Know, Protect & Govern your data

MS Purview Information Protection discovers, classifies, and protects sensitive and busines critical content throughout its lifecycle across the org. (import, store, classify).

- Know your data - orgs can understand their data landscape and identify important data across on-prem, cloud, and hybrid envs (trainable classifiers, activity explorer, content exporer)
- Protect your data - orgs can apply flexible protection actions (encryption, access restrictions, visual markings)
- Prevent data loss - orgs can detect risky behaviour and prevent accidental oversharing of sensitive info (data loss prevention policies, endpoint data loss prevention)
- Govern your data - Orgs can automatically keep, delte and store data in a compliant manner (retention policies, retention labels, records management)

Data classification capabilties of compliance portal

MS Purview provides 3 ways of identifying items to be classified:

- manually by users
- automated pattern recognition (sensitive information types)
- machine learning

Sensitive Information Types (SIT)

Pattern based classifiers. Purview has many built in:

- Credit card numbers
- Passport or identification numbers
- Bank account numbers
- Health service numbers

Trainable classifiers

AI & ML that classify org data. Two types available:

- Pre-trained (MS has created and trained them so you can use them immediately)

- Custom trainable (contracts, invoices, customer records)

! only works with items that are not encrypted !

Sensitivity labels and policies

Enable labling and protection of content without affecting productivity or collaboration.

Labels are:

Customisable: Admins can create different categories specific to org e.g. Personal, Public, Confidential, Highly Confidential

Clear text: Because each label is stored in clear text in metadata, third party apps can apply own protective actions if necessary

Persistent: After applying label, it is stored in emtadate of email or ducment (which moves with content, including protection settings)

Each item supporting sensitivity labels can only have one label applied at a time!

Sensitivity labels can be configured to:

- Encrypt
- Mark content (e.g. watermarks, headers or footers)
- Apply label automatically
- Protect content in containers such as sites and groups
- Extend sensitivity labels to third party apps and services
- Classify content without using any protection settings

After sensitivity labels are created, they need to be published to make them available to people and services in the org - published to users or groups through label policies. These allow admins to:

- Choose users and groups that can see labels
- Apply a default label (users can change label if they think there is a more appropriate one)
- Require justification for label changes
- Require users to apply a label (mandatory labelling)

- Link users to custom help pages

Data loss prevention

MS Purview Data Loss Prevention (DLP) is a way to protect sensitive info and prevent inadvertant disclosure. With DLP policies admins can:

- Identify, monitor, and protect sensitive information across M365 (OneDrive for Business, SharePoint Online, MS Teams, Exchange Online)
- Help users learn how compliance works without interrupting workfrlow.
- View DLP reports

DLP policies enforce rules that conssit of:

- Conditions that the content has to match before rule is enforced
- Actions that the admin wants the rule to take automatically when it matches a condition
- Locations wehre the policy will apply (e.g. Exchange, SharePoint, OneDrive)

Endpoint data loss prevention

Endpoint DLP extens activity monitoring of DLP to items physically stored on Win 10, 11 and MacOS (Catalina 10.15+). It can audit activities users do such as:

- Creating an item
- Renaming an item
- Copying items to removable media
- Copying items to network shares
- Printing documents
- Accessing items using unallowed apps and browsers

Also extends to MS Teams (so users cannot share sensitive info via chat and channel messages)

Retention Policies and retention labels

Helps orgs manage and govern info by ensuring it is only kept for a require time, then permanently deleted. This can:

- Comply proactively with industry regulations and policies
- Reduce risk when there's litigation or a security breach
- Ensure users only work with content that is current and relevant to them

Policies

Are used to assign the same retention settings to content at a site or mailbox level. A single policy can be applied to multiple locations (or specific locations and users). Items inherit the retention settings from their container specified in retention policy.

Labels

Are used to assign retention settings at an item level (folder, doc, email). Retention settings move with document/content. Admins can enable users to apply label manually. A label can be applied automatically if certain conditions are met.

Records management

Orgs of all types require a management solution to manage regulatory, legal, and business critical records across corp data. It also helps to demonstrate compliance. MS Purview Records Management includes:

- Labeling content as record
- Establishing retention and deletion policies within record label
- Triggering event-based retention
- Reeviewing and validating disposition
- Proof of records deletion
- Exporting information about disposed items

Common use cases for records management

- Enabling admins and users to manually apply retention and deletion actions for docs and emails
- Automatically applying retention and deleting actions for docs and emails
- Enable sit admins to set default retain and delte actions for all content in a Sharepoint library, folder, or doc set

- Enable users to automatically apply retain and delete actions to emails using Outlook rules