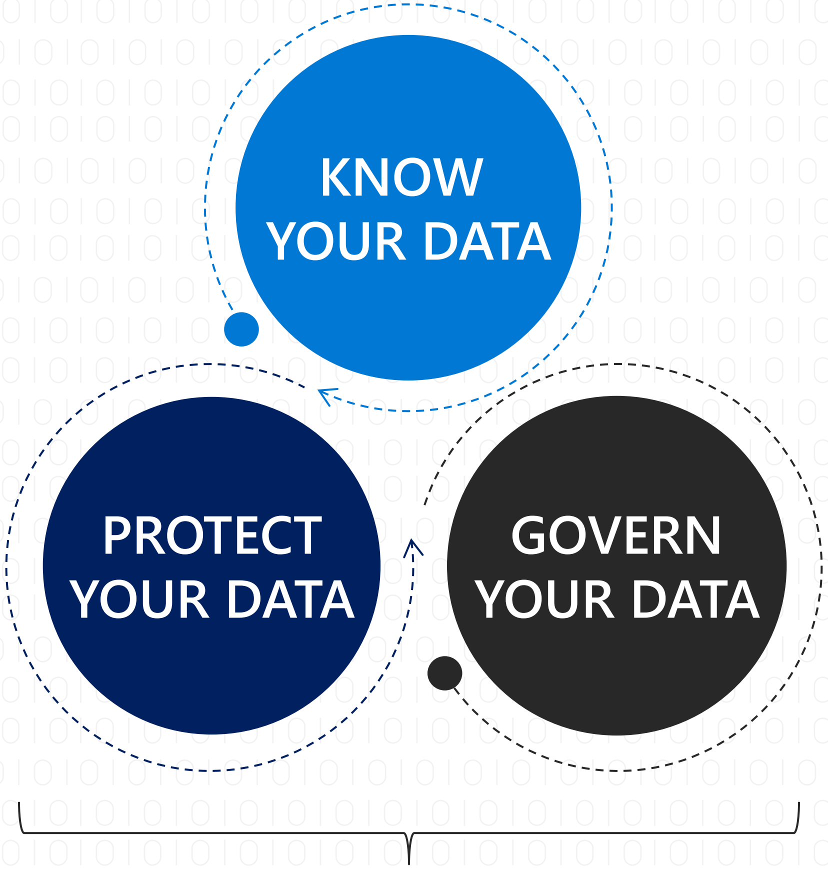
Information Protection & Governance

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

Understand your data landscape and identify important data across your hybrid environment



KNOW YOUR DATA

PROTECT YOUR DATA

GOVERN YOUR DATA

Apply flexible protection actions including encryption, visual markings and DLP

Automatically retain, delete, and store data and records in compliant manner

Powered by an intelligent platform

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

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:

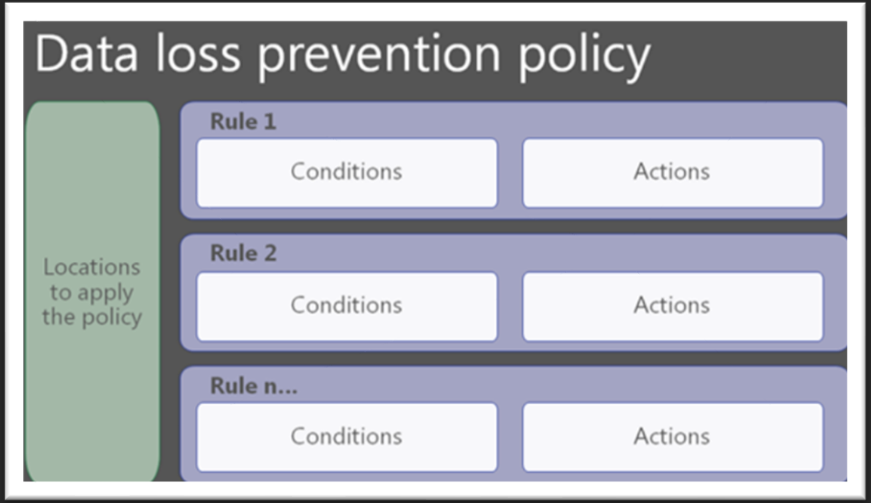
- Identify sensitive information across many locations and apps
- Prevent the accidental sharing of sensitive information
- Monitor and protect sensitive information in the desktop versions of Excel, PowerPoint, and Word
- Help users learn how to stay compliant without interrupting their workflow

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

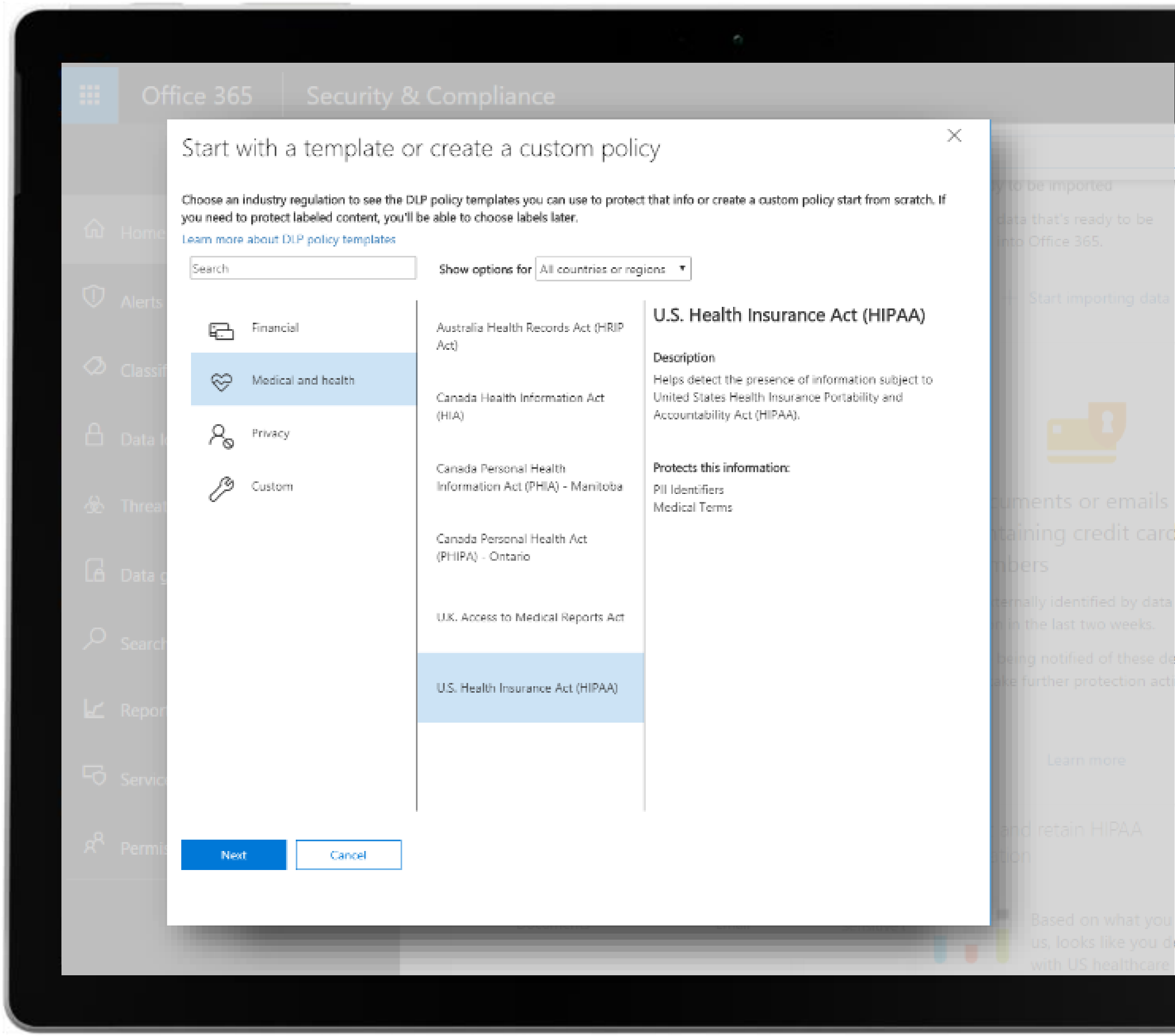
Built-in Policies & Templates

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



Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later.

Learn more about DLP policy templates

Search

Show options for: All countries or regions

- Financial
- Medical and health
- Privacy
- Custom

- Australia Health Records Act (HRIP Act)
- Canada Health Information Act (HIA)
- Canada Personal Health Information Act (PHIA) - Manitoba
- Canada Personal Health Act (PHIPA) - Ontario
- U.K. Access to Medical Reports Act
- U.S. Health Insurance Act (HIPAA)

U.S. Health Insurance Act (HIPAA)

Description

Helps detect the presence of information subject to United States Health Insurance Portability and Accountability Act (HIPAA).

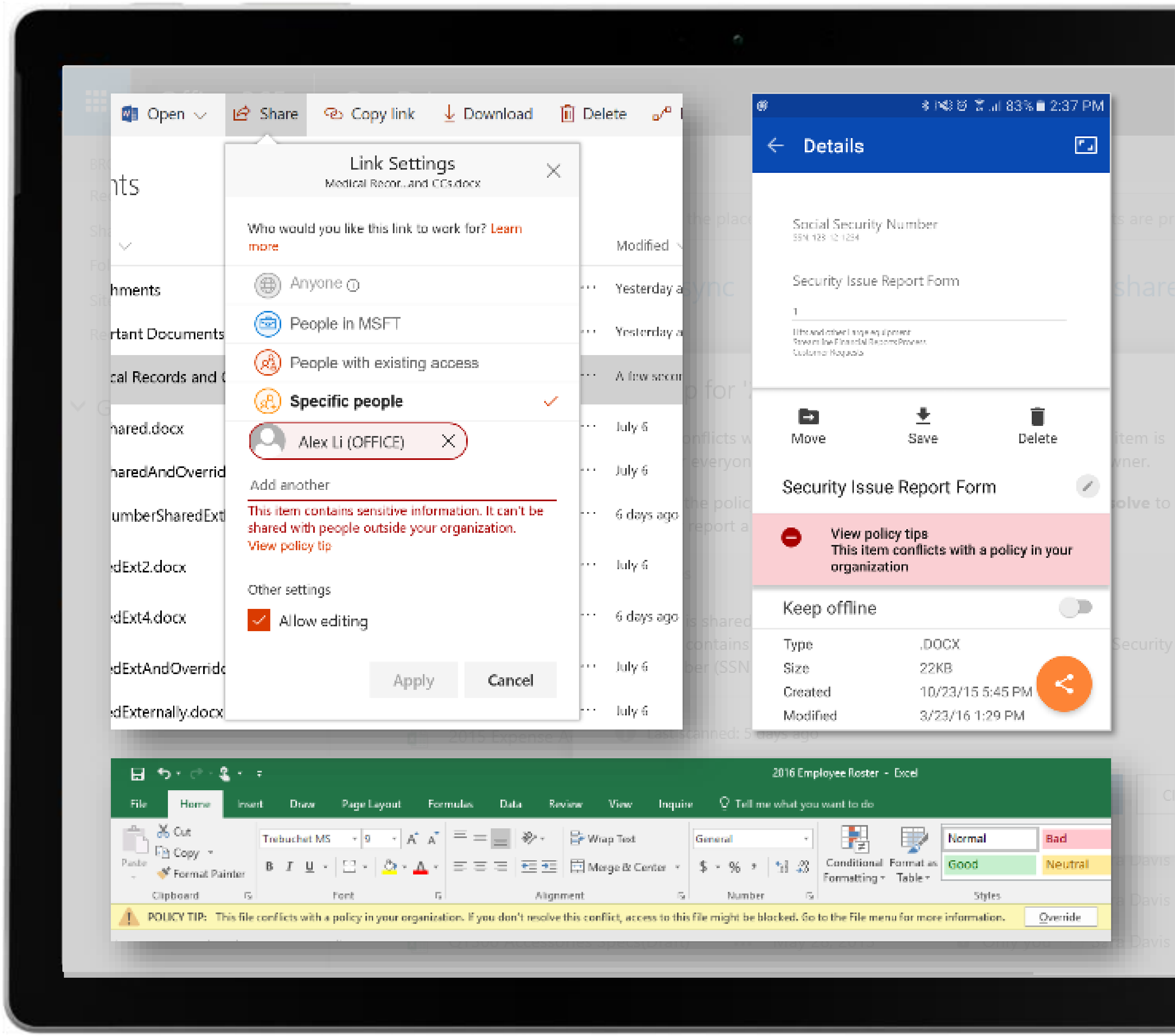
Protects this information:

PII Identifiers
Medical Terms

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.



Who would you like this link to work for? Learn more

This item contains sensitive information. It can't be shared with people outside your organization. View policy tip

☑ Allow editing

Social Security Number

Security Issue Report Form

View policy tips
This item conflicts with a policy in your organization

Type	.DOCX
Size	22KB
Created	10/23/15 5:45 PM
Modified	3/23/16 1:29 PM

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.

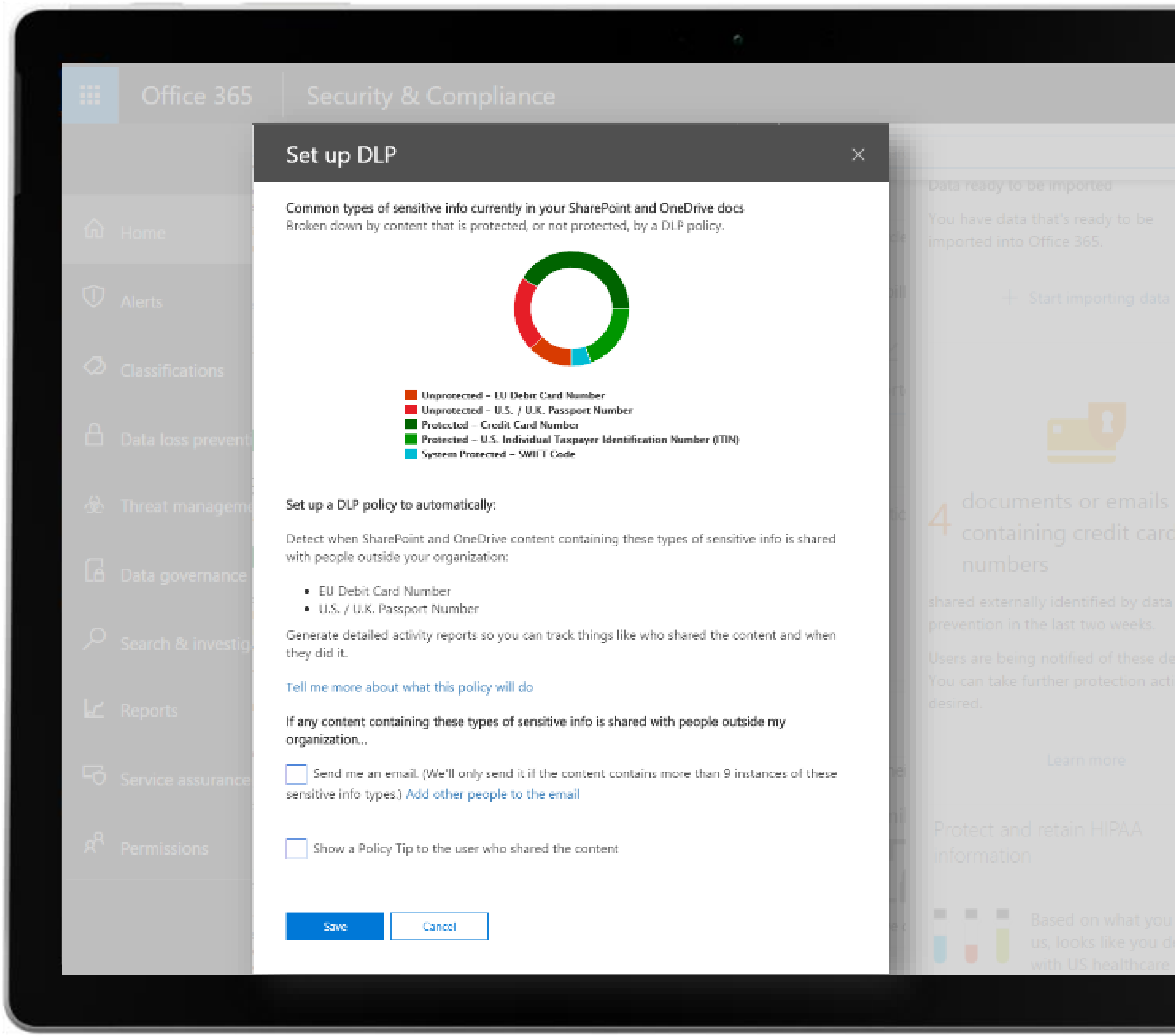
Usage-driven recommendations

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


Office 365
Security & Compliance
Home
Alerts
Classifications
Data loss prevent
Threat managem
Data governance
Search & investig
Reports
Service assurance
Permissions
Data ready to be imported
You have data that's ready to be imported into Office 365.
+ Start importing data
4 documents or emails containing credit card numbers
shared externally identified by data prevention in the last two weeks.
Users are being notified of these de You can take further protection acti desired.
Learn more
Protect and retain HIPAA information
Based on what you us, looks like you d with US healthcare

Set up DLP

×

Common types of sensitive info currently in your SharePoint and OneDrive docs
Broken down by content that is protected, or not protected, by a DLP policy.

- 🟥 Unprotected – EU Debit Card Number
- 🟥 Unprotected – U.S. / U.K. Passport Number
- 🟩 Protected – Credit Card Number
- 🟩 Protected – U.S. Individual Taxpayer Identification Number (ITIN)
- 🟦 System Protected – SWIFT Code

Set up a DLP policy to automatically:

Detect when SharePoint and OneDrive content containing these types of sensitive info is shared with people outside your organization:

- EU Debit Card Number
- U.S. / U.K. Passport Number

Generate detailed activity reports so you can track things like who shared the content and when they did it.

Tell me more about what this policy will do

If any content containing these types of sensitive info is shared with people outside my organization...

□ Send me an email. (We'll only send it if the content contains more than 9 instances of these sensitive info types.) Add other people to the email

□ Show a Policy Tip to the user who shared the content

Save Cancel

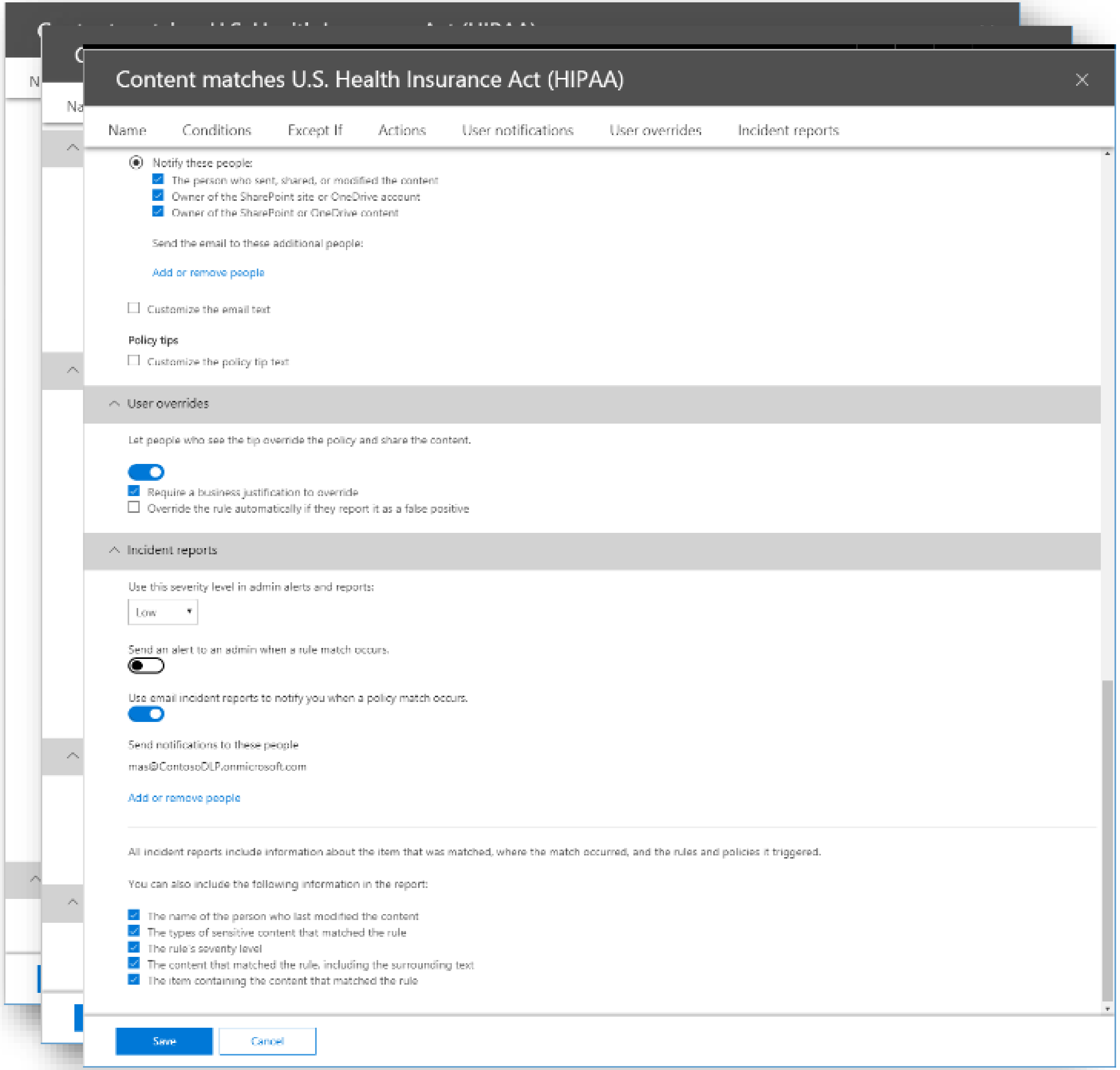
Rich customization

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



Content matches U.S. Health Insurance Act (HIPAA)

● 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

□ Customize the policy tip text

User overrides

Let people who see the tip override the policy and share the content.

☑ Require a business justification to override

□ Override the rule automatically if they report it as a false positive

Incident reports

Use this severity level in admin alerts and reports:

Low

Send an alert to an admin when a rule match occurs.

Use email incident reports to notify you when a policy match occurs.

Send notifications to these people

mas@ContosoDLP.onmicrosoft.com

Add or remove people

All incident reports include information about the item that was matched, where the match occurred, and the rules and policies it triggered.

You can also include the following information in the report:

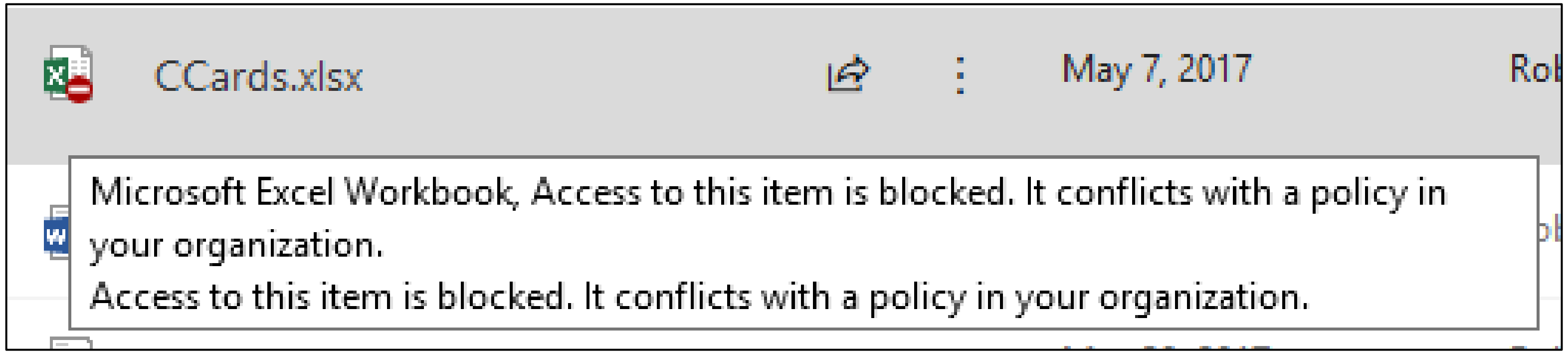
☑ The name of the person who last modified the content

☑ The types of sensitive content that matched the rule

☑ The rule's severity level

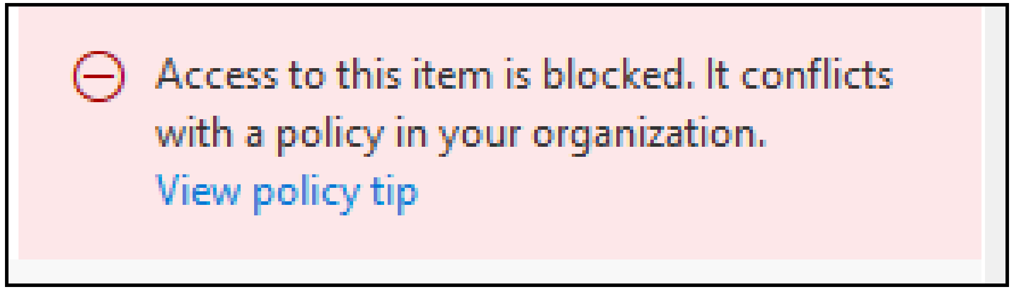
☑ The content that matched the rule, including the surrounding text

☑ The item containing the content that matched the rule

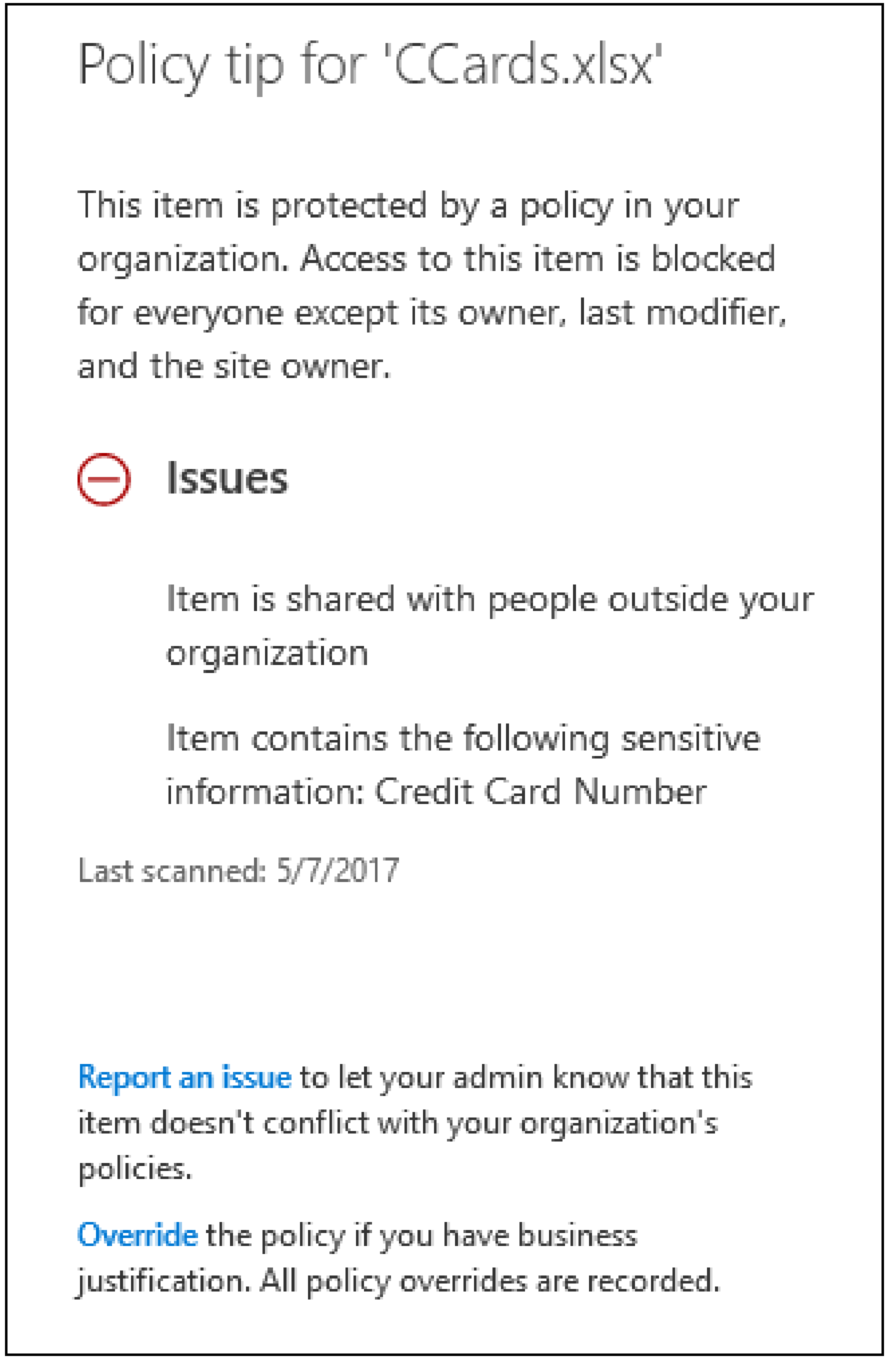


CCards.xlsx May 7, 2017 Rob

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.

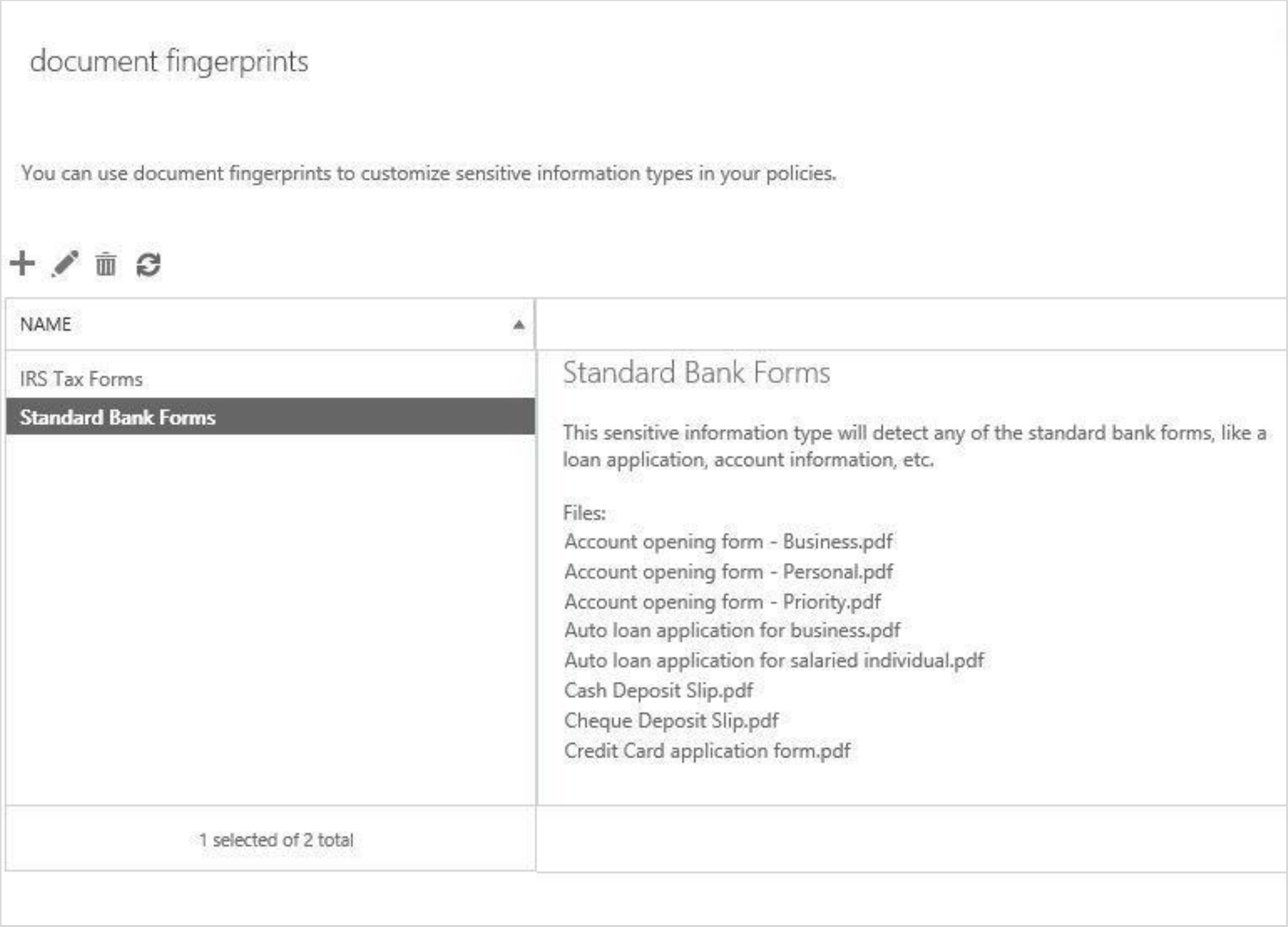
DLP document fingerprinting

* **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



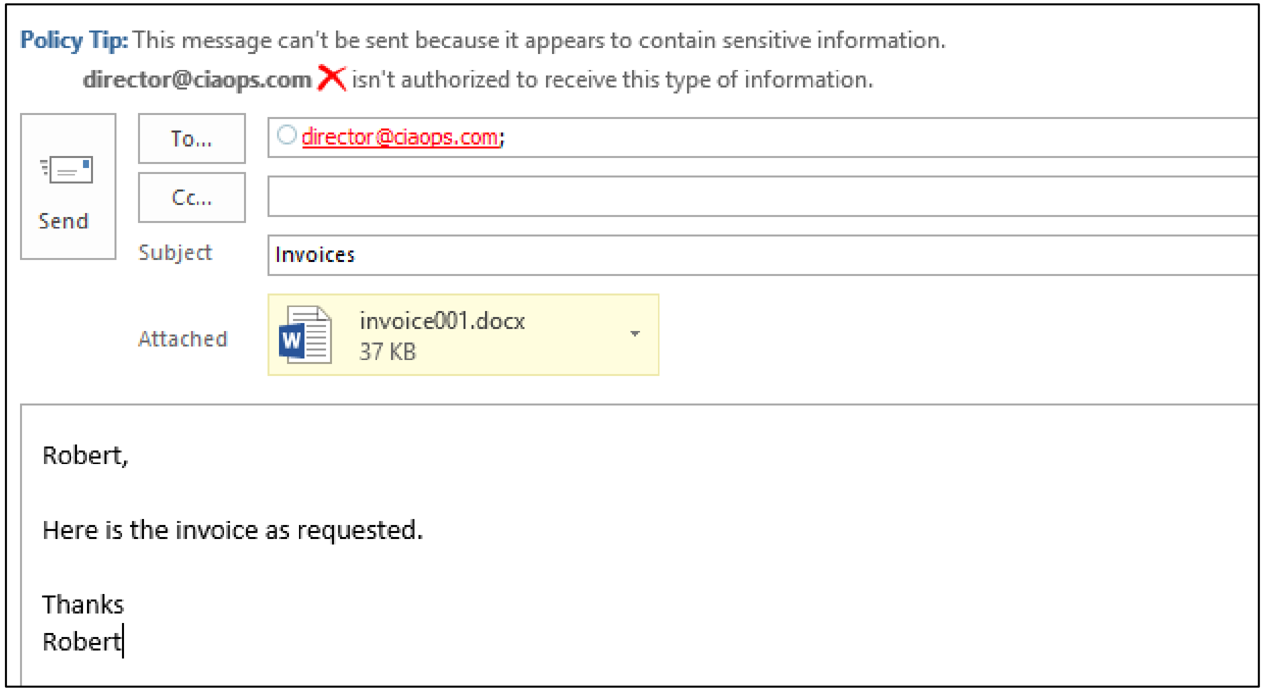
document fingerprints

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

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



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.

To... director@ciaops.com;

Cc...

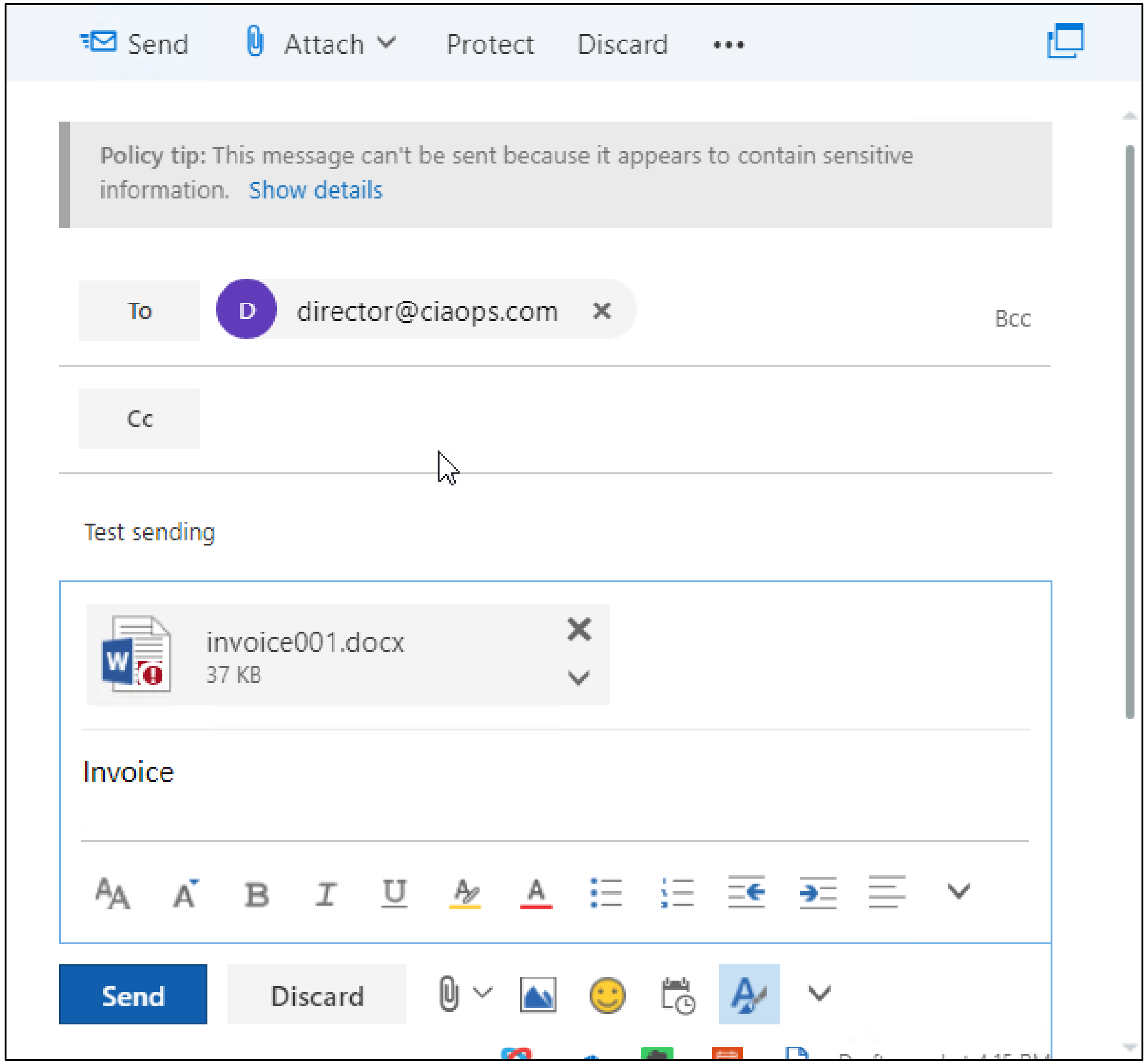
Subject: Invoices

Attached: invoice001.docx 37 KB

Robert,

Here is the invoice as requested.

Thanks
Robert



Policy tip: This message can't be sent because it appears to contain sensitive information. Show details

To: D director@ciaops.com

Cc

Bcc

Test sending

invoice001.docx 37 KB

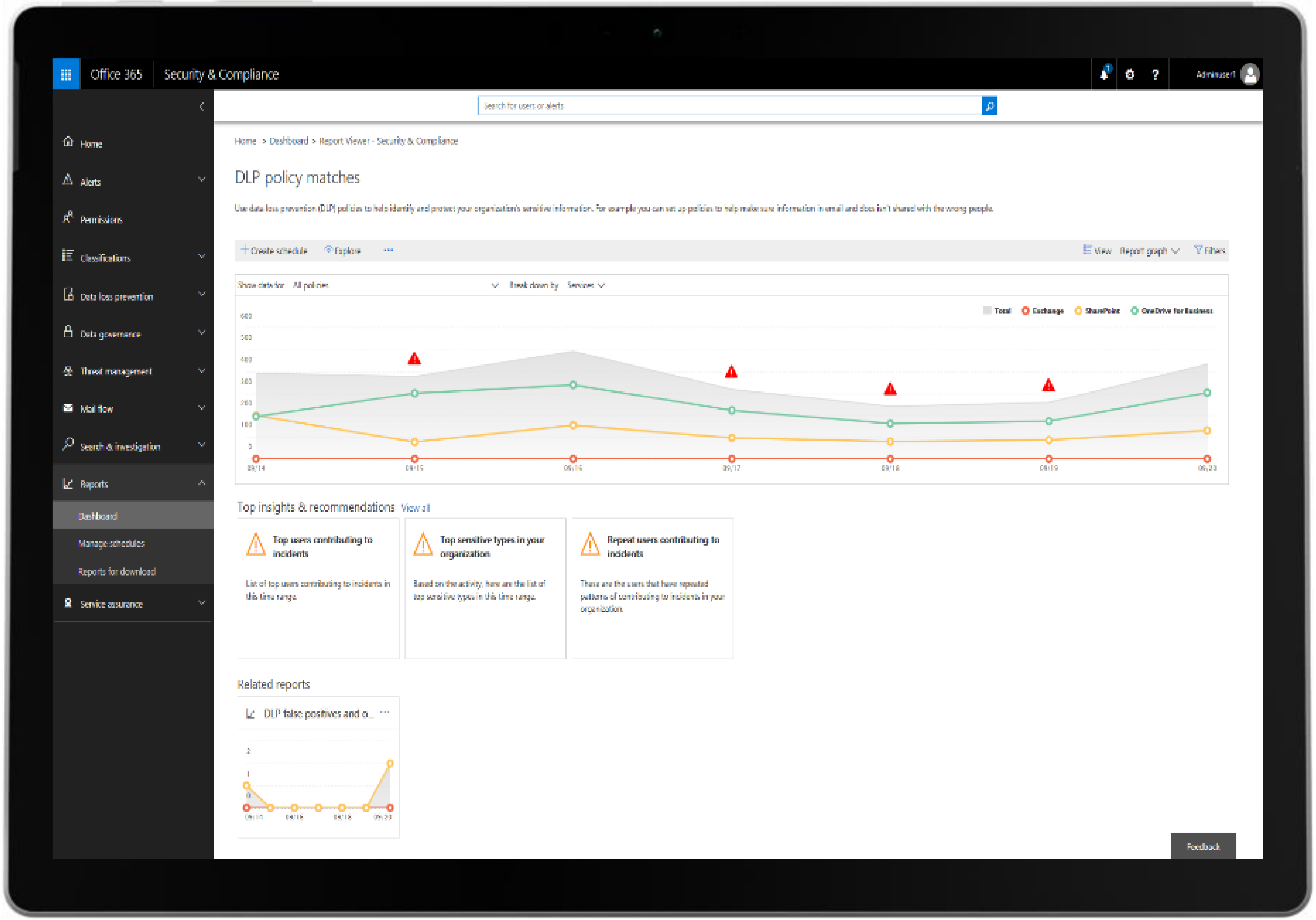
Invoice

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



DLP policy matches

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

Top insights & recommendations

Top users contributing to incidents

List of top users contributing to incidents in this time range.

Top sensitive types in your organization

Based on the activity, here are the list of top sensitive types in this time range.

Repeat users contributing to incidents

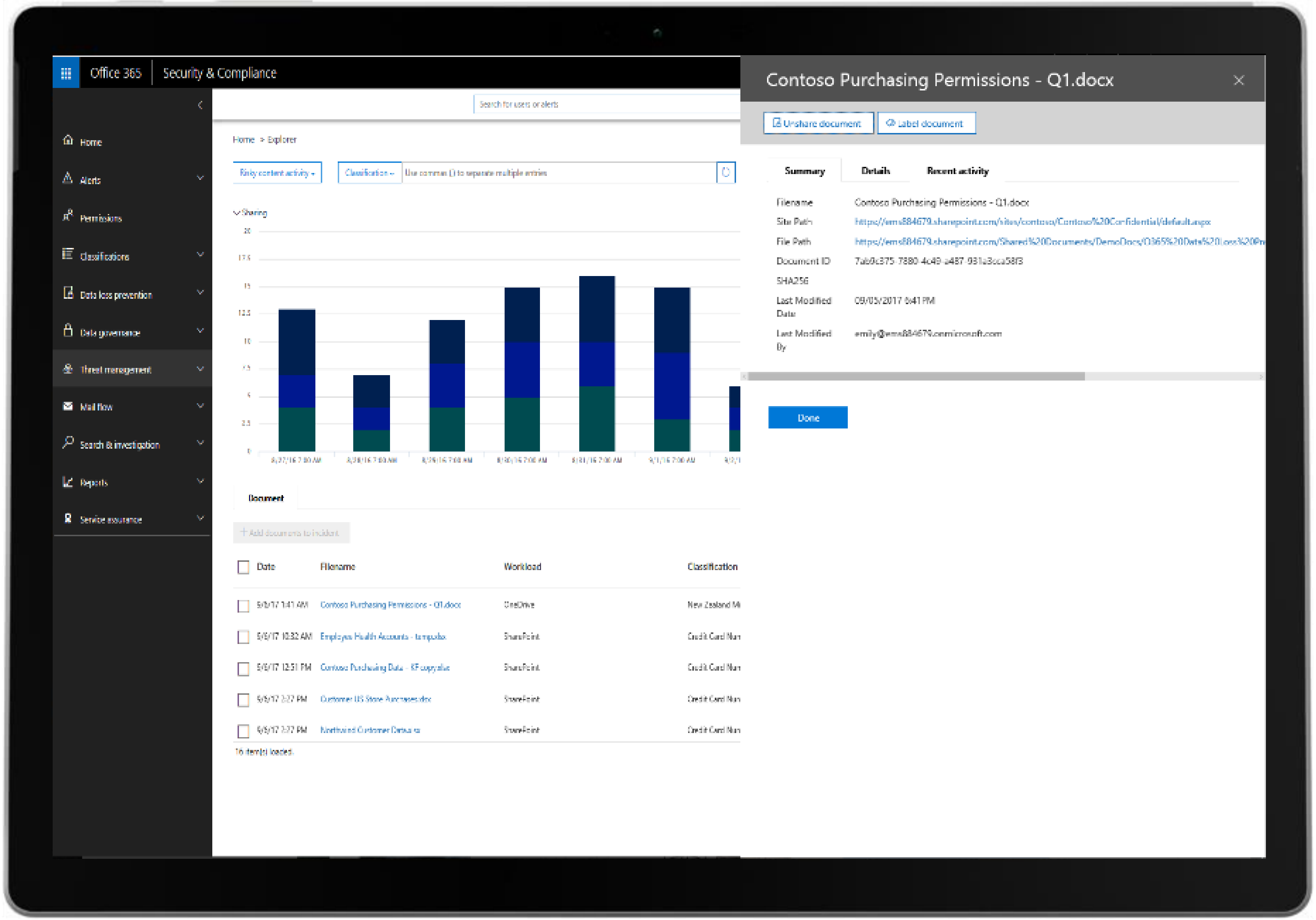
These are the users that have repeated patterns of contributing to incidents in your organization.

Related reports

Investigate and **Remediate**

Investigate policy violation in your organization

Take remediation steps for documents to prevent further risk



□ Date	Filename	Workload	Classification
□ 5/8/17 1:41 AM	Contoso Purchasing Permissions - Q1.docx	OneDrive	New Zealand Mi
□ 5/6/17 10:32 AM	Employee Health Accounts - template	SharePoint	Credit Card Nun
□ 5/6/17 12:51 PM	Contoso Purchasing Data - KF copy.xlsx	SharePoint	Credit Card Nun
□ 5/5/17 2:27 PM	Customer US Store Purchases.docx	SharePoint	Credit Card Nun
□ 5/5/17 2:27 PM	Northwind Customer Data.csv	SharePoint	Credit Card Nun

16 item(s) loaded.

Filename	Contoso Purchasing Permissions - Q1.docx
Site Path	https://ems884679.sharepoint.com/sites/contoso/Contoso%20Confidential/default.aspx
File Path	https://ems884679.sharepoint.com/Shared%20Documents/DemoDocs/O365%20Data%20Loss%20Pr
Document ID	7ab0c375-7880-4c49-a487-931a3cca58f3
SHA256	
Last Modified Date	09/05/2017 6:41 PM
Last Modified By	emily@ems884679.onmicrosoft.com

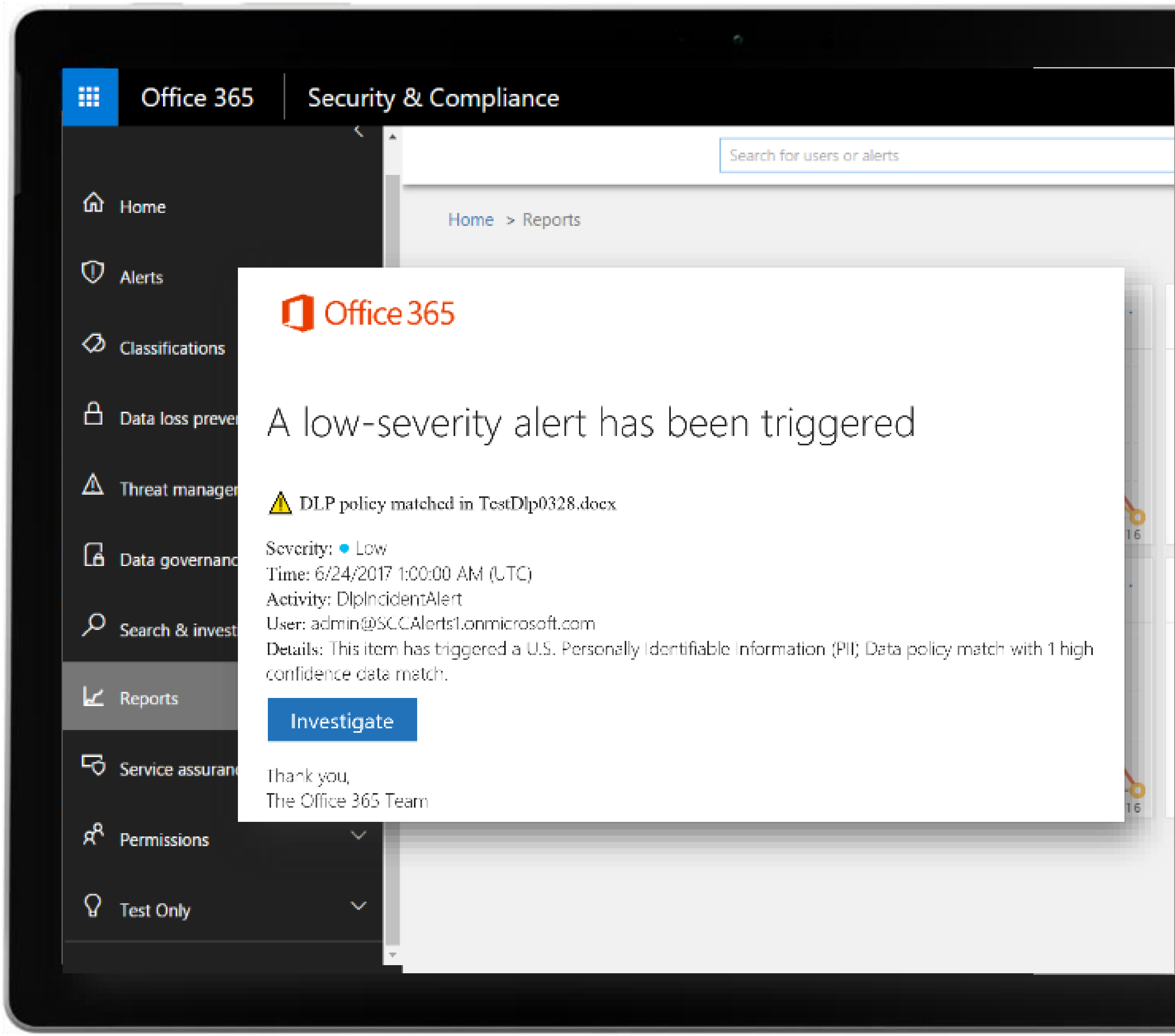
DLP **alerts and notification**

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



Office 365

A low-severity alert has been triggered

⚠ DLP policy matched in TestDlp0328.docx

Severity: ● Low
Time: 6/24/2017 1:00:00 AM (UTC)
Activity: DlpIncidentAlert
User: admin@SCCAlerts1.onmicrosoft.com
Details: This item has triggered a U.S. Personally Identifiable Information (PII) Data policy match with 1 high confidence data match.

Investigate

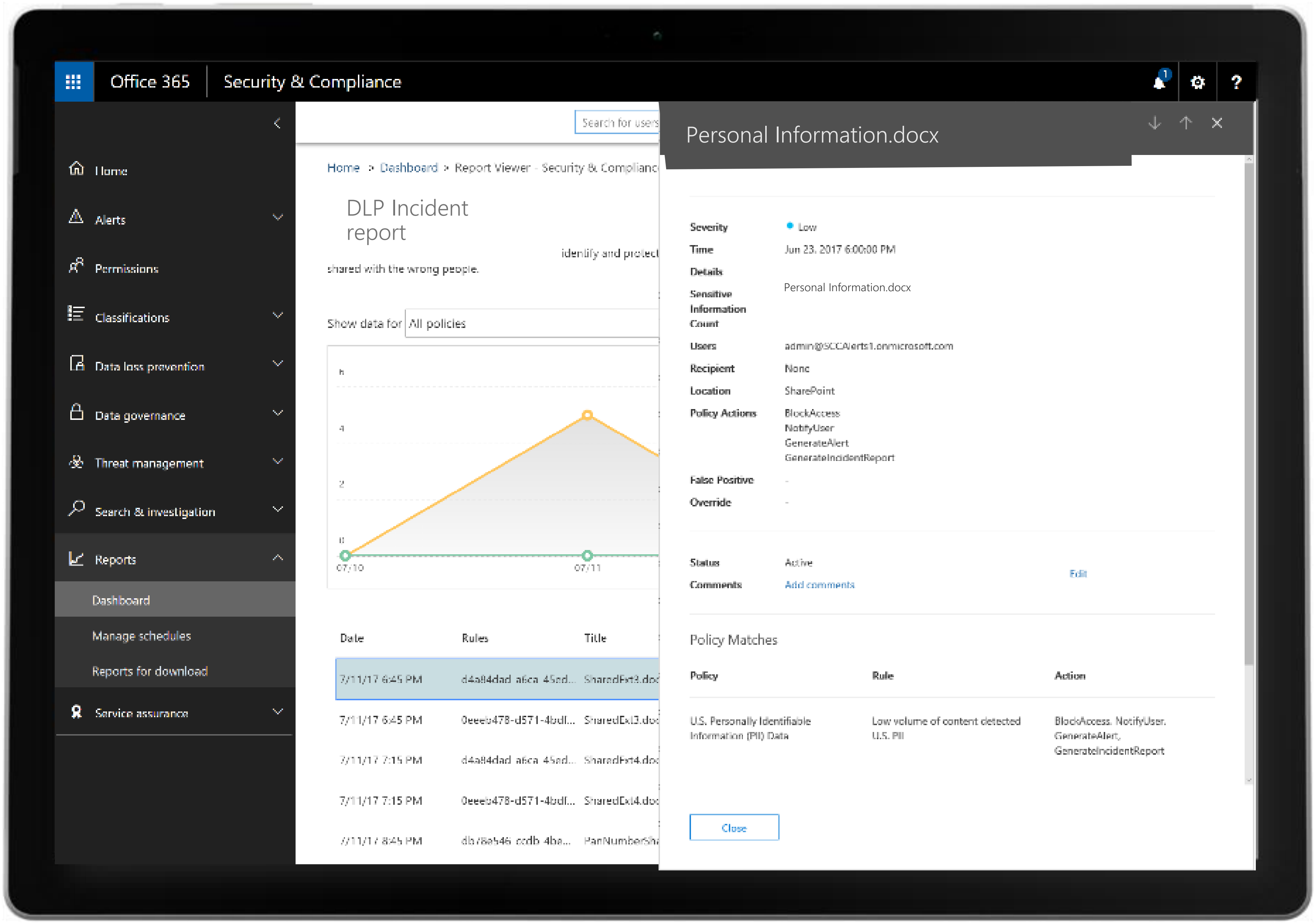
Thank you,
The Office 365 Team

Incident Level View

Complete view of DLP detection for quick assessment of impact

Consolidates applicable policies, rules, detected classifications

Optionally includes sensitive data matches



DLP Incident report

identify and protect

shared with the wrong people.

Show data for All policies

Date	Rules	Title
7/11/17 6:45 PM	d4a84dad a6ca 45ed...	SharedExt3.doc
7/11/17 6:45 PM	0eeeb478-d571-4bdf...	SharedExl3.doc
7/11/17 7:15 PM	d4a84dad a6ca 45ed...	SharedExt4.doc
7/11/17 7:15 PM	0eeeb478-d571-4bdf...	SharedExl4.doc
7/11/17 8:45 PM	db78a546 ccdb 4ba...	PanNumberSha

Personal Information.docx

Severity	● Low
Time	Jun 23, 2017 6:00:00 PM
Details	
Sensitive Information Count	Personal Information.docx
Users	admin@SCCAlerts1.onmicrosoft.com
Recipient	None
Location	SharePoint
Policy Actions	BlockAccess NotifyUser GenerateAlert GenerateIncidentReport
False Positive	-
Override	-

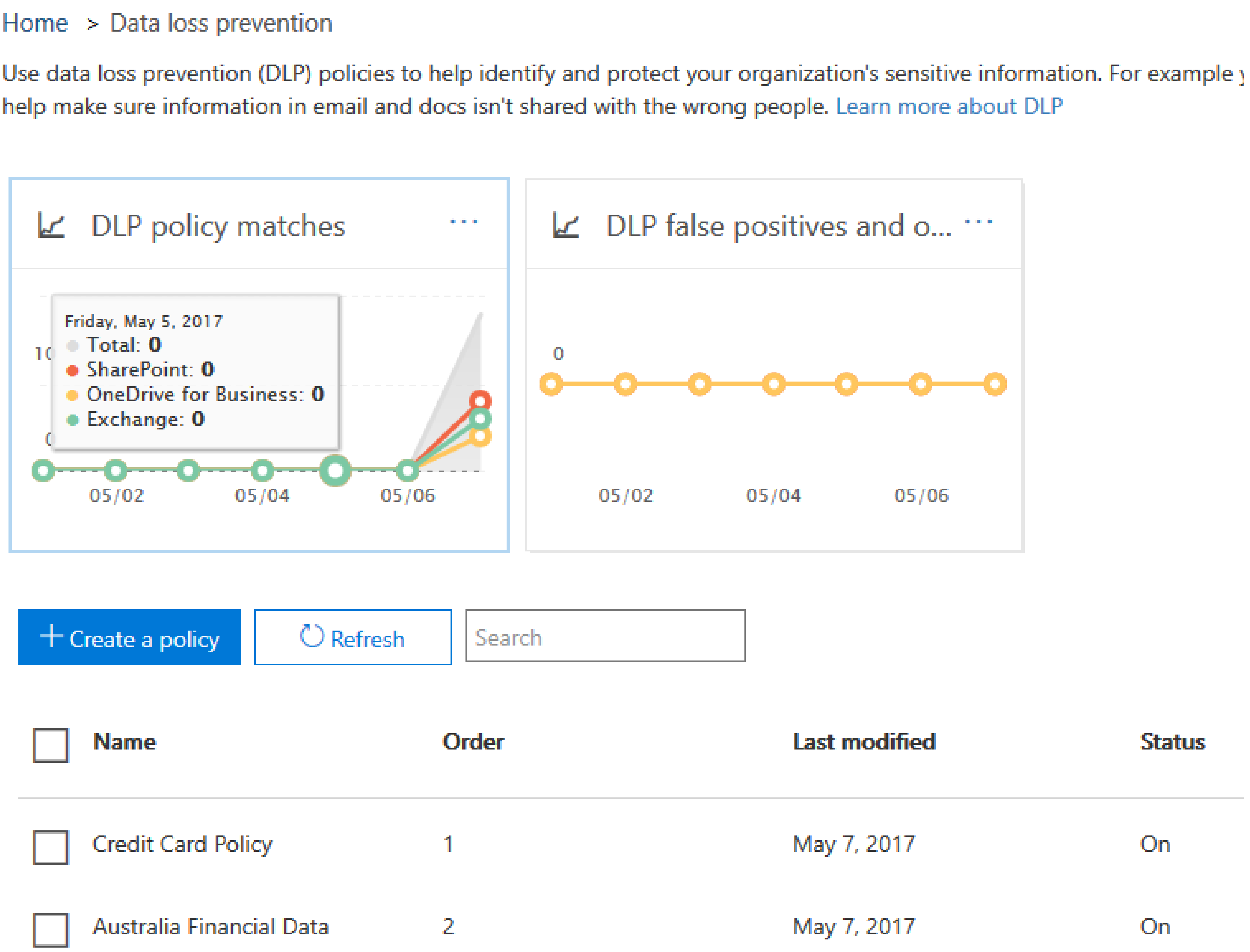
Status	Active
Comments	Add comments

Edit

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



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

DLP policy matches ···

Friday, May 5, 2017
- ● Total: **0**
- ● SharePoint: **0**
- ● OneDrive for Business: **0**
- ● Exchange: **0**

DLP false positives and o... ···

+ 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

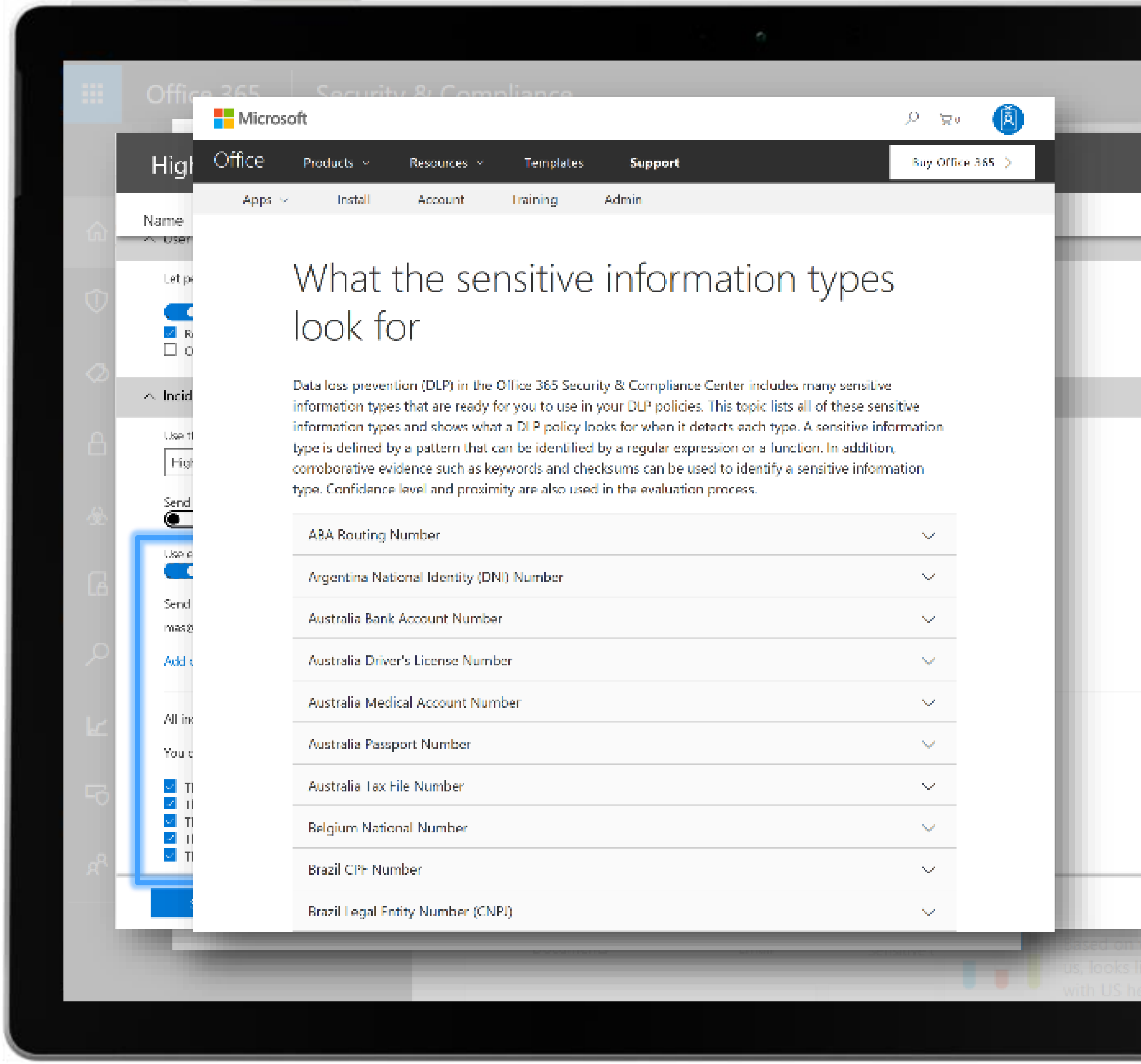
Get started today with templates

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



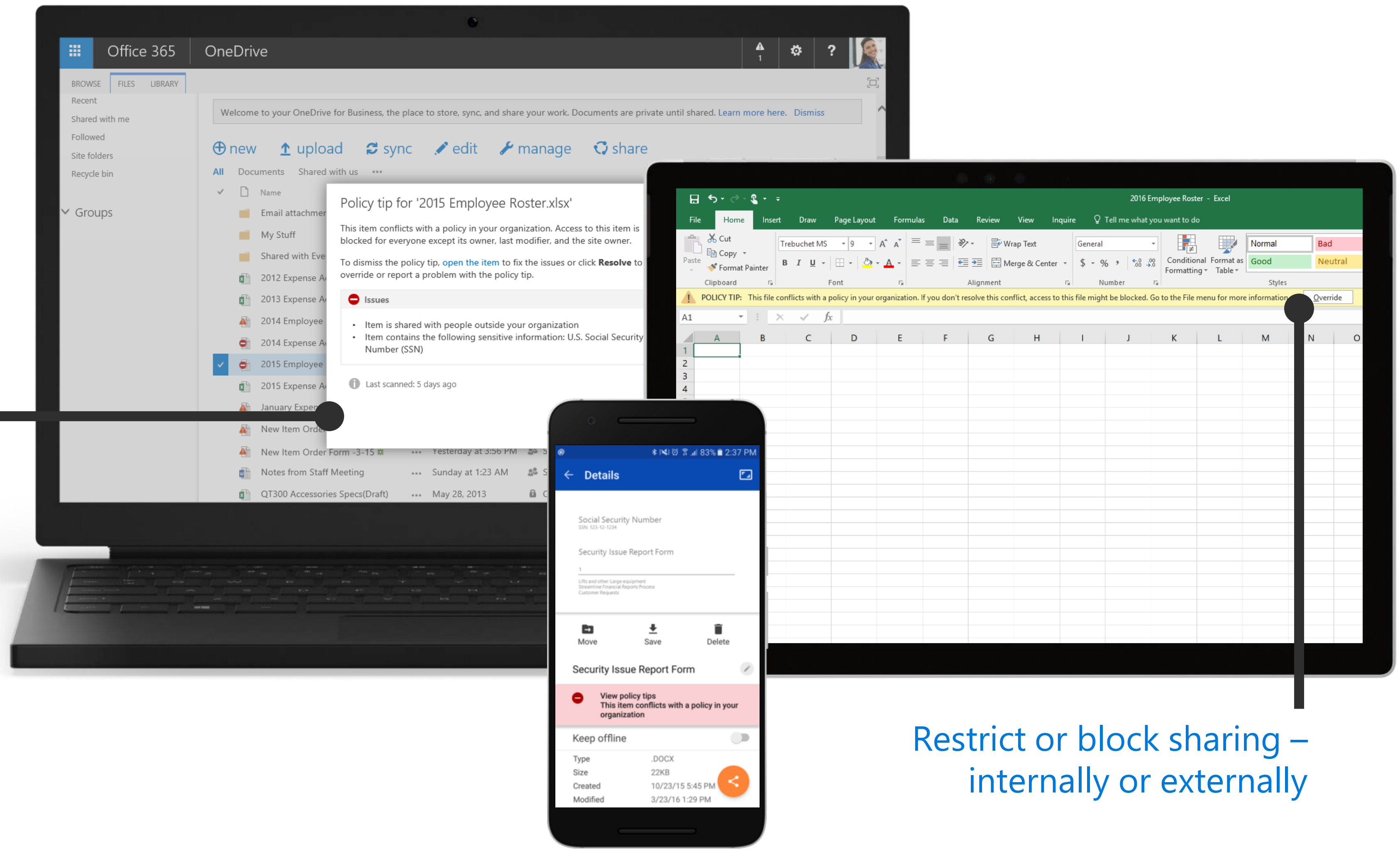
What the sensitive information types look for

Data loss prevention (DLP) in the Office 365 Security & Compliance Center includes many sensitive information types that are ready for you to use in your DLP policies. This topic lists all of these sensitive information types and shows what a DLP policy looks for when it detects each type. A sensitive information type is defined by a pattern that can be identified by a regular expression or a function. In addition, corroborative evidence such as keywords and checksums can be used to identify a sensitive information type. Confidence level and proximity are also used in the evaluation process.

- 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



Welcome to your OneDrive for Business, the place to store, sync, and share your work. Documents are private until shared. Learn more here. Dismiss

Email attachmen
My Stuff
Shared with Eve
2012 Expense A
2013 Expense A
2014 Employee
2014 Expense A
2015 Employee
2015 Expense A
January Expen
New Item Orde
New Item Order Form -3-15 Yesterday at 3:56 PM
Notes from Staff Meeting Sunday at 1:23 AM
QT300 Accessories Specs(Draft) May 28, 2013

Policy tip for '2015 Employee Roster.xlsx'

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.

To dismiss the policy tip, open the item to fix the issues or click **Resolve** to override or report a problem with the policy tip.

Issues

- Item is shared with people outside your organization
- Item contains the following sensitive information: U.S. Social Security Number (SSN)

Last scanned: 5 days ago

2016 Employee Roster - Excel

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. Override

Security Issue Report Form

View policy tips
This item conflicts with a policy in your organization

Keep offline

Type .DOCX
Size 22KB
Created 10/23/15 5:45 PM
Modified 3/23/16 1:29 PM

Policy tips to
warn end users

Restrict or block sharing –
internally or externally