I Have Microsoft Purview....Now What?

M365 TWIN CITIES

Please thank our sponsors

DEVICIE

About Us

David Drever

Associate Director, Protiviti

M365 and Security MVP

https://linktr.ee/davidmdrever

Deep Trivedi

Senior Manager, Protiviti

Microsoft Data Security Adoption & Organizational Change Management

https://linktr.ee/deeptrivedi

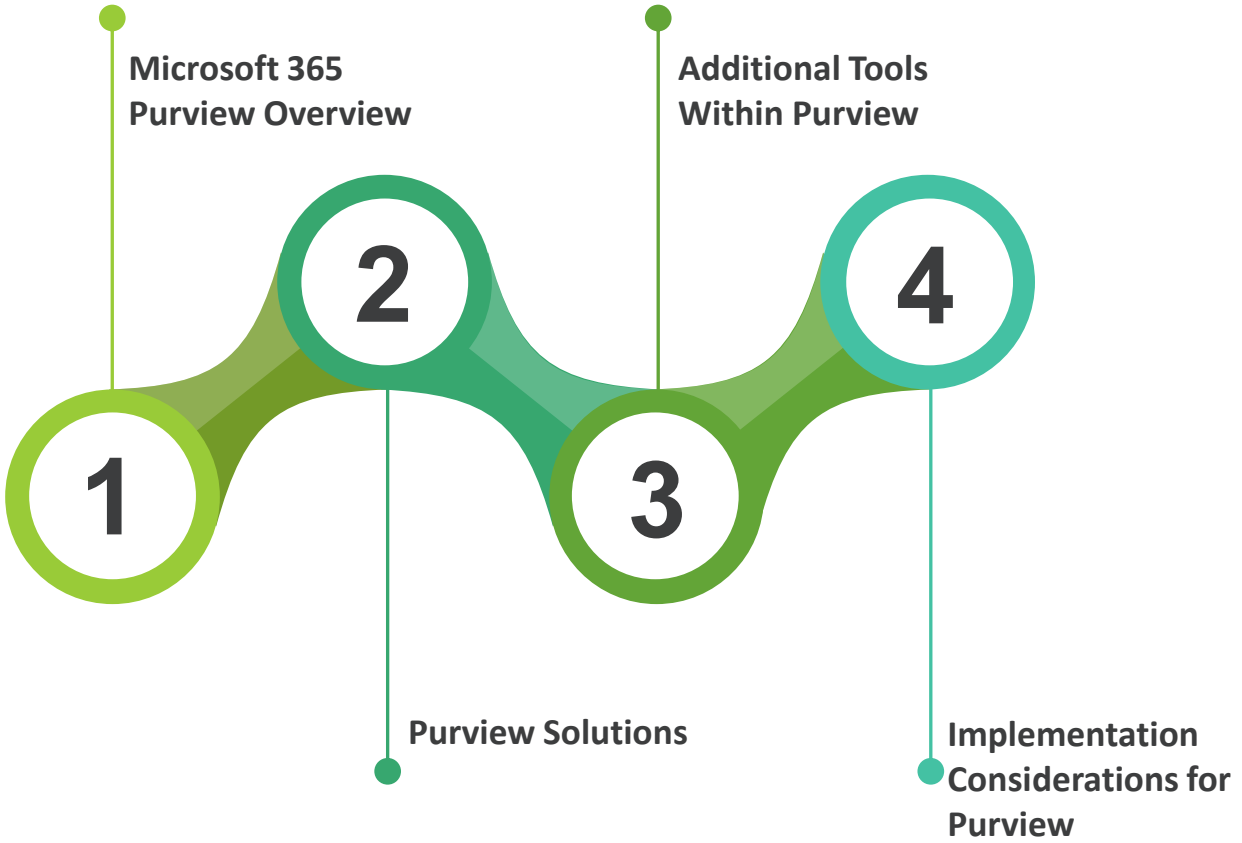
Anna Bordioug

Senior Consultant, Protiviti

Microsoft Data Security Specialist

https://linktr.ee/annabordioug

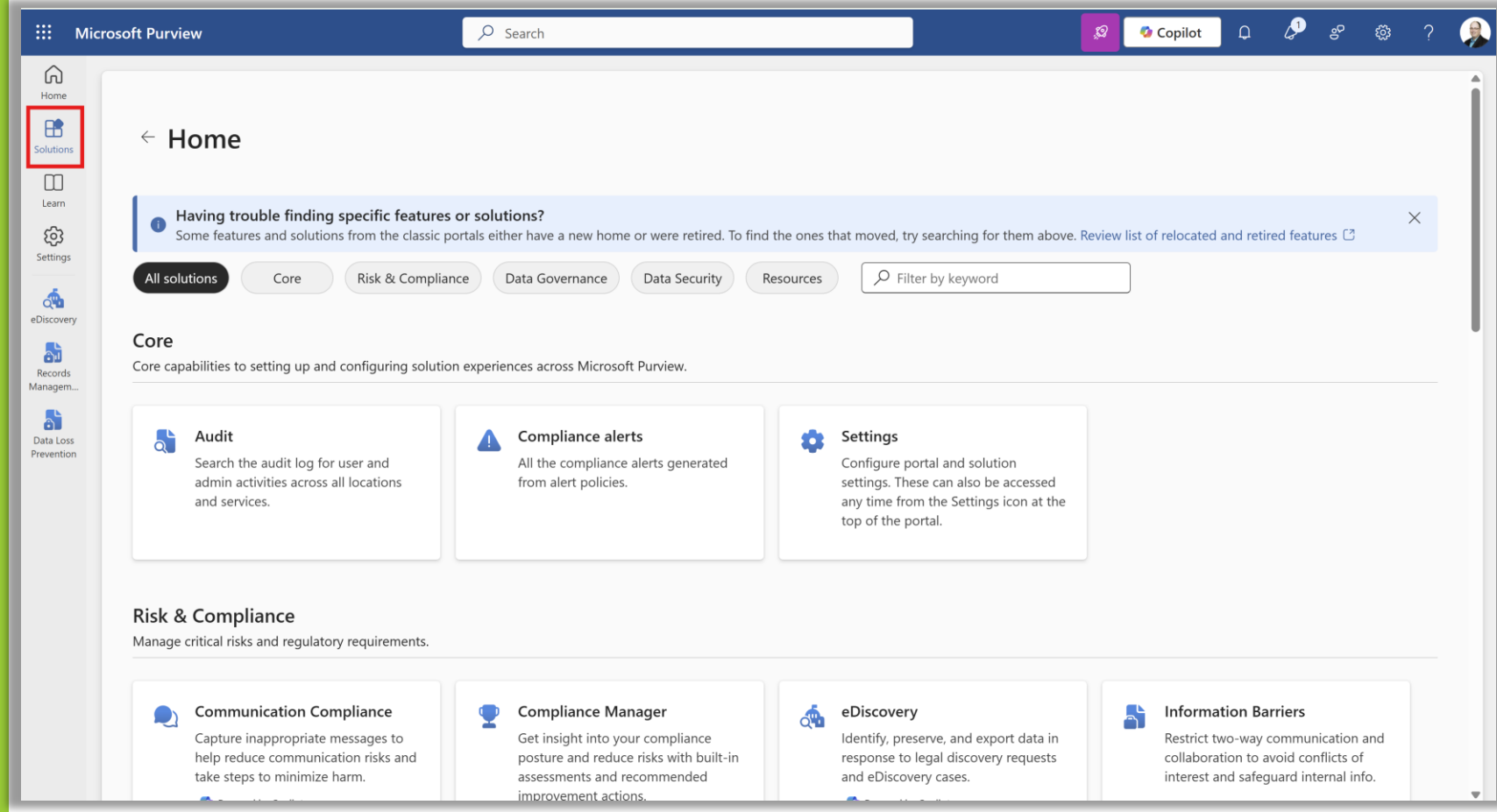
Today’s Topics



Purview Overview

Microsoft Purview from 50,000 Feet

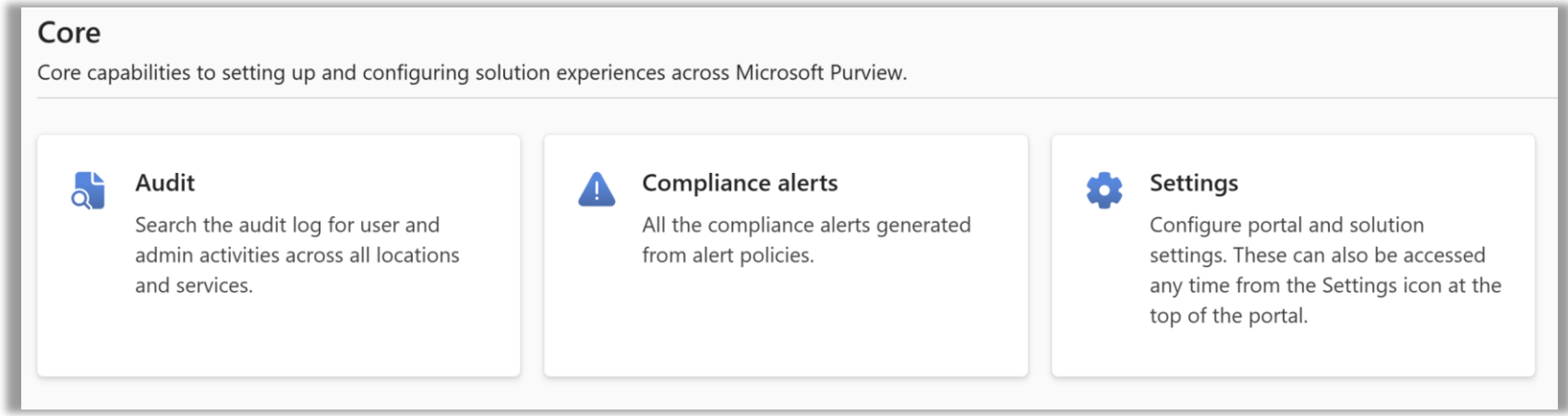
Purview is a Suite of Products (Solutions)



Microsoft Purview from 50,000 Feet

Purview is a Suite of Products (Solutions)

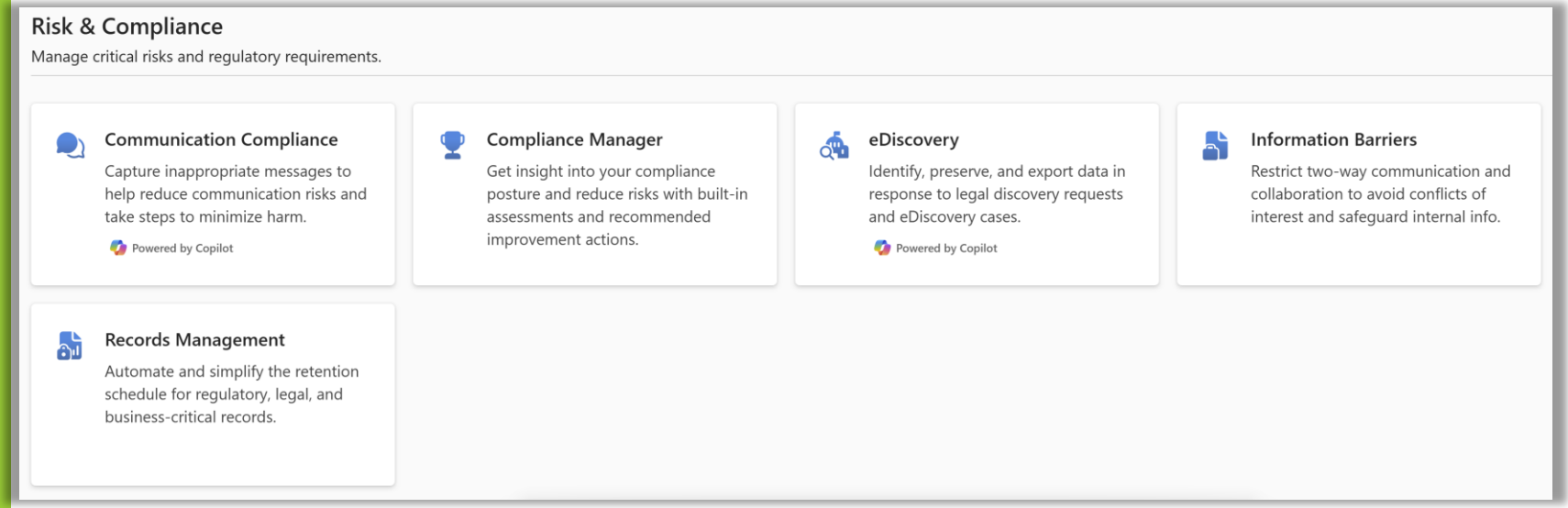
- Broken into four (4) main categories
  1. **Core** – Supporting components for every solution within Purview



Microsoft Purview from 50,000 Feet

Purview is a Suite of Products (Solutions)

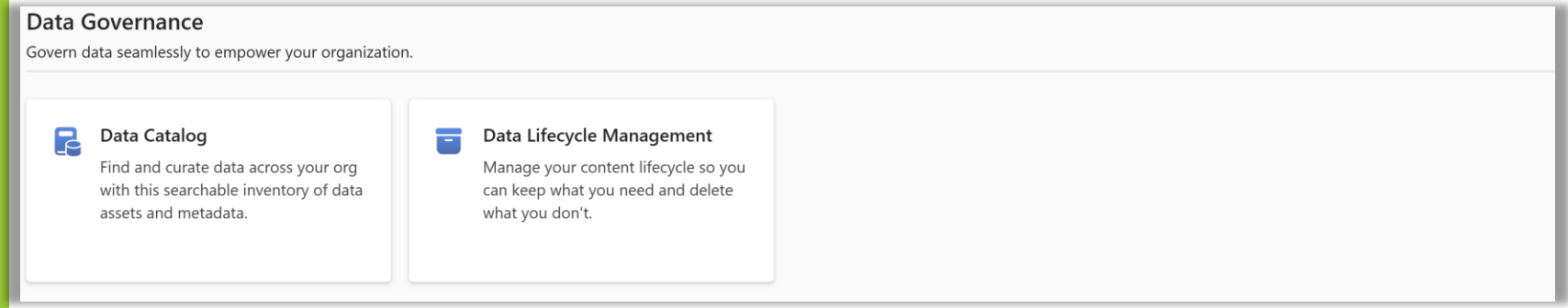
- Broken into four (4) main categories
  2. **Risk & Compliance** – Focuses on information management and governance



Microsoft Purview from 50,000 Feet

Purview is a Suite of Products (Solutions)

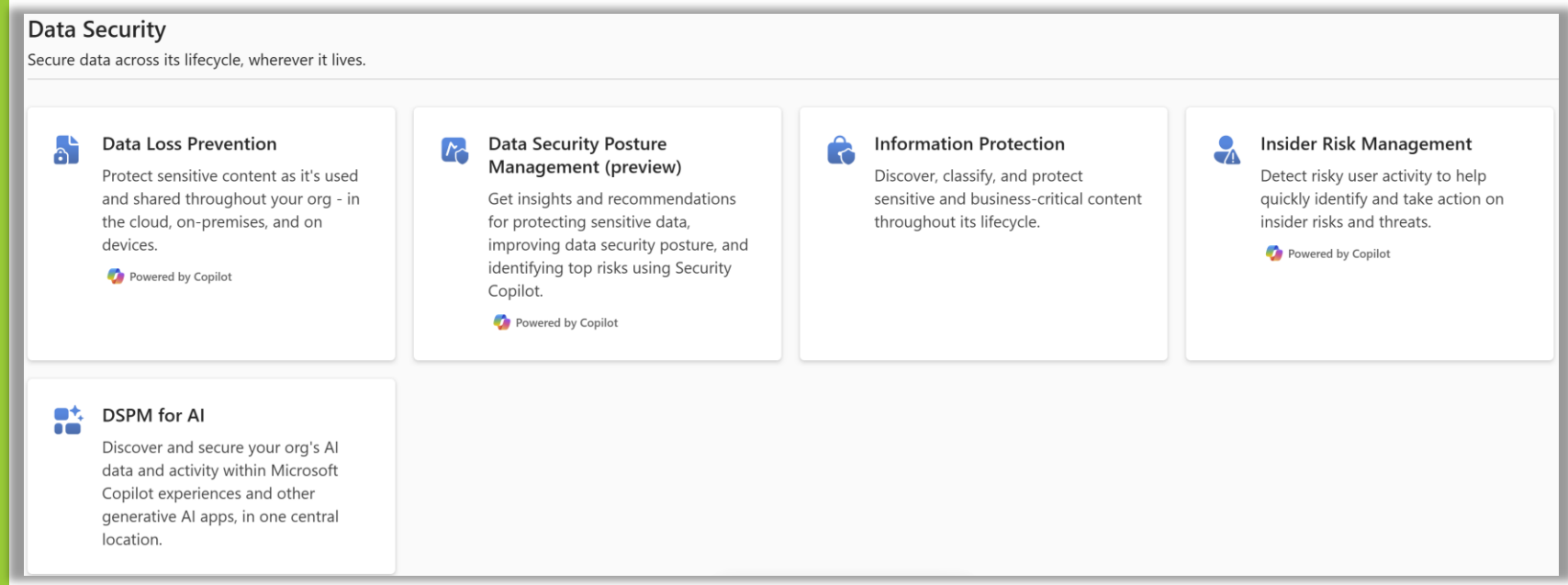
- Broken into four (4) main categories
  3. **Data Governance** – Govern content stored in both structured and unstructured locations.

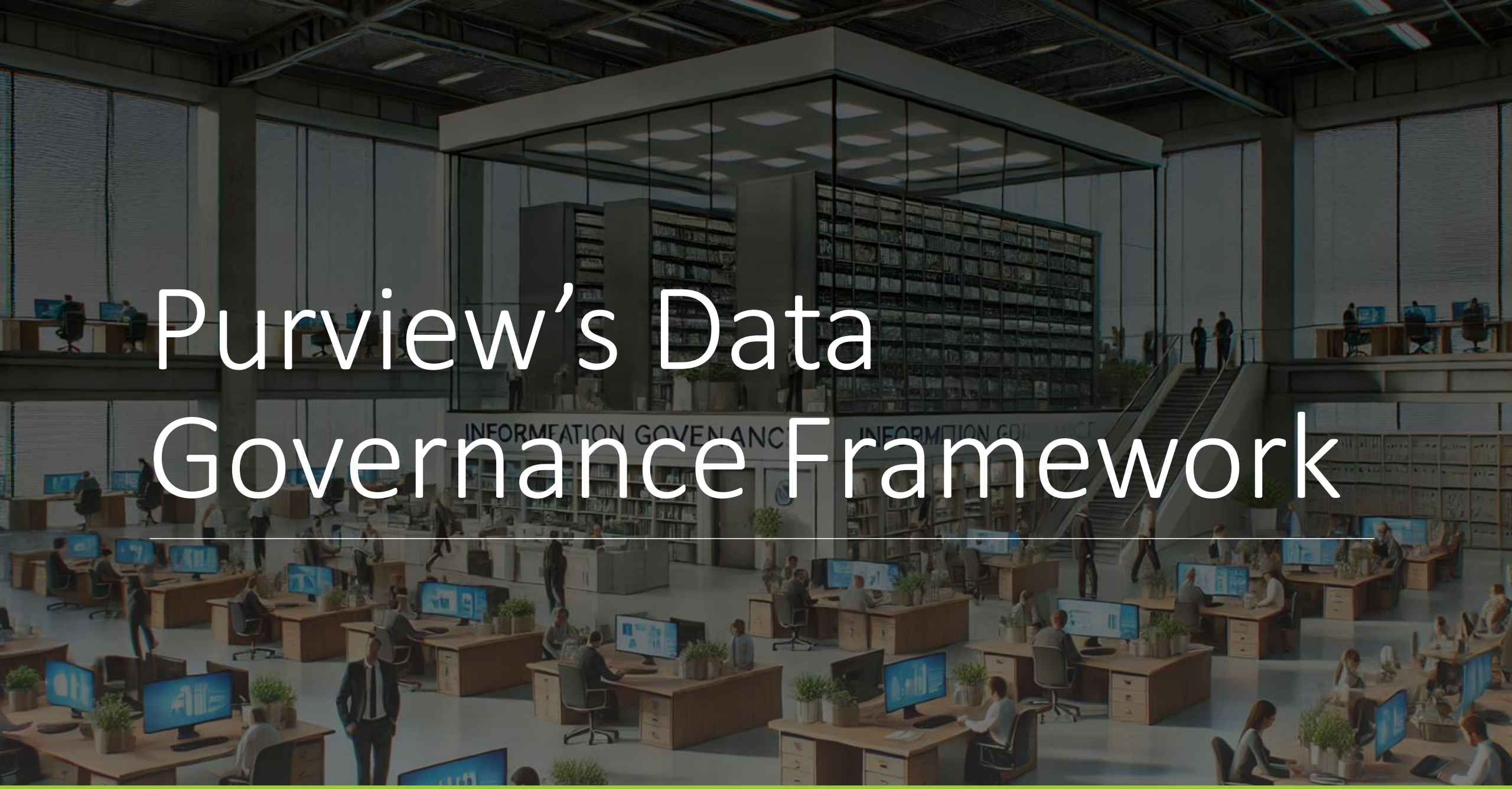


Microsoft Purview from 50,000 Feet

Purview is a Suite of Products (Solutions)

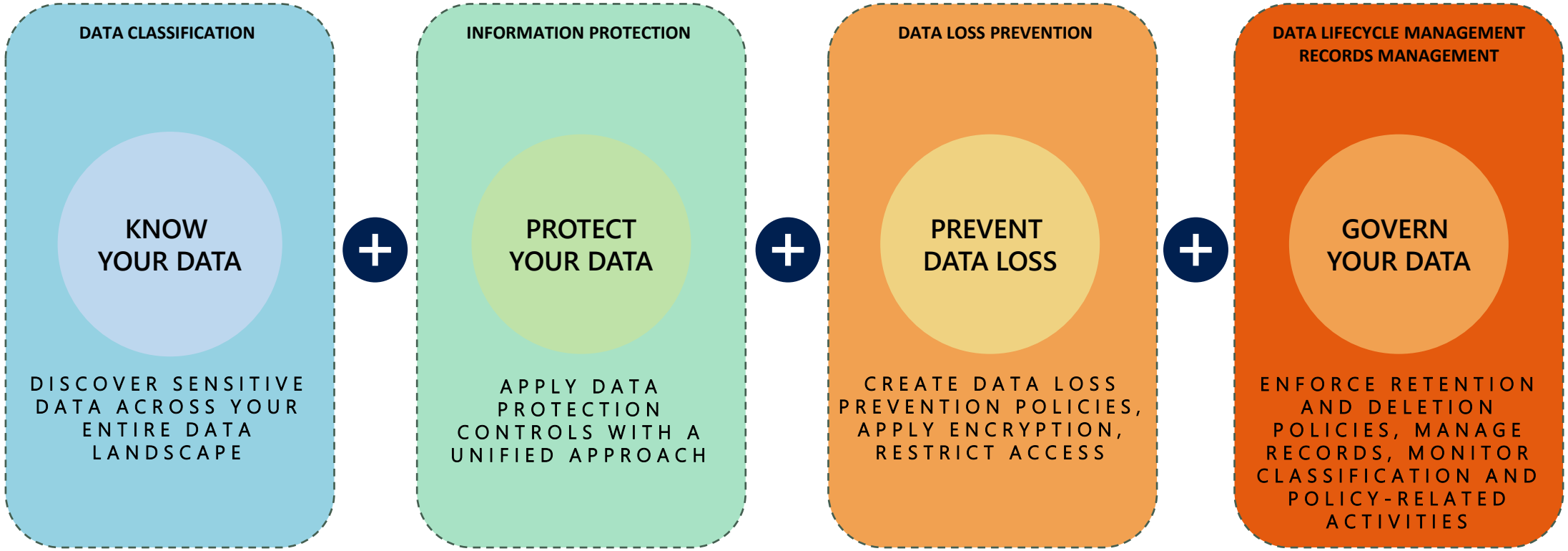
- Broken into four (4) main categories
  4. **Data Security** – Securing data in any location including the act of sharing.





Purview's Data Governance Framework

Data Governance Framework



Framework Support within Purview

Microsoft Purview Information Protection Discovery

Microsoft Purview Provides a variety of methods to discovery sensitive information within the tenant.

Sensitive Information Types (SITs)

Custom algorithms that detect sensitive information within content

Trainable Classifiers

Machine-learning (teaching) capabilities to recognize sensitive data based on text patterns, context, and semantics.

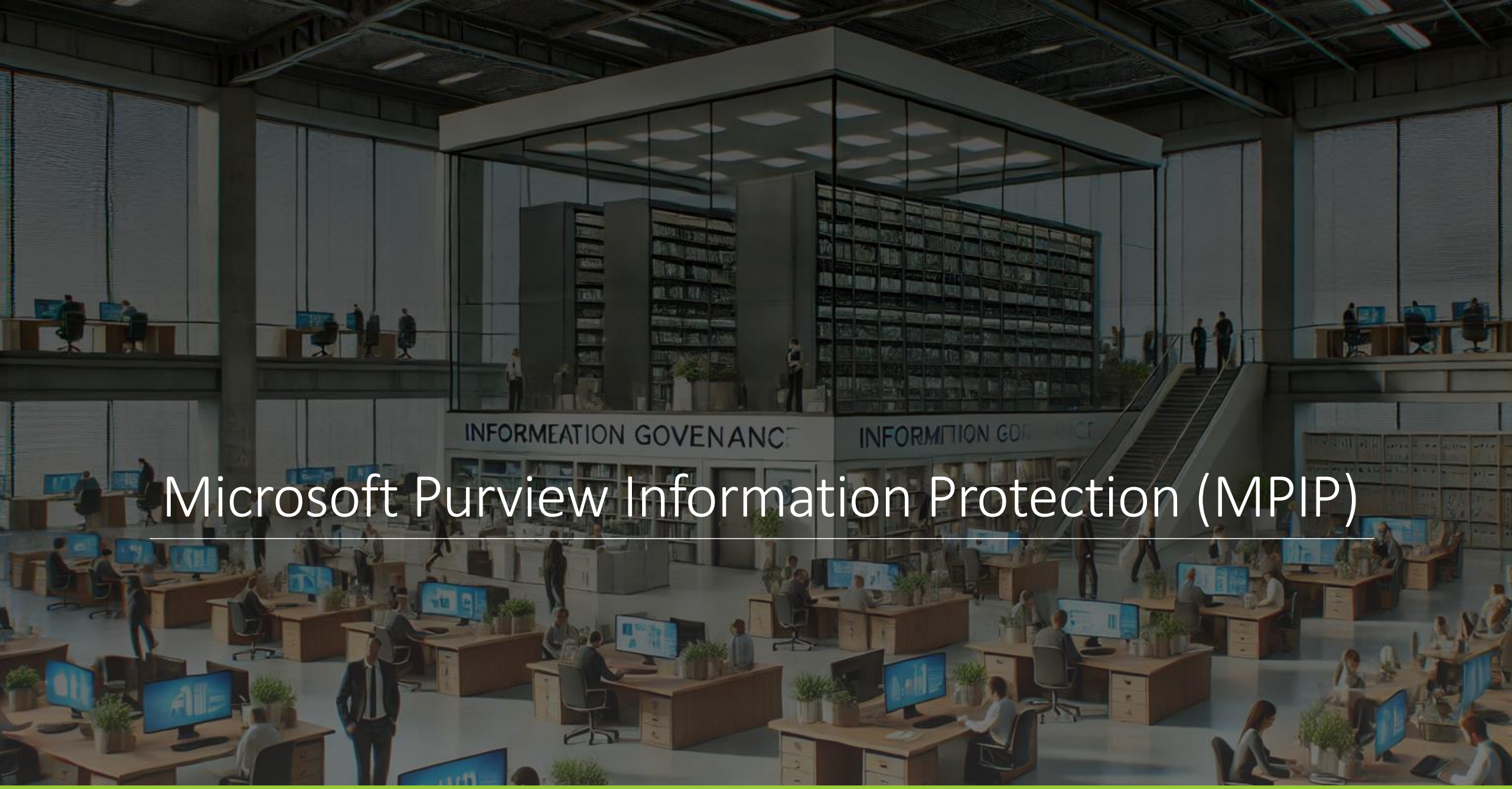
Exact Data Match (EDM)

Database of terms, phrases, IDs, etc. the system searches for within content to flag as sensitive.

Document Fingerprinting

Machine-learning (teaching) capabilities to recognize the format of a document and related content to detect sensitive information.

The Solutions in Purview



Microsoft Purview Information Protection (MPIP)

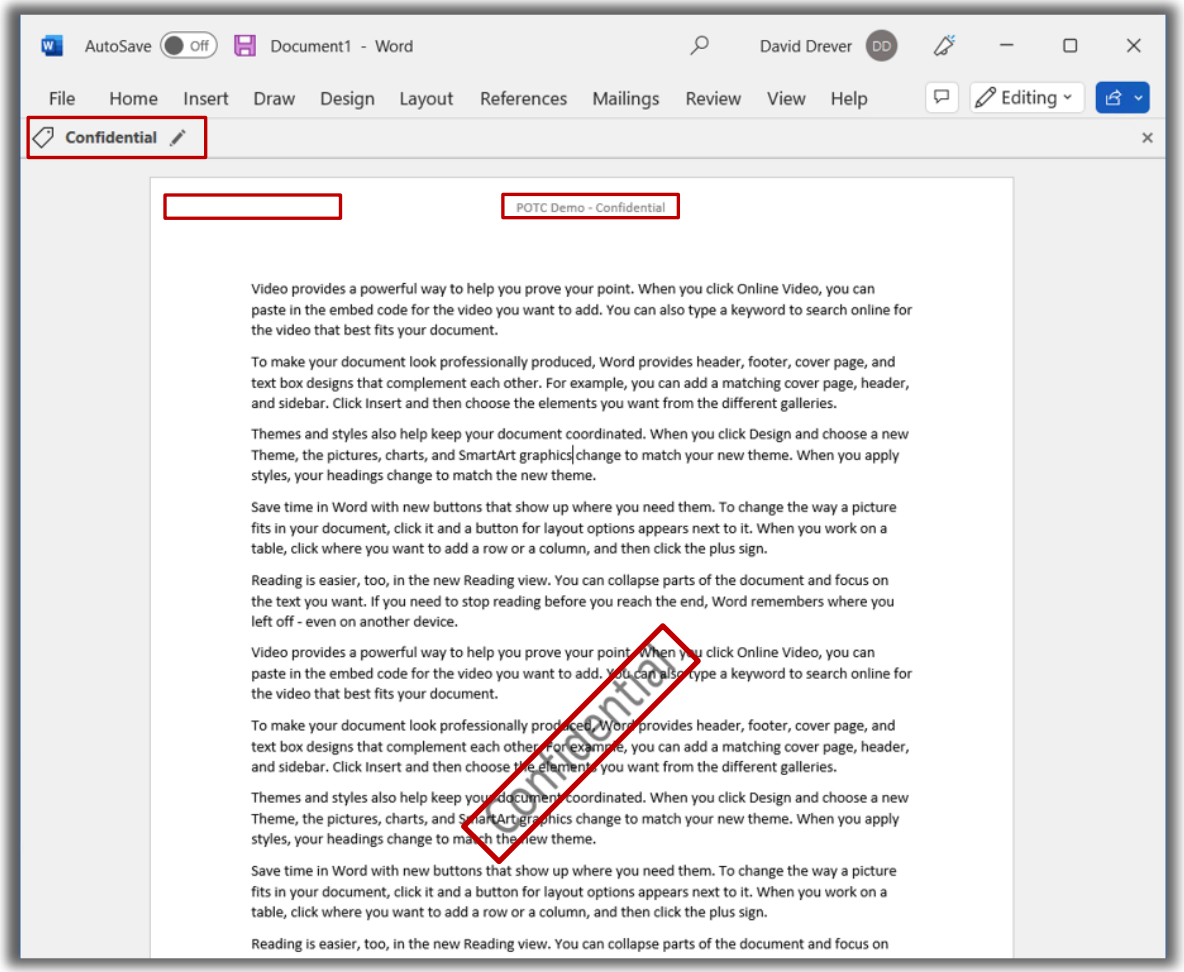
Microsoft Purview Information Protection

Sensitivity Label Capabilities:

- Content Markup when labels are applied to content:
  - Headers and/or Footers
    - Multiple colors available
    - Left, Center, or Right justified
    - Variable font size
  - Watermark
    - Multiple colors available
    - Variable font size
    - Variable font direction
- Encryption
  - Independent of location security. Dependent on the label configurations

- Auto-Application of Sensitivity based on:
  - Sensitive Information Within Content
  - Recognizable Format (contracts, invoices, etc)

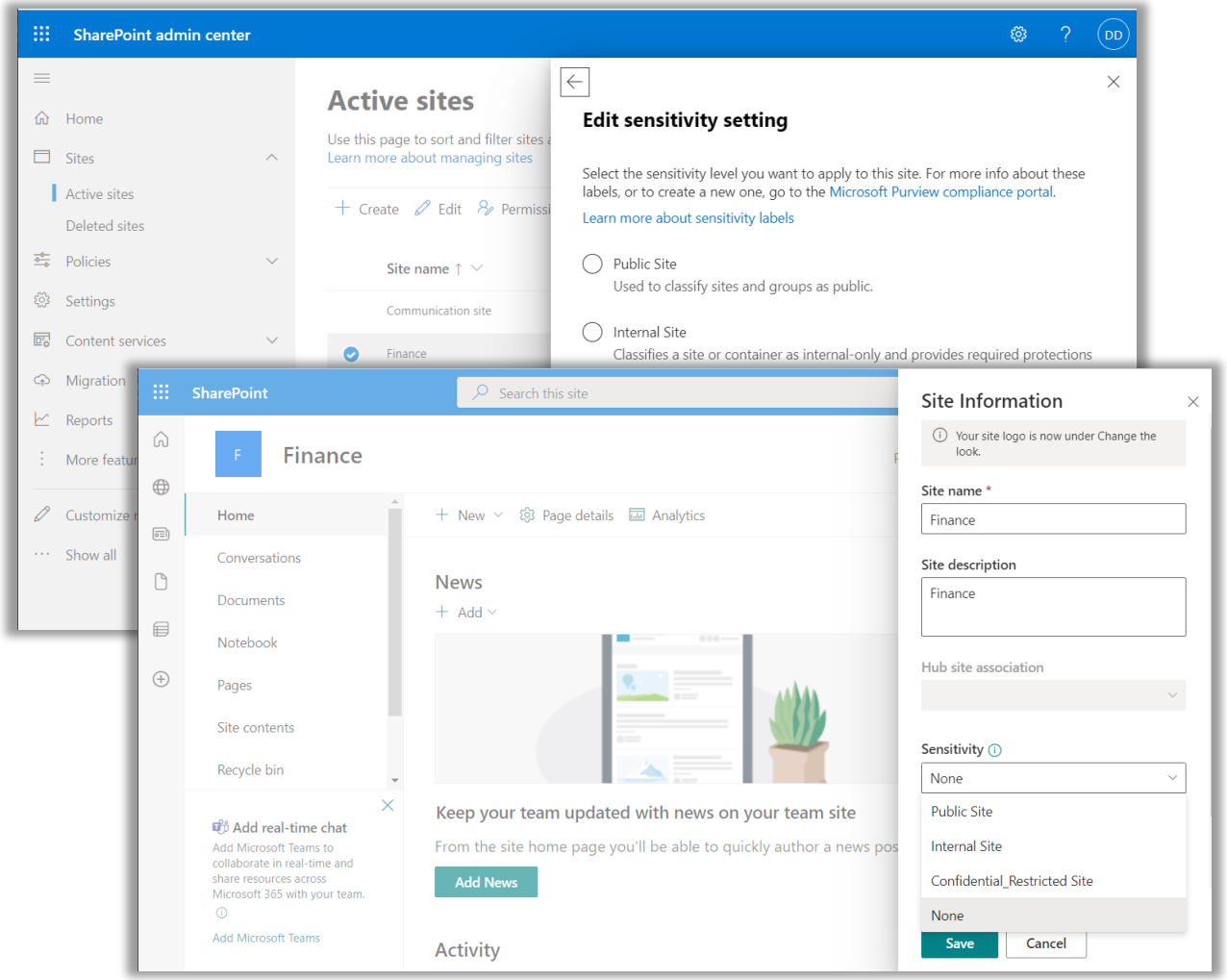
- Protection of SharePoint Sites and Microsoft Teams
  - Adds additional protections at the site level to control the sharing of sensitive data



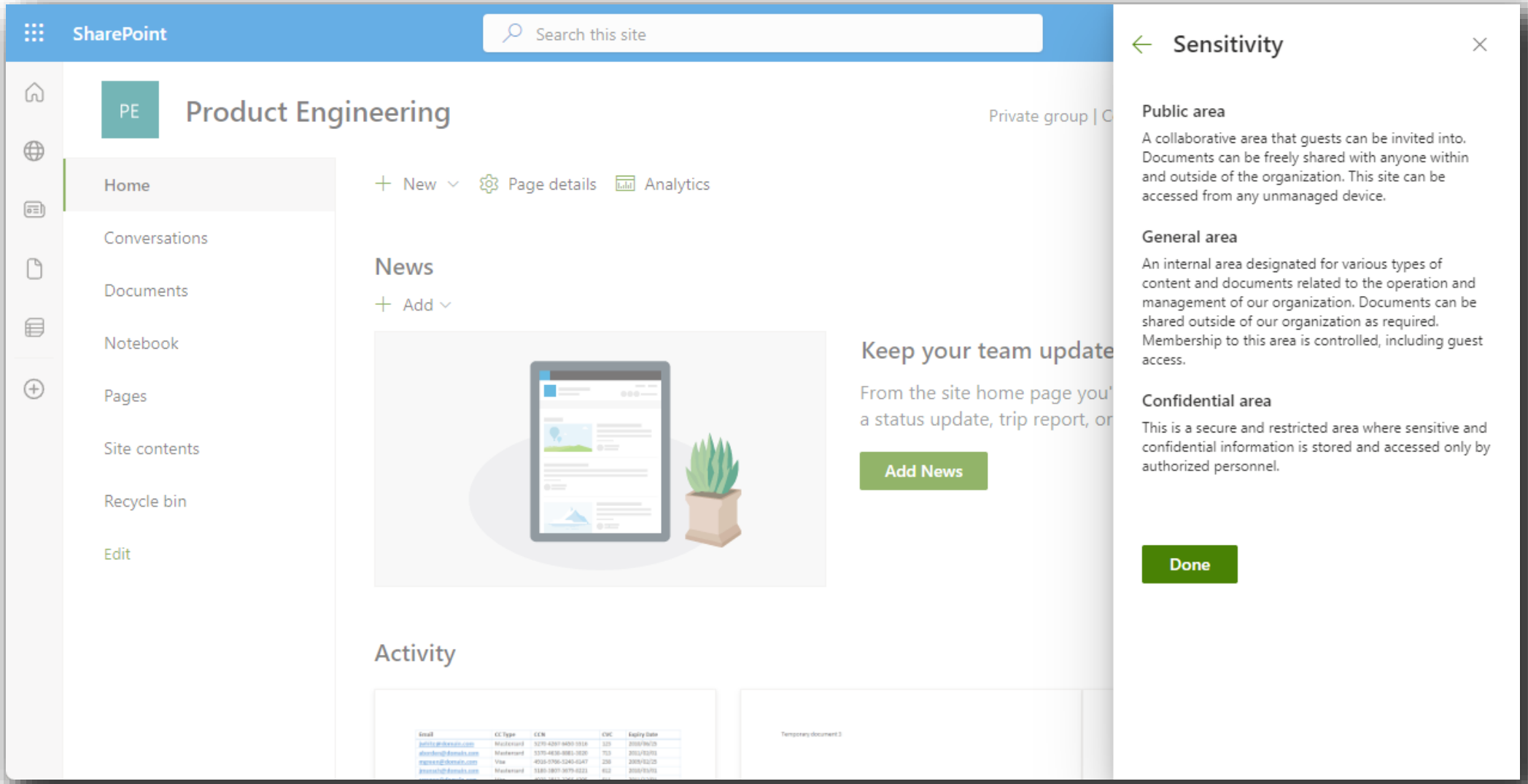
Microsoft Purview Information Protection

Site and Group Sensitivity Labels

- Does apply default sensitivity to content within the site.
- Applies additional controls to sites:
  - Block external users
  - Enforce managed devices
  - Site Owner permission granting controls
- Apply Authentication Contexts to sites for use with Conditional Access
- Automatically notifies users and administrators if highly sensitive content is uploaded to the site.



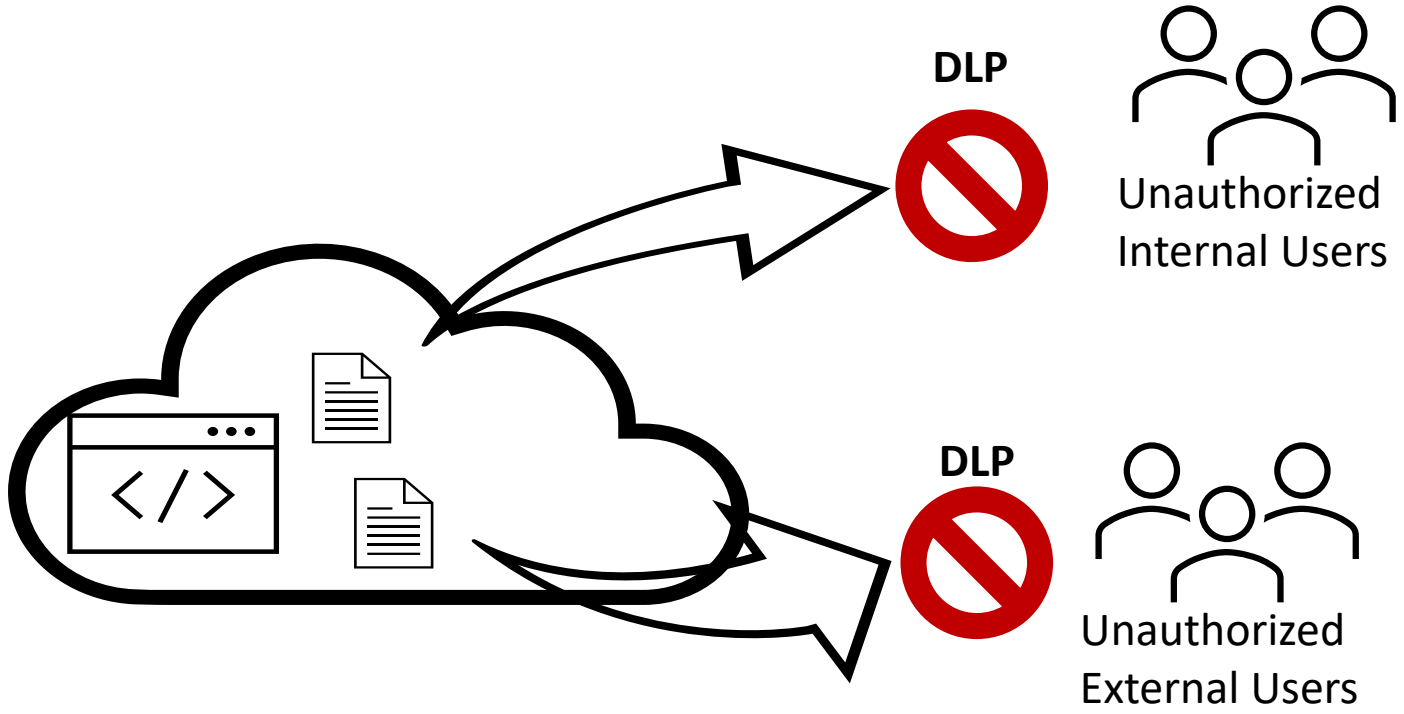
Microsoft Purview Information Protection



Data Loss Prevention (DLP)

Data Loss Prevention (DLP)

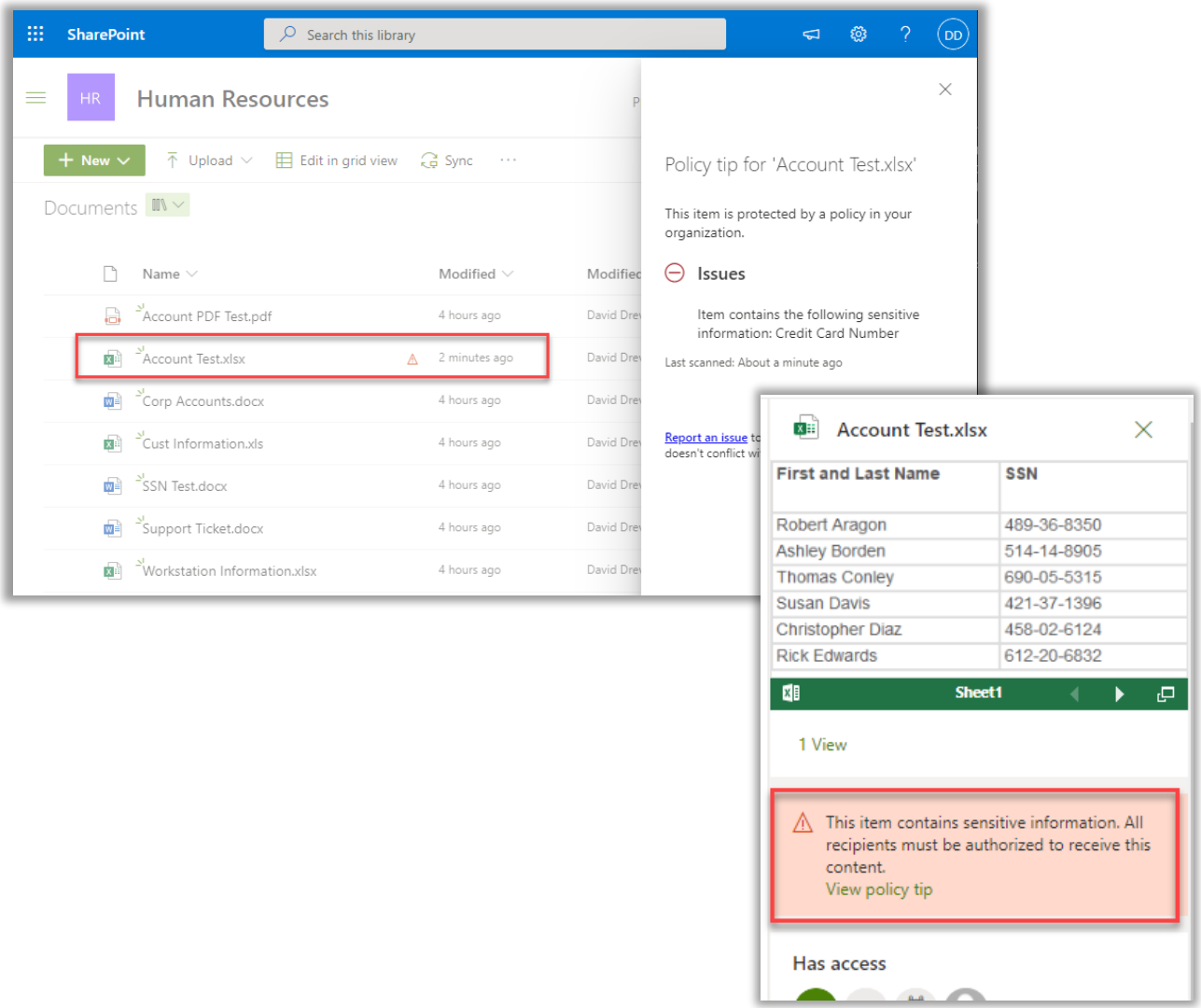
A Data Loss Prevention policy's primary use is to protect data flow within the organization. A DLP policy tracks when content is shared and made available for others when stored within supported locations such as SharePoint Online.



Data Loss Prevention (DLP)

Data Loss Prevention Capabilities:

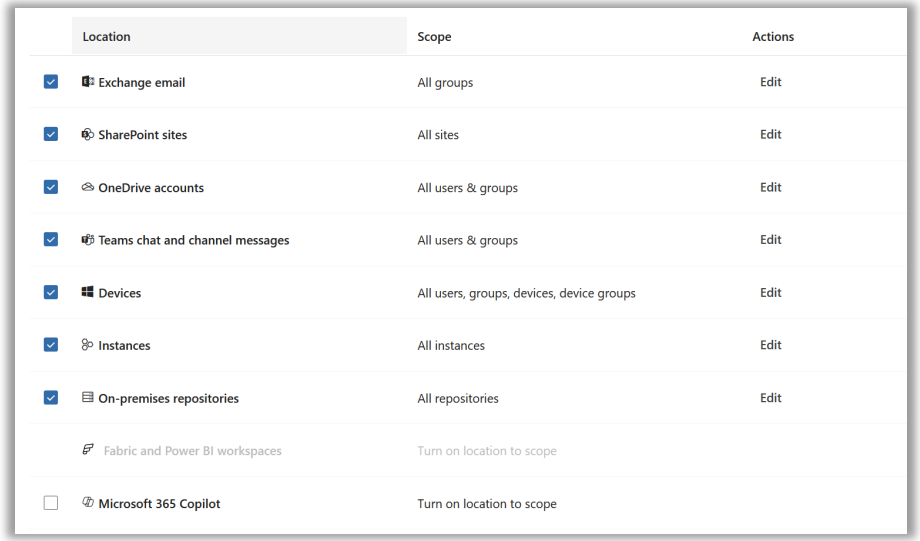
- Helps to ensure an organization's data does not end up where it shouldn't be.
- Can be used to locate and report on sensitive data within the organization.
- Capable of scanning for sensitive data similarly to sensitivity labels, but also works with the foundation set by MPIP to build rules based on a document's sensitivity classification.
- Supports the following locations:
  - Exchange, SharePoint, OneDrive
  - Teams Chat and Channel messages
  - Microsoft Defender for Cloud App Instances
  - On-Premises Repositories (through AIP Scanner)
  - Power BI (currently in preview)



Data Loss Prevention Supported Locations

Through integration with other Microsoft 365 features, Data Loss Prevention can extend to many different locations:

- Windows 10, 11, future versions (via Microsoft Defender and Endpoint DLP)
- MacOS (via Microsoft Defender and Endpoint DLP)
- File shares and on-premises SharePoint environments (via AIP Scanner)
- Non-Microsoft cloud locations (via Defender for Cloud Apps)
    - Dropbox, Box, etc



Data Loss Prevention Supported Locations

	Location	Scope	Actions
☑	Exchange email	All groups	Edit
☑	SharePoint sites	All sites	Edit
☑	OneDrive accounts	All users & groups	Edit
☑	Teams chat and channel messages	All users & groups	Edit
☑	Devices	All users, groups, devices, device groups	Edit
☑	Instances	All instances	Edit
☑	On-premises repositories	All repositories	Edit
	Fabric and Power BI workspaces	Turn on location to scope	
☐	Microsoft 365 Copilot	Turn on location to scope	

Data Lifecycle Management & Records Management

Purview's Approach to Records Management

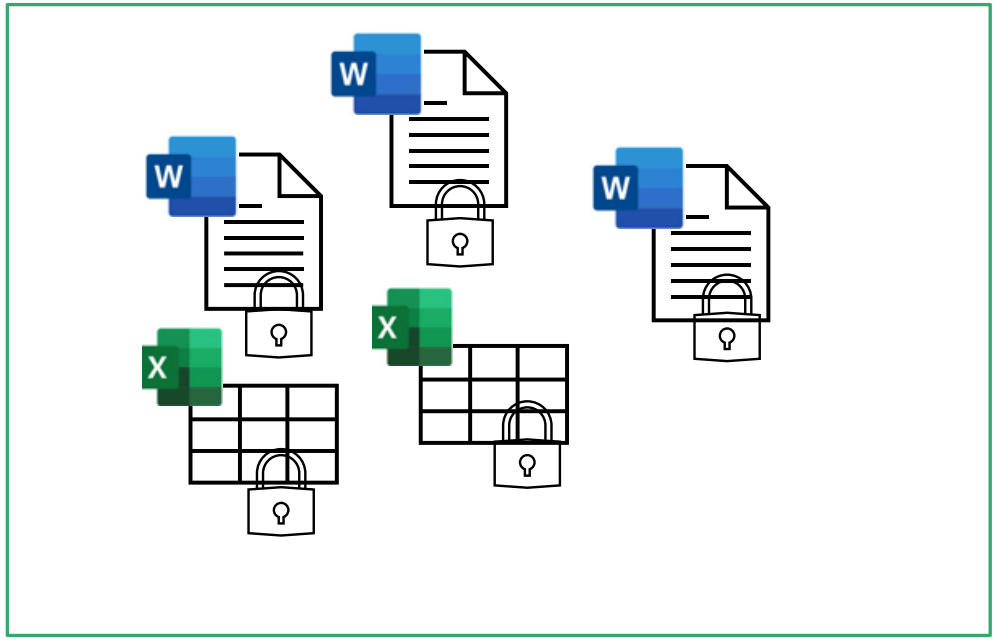
In-Place Records Management	• When declared as a record, data is not moved but maintained at the location it is currently stored. This helps to ensure users know where their data resides. • When documents are archived for retention purposes they do not need to move. Microsoft 365 (M365) tracks and maintains content where it is. • In fact, in order to move a declared record special permissions are required to do so.
Disposition Control	• Once data is no longer required M365 doesn't simply remove it or archive it. – It can do this, but the preferred method is disposition reviews • Disposition reviews allow data owners to determine if data should be maintained or removed.
Information Management is more than Retention	• Labeled data (sensitivity or retention) can be used for easier searchability and organization • Labels applied to data can be used for protecting data. The system can search for particular labels to apply protections to. • Protection of sensitive data is a key component of records management in M365
Balancing the Experience	• Records Management can be invasive. In some cases the processes can be so complex they are no longer user friendly – Things don't get done • M365 provides automation processes to decrease user involvement, but still give the business the required controls to ensure proper data governance.

Records Management

Retention Policies

- Applied to containers and apply a consistent retention policy to all content within the container (Umbrella approach).
- Applied when content is deleted by moving deleted content to a hidden folder or library (only admins can access hidden folder or library)
- Retention period is triggered either on created or last modified date of the content
- Occurs “behind-the-scene”. It is not something that users can directly interact with

Retention Policy

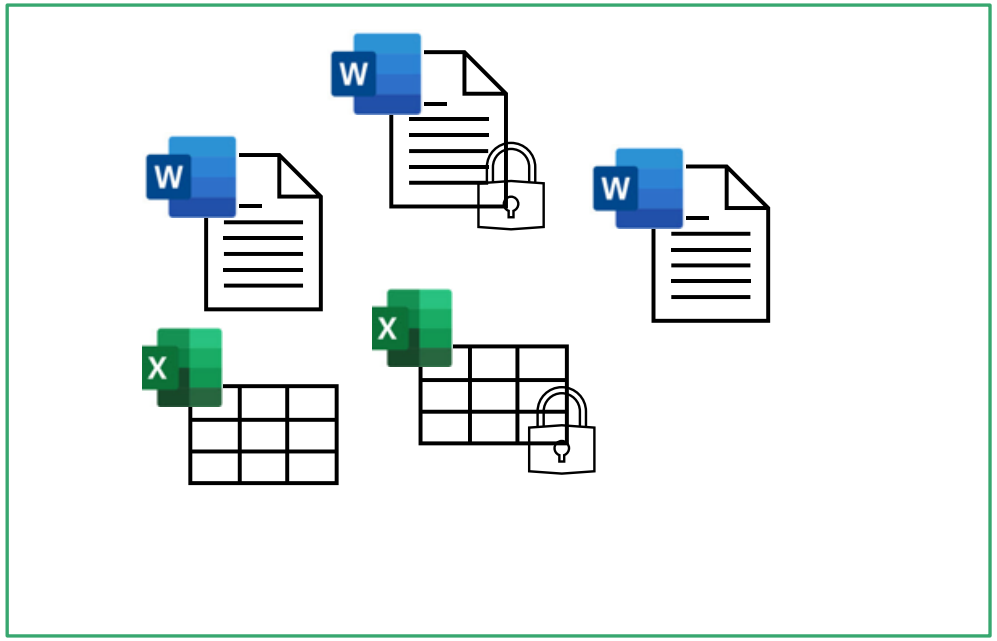


Records Management

Retention Labels

- Enable granular retention periods to be assigned to individual documents and emails within the same container
- Can be manually applied (user interaction) to emails or documents (e.g. user selects a retention label for a file in a SharePoint site or an email)
- Advanced trigger support for retention periods
- Disposition Reviews available
- Event Based retention where retention periods begin based on a non-standard event within an organization (Employee termination, Fiscal Year-End, etc)

Retention Label



eDiscovery

eDiscovery

eDiscovery within Microsoft 365:

- Primarily used for determining content necessary for evidence in any legal actions (internal policies or external legal actions). Allows authorized users to search, investigate and place Office 365 content and conversations on hold
- Can also be used to provide enhanced search capabilities within the Microsoft 365 Platform
- In the event of a legal case, eDiscovery case results can be preserved, exported and analyzed outside of Office 365
  - Retention Label rules will not affect content on hold via eDiscovery

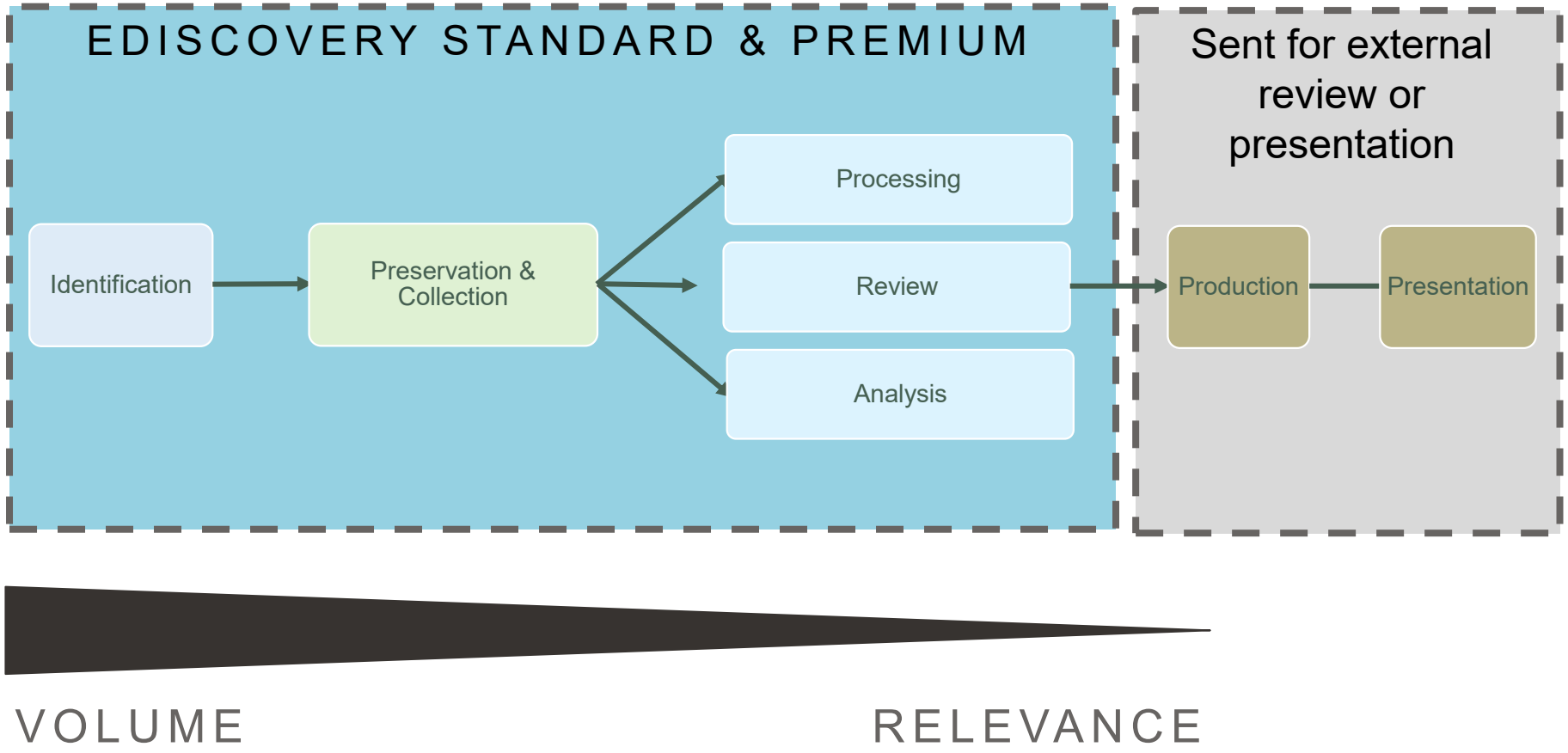
M365 eDiscovery can search:

- Exchange Online Mailboxes
- SharePoint Online Sites
- OneDrive for Business
- Microsoft 365 Groups
- Yammer Groups
- Microsoft Teams
  - When SharePoint site(s) for a team are included in the search

M365 eDiscovery has limited or no ability to search:

- Locally/offline encrypted files uploaded to SharePoint Online, OneDrive, or Microsoft Teams
- Microsoft Team Meeting Recordings

eDiscovery Model

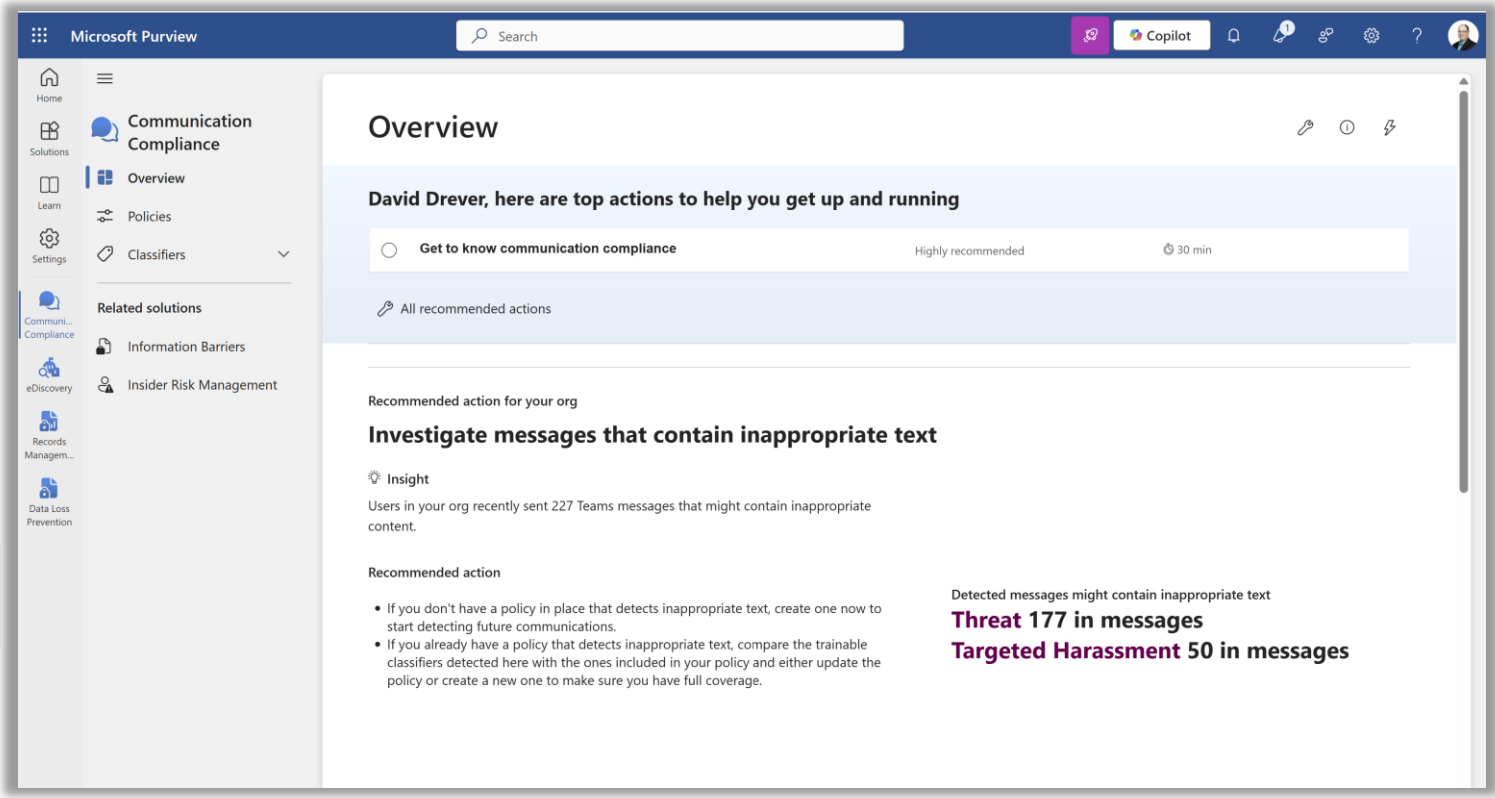


Communication Compliance

Communication Compliance

Communication Compliance within Microsoft 365:

- Primarily used to detect, retain, and alert authorized personnel of inappropriate communication within Microsoft 365 communication pathways:
  - Microsoft Teams chat messages
  - Microsoft Exchange email messages
  - Viva Engage (Yammer) Posts
- Can integrate with eDiscovery to integrate with related cases



Communication Compliance monitors for:

- Inappropriate language
- Sensitive information
- Custom-defined words and phrases based on internal policies (i.e. highly sensitive projects)
- Inappropriate images

Insider Risk Management

Insider Risk Management

"Data doesn't move itself; people move data"

Email

Received a confidential file via email

Messages

Shared a copy of the file with a few colleagues via Teams

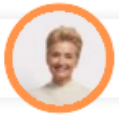
Cloud apps

Uploaded a copy to a personal Dropbox account to share with external vendors

Devices

Downloaded a copy of the file to devices to work offline

Inadvertent



Data expose → Data leak → Data hoarding

Shared storage

Downloaded and deleted an unusual volume of confidential files from SharePoint

Email

Sent a copy of one file to an external recipient via email

Cloud apps

Uploaded two confidential files to a personal Dropbox account

Devices

Printed one confidential file

Saved three confidential files to a USB

Malicious

Data sabotage → Data theft → Data theft → Data theft

Insider Risk Management

Insider Risk Management within Microsoft 365:

- Monitors for inadvertent and malicious activities of users internal to the organization.
- Provides authorized personnel to review and act upon suspicious behavior captured through the various signals within Microsoft 365. Integrates with eDiscovery to build full reviews of content as necessary
- Provides capabilities to protect against internal risks that can lead to:
  - Leaks of sensitive data and data spillage
  - Confidentiality violations
  - Intellectual property (IP) theft
  - Fraud
  - Insider trading
  - Regulatory compliance violations

Common policies Insider Risk monitors for:

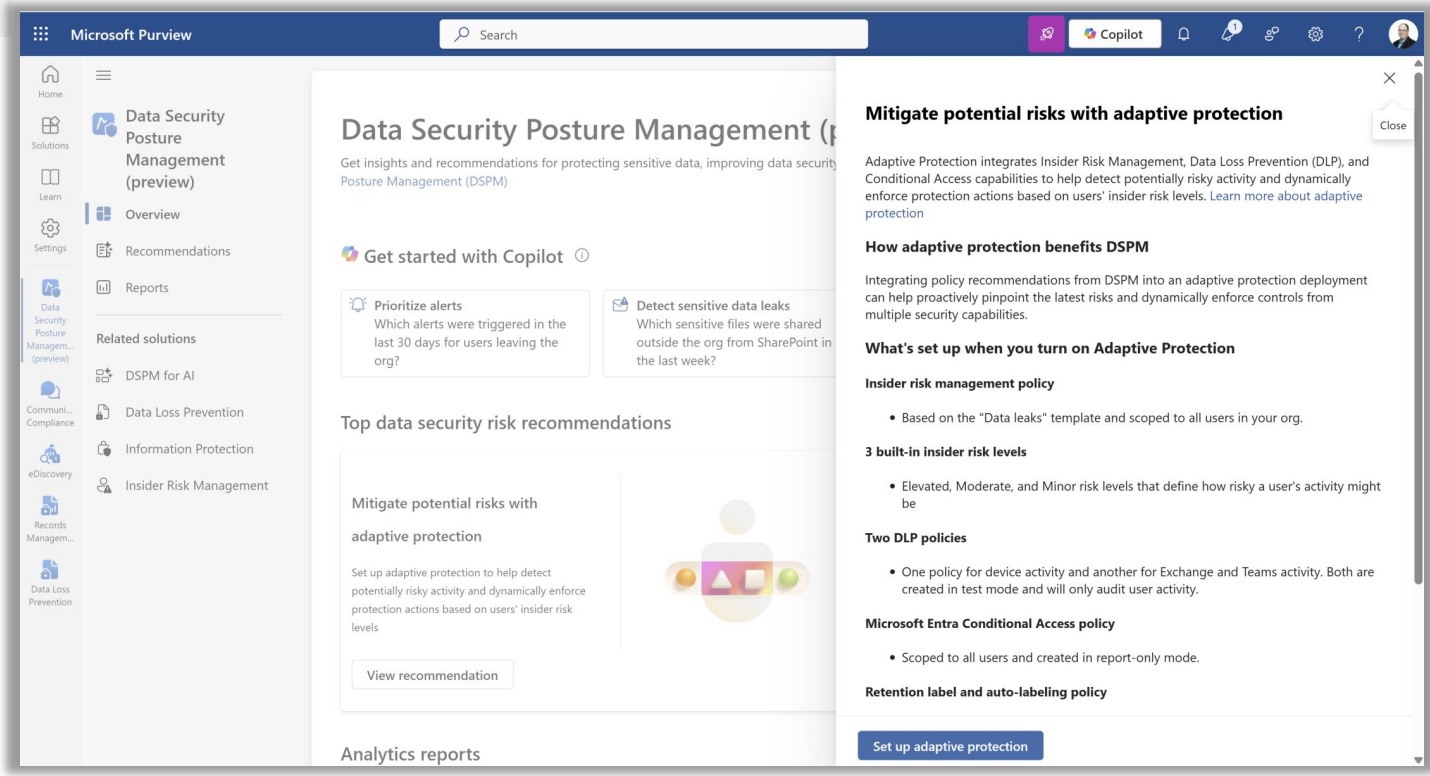
- Data removal by departing employees
  - Monitors exfiltration indicators
  - Can integrate with HR systems to monitor user activity when the HR system is updated for termination
- Risky browser behavior
  - Monitors risky behavior conducted via browsers (e.g., navigating to a risky site)
- Risky AI usage
  - Monitors risky prompts in Copilot and browsing to third-party GenAI sites
  - Can integrate with HR systems to monitor user activity when the HR system is updated for termination

Data Security Posture Management

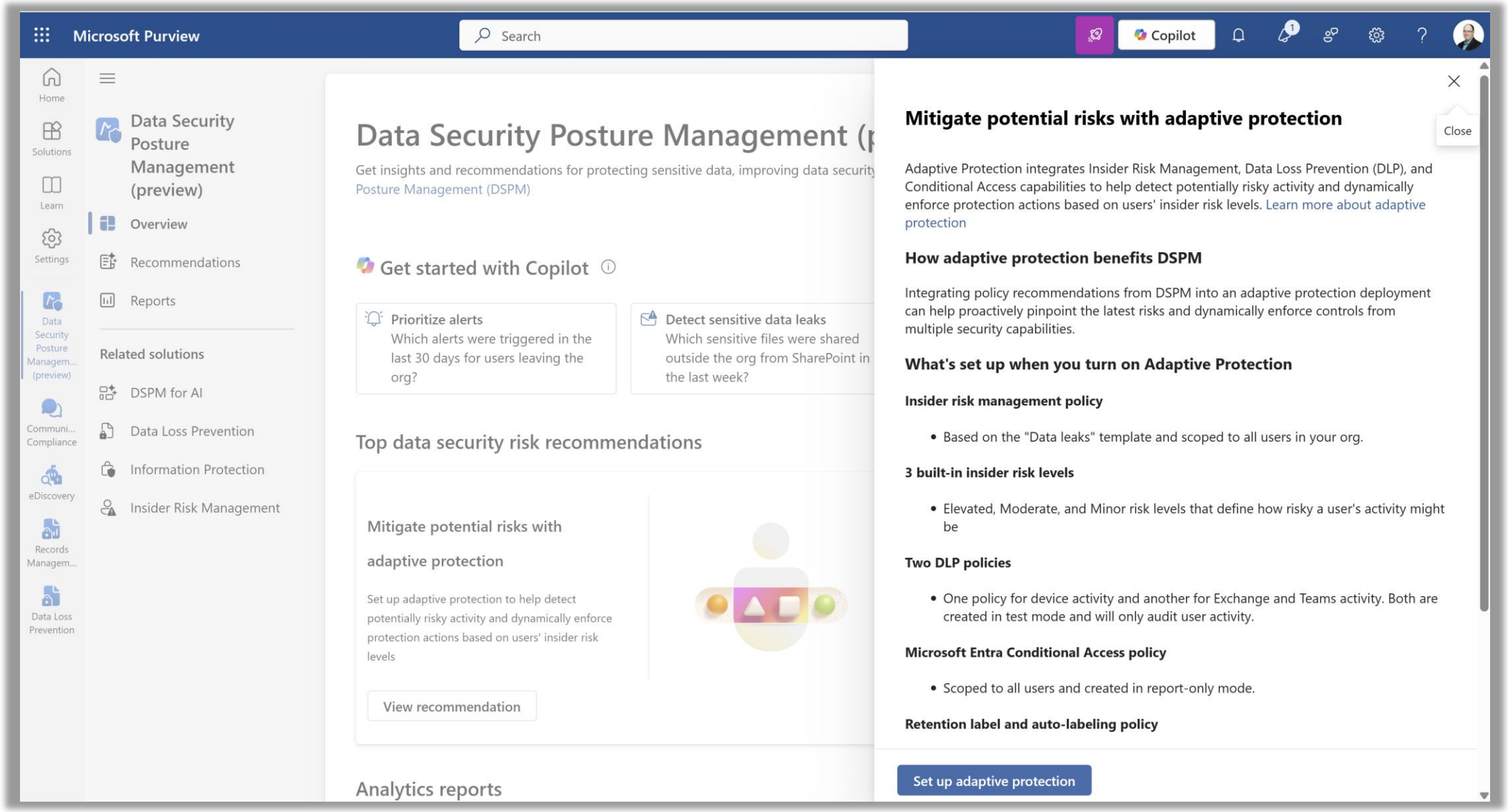
Data Security Posture Management

Monitor Your Content Risk within Microsoft Purview:

- **Data Risk Visibility**: Context-aware insights and continuous assessments to identify and address exposed or unprotected data.
- **Actionable Guidance**: Recommends Insider Risk and DLP policies to reduce data security gaps.
- **Copilot Integration**: Investigate alerts and uncover risk patterns using Microsoft Security Copilot.
- **Posture Analytics**: Trend reports on label usage, DLP coverage, and risky behaviors over time.



Data Security Posture Management

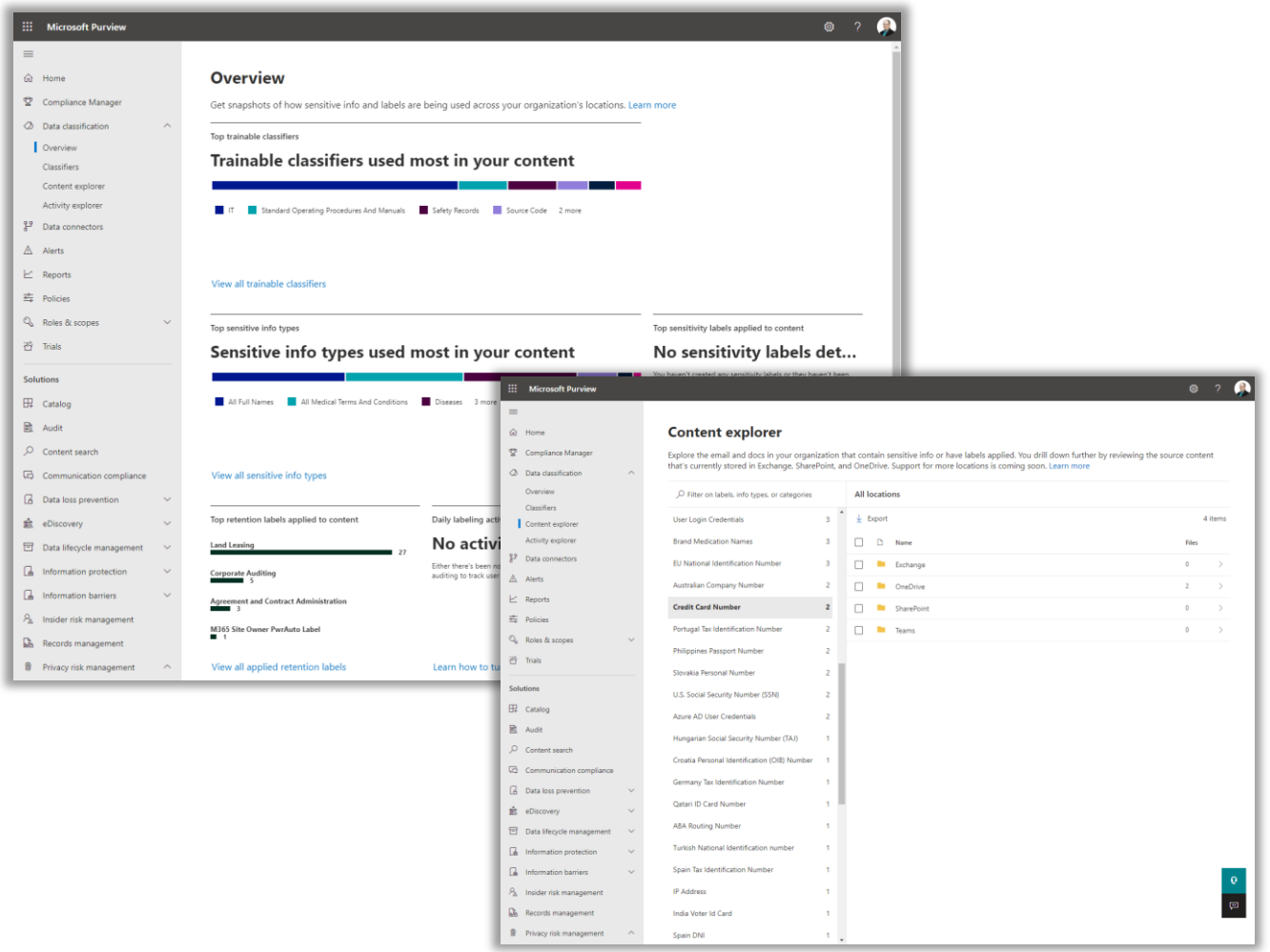


Additional Tools and Solutions within Purview

Additional Tools and Solutions within Purview

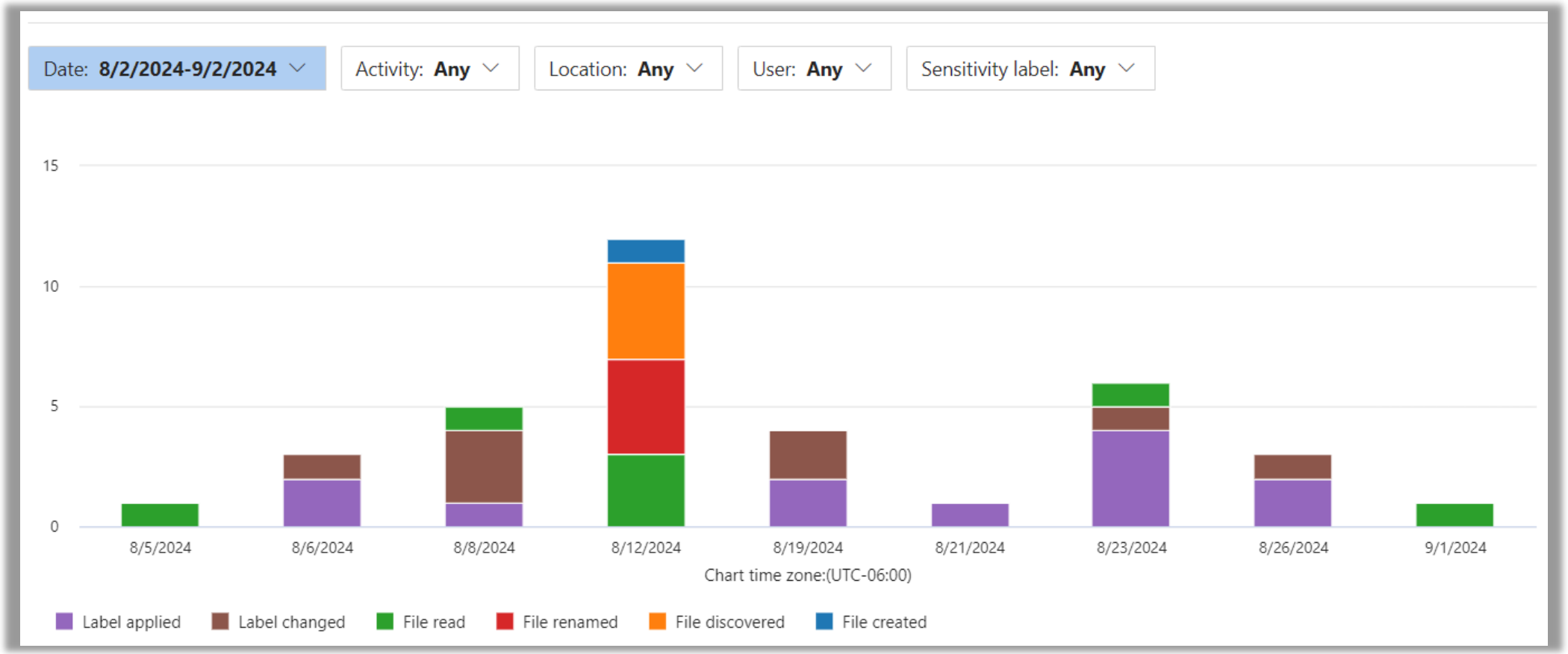
Data Classification Console

- Provides a high-level view into how sensitive information is being tracked within the Microsoft 365 environment
- Monitors sensitivity and retention label usage within the organization
- Provides the ability to create and update custom classifiers and sensitive information types monitored within Microsoft 365
- Provides an overview of sensitive information found within the environment, the type if information, and where it is stored
- Provides dashboards and reports when content is labeled by users or when the labels are removed or modified on content



Activity Explorer

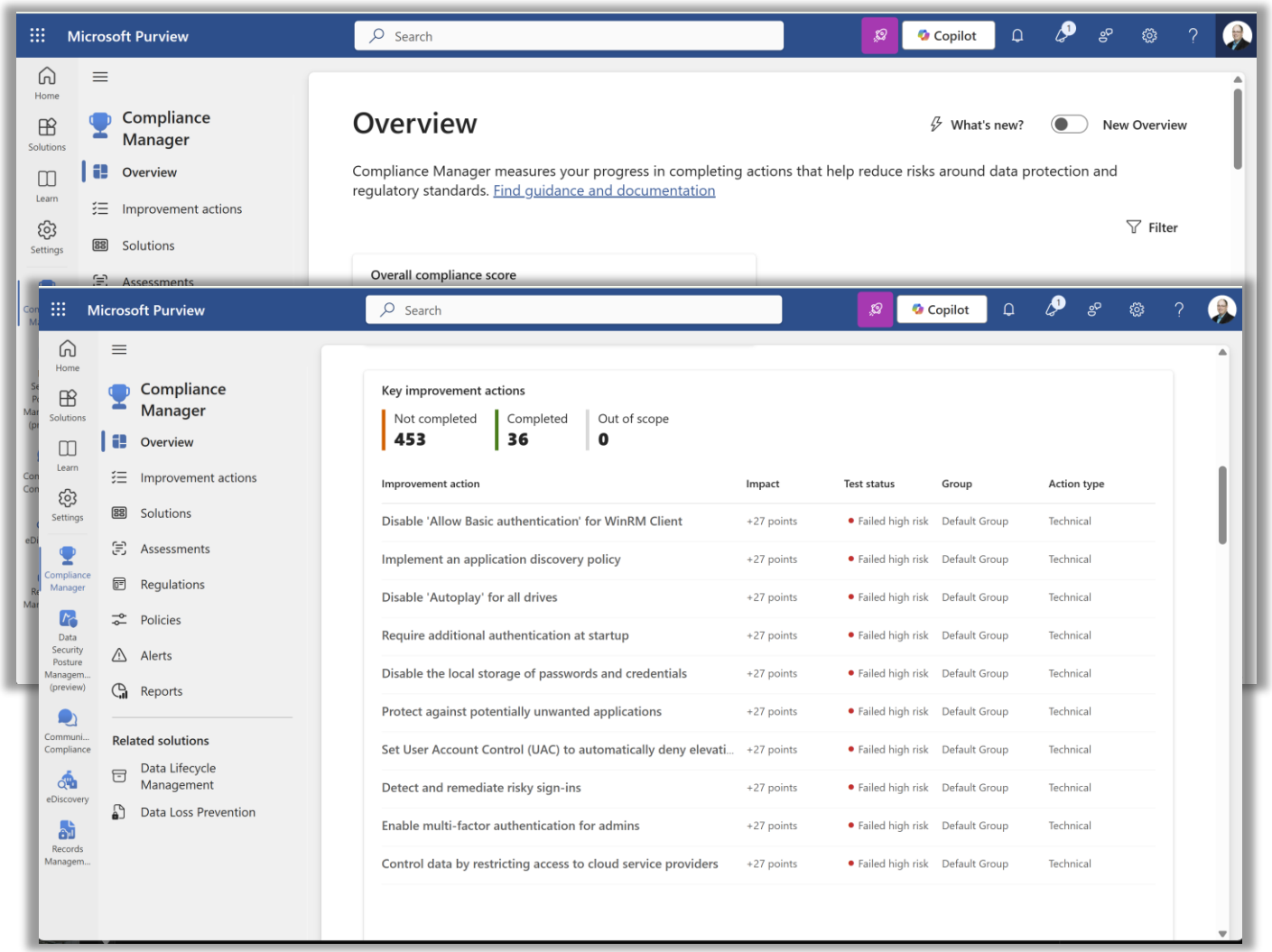
- Supports your Data Protection Program by monitoring what is happening with your labeled content.
- Pulls the data from Microsoft 365 audit logs
- Provides up to 30 days of data



Additional Tools and Solutions within Purview

Compliance Manager:

- Monitors risks to an organization's environment by examining controls configured within the organization to protect its sensitive information and users
- Activities are given a score based on the level of protection offered. The score is then provided to system administrators to provide a high-level view of the environment's compliance risk.
- Capable of applying specific templates to monitor necessary regulatory and legal requirements such as Personal Information Protection and Electronic Documents Act (PIPEDA) and Canadian Consumer Privacy Protection Act (CPPA)
- Over 360 templates available to run against the Microsoft 365 environment



Information Barriers

- Helps to protect conflicts of interest between different departments within the organization.
- Restricts two-way communication between groups within the organization
- Blocks collaboration across the following workloads:
  - MS Teams
    - Chats
    - Instant messaging
    - Meeting inclusion
  - Exchange
    - Information barriers can use Exchange properties to establish a policy but do not currently control communication within Exchange.
    - Mail-flow rules should still be used, or Exchange communication control
  - SharePoint
    - Adding conflicting members to a site
    - Site searches

Implementing Purview

Implementing Purview

Purview Is Always Active

- Most solutions within Purview are active when the tenant is created
  - Lack of organizational-specific configurations
- Consider carefully authorized access within Purview
  - Some solutions can provide views into content regardless of access to the content
  - Some components of Purview require special permissions (can't even be viewed by administrators)
- Map and prioritize the organization's primary goals with the capabilities of Purview

Organizational Recommendations

- Focus on identifying and classifying sensitive information
  - Create sensitivity labels based on approved security classification
  - Pilot deployment of MPIP to protect sensitive information, use lessons learned to deploy organizational-wide.
- Build on the MPIP foundation and pilot Data Loss Prevention within Microsoft 365 workloads.
- Integrate with other tools rolled out or being rolled out within Microsoft 365 (Defender for Endpoint)
- Pilot and deploy records controls to ensure data is maintained for its required lifecycle

Thank you!

David Drever

Associate Director, Protiviti

M365 and Security MVP

https://linktr.ee/davidmdrever

Deep Trivedi

Senior Manager, Protiviti

Microsoft Data Security Adoption & Organizational Change Management

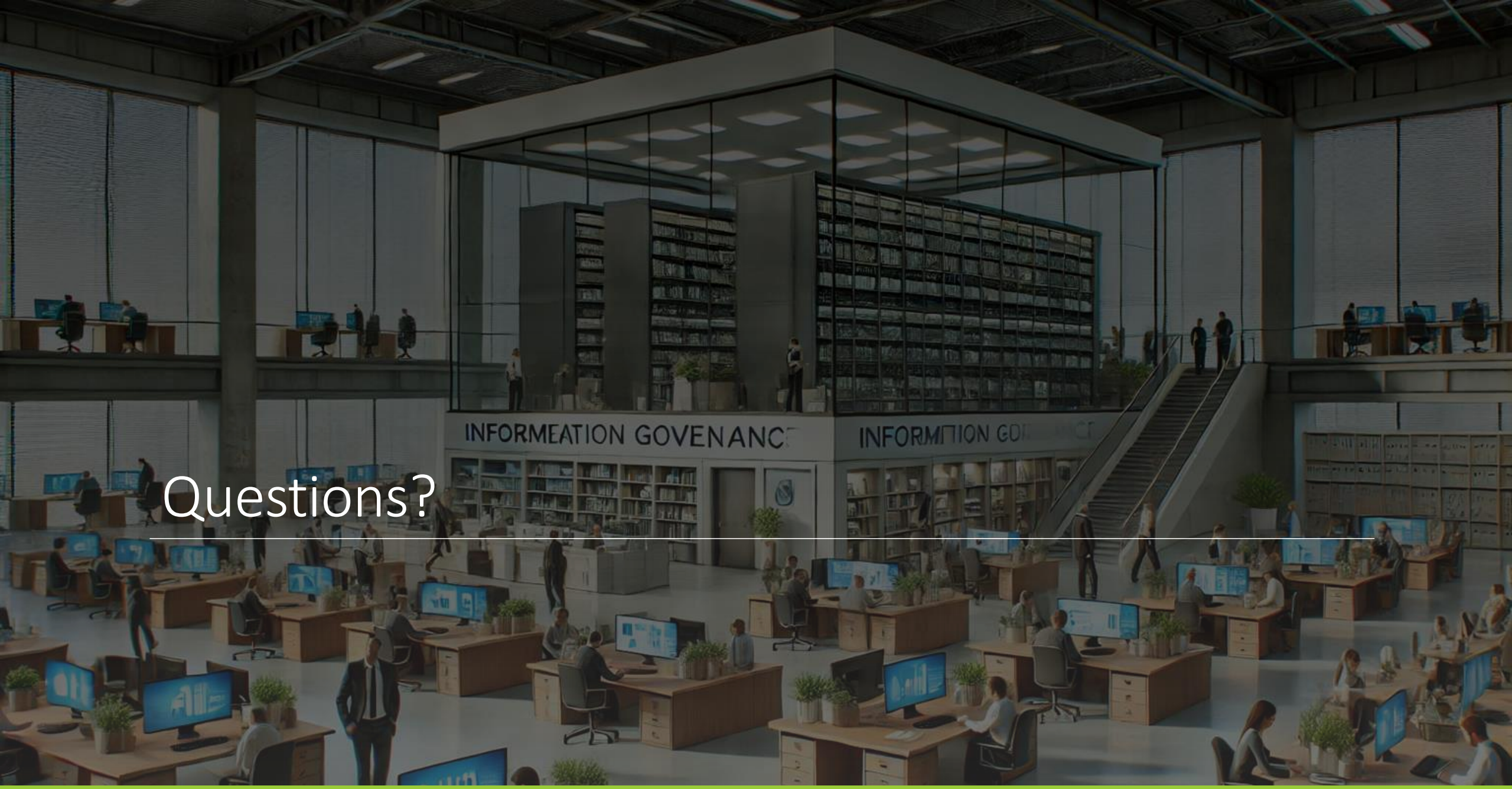
https://linktr.ee/deeptrivedi

Anna Bordioug

Senior Consultant, Protiviti

Microsoft Data Security Specialist

https://linktr.ee/annabordioug



Questions?

Submit session feedback

M365 TWIN CITIES