



**INGRAM MICRO CLOUD** More as a Service™

June 19, 2024

# Microsoft Purview Information Protection

Diego Lens  
Ingram Micro Cloud BeNeLux

**Course will start at 9h15**

More as a Service™

1



Wifi SSID  
**Ingram\_Guest Welcome!**

**INGRAM MICRO CLOUD** More as a Service™

June 19, 2024

# Microsoft Purview Information Protection

Diego Lens  
Ingram Micro Cloud BeNeLux

**Course will start at 9h15**

More as a Service™

2

# Diego Lens

- 24 Years working in Distribution
- Cloud Enablement
- Sales/Technical Trainings
- Microsoft Azure
- Microsoft 365
- Azure Virtual Desktop

- [diego.lens@ingrammicro.com](mailto:diego.lens@ingrammicro.com)
- [linkedin.com/in/diegolens](https://www.linkedin.com/in/diegolens) 



3

Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.



3

# Modern Cloud Platforms

<https://ingram.cloudchampion.be/calendar>



24-Jan: Microsoft Azure Story Telling (Sales)

6-Feb: Microsoft Azure Mission 65 (Tech)

22-Feb: Azure Arc (Tech)

6-Mar: Microsoft Azure Fundamentals (Both)

20-Feb: Microsoft Azure Assessment & Migration (Hands-On)

21-Mar: Azure Lighthouse & Cost Management (Tech)

Legend:  
 ● Sales  
 ● Tech  
 ● Both  
 🖐️ Hands-On

4

Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.



4

# Seamless Security

<https://ingram.cloudchampion.be/calendar>

31-Jan 28-Feb 27-Mar

27-Feb 21-Feb 20-Mar

- Sales
- Tech
- Both
- Hands-On

5 Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission. INGRAM

5

# Connected Workplace

7-Feb 19-Apr

29-Mar

- Sales
- Tech
- Both
- Hands-On

<https://ingram.cloudchampion.be/calendar>

6 Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission. INGRAM

6

# Business Performance & Artificial Intelligence



Coming Soon

17-Apr

- Sales
- Tech
- Both
- ✋ Hands-On

29-Feb



<https://ingram.cloudchampion.be/calendar>

7

Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.



7

# Ingram Micro Cloud



16-Jan

9-Feb

- Sales
- Tech
- Both
- ✋ Hands-On

8-Feb



<https://ingram.cloudchampion.be/calendar>

8

Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.



8



# Agenda

- Information Protection Challenges
- Microsoft Information Protection
- Know Your Data
- Protect Your Data
- Microsoft Purview Roadmap
- Prevent Data Loss
- Govern Your Data
- Information Protection Licensing

INTEGRAL MICROSOFT CLOUD



# Information Protection Challenges

INTEGRAL MICROSOFT CLOUD - More as a Service

▶ More as a Service™

# Protecting data is challenging

#1

Protecting and governing sensitive data is biggest concern in complying with regulations<sup>1</sup>

63%

of organizations fear data leak/spillage during the pandemic<sup>2</sup>

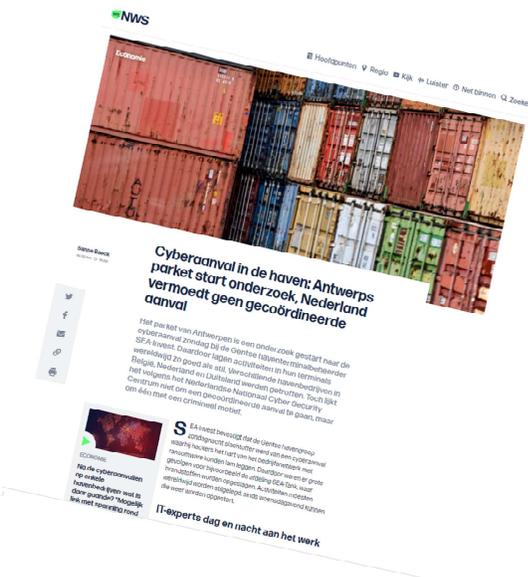
88%

of organizations no longer have confidence to detect and prevent loss of sensitive data<sup>3</sup>

<sup>1</sup> Microsoft: GDPR research, 2017  
<sup>2</sup> Microsoft: COVID Security Priorities Survey 2020  
<sup>3</sup> Forrester: Security Concerns, Approaches and Technology Adoption. December 2018

11

# Cyber Attacks



CONDUENT

05-06-2020 | door: Redactie

Conduent is getroffen door Maze ransomware aanval

Outsourcer Conduent meldt dat zijn Europese activiteiten zijn getroffen door Maze ransomware waarbij sprake is van het lekken van interne bedrijfsdocumenten.

Emsisoft, evenals het beveiligingsbedrijf Bad Packets, melden dat Conduent lijkt te zijn getroffen door Maze ransomware. Maze heeft eerder Cognizant in april getroffen.

Bij de Conduent-aanval hebben de hackers twee zip-bestanden gepubliceerd over documenten die betrekking hebben op het werk van het bedrijf in Duitsland naar verluidt over Vodafone Deutschland.

Deze bestanden zijn woensdag vrijgegeven op een site die Maze-aanvallen publiceert.

Conduent is opgericht als nieuwe bedrijf nadat Xerox in 2016 zijn outsourcingactiviteiten voor bedrijfsprocessen had stopgezet.

12

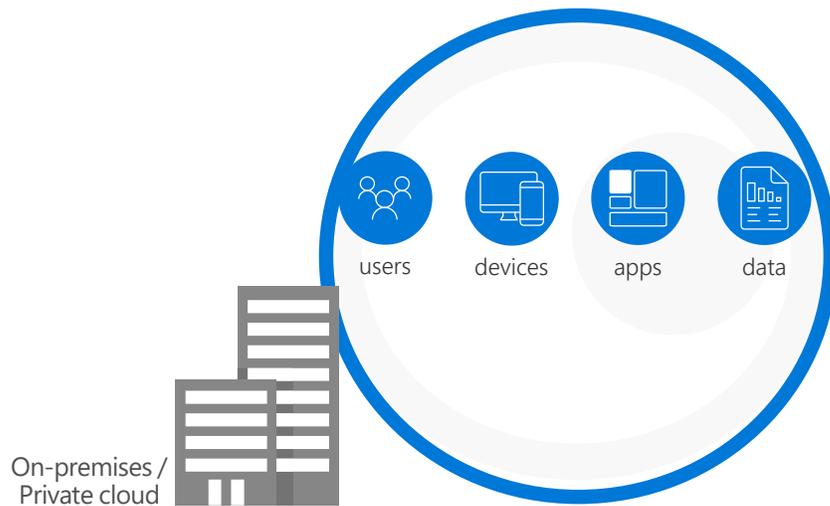
# Information Protection Challenges



- ✓ Rapid shift in how people work
- ✓ Balance security with productivity
- ✓ Cost of breaches and regulations
- ✓ Struggle with 'dark data'
- ✓ Complex patch work of 'bolt-on' solutions
- ✓ Correlating various signals to assess risk

13

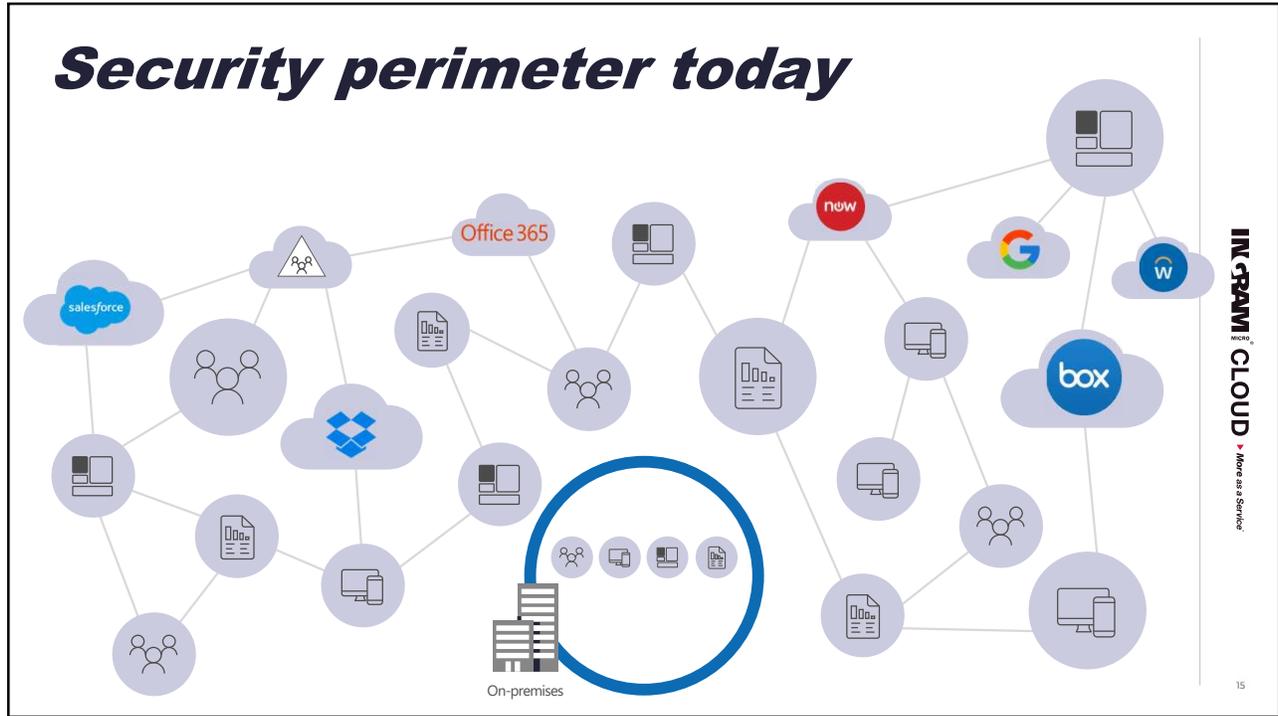
# Security perimeter in the past



INTEGRATED CLOUD Micro Move as a Service

14

14



15

**Microsoft Purview Information Protection**

INTEGRATED MICROSOFT CLOUD - More as a Service

► More as a Service™

The image shows a top-down view of a person's hands holding a pen and pointing at a document. The document contains several charts and graphs, including a pie chart with segments labeled 11%, 17%, and 20%. The text 'Microsoft Purview Information Protection' is overlaid in large white font. The background is a soft-focus office desk with a smartphone, a notebook, and a coffee cup. The logo 'INTEGRATED MICROSOFT CLOUD - More as a Service' is on the left, and '► More as a Service™' is at the bottom right.

16

# Microsoft Security Area's

The diagram illustrates four Microsoft Security Areas arranged in a 2x2 grid. Each area is represented by a purple box with a white plus sign and a corresponding icon. The top-left area is 'PROTECT USERS' with a group of people icon. The top-right area is 'PROTECT DEVICES' with a laptop and smartphone icon. The bottom-left area is 'PROTECT EMAIL & DOCUMENTS' with a folder icon. The bottom-right area is 'MANAGE ENTERPRISE SECURITY' with a magnifying glass icon. To the right of the grid is the 'IN GRAMI MICRO CLOUD' logo with the tagline 'More as a Service'. The number '17' is located at the bottom right of the slide.

17

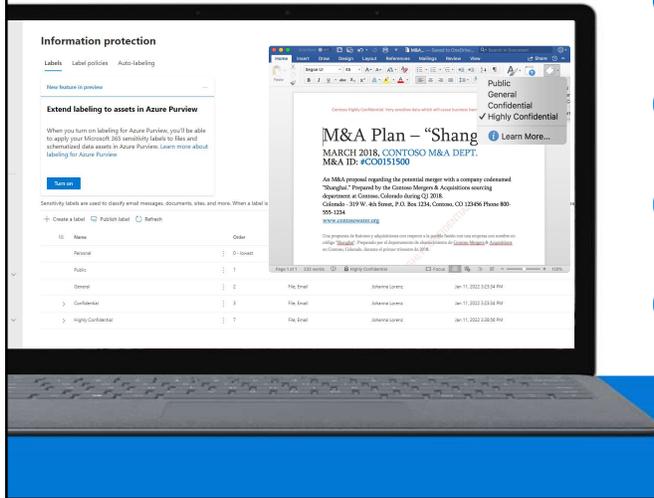
# Microsoft Security Solutions

The diagram illustrates four Microsoft Security Solutions arranged in a 2x2 grid. Each solution is represented by a purple box with a white icon and a corresponding label. The top-left solution is 'IDENTITY AND ACCESS MANAGEMENT' with a network diagram icon. The top-right solution is 'THREAT PROTECTION' with a hand holding a warning sign icon. The bottom-left solution is 'INFORMATION PROTECTION' with a padlock icon. The bottom-right solution is 'SECURITY MANAGEMENT' with a head icon containing a padlock. To the right of the grid is the 'IN GRAMI MICRO CLOUD' logo with the tagline 'More as a Service'. The number '18' is located at the bottom right of the slide.

18

# Microsoft Purview Information Protection

A built-in, intelligent, unified, and extensible platform and solution to protect sensitive data



### Built in

Built-in labeling and protection experience in Office apps, Office 365 services, other MS services like Power BI, Edge, and Windows



### Intelligent

Accuracy in classification via ML based trainable classifiers exact data match and named entities



### Unified

Single admin console to configure and manage your policies and view analytics across on-premises, Office apps, Microsoft 365 services, third-party services (via Microsoft Defender for Cloud Apps), and devices

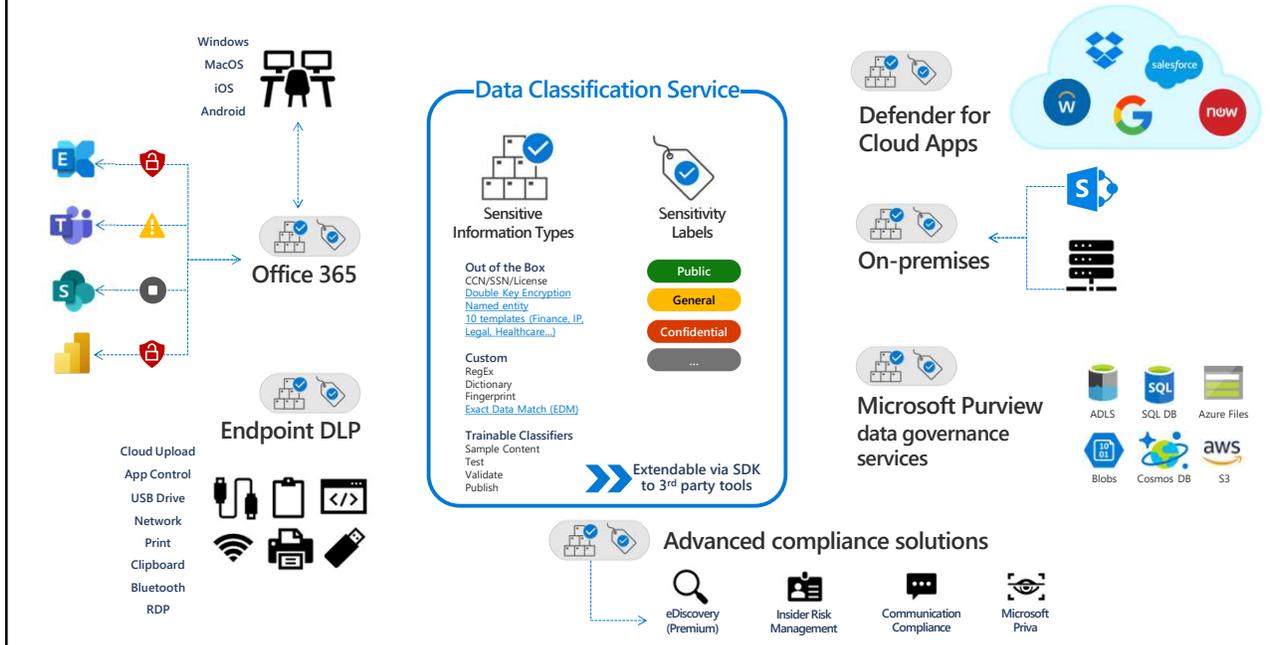


### Extensible

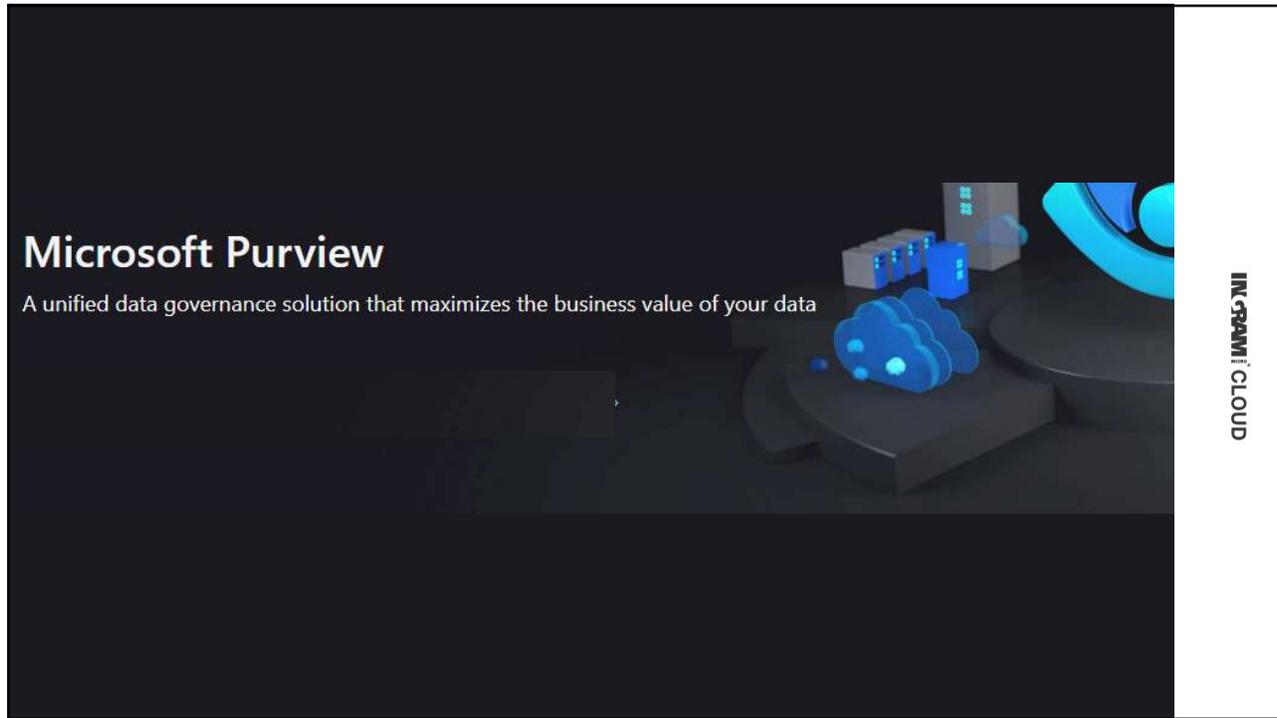
MIP SDK extends the protection experience, in a consistent way, to popular non-Microsoft apps and services

19

## Microsoft Purview Information Protection Framework



20



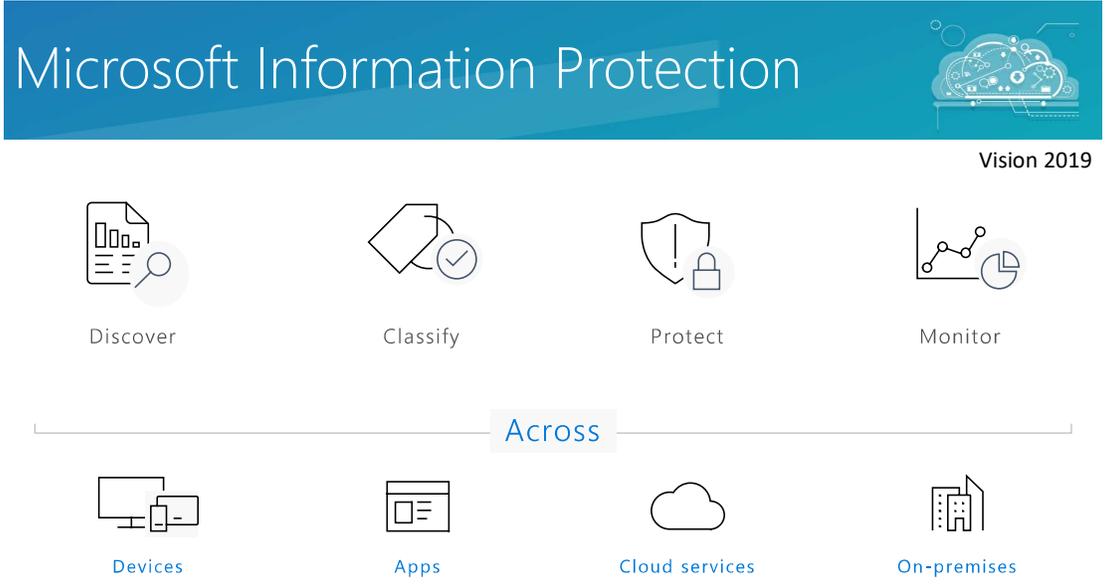
21

## ***Microsoft Purview Product Suite***

<b>Current Name</b>	<b>New Name</b>	<b>Current Name</b>	<b>New Name</b>
Double Key Encryption for Microsoft 365	Microsoft Purview Double Key Encryption	Microsoft 365 Basic Audit	Microsoft Purview Audit (Standard)
Records Management in Microsoft 365	Microsoft Purview Records Management	Microsoft 365 Advanced Audit	Microsoft Purview Audit (Premium)
Office 365 Core eDiscovery	Microsoft Purview eDiscovery (Standard)	Microsoft 365 Communication Compliance	Microsoft Purview Communication Compliance
Office 365 Advanced eDiscovery	Microsoft Purview eDiscovery (Premium)	Microsoft Compliance Manager	Microsoft Purview Compliance Manager
Microsoft 365 Information Barriers	Microsoft Purview Information Barriers	Office 365 Customer Lockbox	Microsoft Purview Customer Lockbox
Microsoft Information Protection	Microsoft Purview Information Protection	Azure Purview Data Catalog	Microsoft Purview Data Catalog
Microsoft 365 Insider Risk Management	Microsoft Purview Insider Risk Management	Microsoft 365 Data Connectors	Microsoft Purview Data Connectors
Azure Purview portal	Microsoft Purview governance portal	Microsoft Information Governance	Microsoft Purview Data Lifecycle Management
Microsoft 365 compliance center	Microsoft Purview compliance portal	Office 365 Data Loss Prevention	Microsoft Purview Data Loss Prevention
Azure Purview Data Insights	Microsoft Purview Data Estate Insights	Azure Purview Data Map	Microsoft Purview Data Map
Microsoft 365 Customer Key	Microsoft Purview Customer Key		

22

# Microsoft Information Protection



Vision 2019

Discover      Classify      Protect      Monitor

Across

Devices      Apps      Cloud services      On-premises

<https://aka.ms/MIPdocs>      INGRAM CLOUD

The diagram illustrates the Microsoft Information Protection (MIP) Vision 2019. It features a central horizontal line labeled "Across" that spans four categories: Devices, Apps, Cloud services, and On-premises. Above this line are four main stages: Discover (represented by a document icon with a magnifying glass), Classify (represented by a document icon with a checkmark), Protect (represented by a shield icon with a lock), and Monitor (represented by a line graph icon with a pie chart). The INGRAM CLOUD logo is located in the bottom right corner.

23

# Microsoft Information Protection



Vision 2020

Understand your data landscape and identify important data across your hybrid environment

**KNOW YOUR DATA**

Apply flexible protection actions including encryption, access restrictions and visual markings

**PROTECT YOUR DATA**

Detect risky behavior and prevent accidental oversharing of sensitive information

**PREVENT DATA LOSS**

Automatically retain, delete, and store data and records in a compliant manner

**GOVERN YOUR DATA**

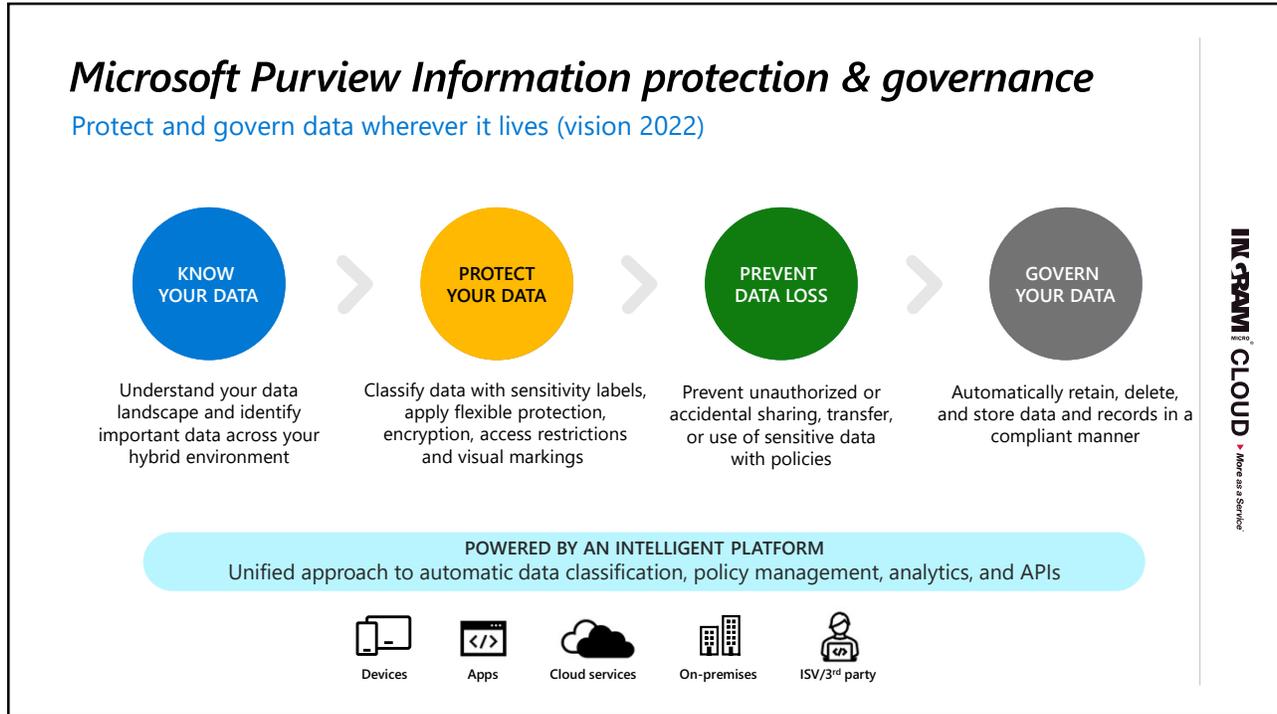
Powered by an intelligent platform

Unified approach to automatic data classification, policy management, analytics and APIs

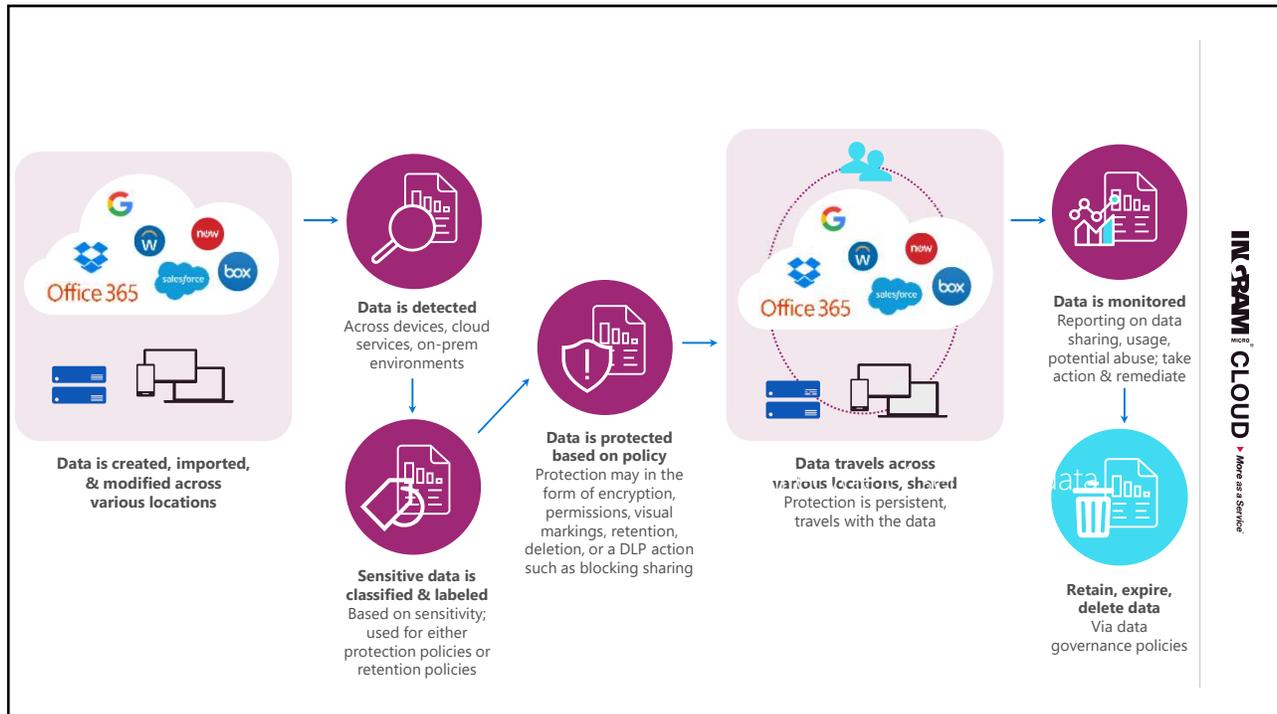
<https://aka.ms/MIPdocs>      INGRAM CLOUD

The diagram illustrates the Microsoft Information Protection (MIP) Vision 2020. It features a central circular flow of four main stages: Know Your Data, Prevent Data Loss, Govern Your Data, and Protect Your Data. Each stage is accompanied by a descriptive text box. The background is filled with a pattern of binary code (0s and 1s). The INGRAM CLOUD logo is located in the bottom right corner.

24



25



26

# MIP : Finding more information



- [https://www.yammer.com/askipteam/#/home?type=my\\_all](https://www.yammer.com/askipteam/#/home?type=my_all)
- <https://docs.microsoft.com/en-us/azure/information-protection/>



27

# History of Azure Information Protection



ADRMS

Azure RMS

Secure Islands  
acquisition

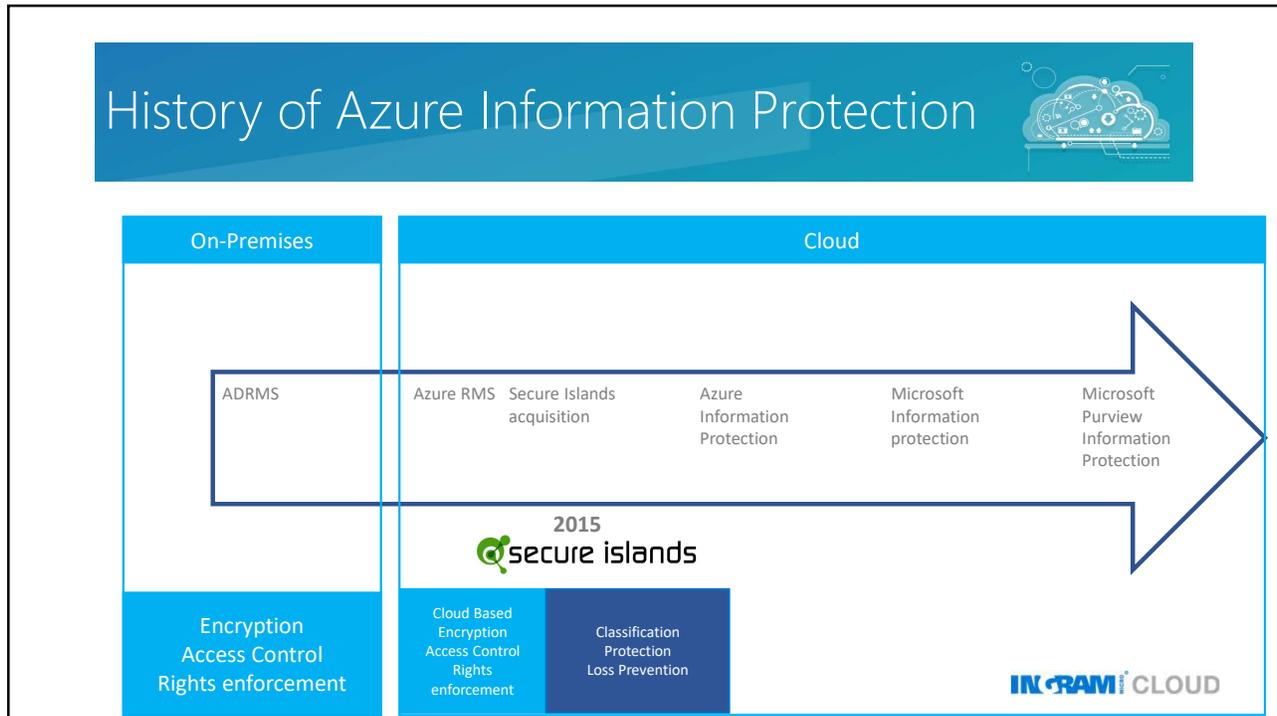
Azure  
Information  
Protection

Microsoft  
Information  
protection

Microsoft  
Purview  
Information  
Protection



28



29

## RMS, IRM or AIP ?



### On-Premises products

AD RMS (Active Directory Rights Management)

- Also referred as HYOK (Hold Your Own Key)

Windows RMS (Windows Rights Management Services)



### Cloud Based

Azure **RMS** (Azure Rights Management Services)

Microsoft RMS (Both AD RMS + Azure RMS)

**IRM** (Information Rights Management)

- Office implementation with AD RMS of Azure RMS (Older version of RMS)

**AIP** (Azure Information Protection)

- The new umbrella for the Cloud Based solutions above
- **Azure RMS** is still used as the protection technology for AIP

<https://docs.microsoft.com/en-us/azure/information-protection/aka>

**INGRAM** CLOUD

30

## Know your Data



- Sensitive information types
  - Identify sensitive data
- Trainable classifiers
  - Classify your data with built-in classifiers & own classifiers
- Microsoft Purview Information Protection scanner

INCRAMI CLOUD

31

## Protect your data



- Sensitivity labels
- Azure Information Protection Unified labeling
- Double Key Encryption
- AIP Unified labeling Scanner
- Microsoft Cloud App Security
- Microsoft Information Protection SDK

INCRAMI CLOUD

32

## Prevent Data Loss



- Data loss prevention (DLP)



INCRAMI CLOUD

33

## Govern your data



- Retain, delete and store data
- Microsoft Information Governance
- Retention Policies
- Retention Labels

INCRAMI CLOUD

34



Journey to the Cloud

# LAB 1 Task2

**TASK1 : CREATE WINDOWS 10 TEST DEVICE**



**INGRAM | CLOUD**

35

```

VM Name: W11 Public IP Address: 104.40.230.146
VM Name: UPCONNECTOR Public IP Address: 40.68.175.146
VM Name: PUR-1 Public IP Address: 172.166.177.67
VM Name: PUR-10 Public IP Address: 172.167.44.62
VM Name: PUR-11 Public IP Address: 172.166.232.73
VM Name: PUR-12 Public IP Address: 172.167.185.102
VM Name: PUR-2 Public IP Address: 172.166.194.188
VM Name: PUR-3 Public IP Address: 172.167.121.177
VM Name: PUR-4 Public IP Address: 172.167.11.105
VM Name: PUR-5 Public IP Address: 172.166.193.7
VM Name: PUR-6 Public IP Address: 172.167.139.138
VM Name: PUR-7 Public IP Address: 172.167.32.157
VM Name: PUR-8 Public IP Address: 172.166.248.5
VM Name: PUR-9 Public IP Address: 172.166.201.54

```

**INGRAM | CLOUD**

<https://bit.ly/imcpurview>

36



**Journey to the Cloud**

# Know Your Data

-  Discover
-  Classify
-  Protect
-  Monitor

**INCRAM** CLOUD

37

## Know your data – Top of mind questions

-  Where is my sensitive data located?
-  What are the risky activities happening in my organization – files shared externally, across 1<sup>st</sup> and 3<sup>rd</sup> party apps?
-  I need to comply with a new regulation? Where is my PII data located & where is it being generated?
-  How do I control data sprawl and build a strategy for dark data disposal before I bring data to the cloud from on-premise?
-  How do I see activity around classification and labeling across retention and sensitivity labels once they have been used across governance and retention outcomes?
-  How do I automate and scale classification across different types of data in my organization?

**INCRAM** CLOUD

38

# Tools to know your data

Know Your Data  
Understand your data landscape across your hybrid environment

Microsoft 365

- Data discovery
- Trainable classifiers
- Intelligent classification
- Automated protection & governance
- Auto-labeling
- End-user experience
- Exploration & refinement
- Content explorer
- Activity explorer

INTEGRAM CLOUD

39

# Discover your Data

- Discover**  
Scan & detect sensitive data based on policy
- Classify**  
Classify data and apply labels based on sensitivity
- Protect**  
Apply protection actions, including encryption, access restrictions
- Monitor**  
Reporting, alerts, remediation

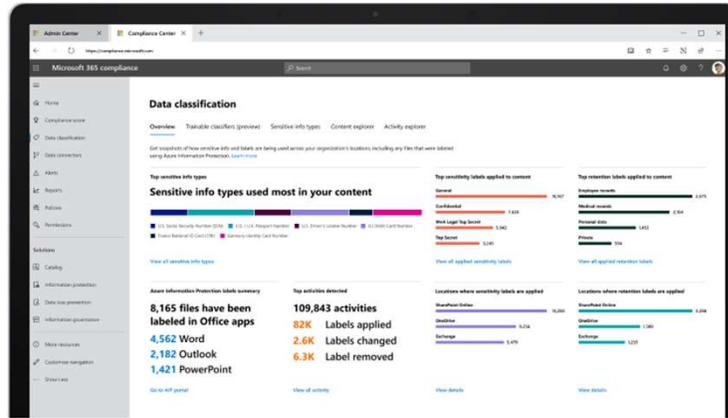
INTEGRAM CLOUD

40

# Discovering Data



- What Sensitive Information does exist in the Organization ?



INCRAM CLOUD

41

# Discover Sensitive Data



- Microsoft Purview Information Protection Scanner
- AIP unified labeling client
- Microsoft Defender for Endpoints
- Microsoft Cloud App Security



INCRAM CLOUD

42

## What does Microsoft Purview Information Protection scanner do ?



Scans on-prem repositories: file shares, NAS or any other CIFS based repositories, or SharePoint 2013/2016

Remark : NFS Shares in Private Preview on 21/09/2020



Discover data in the scanned repositories and match it against AIP policy (sensitive info types, location or custom property)



Labels and protects the discovered data per AIP policy. AIP scanner uses the same AIP policy as AIP clients.



Create a report of discovered data, including the matched conditions for found patterns

**INCRAM** CLOUD

43

## Why Microsoft Purview Information Protection scanner ?



- Our business policy, compliance or regulation (GDPR) requires all files to be classified.  
We label new created data using AIP client, but
  - What about the data that was created before we started to use AIP?
  - We had another solution and we want AIP to leverage the existing 3<sup>rd</sup> label
  - Some files are generated by automatic processes rather than created by end users
- We want to migrate to the cloud, but
  - We want to know what is going to be migrated
  - We want to label and encrypt data before it's moved to the cloud
  - We want to decide what data is move to the cloud and what stays on perm

**INCRAM** CLOUD

44

## Microsoft Purview Information Protection scanner in portal

Settings > Information protection scanner

### Information protection scanner

Use the scanner to discover, classify, and protect files stored in network shares and on-premises SharePoint document libraries and folders. [Learn more about the scanner](#)

For support related to the information protection scanner, visit [Help + support](#) within the Azure portal.

Clusters Nodes Content scan jobs

+ Add Refresh 0 items Search

Name	Description	Content scan job	Nodes
------	-------------	------------------	-------



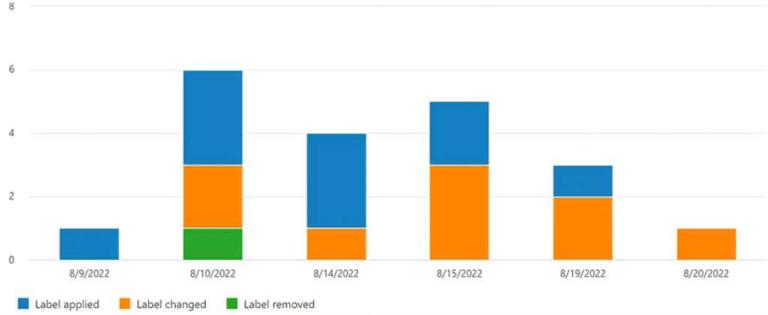
45

## Microsoft Purview Information Protection scanner Discovery

### Query Audit Events in Activity Explorer

Date: 8/1/2022-8/26/2022 Activity: LabelApplied, LabelChanged, LabelRemoved Location: Any

User: Any Sensitivity label: Any Application: Microsoft Azure Information Protection... Show less



Date	Label Applied	Label Changed	Label Removed
8/9/2022	1	0	0
8/10/2022	3	2	1
8/14/2022	3	1	0
8/15/2022	2	3	0
8/19/2022	1	2	0
8/20/2022	0	1	0



46

# Endpoint Data Discovery



AIP client	<ul style="list-style-type: none"> <li>Any set / remove / relabel event</li> <li>Sensitive info types and custom regexes on file Save (preview)</li> </ul>	<ul style="list-style-type: none"> <li>Win 7/8/10 + Office 2010/13/16</li> <li>Requires AIP client</li> <li>Runs inside the app and inspect only files opened by app that uses AIP client</li> </ul>
WDATP and AIP integration	<ul style="list-style-type: none"> <li>Labeled files created (for ex. downloaded) or modified on the endpoint</li> <li>Sensitive info types and custom info-types matched in content (coming soon)</li> </ul>	<ul style="list-style-type: none"> <li>Latest Win 10 (RS-5 at least)</li> <li>No additional SW required</li> <li>Runs on the OS level and inspect all newly created or modified files</li> </ul>

INCRAM CLOUD

47

# Microsoft Cloud App Security Integration



Cloud App Security

Settings

Search

System

Organization details

Mail settings

Export settings

Auto sign out

Cloud Discovery

Score metrics

Snapshot reports

Continuous reports

Automatic log upload

App tags

Exclude entities

User enrichment

**Azure Information Protection**

Azure Information Protection settings

Automatically scan new files for Azure Information Protection classification labels and content inspection warnings

Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant

[Get more info in the Azure Information Protection integration guide](#)

[Save](#) We secure your data as described in our [privacy statement](#).

**Inspect protected files**

File policies can inspect content in Azure Information Protection protected files. To inspect protected files, grant Cloud App Security permission in Azure AD.

[Grant permission](#)

INCRAM CLOUD

48

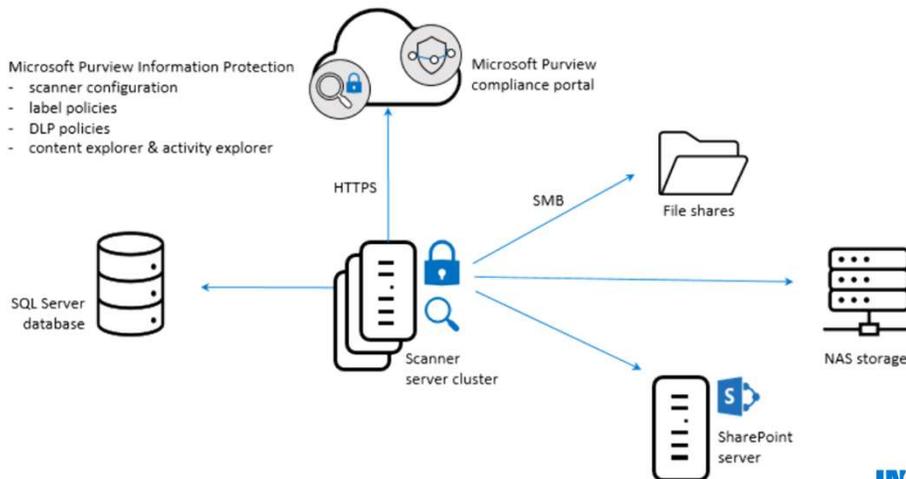
# How to Start ?

- Start by discovery of your data, if you do not know what to search for just discovery all built-in infotypes
- Analyze the results and proceed to policy enforcement once you are confident
- Use discovery reports to find data at risk, abnormal behavior
- Use AIP client reports to find sensitive not scanner repos



49

# Microsoft Purview Information Protection Scanner Overview



50

## Microsoft Purview Information Protection scanner Requirements (1/5)



- Windows Server 2012R2 / 2016 / 2019 (64 bit)
- 4 core processors / 8 GB RAM /
- Internet Access (port 443)
- Unified Azure Information Protection client
- SQL database (SQL Express also possible)
- File Server(s) or SharePoint Server(s) or NFS shares
- A Service Account for the AIP Scanner Service

<https://learn.microsoft.com/en-us/azure/information-protection/deploy-aip-scanner-prereqs>

INGRAM CLOUD

51

## Create a Microsoft Purview Information Protection scanner Cluster (2/5)



### Information protection scanner

Use the scanner to discover, classify, and protect files stored in network shares.

For support related to the information protection scanner, visit [Help + support](#) within the scanner.

Clusters Nodes Content scan jobs

+ Add Refresh

Name	Description

Delete

Name \*

Ingram Cluster

Description

Ingram Information Protection Scanner

Save

Cancel

INGRAM CLOUD

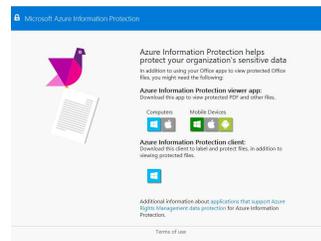
52

## Install the AIP Scanner Software (3/5)



- Download the AIP Client
- <https://portal.azure.com/#/Download>
- Launch the Install-AIPScanner command

```
PowerShell
Install-AIPScanner -SqlServerInstance <name> -Cluster <cluster name>
```



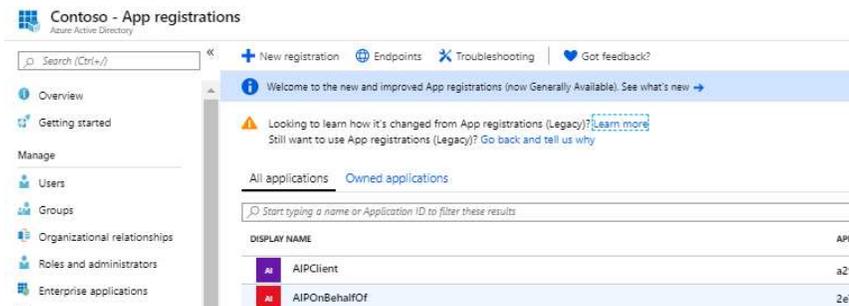
INCRAM CLOUD

53

## Get an Azure AD Token for the Scanner (4/5)



- Set-AIPAuthentication
  - webAppId <ID of the "Web app / API" application>
  - webAppKey <key value generated in the "Web app / API" application>
  - nativeAppId <ID of the "Native" application>



INCRAM CLOUD

54

# Scan your Files (5/5)



- <https://portal.azure.com>



55

## Information Protection Packaging

Information Protection Feature	M365 Business Premium	M365 Enterprise E3	M365 Enterprise E5	Other
Windows Information Protection	Yes	Yes	Yes	
RMS, DLP	Yes	Yes	Yes	
Azure Information Protection P1	Yes	Yes	Yes	
Azure Information Protection P2			Yes	
Microsoft Intune	Yes	Yes	Yes	
Microsoft Cloud App Security			Yes	
AIP for Office 365	Option	Yes	Yes	
Automatic Labeling			Yes	



56

56

# Information Protection Plans

Information Worker Plans										Frontline Worker Plans							
Microsoft 365				Office 365			Enterprise Mobility Security			Windows 10		Microsoft 365					Office 365
E3	E5	E5 Security Add-on	E5 Compliance Add-on	E1	E3	E5	E3	E5	Pro (for reference)	Enterprise E3	Enterprise E5	F1	F3	F5 Security Add-on	F5 Compliance Add-on	F5 Sec + Comp Add-on	F3
\$32	\$57	\$12	\$12	\$8	\$20	\$35	\$8.80	\$14.80		\$5	\$10	\$2.25	\$8	\$8	\$8	\$13	\$4

USD ERP per user per month

Information protection	Plan 1	Plan 2	Plan 2	AIP for O365	AIP for O365	Plan 1	Plan 2			Plan 1	Plan 1		Plan 2	Plan 2
Azure Information Protection														
Manual sensitivity labels	•	•			•	•	•						•	•
Automatic sensitivity labels	•	•			•	•	•						•	•
Machine Learning-based sensitivity labels		•											•	•
Office 365 Data Loss Prevention (DLP) for emails and files	•	•			•	•							•	•
Communication DLP (Teams chat)	•	•											•	•
Endpoint DLP	•	•			•								•	•
Basic Office Message Encryption	•	•			•	•	•				•	•		
Advanced Office Message Encryption	•	•			•	•							•	•
Customer Key for Office 365	•	•			•	•							•	•

INGRAM MICRO CLOUD



## New Microsoft Purview Information Protection labeling client

**MS** Martin Sieber – March 21 at 09:04 PM  
 ☰ New Microsoft Purview Information Protection labeling client / Updated support lifecycle for AIP 2.x clients

The Azure Information Protection unified labeling client is joining the Purview family!

The Microsoft Purview Information Protection labeling client replaces the AIP UL client and includes the PowerShell, Scanner, File Labeler (previously AIP Classify & Protect) and Viewer. Client versions for the rebranded client begin with 3.X and do not include the AIP Add-in for Office.

Preview the Microsoft Purview Information Protection labeling client on April 11, 2024 from the Microsoft Download Center. The new client is Generally Available starting May 11, 2024 and is supported through May 11, 2025.

For AIP 2.x clients, we updated the support lifecycle on <https://learn.microsoft.com/en-us/azure/information-protect...>. The AIP Add-in for Office will continue to be supported until April 11, 2024, but support for the other AIP components of the latest AIP versions has been extended to allow time to switch to the new client:

- Version 2.17.67.0 AIP Add-in for Office is supported until 04/11/2024. AIP PowerShell, Scanner, Classify & Protect and Viewer are supported until 06/30/2024.
- Version 2.17.66.0 AIP Add-in for Office is supported until 04/11/2024. AIP PowerShell, Scanner, Classify & Protect and Viewer are supported until 06/30/2024.
- Version 2.16.73.0 AIP Add-in for Office is supported until 04/11/2024. AIP PowerShell, Scanner, Classify & Protect and Viewer are supported until 04/25/2024.



Journey to the Cloud

# LAB 1

**TASK 2 : PREPARE WINDOWS 10 DEVICE**  
**TASK 3 : CONNECT AS A USER**  
**TASK 4 : VERIFY LICENSES**



59



Journey to the Cloud

# Protect Your Data



**KNOW YOUR DATA**  
Understand your data landscape and identify important data across your hybrid environment

**PREVENT DATA LOSS**  
Detect risky behavior and prevent accidental oversharing of sensitive information

**PROTECT YOUR DATA**  
Apply flexible protection actions including encryption, access restrictions and visual markings

**GOVERN YOUR DATA**  
Automatically retain, delete, and store data and records in a compliant manner



60

# Information Protection Vocabulary



INTEGRAM CLOUD

61

# Classification



- Microsoft Purview provides three ways to classify your data :
  1. Manually by users
  2. Automated with Sensitive Information Types (SIT)
  3. Automated with Machine Learning

INTEGRAM CLOUD

62

## 1. Manual Classification



- Requires human judgment and action
- Users/Admins categorize content as they encounter it



INCRAMI CLOUD

63

## 2. Sensitive Information Types



- A Sensitive information Type (SIT) is the ability to determine the confidentiality of specific sets of sensitive information
- A Sensitive information Type is a regular expression or **pattern-based expression** that can help identify the data

`([0-9]+?)-\d{3}-^[A-Z]+`



INCRAMI CLOUD

64

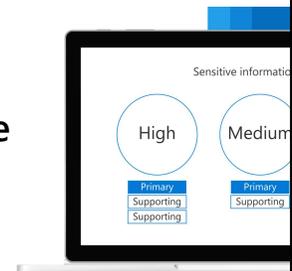
## Different Sensitive Info Types



- Two Types
  - Preset Information Types
    - Social Security Number
    - Bank Card Numbers
    - Belgium eID
    - ...
  - Custom Info Types
    - Own Regular Expression definition
    - Keywords
    - Dictionaries

Microsoft 365

### Confidence levels



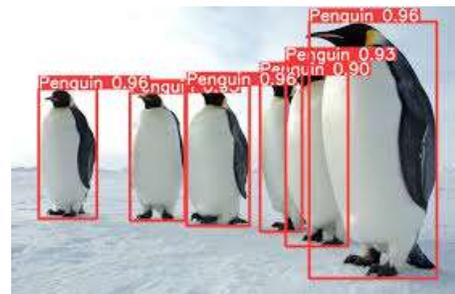
IN-CRAM i CLOUD

65

## 3. Trainable Classifiers



- Data that isn't easily identified
  - by Manual Categorizing
  - by Automated Pattern-matching (Sensitive Information Types)
- Search content by giving similar samples
  - Give multiple similar samples
  - Narrow your search by giving more samples
  - Train the system to detect that kind of data



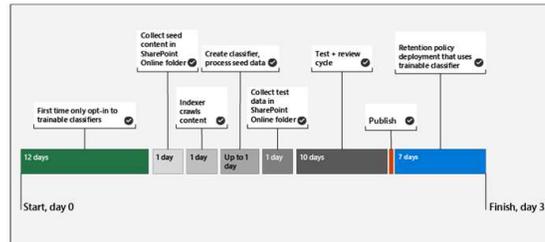
IN-CRAM i CLOUD

66

## Different Trainable Classifiers



- Two Types
  - Pre-trained classifiers
    - Discrimination
    - Financial Audit Reports
    - Harrassment
    - Healthcare
    - ...
  - Custom trainable classifiers
    - Create your own Classifiers
    - Feed examples that are definitely in the category
    - Sort out :
      - True Positives
      - True Negatives
      - False Positives
      - False Negatives



True Positive	False Positive
False Negative	True Negative

INTEGRAM CLOUD

67

## What are Sensitivity Labels ?



- Metadata Written into document Files
- Travels with the document as it moves
- In clear text so that other systems such as a DLP engine can read it
- Used for the purpose of applying a protection action or data governance action – determined by a policy
- Can be customized per the organization's needs



INTEGRAM CLOUD

68

## Default Sensitivity Labels



- **Non-Business** data which does not belong to Contoso. Data is not encrypted and cannot be tracked or revoked. Do not use Non-Business to classify any personal data which is collected by or which belongs to Contoso. Such content should be classified as either Confidential or Highly Confidential.
- **Public** To be used for business data specifically prepared and approved for public consumption. Data is not Encrypted and owners cannot track or revoke content using AIP.
- **General** To be used for business data which is NOT meant for public consumption. However, this can be shared with internal employees, business guests and external partners as needed. Data is not Encrypted and owners cannot track or revoke content using AIP. This is default label.
- **Confidential** To be used on sensitive business data which could cause business harm if over-shared. Recipients (see table above) are trusted and get full delegation rights (including the ability to remove the Encryption). Data is protected using AIP and owners can track and revoke content.
- **Highly Confidential** To be used on very sensitive business data which would certainly cause business harm if over-shared. Recipients do NOT get delegation rights (or rights to modify or remove the Encryption). Data is protected using AIP and owners can track and revoke content.

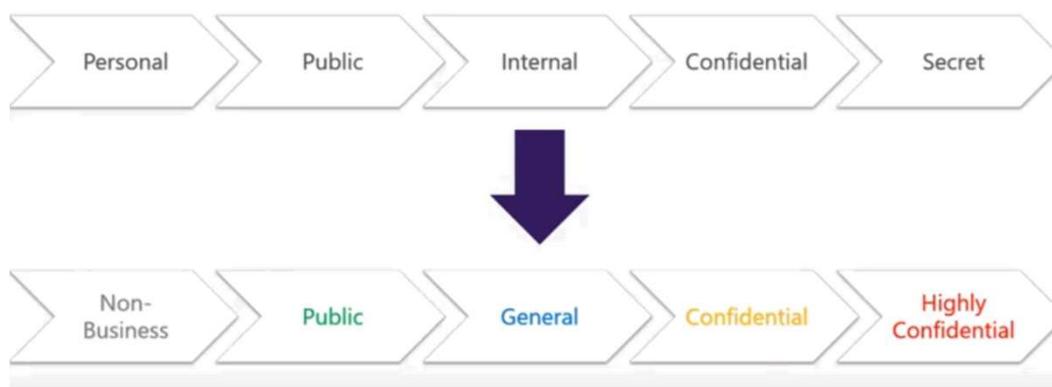
INTEGRAM CLOUD

69

## Microsoft New Default Taxonomy Labels



Starting April 2019



INTEGRAM CLOUD

70

## Configuring Sensitivity Labels



- Name
- Scope (Files, Emails, Teams, Sharepoint, PC)
- Protection (Encryption, Visual Marking)
- Permissions (Read, Write, Delete, Print)
- Auto-labeling settings
- Visual Marking (watermark / header / footer)
- Conditions
  - Sensitive info types
  - Trainable classifiers

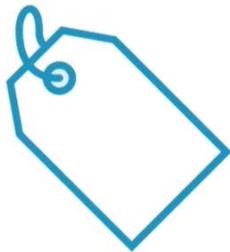
### Edit sensitivity label

- Name & description
- Scope**
- Files & emails
- Groups & sites
- Finish

INTEGRAM CLOUD

71

## Label Settings



Common

Name



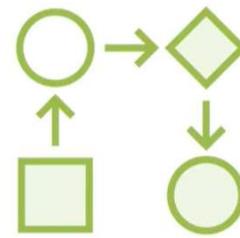
Visual Marking

Visual existence of Label



Protection

Encryption



Conditions

Automatic Labeling

INTEGRAM CLOUD

72

## Visual Markings



- Watermark – Header – Footer Added



73

## Benefits of labeling



- A label travels with the data
- Labels can be applied automatically based on Sensitive Info Types



INGRAM CLOUD

74

## Other Possible Sensitivity Labels

- L1 PUBLIC
- L2 RESTRICTED
- L3 CONFIDENTIAL
- L4 SECRET

- PUBLIC
- INTERNAL
- CONFIDENTIAL
- SECRET

- PUBLIC
- INTERNAL
- CONFIDENTIAL
- STRICTLY CONFIDENTIAL

- PUBLIC
- INTERNAL
- CONFIDENTIAL

- INTERNAL
- CONFIDENTIAL
- SECRET

- OFFICIAL
- SECRET
- TOP SECRET



75

## Sub-Labels

- Within a label you can create sublabels
- Users can select just one label at a time for each document
- Sub-Labels can only go One-Level deep !
- Labels and Sub-Labels have a priority order

LABEL DISPLAY NAME

- Personal
- General
- Internal
- Confidential - All Employees
- DiegoOnly
- Contoso Internal
- Highly Confidential



76

# Dynamic Marking



Variable	Description	Example when label applied
<code>\$(Item.Label)</code>	Current label display name	General
<code>\$(Item.Name)</code>	Current file name or email subject	Sales.docx
<code>\$(Item.Location)</code>	Current path and file name of the document, or the email subject for an email	\\Sales\2020\Q3\Report.docx
<code>\$(User.Name)</code>	Current user display name	Richard Simone
<code>\$(User.PrincipalName)</code>	Current user Azure AD user principal name (UPN)	rsmione@contoso.com
<code>\$(Event.DateTime)</code>	Current date and time for the local time zone	8/10/2020 1:30 PM

INCRAM CLOUD

77

Journey to the Cloud

# LAB 2

## SENSITIVITY LABELS AND POLICIES

INCRAM CLOUD

78



# Module 3 : Unified Labeling

**INGRAM MICRO** CLOUD

79

## ***Labeling Client for Office Apps***

- You can label your office documents using:
  - AIP Unified Labeling Add-in for Office Applications
    - Does exist already multiple years
    - Deprecated in 2024
    - Built-in client disabled when AIP Client is installed (Registry Key)
  - Built-In labeling
    - More stability
    - Better performance
    - Latest Purview Features
    - Labeling technology extends across platforms (Windows, macos, IOS, Android, Web)

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-aip?view=o365-worldwide>

80

## ***Built-In Labeling Client***

- You need to deploy Office 365 as a Subscription Edition
  - For example Microsoft 365 Apps for Enterprise or Microsoft 365 Apps for Business
- Built-In labeling is not available with Standalone editions (Office Perpetual)
- Look and feel of labeling is different
- Only for labeling Office Documents & Emails
  - Word, Excel, Powerpoint, Outlook
- Supported on Windows, macOS, iOS, Android and Office Web Applications

81

## ***AIP Unified Labeling Client***

- Contains the following capabilities & components :
  - AIP Unified labeling Add-In for Office apps in Windows (retirement April 11, 2024)
  - AIP Viewers on Windows / iOS / Android
  - AIP PowerShell extension
  - Right-click Classify & Protect (File Explorer support)
  - AIP Scanner
  - Can Label / Encrypt other document types as well
  - Download link :
    - <https://www.microsoft.com/en-us/download/details.aspx?id=53018>

Verify that the Outlook client is using built-in labeling. To do this, check the following registry subkey on the client computer:

```
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Security\Labels
```

If the registry subkey is present, and the `UseOfficeForLabeling` value is set to 0, this indicates that Outlook is using the AIP client instead of the built-in support for sensitivity labels. In this case, set the `UseOfficeForLabeling` value to 1 so that Outlook uses the built-in support for sensitivity labels.

82

## ***Office 365 File Type Supported Classification & Protection***

.doc	.potx	.vsdm	.xlsb
.docm	.pps	.vsdx	.xlt
.docx	.ppsm	.vssm	.xlsm
.dot	.ppsx	.vssx	.xlsx
.dotm	.ppt	.vstm	.xltm
.dotx	.pptm	.vstx	.xltx
.potm	.pptx	.xls	.xps

83

## ***Other File Type Supported Classification & Protection***

Original file name extension	Protected file name extension
.bmp	.pbmp
.gif	.pgif
.jif	.pjif
.jpe	.pjpe
.jpeg	.pjpeg
.jpg	.pjpg
.jt	.pjt
.png	.ppng
.tif	.ptif
.tiff	.ptiff
.txt	.ptxt
.xla	.pxla
.xlam	.pxlam
.xml	.pxml

84

# File Type Classification

- 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	.xlsb
.dot	.ppsx	.vss	.xlt
.dotm	.ppt	.vssm	.xlsm
.dotx	.pptm	.vst	.xlsx
.potm	.pptx	.vstm	.xltn
	.vdw	.vssx	.xltx

<https://learn.microsoft.com/en-us/azure/information-protection/rms-client/client2-admin-guide-file-types>

85

## Sensitive Info Types



- Two Types
  - Preset Information Types
    - Social Security Number
    - Bank Card Numbers
    - Belgium eID
    - ...
  - Custom Info Types
    - Own Regular Expression definition
    - Keywords
    - Dictionaries

86

## Custom Info Types



Choose the type of condition ⓘ

Information Types **Custom**

\* Name

ABC Corp Customer Number ✓

\* Match exact phrase or pattern ⓘ

\s[A-Z]{2}-[0-9]{5}\s ✓

Same regular expression  
as the custom sensitive  
information type

Match as a regular expression

Off **On** ★

Match with case sensitivity

Off **On**

\* Minimum number of occurrences

1

Count occurrences with unique values only

Off **On**

INCRAMI CLOUD

87

## Regular Expressions



- [a-z] Any lowercase Letter
- [a-z0-9] Any Number or lowercase Letter
- \. Escape character for special characters . ( ) [ ] ^ \$
- \.? A point can follow but do not need to follow
- a{1,9} Preceding character minimum 1x, maximum 9x
- . Any character
- \d decimal character 0-9
- (?ab|cd|ef) ab or cd or ef
- \s whitespace

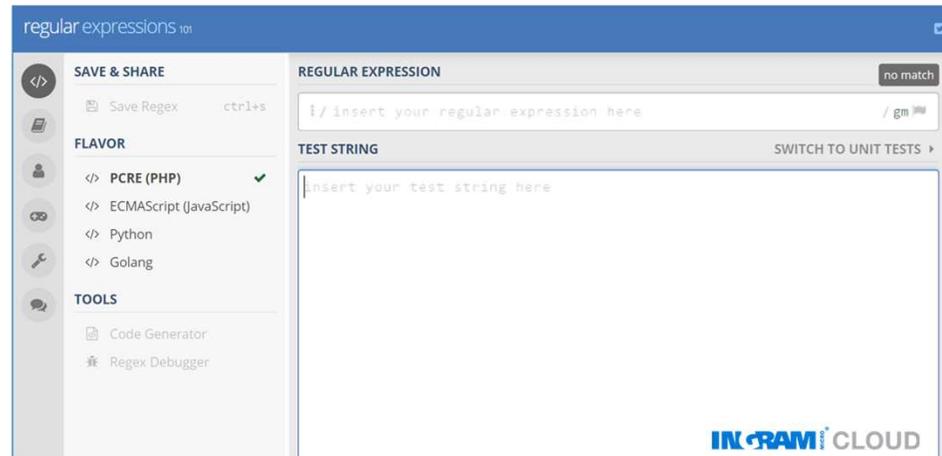
INCRAMI CLOUD

88

## Test your Regular Expressions



- <https://regex101.com>



89

## Examples Pre-trained classifiers



- Resumes (overview of accounts, profession, qualification, experience)
- Source Code (C#, C++, Java, Perl, Python, ...)
- Harassment (offensive language, religion, gender, sexual orientation)
- Profanity (offensive language, embarrassing people)
- Threat (offensive language, physical harm, damage)

<https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about?view=o365-worldwide>

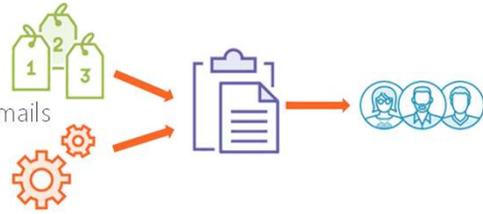
INGRAM CLOUD

90

## Label Policies (Publishing Labels)



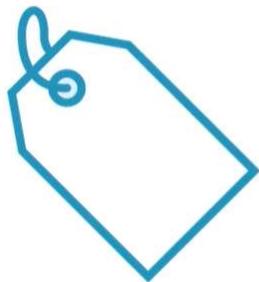
- A Group of Labels and Label Settings pushed to a group of Users or all Users is called a Policy
- A Policy contains :
  - Labels
    - Apply Classification Value to documents and Emails
    - Labels are part of a specific Policy
  - Settings
    - Change the Default behavior of the AIP Client
- A Policy is assigned to Users, Groups of Users, All Users



INCRAMI CLOUD

91

## Policy Components



Common  
Name



Groups and  
Users



Labels



Global  
Overrides

INCRAMI CLOUD

92



Journey to the Cloud

# LAB 3

UNIFIED LABELING AGENT  
CUSTOM INFO TYPES



**INTEGRAM** CLOUD

93



Journey to the Cloud

# Prevent Data Loss



**KNOW YOUR DATA**  
Understand your data landscape and identify important data across your hybrid environment

**PREVENT DATA LOSS**  
Detect risky behavior and prevent accidental oversharing of sensitive information

**PROTECT YOUR DATA**  
Apply flexible protection actions including encryption, access restrictions and visual markings

**GOVERN YOUR DATA**  
Automatically retain, delete, and store data and records in a compliant manner

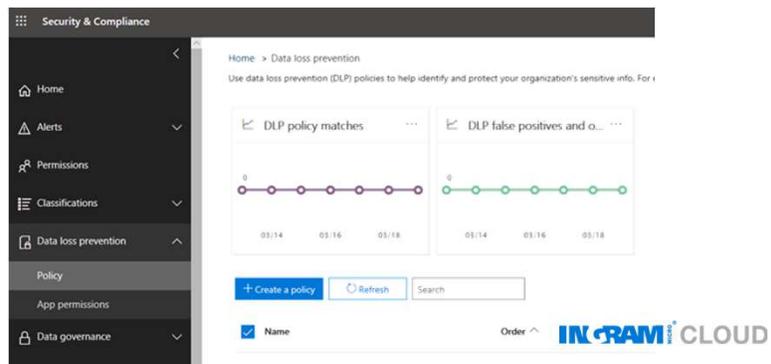
**INTEGRAM** CLOUD

94

## Data Loss Prevention



- Identify sensitive information
- Prevent the accidental sharing
- Monitor and protect sensitive information



95

## Reuse Sensitive Information Types



- Use the same sensitive information types as in AIP

Sensitive information types (81)	
<input type="checkbox"/> Name	Publisher
<input type="checkbox"/> ABA Routing Number	Microsoft Corporation
<input type="checkbox"/> Argentina National Identity (DNI) Number	Microsoft Corporation
<input type="checkbox"/> Australia Bank Account Number	Microsoft Corporation
<input type="checkbox"/> Australia Driver's License Number	Microsoft Corporation
<input type="checkbox"/> Australia Medical Account Number	Microsoft Corporation
<input type="checkbox"/> Australia Passport Number	Microsoft Corporation
<input type="checkbox"/> Australia Tax File Number	Microsoft Corporation
<input type="checkbox"/> Belgium National Number	Microsoft Corporation
<input type="checkbox"/> Brazil CPF Number	Microsoft Corporation
<input type="checkbox"/> Brazil Legal Entity Number (CNPJ)	Microsoft Corporation
<input type="checkbox"/> Brazil National ID Card (RG)	Microsoft Corporation

INGRAM CLOUD

96

# DLP Configuration



- Rules
  - Protect your Data
- Conditions
  - When ?
- Actions
  - How ?
- Locations
  - Exchange Online
  - OneDrive
  - SharePoint
  - Teams
  - ...

**INCRAM** CLOUD

97

# DLP Location Configuration

Choose locations

Status	Location	Include	Exclude
<input checked="" type="checkbox"/>	Exchange email	All <a href="#">Choose distribution groups</a>	None <a href="#">Exclude distribution groups</a>
<input checked="" type="checkbox"/>	SharePoint sites	All <a href="#">Choose sites</a>	None <a href="#">Exclude sites</a>
<input checked="" type="checkbox"/>	OneDrive accounts	All <a href="#">Choose accounts</a>	None <a href="#">Exclude accounts</a>
<input checked="" type="checkbox"/>	Teams chat and channel messages	All <a href="#">Choose accounts</a>	None <a href="#">Exclude accounts</a>

**INCRAM** CLOUD

98

## New DLP Locations in 2020



<input checked="" type="checkbox"/> On	Exchange email	All	Choose distribution group
<input checked="" type="checkbox"/> On	SharePoint sites	All	Choose sites
<input checked="" type="checkbox"/> On	OneDrive accounts	All	Choose account
<input checked="" type="checkbox"/> On	Teams chat and channel messages	All	Choose account
<input checked="" type="checkbox"/> On	Devices	All	Choose user or group
<input type="checkbox"/> Off	Microsoft Cloud App Security		

INCRAM CLOUD

99

## Data Loss Prevention for Endpoints



- Available in Plan 2 Bundles
- Protect Documents on the Device

INCRAM CLOUD

100

## New DLP Locations in 2021

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> On	Exchange email	All Choose distribution group	None Exclude distribution group
<input checked="" type="checkbox"/> On	SharePoint sites	All Choose sites	None Exclude sites
<input checked="" type="checkbox"/> On	OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group
<input checked="" type="checkbox"/> On	Teams chat and channel messages	All Choose account or distribution group	None Exclude account or distribution group
<input checked="" type="checkbox"/> On	Devices	All Choose user or group	None Exclude user or group
<input checked="" type="checkbox"/> On	Microsoft Cloud App Security	All Choose instance	None Exclude instance
<input checked="" type="checkbox"/> On	On-premises repositories	All Choose repositories	None Exclude repositories




101

## DLP Locations 2022

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> On	Exchange email	All Choose distribution group	None Exclude distribution group
<input checked="" type="checkbox"/> On	SharePoint sites	All Choose sites	None Exclude sites
<input checked="" type="checkbox"/> On	OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group
<input checked="" type="checkbox"/> On	Teams chat and channel messages	All Choose account or distribution group	None Exclude account or distribution group
<input checked="" type="checkbox"/> On	Devices	All Choose user or group	None Exclude user or group
<input checked="" type="checkbox"/> On	Microsoft Defender for Cloud Apps	All Choose instance	None Exclude instance
<input checked="" type="checkbox"/> On	On-premises repositories	All Choose repositories	None Exclude repositories
<input type="checkbox"/> Off	Power BI (preview)		

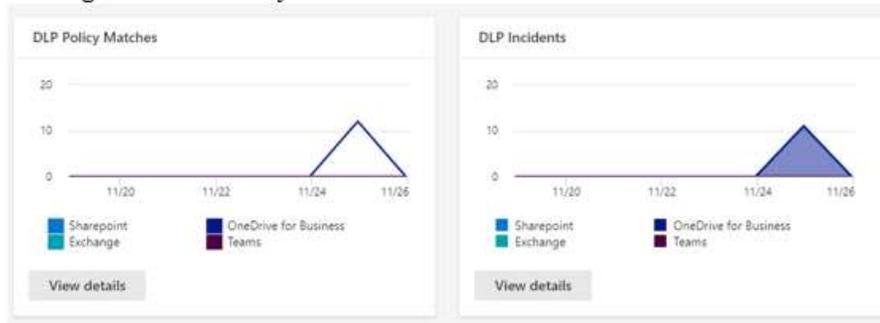



102

# DLP Notifications & Alerts



- <https://compliance.microsoft.com>



INCRAM CLOUD

103

Journey to the Cloud

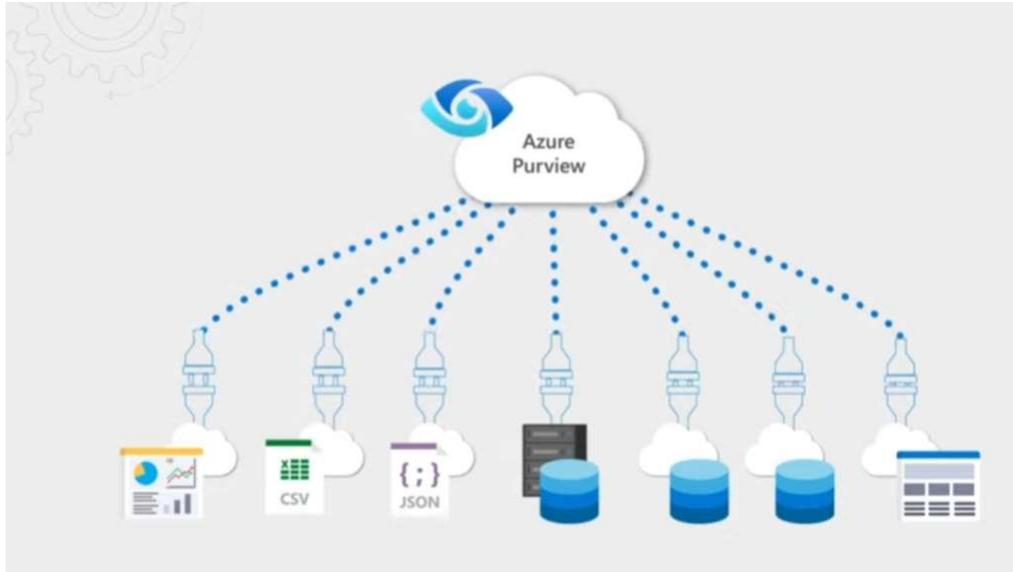
# LAB 4

MODULE 4 : DATA LOSS PREVENTION (DLP)

INCRAM CLOUD

104

# Connecting to different data sources

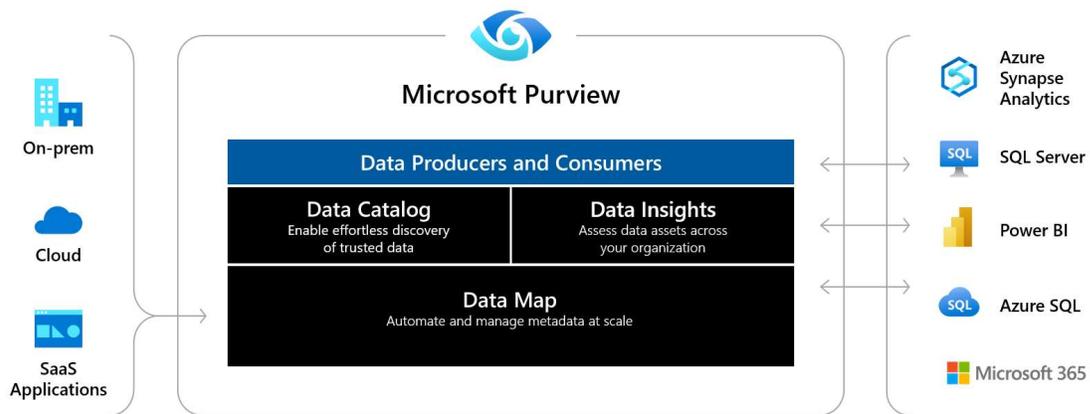


INTEGRATE MICROSOFT CLOUD > Move as a Service

105

105

# Microsoft Purview Roadmap

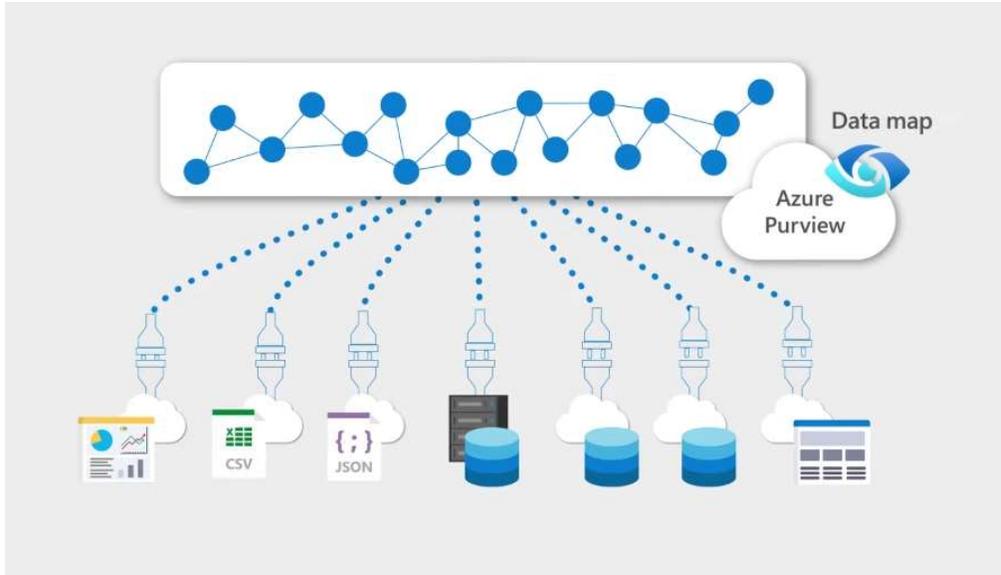


INTEGRATE MICROSOFT CLOUD > Move as a Service

106

106

## Microsoft Purview Data map



107

## Microsoft Purview Data Map

- Microsoft Purview Data Map is a metadata store
- Labels are applied to the asset metadata; not applied to the actual files
- Sensitivity labels don't modify your files and databases
- Labels are applied to the Asset Metadata



108

# Microsoft Purview Data Map Preview



Create labels



Register asset



Scan asset



Classifications found



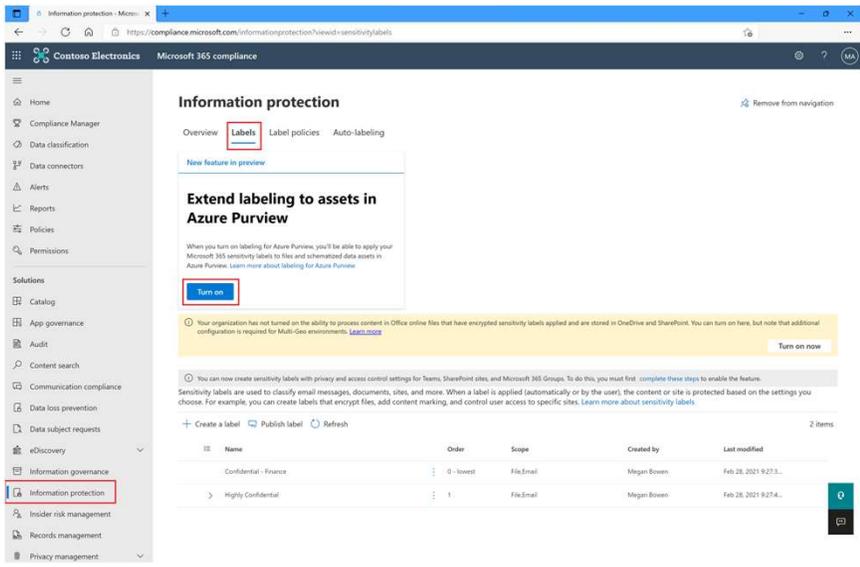
Labels applied

Data type	Sources
Automatic labeling for files	<ul style="list-style-type: none"> <li>- Azure Blob Storage</li> <li>- Azure Files</li> <li>- Azure Data Lake Storage Gen 1 and Gen 2</li> <li>- Amazon S3</li> </ul>
Automatic labeling for schematized data assets	<ul style="list-style-type: none"> <li>- SQL server</li> <li>- Azure SQL database</li> <li>- Azure SQL Database Managed Instance</li> <li>- Azure Synapse Analytics workspaces</li> <li>- Azure Cosmos Database (SQL API)</li> <li>- Azure database for MySQL</li> <li>- Azure database for PostgreSQL</li> <li>- Azure Data Explorer</li> </ul>

109


109

# Extend labeling to assets Preview



110


110

## ***Limitations of MS Purview Data Maps***

- Data Maps supports automatic labeling only
- Manual applying a label to a Data Map is not possible
- Scanning for credentials is not supported
- Data Maps does not support encryption (only Metadata)
- Microsoft Purview Data Map does not currently provide DLP capabilities
- Trainable Classifiers are not supported yet

111

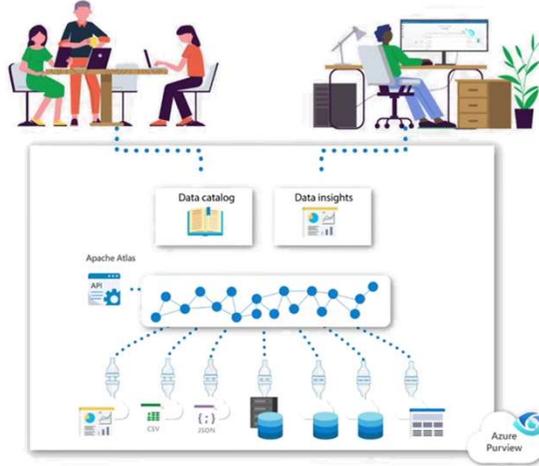
## ***Licensing***

- Microsoft Purview Data Map :
  - Microsoft 365 E5/A5
  - Office 365 E5

112

# Microsoft Purview Data Catalog

- Spend less time looking for data
- Have more time getting value of your data
- Create insights into data sets



- <https://aka.ms/AzurePurview>
- <https://azure.microsoft.com/en-us/services/data-catalog/>

INGRAM MICRO CLOUD Move as a Service

113

113



Journey to the Cloud

## Govern your Data

Understand your data landscape and identify important data across your hybrid environment

KNOW YOUR DATA

Detect risky behavior and prevent accidental oversharing of sensitive information

PREVENT DATA LOSS

Apply flexible protection actions including encryption, access restrictions and visual markings

PROTECT YOUR DATA

Automatically retain, delete, and store data and records in a compliant manner

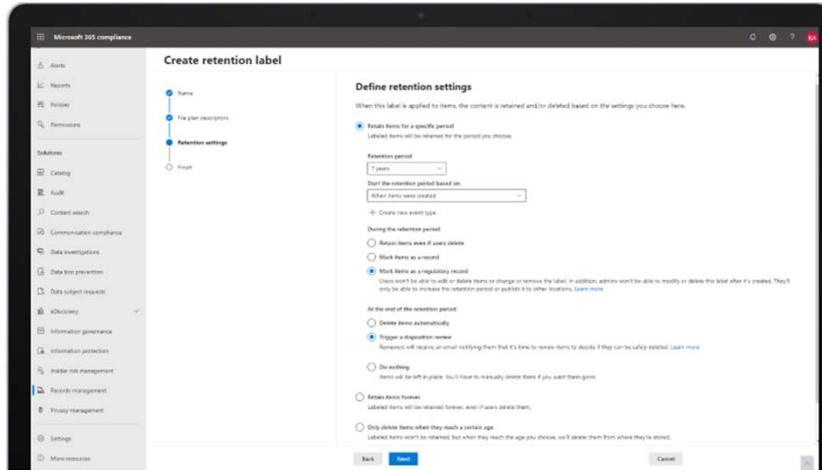
GOVERN YOUR DATA



114

57

# Microsoft Information Governance



INCRAM CLOUD

115

# Records Management



- <https://compliance.microsoft.com/recordsmanagement>
- Intelligent Classification
- Regulations
- Corporate Policies

### Information protection & governance

Classify, protect, and retain your data where it lives and wherever it goes.



### Data loss prevention

Detects sensitive content as it's used and shared throughout your organization, in the cloud and on devices, and helps prevent accidental data loss.



### Information governance

Manages your content lifecycle using solutions to import, store, and classify business-critical data so you can keep what you need and delete when you don't.



### Information protection

Discovers, classifies, and protects sensitive and business-critical content throughout its lifecycle across your organization.



INCRAM CLOUD

116

## Retention Labels



- Retention labels for different types of content
- Compare with Sensitivity Labels

<input type="checkbox"/> Name	Created by	Retention period
<input type="checkbox"/> PII Retention Policy	Megan Bowen	7 years
<input type="checkbox"/> Medical Records Retention Policy	Megan Bowen	7 years
<input type="checkbox"/> Product Retired	Megan Bowen	10 years
<input type="checkbox"/> Employee Records	Megan Bowen	Forever
<input type="checkbox"/> Personal Financial PII	Megan Bowen	3 years
<input type="checkbox"/> Private	Megan Bowen	5 years

INCRAM CLOUD

117

## Retention Policies



- Data is increasing daily
  - Comply with industry regulations
  - Comply with internal policies
  - Reduce risk of security breach
  - Share knowledge effectively
- Retaining
  - Content can't be permanently deleted before ...
- Deleting
  - Content permanently delete at the end of ...

INCRAM CLOUD

118

## Retention Actions



- Retain Only
- Delete Only
- Retain and Delete

INCRAMI CLOUD

119

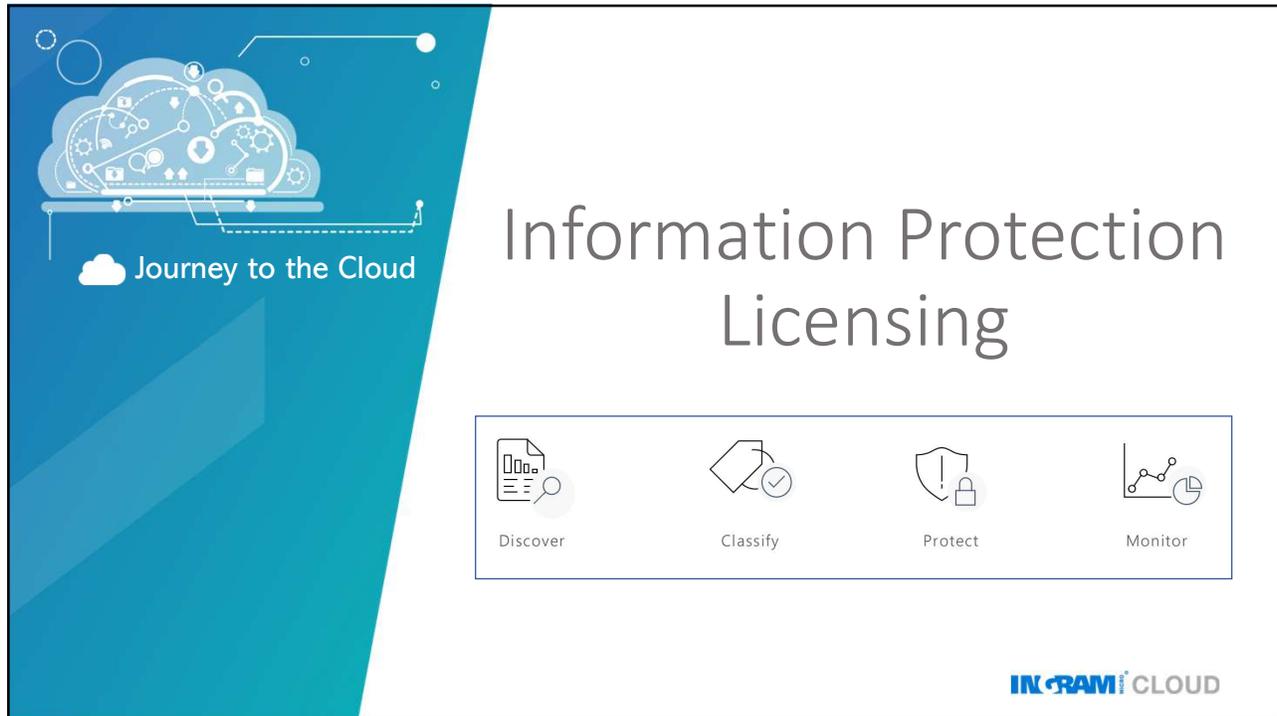
## Apply Retention Policies



- Exchange email
- SharePoint site
- OneDrive accounts
- Microsoft 365 Groups
- Skype for Business
- Exchange public folders
- Teams channel messages
- Teams chats
- Yammer community messages
- Yammer private messages

INCRAMI CLOUD

120



**Journey to the Cloud**

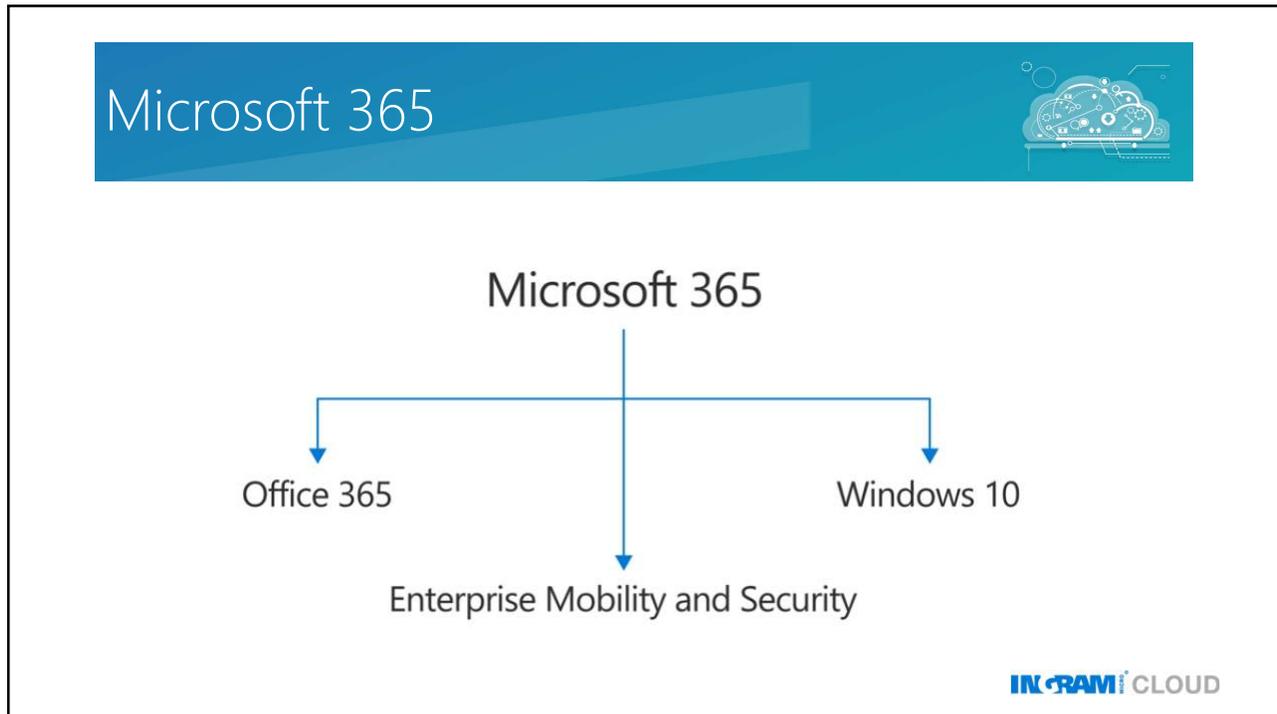
# Information Protection Licensing

Discover    Classify    Protect    Monitor

**INTEGRAM** CLOUD

This slide features a blue header with a cloud icon and the text 'Journey to the Cloud'. The main title is 'Information Protection Licensing'. Below the title is a horizontal bar containing four icons and their corresponding labels: a document icon for 'Discover', a document with a checkmark for 'Classify', a shield with a lock for 'Protect', and a line graph for 'Monitor'. The INTEGRAM CLOUD logo is in the bottom right corner.

121



## Microsoft 365

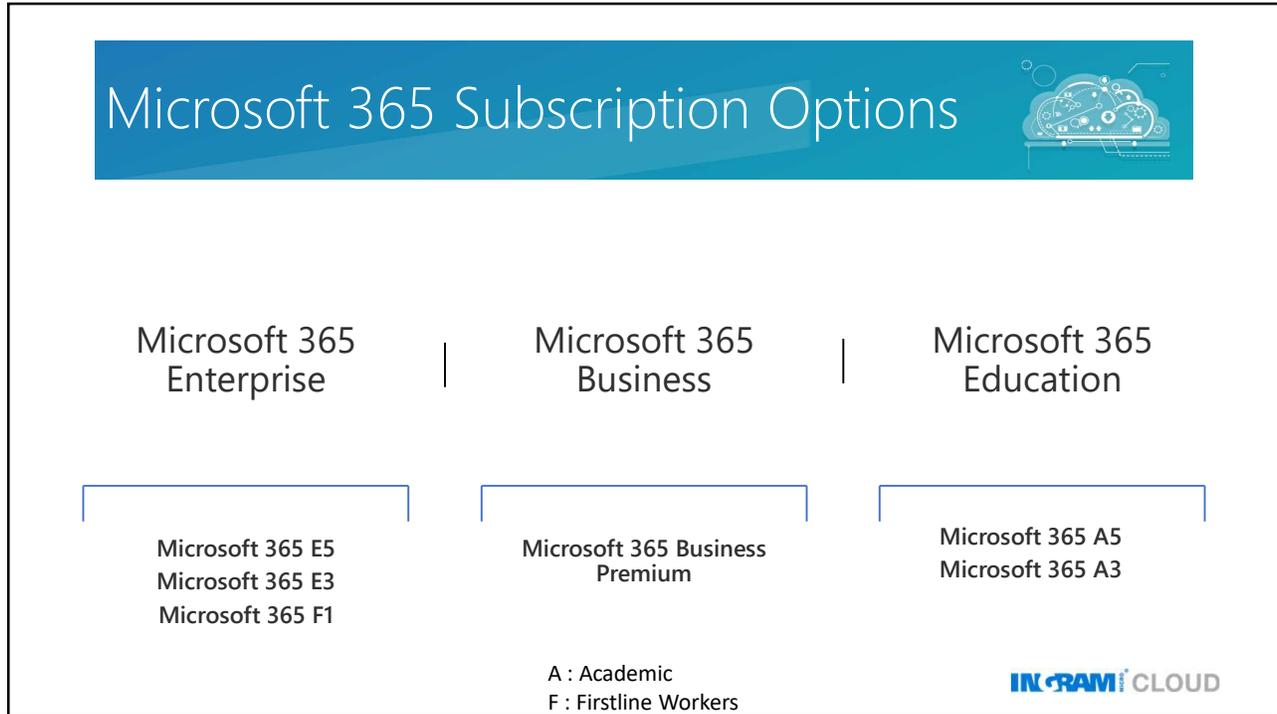
Office 365    Enterprise Mobility and Security    Windows 10

**INTEGRAM** CLOUD

This slide has a blue header with the text 'Microsoft 365' and a cloud icon. Below the header is a diagram showing 'Microsoft 365' at the top, with three arrows pointing down to 'Office 365', 'Enterprise Mobility and Security', and 'Windows 10'. The INTEGRAM CLOUD logo is in the bottom right corner.

122

# Microsoft 365 Subscription Options



The diagram shows three main categories of Microsoft 365 subscriptions: Enterprise, Business, and Education. Each category has a list of specific plans below it. The Enterprise category includes E5, E3, and F1. The Business category includes Business Premium. The Education category includes A5 and A3. A legend at the bottom indicates that 'A' stands for Academic and 'F' for Firstline Workers. The INGRAM CLOUD logo is in the bottom right corner.

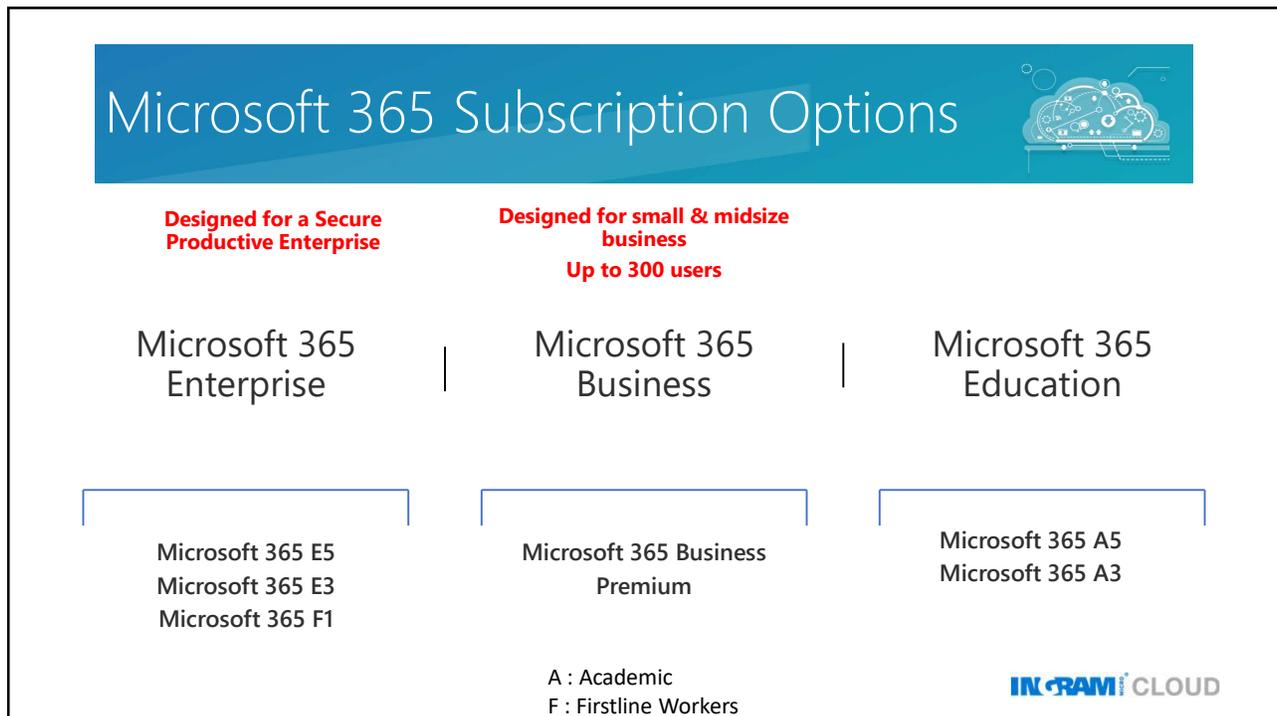
Microsoft 365 Enterprise	Microsoft 365 Business	Microsoft 365 Education
<ul style="list-style-type: none"> <li>Microsoft 365 E5</li> <li>Microsoft 365 E3</li> <li>Microsoft 365 F1</li> </ul>	<ul style="list-style-type: none"> <li>Microsoft 365 Business Premium</li> </ul>	<ul style="list-style-type: none"> <li>Microsoft 365 A5</li> <li>Microsoft 365 A3</li> </ul>

A : Academic  
F : Firstline Workers

INGRAM CLOUD

123

# Microsoft 365 Subscription Options



This diagram is similar to the one on page 123 but includes additional descriptive text for the Enterprise and Business categories. The Enterprise category is described as 'Designed for a Secure Productive Enterprise'. The Business category is described as 'Designed for small & midsize business' and 'Up to 300 users'. The Education category remains the same. The legend and INGRAM CLOUD logo are also present.

Microsoft 365 Enterprise	Microsoft 365 Business	Microsoft 365 Education
<p><b>Designed for a Secure Productive Enterprise</b></p> <ul style="list-style-type: none"> <li>Microsoft 365 E5</li> <li>Microsoft 365 E3</li> <li>Microsoft 365 F1</li> </ul>	<p><b>Designed for small &amp; midsize business</b> <b>Up to 300 users</b></p> <ul style="list-style-type: none"> <li>Microsoft 365 Business Premium</li> </ul>	<ul style="list-style-type: none"> <li>Microsoft 365 A5</li> <li>Microsoft 365 A3</li> </ul>

A : Academic  
F : Firstline Workers

INGRAM CLOUD

124

## Enterprise Mobility + Security



- Bundles five products
  - Entra ID
  - Microsoft Intune
  - Information Protection
  - Microsoft Cloud App Security
  - Advanced Threat Analytics

**INTEGRAM** CLOUD

125

## EnterPrise Mobility & Security Suites



- EM + S E5
- EM + S E3

BENEFIT / EM+S SKU	Identity & access management	Managed mobile productivity	Information protection	Identity-driven security
<b>EM+S E5</b>	Azure Active Directory Premium P2	Microsoft Intune	Azure Information Protection Premium P2	Microsoft Cloud App Security
<b>EM+S E3</b>	Azure Active Directory Premium P1	Microsoft Intune	Azure Information Protection Premium P1	Microsoft Advanced Threat Analytics

**INTEGRAM** CLOUD

126

# Microsoft 365 E3, E5, E5 Security, E5 Compliance



Information protection	Microsoft 365			
	E3	E5	E5 Security <sup>2</sup>	E5 Compliance <sup>1</sup>
Azure Information Protection Plan 1	•			•
Azure Information Protection Plan 2		•		•
Manual, default, and mandatory sensitivity labeling in Microsoft 365 apps	•	•		
Automatic sensitivity labeling in Microsoft 365 apps		•		•
Manual sensitivity labeling for Teams meetings <sup>2</sup>		•		•
Manual labeling with the AIP app and plugin	•	•		
Automatic labeling in the AIP plugin		•		•
Default sensitivity labels for SharePoint document libraries		•		•
Automatic sensitivity labels in Exchange, SharePoint, and OneDrive		•		•
Sensitivity labels based on Machine Learning/Trainable Classifiers/Exact Data Match		•		•
Sensitivity labeling for containers in Microsoft 365	•	•		
Basic Message Encryption	•	•		
Advanced Message Encryption		•		
Customer Key		•		
Personal Data Encryption	•	•		

Description	SKU	PFAM	License/Device		
			Pool	Buy	1M Subscr
M365 E5 IP & Govern Sub Per User	1C9-00002	M365 E5 IP & Govern	SER		5.57

**IPG SKU Information Protection & Governance**



127

# IPG E5 or IPG F5



Security and compliance	+ = Can be added N/A = Not available			
	E3	E5	F1	F3
Microsoft 365 E5 Security	+	•	N/A	N/A
Microsoft 365 E5 Compliance	+	•	N/A	N/A
Microsoft 365 E5 Info Protection and Governance	+	•	N/A	N/A
Microsoft 365 E5 Insider Risk Management	+	•	N/A	N/A
Microsoft Purview Insider Risk Management forensic evidence <sup>15</sup>	N/A	+	N/A	N/A
Microsoft 365 E5 eDiscovery and Audit	+	•	N/A	N/A
Microsoft 365 F5 Security	N/A	N/A	+	+
Microsoft 365 F5 Compliance	N/A	N/A	+	+
Microsoft 365 F5 Security + Compliance	N/A	N/A	+	+
Microsoft 365 F5 Info Protection and Governance	N/A	N/A	+	+
Microsoft 365 F5 Insider Risk Management	N/A	N/A		
Microsoft 365 F5 eDiscovery and Audit	N/A	N/A		
Microsoft Defender for Identity	+	•		



128

# IPG E5 SKU + Business Premium





## Supplemental Licenses for Small and Medium-sized Businesses

+ = Included  
 + = Can be added  
 N/A = Not available

	Microsoft Teams Essentials <sup>1</sup>	Microsoft 365 Business		
		Basic	Standard	Premium
<b>Security and Compliance</b>				
Microsoft 365 E5 Info Protection and Governance	N/A	+ <sup>1</sup>	+ <sup>1</sup>	+ <sup>2</sup>
Microsoft 365 E5 Insider Risk Management	N/A	+	+	+
Microsoft 365 E5 eDiscovery and Audit	N/A	+	+	+
Microsoft Defender for Business	N/A	+ <sup>3</sup>	+ <sup>3</sup>	+ <sup>3</sup>
Microsoft Defender for Business servers add-on for Microsoft Defender for Business	N/A	+ <sup>3</sup>	+ <sup>3</sup>	+ <sup>3</sup>
Microsoft Defender for Identity	N/A	+	+	+
Microsoft Defender for Office 365 Plan 1	N/A	+	+	+
Microsoft Defender for Office 365 Plan 2	N/A	+	+	+
Microsoft Defender for Cloud Apps	N/A	+	+	+
App governance add-on for Microsoft Defender for Cloud Apps	N/A	+ <sup>2</sup>	+ <sup>2</sup>	+ <sup>2</sup>
Microsoft Defender for Endpoint Plan 1	N/A	+	+	+
Microsoft Defender for Endpoint Plan 2	N/A	+	+	+
Premium Assessments add-on for Compliance Manager <sup>4</sup>	N/A	+	+	+
Azure Active Directory Premium Plan 1	N/A	+	+	+
Azure Active Directory Premium Plan 2	N/A	+	+	+
Microsoft Intune	N/A	+	+	+
Microsoft Purview Data Loss Prevention (for email and files)	N/A	+	+	+
Exchange Archiving	N/A	+	+	+
Microsoft Intune Remote Help	N/A	+ <sup>4</sup>	+ <sup>4</sup>	+

<sup>1</sup> Requires E5D E5 or Azure Information Protection Plan 1, standalone required.  
<sup>2</sup> Requires Microsoft Defender for Cloud Apps.  
<sup>3</sup> Get details for available plans here.  
<sup>4</sup> Requires Microsoft Intune.  
<sup>5</sup> Requires Microsoft Defender for Business or Microsoft 365 Business Premium. Maximum quantity/seat cap is 60 licenses per customer.



129

# Wrap-up



- The Security Opportunity
- Microsoft Information Protection
- Know Your Data
- Protect Your Data
- Prevent Data Loss
- Govern Your Data
- Information Protection Licensing





130



Journey to the Cloud

Thank You !



INGRAM i CLOUD