Implementing Purview Information Protection with the Traffic Light Protocol

TechCon 365 Dallas
November 15, 2024

envision IT

Peter Carson

- President, Envision IT
- 14X Microsoft M365 MVP
- Regular industry speaker
- pcarson@envisionit.com
- blog.petercarson.ca
- envisionit.com
- extranetusermanager.com
- linkedin.com/in/petercarson
- President Toronto SharePoint User Group

3 Key Takeaways

1 Information Protection is something many organizations are licensed for but haven’t implemented.

2 Cybersecurity is not one size fits all. Make your protection appropriate to the content.

3 Copilot Readiness is driving much of this, but safe external sharing is another big driver.

Agenda

- Introductions
- What and Why of Information Protection
- Microsoft Purview
- Traffic Light Protocol
- Implementation
- Summary, Q&A and Closing

Why is Information Protection Important?

- Every organization has different levels of sensitivity of content
- How you manage access to content should be different depending on its sensitivity

Low

- Training with no corporate IP – workplace safety, wellness
- External stakeholder feedback

Medium

- General business data

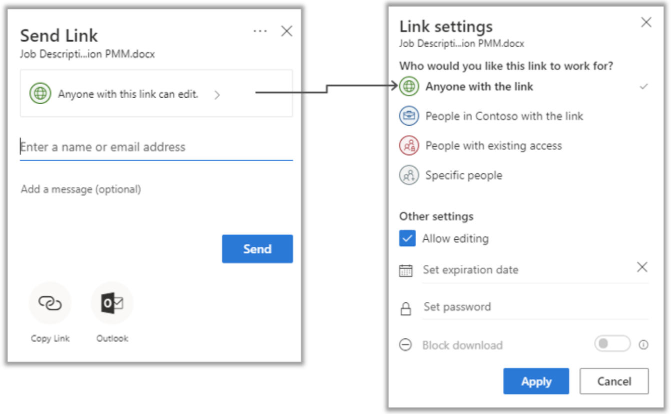
High

- Personal Health Information
- Employee HR data
- Financial data

Key Drivers for Information Protection

Copilot Readiness

External Sharing



Send Link

Job Descripti...ion PMM.docx

Anyone with this link can edit. >

Enter a name or email address

Add a message (optional)

Send

Copy Link

Outlook

Link settings

Job Descripti...ion PMM.docx

Who would you like this link to work for?

- Anyone with the link ✓
- People in Contoso with the link
- People with existing access
- Specific people

Other settings

☑ Allow editing

Set expiration date

Set password

Block download

Apply

Cancel

Cybersecurity

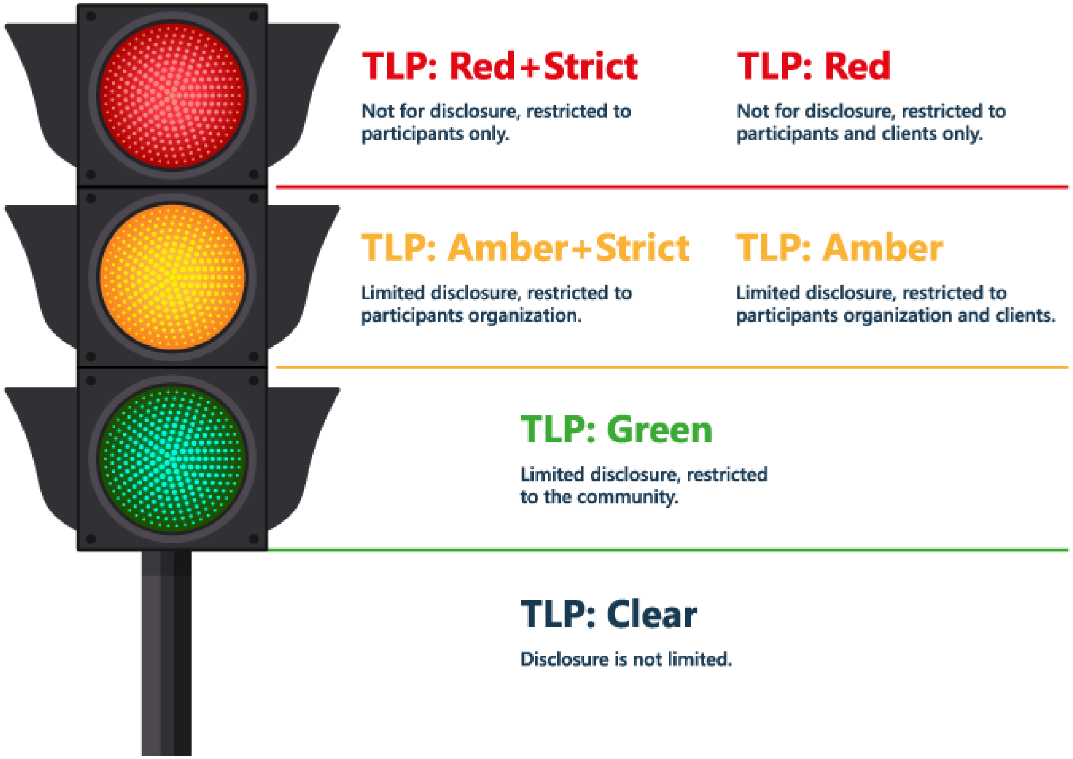
Information Protection

- Data Discovery and Classification
- Sensitivity Labels
- Data Loss Prevention
- AI Powered Classifiers

Data Discovery and Classification

- Identify and classify sensitive data
- Automated scanning, classification, and cataloging of data assets
- Comprehensive platform for data governance across hybrid and multi-cloud environments

Sensitivity Labels



TLP: Red+Strict

Not for disclosure, restricted to participants only.

TLP: Red

Not for disclosure, restricted to participants and clients only.

TLP: Amber+Strict

Limited disclosure, restricted to participants organization.

TLP: Amber

Limited disclosure, restricted to participants organization and clients.

TLP: Green

Limited disclosure, restricted to the community.

TLP: Clear

Disclosure is not limited.

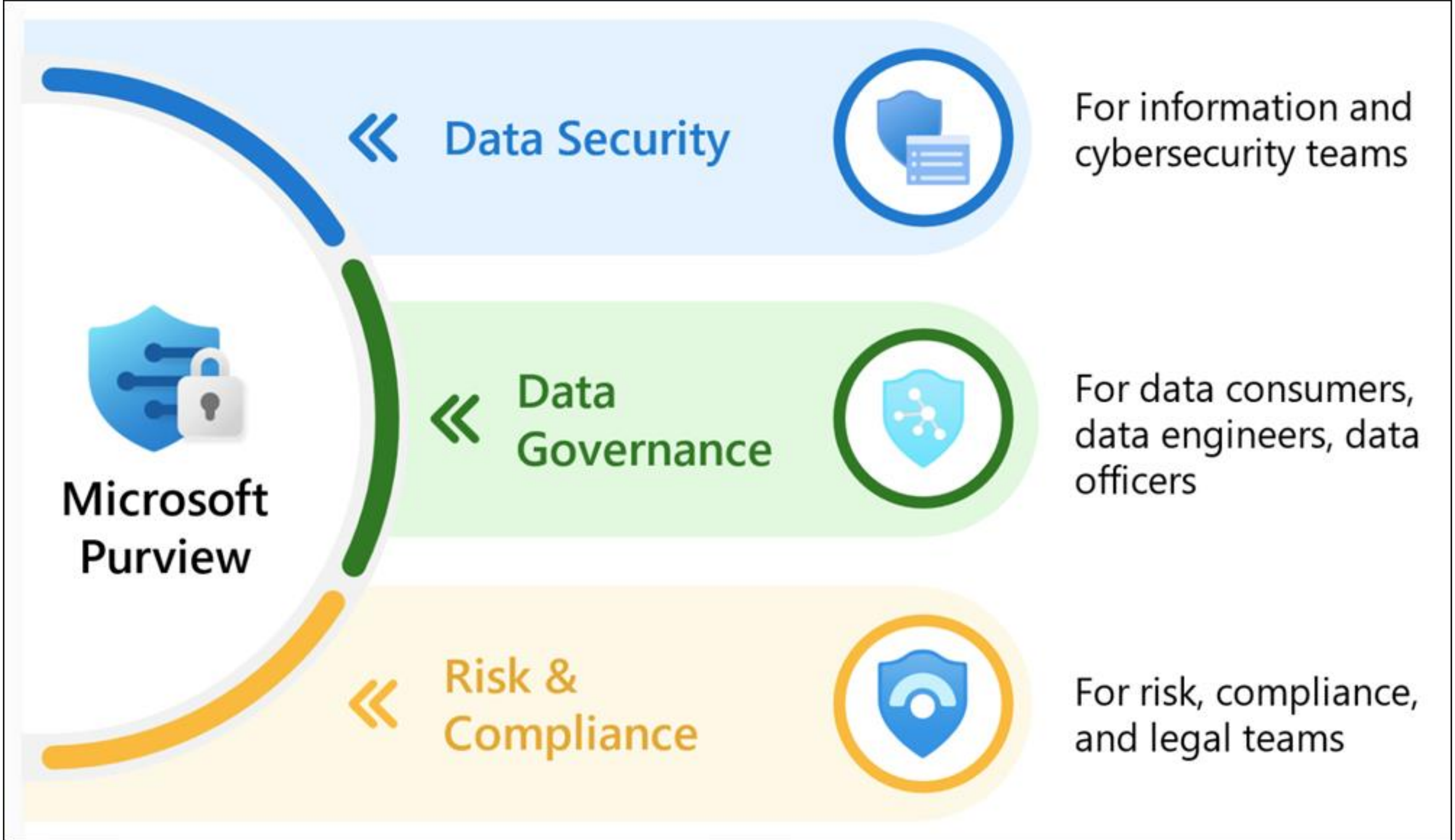
- Apply labels to data to enforce protection policies
- Control how content is handled and shared
- Designed to protect sensitive information

Data Loss Prevention (DLP)

- Prevent data breaches by monitoring and controlling the sharing of sensitive information
- Meet compliance requirements
- Risk management

AI-Powered Classifiers

- Utilize AI to accurately classify data based on content and context
- Enhance the precision of data protection measures
- An emerging technology



Microsoft Purview

Data Security

For information and cybersecurity teams

Data Governance

For data consumers, data engineers, data officers

Risk & Compliance

For risk, compliance, and legal teams

Purview Labels

Retention

- Manage lifecycle of data
- Specify how long content should be kept and then what actions should be taken
- Ensure compliance with regulations and internal policies
- Typically many (could be hundreds) of labels

Sensitivity

- Designed to protect sensitive information
- Classifying and secure
- Control how content is handled and shared
- Small number of labels

Microsoft Purview Information Protection

- Discover, classify, and protect sensitive data
- Data Discovery
  - Identify and classify sensitive data
  - On-premises, in the cloud, or in hybrid environments
- Sensitivity Labels
  - Apply labels to data to enforce protection policies like encryption, access restrictions, and visual markings
- Data Loss Prevention (DLP)
  - Prevent data breaches by using DLP policies to monitor and control the sharing of sensitive information
- AI-Powered Classifiers
  - Use AI to accurately classify data based on content and context, enhancing the precision of data protection measures

Purview Licensing Recommendations

Microsoft licensing is never a simple topic, and Purview is no exception. A few good resources to help navigate this are:

[Microsoft Compliance and Information Protection Licensing Guide]

[All About Microsoft Purview Sensitivity Labels]

[Microsoft 365 Licensing]

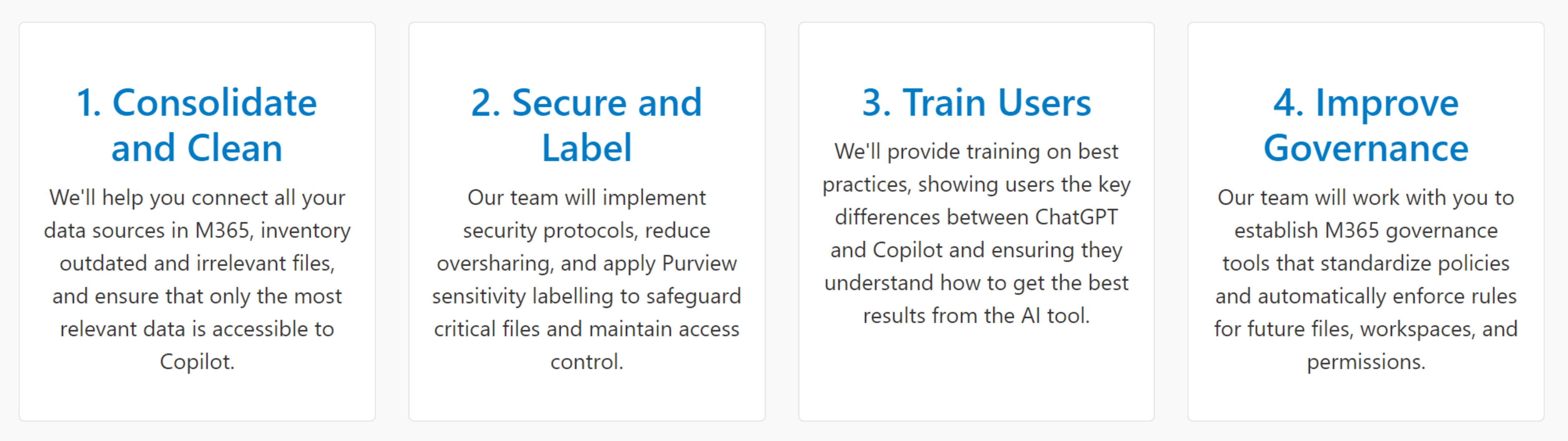
The simple version: users require E3 or above to apply a label manually, while automatic policy-driven application of labels requires E5

Microsoft 365 E3 or E5 compliance licenses can be added to other licenses

Licensing Resources

- Compare Microsoft 365 Enterprise Plans | Microsoft 365
- Modern-Work-Plan-Comparison-ENT-1-16-2024.pdf
- Home | M365 Maps

Preparing for Copilot Success



1. Consolidate and Clean

We'll help you connect all your data sources in M365, inventory outdated and irrelevant files, and ensure that only the most relevant data is accessible to Copilot.

2. Secure and Label

Our team will implement security protocols, reduce oversharing, and apply Purview sensitivity labelling to safeguard critical files and maintain access control.

3. Train Users

We'll provide training on best practices, showing users the key differences between ChatGPT and Copilot and ensuring they understand how to get the best results from the AI tool.

4. Improve Governance

Our team will work with you to establish M365 governance tools that standardize policies and automatically enforce rules for future files, workspaces, and permissions.

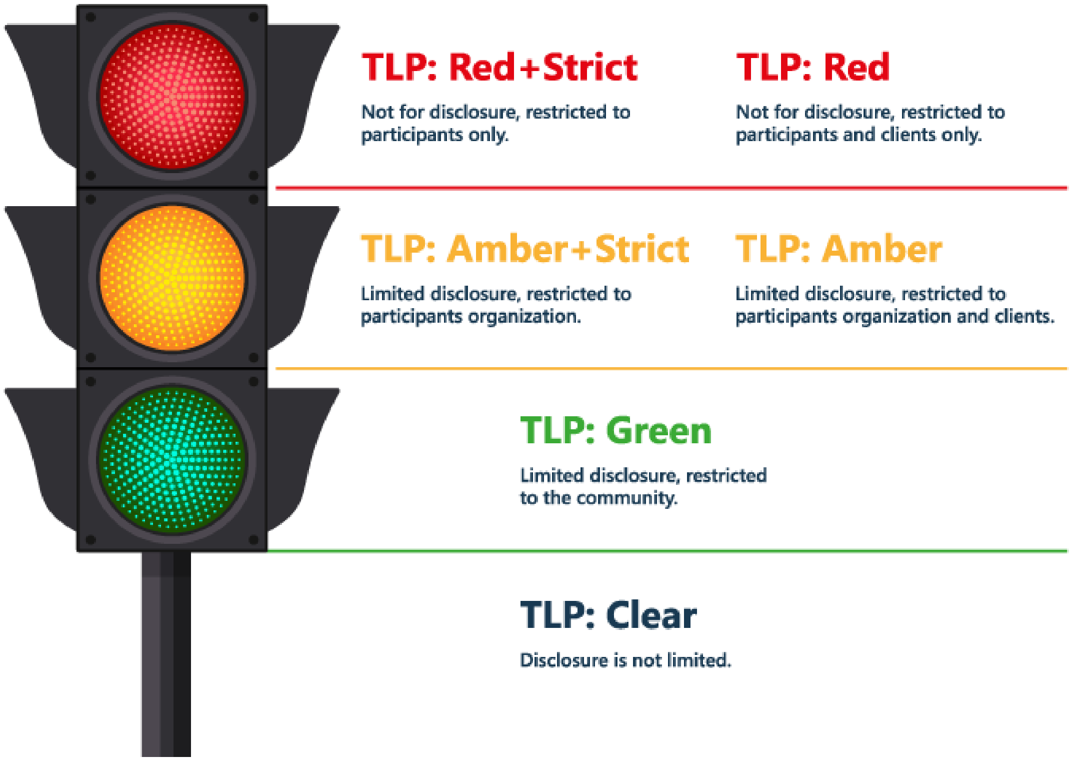
[Copilot Readiness | Envision IT]

Traffic Light Protocol: Simplifying Sensitivity Labels in Microsoft 365

The **Traffic Light Protocol (TLP)** is a classification system that uses color-coded labels to categorize and control the sharing of sensitive information.

- Developed by the UK’s National Infrastructure Security Coordination Centre in the early 2000s
- Encourages sharing of sensitive information
- Adopted by the US Cybersecurity and Infrastructure Security Agency (CISA)
- Not a technical solution and not part of Purview

TLP Labels and their Meanings



TLP: Red+Strict

Not for disclosure, restricted to participants only.

TLP: Red

Not for disclosure, restricted to participants and clients only.

TLP: Amber+Strict

Limited disclosure, restricted to participants organization.

TLP: Amber

Limited disclosure, restricted to participants organization and clients.

TLP: Green

Limited disclosure, restricted to the community.

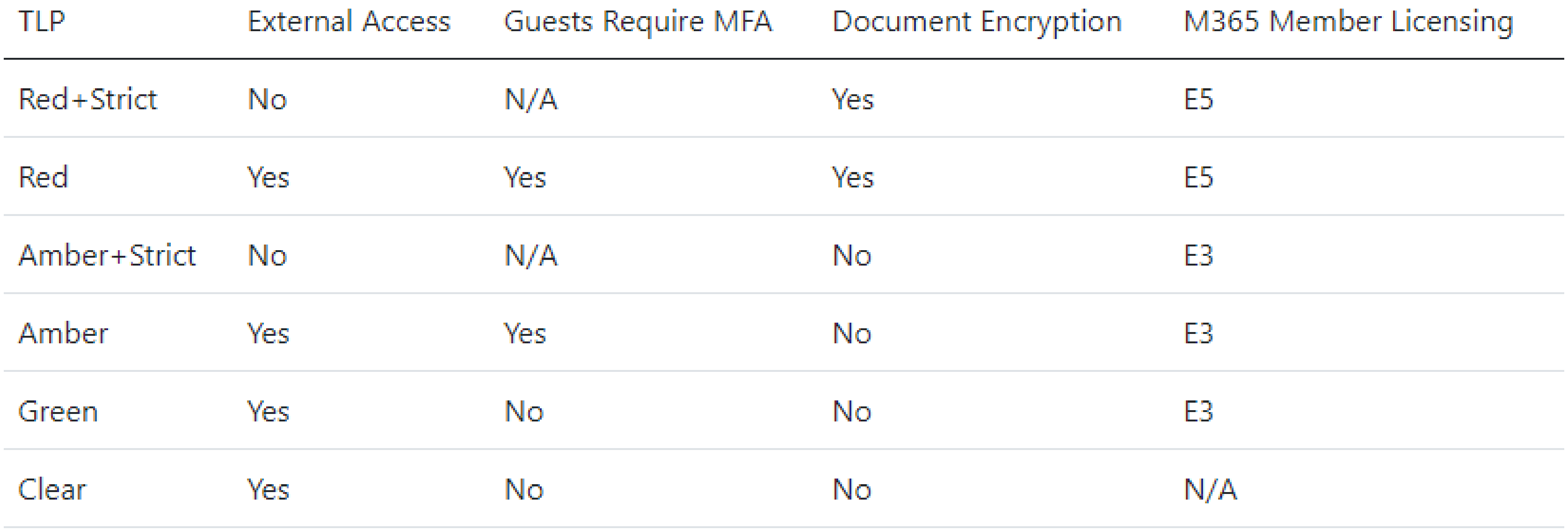
TLP: Clear

Disclosure is not limited.

- **Red:** Most sensitive information; requires MFA and document encryption
- **Amber:** Sensitive information; external sharing allowed with MFA
- **Green:** Less sensitive; accessible to guests without MFA
- **Clear:** Public information; accessible without restrictions

TLP and External Access in Microsoft 365

Below is a suggested implementation of TLP for defining guest access in Microsoft 365:



TLP	External Access	Guests Require MFA	Document Encryption	M365 Member Licensing
Red+Strict	No	N/A	Yes	E5
Red	Yes	Yes	Yes	E5
Amber+Strict	No	N/A	No	E3
Amber	Yes	Yes	No	E3
Green	Yes	No	No	E3
Clear	Yes	No	No	N/A

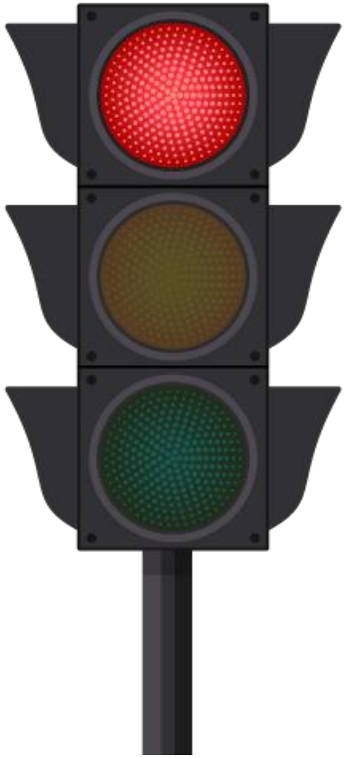
TLP Green

- Low sensitivity content
- Can be shared externally
- No MFA requirement for external guests

TLP Amber

- Medium sensitivity content
- Can be shared externally
- External guests require MFA
- Strict doesn’t allow external sharing

TLP Red



- High sensitivity content
- Can be shared externally
- External guests require MFA
- Office and PDF documents are encrypted
- Strict doesn’t allow external sharing

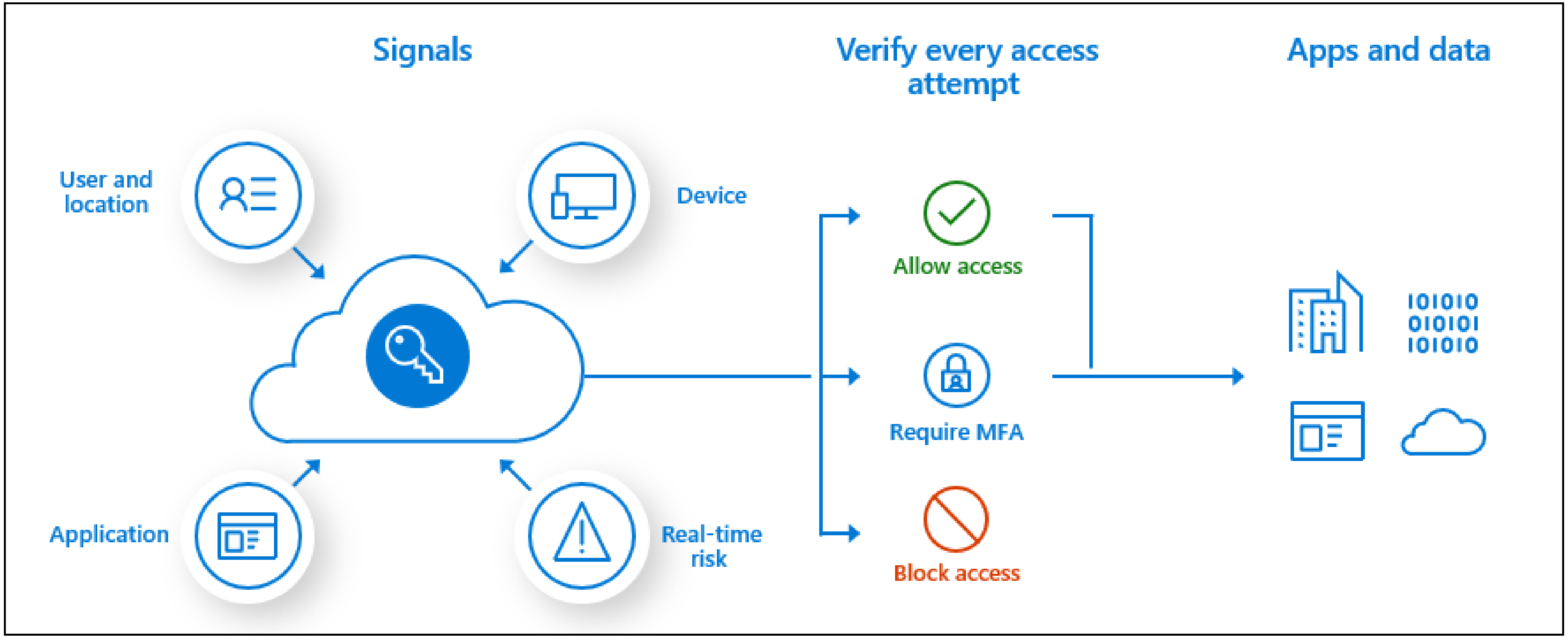
Benefits of TLP in Microsoft 365

Clear, consistent classification for sensitive data

Secure external sharing with appropriate MFA and encryption

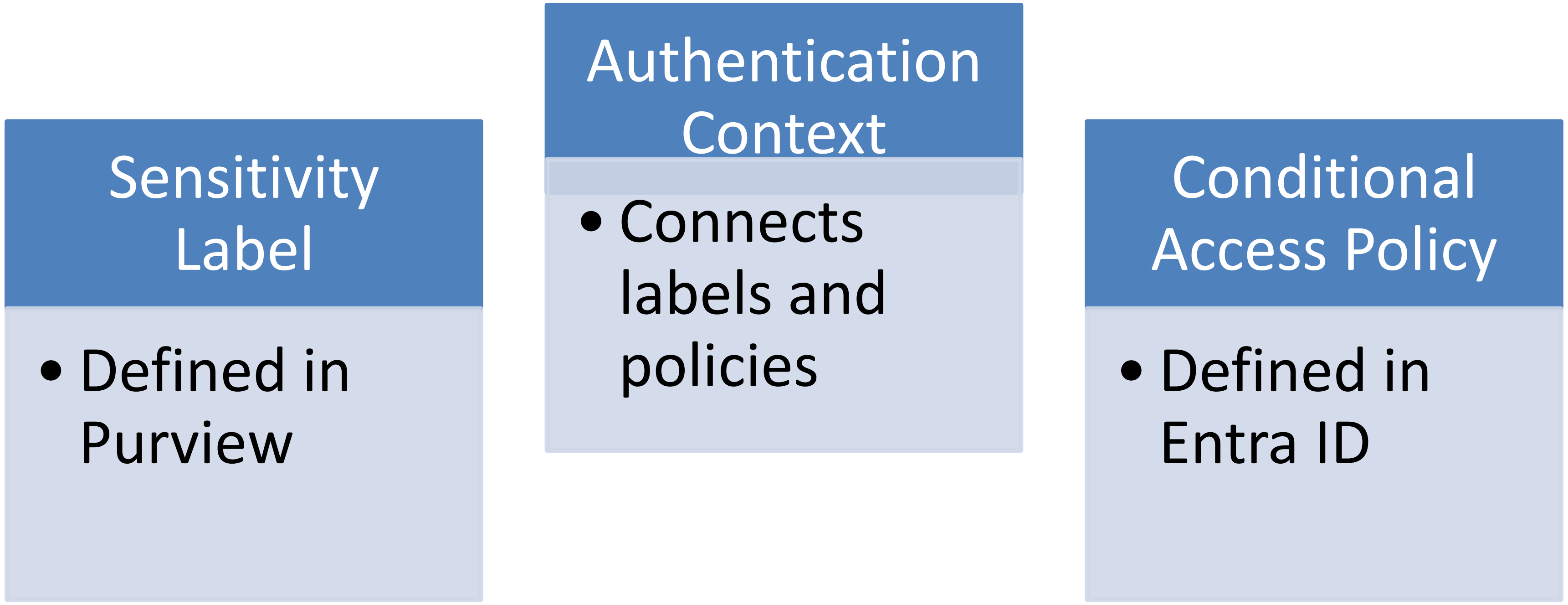
Enhanced governance and protection via Microsoft Purview

Conditional Access Policies



Set up Microsoft Entra Conditional Access | Microsoft Learn

Authentication Context



Sensitivity Label

- Defined in Purview

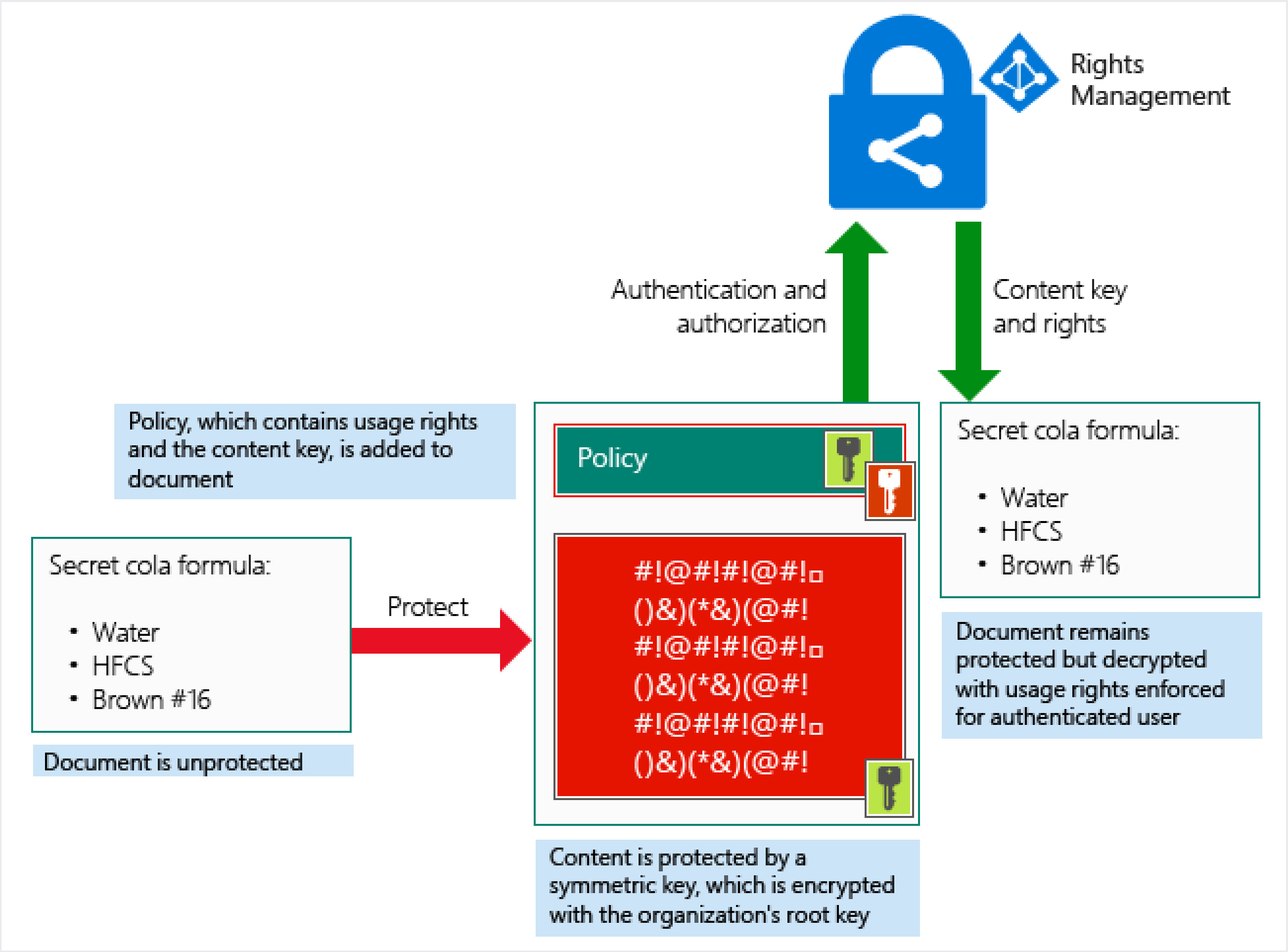
Authentication Context

- Connects labels and policies

Conditional Access Policy

- Defined in Entra ID

Data Encryption


Rights Management
Authentication and authorization
Content key and rights
Policy, which contains usage rights and the content key, is added to document
Policy
Secret cola formula:
• Water
• HFCS
• Brown #16
Protect
#!@#!#!@#!▫
()&)(*&)(@#!
#!@#!#!@#!▫
()&)(*&)(@#!
#!@#!#!@#!▫
()&)(*&)(@#!
Secret cola formula:
• Water
• HFCS
• Brown #16
Document is unprotected
Document remains protected but decrypted with usage rights enforced for authenticated user
Content is protected by a symmetric key, which is encrypted with the organization's root key

How Azure RMS works - Azure Information Protection | Microsoft Learn

Phase One Implementation of Purview

1. Define Container Labels → Create Green and Amber labels in Purview for SharePoint sites and containers, setting rules to determine external access and MFA requirements.
2. Establish Authentication Contexts → Set specific authentication contexts for each label to ensure appropriate security checks like multi-factor authentication are enforced for external users.
3. Build Conditional Access Policies → Create policies that apply the correct access control based on membership and guest status.
4. Inventory and Label Existing Sites → Audit current SharePoint and Teams sites, applying appropriate labels based on their sensitivity.

Phase Two Implementation of Purview

1. Define Content Labels → Extend TLP sensitivity labels to individual documents by configuring Purview to recognize and protect highly sensitive content.
2. Apply Access Controls & Document Marking → Configure Azure Information Protection and Rights Management to enforce encryption and granular permissions.
3. Set Default Label Rules → Link document labels to container-level labels, ensuring documents inherit sensitivity levels from the SharePoint site or container they reside in.
4. Configure Azure Services → Set up Azure Information Protection and Rights Management for automatic labeling and encryption of Red-level documents.
5. Auto-Labeling → Enable automatic labeling based on predefined conditions, using E5 licensing for consistent protection.
6. Implement Add'l Authentication Contexts → Add further conditional access policies to provide secure external access and MFA based on sensitivity.

Midsize Ontario City

Large Scale M365 Implementation

- Governance Solution for Teams/SP
  - Proliferation of Ad Hoc Teams and SP Sites
  - Leverage Properly Defined SP & Teams Structure
  - Migration into New Structure
    - Multiple Meetings with large number of groups for planning purposes
    - Actual Migration

Teams First IA

- Logical organization of Content
- Intuitive Navigation, Search
- Teams, Hub sites, SharePoint

Adoption & Governance

- Orchestry for M365 Adoption and Governance
- Templates, Provisioning
- Self-service
- End-to-end lifecycle Management
  - Templates
  - Approvals
  - Policies for Naming Conventions
  - Archiving
- Policy Enforcement
- User Management

Federal / Provincial / Municipal Agency

Large Scale ECM Implementation

- Previously completed ECM Strategy engagement
- Defined new modern IA
- Migration into New Structure
  - Multiple Meetings with large number of groups for planning purposes
  - Actual Migration

Purview Implementation

- Information Protection Workshop
- Configuration of Microsoft Purview sensitivity labels
- Entra ID Authentication Contexts and Conditional Access Policies
- Rights Management for document encryption and watermarking
- External sharing strategy and information architecture
- EUM Data Room POC with trial license

Adoption & Governance

- Orchestry for M365 Adoption and Governance
- Templates, Provisioning
- Self-service
- End-to-end lifecycle Management
  - Templates
  - Approvals
  - Policies for Naming Conventions
  - Archiving
- Policy Enforcement
- User Management

Provincial Healthcare Agency

SharePoint Online Migration

- 19 SharePoint on premises farms 2010 through 2016
- Migrating into SharePoint Online
- Including Forms and Workflows
- All farms have been independently managed
  - Migration into New Structure
    - Multiple Meetings with large number of groups for planning purposes
    - Actual Migration

Purview Implementation

- Already had sensitivity labels established
- Setting up authentication contexts
- Conditional Access Policies
- eDiscovery

Members Portal

- Migrated off SharePoint 2013 to SharePoint Online
- Users were created as cloud only guest accounts
- SharePoint Online Communication Sites
- EUM Product used for user management
  - Leads are able to manage their own users

Microsoft Reporting

- Data access governance reports for SharePoint sites - SharePoint in Microsoft 365 | Microsoft Learn
- Sharing links reports
  - "Anyone" links
  - "People in the organization" links
  - "Specific people" links shared externally
- Sensitivity labels applied to files

Third Party Tools

ShareGate
by workleap

AvePoint
Insights
For Microsoft 365

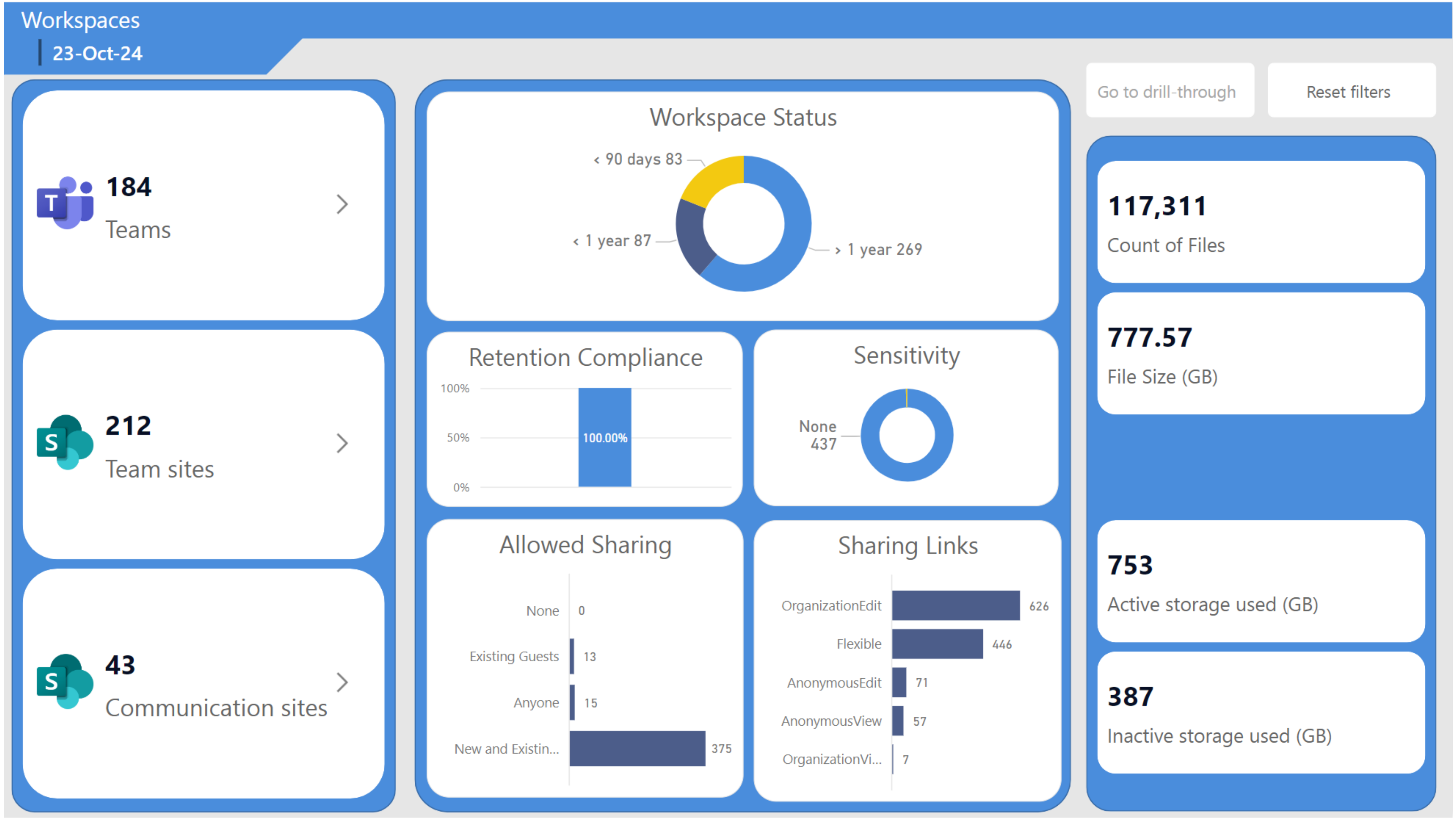
Orchestry

Rencore
governance

envision IT

BCC

Power BI Microsoft 365 Dashboard



Workspaces
23-Oct-24

Go to drill-through

Reset filters

184
Teams

212
Team sites

43
Communication sites

117,311
Count of Files

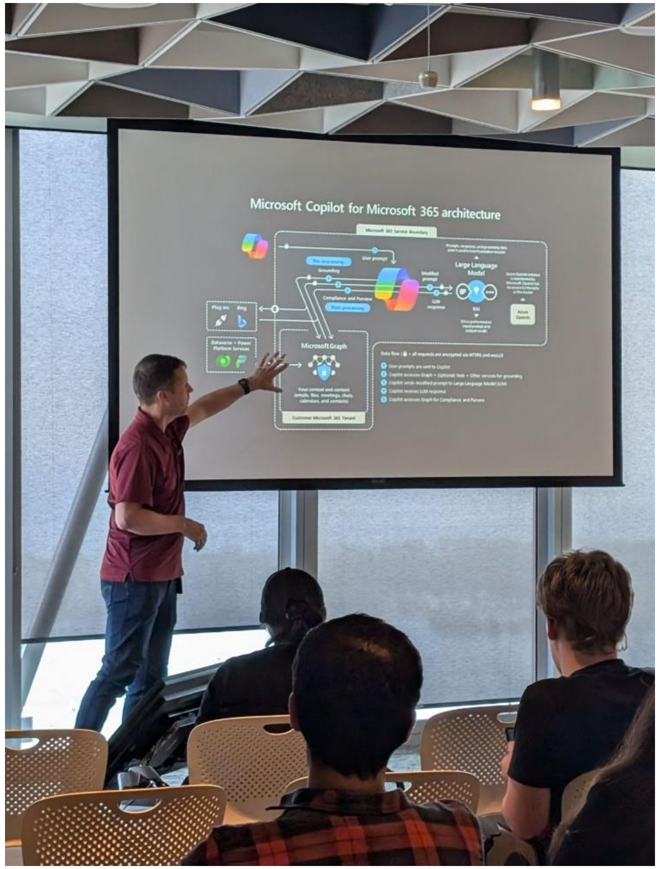
777.57
File Size (GB)

753
Active storage used (GB)

387
Inactive storage used (GB)

Purview Information Protection Workshop

- Learn about:
  - Intro to Purview Information Protection
  - Identify and create sensitive information types
  - Create sensitivity labels following the Traffic Light Protocol approach and use auto-labeling policies based on these labels
  - Intro to authentication contexts and conditional access policies
  - Intro to DLP



Envision IT Purview Information Protection Engagement

- Licensing and tenant setup review and recommendations
- Information Protection Workshop
- Configuration of Microsoft Purview:
  - Sensitivity labels
  - Entra ID Authentication Contexts and Conditional Access Policies
  - Rights Management for document encryption and watermarking
  - Microsoft 365, Teams, and SharePoint configuration
- External sharing strategy and information architecture

3 Key Takeaways

1 Information Protection is something many organizations are licensed for but haven’t implemented.

2 Cybersecurity is not one size fits all. Make your protection appropriate to the content.

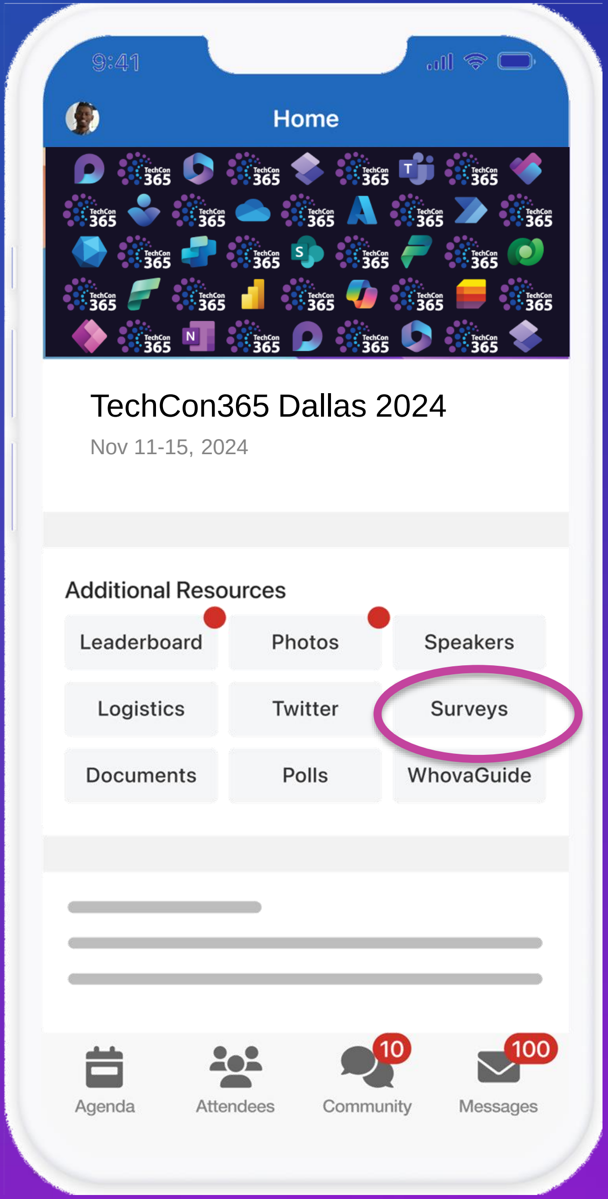
3 Copilot Readiness is driving much of this, but safe external sharing is another big driver.

Thank you!

Any Questions?

How was the session?

Search for WHOVA in the App Store or Google Play



TechCon365 Dallas 2024

Nov 11-15, 2024

Fill out the Surveys in the **TechCon 365 Dallas Event App** and be eligible to win **PRIZES!**

TechCon 365

techcon365.com/Dallas