Microsoft Information Protection

Protect your data using labels

- Customizable
- Persists as container metadata or file metadata
- Readable by other systems
- Determines DLP policy based on labels
- Extensible to partner solutions

- Manual or Automated Labels
- Apply to content or containers
- Label data at rest, data in use, or data in transit
- Enable protection actions based on labels
- Seamless end user experience across productivity applications

Control access to your data and documents

The problem:

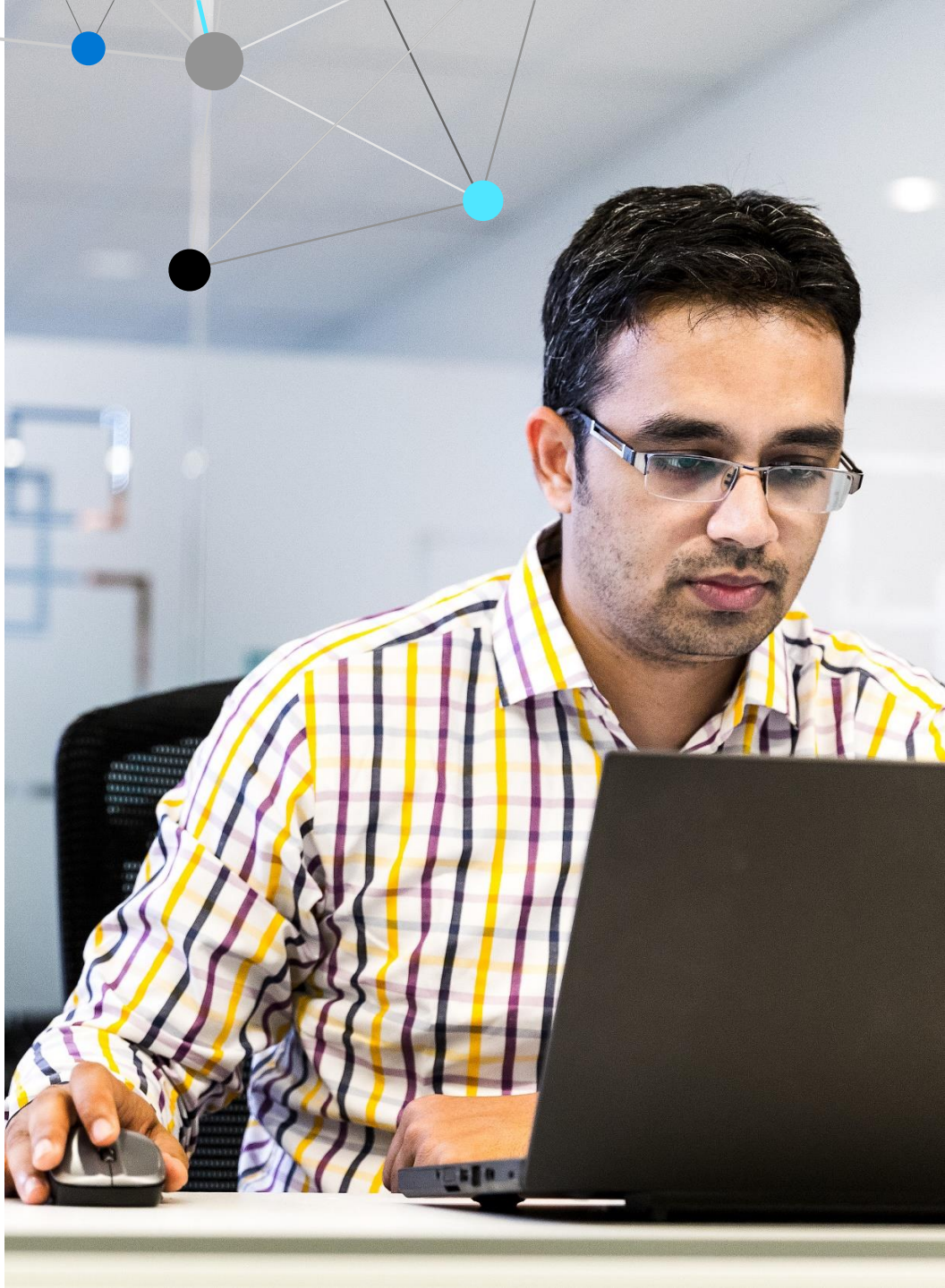
Files containing sensitive information often leave the four walls of your business. This puts your data at risk of falling into the wrong hands.

The solution:

Azure Information Protection gives you control over who can access your emails and documents.

You can control whether an email can be forwarded, printed, or viewed by non-employees.

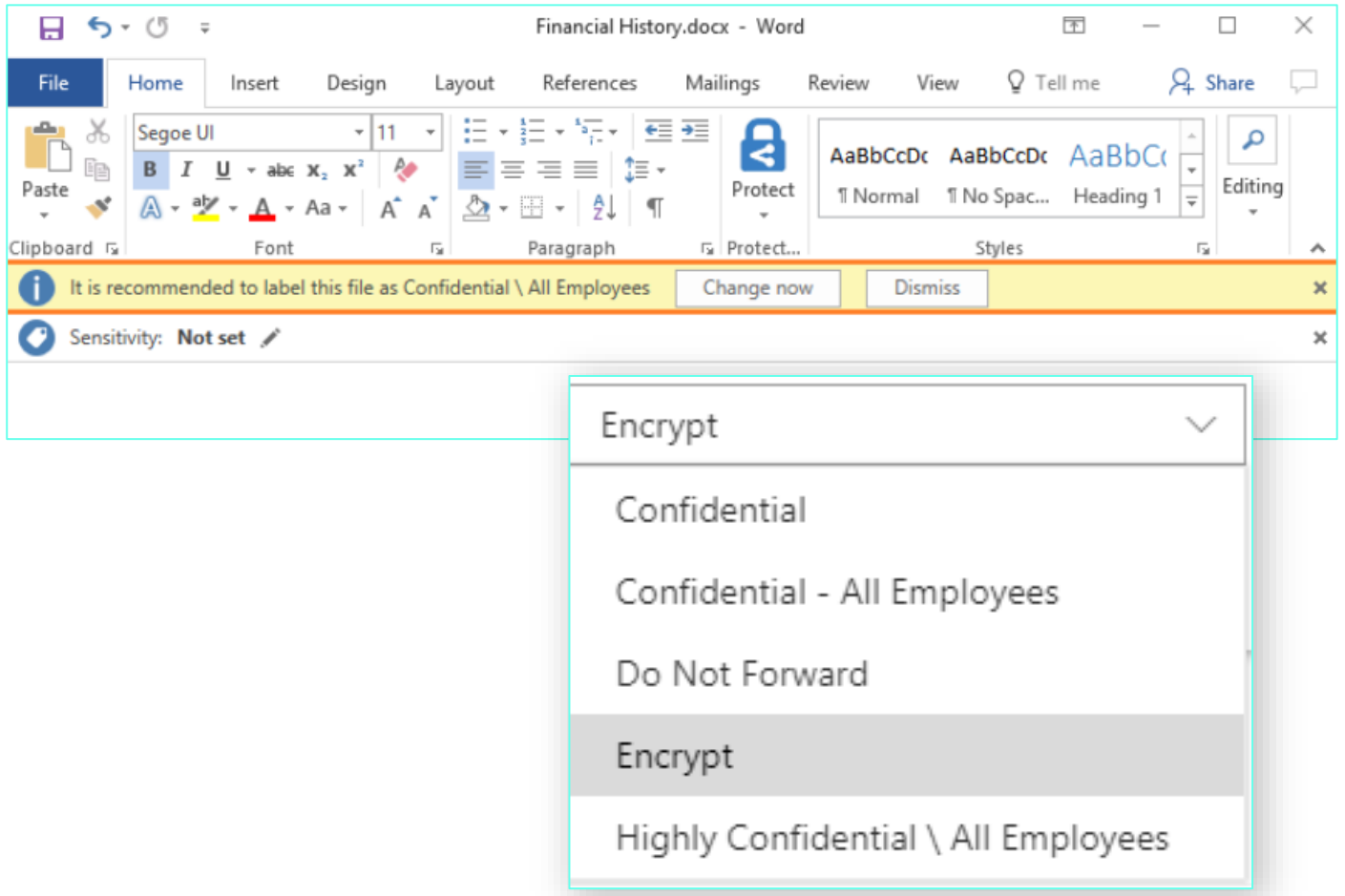
You can control whether a document can edited, printed, or viewed by non-employees. You can also revoke access.



Microsoft Information Protection (MIP)

What it is:

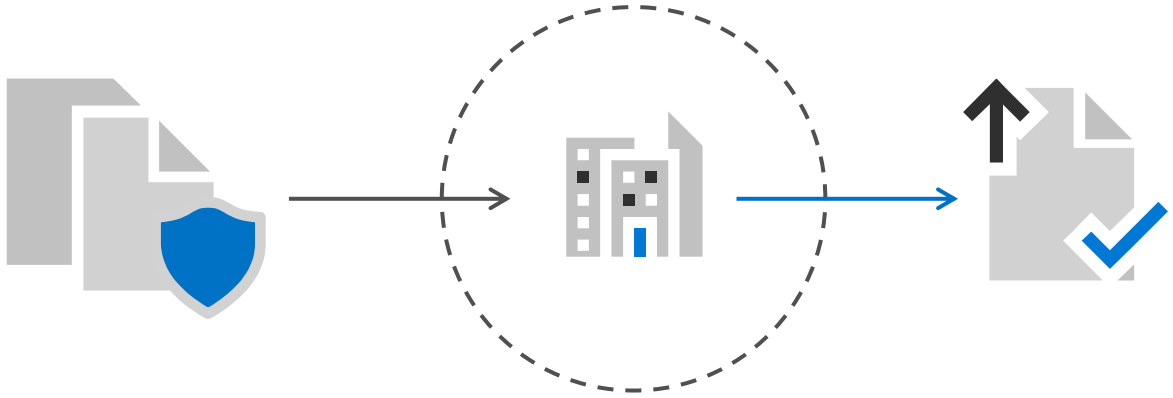
Microsoft Information Protection helps an organization to classify protect its documents and emails, either by restricting the ability to forward and print, or by applying labels.



Protection follows document, even after it leaves your organization

Restrict access, even if the file is saved outside the company

The restrictions and protections stay with the files and emails regardless of the location. Even if the file is emailed outside the company, or saved to an employee's personal computer, you remain in control of your data.



Encrypt emails

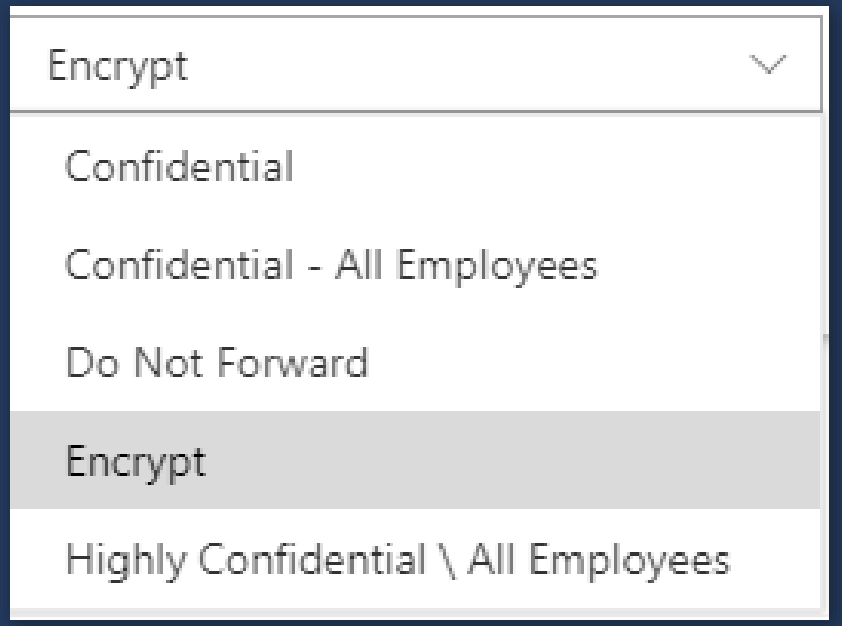
The problem:

Sensitive information is sometimes sent via email

The open nature of email systems means this information is at risk of being read by unauthorized people

The solution:

Encrypt email sent from Microsoft 365 Business, so only the intended recipient can access it.



Microsoft Information Protection

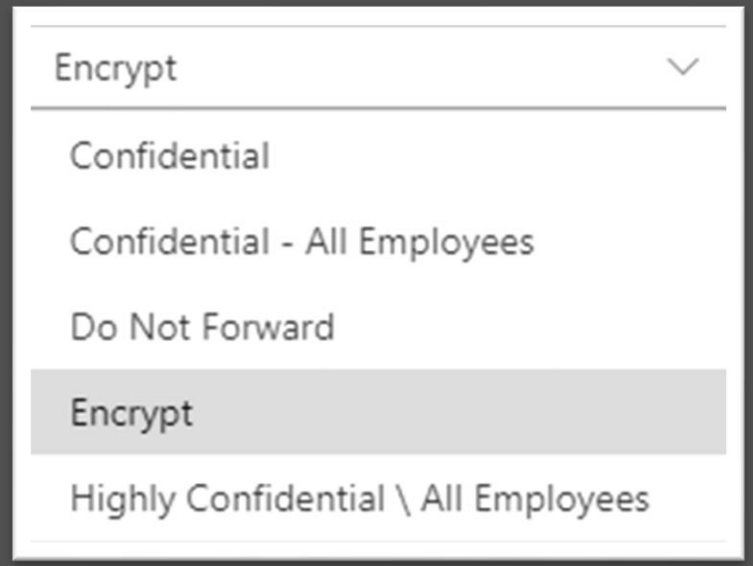
Some examples of how it can be used

You can restrict a sales forecast spreadsheet so that it cannot be accessed by anyone outside your organization.

Your CEO can give managers a heads up about an upcoming reorganization, and mark it “Do Not Forward” so they don’t accidentally pass it along.

You can prevent users from sending Reply-All response to a company-wide email.

When an employee leaves your company, you can revoke access to a master list of customers.



Email encryption

What it is:

Azure Information Protection provides easy-to-use email encryption capabilities for sending encrypted email

Basic encryption on be default

How it works:

The message text and all attachments are encrypted.

Only the recipient can decipher the message for reading.

Anyone else who tries to open the email sees indecipherable text.

Identity verification:

The way the recipient verifies their identity depends on their email system:

- For Office 365 users, authentication happens automatically
- Google, Yahoo, or Outlook.com/Hotmail users sign in with their Google, Yahoo, or Microsoft account
- All others sign in with a one-time passcode

Sending an encrypted email

Note: This demo is most effective if you send an encrypted email to an Outlook.com account, and a separate message to a Gmail account, so the audience can see the two experiences.

To send an encrypted message

To send an encrypted message from Outlook:

- Select **Options** > **Permissions**
- Select the protection option you need

To send an encrypted message from Outlook on the web:

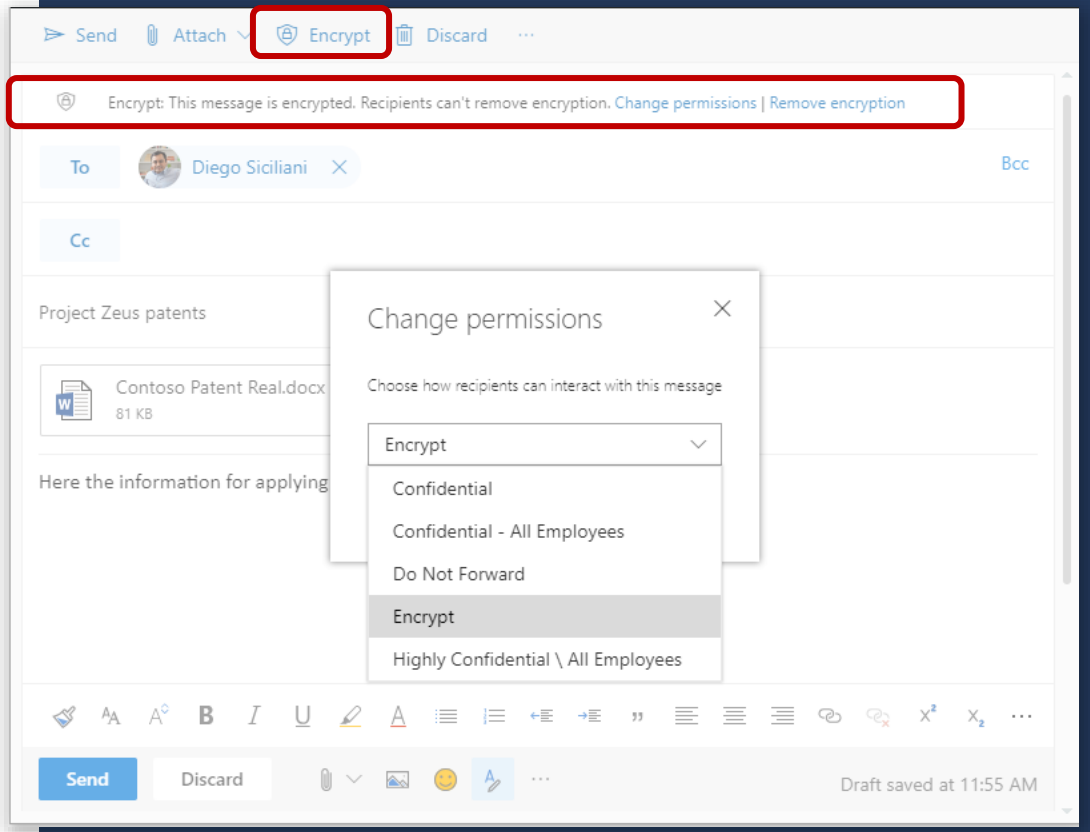
- Select the **Encrypt** button

To view an encrypted message

For email recipients with Office 365, the decryption will happen automatically, and the message will be decrypted upon on opening it.

For recipients not using Office 365, the encrypted message will contain a link in the message body.

- Select Read the message
- Select how you'd like to sign in to read the message
  - If your email provider is Google, Yahoo, or Microsoft, you can select Sign in with Google, Yahoo, or Microsoft respectively
  - Otherwise, select sign in with a one-time passcode. Once you receive the passcode in an email message, make a note of the passcode, then return to the web page where you requested the passcode and enter the passcode, and select CONTINUE



Labelling

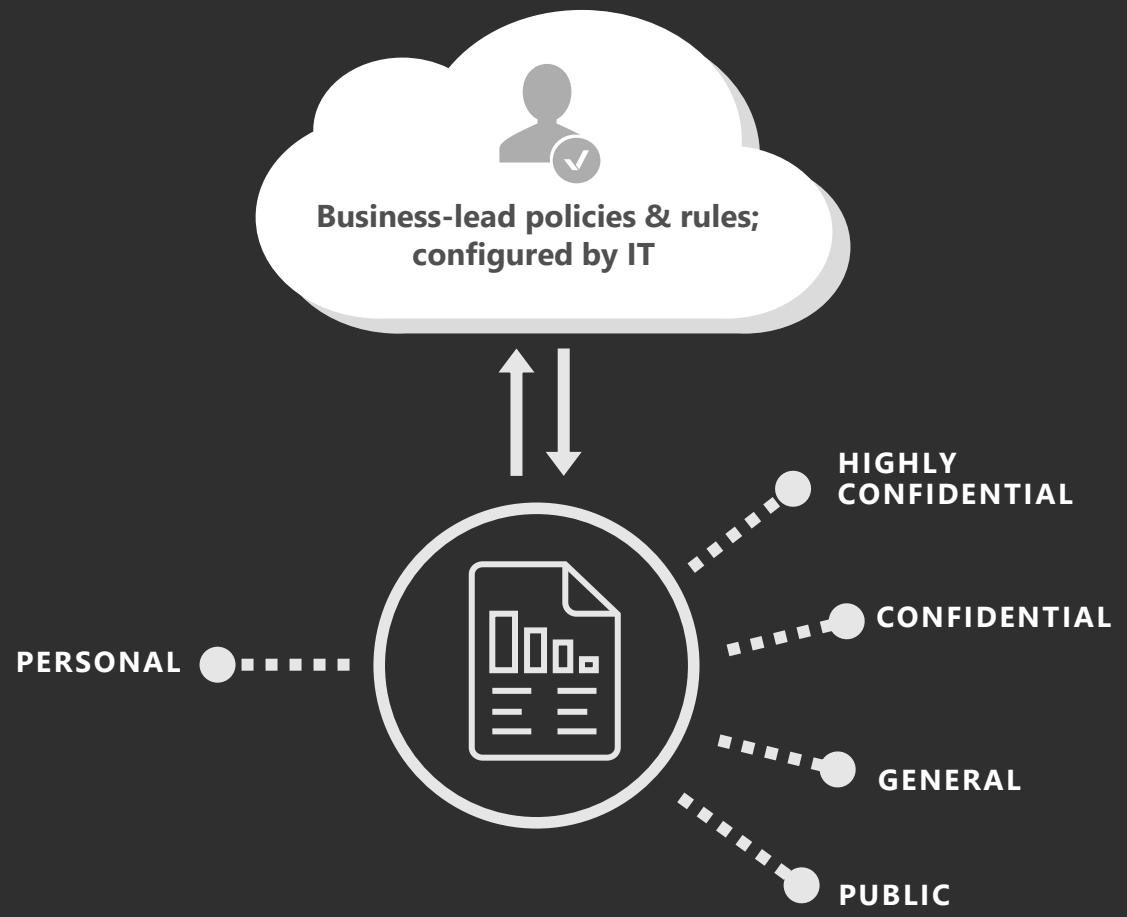
CLASSIFY INFORMATION BASED ON **SENSITIVITY**

Automatic classification
Policies can be set by IT Admins for automatically applying classification and protection to data

Recommended classification
Based on the content you're working on, you can be prompted with suggested classification

Manual reclassification
You can override a classification and optionally be required to provide a justification

User-specified classification
Users can choose to apply a sensitivity label to the email or file they are working on with a single click



SENSITIVITY LABELS **PERSIST WITH THE DOCUMENT**

Document labeling – what is it?

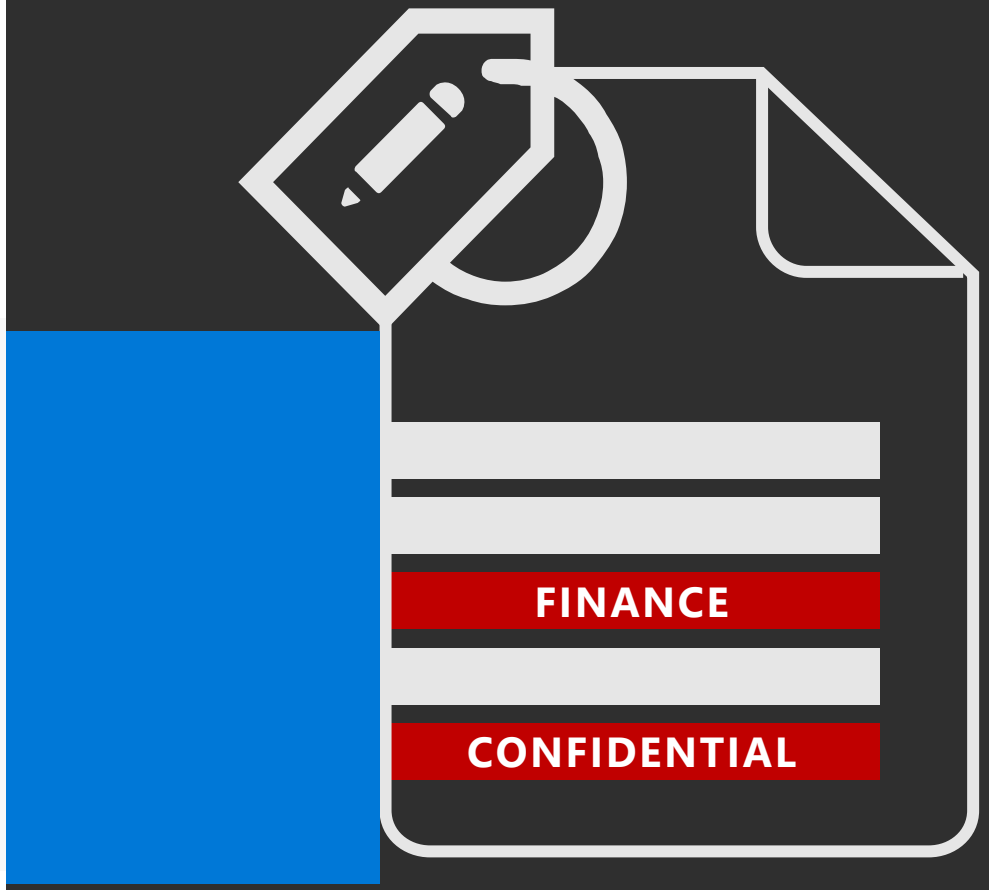
Metadata written into document files

Travels with the document as it moves

In clear text so that other systems such as a DLP engine can read it

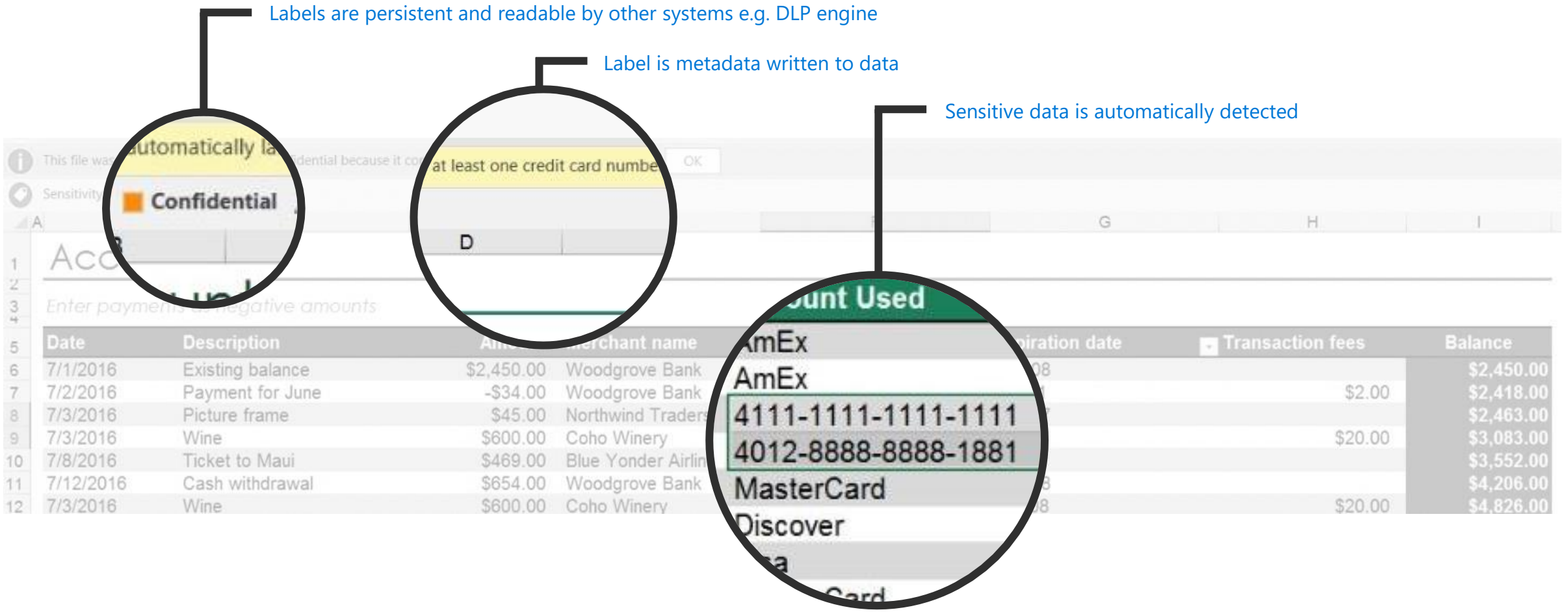
Used for the purpose of apply a protection action or data governance action – determined by policy

Can be customized per the organization's needs



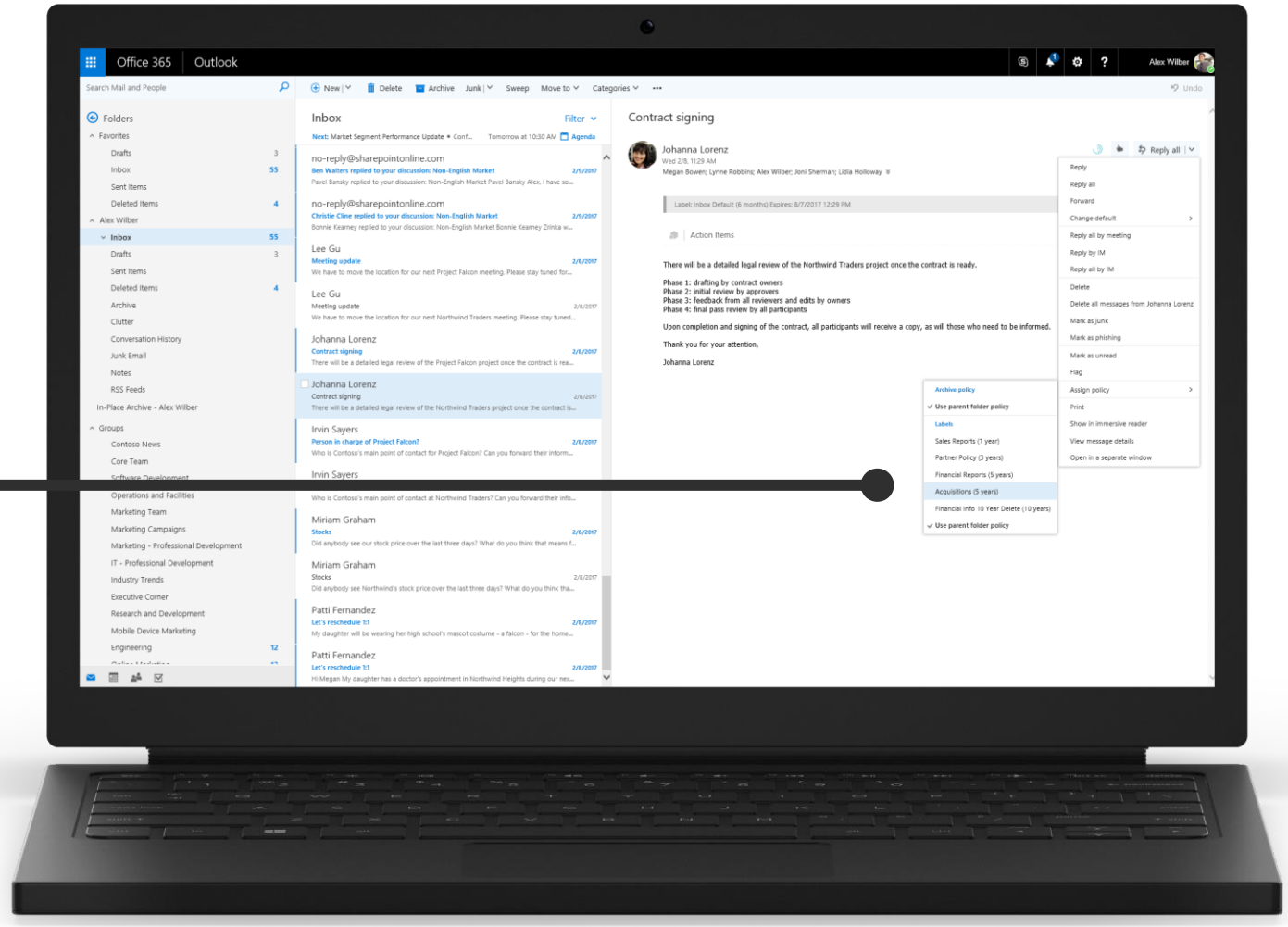
CLASSIFICATION & LABELING EXAMPLE – **SENSITIVE DATA**

Discover personal data and apply persistent labels



CLASSIFICATION & LABELING EXAMPLE – **DATA GOVERNANCE**

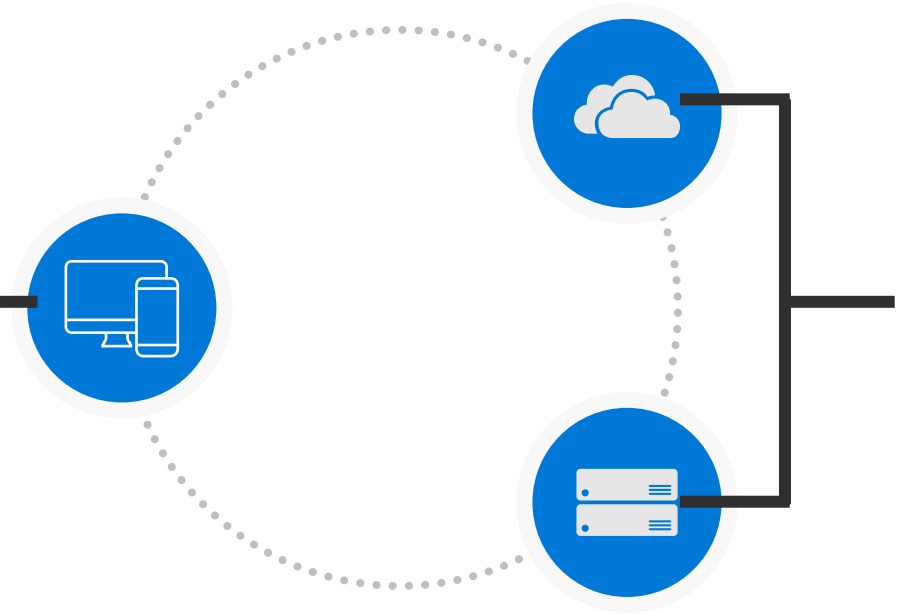
Labeling can be end-user driven
or automatically applied



PROTECT SENSITIVE DATA ACROSS YOUR ENVIRONMENT

Devices

- Drive encryption
- Remote wipe
- Business data separation



Cloud & on-premises

- File encryption
- Permissions and rights-based restrictions
- DLP actions to prevent sharing
- Policy tips & notifications for end-users
- Visual markings in documents
- Control and protect data in cloud apps with granular policies and anomaly detection
- Data retention, expiration, deletion

- Name
- Administrative Units
- Type
- **Retention settings**
- Finish

Decide if you want to retain content, delete it, or both

(•) **Retain items for a specific period**
Items will be retained for the period you choose.

Retain items for a specific period

7 years

Start the retention period based on

When items were created

At the end of the retention period

(•) **Delete items automatically**

( ) **Do nothing**

( ) **Retain items forever**
Items will be retained forever, even if users delete them.

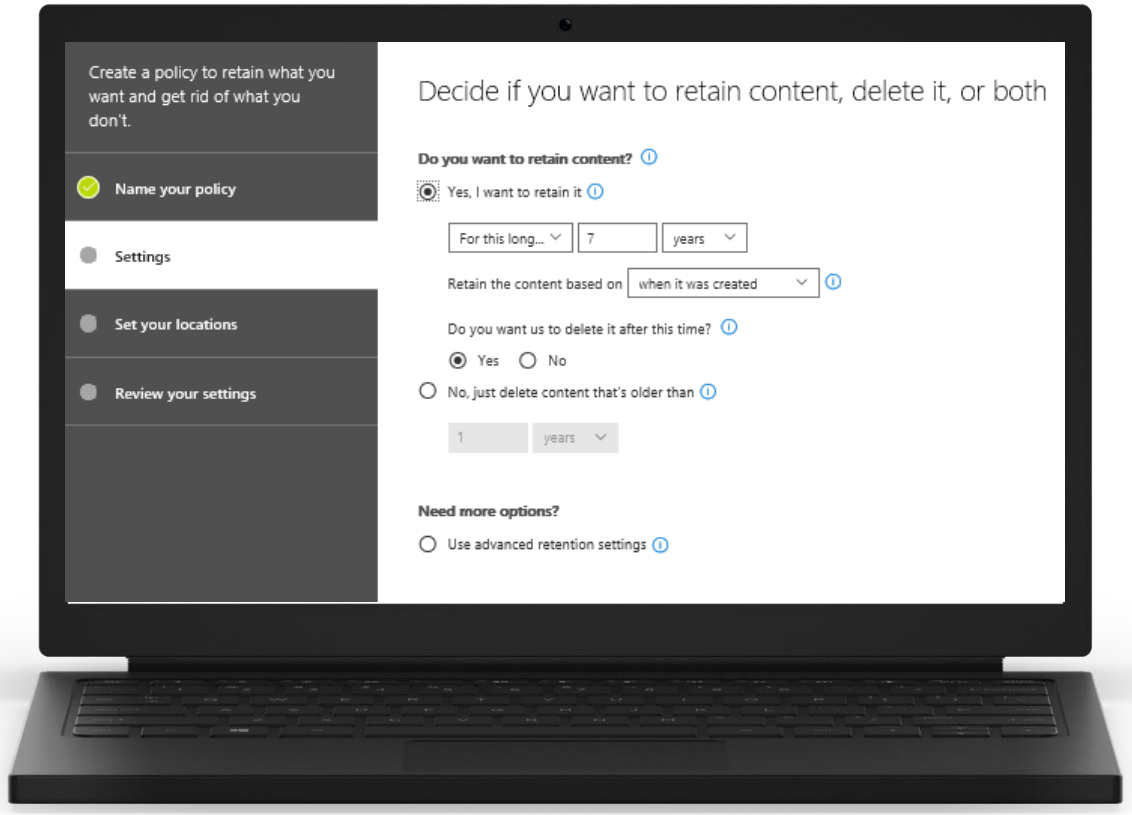
( ) **Only delete items when they reach a certain age**
Items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

AUTOMATICALLY **RETAIN AND DELETE** DOCUMENTS IN OFFICE 365 WITH **DATA GOVERNANCE**

Retention
Retain content in sites, mailboxes, and public folders indefinitely or for a specific duration

In-place
Data remains in its original location in Office 365 and users can continue to work with their documents or mail, but a copy of the content as it existed when you initiated the policy is preserved

Delete data
A retention policy can both retain and then delete data, or simply delete old data without retaining it



MONITOR **DLP** AND **DATA GOVERNANCE EVENTS**

Know when policy is violated
Incident report emails alert you in real time when content violates policy

See the effectiveness of your policies
Built in reports help you see historical information and tune policies

Integrates with other systems
Leverage the Activity Management API to pull information into SIEM and workflow tools