Microsoft

CSP Masters Program in person series
Technical training

Microsoft

Protecting against data loss

How can I protect my customer from data loss?

Name: Bob D

Role: Technical Consultant

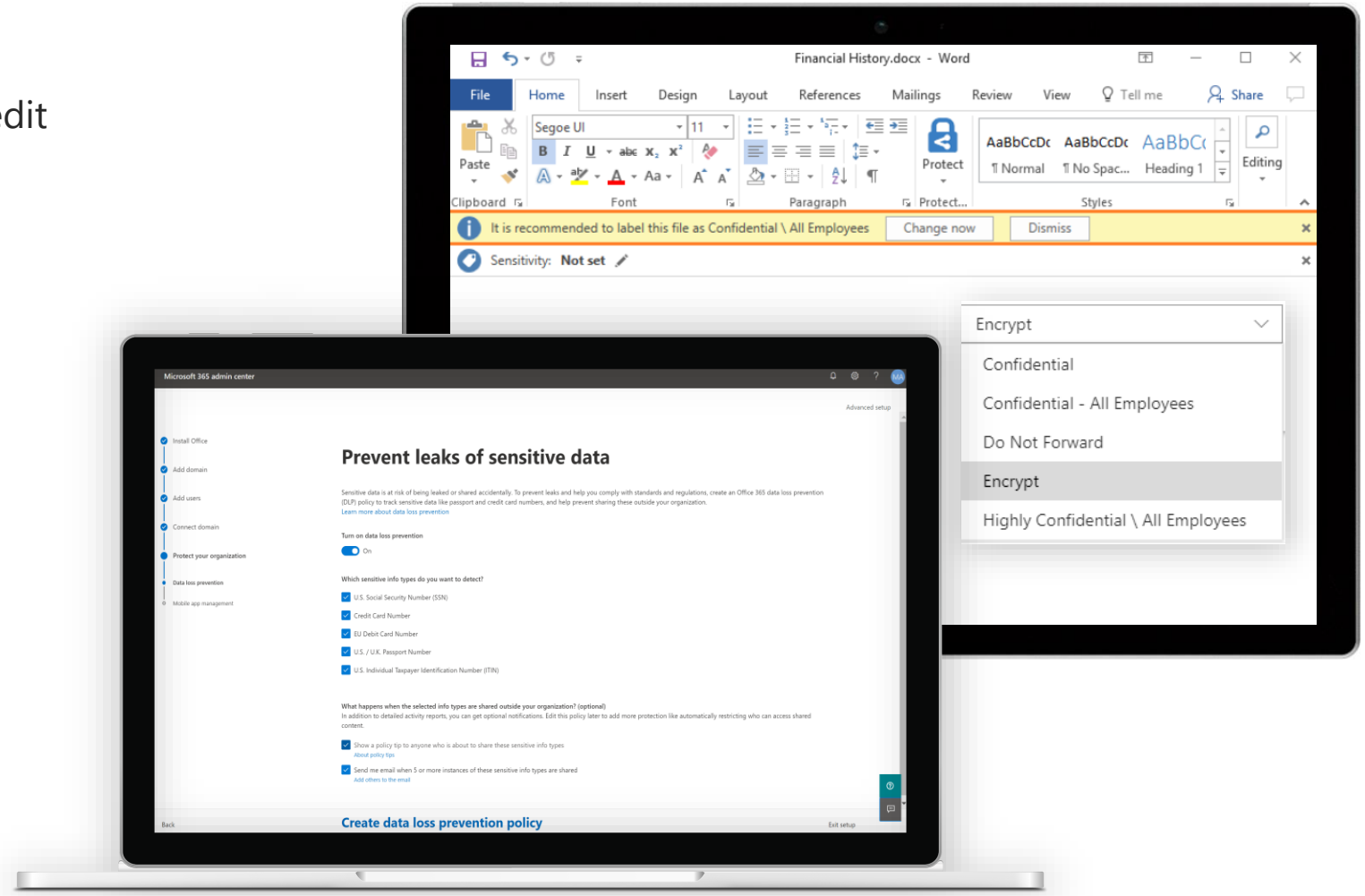
Company: Partner

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.



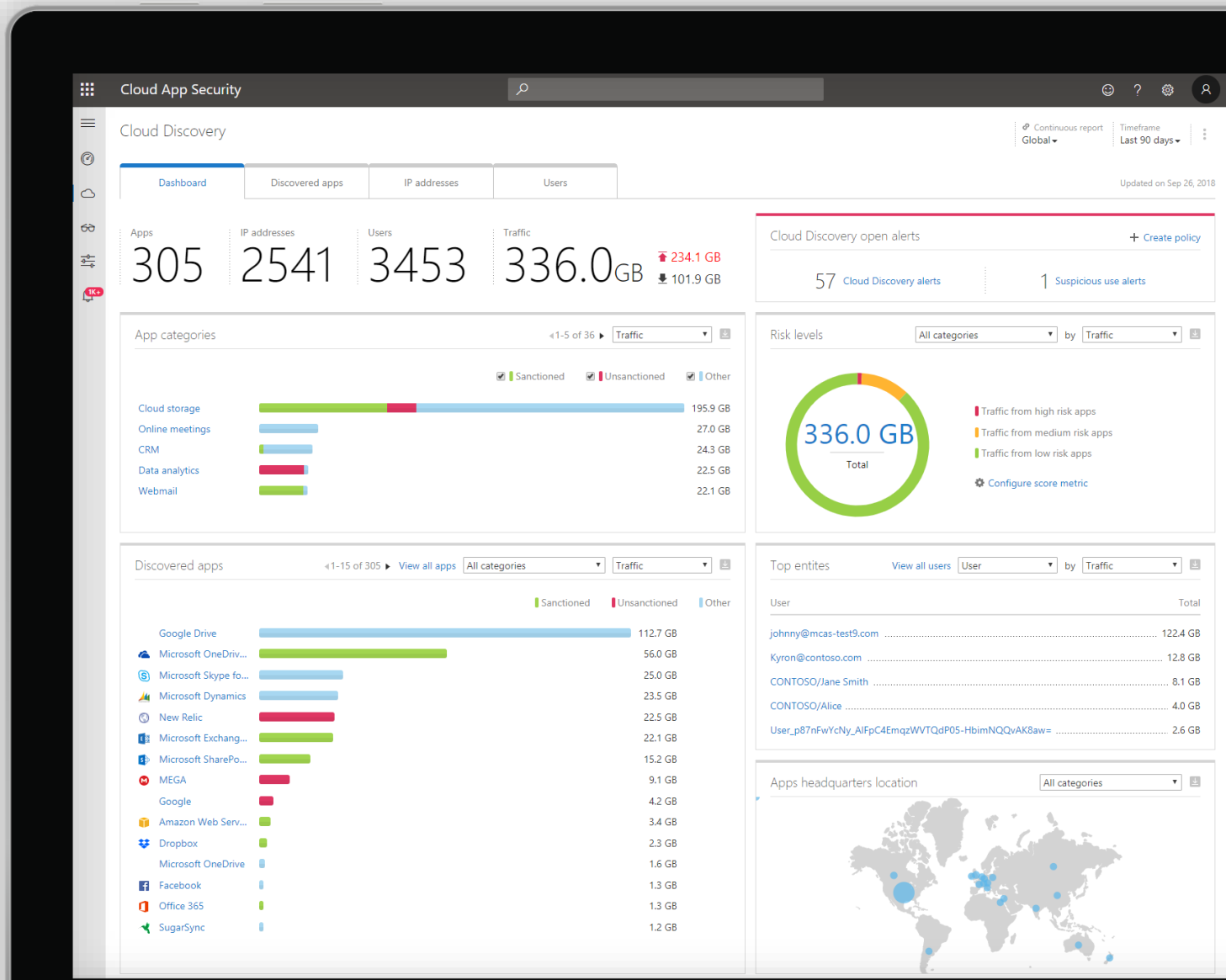
Get visibility into cloud app use with Cloud App Discovery

Discover cloud app usage to understand shadow IT risk

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

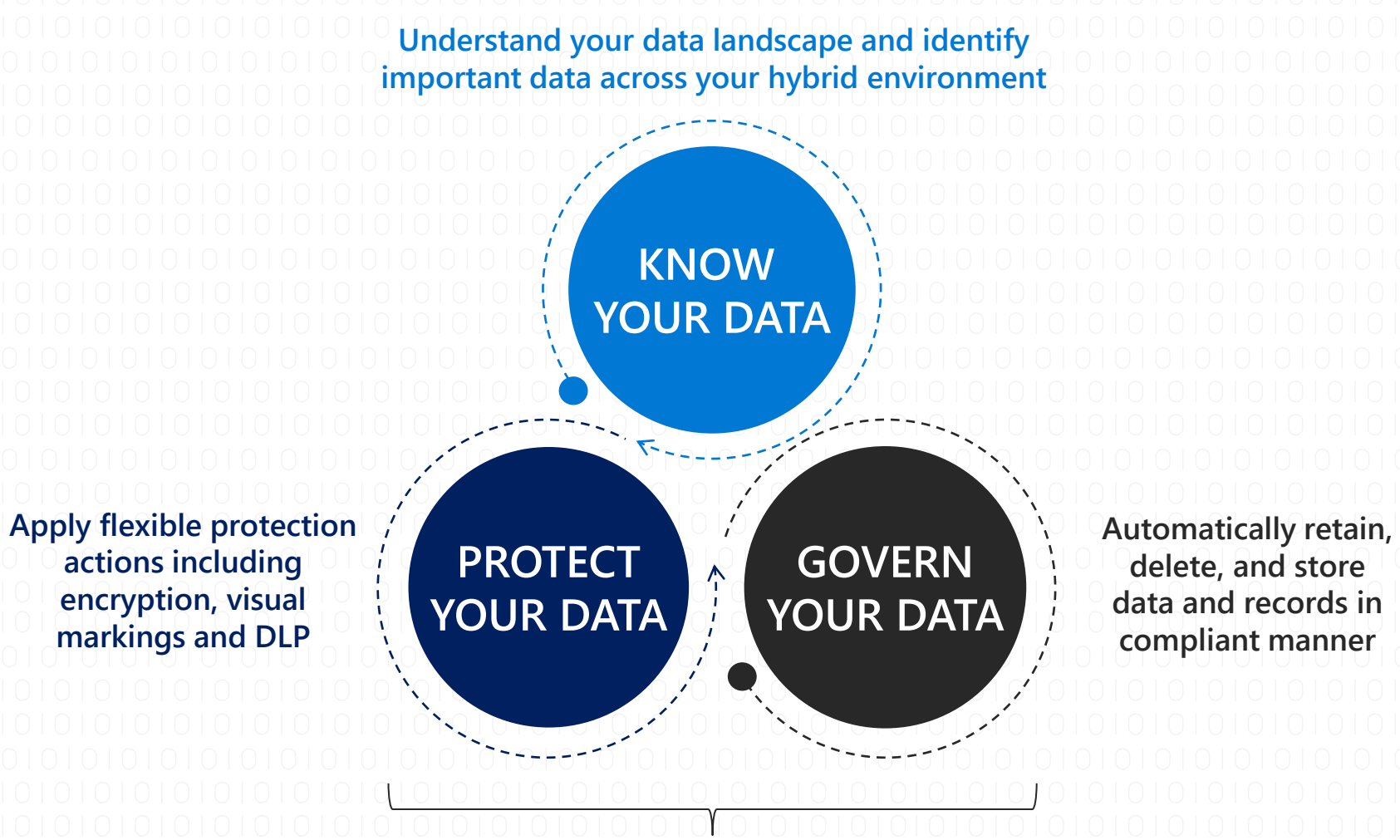
Understand usage patterns and identify high risk users. Export data for additional analysis

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



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

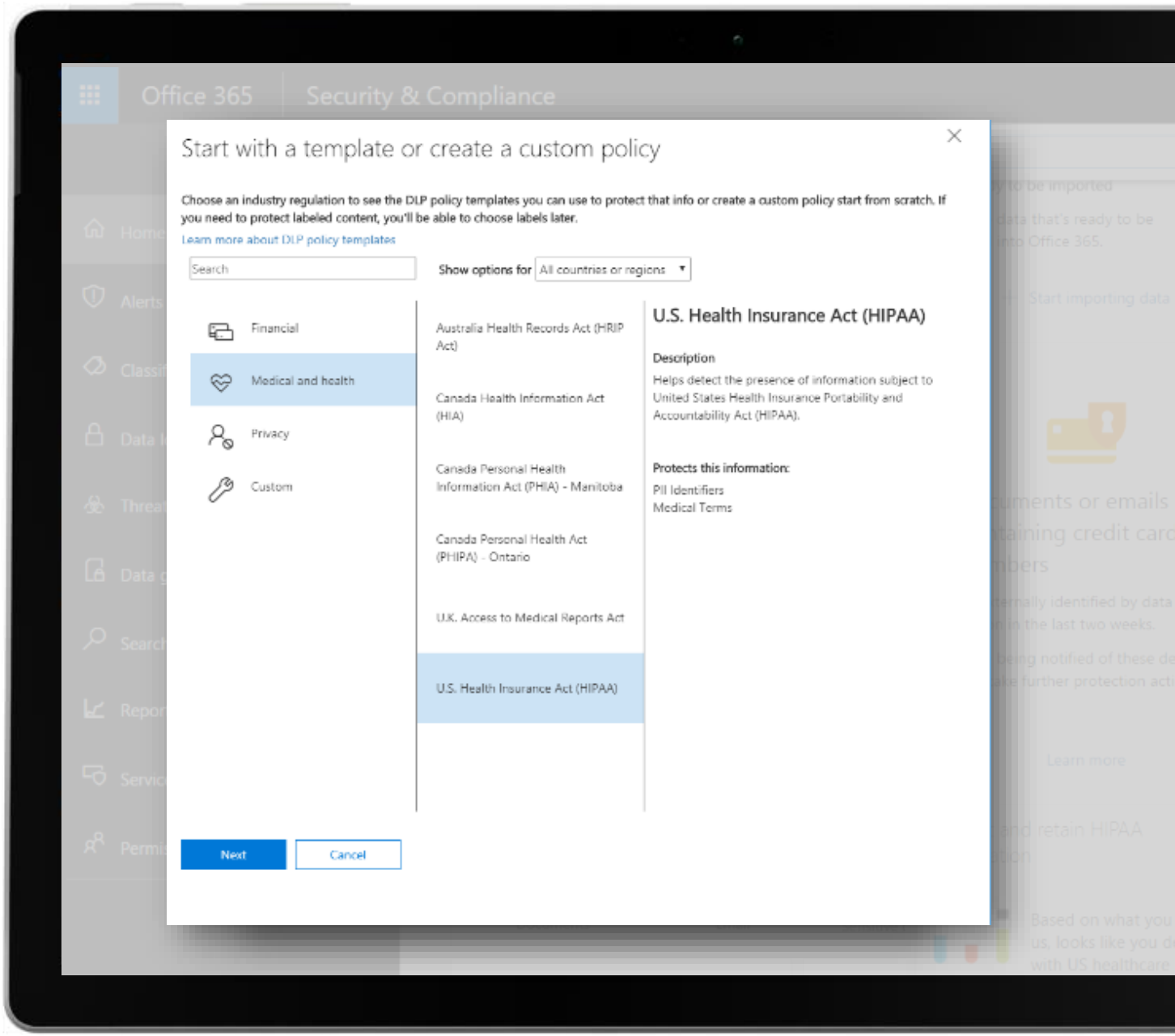
Built-in Policies & Templates

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

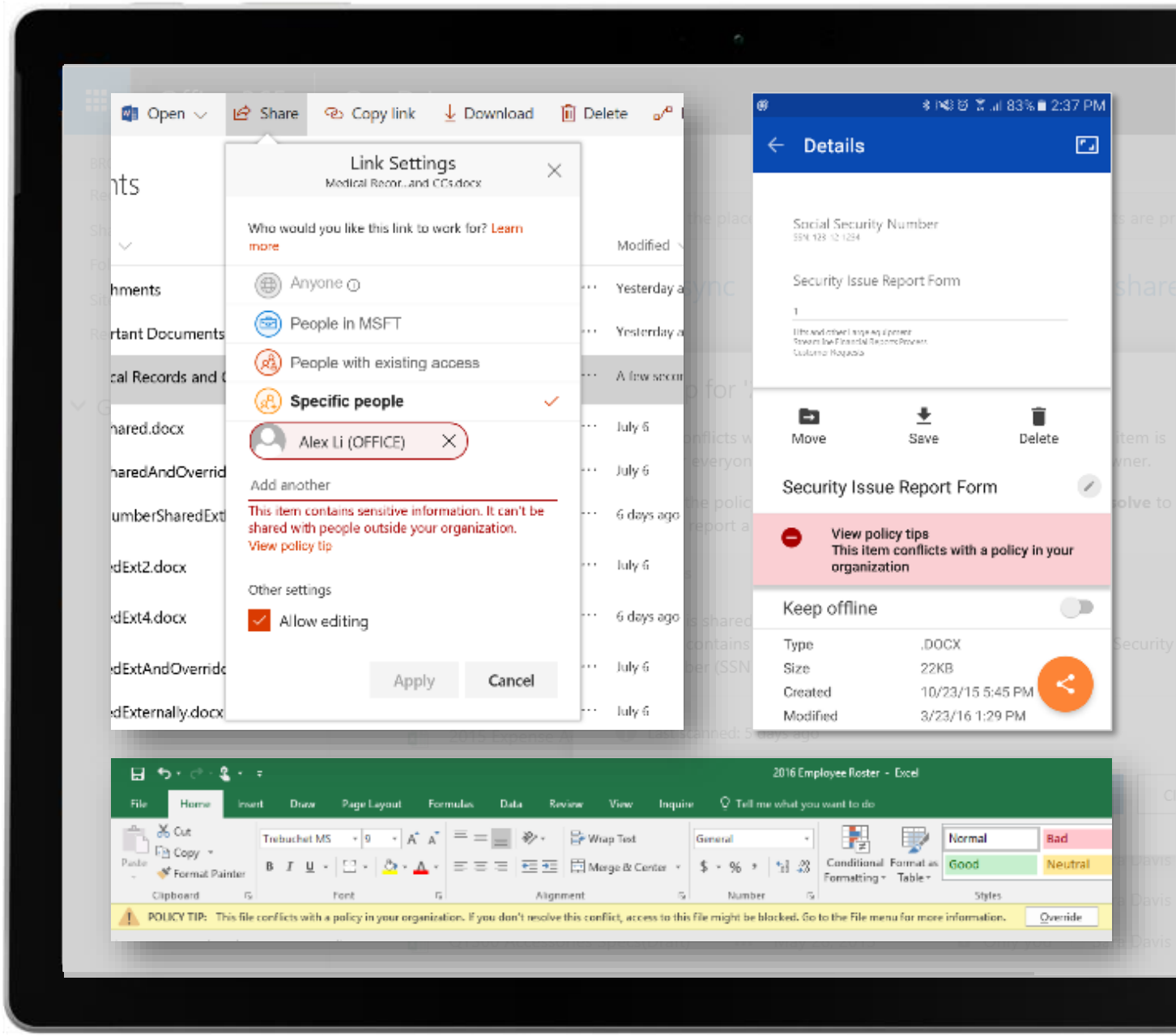
System-generated insights with step-by-step enablement for additional protection controls



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.



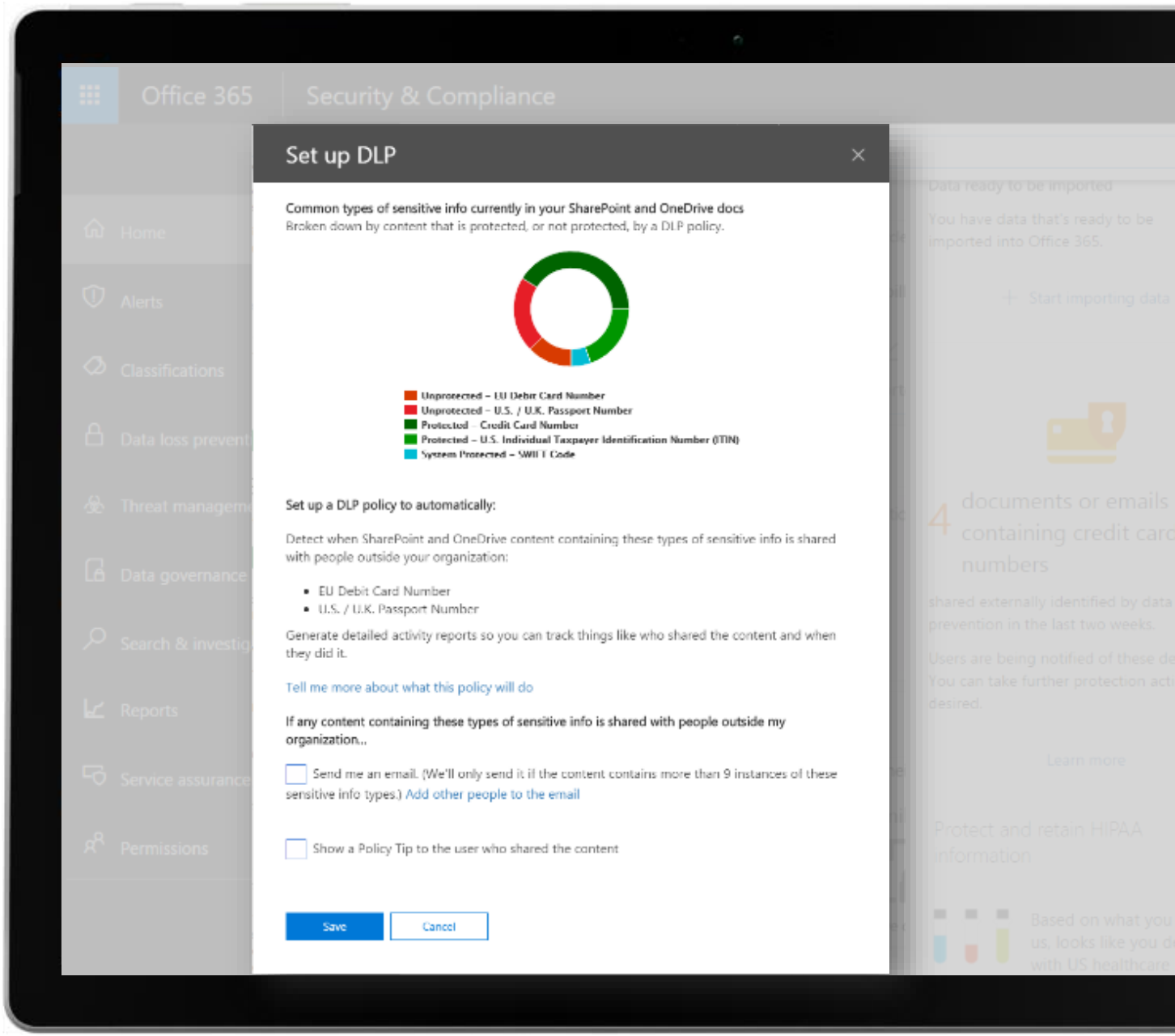
Usage-driven recommendations

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



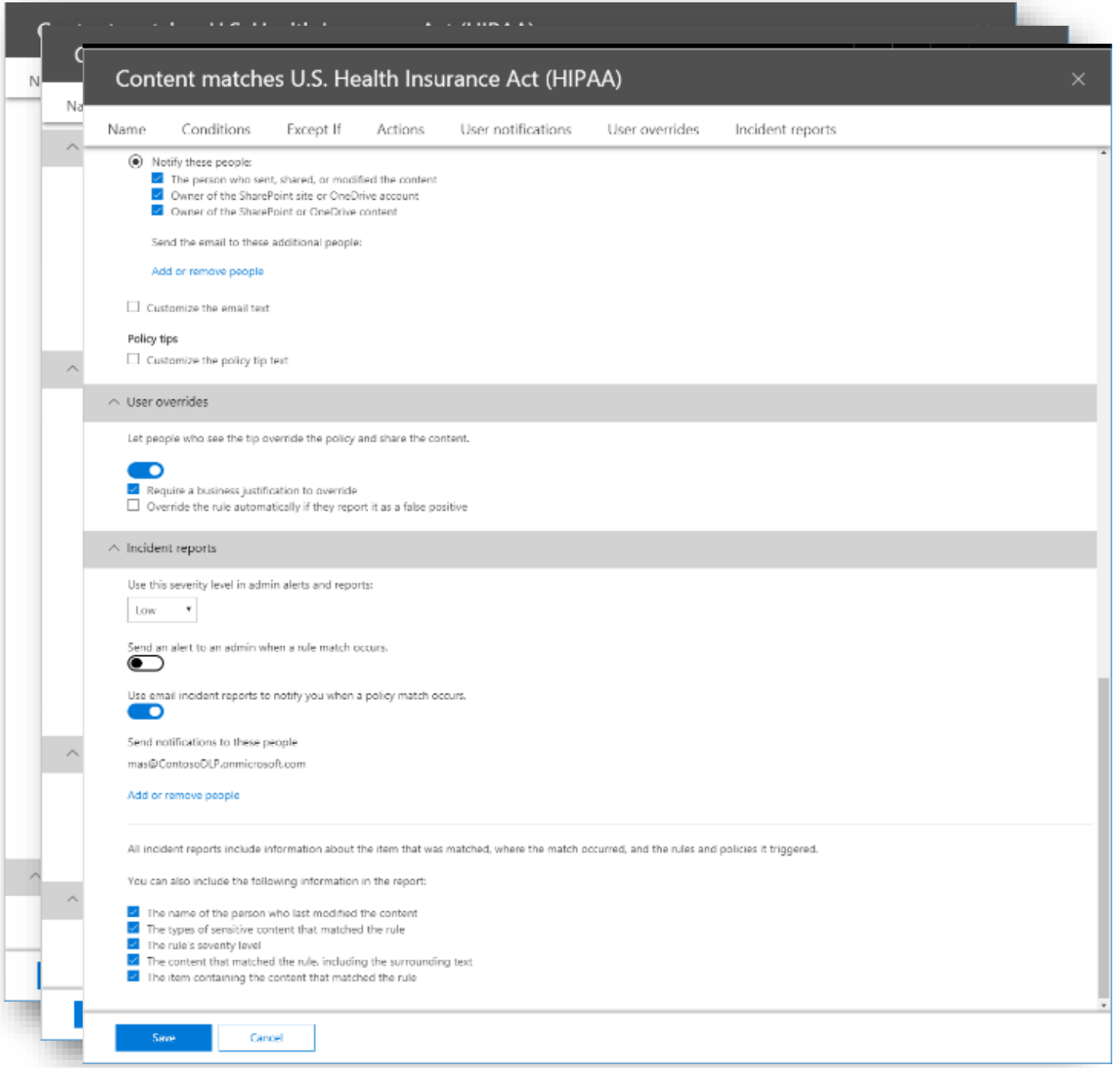
Rich customization

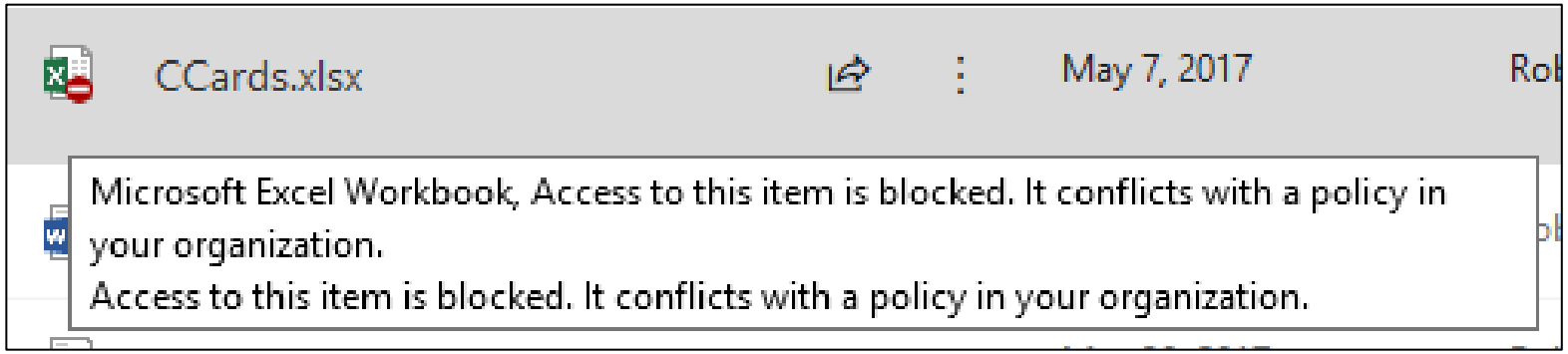
Conditions & Exceptions describe what the content looks like (or doesn't look like), and what events to look for.

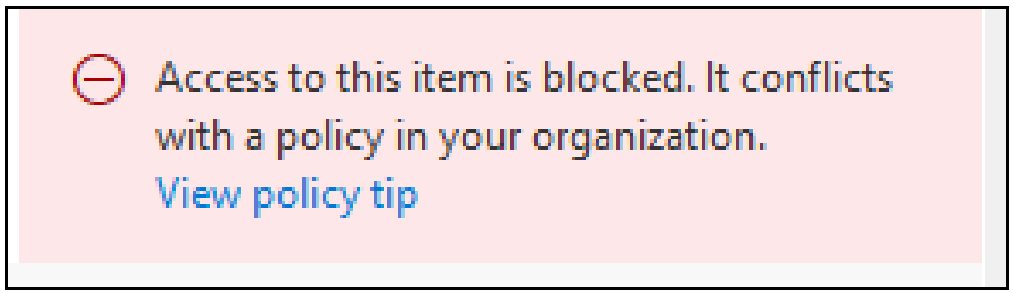
Actions define what type of automatic remediation you want to take when the conditions match

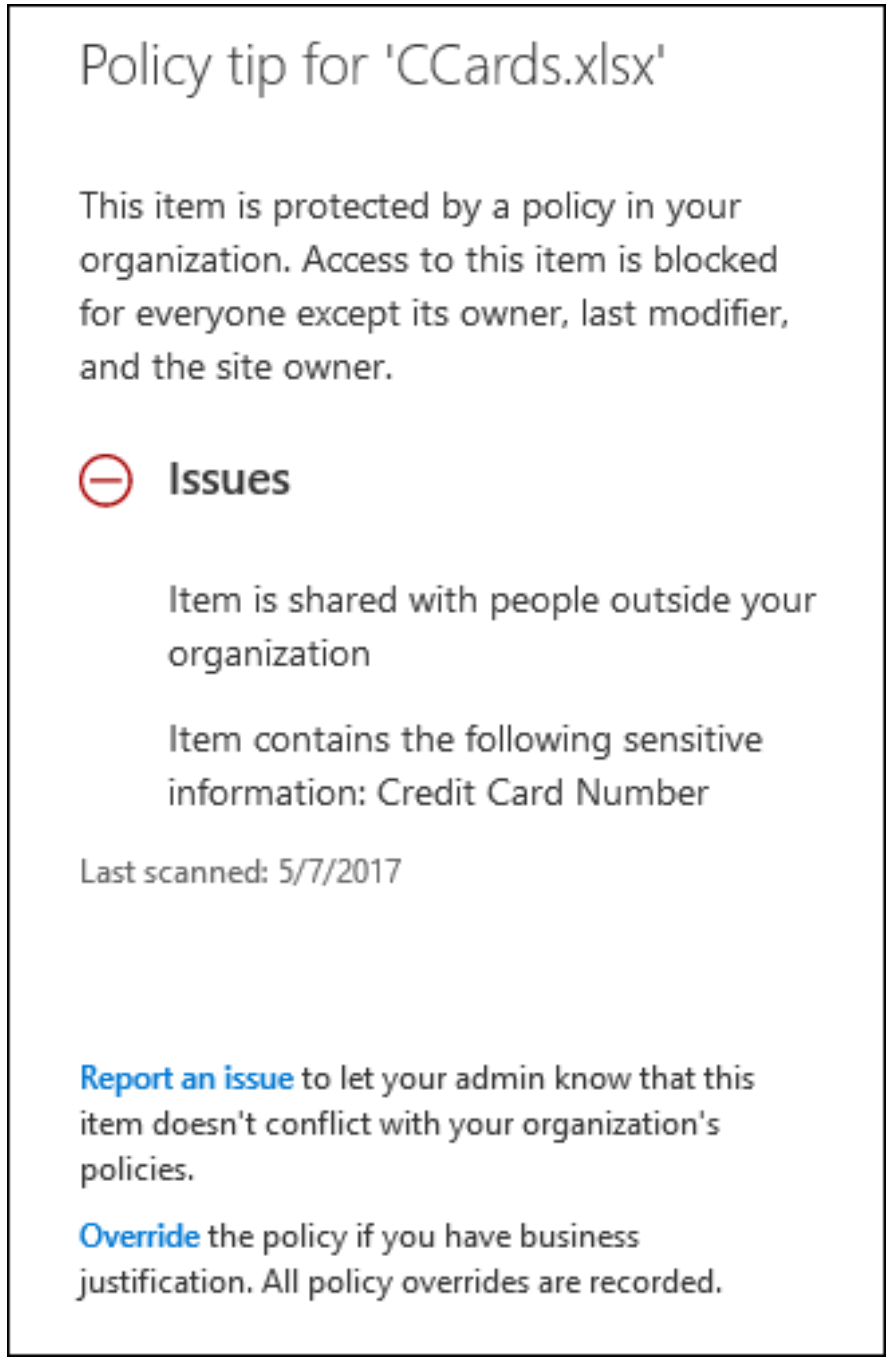
User notifications & overrides define what the user sees, and if they have the ability to override with a business justification

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




CCards.xlsx
May 7, 2017
Microsoft Excel Workbook, Access to this item is blocked. It conflicts with a policy in your organization.
Access to this item is blocked. It conflicts with a policy in your organization.


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


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
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.

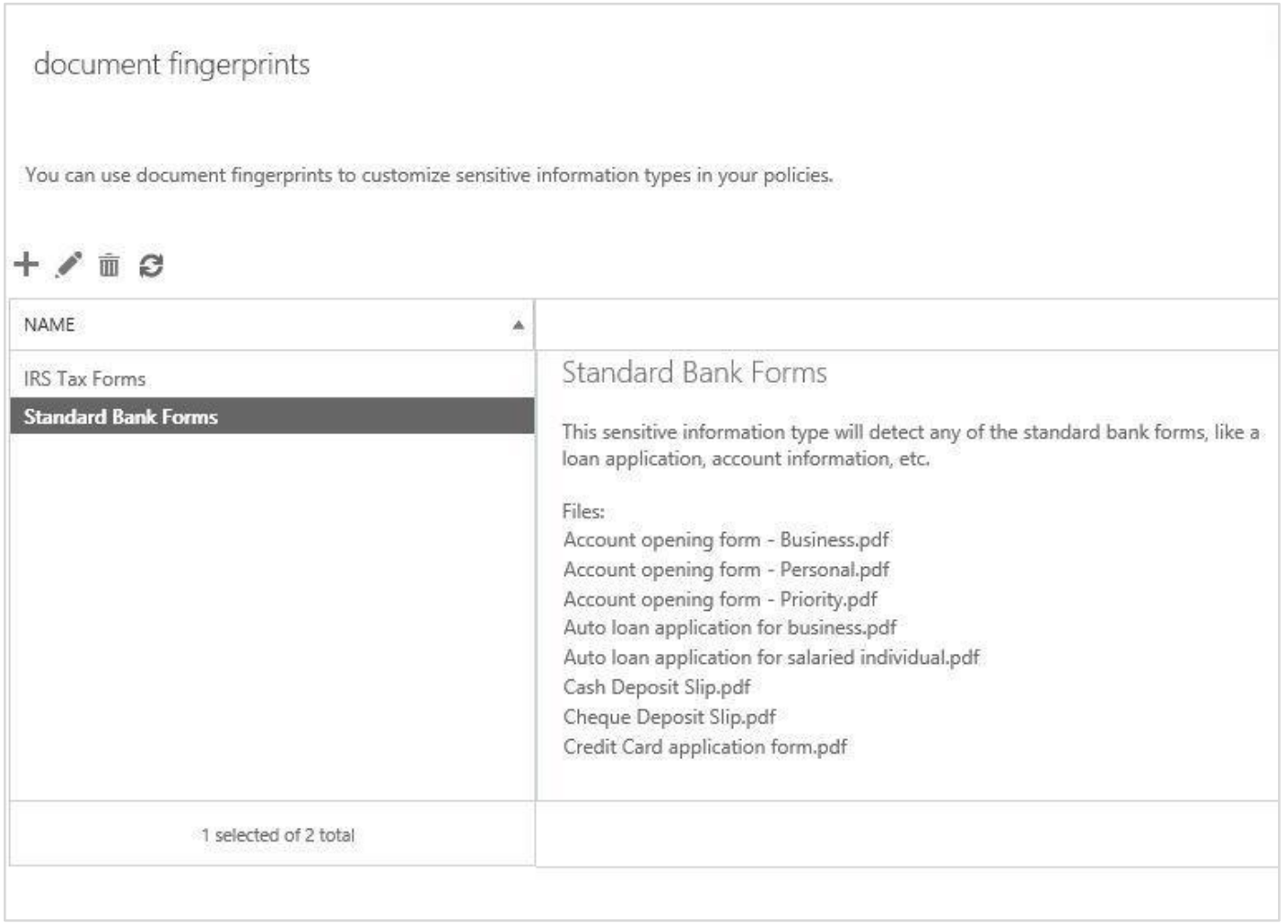
DLP document fingerprinting

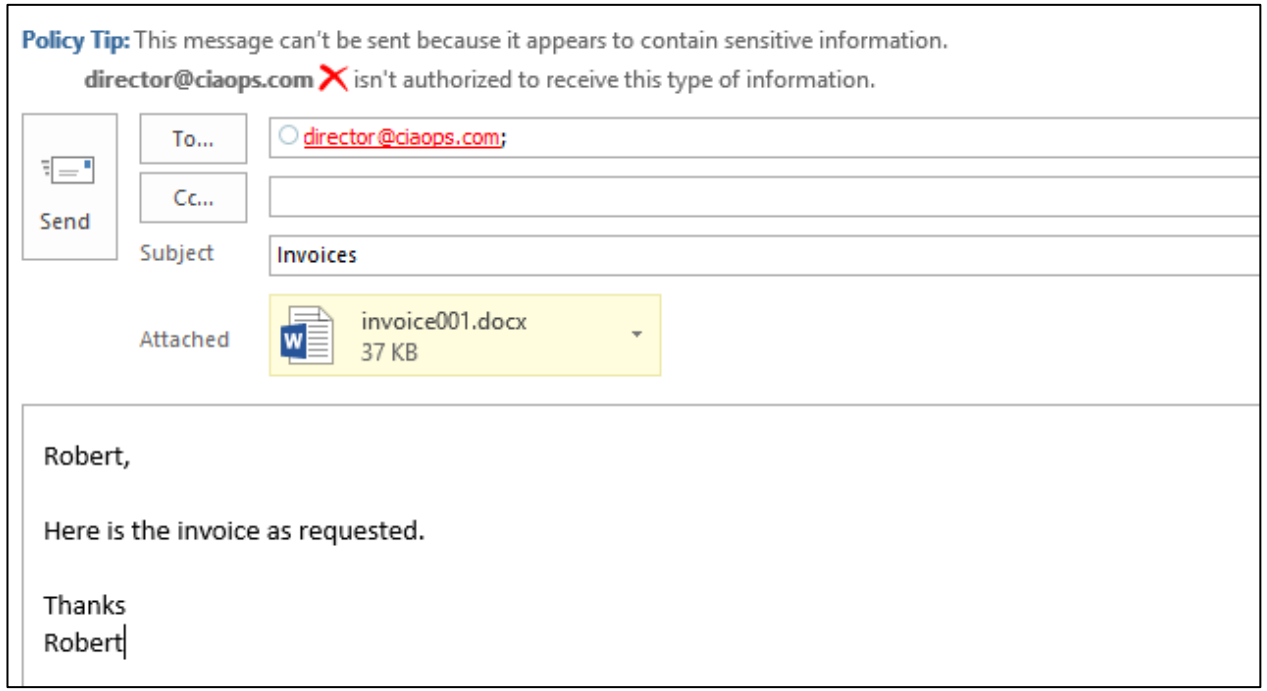
* **Note** that you can currently create a document fingerprint only by using PowerShell in the Security & Compliance Center.

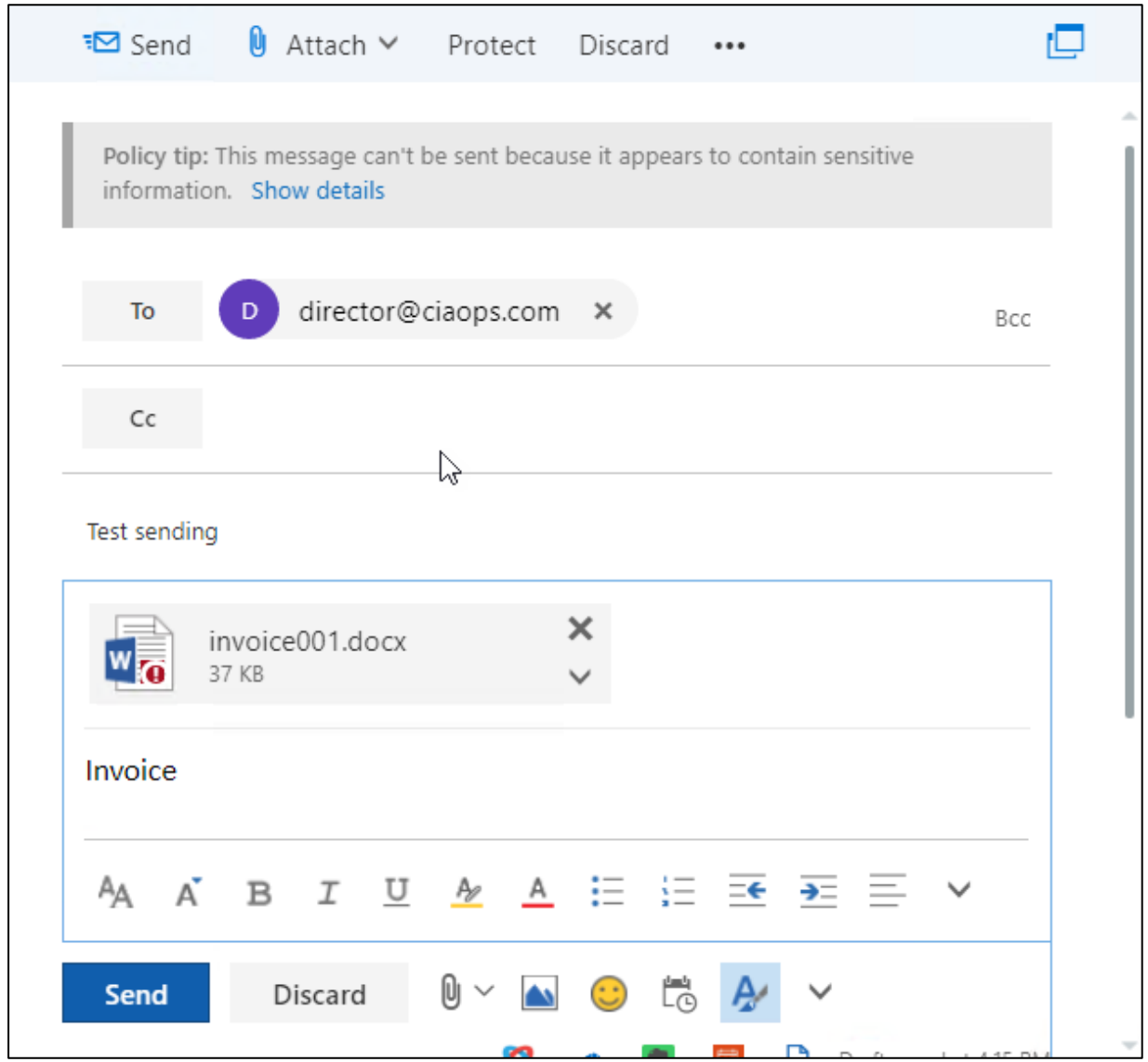
Scan email and attachments to look for patterns that match document templates

Protect sensitive documents from being accidently shared outside your organization

No coding required; simply upload sample documents to create fingerprints




Policy Tip: This message can't be sent because it appears to contain sensitive information.
director@ciaops.com isn't authorized to receive this type of information.
Send
To...
director@ciaops.com;
Cc...
Subject
Invoices
Attached
invoice001.docx
37 KB
Robert,
Here is the invoice as requested.
Thanks
Robert

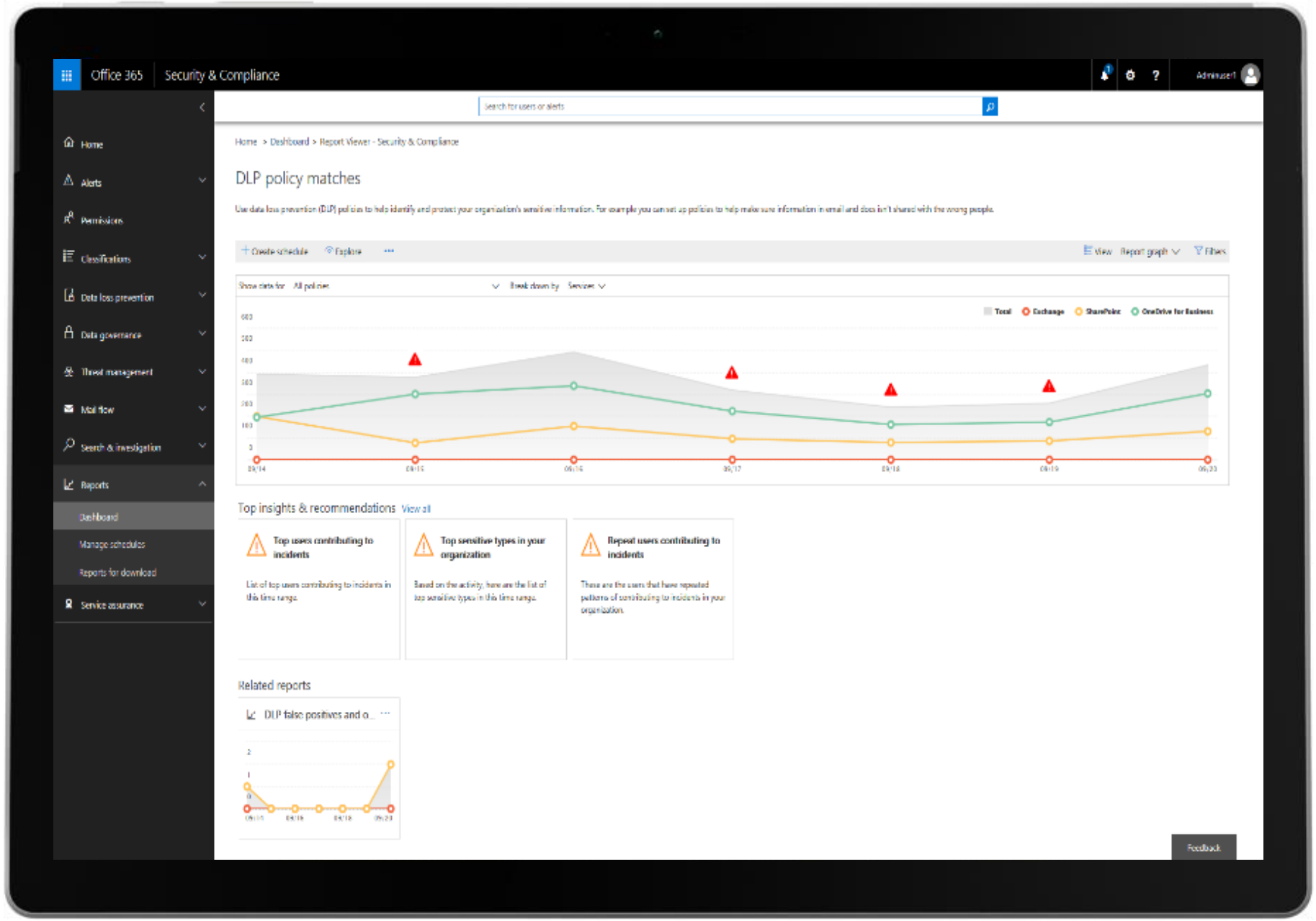

Send
Attach
Protect
Discard
Policy tip: This message can't be sent because it appears to contain sensitive information. Show details
To
director@ciaops.com
Bcc
Cc
Test sending
invoice001.docx
37 KB
Invoice
Send
Discard

Smart Reports

Smart report insights provide information on data abnormalities

Suggest actions to take to remediate

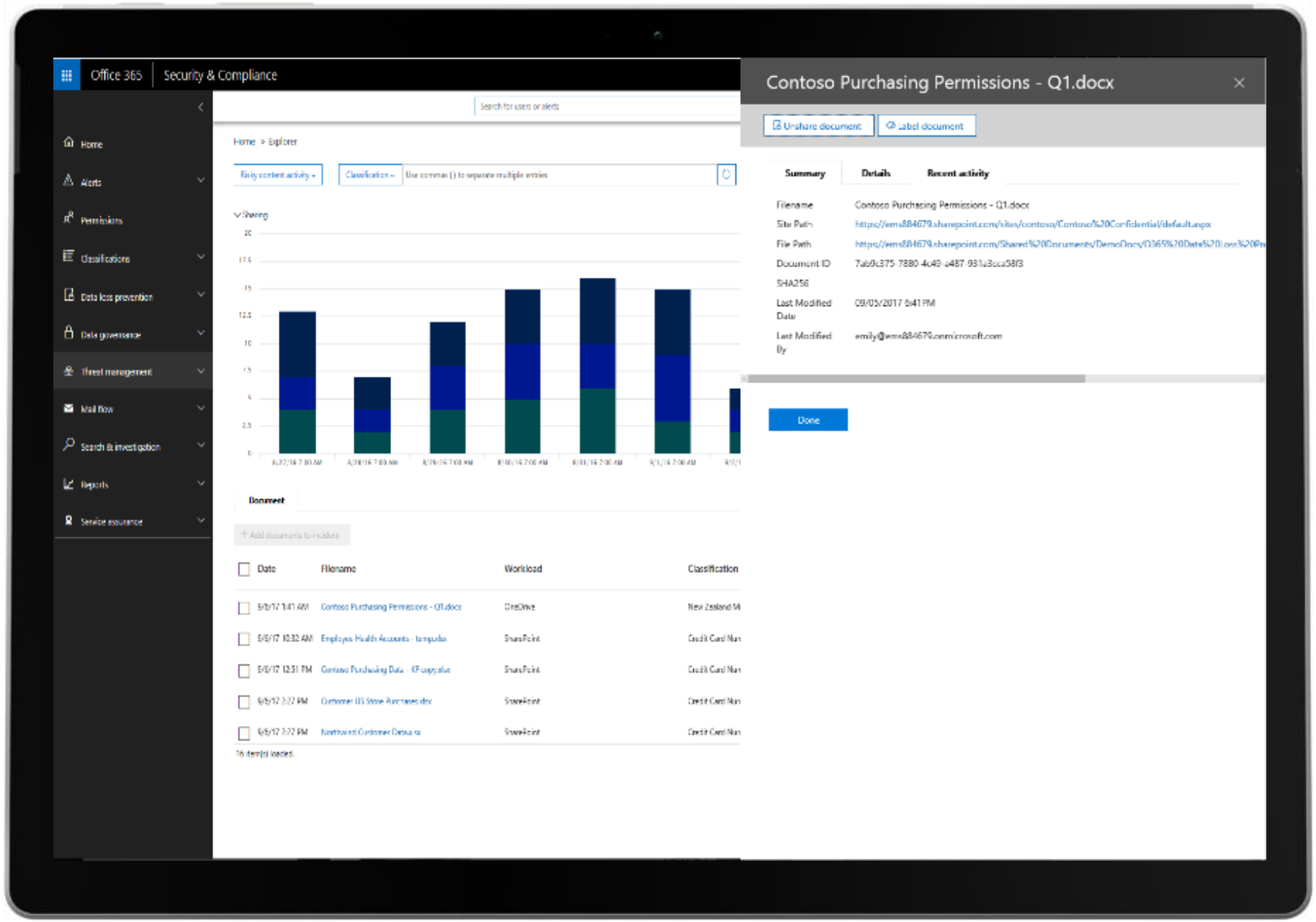
Enable admins to continue their investigation through the explorer



Investigate and **Remediate**

Investigate policy violation in your organization

Take remediation steps for documents to prevent further risk



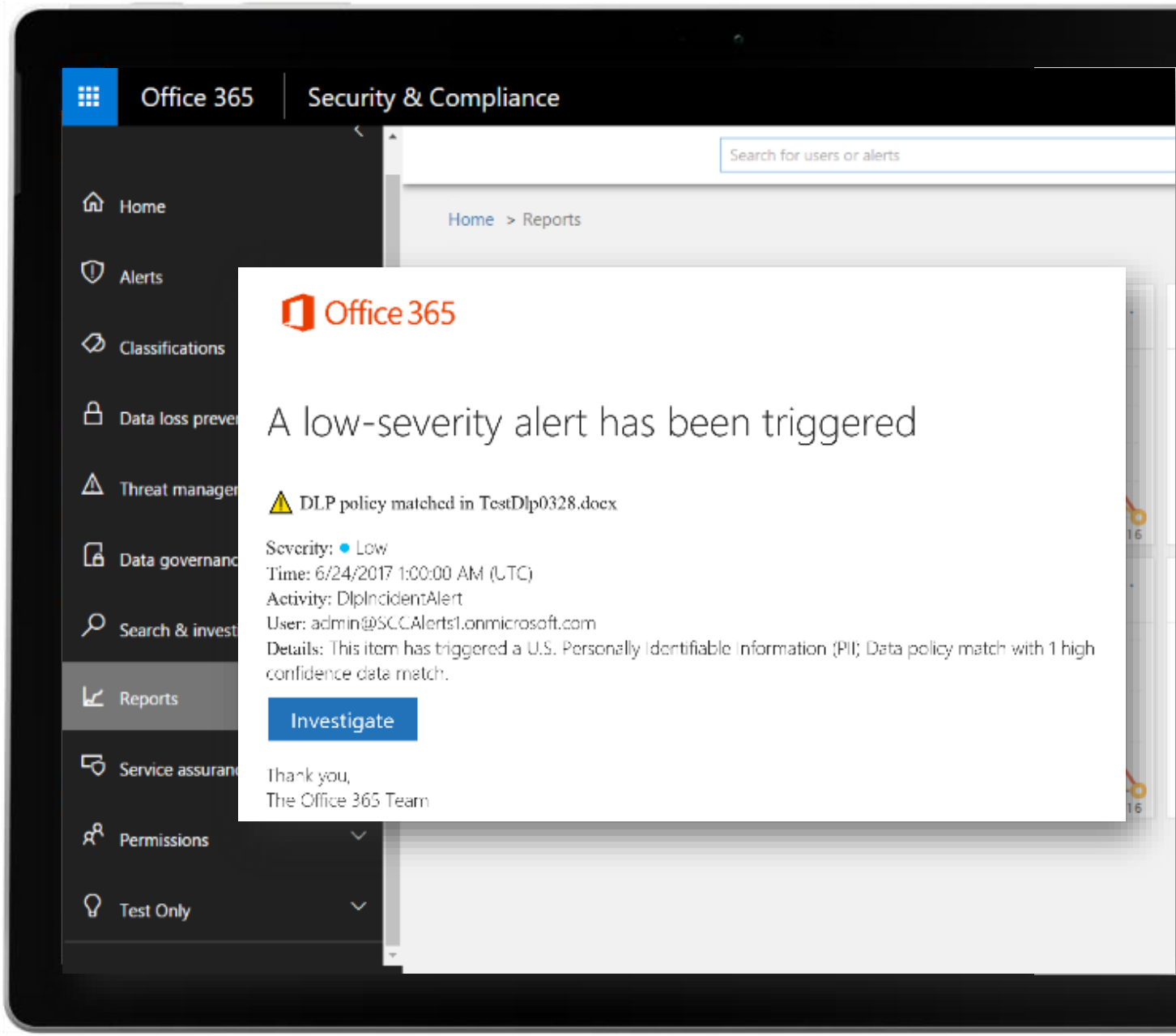
DLP **alerts and notification**

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

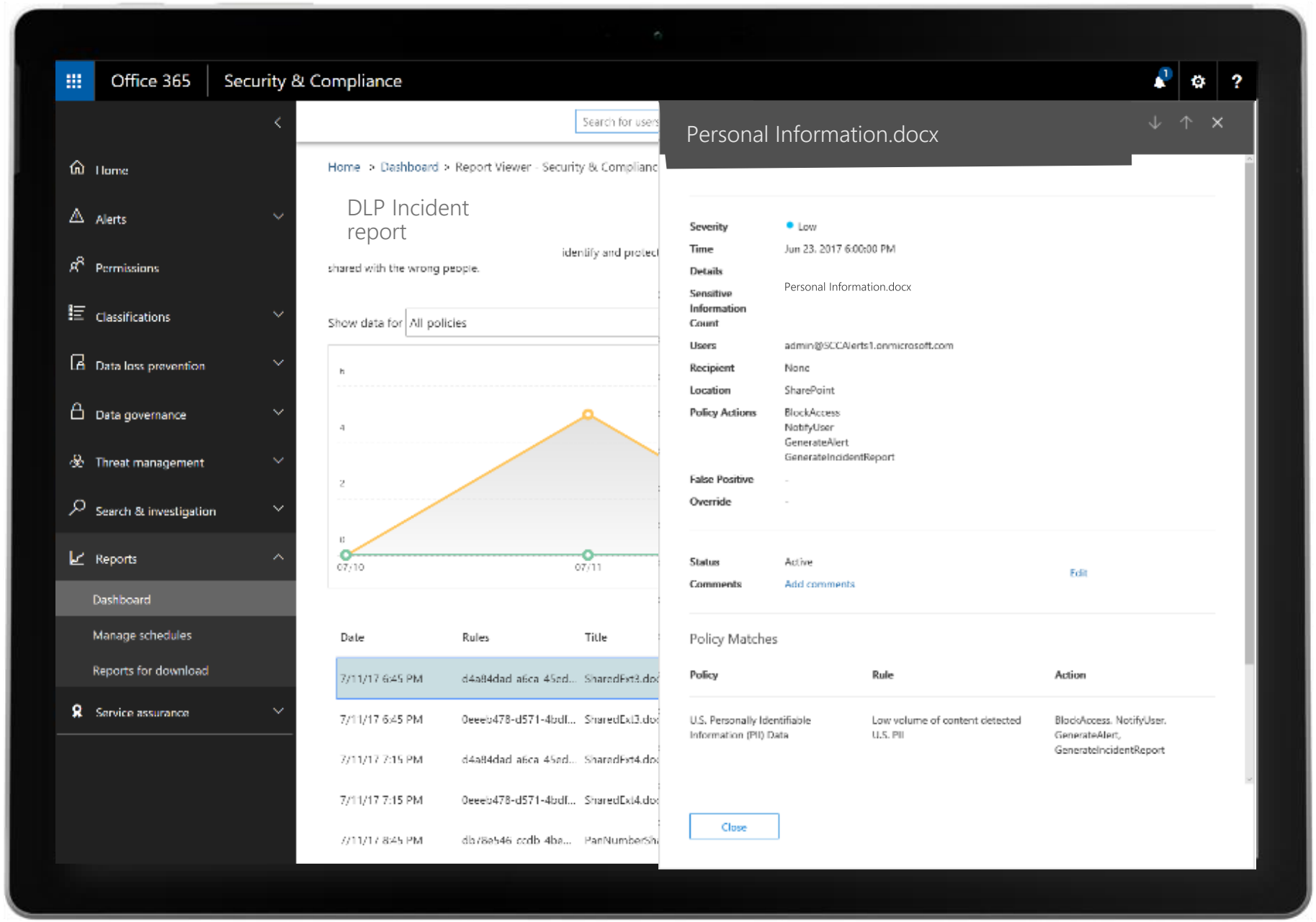


Incident Level View

Complete view of DLP detection for quick assessment of impact

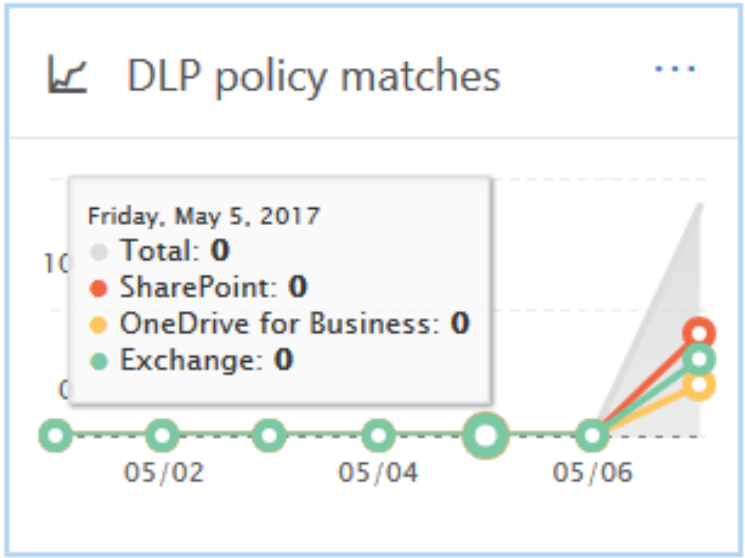
Consolidates applicable policies, rules, detected classifications

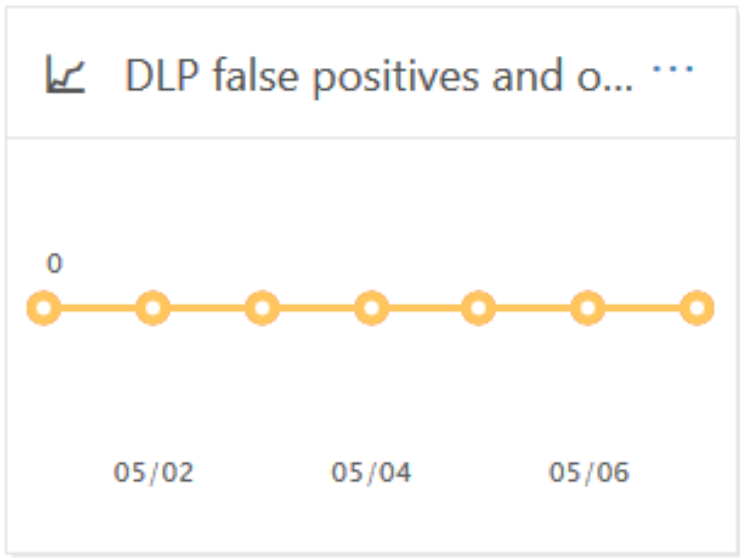
Optionally includes sensitive data matches



Home > Data loss prevention

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





+ Create a policy Refresh Search

Name	Order	Last modified	Status
Credit Card Policy	1	May 7, 2017	On
Australia Financial Data	2	May 7, 2017	On

Best practices

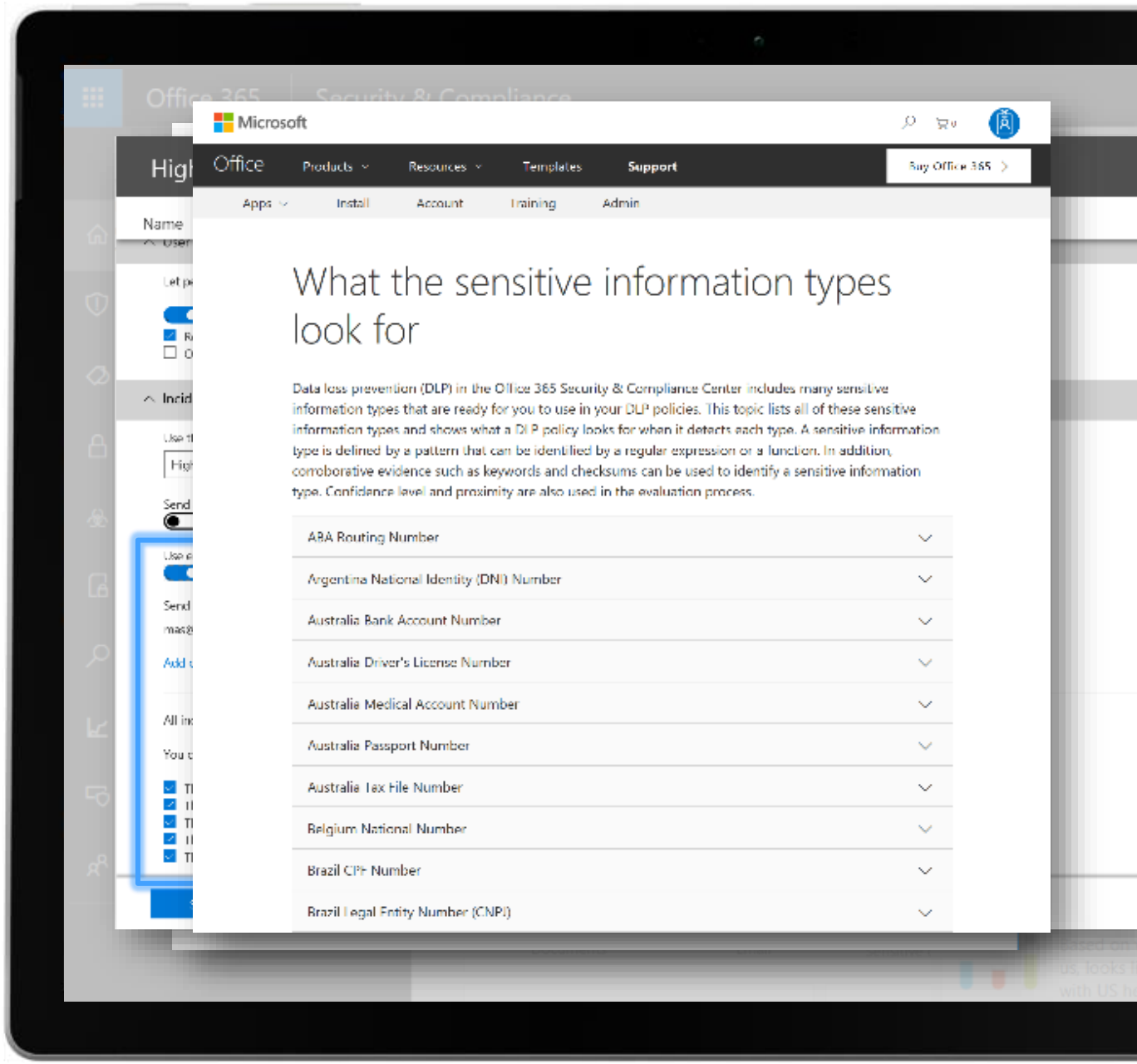
Get started today with templates

Use test mode to audit impact before impacting *anyone*

Turn on Email Incident Reports to see policy match accuracy results

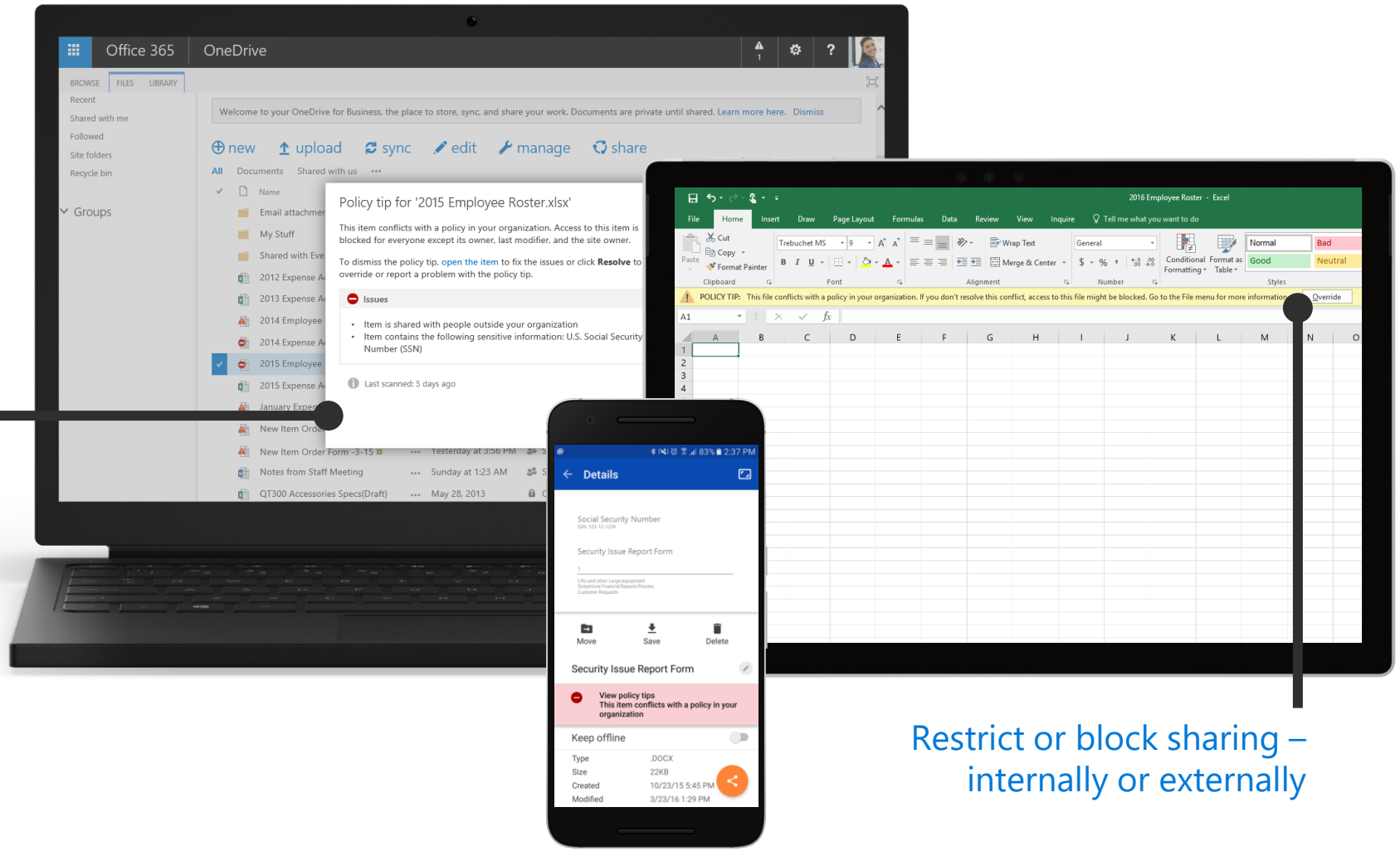
Use valid sample data when testing

- http://aka.ms/dlpsensitivetypes



PROTECTION EXAMPLE:
DLP POLICY TO **LIMIT DOCUMENT SHARING**

Across Office client applications – mobile, desktop & tablets



Policy tips to warn end users

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:

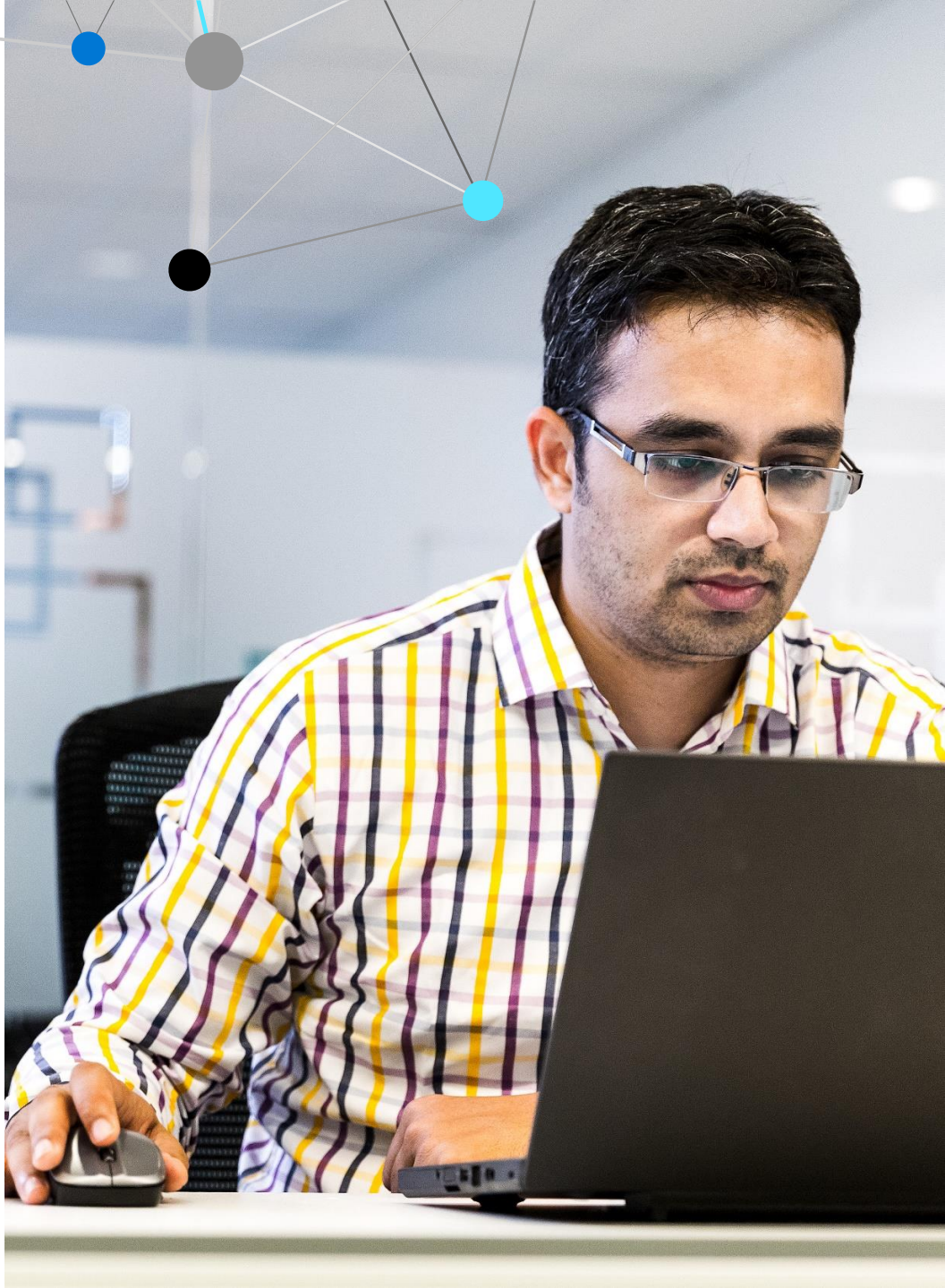
Files containing sensitive information often leave the four walls of your business. This puts your data at risk of falling into the wrong hands.

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.

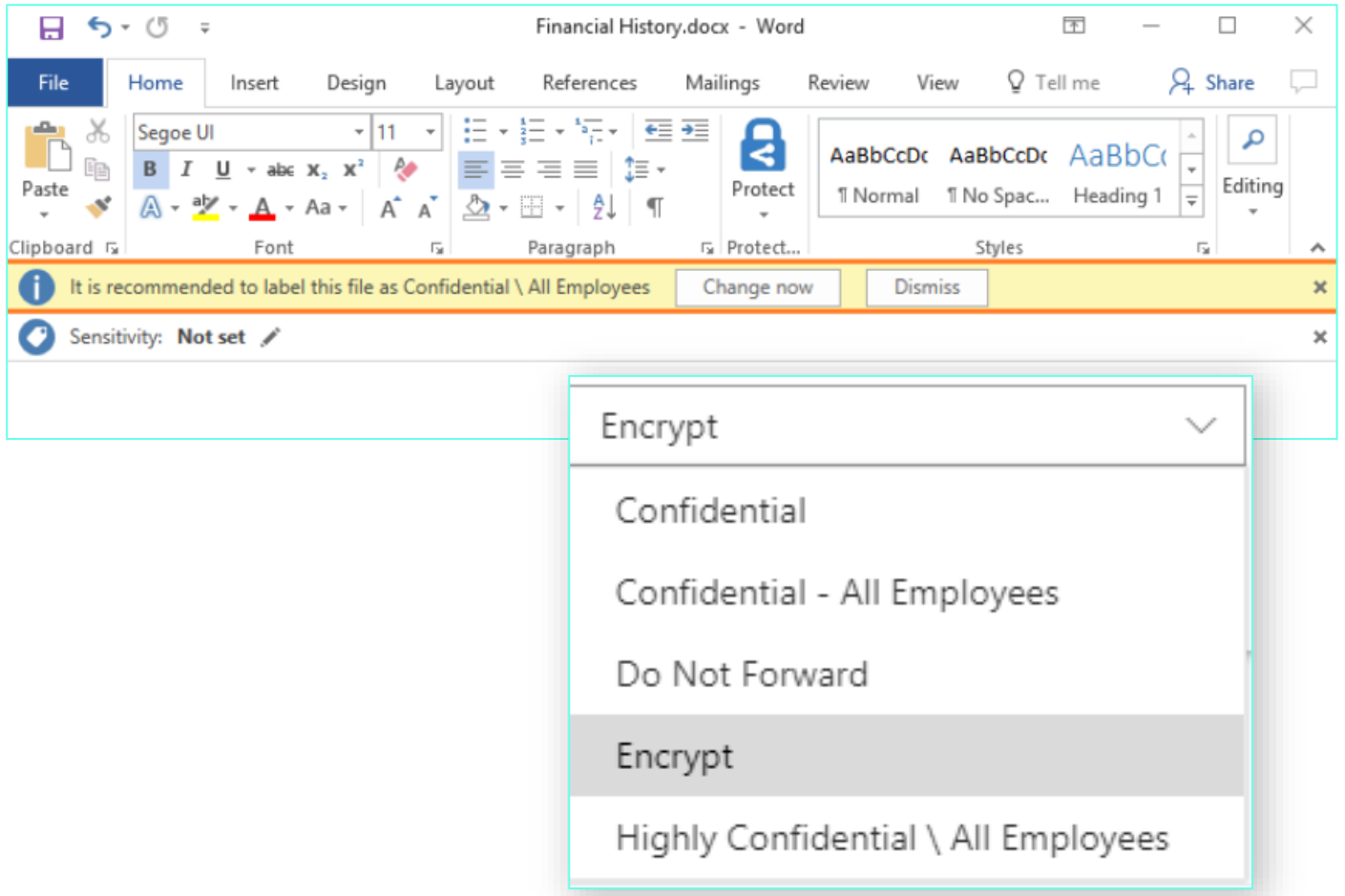
You can control whether a document can edited, printed, or viewed by non-employees. You can also revoke access.



Microsoft Information Protection (MIP)

What it is:

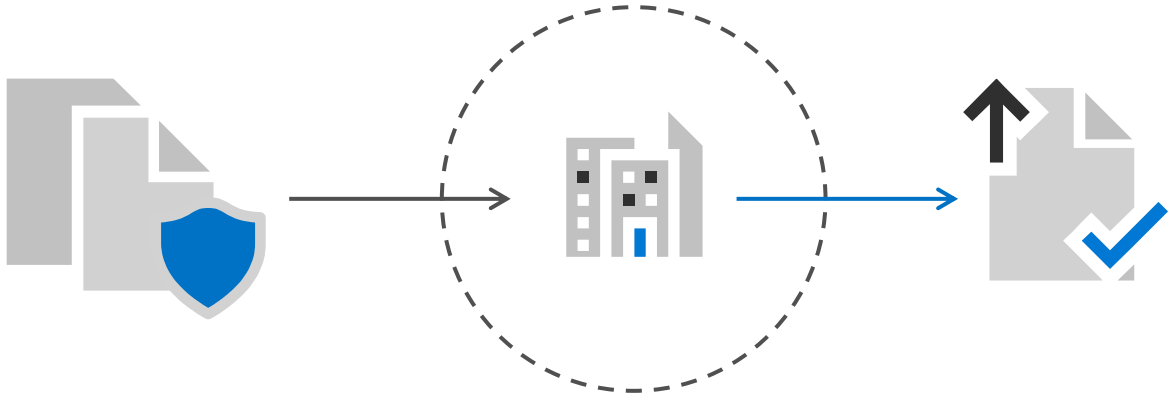
Microsoft Information Protection helps an organization to classify protect its documents and emails, either by restricting the ability to forward and print, or by applying labels.



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

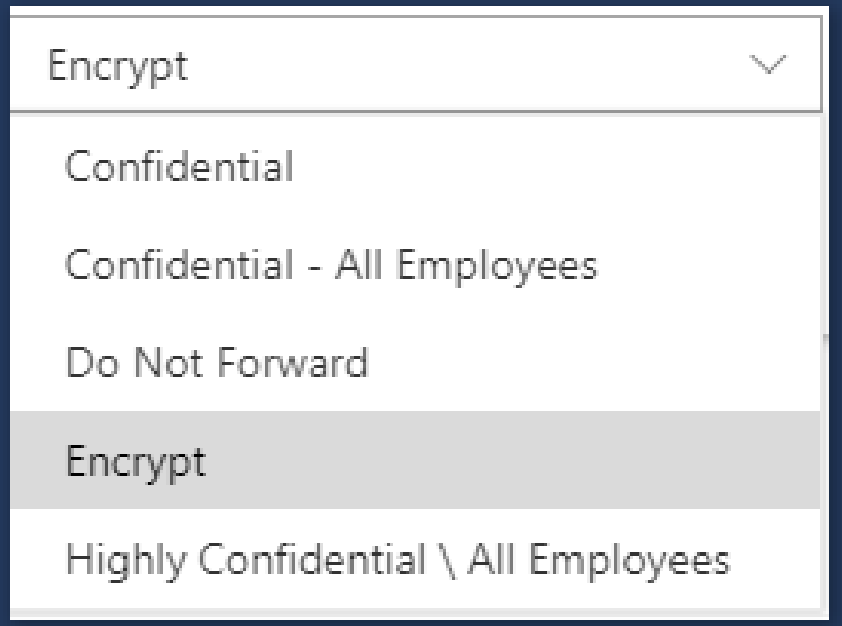
The problem:

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

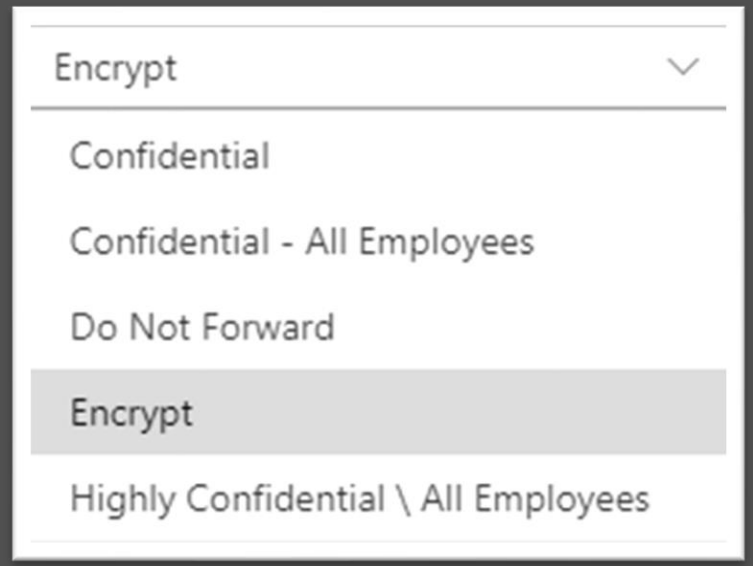
Some examples of how it can be used

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:

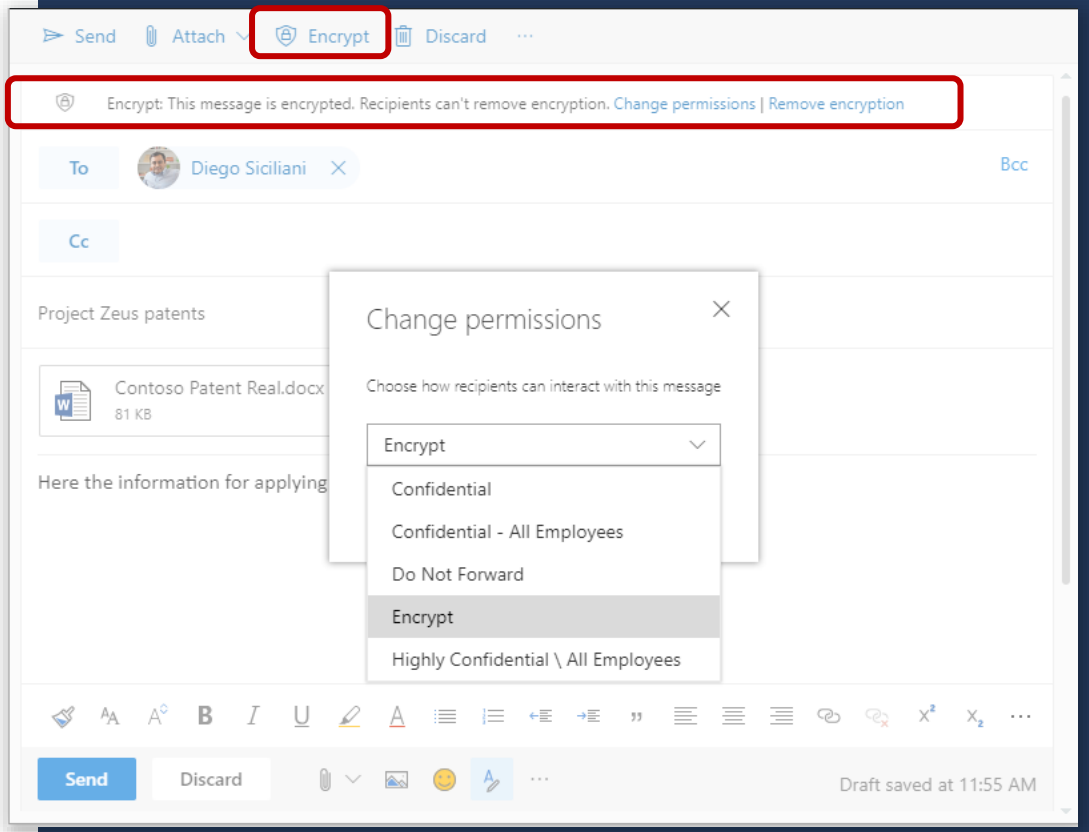
- Select the **Encrypt** button

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



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

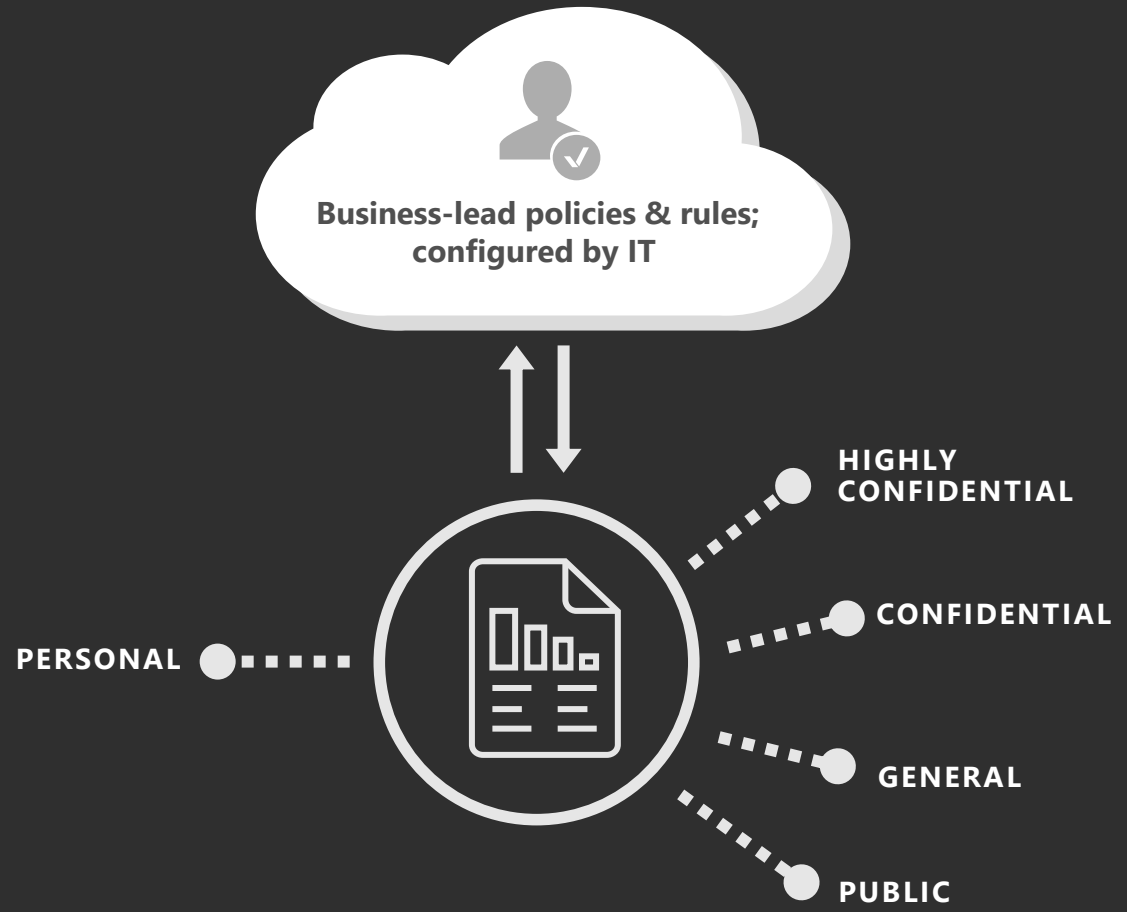
CLASSIFY INFORMATION BASED ON **SENSITIVITY**

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?

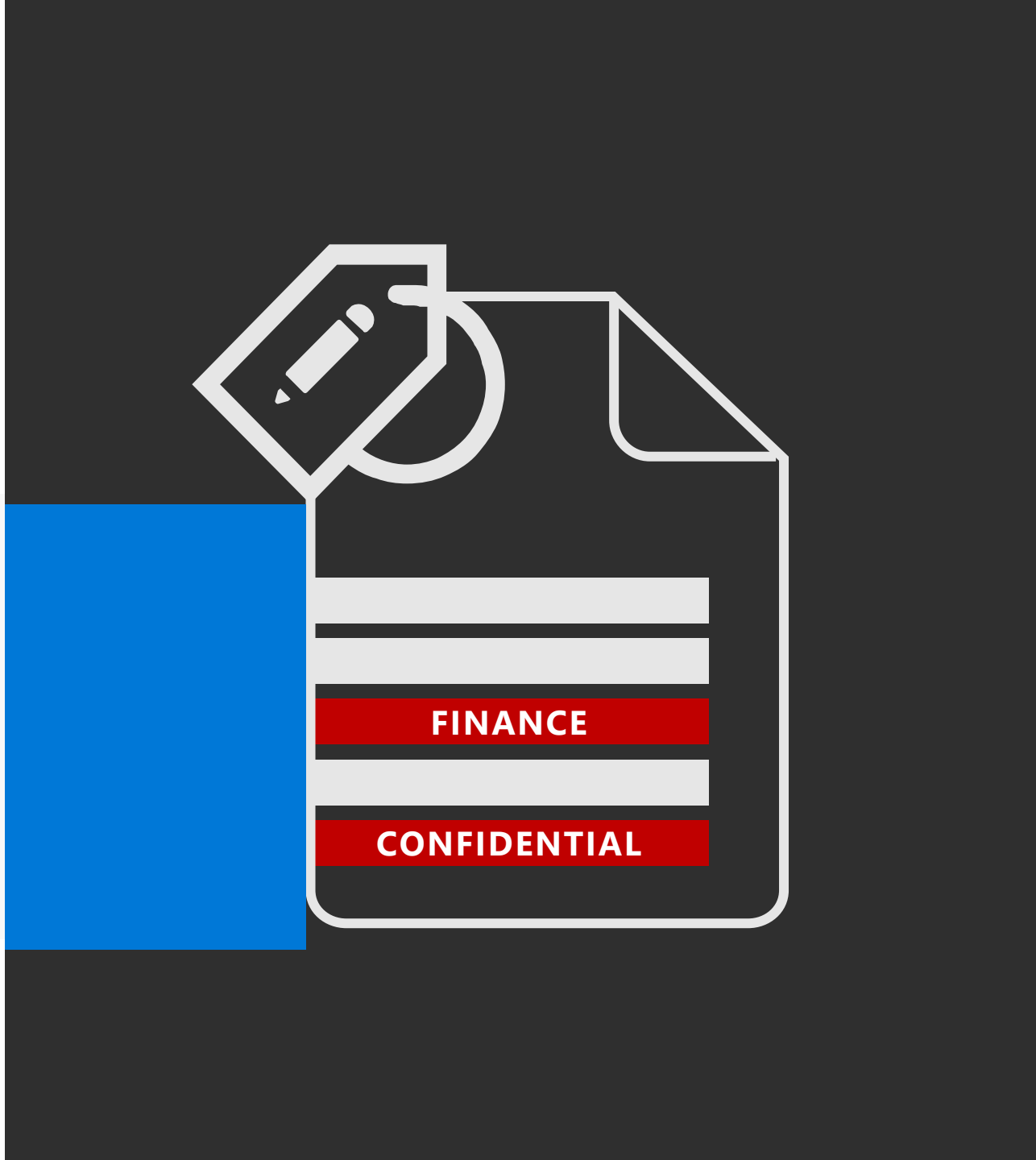
Metadata written into document files

Travels with the document as it moves

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

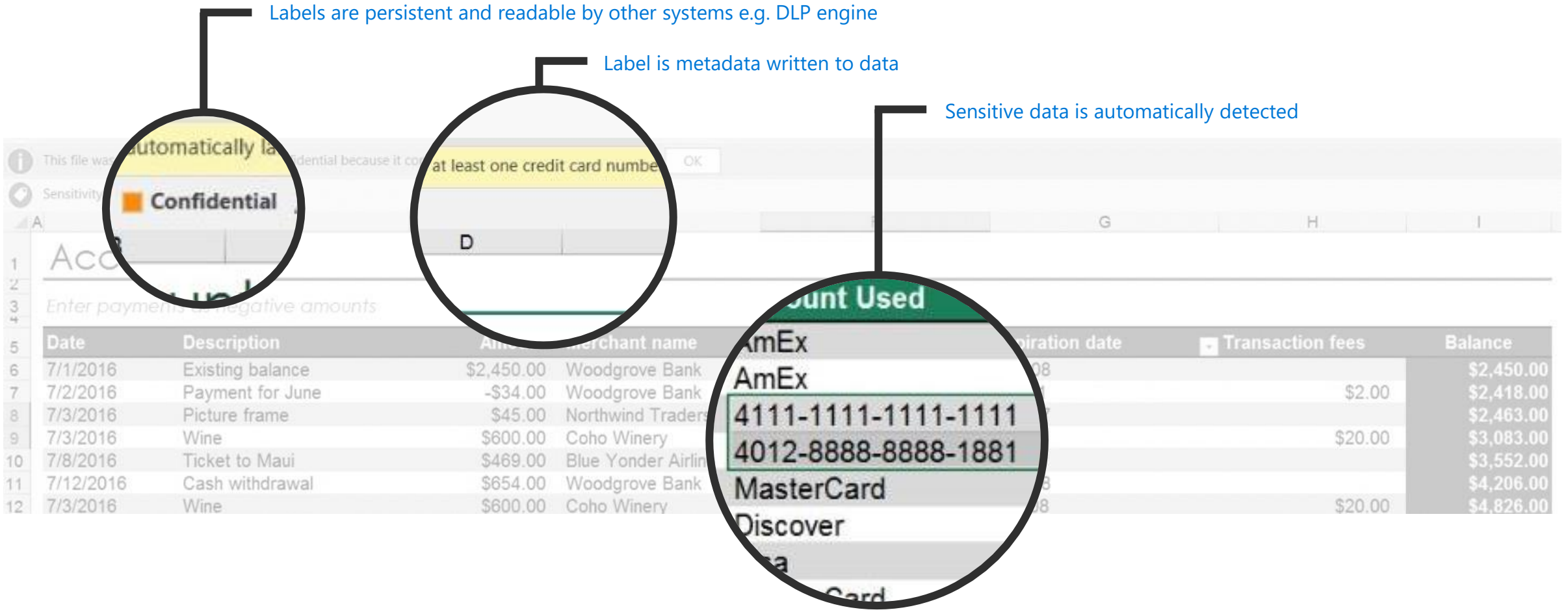
Used for the purpose of apply a protection action or data governance action – determined by policy

Can be customized per the organization's needs



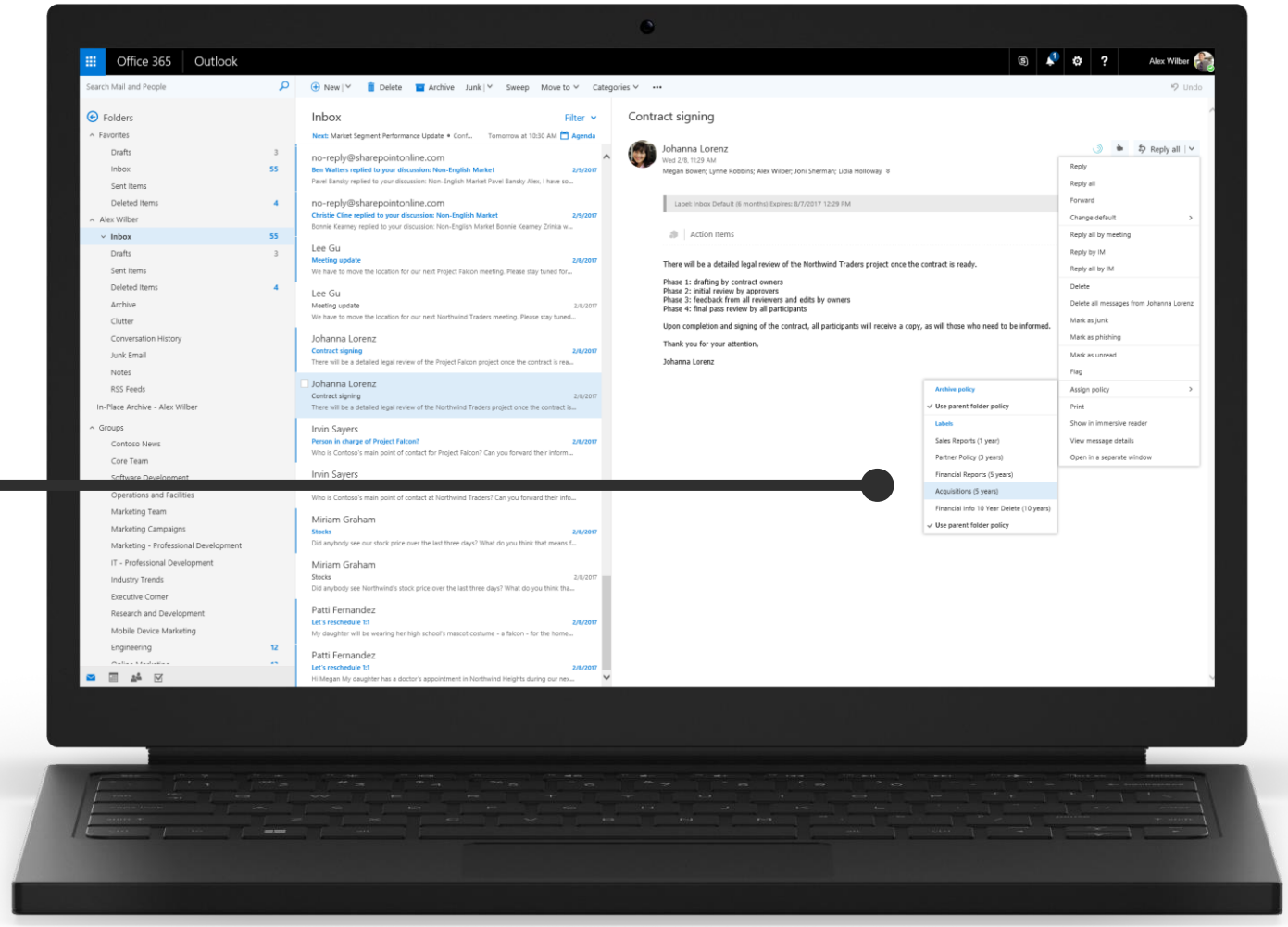
CLASSIFICATION & LABELING EXAMPLE – **SENSITIVE DATA**

Discover personal data and apply persistent labels



CLASSIFICATION & LABELING EXAMPLE – **DATA GOVERNANCE**

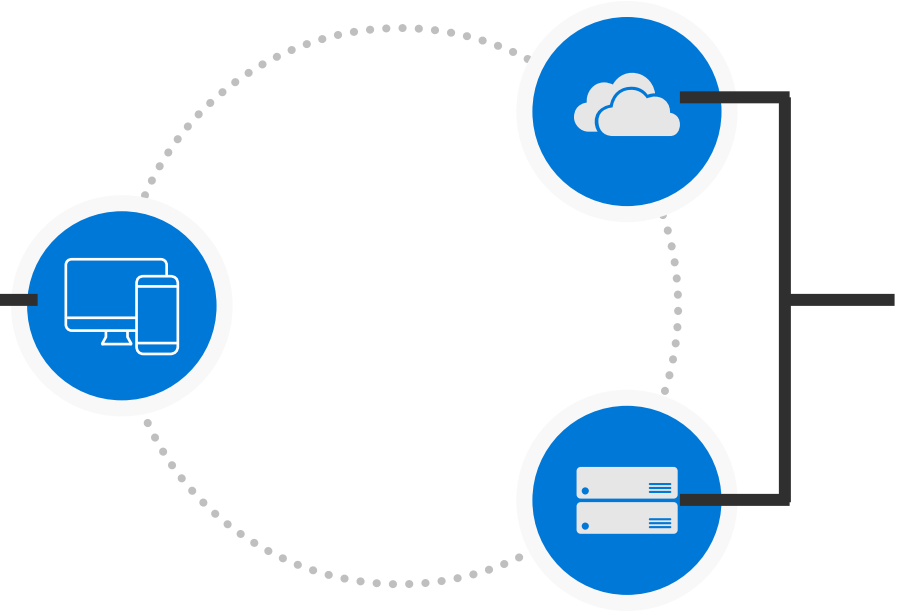
Labeling can be end-user driven
or automatically applied



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.

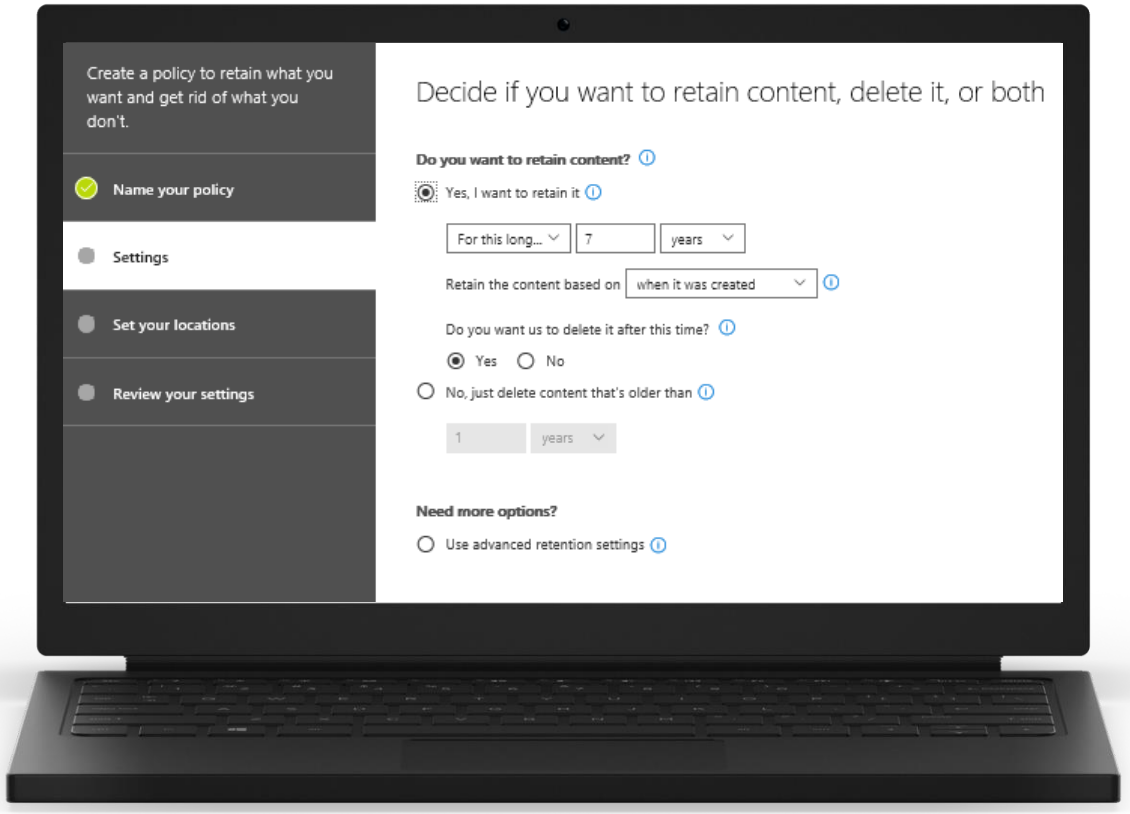
( ) **Only delete items when they reach a certain age**
Items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

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