

I Have Microsoft Purview...Now What?



Records Management

Inside Risk Management

Information Governance

Information Governance

DLP

MIP

OR

How Microsoft Defends Your Data





Please thank our sponsors



About Me



David Drever

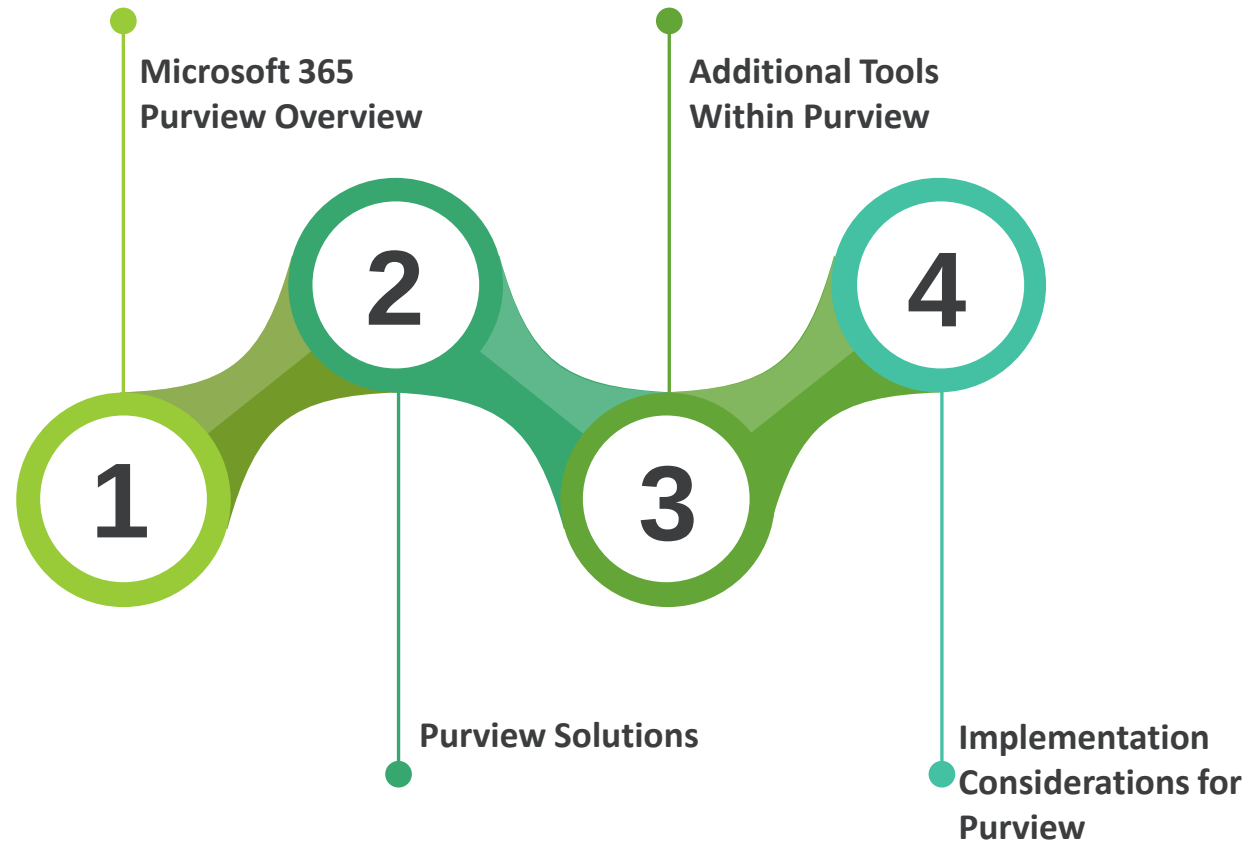
Associate Director, Protiviti

M365 and Security MVP

<https://linktr.ee/davidmdrever>



Today's Topics



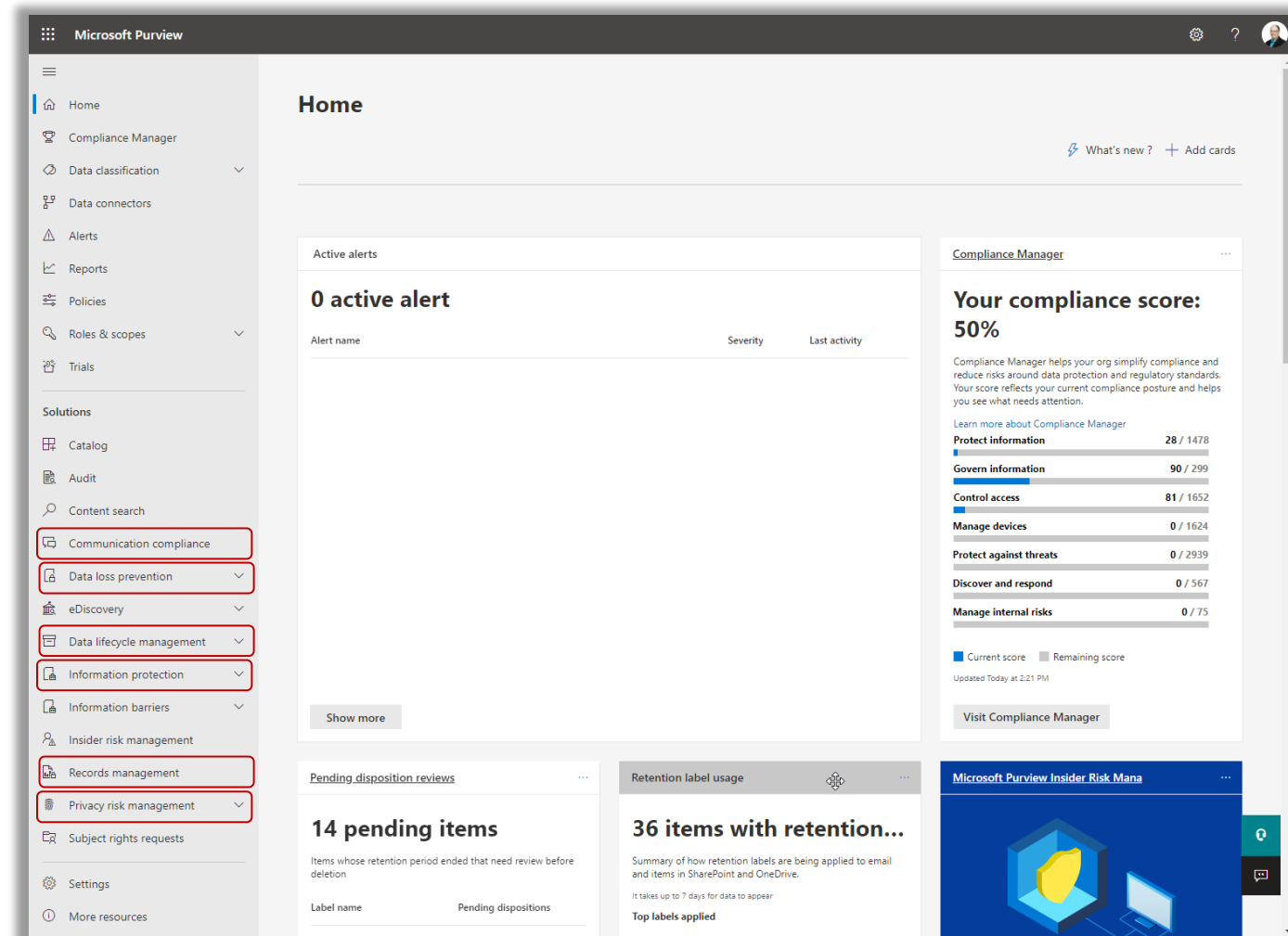


Purview Overview

Microsoft Purview from 50,000 Feet

Purview is a Suite of Products

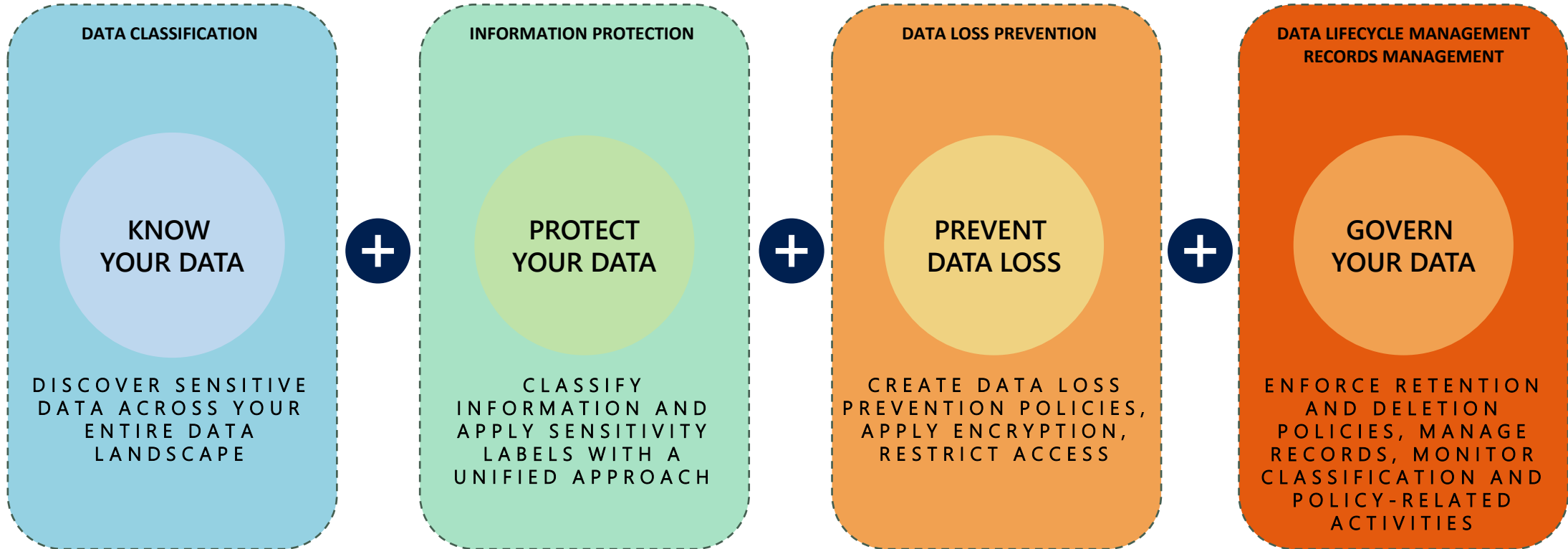
- Purview is not a single tool within Microsoft 365 but is a suite of tools or products.
- Focuses on:
 - Data identification
 - Data Protection
 - Data Governance
- Assists organizations in protecting their sensitive information, whether it is:
 - Sensitive information in documents
 - Records that must be maintained
 - Communication between colleagues
 - Private information within content





Purview's Data Governance Framework

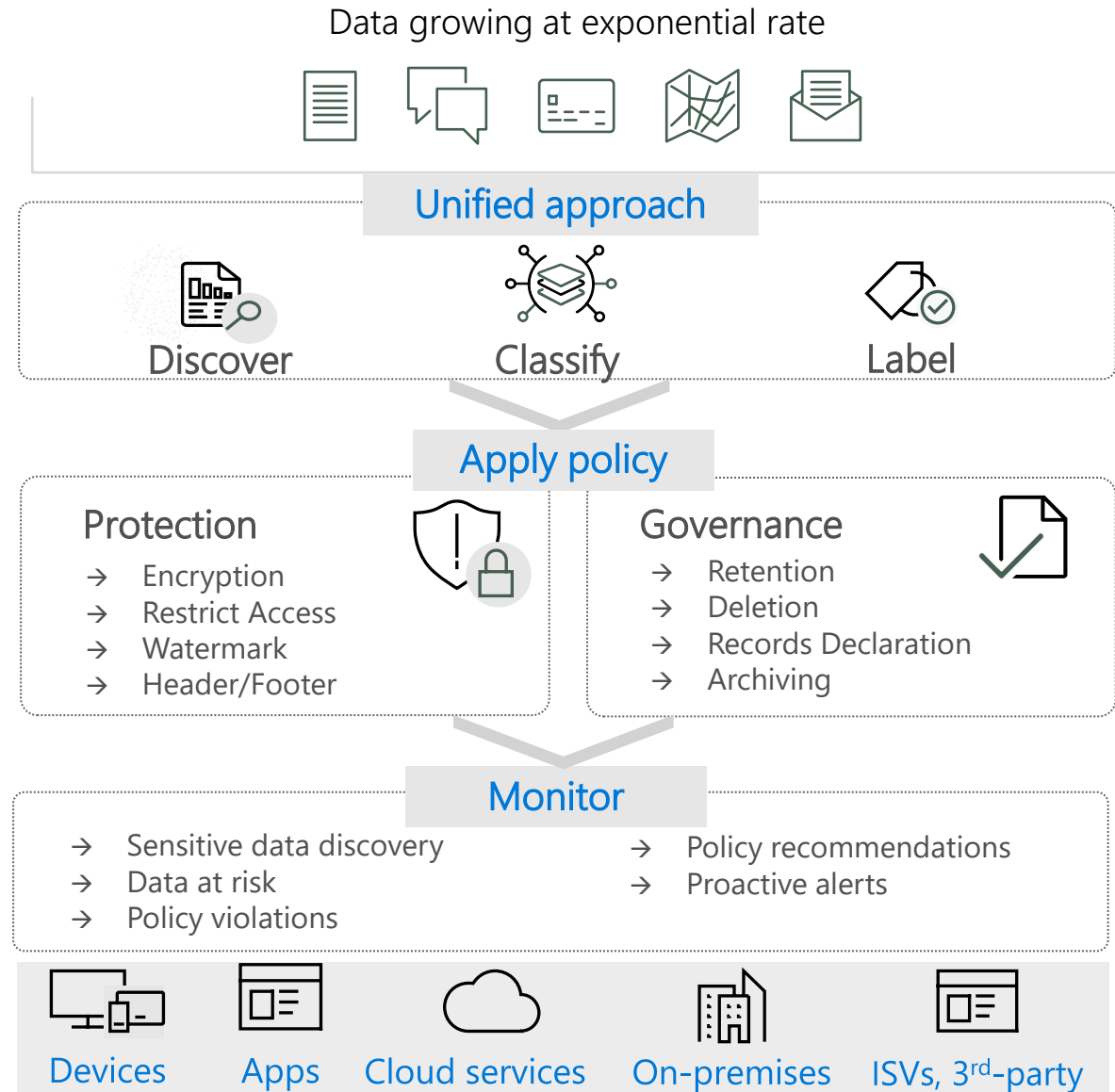
Data Governance Framework



Information Governance and Protection In One Platform

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

- ❖ Unified approach to discover, classify & label
- ❖ Automatically apply policy-based actions
- ❖ Proactive monitoring to identify risks
- ❖ Broad coverage across locations



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

Microsoft Purview's form recognition system for identifying content within the storage locations of the organization.



Exact Data Match (EDM)

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



Document Fingerprinting

Built on phrases and word order to build a "fingerprint" of the document to recognize in others.



The Big Players in Purview

INFORMATION GOVERNANCE

INFORMATION GOVERNANCE



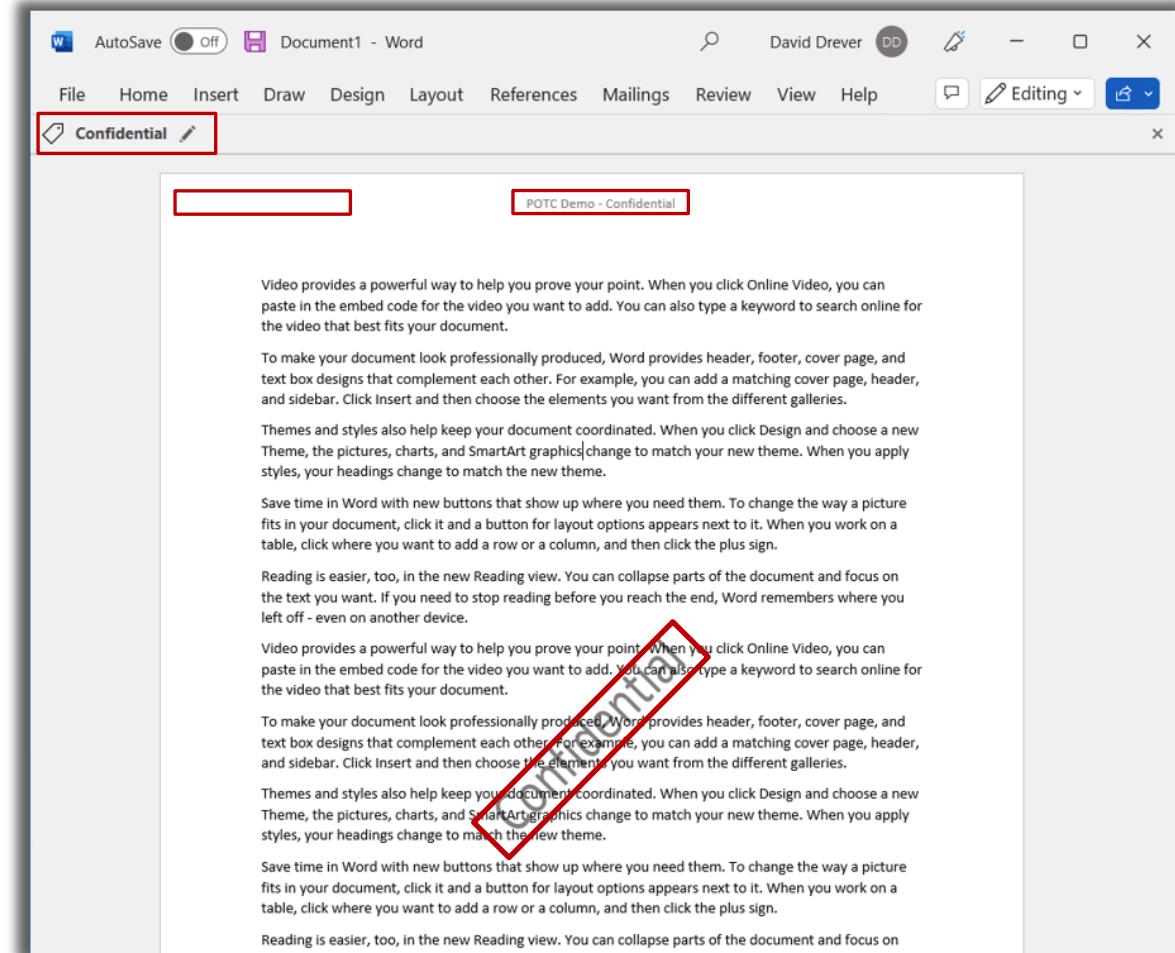
Microsoft Purview Information Protection (MPIP)

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 NOT 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.

The image displays two overlapping screenshots from the Microsoft SharePoint interface. The background screenshot shows the 'SharePoint admin center' with a sidebar menu on the left containing options like Home, Sites, Policies, Settings, Content services, Migration, Reports, and More features. The main content area is titled 'Active sites' and lists site categories: Communication site, Finance (selected), and Internal site. Overlaid on this is a 'SharePoint' site view for a site named 'Finance'. The site view shows a left-hand navigation pane with options like Home, Conversations, Documents, Notebook, Pages, Site contents, and Recycle bin. The main content area displays a 'News' section with a '+ Add' button and a 'Keep your team updated with news on your team site' message. In the bottom right corner, a 'Site Information' dialog box is open, showing fields for 'Site name' (Finance), 'Site description' (Finance), and 'Hub site association'. The 'Sensitivity' dropdown is set to 'None', with other options like 'Public Site', 'Internal Site', and 'Confidential_Restricted Site' visible. 'Save' and 'Cancel' buttons are at the bottom of the dialog.

Microsoft Purview Information Protection

The screenshot shows a SharePoint site for 'Product Engineering' (PE). The left sidebar contains navigation links: Home, Conversations, Documents, Notebook, Pages, Site contents, Recycle bin, and Edit. The main content area has a 'News' section with an 'Add News' button and an 'Activity' section with a table of records. A 'Sensitivity' pane is open on the right, showing three sensitivity levels: Public area, General area, and Confidential area, each with a description and a 'Done' button.

SharePoint Search this site

PE Product Engineering Private group | C

+ New ▾ ⚙ Page details 📊 Analytics

News
+ Add ▾

Keep your team updated
From the site home page you can post a status update, trip report, or...

Add News

Activity

Email	CC Type	CCN	CNC	Expiry Date
john.d@domain.com	Mastercard	5279 4287 9409 1818	325	2018/06/28
john.d@domain.com	Mastercard	5279 4287 9409 1818	713	2018/12/12
john.d@domain.com	Visa	4024 5796 5245 4247	250	2018/12/12
john.d@domain.com	Mastercard	5185 1837 3079 0221	612	2018/12/12
john.d@domain.com	Mastercard	5279 4287 9409 1818	325	2018/06/28

Temporary document 3

Sensitivity

Public area
A collaborative area that guests can be invited into. Documents can be freely shared with anyone within and outside of the organization. This site can be accessed from any unmanaged device.

General area
An internal area designated for various types of content and documents related to the operation and management of our organization. Documents can be shared outside of our organization as required. Membership to this area is controlled, including guest access.

Confidential area
This is a secure and restricted area where sensitive and confidential information is stored and accessed only by authorized personnel.

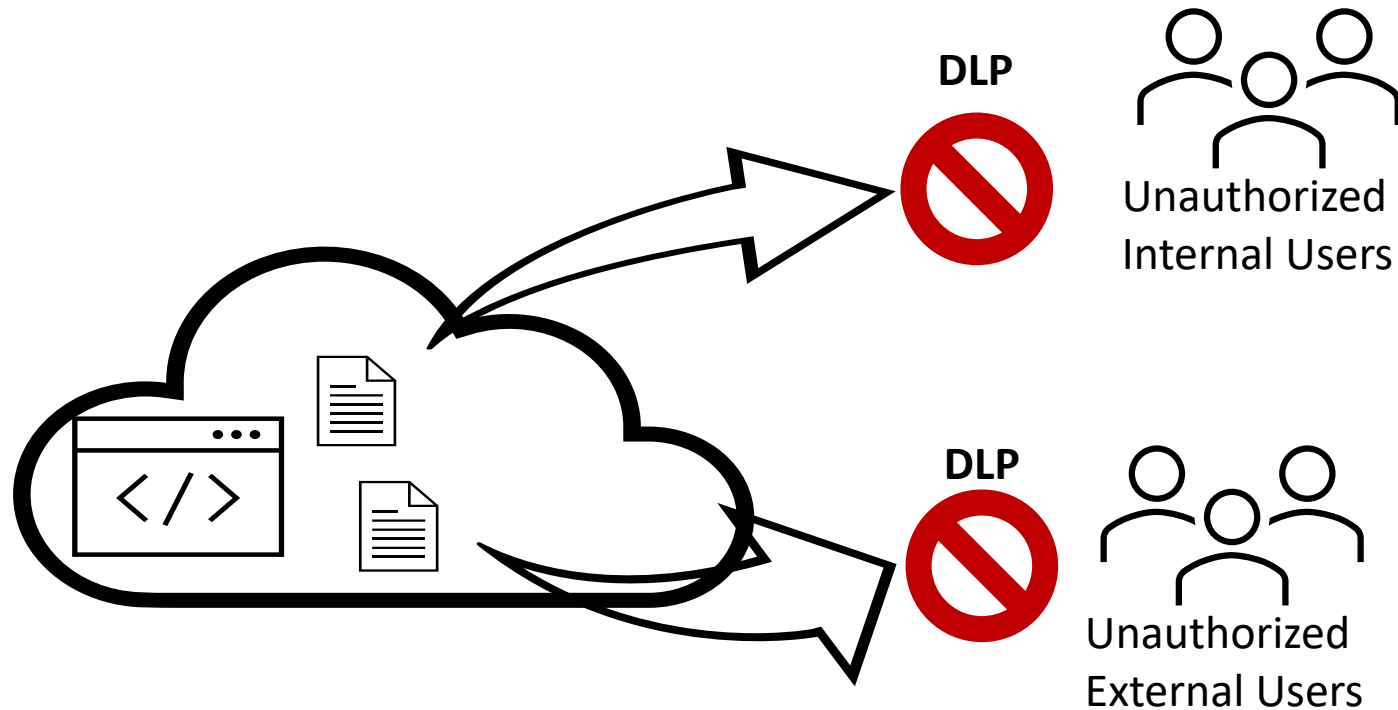
Done



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 MIP 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)

The screenshot shows a SharePoint library named 'Human Resources'. A file named 'Account Test.xlsx' is highlighted with a red box. A policy tip for this file is displayed, stating: 'Policy tip for 'Account Test.xlsx'. This item is protected by a policy in your organization. Issues: Item contains the following sensitive information: Credit Card Number. Last scanned: About a minute ago. Report an issue to doesn't conflict with'.

The file 'Account Test.xlsx' is an Excel spreadsheet. The first sheet, 'Sheet1', contains a table with two columns: 'First and Last Name' and 'SSN'. The table contains six rows of data:

First and Last Name	SSN
Robert Aragon	489-36-8350
Ashley Borden	514-14-8905
Thomas Conley	690-05-5315
Susan Davis	421-37-1396
Christopher Diaz	458-02-6124
Rick Edwards	612-20-6832

Below the table, a red box highlights a warning message: 'This item contains sensitive information. All recipients must be authorized to receive this content. View policy tip'.

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

Status	Location	Included	Excluded
☒ On	 Exchange email	All Choose distribution group	None Exclude distribution group
☒ On	 SharePoint sites	All Choose sites	None Exclude sites
☒ On	 OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group
☒ On	 Teams chat and channel messages	All Choose account or distribution group	None Exclude account or distribution group
☒ On	 Devices	All Choose user or group	None Exclude user or group
☒ On	 Microsoft Defender for Cloud Apps	All Choose instance	None Exclude instance
☒ On	 On-premises repositories	All Choose repositories	None Exclude repositories
☐ Off	 Power BI		

Data Loss Prevention Supported Locations

Status	Location	Included	Excluded
☒ On	 Exchange email	All Choose distribution group	None Exclude distribution group
☒ On	 SharePoint sites	All Choose sites	None Exclude sites
☒ On	 OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group
☒ On	 Teams chat and channel messages	All Choose account or distribution group	None Exclude account or distribution group
☒ On	 Devices	All Choose user or group	None Exclude user or group
☒ On	 Microsoft Defender for Cloud Apps	All Choose instance	None Exclude instance
☒ On	 On-premises repositories	All Choose repositories	None Exclude repositories
☐ Off	 Power BI		



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

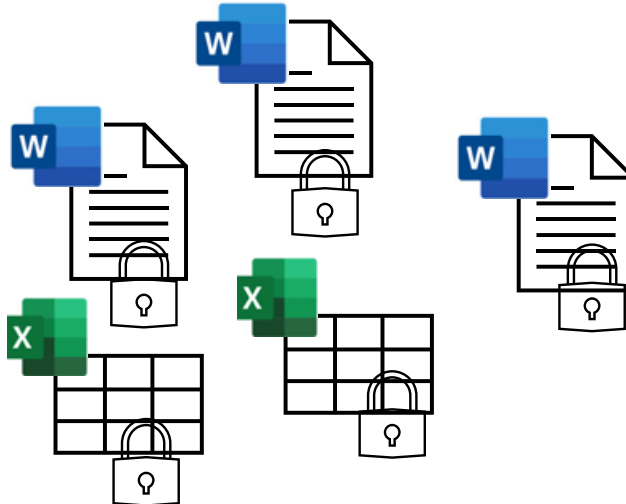
- Records Management can be invasive. In some cases the processes can be so complex they are no longer user friendly
 - Things don't get done
- M365 provides automation processes to decrease user involvement, but still give the business the required controls to ensure proper data governance.

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-scenes”. It is not something that users can directly interact with

Retention Policy

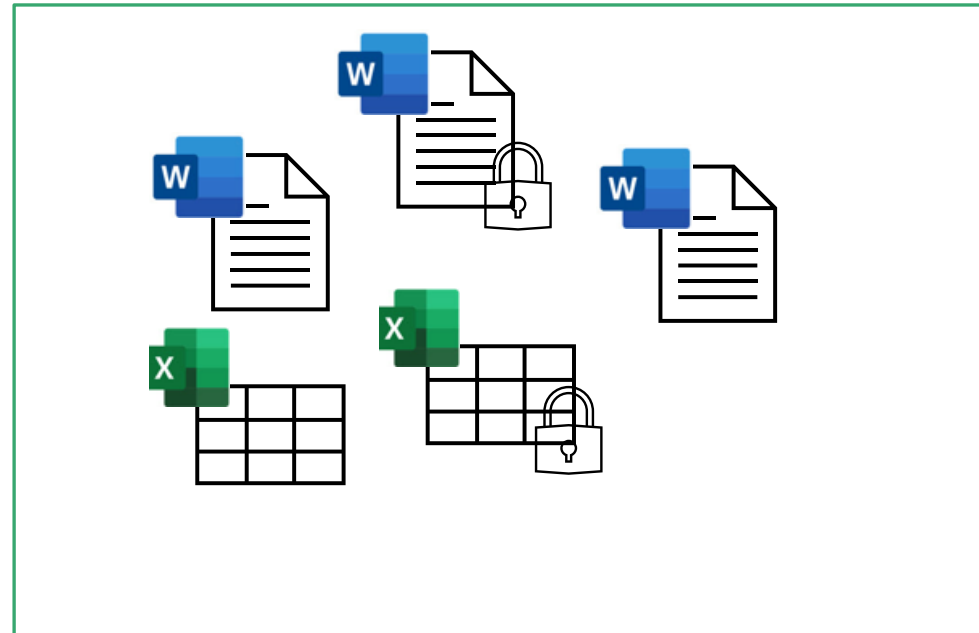


Records Management

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



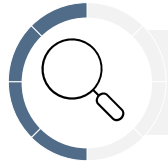


eDiscovery

INFORMATION GOVERNANCE

INFORMATION GOVERNANCE

eDiscovery



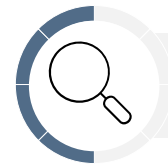
eDiscovery within Microsoft 365:

- 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:

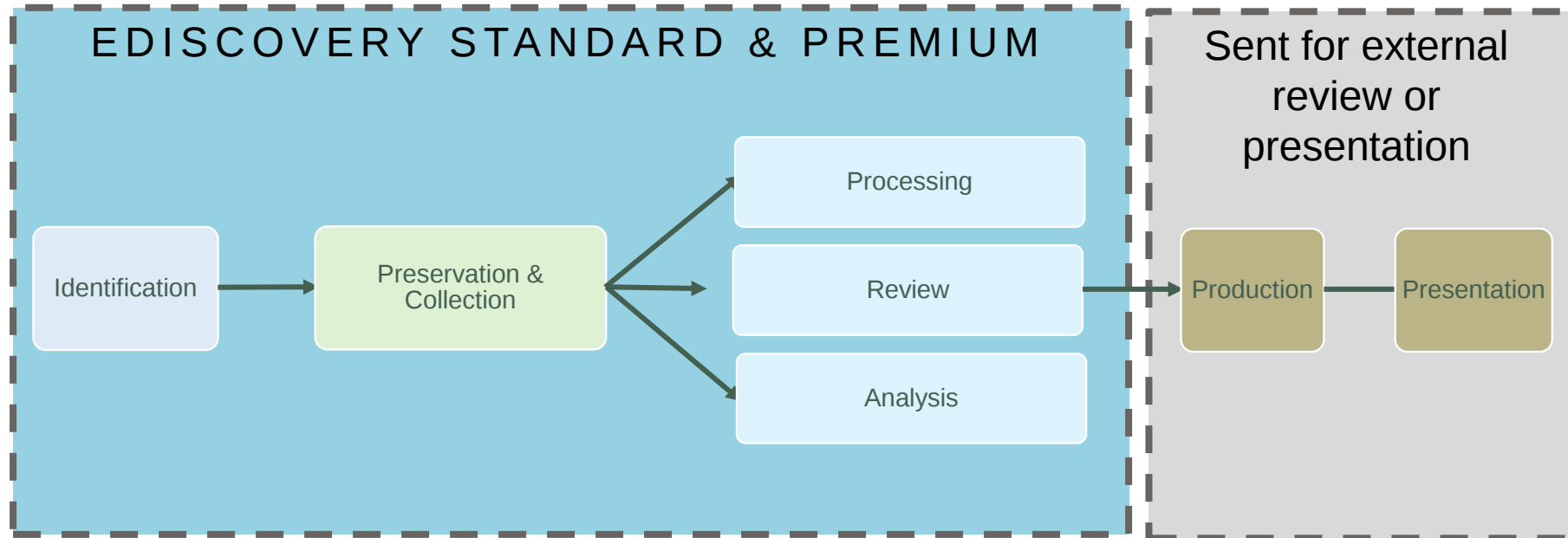
- Exchange Online Mailboxes
- SharePoint Online Sites
- OneDrive for Business
- Microsoft 365 Groups
- Yammer Groups
- Microsoft Teams
 - When SharePoint site(s) for a team are included in the search



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

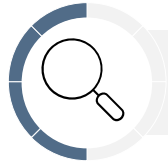


VOLUME **RELEVANCE**



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

The screenshot shows the Microsoft Purview Communication Compliance dashboard. The left sidebar contains a navigation menu with options like Compliance manager, Data classification, Data connectors, Alerts, Reports, Policies, Roles & scopes, Trials, Solutions, Catalog, Audit, Content search, Communication compliance (selected), Data loss prevention, eDiscovery, Data lifecycle management, Information protection, Information barriers, Insider risk management, Records management, Privacy risk management, Subject rights requests, Settings, More resources, and Customize navigation. The main content area is titled 'Communication compliance' and has tabs for 'Overview' and 'Policies'. Below the tabs, a message from David Drever states: 'David Drever, here are top actions to help you get up and running'. A table lists four recommended actions: 'Get to know communication compliance' (Highly recommended, 30 min), 'Assign permissions to ensure your team can get their jobs done' (Required, 15 min), 'Create distribution groups for users' whose communications you want to detect' (Optional, 15 min), and 'Create your first policy to start detecting communications' (Required, 10 min). Below this table is a link for 'All recommended actions'. The section 'Recommended action for your org' is titled 'Take control of sensitive info in messages' and includes an 'Insight' section stating that 11 Teams and 103 email messages contain sensitive info. It provides a 'Recommended action' with two bullet points: 'If you don't have a policy in place that detects sensitive info, create one now to start detecting future communications.' and 'If you already have a policy that detects sensitive info, compare the info types detected here with the ones included in your policy and either update the policy or create a new one to make sure you have full coverage.' A 'Create Policy' button is visible. On the right, a section titled 'Messages that include sensitive info types' shows a list of detected sensitive info types: 'All Full Names', 'New Zealand Driver License Number', 'All Credential Types', 'Slovenia Tax Identification Number', and 'General Password'. A progress bar indicates that 11 more info types were detected.



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



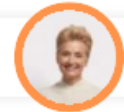
Data expose



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



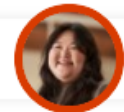
Data theft



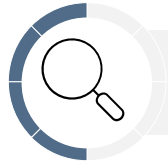
Data theft



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



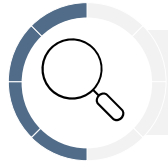
Common policies Insider Risk monitors for:

- 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
- Security Policy Violations
 - Can integrate with Defender for Endpoint to monitor suspicious activity occurring directly on organization-owned workstations



Privacy Risk Management

Insider Risk Management



Privacy Risk Management within Microsoft Purview:

- Where MPIP and DLP focus on the organization's sensitive information, MPRM focuses on identifying privacy risks within the organization.
- MPRM focuses on:
 - Oversharing of personal data
 - Sharing of personal data across departments or even GEO locations.
 - Unused personal data stored by the organization
- Create Policies to scan and alert identified stakeholders when private data risks are identified.



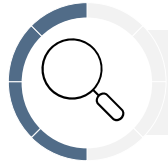
Common policies Privacy Risk monitors for:

- Data Overexposure
 - Monitors for private information that is shared or made available to too many people both within and outside the organization.
 - Supports multiple cloud locations including Azure Storage, Azure SQL, and Amazon S3
- Data Transfers
 - Identify boundaries within the organization:
 - Team
 - Department
 - Regions
 - Etc
 - Monitor content that crosses these boundaries
- Data Minimization
 - Scans for unused (read or modified) content that contains private information

Additional Tools and Solutions within Purview

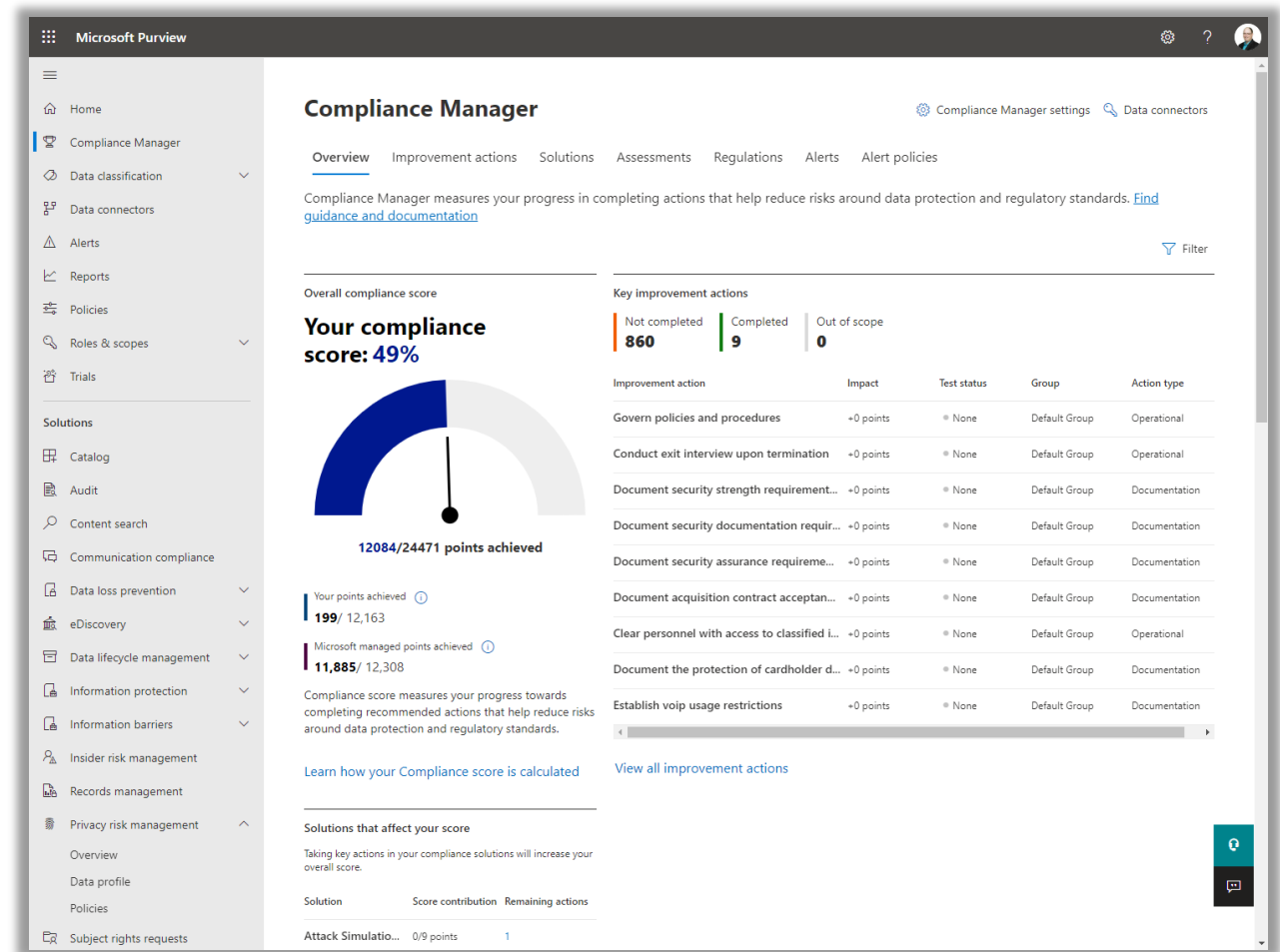


Additional Tools and Solutions within Purview

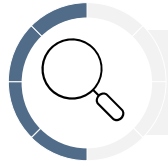


Compliance Manager:

- 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

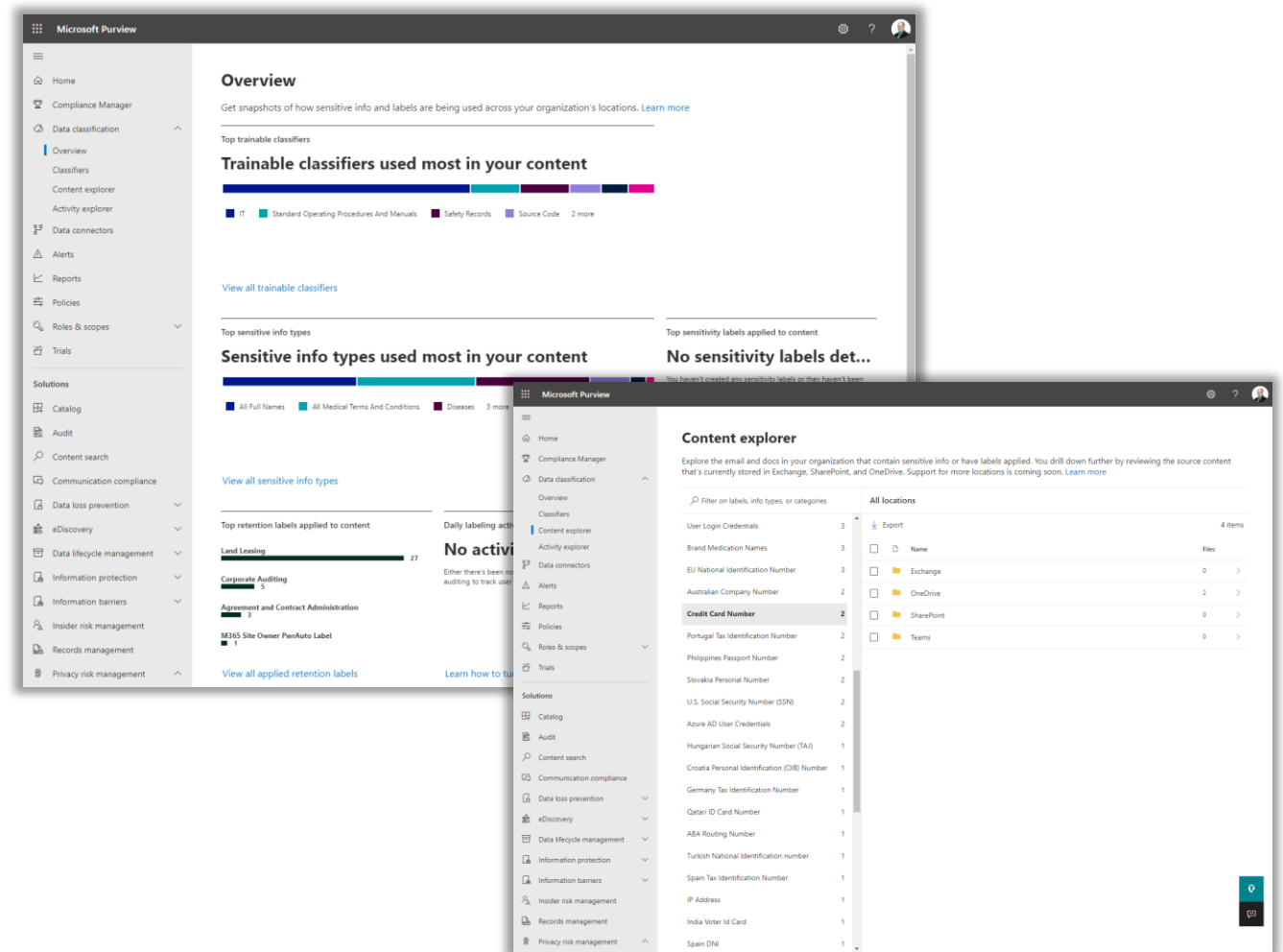


Additional Tools and Solutions within Purview



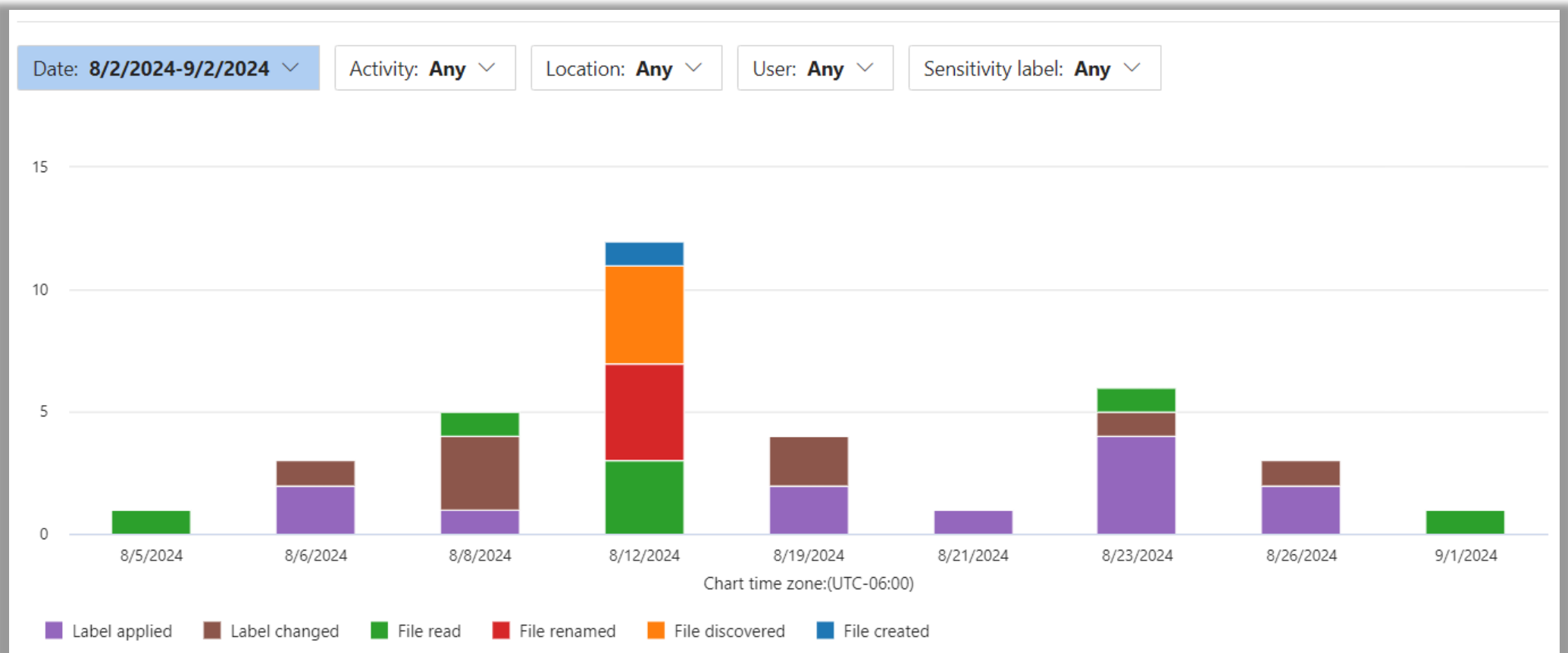
Data Classification Console

- 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 of 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



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 MIP to protect sensitive information, use lessons learned to deploy organizational-wide.
- Build on the MIP 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

Submit session feedback



THANK YOU



David Drever

Associate Director, Protiviti

M365 and Security MVP

<https://linktr.ee/davidmdrever>

