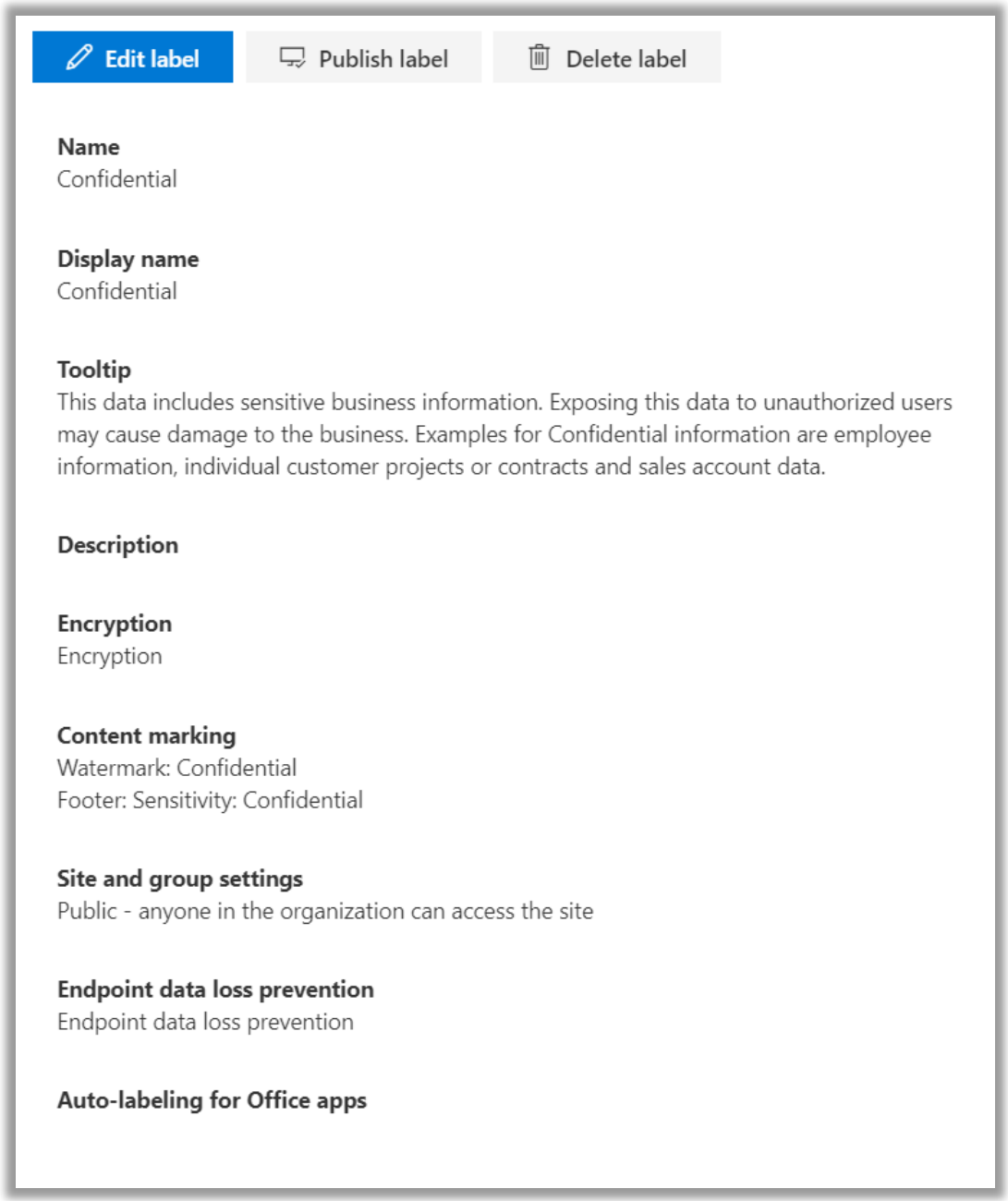
Sensitivity Labels

Retention 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

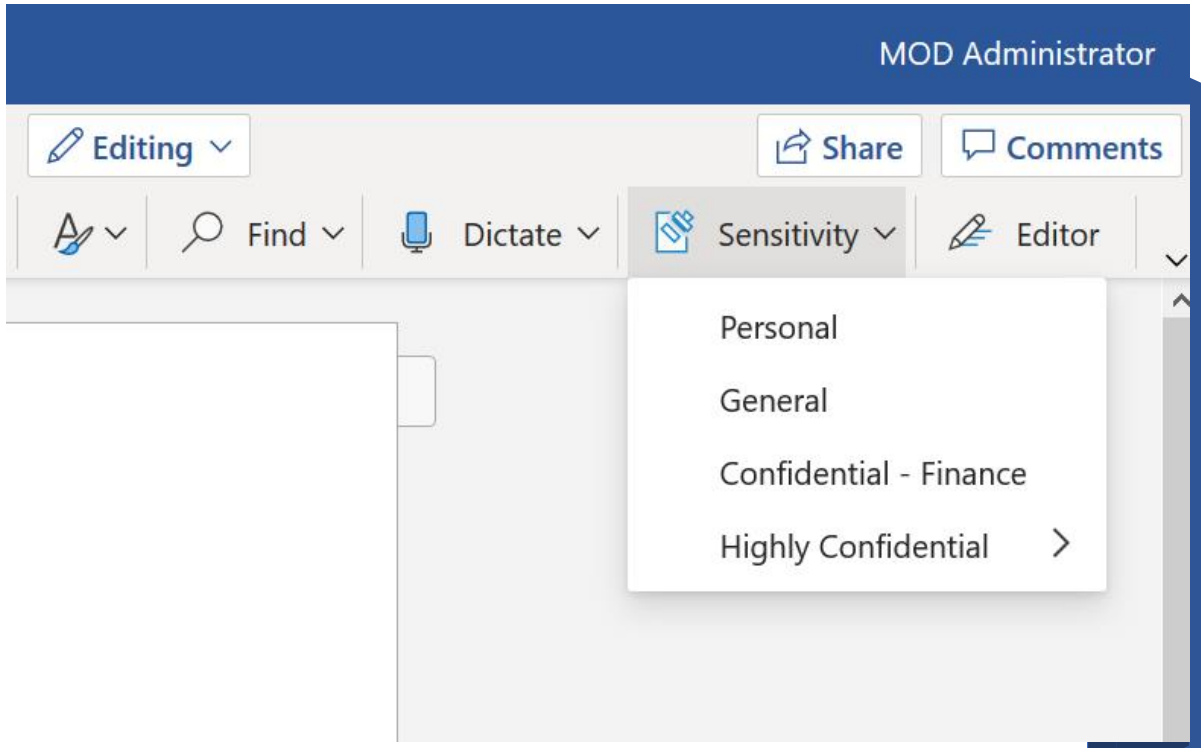
https://docs.microsoft.com/en-us/azure/information-protection/rms-client/aip-clientv2



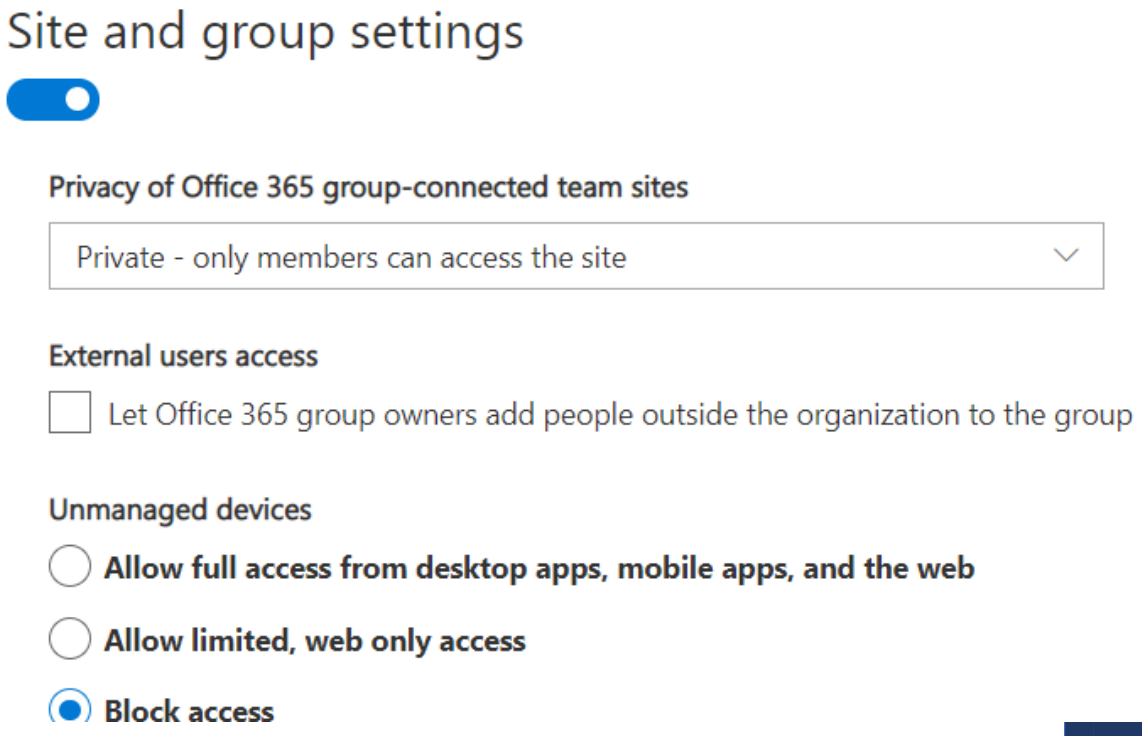
Understanding sensitivity labels

- 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



Sensitivity Labels with Teams and SharePoint

Do you have a strategy for managing your sensitive data?

Where is your data?

What is your data?

Who is accessing your data?

Does your data travel externally?

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

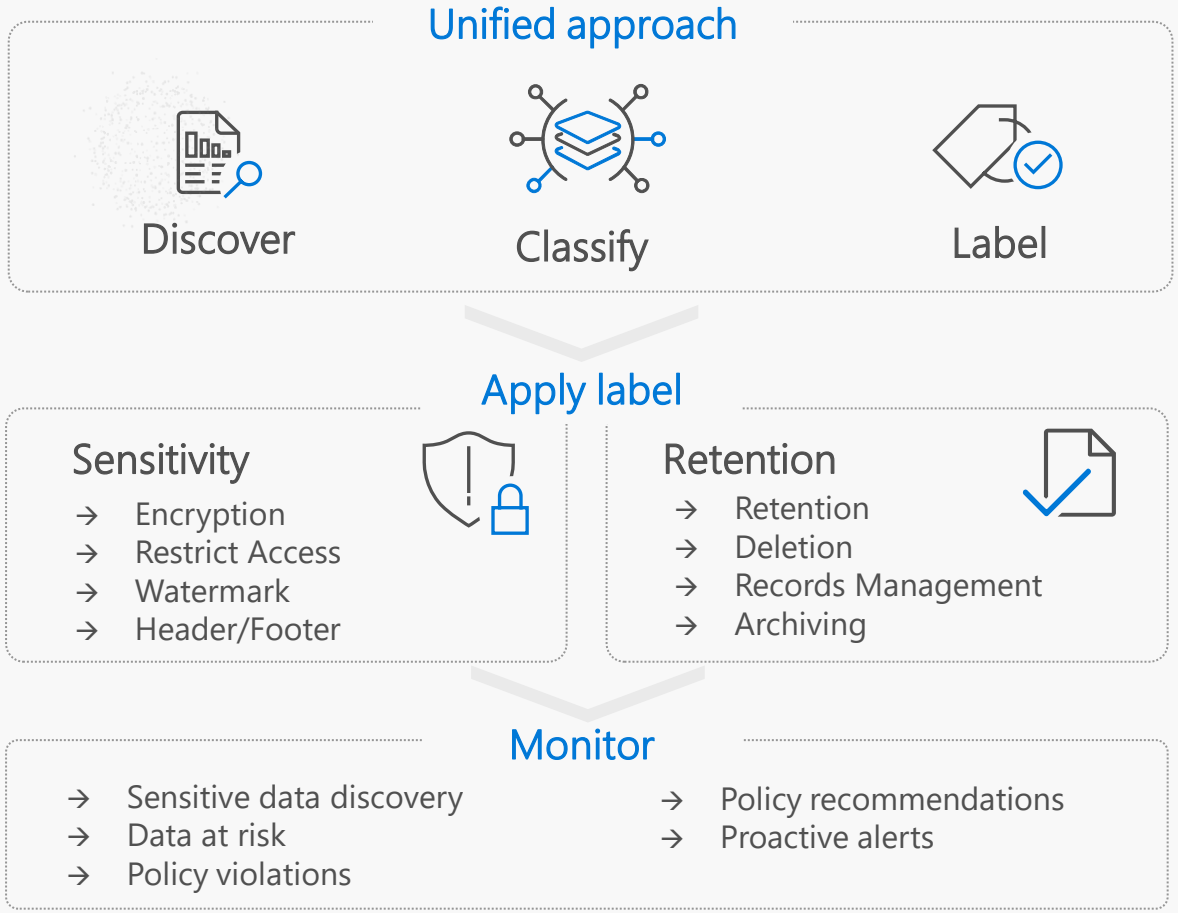
Company Intellectual Property (IP), Employee Directory, Purchase Orders

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



DEMO

Using Sensitivity Labels for Document Protection and Monitoring

Licensing

• E3 (P1)	• E5 (P2)
• Classification and Labelling • Encryption and Rights Management • Tracking and Reporting	• Recommendations • Automation • AIP Scanner

For native labelling client: Office ProPlus version 1910 or higher

Microsoft Information Protection

- Sensitivity Labels for Teams / SPO / O365 Groups
- Co-authoring encrypting documents
- PowerBI support for Sensitivity Labels
- Unified Labelling Scanner Network Discovery Feature
- PowerShell support

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

- Deployment Guide from Microsoft (aka.ms/MIPDocs) and Information Protection Ninja Training (aka.ms/MIPNinja)

Q&A

Time for questions