



# CSP Masters Program in person series

## Technical training



# Protecting against data loss

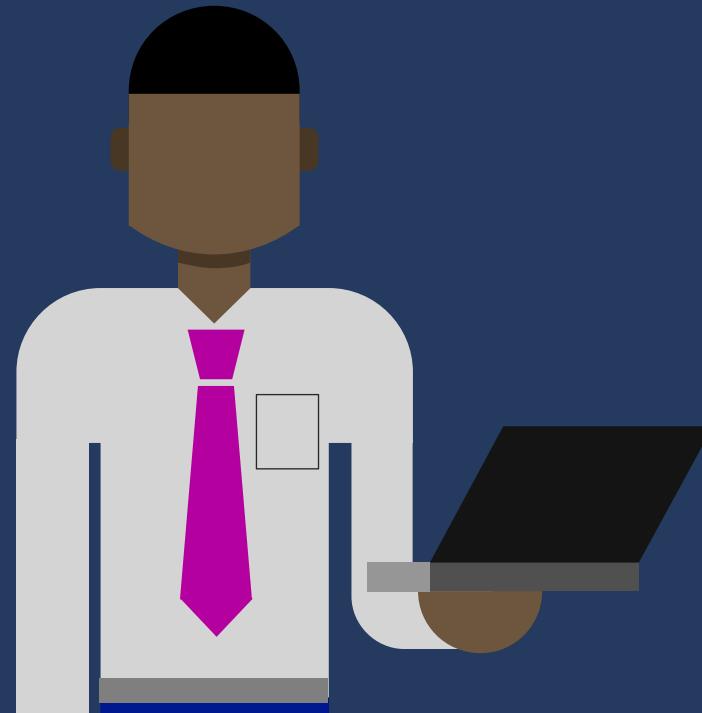


# How can I protect my customer from data loss?

**Name:** Bob D

**Role:** Technical Consultant

**Company:** Partner

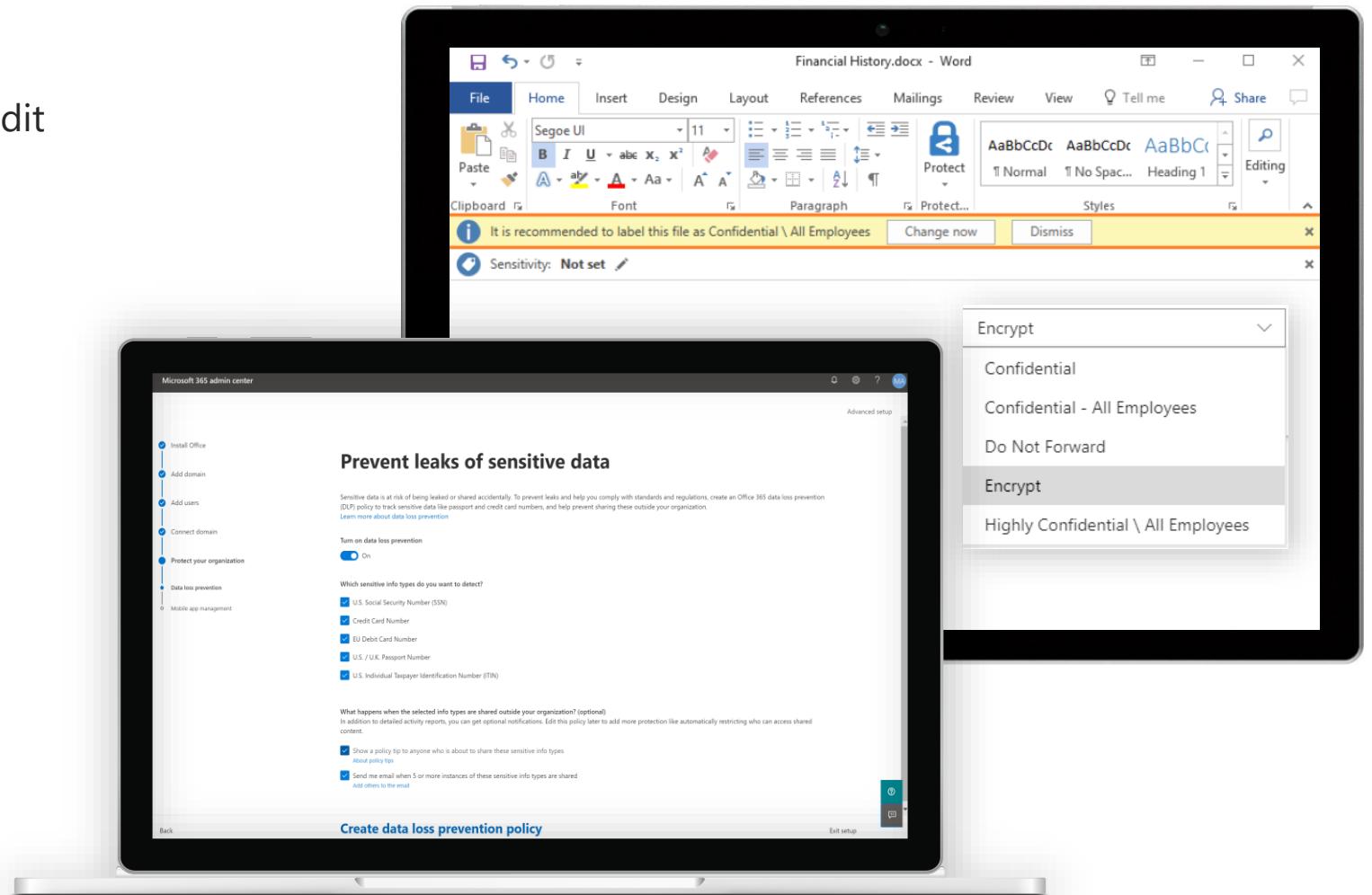


# Safeguard business data with DLP and Azure Information Protection

Prevent sharing of sensitive information like credit card numbers using preconfigured DLP policy templates for HIPAA, PCI\_DSS, SSN etc

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

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



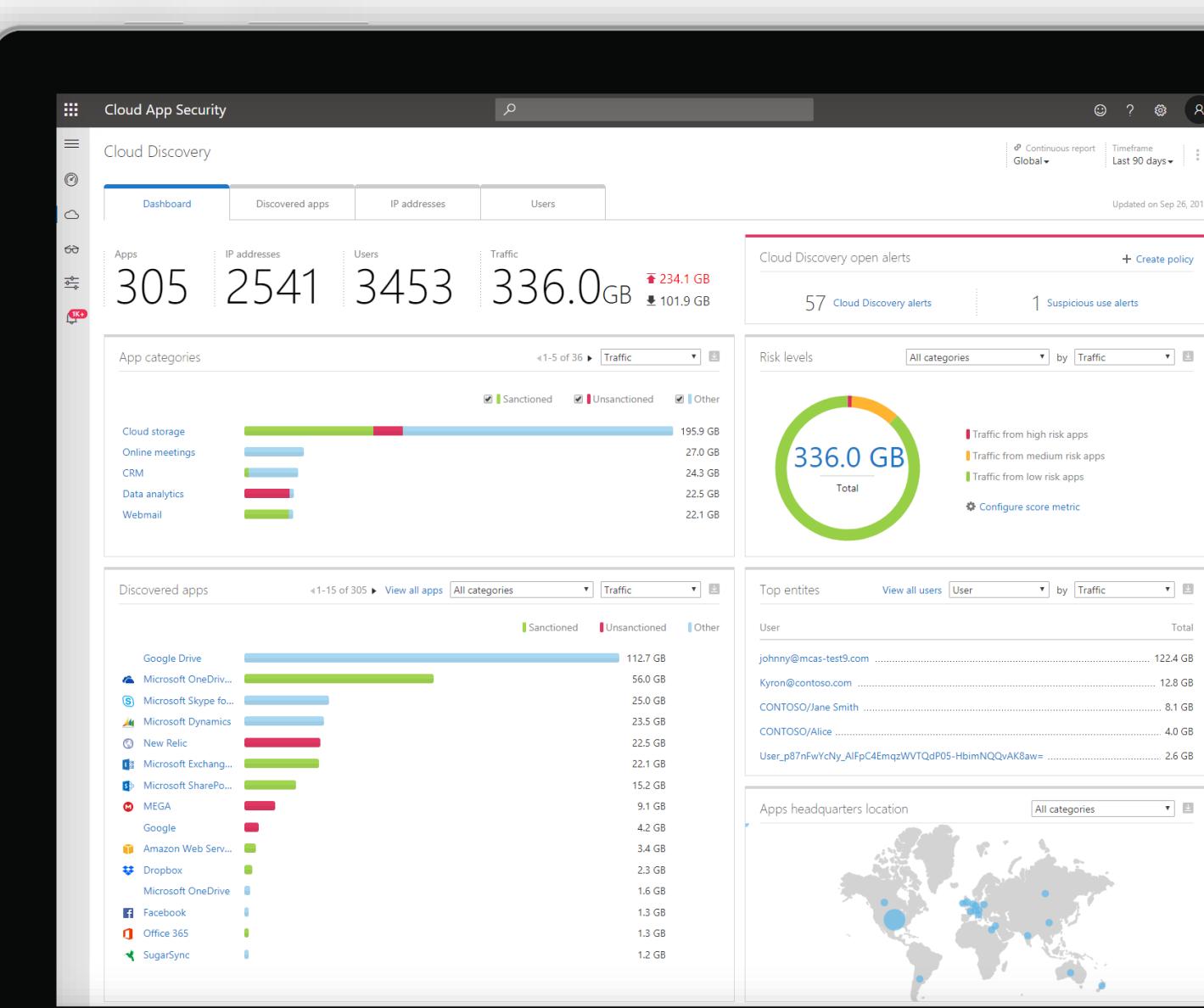
# Get visibility into cloud app use with Cloud App Discovery

Discover cloud app usage to understand shadow IT risk

Understand the security of your cloud apps with risk assessment for 16,000+ cloud apps

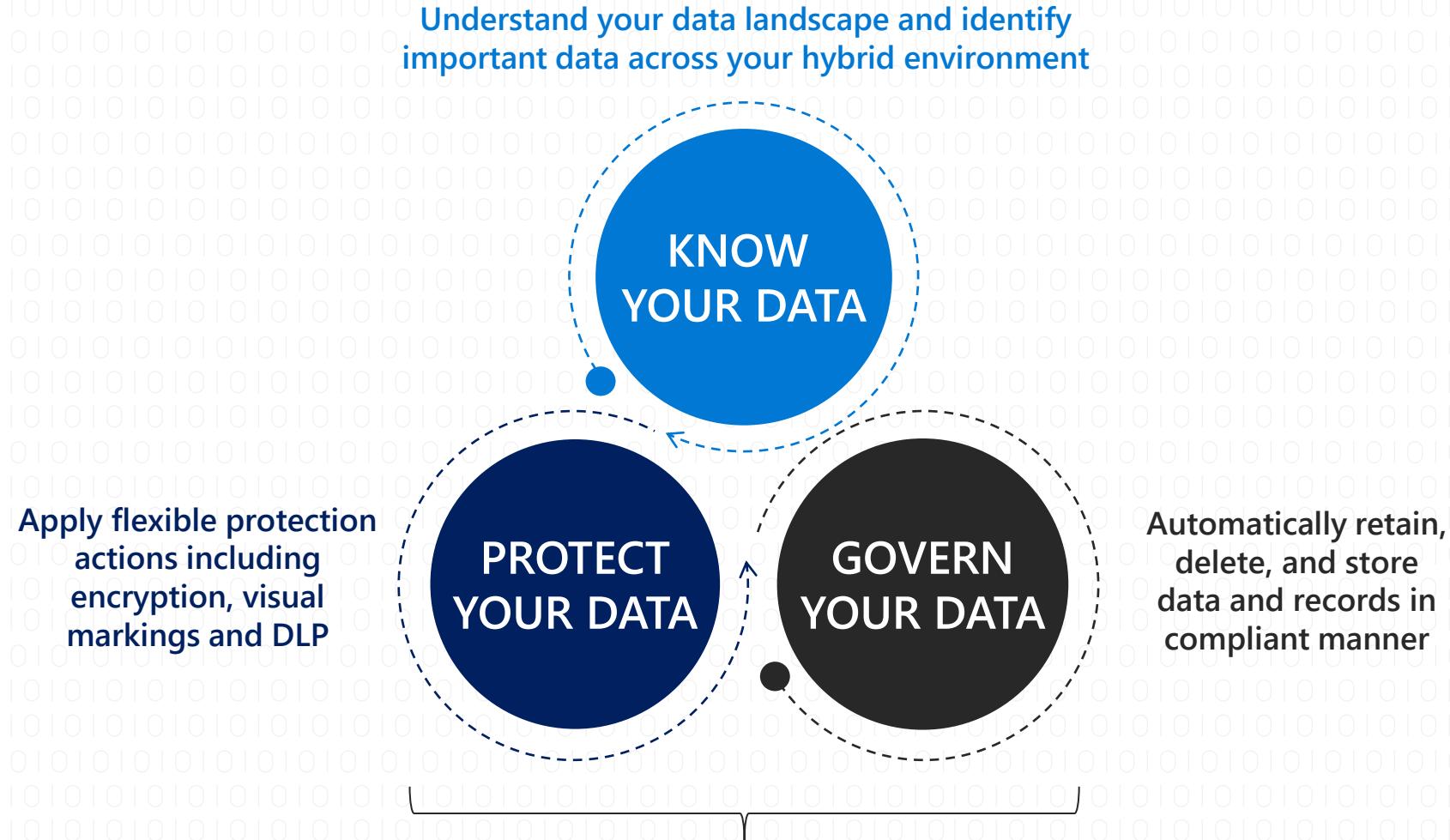
Understand usage patterns and identify high risk users. Export data for additional analysis

Prioritize applications to bring under IT control and integrate applications to enable single sign-on and user management



# Information Protection & Governance

Protect and govern data  
– **wherever** it lives



Unified approach to automatic data classification, policy management, analytics and APIs

# Protect and control your data and documents



Encrypt  
email



Apply restrictions  
to email and  
documents



Protect against  
data leaks



Archive  
email data

# DEMO

# Protect and control your data and documents

---



Encrypt  
email



Apply restrictions  
to email and  
documents



Protect against  
data leaks



Archive  
email data

# Protect against accidental data leaks

## The problem:

It is difficult and unrealistic to expect employees to manually check every email or document shared for sensitive information before sharing files outside the company.

## The solution:

Enable Data Loss Prevention (DLP) policies to automatically identify sensitive information and inform users before sharing this data externally.



# Why do organizations need DLP?

Data leakage often occurs inadvertently

Need protection without inhibiting productivity

Users need guidance to make the right decisions



# Data Loss Prevention

## What it is:

The Data Loss Prevention policies help businesses **identify, monitor, and protect sensitive information** through deep content analysis.

Examples of sensitive information that you might want to prevent from leaking outside your organization include personally identifiable information (PII) such as credit card numbers, social security numbers, or health records.

## With a DLP policy, you can:

- Identify sensitive information across many locations and apps
- Prevent the accidental sharing of sensitive information
- Monitor and protect sensitive information in the desktop versions of Excel, PowerPoint, and Word
- Help users learn how to stay compliant without interrupting their workflow

# Data Loss Prevention

## How it works

A DLP policy contains a few basic things:

- Where to protect the content
- When and how to protect the content by enforcing **rules** comprised of:
  - **Conditions** the content must match before the rule is enforced
  - **Actions** that you want the rule to take automatically when content matching the conditions is found
- You can use a rule to meet a specific protection requirement, and then use a DLP policy to group together common protection requirements, such as all of the rules needed to comply with a specific regulation



**For example**, you might have a DLP policy that helps you detect the presence of information subject to the Health Insurance Portability and Accountability Act (HIPAA). This DLP policy could help protect HIPAA data (the what) across all SharePoint Online sites and all OneDrive for Business sites (the where) by finding any document containing this sensitive information that's shared with people outside your organization (the conditions) and then blocking access to the document and sending a notification (the actions).

# Data Loss Prevention

## DLP Policy Templates:

DLP comes with templates to save you the work of building a new set of rules from scratch.

You can modify these requirements to fine tune the rule to meet your organization's specific requirements.

## Examples of DLP policy templates:

- HIPAA data
- PCI-DSS data
- Gramm-Leach-Bliley Act data
- Locale-specific personally identifiable information



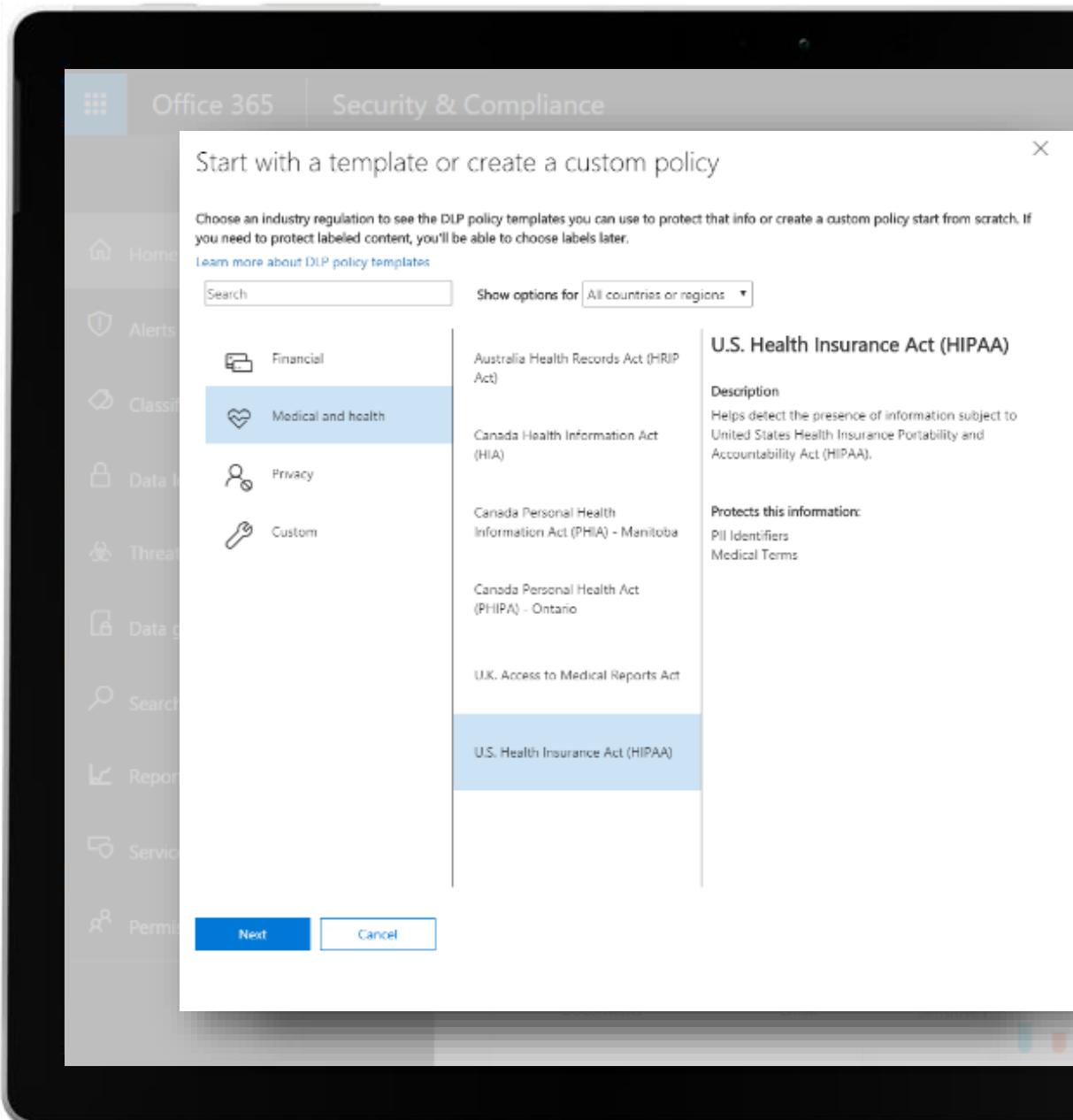
# Built-in Policies & Templates

Proactive default protection policy for most common sensitive content

Over 40 policy templates for common industry regulations and compliance needs – included out of the box

Easy starting point for further customizations

System-generated insights with step-by-step enablement for additional protection controls



# Balancing user productivity and risk

Policy Tips help educate users when they are about to violate a policy.

Available in desktop, web, and mobile apps.

The image displays three separate windows demonstrating the implementation of Policy Tips:

- Microsoft SharePoint / OneDrive:** A screenshot of a file's "Link Settings" dialog box. It shows a dropdown menu asking "Who would you like this link to work for?" with options: "Anyone", "People in MSFT", "People with existing access", and "Specific people". The "Specific people" option is selected, showing a list of users including "Alex Li (OFFICE)". Below this, a red warning message states: "This item contains sensitive information. It can't be shared with people outside your organization." A "View policy tip" link is provided. At the bottom, there are "Apply" and "Cancel" buttons.
- Microsoft SharePoint / OneDrive (Details View):** A screenshot of a file's details page. A red banner at the top reads: "View policy tips This item conflicts with a policy in your organization". Below the banner, the file's metadata is listed: Type: .DOCX, Size: 22KB, Created: 10/23/15 5:45 PM, Modified: 3/23/16 1:29 PM. There are "Move", "Save", and "Delete" buttons at the bottom right.
- Microsoft Excel:** A screenshot of an Excel spreadsheet titled "2016 Employee Roster - Excel". A yellow warning bar at the bottom states: "POLICY TIP: This file conflicts with a policy in your organization. If you don't resolve this conflict, access to this file might be blocked. Go to the File menu for more information." The ribbon tabs shown are Home, Insert, Draw, Page Layout, Formulas, Data, Review, View, and Inquire.

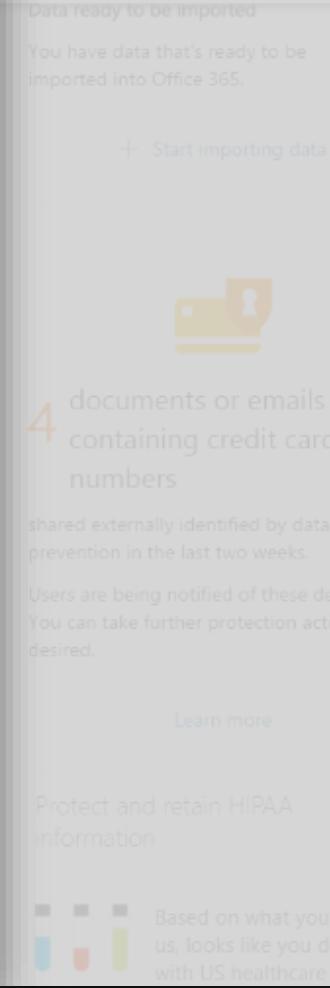
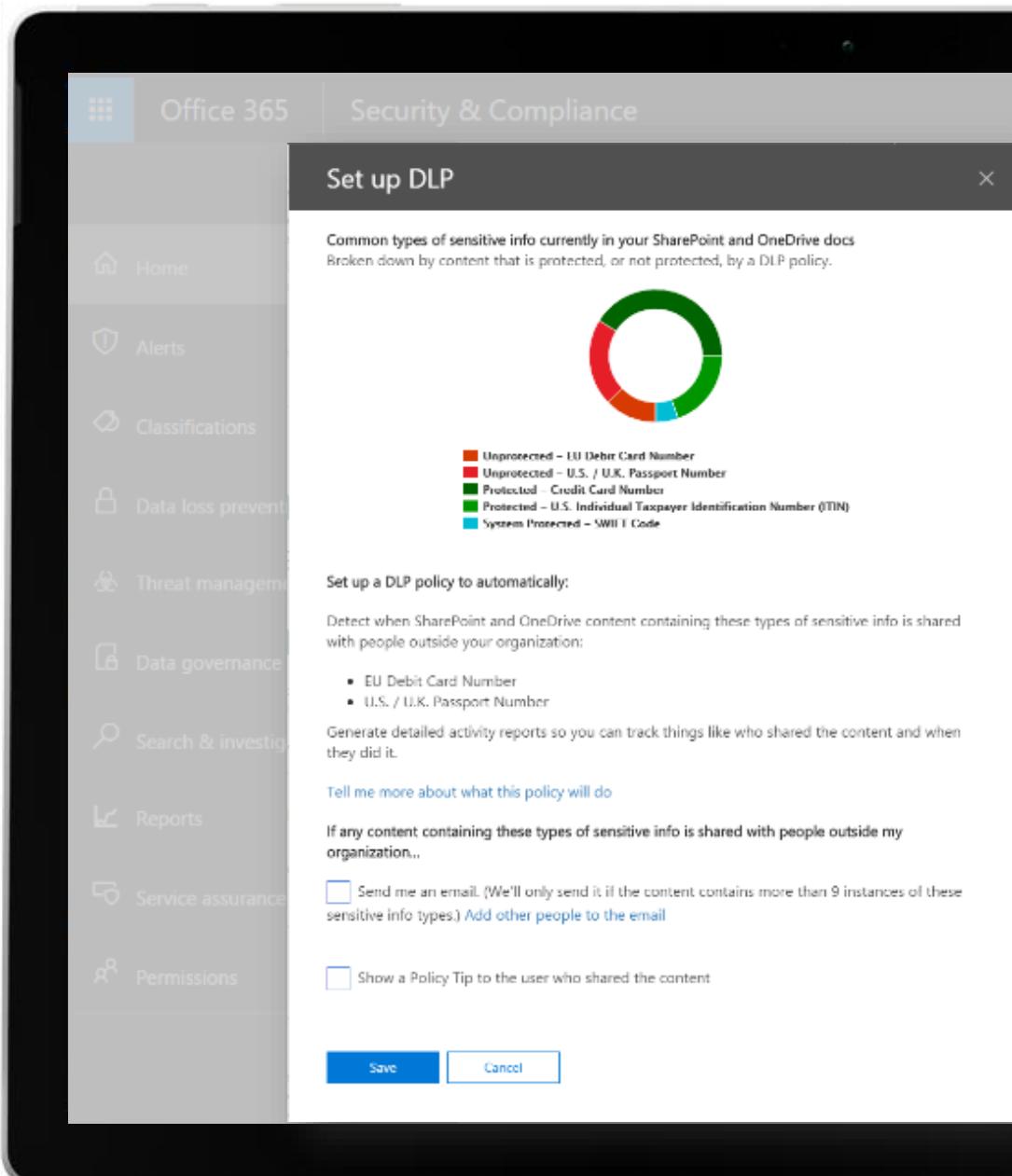
# Usage-driven recommendations

Quick enablement of additional protection

System insights based on actual organizational data usage

Simple step-by-step activation workflows

Deep content analysis using most common sensitive types



# Rich customization

**Conditions & Exceptions** describe what the content looks like (or doesn't look like), and what events to look for.

**Actions** define what type of automatic remediation you want to take when the conditions match

**User notifications & overrides** define what the user sees, and if they have the ability to override with a business justification

**Incident reports** trigger email notifications or Alerts based upon severity of event

The screenshot shows the Microsoft 365 Compliance Center interface for creating a new policy. The title bar reads "Content matches U.S. Health Insurance Act (HIPAA)". The main area is divided into several sections:

- Name:** A dropdown menu is open, showing "Name" and "New".
- Conditions:** A section where users can define what content matches the rule. It includes a list of checked options:
  - Notify these people:
    - The person who sent, shared, or modified the content
    - Owner of the SharePoint site or OneDrive account
    - Owner of the SharePoint or OneDrive content
  - Send the email to these additional people:  
[Add or remove people](#)
  - Customize the email text
- Policy tips:** A section with a checkbox to "Customize the policy tip text".
- User overrides:** A section with a toggle switch to "Require a business justification to override" and a checkbox for "Override the rule automatically if they report it as a false positive".
- Incident reports:** A section where users can set the severity level for admin alerts and reports (set to "Low"), enable email incident reports, and specify notification recipients (mas@ContosoOLP.onmicrosoft.com). It also includes a link to "Add or remove people".
- Information:** A note about incident report details and optional information to include in the report, such as the name of the last modifier, types of sensitive content, rule severity, matched content, and surrounding text.
- Buttons:** "Save" and "Cancel" buttons at the bottom.

## Policy tip for 'CCards.xlsx'

This item is protected by a policy in your organization. Access to this item is blocked for everyone except its owner, last modifier, and the site owner.

### ⊖ Issues

Item is shared with people outside your organization

Item contains the following sensitive information: Credit Card Number

Last scanned: 5/7/2017

⊖ Access to this item is blocked. It conflicts with a policy in your organization.

[View policy tip](#)

[Report an issue](#) to let your admin know that this item doesn't conflict with your organization's policies.

[Override](#) the policy if you have business justification. All policy overrides are recorded.

# DLP document fingerprinting

Scan email and attachments to look  
for patterns that match document  
templates

Protect sensitive documents from  
being accidentally shared outside  
your organization

No coding required; simply upload  
sample documents to create  
fingerprints

\* Note that you can currently create a  
document fingerprint only by using  
PowerShell in the Security & Compliance  
Center.

document fingerprints

You can use document fingerprints to customize sensitive information types in your policies.

+   

NAME
IRS Tax Forms
<b>Standard Bank Forms</b>

Standard Bank Forms

This sensitive information type will detect any of the standard bank forms, like a loan application, account information, etc.

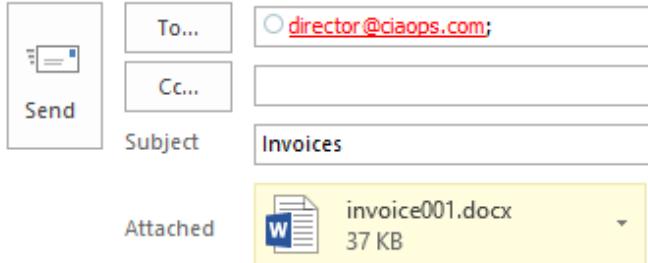
Files:

- Account opening form - Business.pdf
- Account opening form - Personal.pdf
- Account opening form - Priority.pdf
- Auto loan application for business.pdf
- Auto loan application for salaried individual.pdf
- Cash Deposit Slip.pdf
- Cheque Deposit Slip.pdf
- Credit Card application form.pdf

1 selected of 2 total

**Policy Tip:** This message can't be sent because it appears to contain sensitive information.

director@ciaops.com X isn't authorized to receive this type of information.



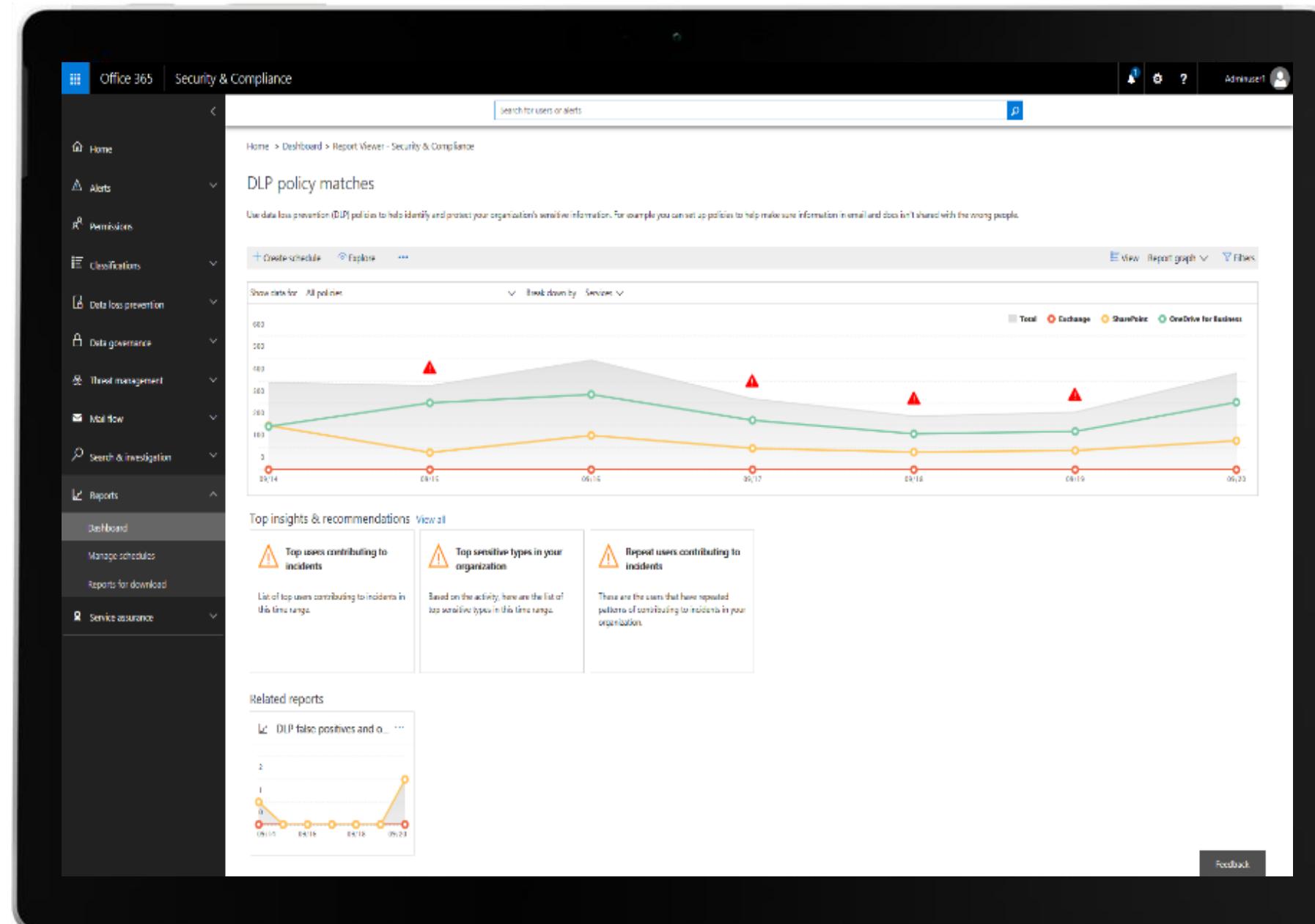
This screenshot shows an email client interface with a policy tip message at the top: 'Policy tip: This message can't be sent because it appears to contain sensitive information. Show details'. The 'To' field is populated with 'director@ciaops.com' and has a purple circular icon with a white 'D'. The 'Cc' field is empty. Below the recipient fields, the text 'Test sending' is visible. In the main body, there is a file attachment 'invoice001.docx' (37 KB). The bottom of the screen displays a toolbar with various editing and sharing icons, including 'Send', 'Discard', and a ribbon of other options.

# Smart Reports

Smart report insights provide information on data abnormalities

Suggest actions to take to remediate

Enable admins to continue their investigation through the explorer



# Investigate and Remediate

Investigate policy violation  
in your organization

Take remediation steps for  
documents to prevent  
further risk

The screenshot shows the Microsoft Office 365 Security & Compliance Center. On the left, a navigation pane lists various compliance categories: Home, Alerts, Permissions, Classification, Data loss prevention, Data governance, Threat management, Mail flow, Search & investigation, Reports, and Service assurance. The 'Classification' tab is selected. The main area displays a bar chart titled 'Sharing' showing activity over time, with a legend indicating blue for 'Sharing' and dark blue for 'Unsharing'. Below the chart is a table titled 'Document' with columns for Date, Filename, Workload, and Classification. The table lists several documents, including 'Contoso Purchasing Permissions - Q1.docx' and 'Customer US Store Purchases.docx', both classified as 'Credit Card Num'. A 'Done' button is visible at the bottom right of the main content area.

Date	Filename	Workload	Classification
5/8/17 1:41 AM	Contoso Purchasing Permissions - Q1.docx	OneDrive	New Zealand M
5/8/17 10:32 AM	Employee Health Accounts - template	SharePoint	Credit Card Num
5/8/17 12:31 PM	Contoso Purchasing Data - KopyCat.xlsx	SharePoint	Credit Card Num
5/8/17 1:27 PM	Customer US Store Purchases.docx	SharePoint	Credit Card Num
5/8/17 3:07 PM	Northwind Customer Demos.xlsx	SharePoint	Credit Card Num

# DLP alerts and notification

Operational view into your protection controls

View into policy application and impact across Office 365 deployment: policy, rule, false positive, override action and incident level views

Proactive notifications of policy violations

Cross-scenario aggregation of signals for more actionable insights

The screenshot shows the Microsoft Office 365 Security & Compliance center. The left sidebar has a dark theme with white icons and text, listing various security features: Home, Alerts, Classifications, Data loss prevention, Threat manager, Data governance, Search & investigation, Reports (which is selected and highlighted in blue), Service assurance, Permissions, and Test Only. The main content area has a light background. At the top right, there is a search bar labeled "Search for users or alerts". Below the search bar, the breadcrumb navigation shows "Home > Reports". In the center, there is a large red "Office 365" logo. To its right, the text "A low-severity alert has been triggered" is displayed. Below this, a yellow warning icon indicates "DLP policy matched in TestDlp0328.docx". Further details are provided: Severity: Low, Time: 6/24/2017 1:00:00 AM (UTC), Activity: DlpIncidentAlert, User: admin@SCCArtists.onmicrosoft.com, and Details: This item has triggered a U.S. Personally Identifiable Information (PII) Data policy match with 1 high confidence data match. A blue "Investigate" button is present at the bottom of this alert card. At the very bottom of the main content area, there is a message from "The Office 365 Team": "Thank you,  
The Office 365 Team".

# Incident Level View

Complete view of DLP detection for quick assessment of impact

Consolidates applicable policies, rules, detected classifications

Optionally includes sensitive data matches

The screenshot shows the Microsoft Office 365 Security & Compliance center. On the left, a navigation pane lists various categories: Home, Alerts, Permissions, Classifications, Data loss prevention, Data governance, Threat management, Search & investigation, Reports (which is selected), Dashboard, Manage schedules, Reports for download, and Service assurance. The main content area is titled "DLP Incident report" and displays a message about identifying and protecting sensitive information shared with the wrong people. It includes a chart showing activity from 07/10 to 07/11, with a single data point at 07/11. Below the chart, a table lists "Policy Matches" with columns for Policy, Rule, and Action. One entry is shown: "U.S. Personally Identifiable Information (PII) Data" with rule "Low volume of content detected U.S. PII" and action "BlockAccess, NotifyUser, GenerateAlert, GenerateIncidentReport". A "Close" button is at the bottom right of the report window.

Personal Information.docx

DLP Incident report

shared with the wrong people.

Show data for All policies

Severity: Low

Time: Jun 23, 2017 6:00:00 PM

Details: Personal Information.docx

Sensitive Information Count: -

Users: admin@SCCAclients1.onmicrosoft.com

Recipient: None

Location: SharePoint

Policy Actions: BlockAccess, NotifyUser, GenerateAlert, GenerateIncidentReport

False Positive: -

Override: -

Status: Active

Comments: Add comments

Date Rules Title

7/11/17 6:45 PM d4a84dad afca 45ad... SharedEx13.doc

7/11/17 6:45 PM 0eee0478-d571-4bd1... SharedEx13.doc

7/11/17 7:15 PM d4a84dad afca 45ad... SharedEx14.doc

7/11/17 7:15 PM 0eee0478-d571-4bd1... SharedEx14.doc

7/11/17 8:45 PM db78e546 ccd8 4ba... PanNumbersSh...

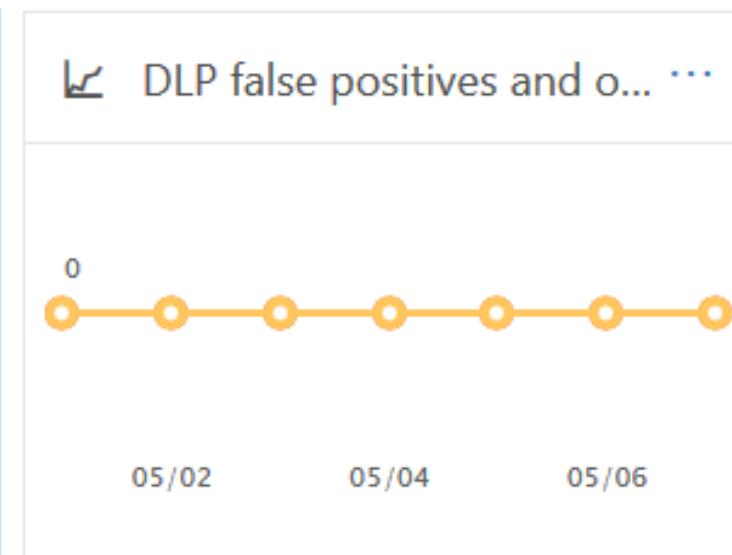
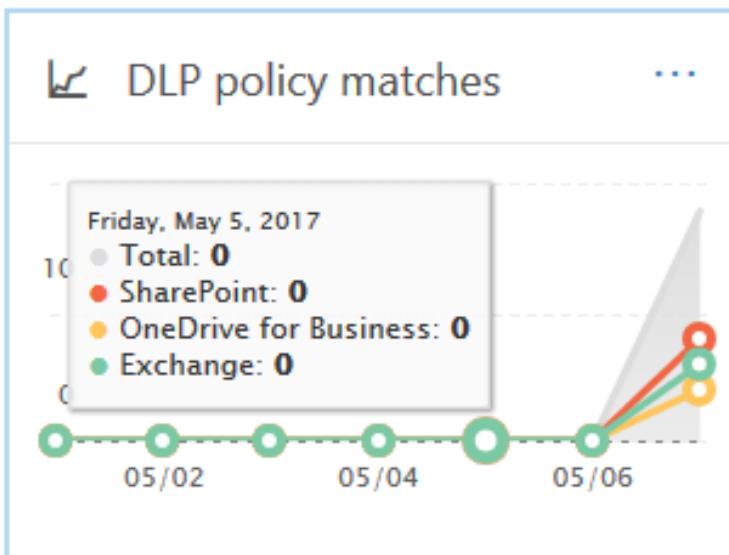
Policy Matches

Policy Rule Action

U.S. Personally Identifiable Information (PII) Data Low volume of content detected U.S. PII BlockAccess, NotifyUser, GenerateAlert, GenerateIncidentReport

Close

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive information. For example, you can help make sure information in email and docs isn't shared with the wrong people. [Learn more about DLP](#)

[+ Create a policy](#)[Refresh](#) Search

<input type="checkbox"/>	Name	Order	Last modified	Status
<input type="checkbox"/>	Credit Card Policy	1	May 7, 2017	On
<input type="checkbox"/>	Australia Financial Data	2	May 7, 2017	On

# Best practices

Get started today with templates

Use test mode to audit impact before impacting \*anyone\*

Turn on Email Incident Reports to see policy match accuracy results

Use valid sample data when testing  
- <http://aka.ms/dlpsensitivetypes>

The screenshot shows a web browser displaying the Microsoft Office 365 Security & Compliance Center. The page title is "What the sensitive information types look for". The content area lists various sensitive information types, each with a dropdown arrow to its right. The listed types include:

- ABA Routing Number
- Argentina National Identity (DNI) Number
- Australia Bank Account Number
- Australia Driver's License Number
- Australia Medical Account Number
- Australia Passport Number
- Australia Tax File Number
- Belgium National Number
- Brazil CPF Number
- Brazil Legal Entity Number (CNPJ)



# PROTECTION EXAMPLE: DLP POLICY TO LIMIT DOCUMENT SHARING

Across Office client applications –  
mobile, desktop & tablets

The image displays three separate Office client applications, each showing a 'Policy tip' or 'Security Issue Report Form' dialog box:

- OneDrive (Laptop):** Shows a 'Policy tip for '2015 Employee Roster.xlsx'' dialog. It states: "This item conflicts with a policy in your organization. Access to this item is blocked for everyone except its owner, last modifier, and the site owner." It lists two issues:
  - Item is shared with people outside your organization
  - Item contains the following sensitive information: U.S. Social Security Number (SSN)
- Excel (Tablet):** Shows a 'POLICY TIP: This file conflicts with a policy in your organization.' dialog. It says: "If you don't resolve this conflict, access to this file might be blocked. Go to the File menu for more information." A 'Override' button is visible.
- Word (Mobile Phone):** Shows a 'Details' screen for a document named 'Social Security Number'. It includes a 'View policy tips' link and a note: "This item conflicts with a policy in your organization".

Annotations on the left side of the image point to the laptop and mobile phone screens with the text: "Policy tips to warn end users". Annotations on the right side point to the tablet and mobile phone screens with the text: "Restrict or block sharing – internally or externally".

# DEMO

# 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:

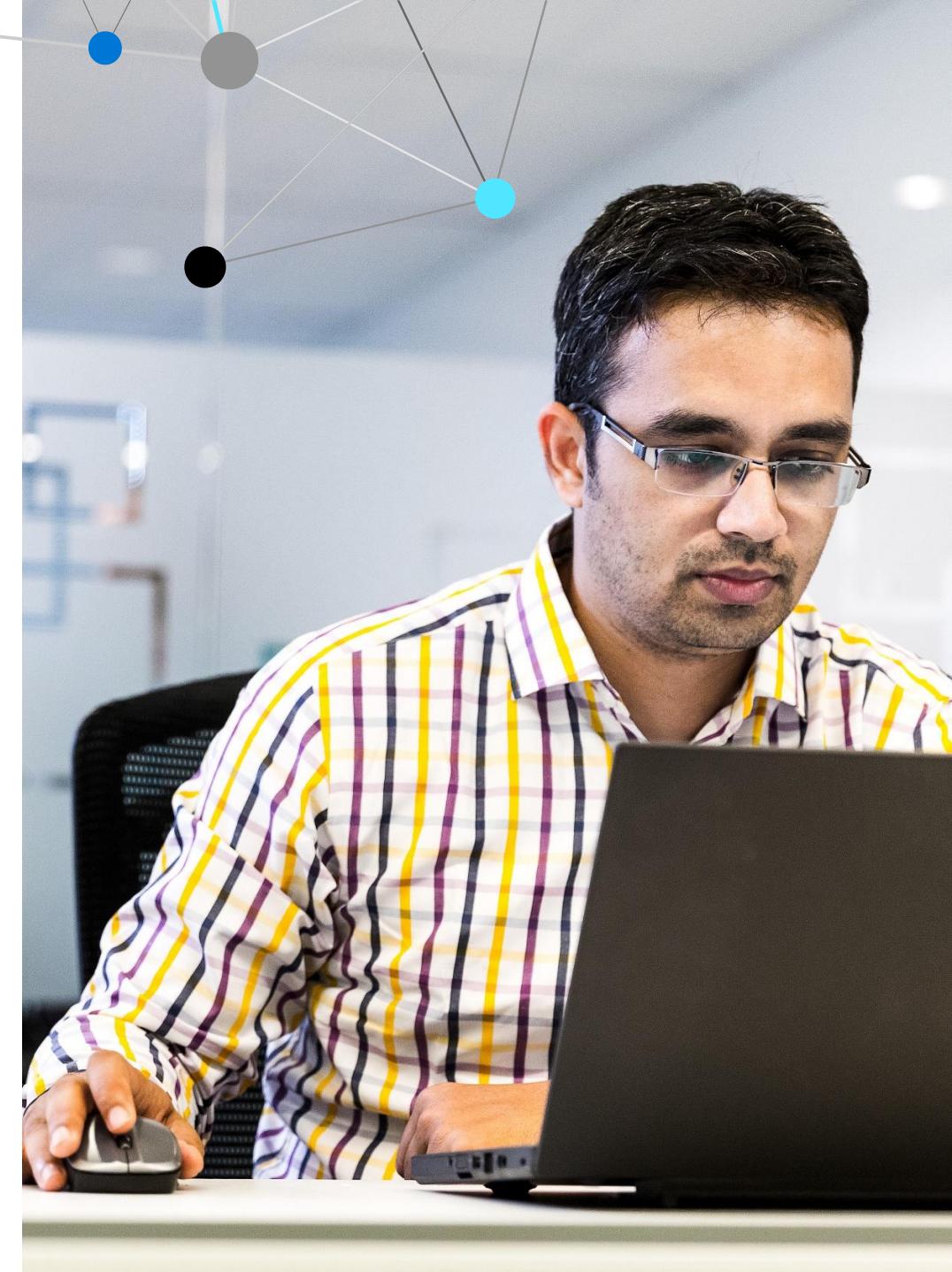
Files containing sensitive information often leave the four walls of your business. This puts your data at risk of falling into the wrong hands.

## 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.

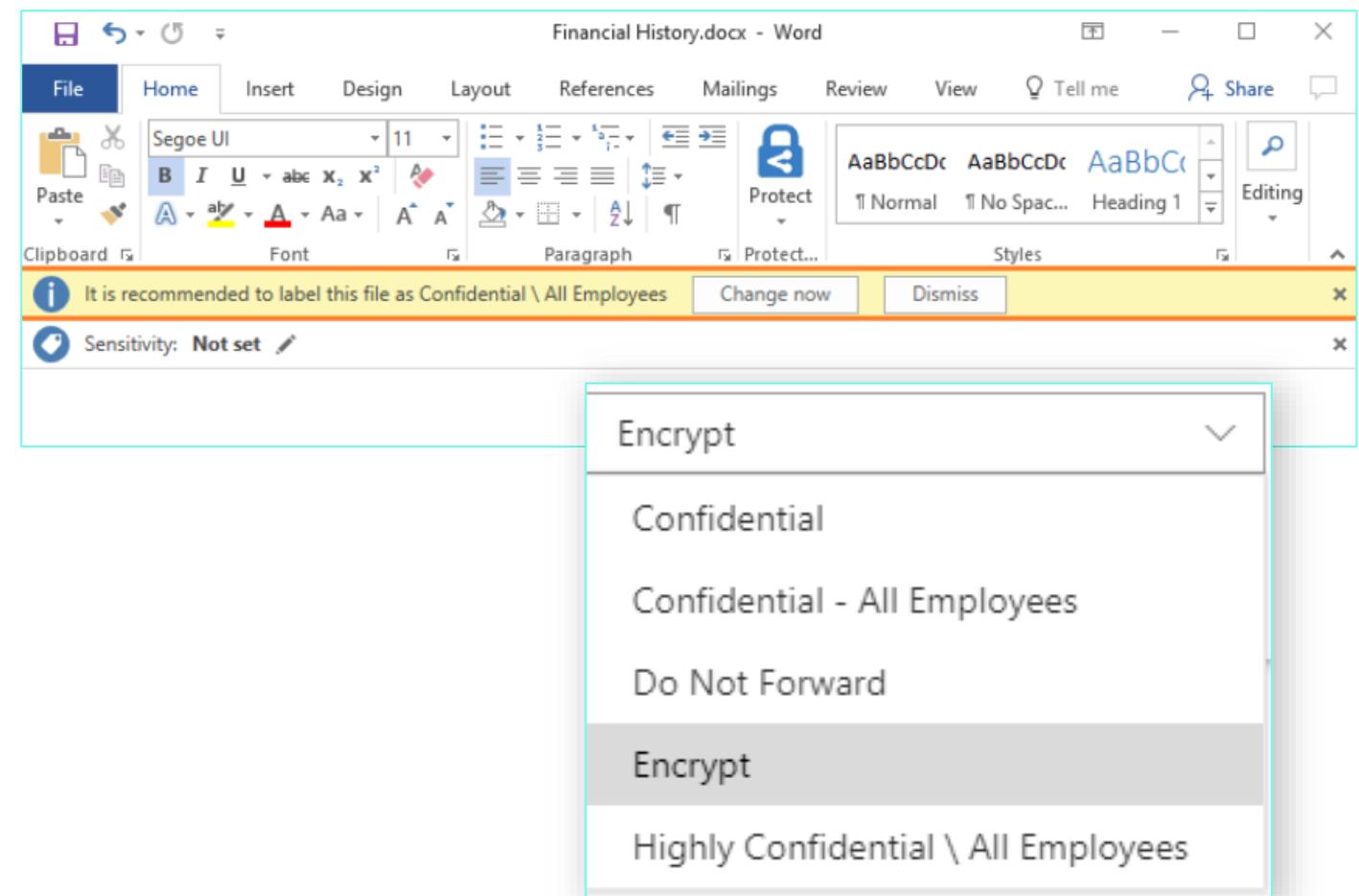
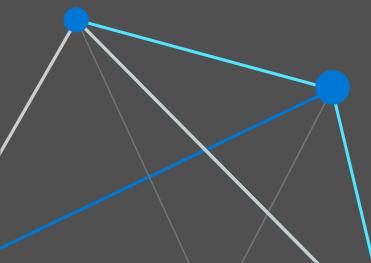
You can control whether a document can be edited, printed, or viewed by non-employees. You can also revoke access.



# Microsoft Information Protection (MIP)

## What it is:

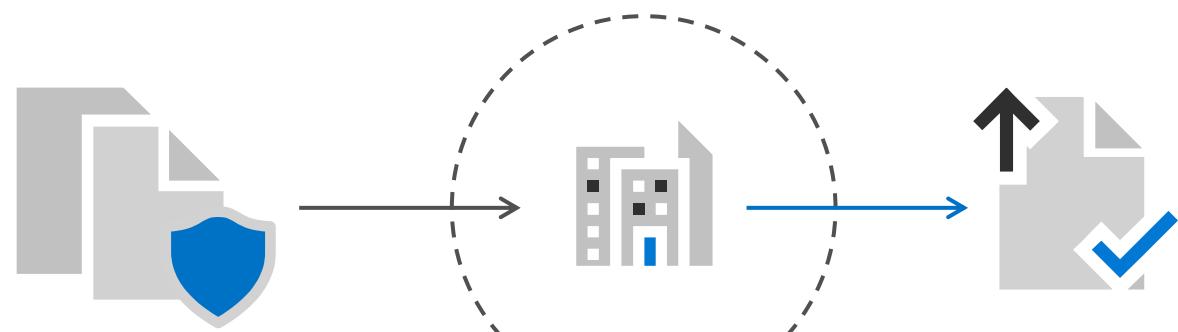
Microsoft Information Protection helps an organization to classify protect its documents and emails, either by restricting the ability to forward and print, or by applying labels.



# 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

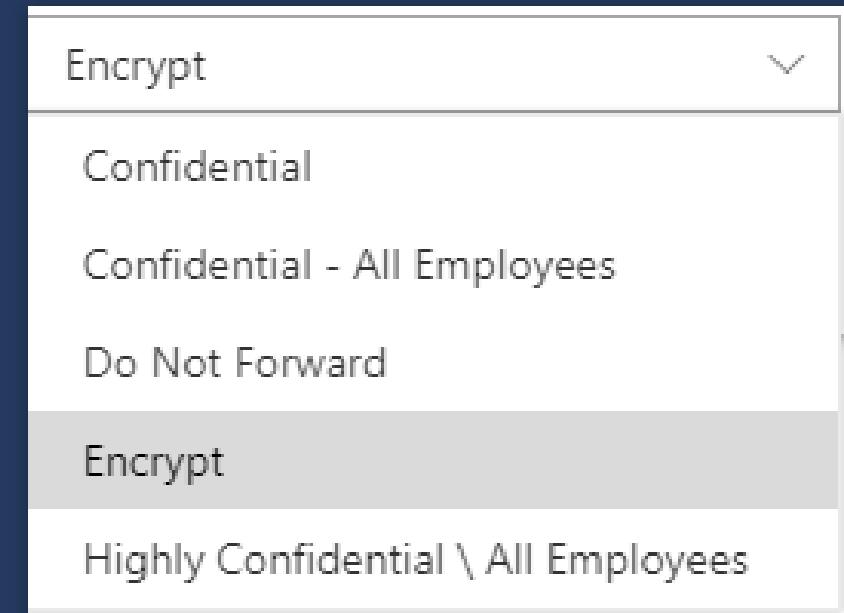
## The problem:

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

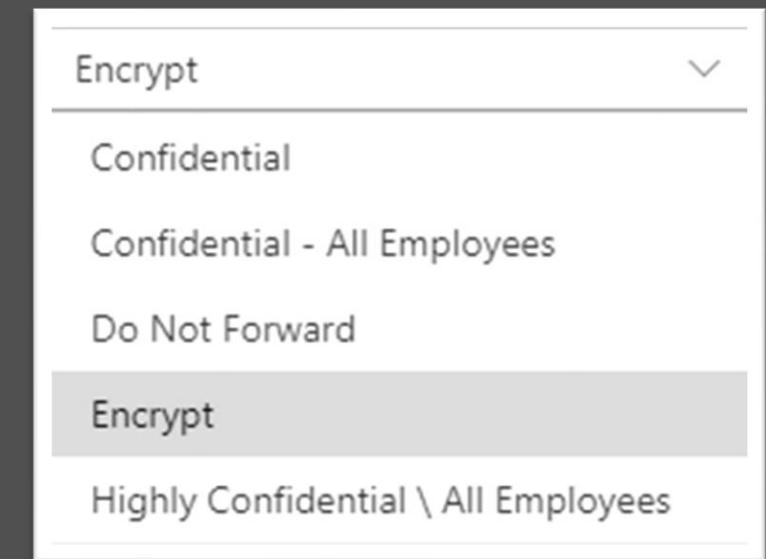
## Some examples of how it can be used

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 by 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:

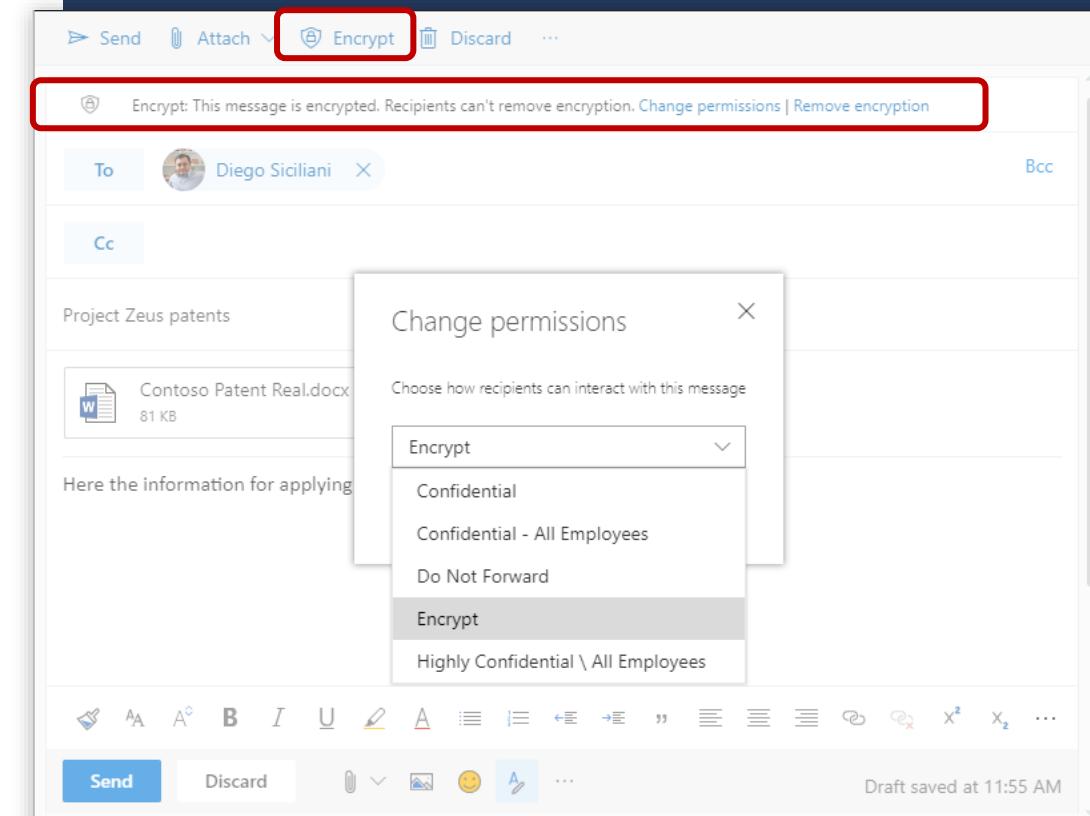
- Select the Encrypt button

## To view an encrypted message

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



# Protect and control your data and documents



Encrypt  
email



Apply restrictions  
to email and  
documents



Protect against  
data leaks



Archive  
email data

# Examples of sensitive business data

"Prices we pay for products"	"Sales forecasts"	"Protected health information"	"Compensation information"	"Product formulations"	"Phone numbers"
"Credit card and drivers license info sent to us by customers"	"Ingredients that go into our hair care products"	"Bank account and ABA numbers"	"Passport info we collect from our international 1099 contractors"	"Credit applications that people send us"	
"Customer SSN and taxpayer IDs"	"Employee files that HR keeps"	"Company financials"	"Customer lists"	"Home addresses"	"Rates we charge"

# 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

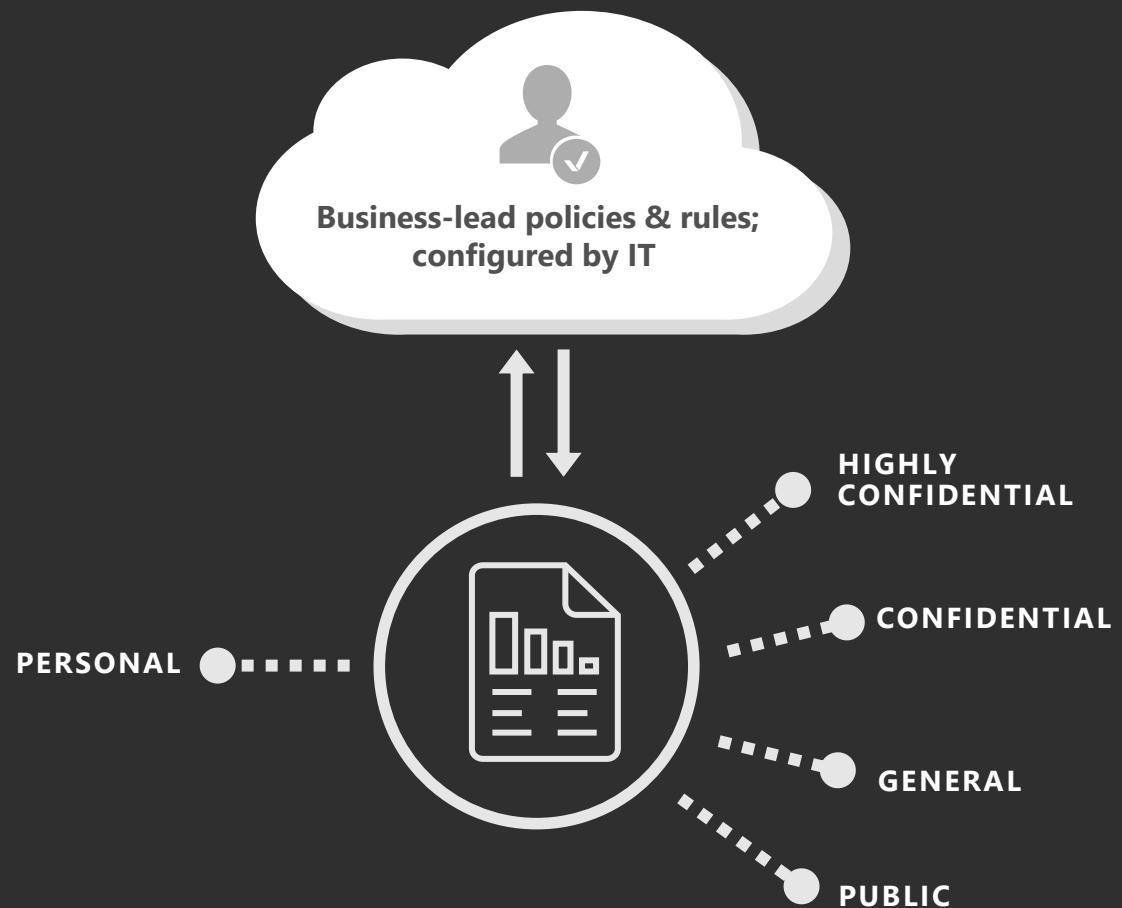
Based on the content you're working on, you can be prompted with suggested classification

## 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?

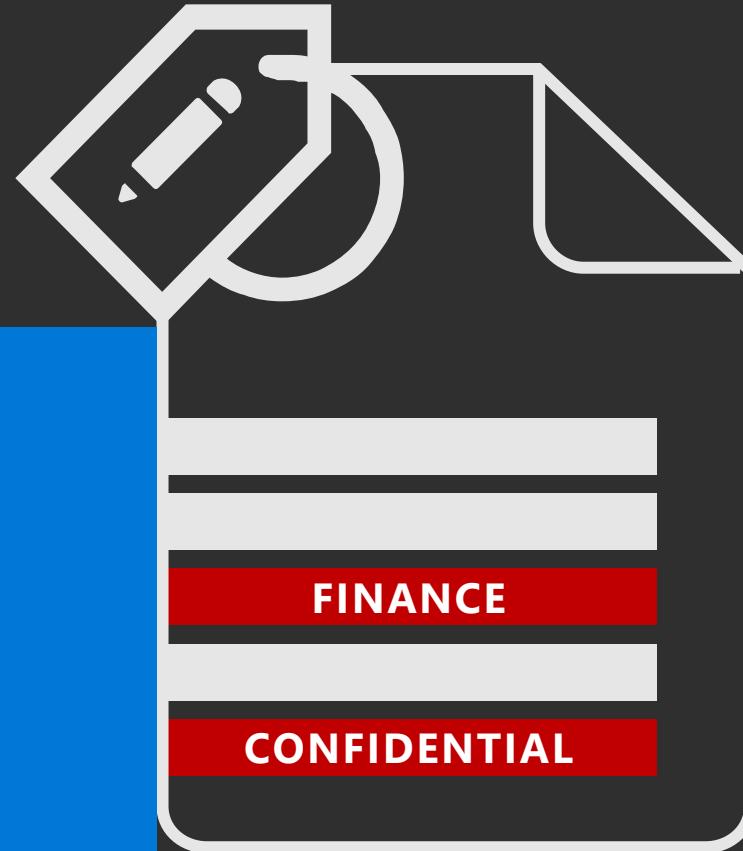
Metadata written into document files

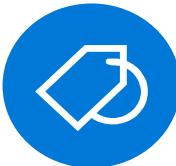
Travels with the document as it moves

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

Used for the purpose of applying 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

Labels are persistent and readable by other systems e.g. DLP engine

Label is metadata written to data

Sensitive data is automatically detected

The screenshot shows a spreadsheet interface with several annotations:

- Annotation 1:** A yellow bar at the top of the first column contains the text "Automatically labeled". Below it, a cell contains the label "Confidential". A callout points to this cell with the text "Labels are persistent and readable by other systems e.g. DLP engine".
- Annotation 2:** A yellow bar at the top of the second column contains the text "at least one credit card number". A callout points to this bar with the text "Label is metadata written to data".
- Annotation 3:** A green bar at the top of the last column contains the text "Count Used". Below it, a table lists credit card information. Two card numbers are highlighted with green boxes: "4111-1111-1111-1111" and "4012-8888-8888-1881". A callout points to these highlighted numbers with the text "Sensitive data is automatically detected".

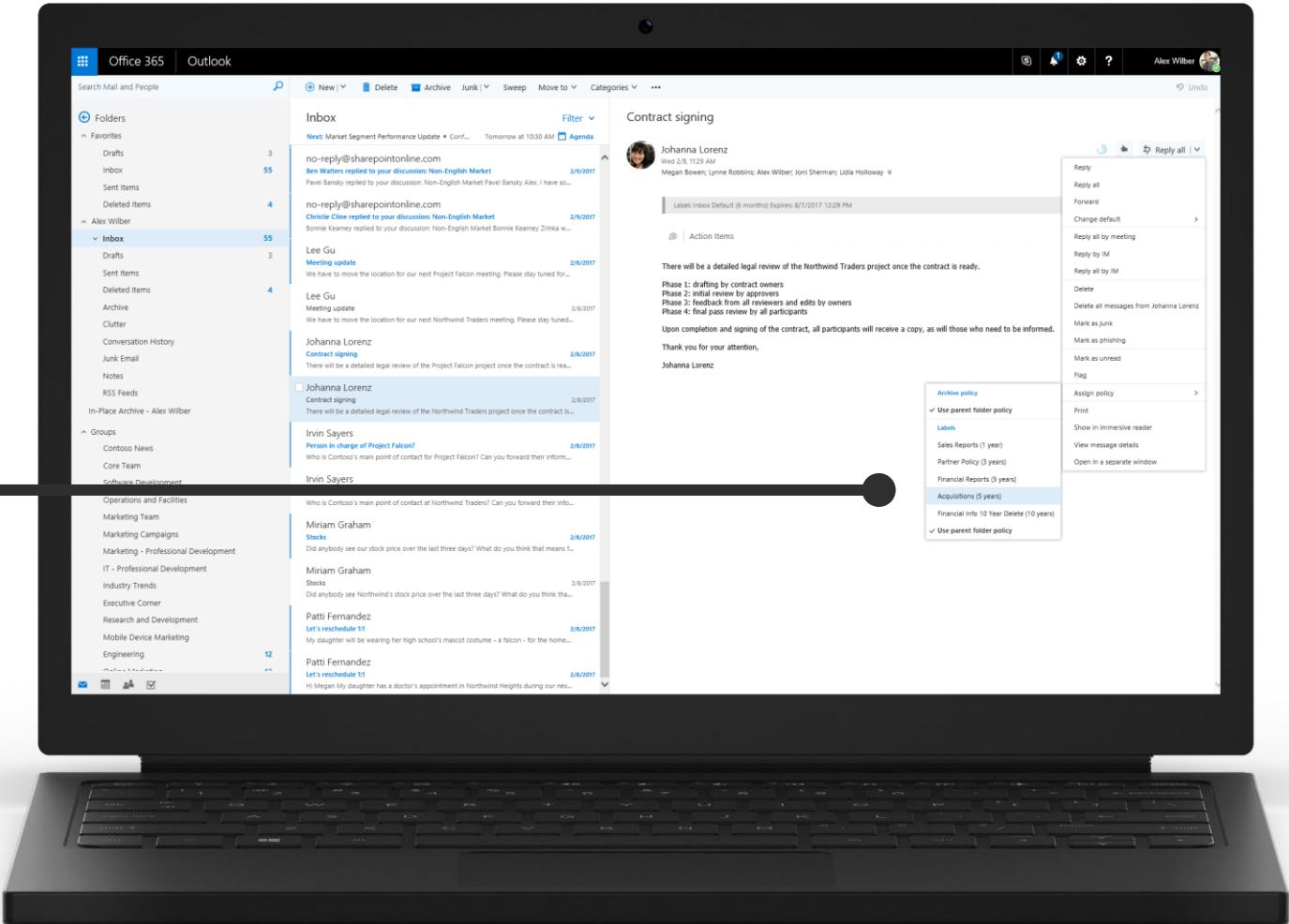
**Spreadsheets Data:**

Date	Description	Amount	Merchant name	Card Type	Expiration date	Transaction fees	Balance
7/1/2016	Existing balance	\$2,450.00	Woodgrove Bank	AmEx	08	\$2.00	\$2,450.00
7/2/2016	Payment for June	-\$34.00	Woodgrove Bank	AmEx	01	\$2.00	\$2,418.00
7/3/2016	Picture frame	\$45.00	Northwind Traders	MasterCard	07	\$20.00	\$2,463.00
7/3/2016	Wine	\$600.00	Coho Winery	Discover	08	\$20.00	\$3,083.00
7/8/2016	Ticket to Maui	\$469.00	Blue Yonder Airlines	VISA	08	\$20.00	\$3,552.00
7/12/2016	Cash withdrawal	\$654.00	Woodgrove Bank	AmEx	08	\$20.00	\$4,206.00
7/3/2016	Wine	\$600.00	Coho Winery	Discover	08	\$20.00	\$4,826.00



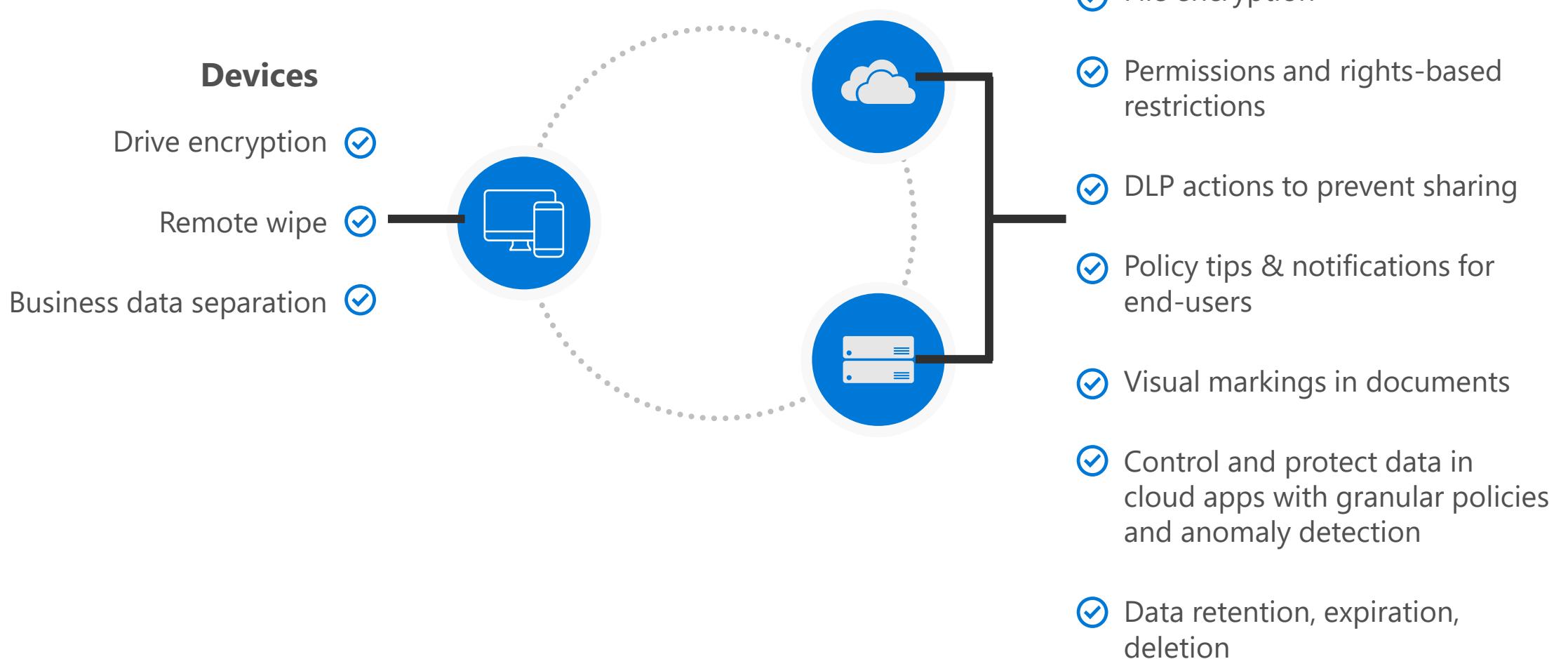
# CLASSIFICATION & LABELING EXAMPLE – DATA GOVERNANCE

Labeling can be end-user driven or automatically applied





# PROTECT SENSITIVE DATA ACROSS YOUR ENVIRONMENT



- 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

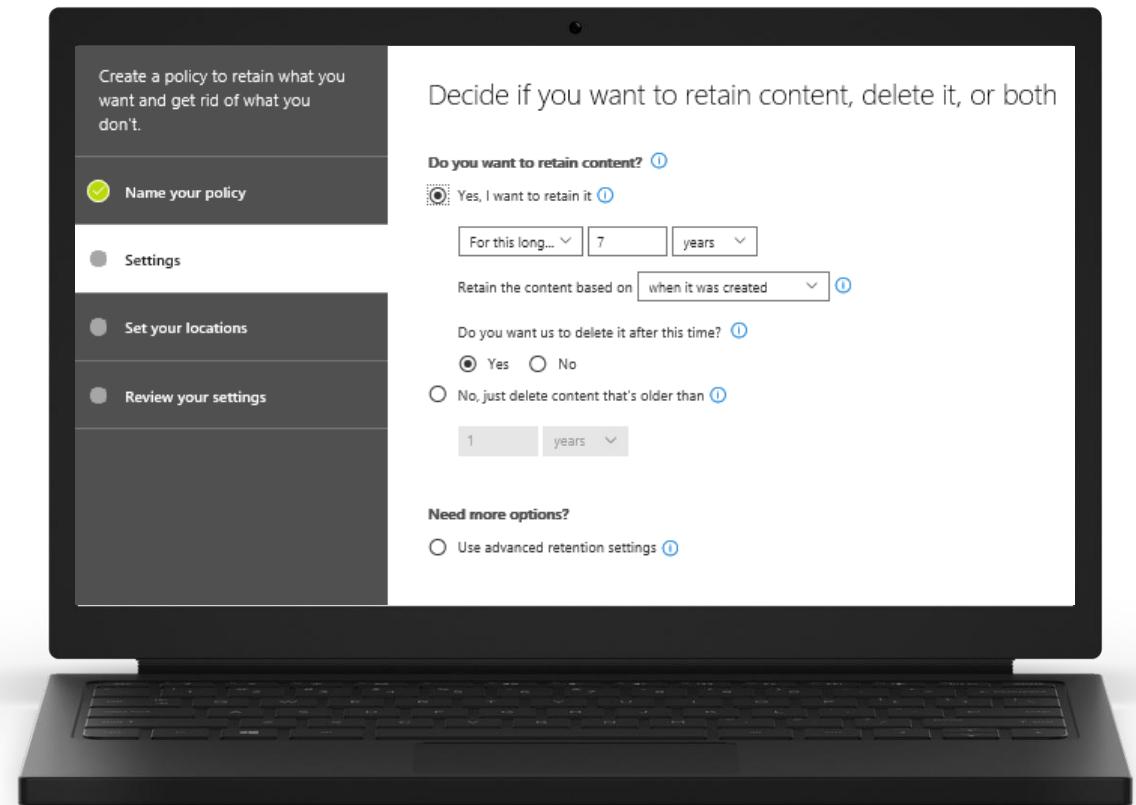
Retain content in sites, mailboxes, and public folders indefinitely or for a specific duration

## 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

