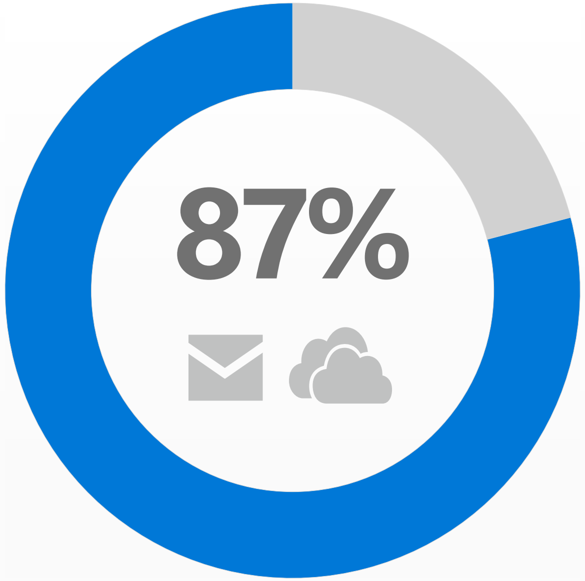
Introduction to

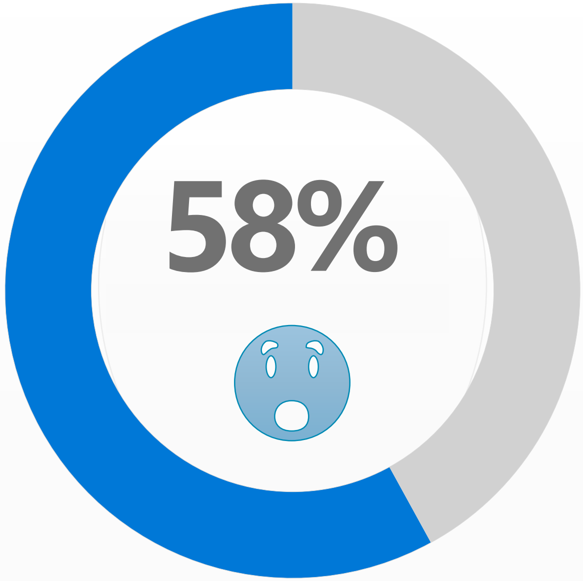
Data Loss Prevention

ignia

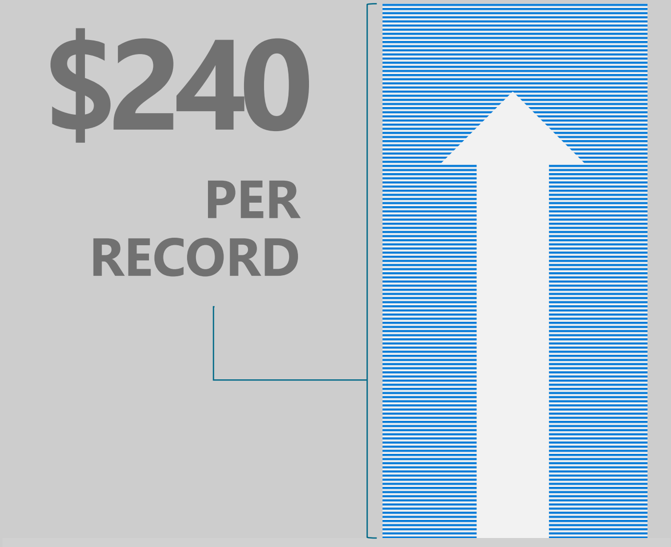
Data Leakage



...of senior managers admit to **regularly** uploading work files to a personal email or cloud account[1]



Have accidentally sent sensitive information to the **wrong person**[1]

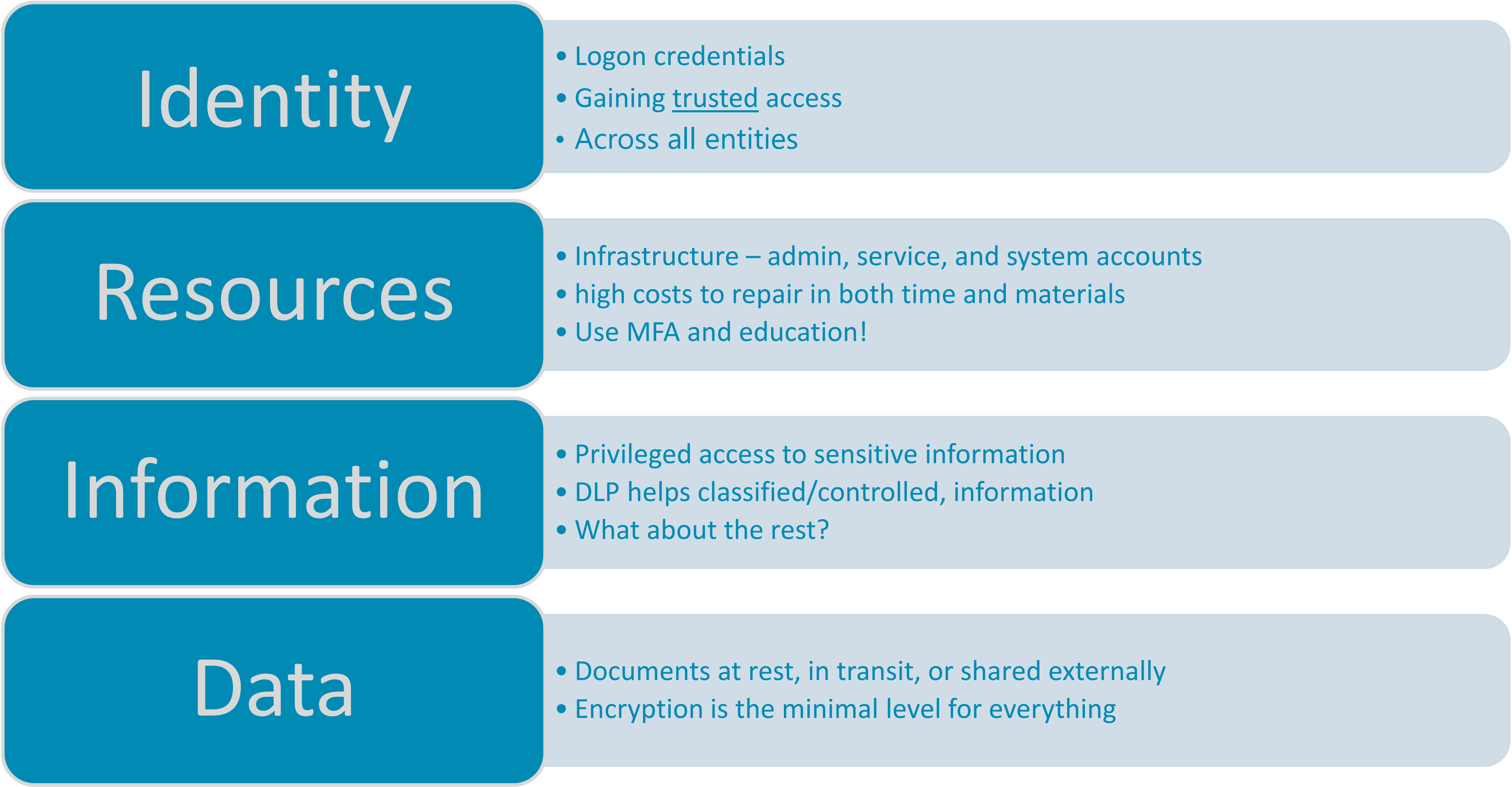


Average per record **cost of a data breach** across all industries[2]

[1] Stroz Friedberg, "On The Pulse: Information Security In American Business," 2013

[2] HIPPA Secure Now, "A look at the cost of healthcare data breaches," Art Gross, March 30, 2012

What needs protecting?



Identity

- Logon credentials
- Gaining trusted access
- Across all entities

Resources

- Infrastructure – admin, service, and system accounts
- high costs to repair in both time and materials
- Use MFA and education!

Information

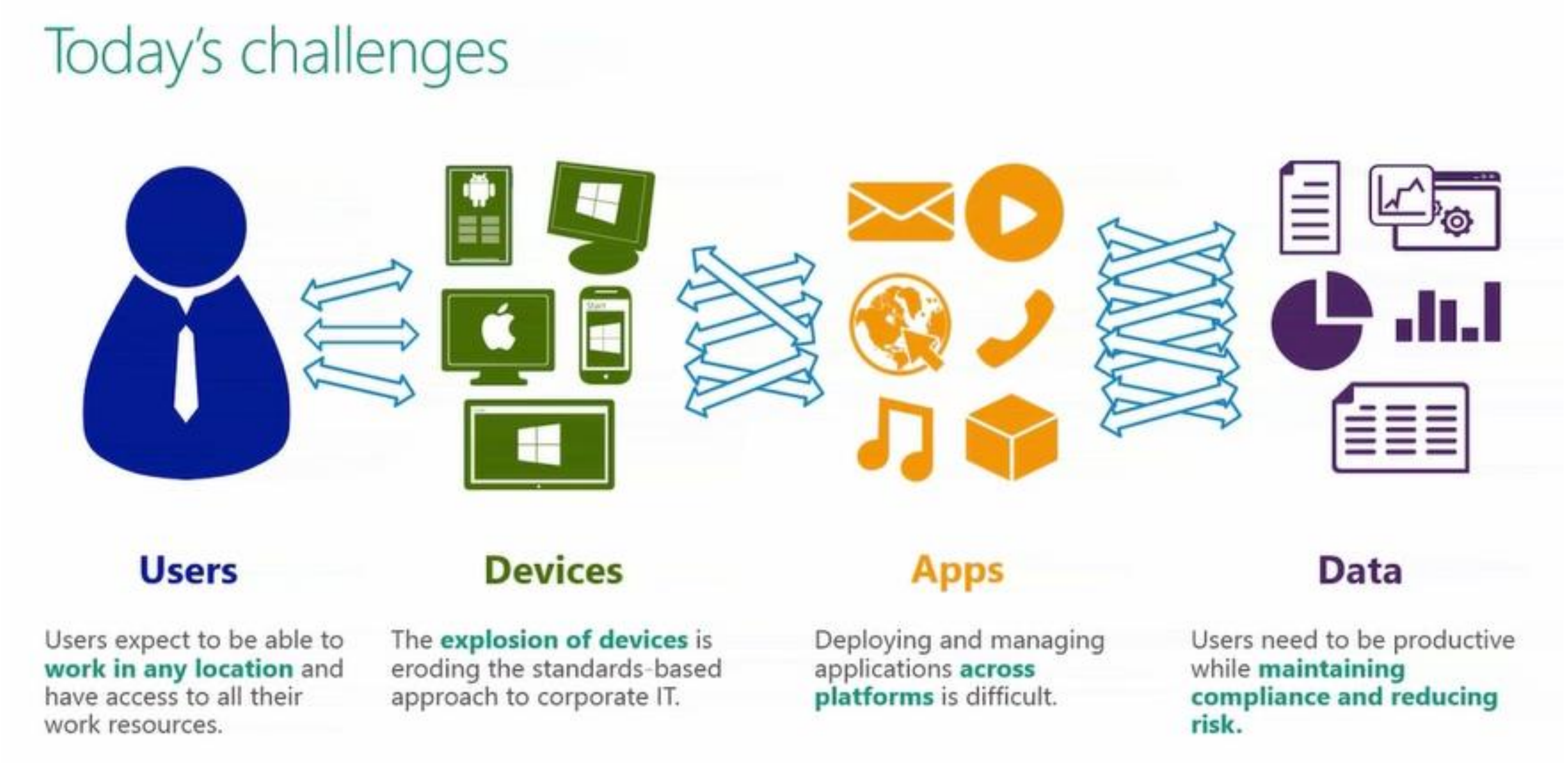
- Privileged access to sensitive information
- DLP helps classified/controlled, information
- What about the rest?

Data

- Documents at rest, in transit, or shared externally
- Encryption is the minimal level for everything

How do we do it?

Protect	Detect	Analyse	Respond
Education and vigilance is key	Understand the scenarios	Know the scale of the problem	Don’t react hastily, follow a plan
Layered approach	Look for anomalies	Identify the potential impact	Call in the experts, including the lawyers if necessary
Technology and People	Test regularly	Protect the logs and other information	Communicate clearly, but securely



Today's challenges

Users

Users expect to be able to **work in any location** and have access to all their work resources.

Devices

The **explosion of devices** is eroding the standards-based approach to corporate IT.

Apps

Deploying and managing applications **across platforms** is difficult.

Data

Users need to be productive while **maintaining compliance and reducing risk.**

DLP detects potential issues

…based on defined rules

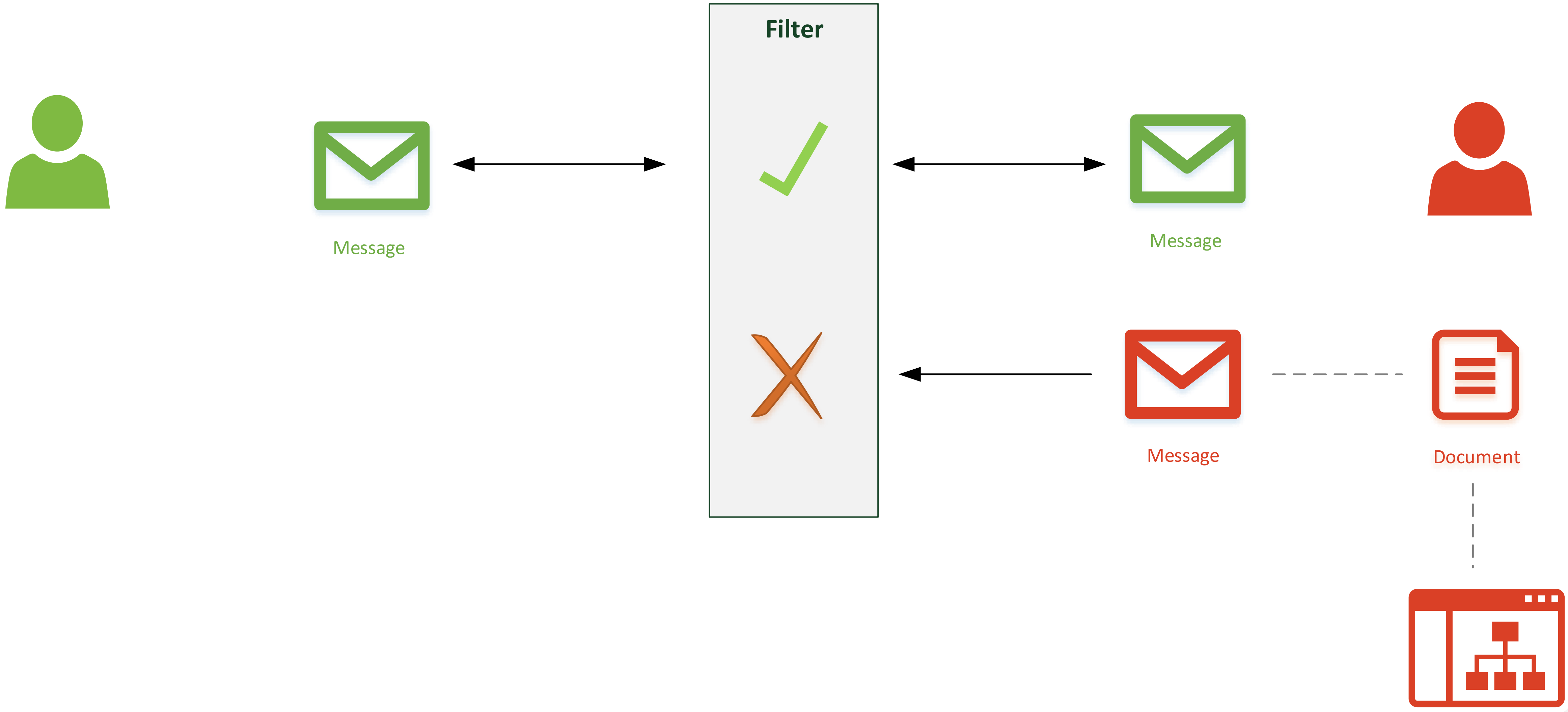
RMS protects the data

…with strong encryption, anywhere

Information Security

Scenarios

ignia



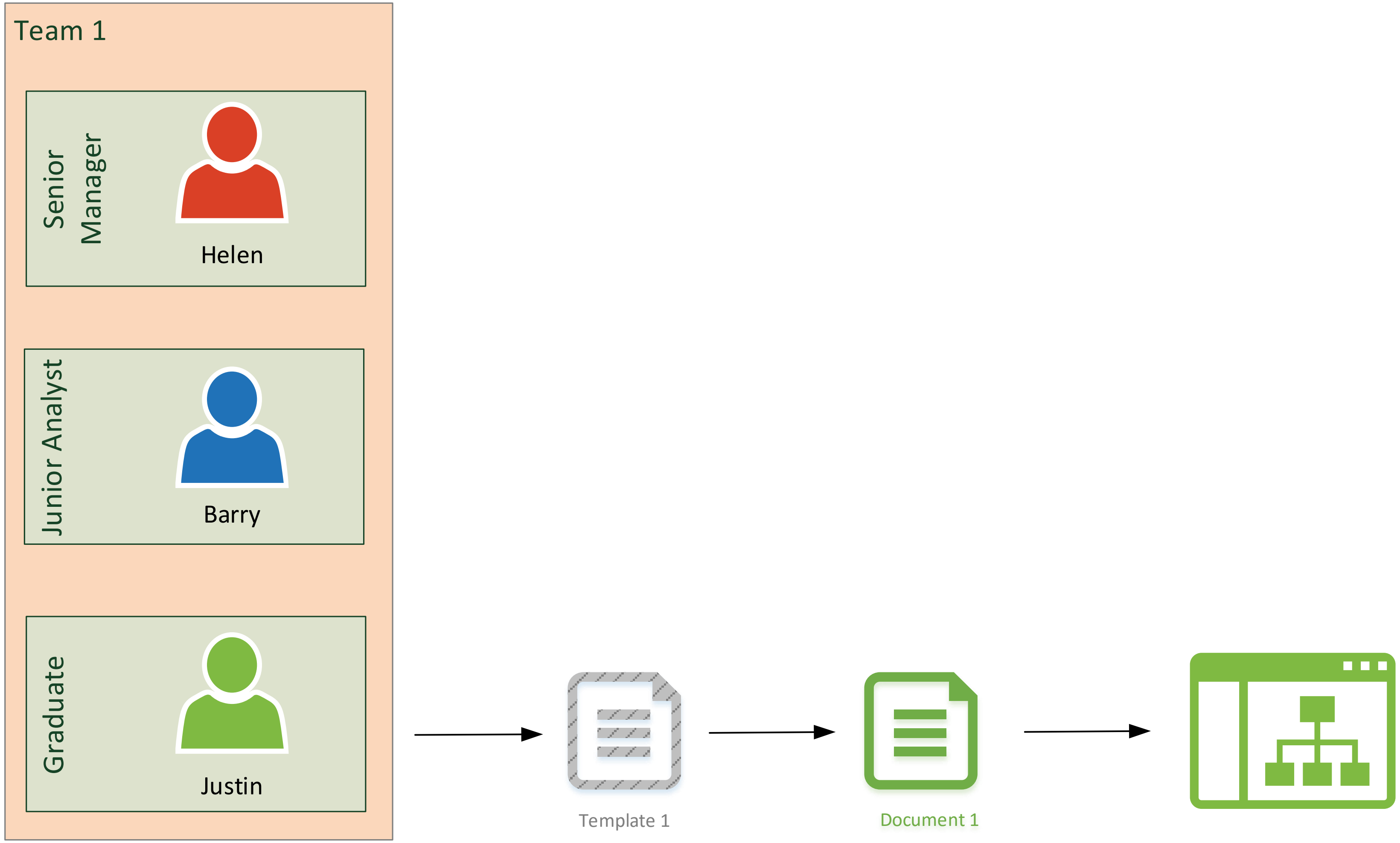
Filter

Message

Message

Message

Document



Team 1

Senior Manager

Helen

Junior Analyst

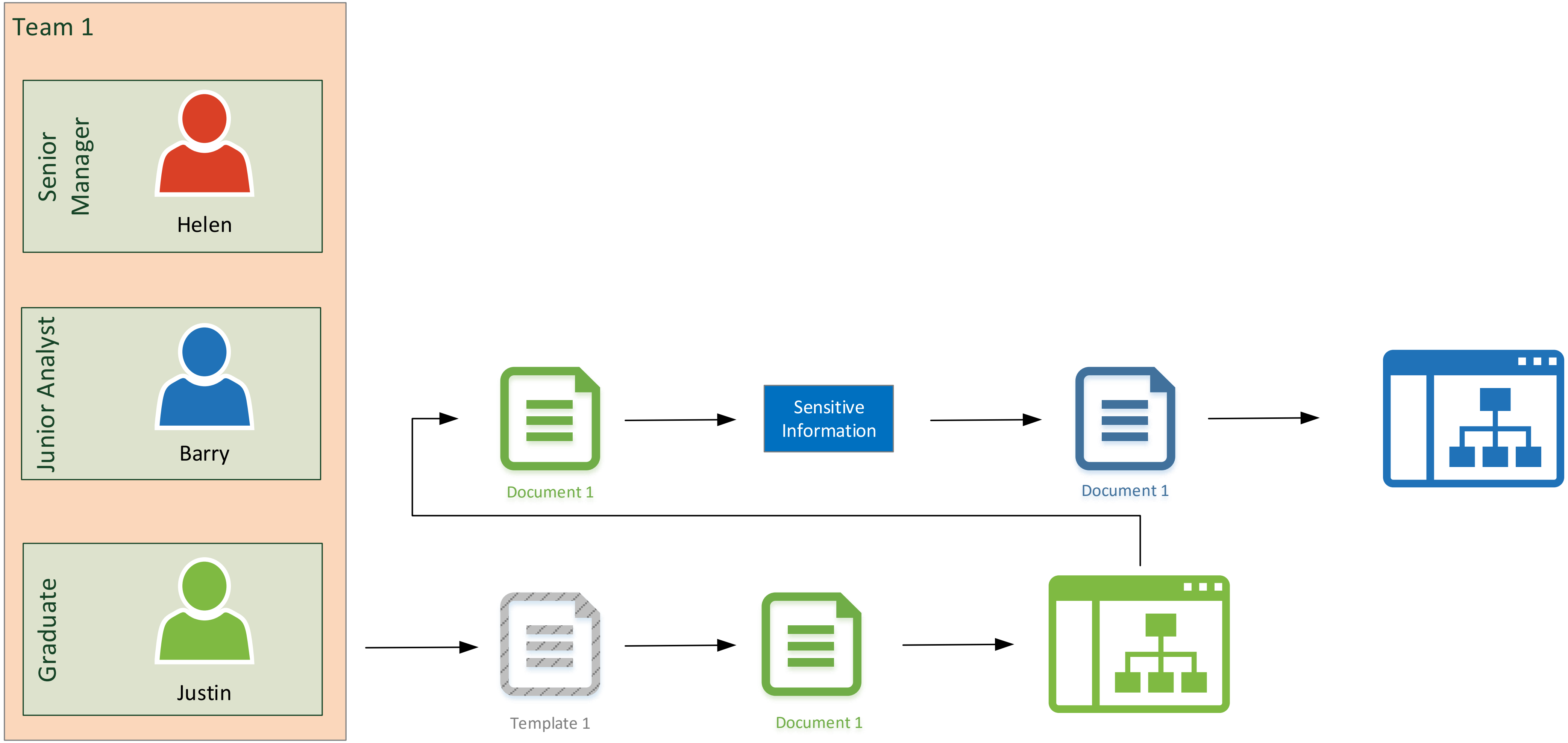
Barry

Graduate

Justin

Template 1

Document 1



Team 1

Senior Manager

Helen

Junior Analyst

Barry

Graduate

Justin

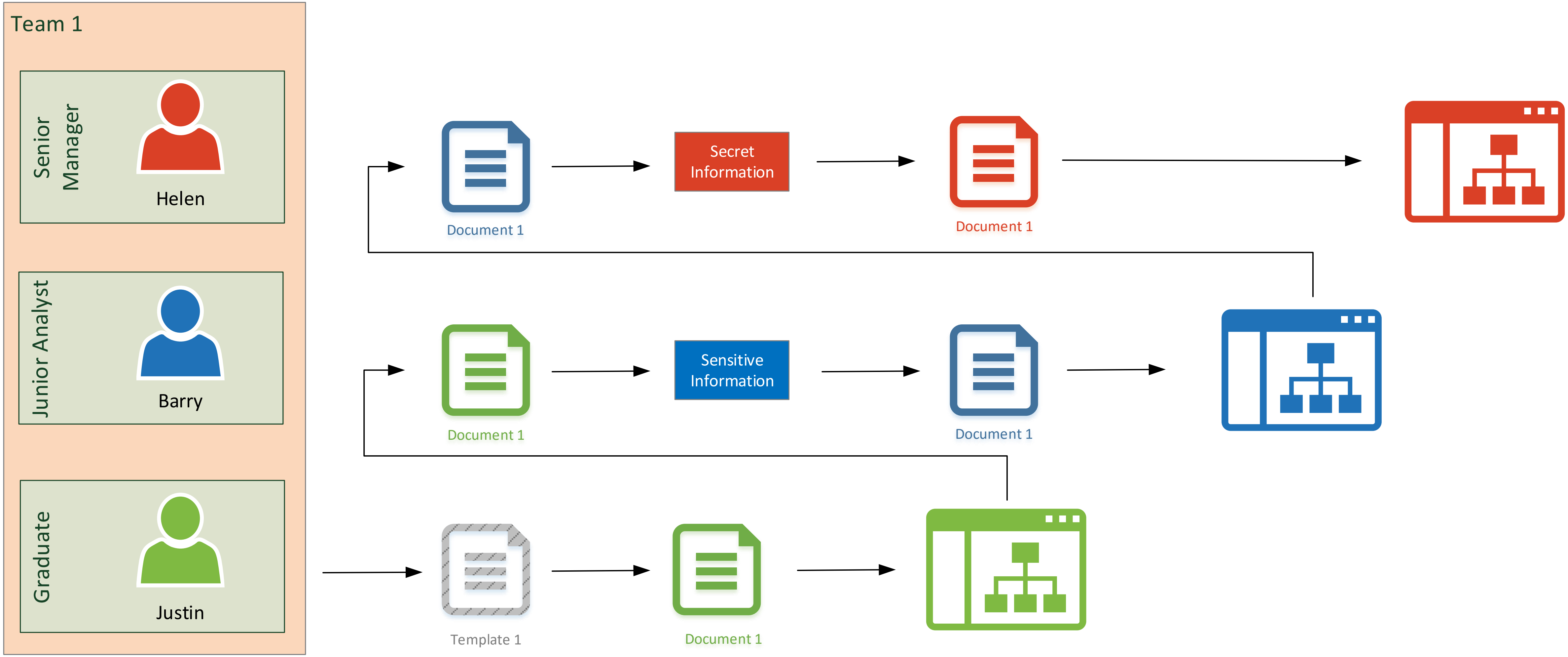
Document 1

Sensitive Information

Document 1

Template 1

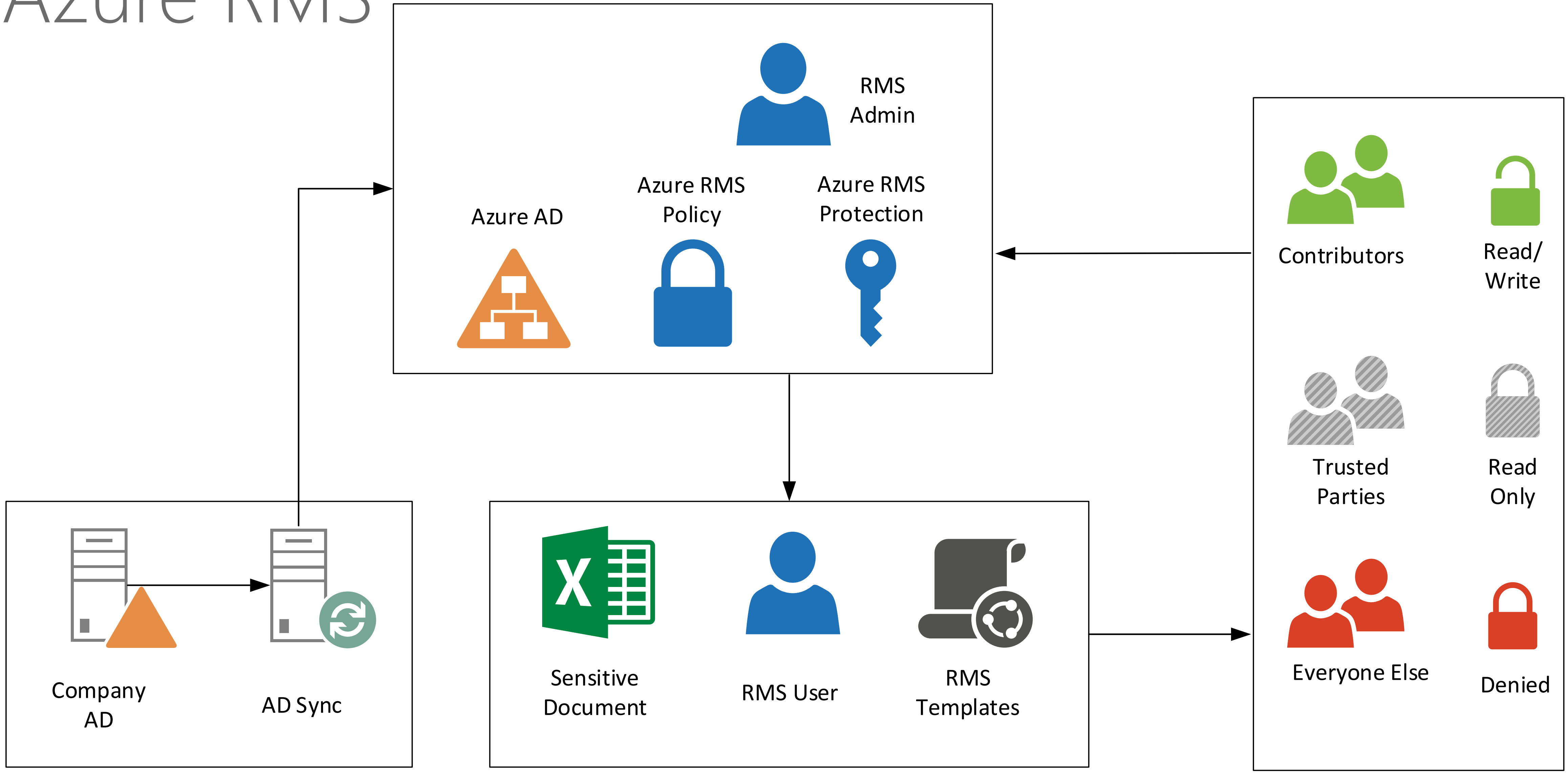
Document 1


Team 1
Senior Manager
Helen
Junior Analyst
Barry
Graduate
Justin
Document 1
Secret Information
Document 1
Document 1
Sensitive Information
Document 1
Template 1
Document 1

RMS

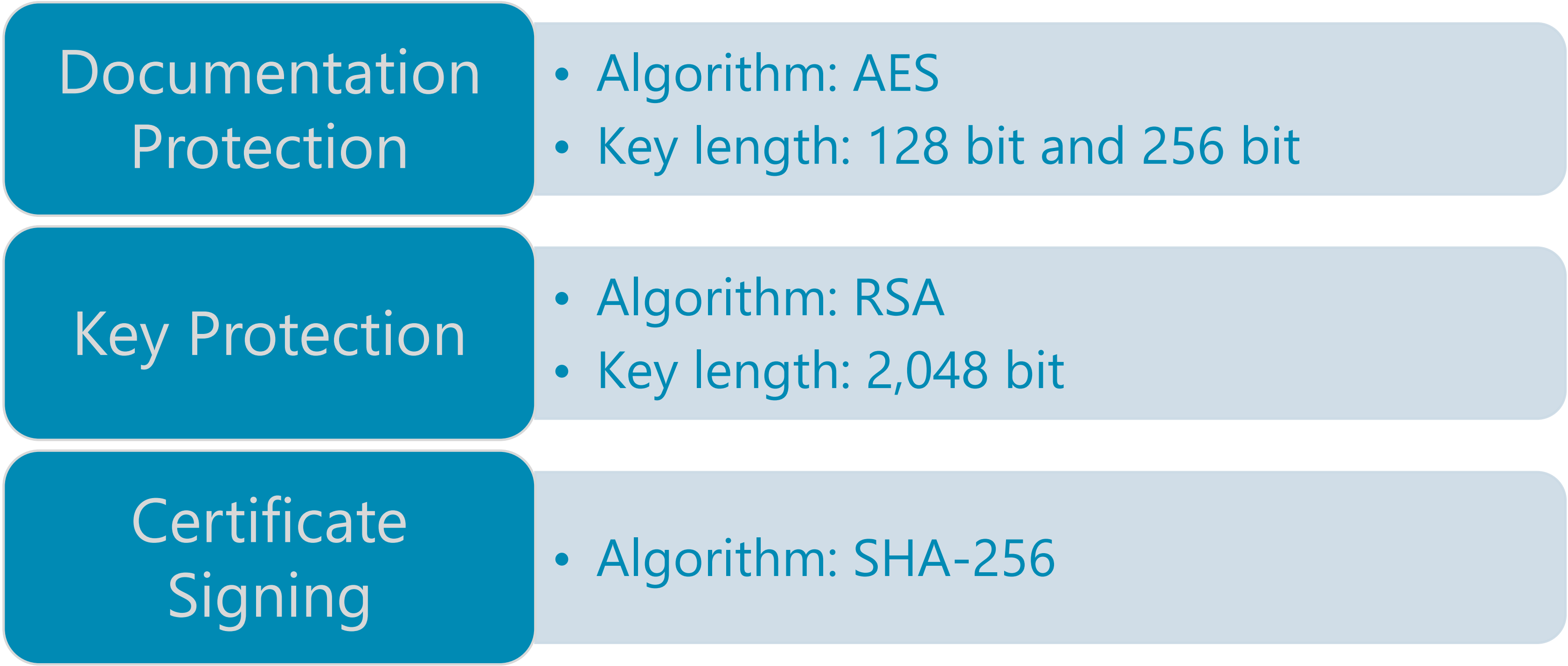
Rights Management Service

Azure RMS


RMS Admin
Azure AD
Azure RMS Policy
Azure RMS Protection
Contributors
Read/ Write
Trusted Parties
Read Only
Everyone Else
Denied
Company AD
AD Sync
Sensitive Document
RMS User
RMS Templates

Azure RMS

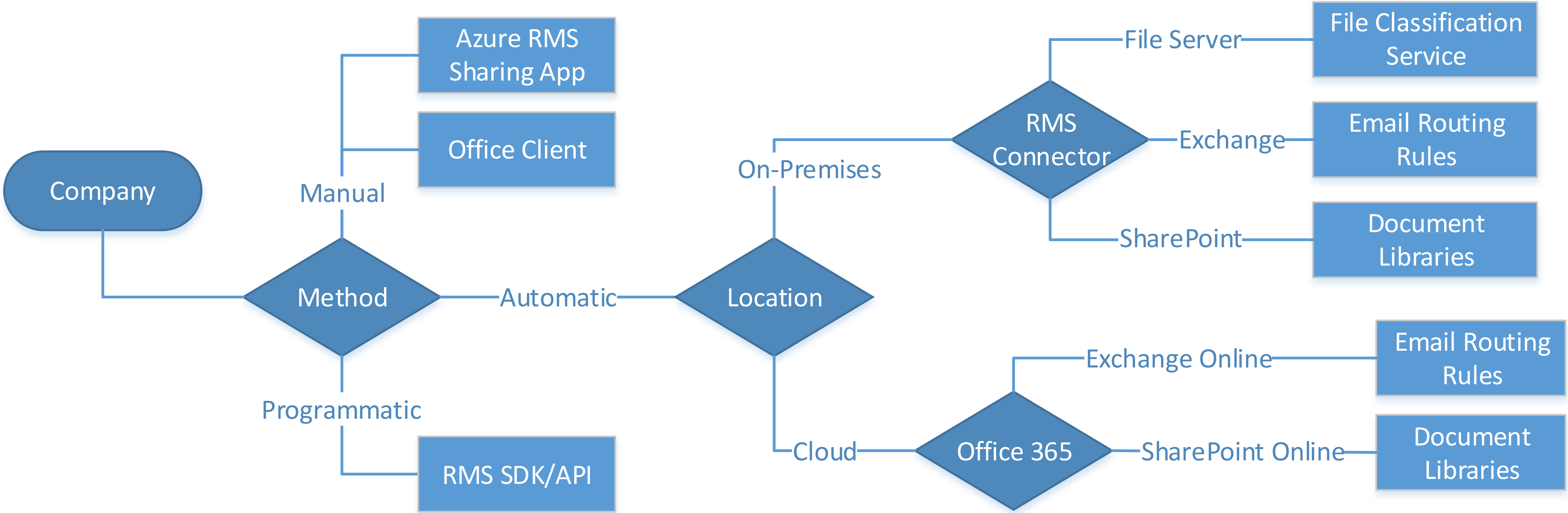
- Microsoft Azure RMS does not store or access the data, it simply makes the data unreadable. Cryptographic controls used by Azure RMS:



Documentation Protection	• Algorithm: AES • Key length: 128 bit and 256 bit
Key Protection	• Algorithm: RSA • Key length: 2,048 bit
Certificate Signing	• Algorithm: SHA-256

Azure RMS

Deployment Options

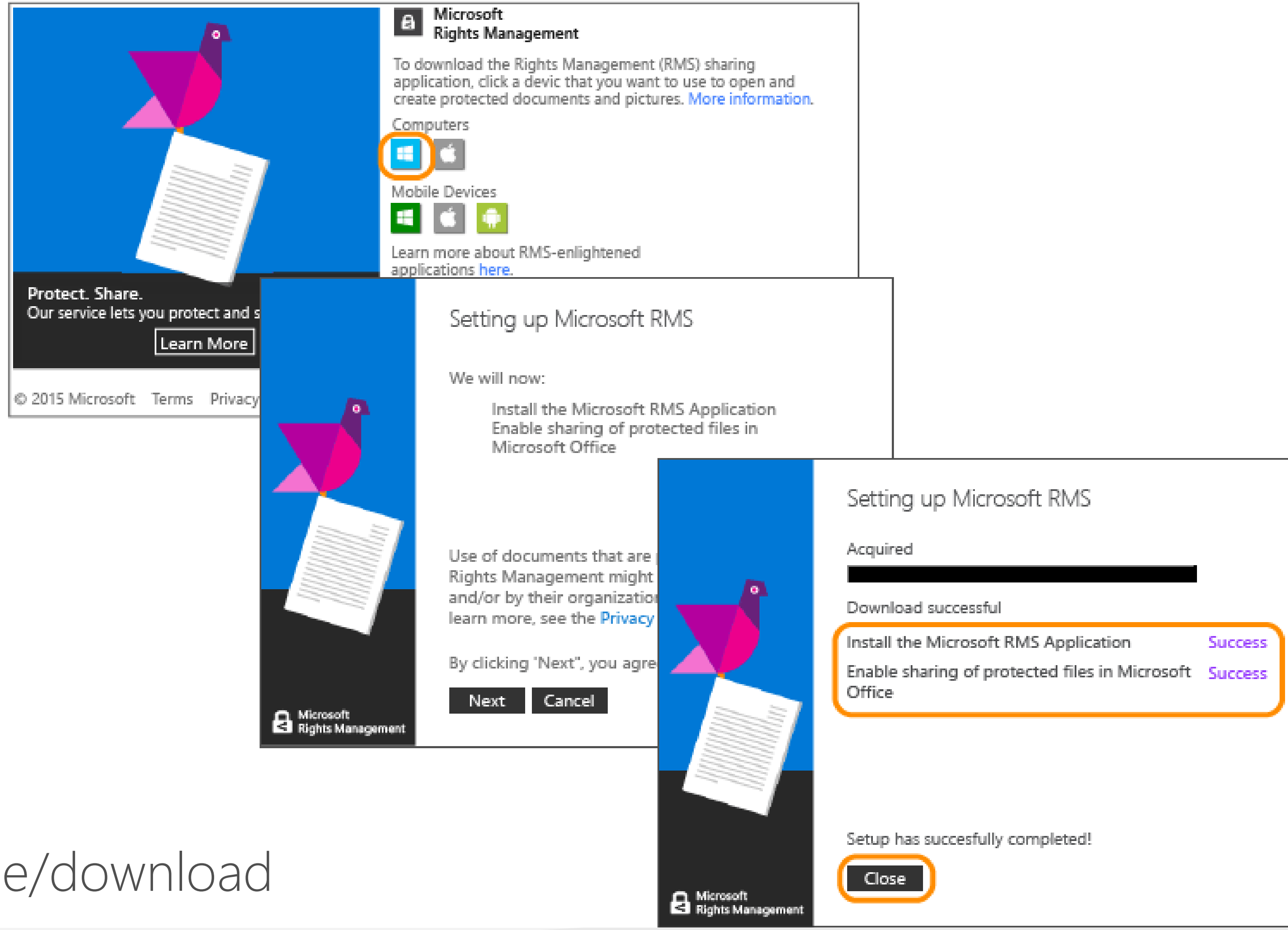


Azure RMS

- Share protected and protect in-place (manual)

Protect local files	Send by email	Copy to storage accounts
Track and revoke	View and use protected files	Remove protection

Azure RMS Sharing App



Microsoft
Rights Management

To download the Rights Management (RMS) sharing application, click a devic that you want to use to open and create protected documents and pictures. More information.

Computers

Mobile Devices

Learn more about RMS-enlightened applications here.

Protect. Share.
Our service lets you protect and s

Learn More

© 2015 Microsoft Terms Privacy

Setting up Microsoft RMS

We will now:

Install the Microsoft RMS Application
Enable sharing of protected files in Microsoft Office

Use of documents that are Rights Management might and/or by their organizatio learn more, see the Privacy

By clicking "Next", you agre

Next Cancel

Microsoft
Rights Management

Setting up Microsoft RMS

Acquired

Download successful

Install the Microsoft RMS Application — Success
Enable sharing of protected files in Microsoft Office — Success

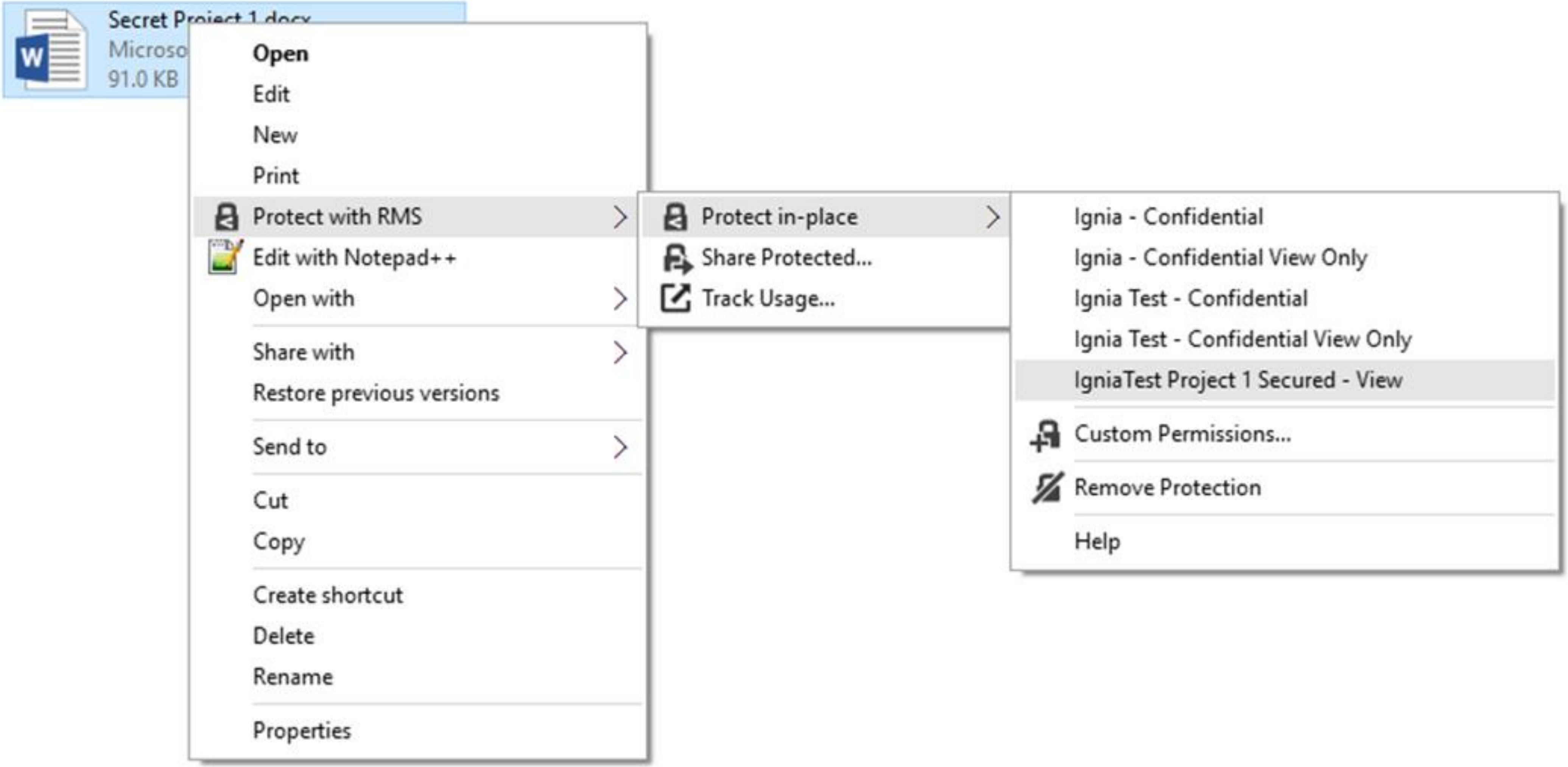
Setup has succesfully completed!

Close

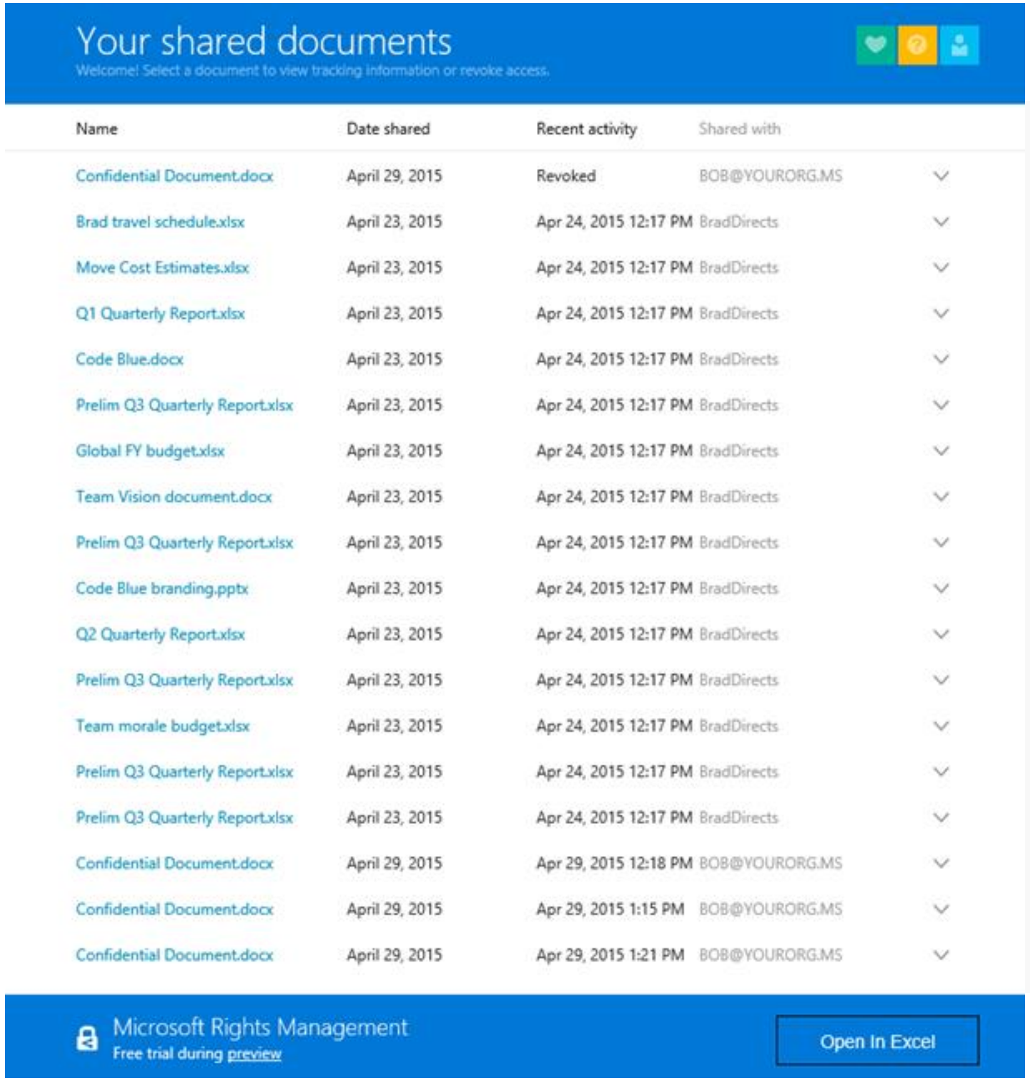
Microsoft
Rights Management

- https://portal.aadrm.com/home/download

Protect in-place



Track & Revoke

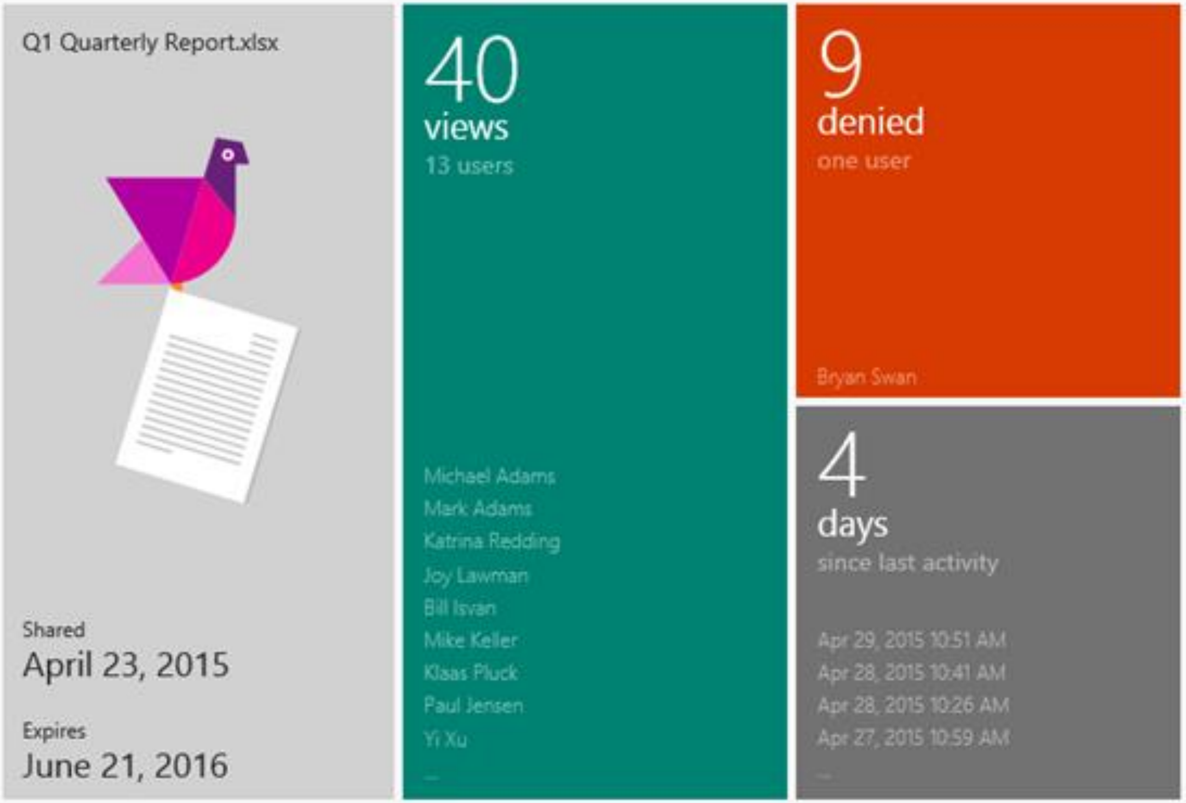


Your shared documents

Welcome! Select a document to view tracking information or revoke access.

Name	Date shared	Recent activity	Shared with
Confidential Document.docx	April 29, 2015	Revoked	BOB@YOURORG.MS
Brad travel schedule.xlsx	April 23, 2015	Apr 24, 2015 12:17 PM	BradDirects
Move Cost Estimates.xlsx	April 23, 2015	Apr 24, 2015 12:17 PM	BradDirects
Q1 Quarterly Report.xlsx	April 23, 2015	Apr 24, 2015 12:17 PM	BradDirects
Code Blue.docx	April 23, 2015	Apr 24, 2015 12:17 PM	BradDirects
Prelim Q3 Quarterly Report.xlsx	April 23, 2015	Apr 24, 2015 12:17 PM	BradDirects
Global FY budget.xlsx	April 23, 2015	Apr 24, 2015 12:17 PM	BradDirects
Team Vision document.docx	April 23, 2015	Apr 24, 2015 12:17 PM	BradDirects
Prelim Q3 Quarterly Report.xlsx	April 23, 2015	Apr 24, 2015 12:17 PM	BradDirects
Code Blue branding.pptx	April 23, 2015	Apr 24, 2015 12:17 PM	BradDirects
Q2 Quarterly Report.xlsx	April 23, 2015	Apr 24, 2015 12:17 PM	BradDirects
Prelim Q3 Quarterly Report.xlsx	April 23, 2015	Apr 24, 2015 12:17 PM	BradDirects
Team morale budget.xlsx	April 23, 2015	Apr 24, 2015 12:17 PM	BradDirects
Prelim Q3 Quarterly Report.xlsx	April 23, 2015	Apr 24, 2015 12:17 PM	BradDirects
Prelim Q3 Quarterly Report.xlsx	April 23, 2015	Apr 24, 2015 12:17 PM	BradDirects
Confidential Document.docx	April 29, 2015	Apr 29, 2015 12:18 PM	BOB@YOURORG.MS
Confidential Document.docx	April 29, 2015	Apr 29, 2015 1:15 PM	BOB@YOURORG.MS
Confidential Document.docx	April 29, 2015	Apr 29, 2015 1:21 PM	BOB@YOURORG.MS

Microsoft Rights Management
Free trial during preview



Q1 Quarterly Report.xlsx

Shared
April 23, 2015

Expires
June 21, 2016

40
views
13 users

Michael Adams
Mark Adams
Katrina Redding
Joy Lawman
Bill Isvan
Mike Keller
Klaas Pluck
Paul Jensen
Yi Xu

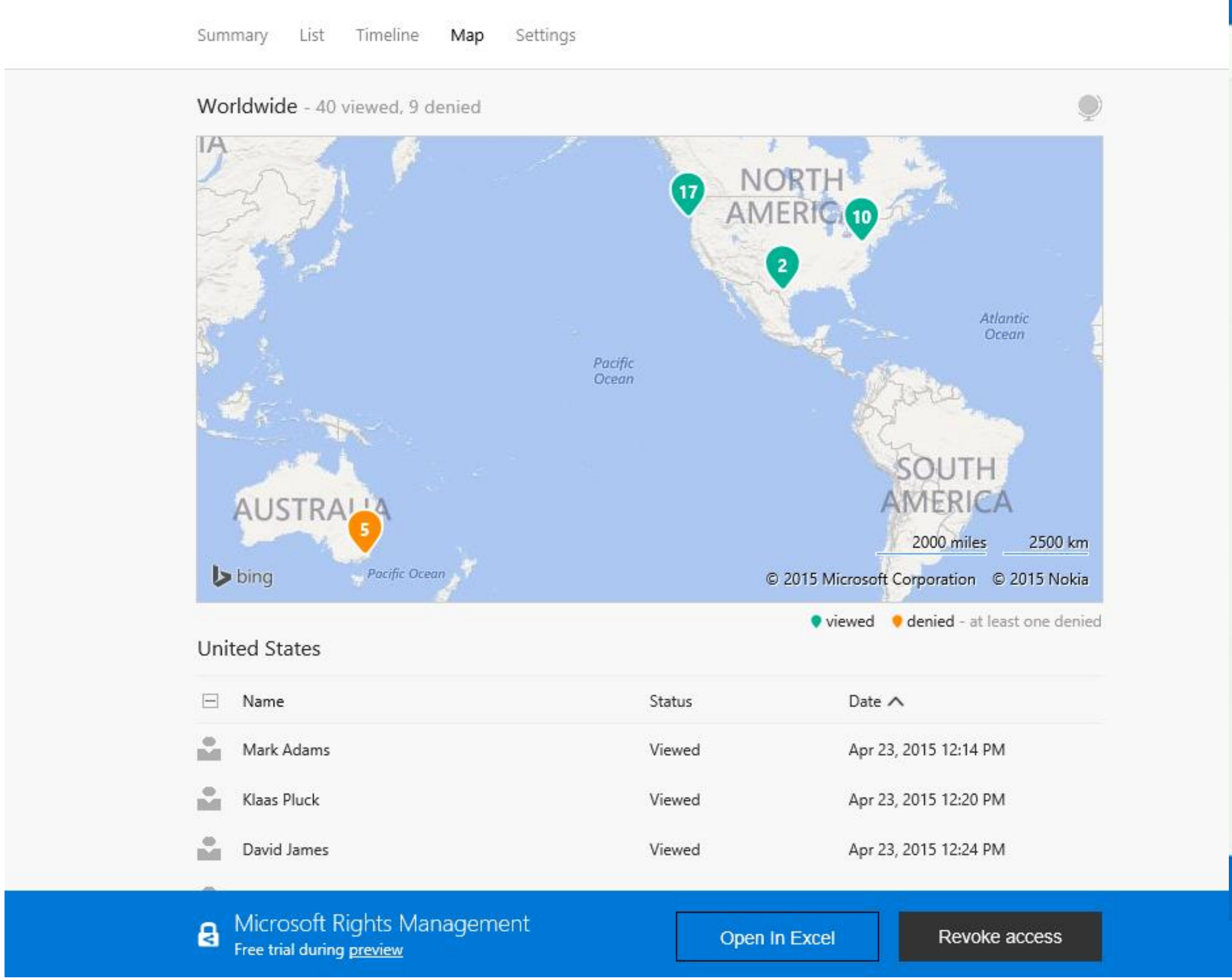
9
denied
one user

Bryan Swan

4
days
since last activity

Apr 29, 2015 10:51 AM
Apr 28, 2015 10:41 AM
Apr 28, 2015 10:26 AM
Apr 27, 2015 10:59 AM

Track & Revoke



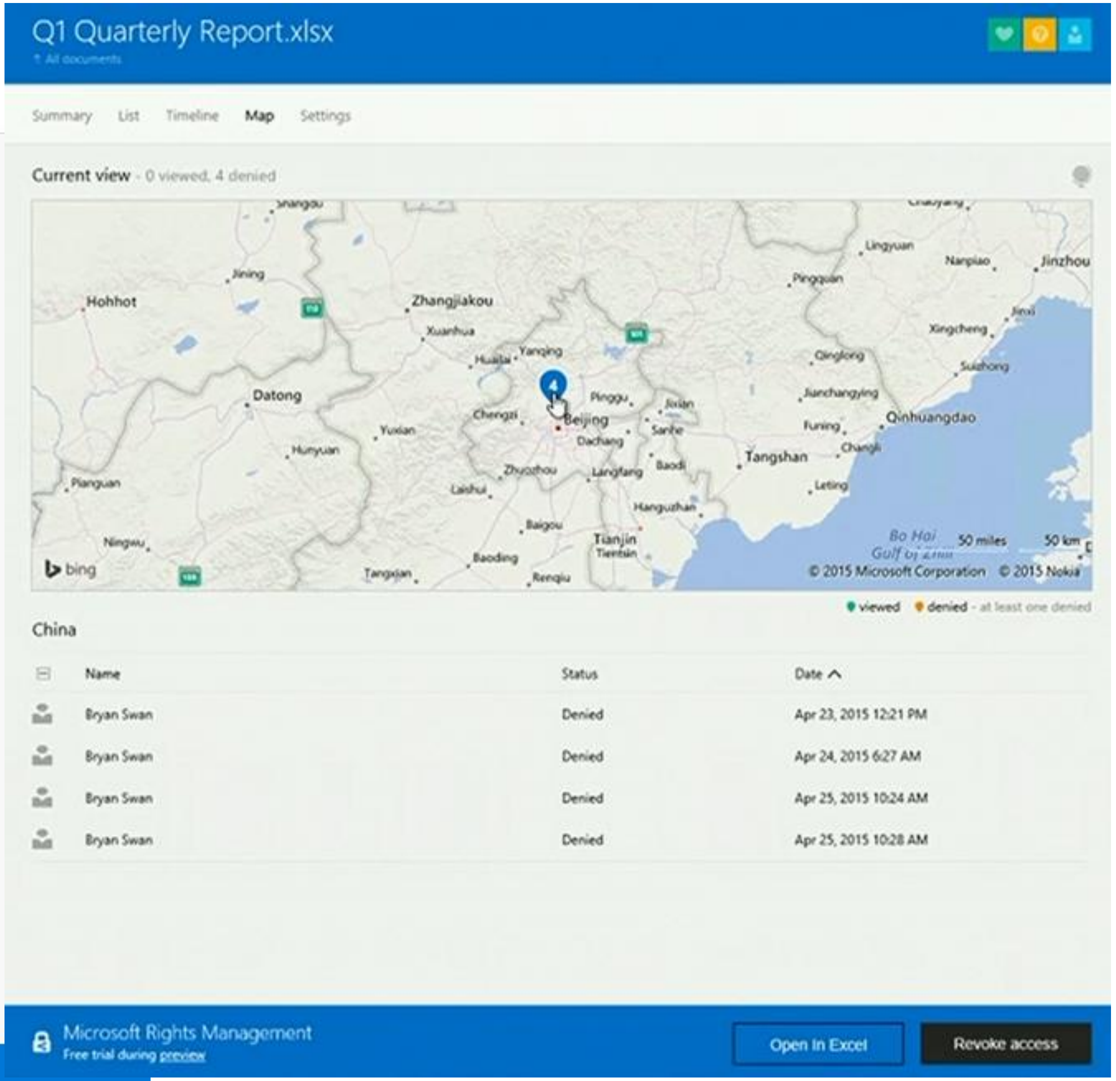
Worldwide - 40 viewed, 9 denied

● viewed ● denied - at least one denied

United States

Name	Status	Date ^
Mark Adams	Viewed	Apr 23, 2015 12:14 PM
Klaas Pluck	Viewed	Apr 23, 2015 12:20 PM
David James	Viewed	Apr 23, 2015 12:24 PM

Microsoft Rights Management
Free trial during preview



Q1 Quarterly Report.xlsx

Current view - 0 viewed, 4 denied

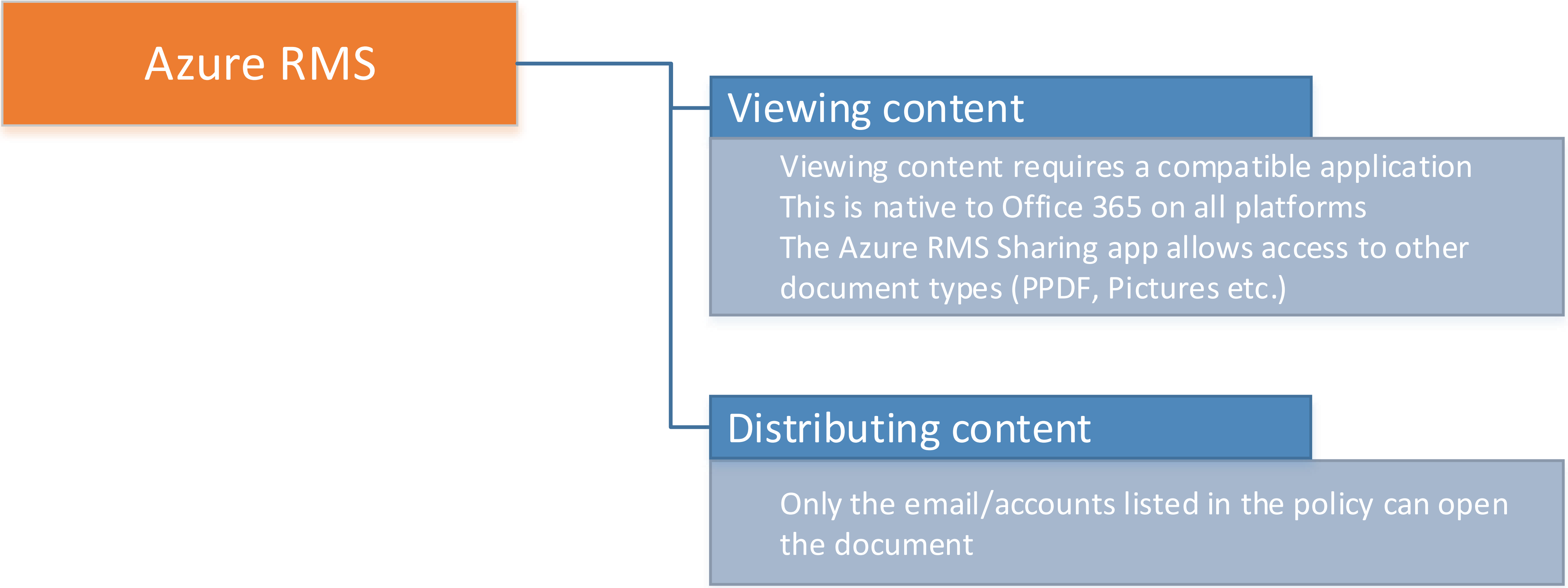
● viewed ● denied - at least one denied

China

Name	Status	Date ^
Bryan Swan	Denied	Apr 23, 2015 12:21 PM
Bryan Swan	Denied	Apr 24, 2015 6:27 AM
Bryan Swan	Denied	Apr 25, 2015 10:24 AM
Bryan Swan	Denied	Apr 25, 2015 10:28 AM

Microsoft Rights Management
Free trial during preview

Considerations



Azure RMS

Viewing content

Viewing content requires a compatible application
This is native to Office 365 on all platforms
The Azure RMS Sharing app allows access to other document types (PPDF, Pictures etc.)

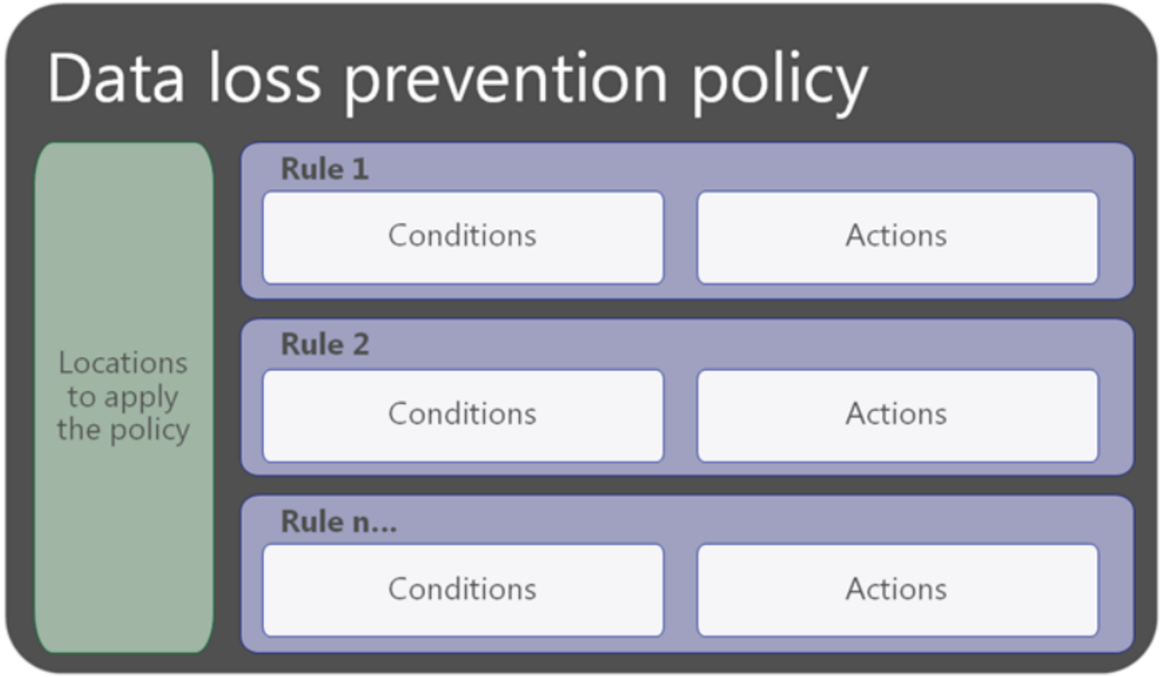
Distributing content

Only the email/accounts listed in the policy can open the document

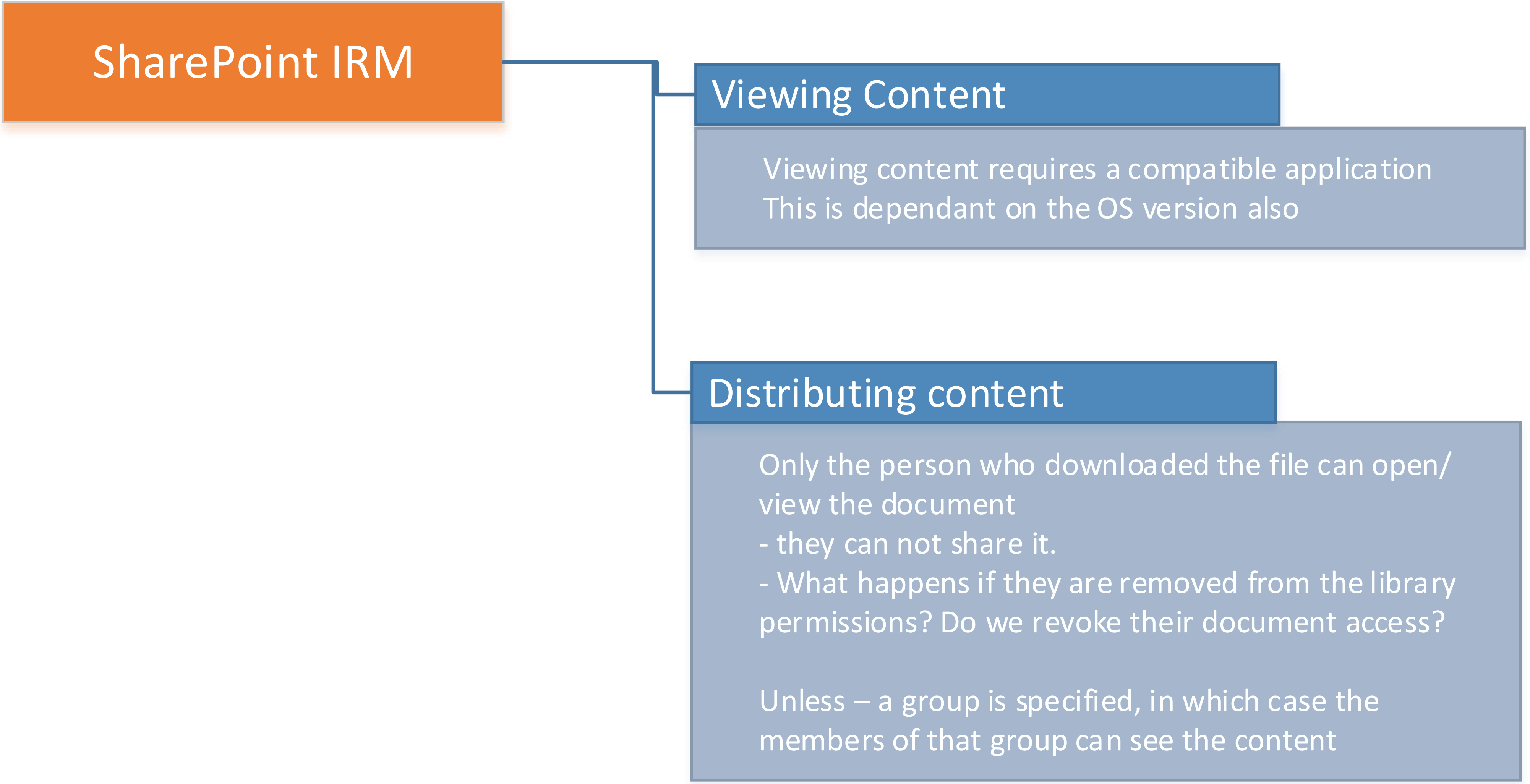
Protection in SharePoint

- Protection is based on document libraries
- Includes OneDrive for Business
- Reduce risk when enabling external sharing
- Automatically block access across sites for specific content
- Compliance reports

  & alerts



Considerations



SharePoint IRM

Viewing Content

Viewing content requires a compatible application
This is dependant on the OS version also

Distributing content

Only the person who downloaded the file can open/ view the document
- they can not share it.
- What happens if they are removed from the library permissions? Do we revoke their document access?

Unless – a group is specified, in which case the members of that group can see the content

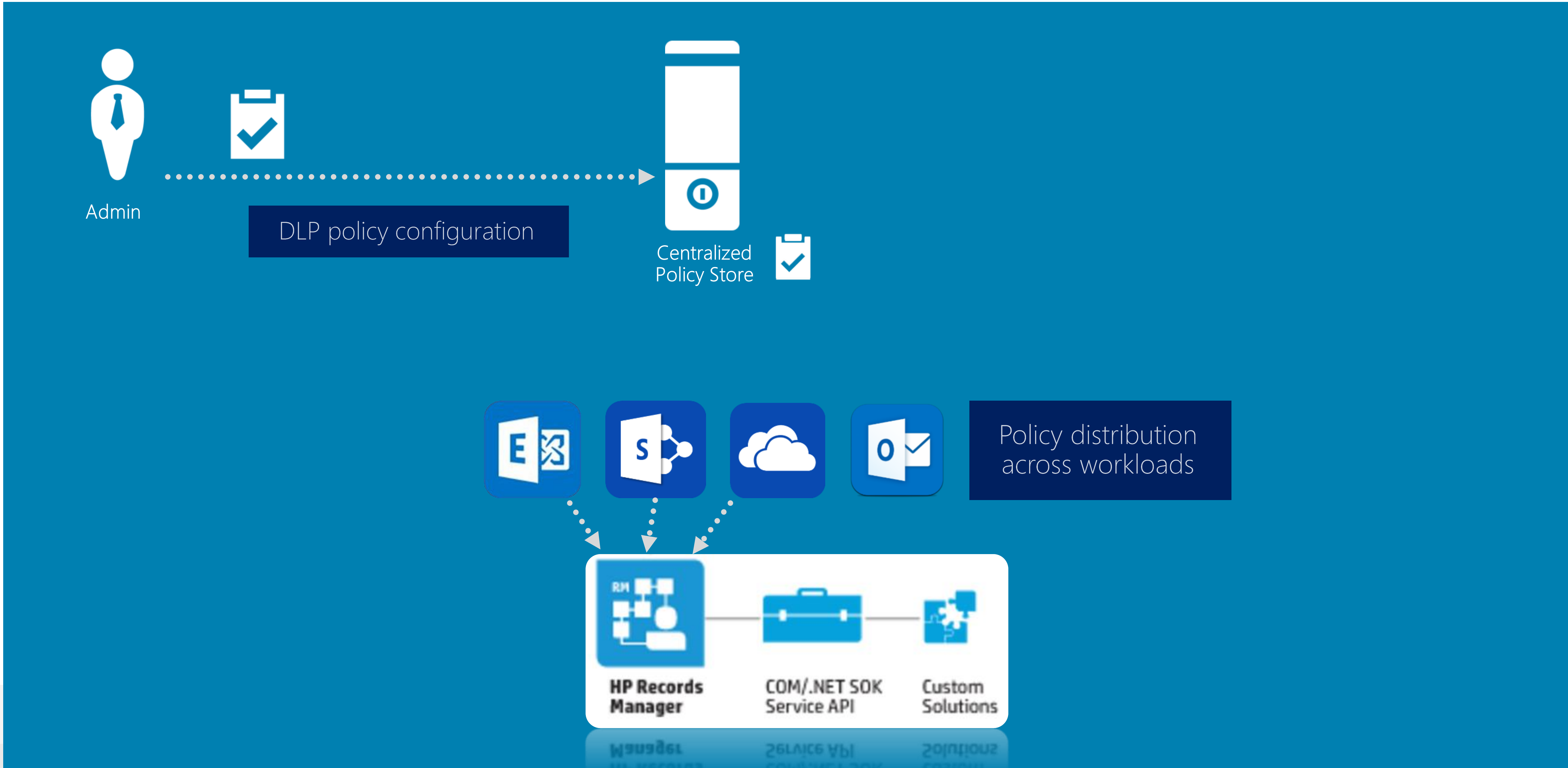
Protection in Exchange

- Prevent deletion of email with specific content types
- Restrict content distribution based on recipient/domain
- Educate users without interrupting workflow
- Document FingerPrinting

DLP

Data Loss Prevention

DLP Walkthrough



Admin

DLP policy configuration

Centralized Policy Store

Policy distribution across workloads

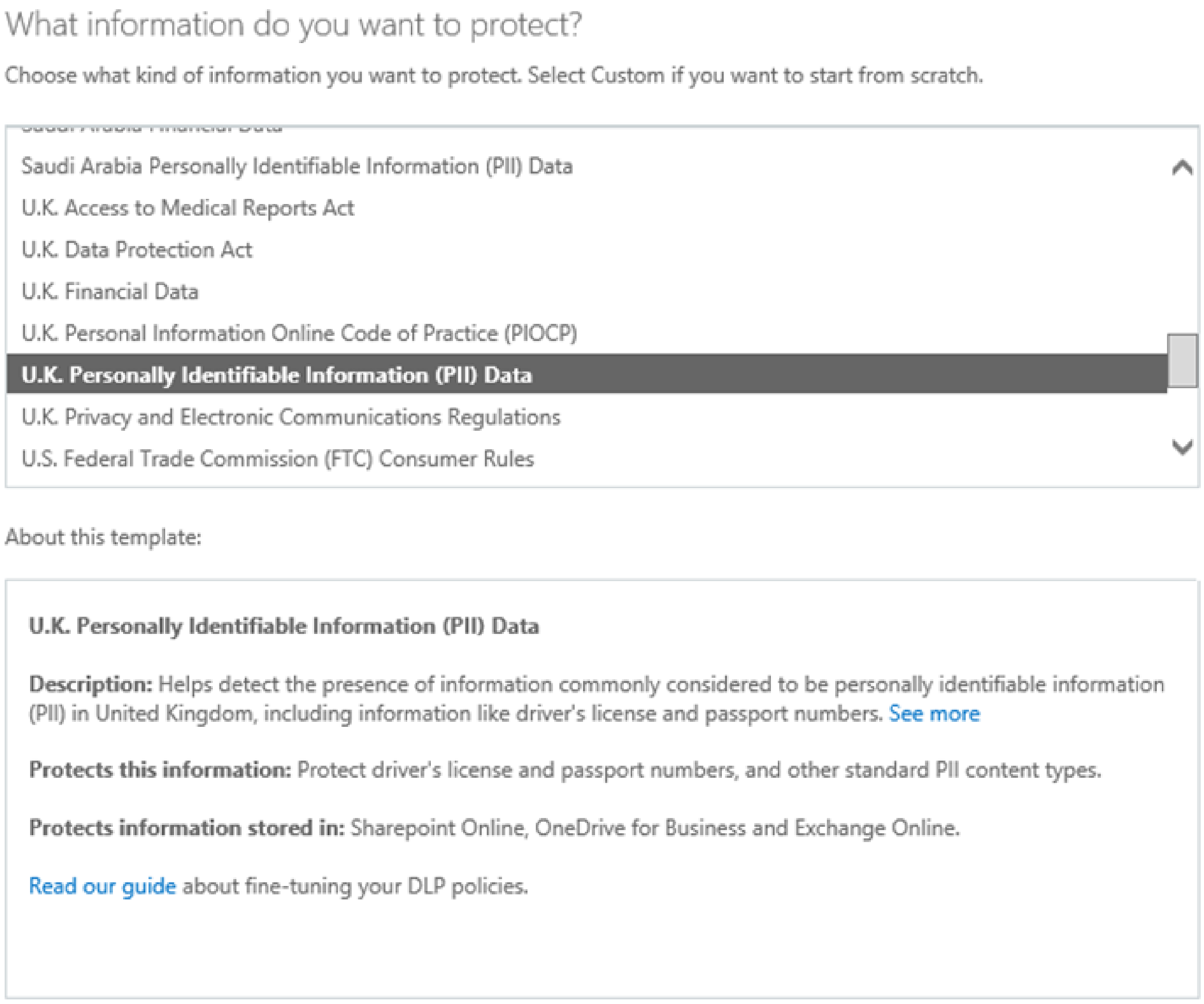
HP Records Manager

COM/.NET SDK Service API

Custom Solutions

DLP: Policy Templates

- Built-in templates based on common regulations from around the globe
- Import DLP policy templates from partners
- or, Build your own



What information do you want to protect?

Choose what kind of information you want to protect. Select Custom if you want to start from scratch.

- Saudi Arabia Financial Data
- Saudi Arabia Personally Identifiable Information (PII) Data
- U.K. Access to Medical Reports Act
- U.K. Data Protection Act
- U.K. Financial Data
- U.K. Personal Information Online Code of Practice (PIOCP)
- **U.K. Personally Identifiable Information (PII) Data**
- U.K. Privacy and Electronic Communications Regulations
- U.S. Federal Trade Commission (FTC) Consumer Rules

About this template:

U.K. Personally Identifiable Information (PII) Data

Description: Helps detect the presence of information commonly considered to be personally identifiable information (PII) in United Kingdom, including information like driver's license and passport numbers. See more

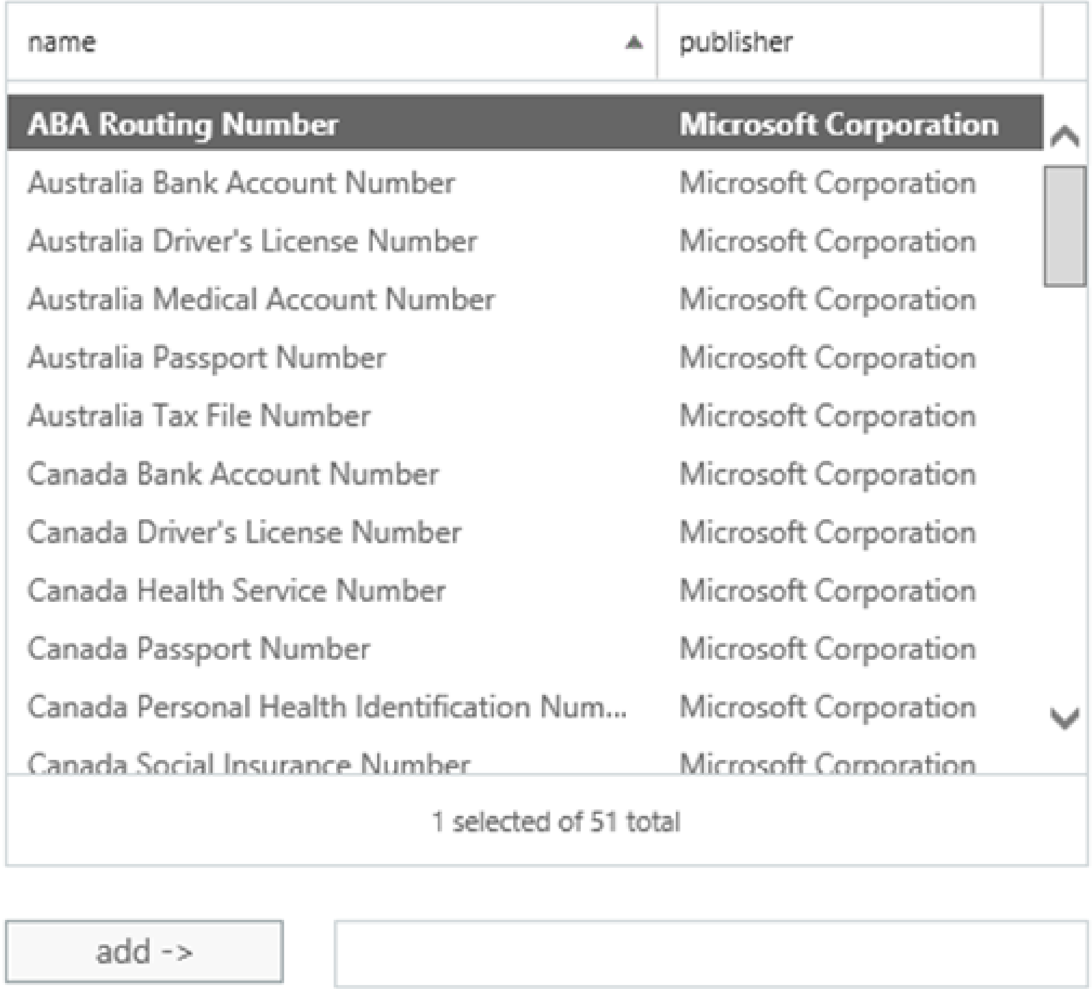
Protects this information: Protect driver's license and passport numbers, and other standard PII content types.

Protects information stored in: Sharepoint Online, OneDrive for Business and Exchange Online.

Read our guide about fine-tuning your DLP policies.

DPL: Sensitive content detection

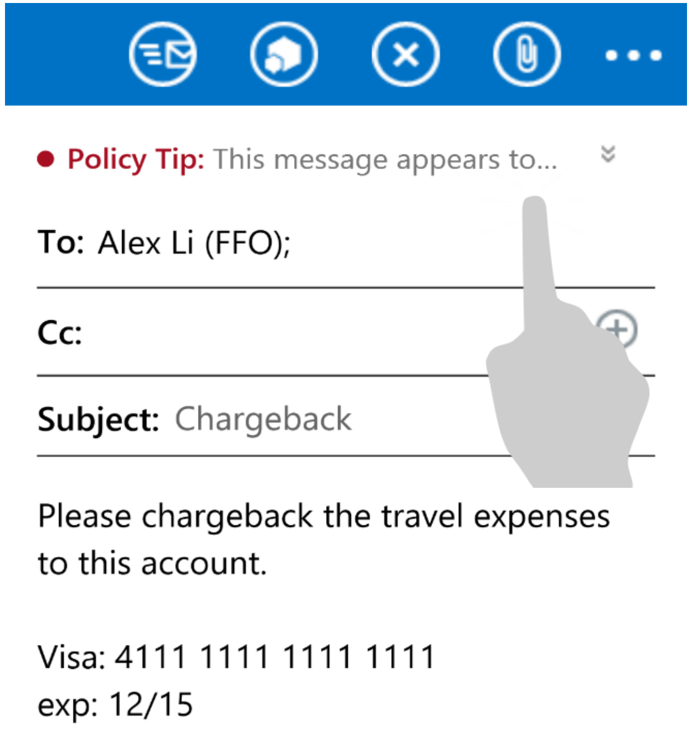
- Predefined rules targeted at sensitive data types
- Advanced content detection
- Combination of regular expressions, keywords, internal functions, validate checksums, formatting, etc.
- Extensibility for defined data types



name	publisher
ABA Routing Number	Microsoft Corporation
Australia Bank Account Number	Microsoft Corporation
Australia Driver's License Number	Microsoft Corporation
Australia Medical Account Number	Microsoft Corporation
Australia Passport Number	Microsoft Corporation
Australia Tax File Number	Microsoft Corporation
Canada Bank Account Number	Microsoft Corporation
Canada Driver's License Number	Microsoft Corporation
Canada Health Service Number	Microsoft Corporation
Canada Passport Number	Microsoft Corporation
Canada Personal Health Identification Num...	Microsoft Corporation
Canada Social Insurance Number	Microsoft Corporation

1 selected of 51 total

UX: Mail



● **Policy Tip:** This message appears to...

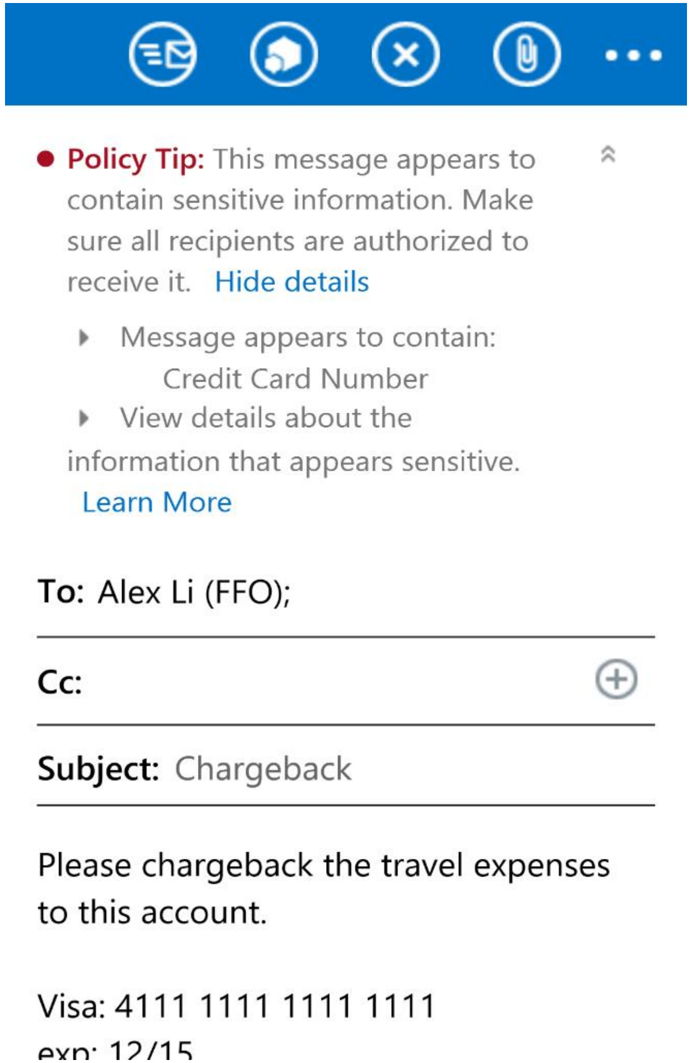
To: Alex Li (FFO);

Cc:

Subject: Chargeback

Please chargeback the travel expenses to this account.

Visa: 4111 1111 1111 1111
exp: 12/15



● **Policy Tip:** This message appears to contain sensitive information. Make sure all recipients are authorized to receive it. Hide details

- Message appears to contain:
  Credit Card Number
- View details about the information that appears sensitive.
  Learn More

To: Alex Li (FFO);

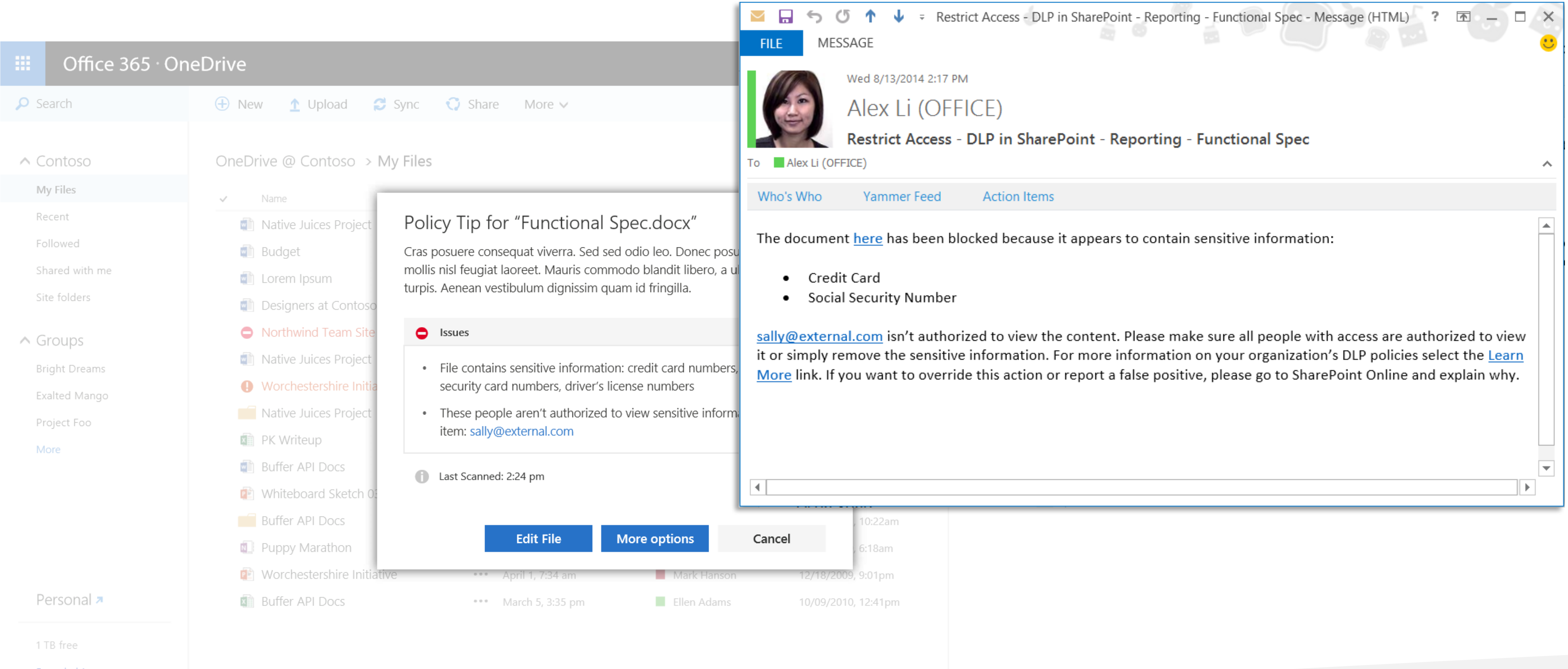
Cc:

Subject: Chargeback

Please chargeback the travel expenses to this account.

Visa: 4111 1111 1111 1111
exp: 12/15

UX: SharePoint & OneDrive



Policy Tip for "Functional Spec.docx"

Cras posuere consequat viverra. Sed sed odio leo. Donec posu mollis nisl feugiat laoreet. Mauris commodo blandit libero, a u turpis. Aenean vestibulum dignissim quam id fringilla.

Issues

- File contains sensitive information: credit card numbers, security card numbers, driver's license numbers
- These people aren't authorized to view sensitive inform item: sally@external.com

Last Scanned: 2:24 pm

Restrict Access - DLP in SharePoint - Reporting - Functional Spec - Message (HTML)
FILE
MESSAGE

Wed 8/13/2014 2:17 PM

Alex Li (OFFICE)

Restrict Access - DLP in SharePoint - Reporting - Functional Spec

To 🟩 Alex Li (OFFICE)

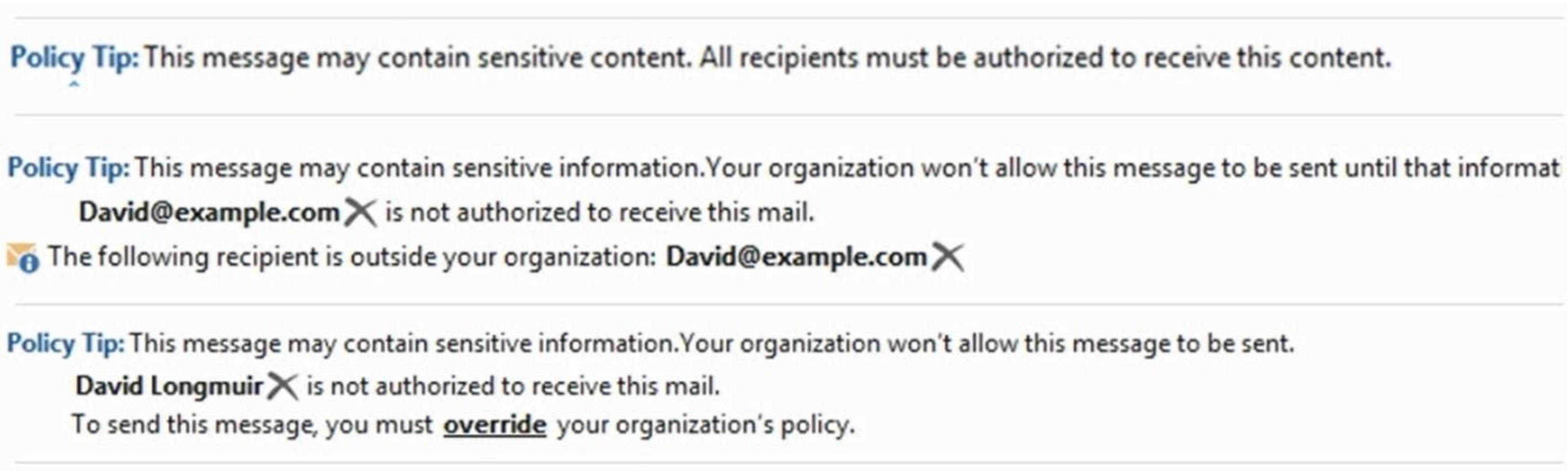
The document here has been blocked because it appears to contain sensitive information:

- Credit Card
- Social Security Number

sally@external.com isn't authorized to view the content. Please make sure all people with access are authorized to view it or simply remove the sensitive information. For more information on your organization's DLP policies select the Learn More link. If you want to override this action or report a false positive, please go to SharePoint Online and explain why.

Customised Policy Tips

Customize Policy Tip messages
Messages for notification, block and override can be customized



Policy Tip: This message may contain sensitive content. All recipients must be authorized to receive this content.

Policy Tip: This message may contain sensitive information.Your organization won't allow this message to be sent until that informat

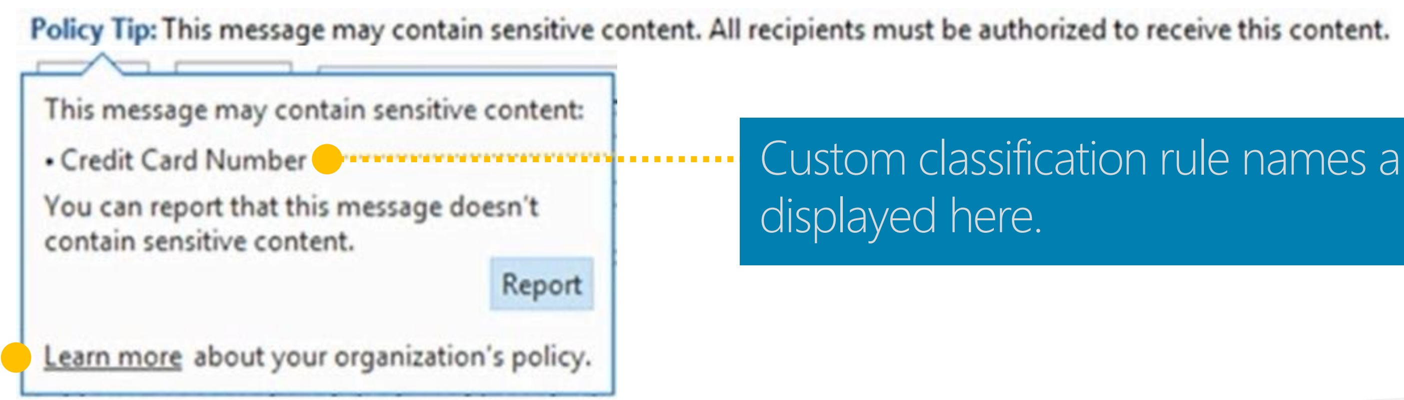
David@example.com ✕ is not authorized to receive this mail.

The following recipient is outside your organization: **David@example.com** ✕

Policy Tip: This message may contain sensitive information.Your organization won't allow this message to be sent.

David Longmuir ✕ is not authorized to receive this mail.

To send this message, you must **override** your organization's policy.



Policy Tip: This message may contain sensitive content. All recipients must be authorized to receive this content.

This message may contain sensitive content:

- Credit Card Number

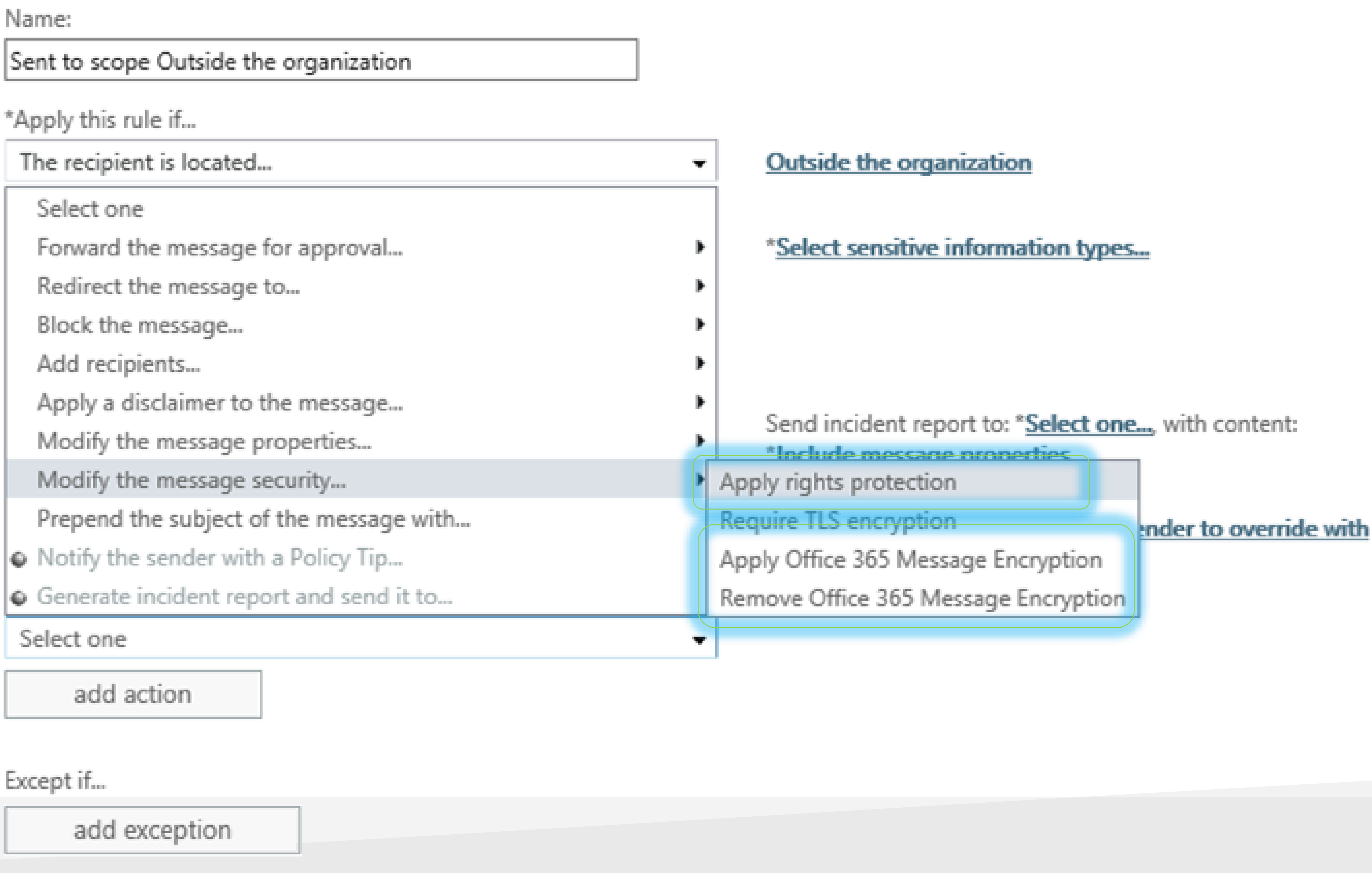
You can report that this message doesn't contain sensitive content.

Learn more about your organization's policy.

Customize link for user education
Specify an internal URL with company policies around handling sensitive content

Custom classification rule names are displayed here.

Integrates with RMS



Name:

Sent to scope Outside the organization

*Apply this rule if...

The recipient is located... — Outside the organization

*Select sensitive information types...

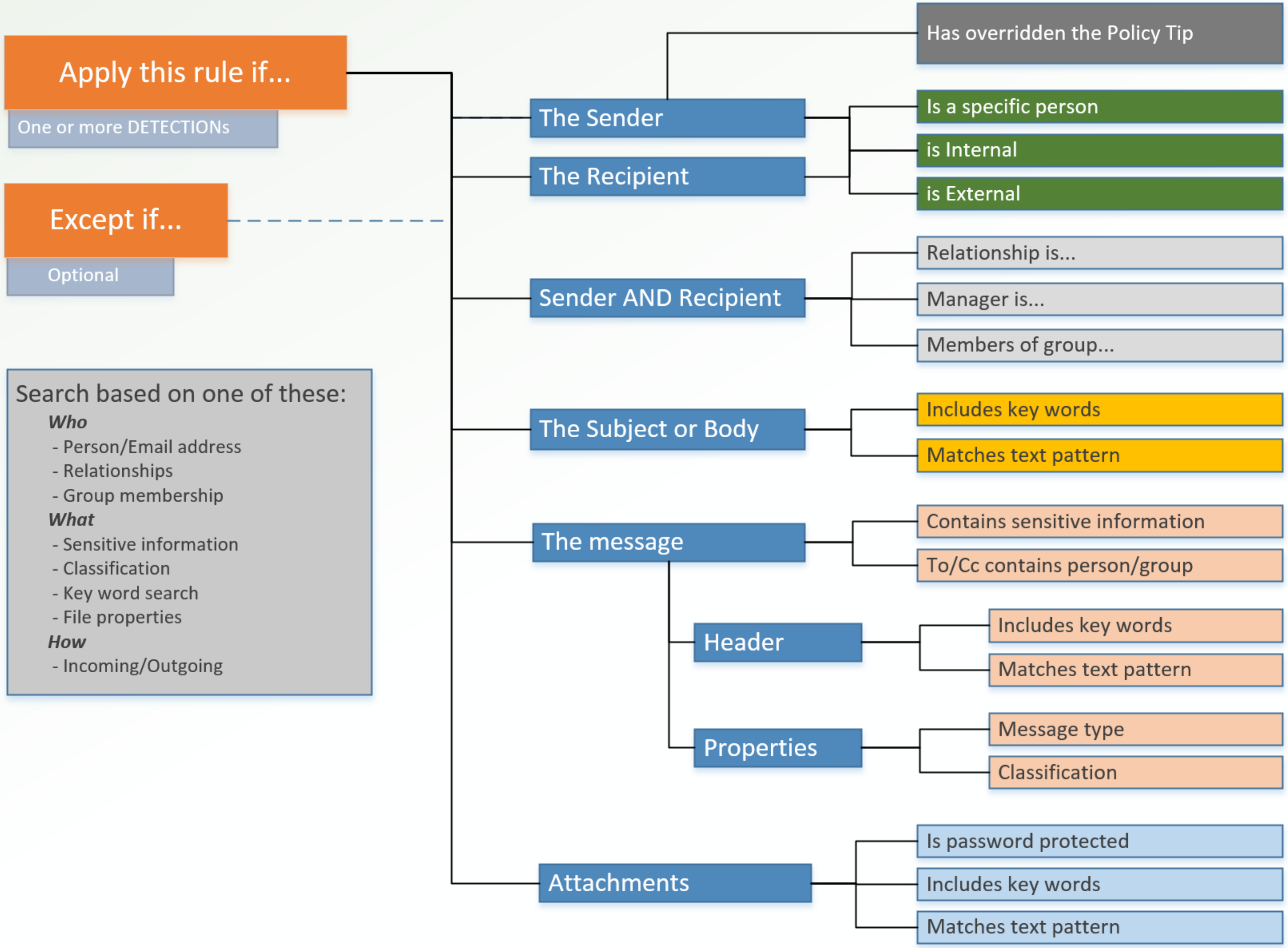
Send incident report to: *Select one..., with content: *Include message properties

ender to override with

Select one
Forward the message for approval...
Redirect the message to...
Block the message...
Add recipients...
Apply a disclaimer to the message...
Modify the message properties...
Modify the message security...
Prepend the subject of the message with...
Notify the sender with a Policy Tip...
Generate incident report and send it to...
Apply rights protection
Require TLS encryption
Apply Office 365 Message Encryption
Remove Office 365 Message Encryption
Select one
add action
Except if...
add exception

Exchange Online – Data Loss Prevention (**DLP**)

DETECTION



Apply this rule if...

One or more DETECTIONs

Except if...

Optional

- The Sender
  - Has overridden the Policy Tip
  - Is a specific person
  - is Internal
  - is External
- The Recipient
  - Is a specific person
  - is Internal
  - is External
- Sender AND Recipient
  - Relationship is...
  - Manager is...
  - Members of group...
- The Subject or Body
  - Includes key words
  - Matches text pattern
- The message
  - Contains sensitive information
  - To/Cc contains person/group
  - Header
    - Includes key words
    - Matches text pattern
  - Properties
    - Message type
    - Classification
- Attachments
  - Is password protected
  - Includes key words
  - Matches text pattern

Search based on one of these:

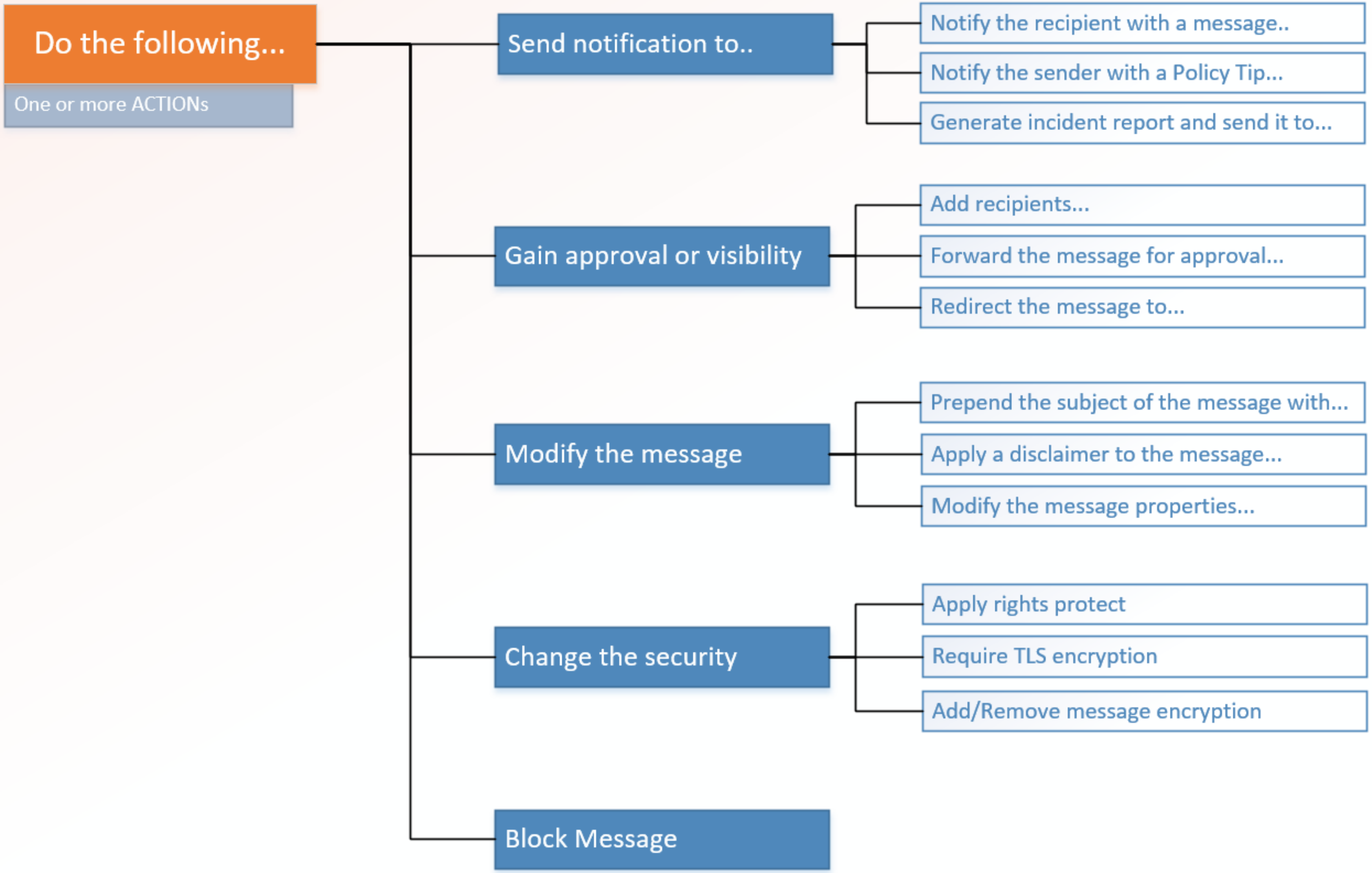
Who
- Person/Email address
- Relationships
- Group membership

What
- Sensitive information
- Classification
- Key word search
- File properties

How
- Incoming/Outgoing

Exchange Online – Data Loss Prevention (DLP)

ACTION



Do the following…

One or more ACTIONs

Send notification to..

- Notify the recipient with a message..
- Notify the sender with a Policy Tip…
- Generate incident report and send it to…

Gain approval or visibility

- Add recipients…
- Forward the message for approval…
- Redirect the message to…

Modify the message

- Prepend the subject of the message with…
- Apply a disclaimer to the message…
- Modify the message properties…

Change the security

- Apply rights protect
- Require TLS encryption
- Add/Remove message encryption

Block Message

Advanced Security Technologies

Cloud App Security (aka Adallom)

Cloud App Security

- Snowden
- Panama

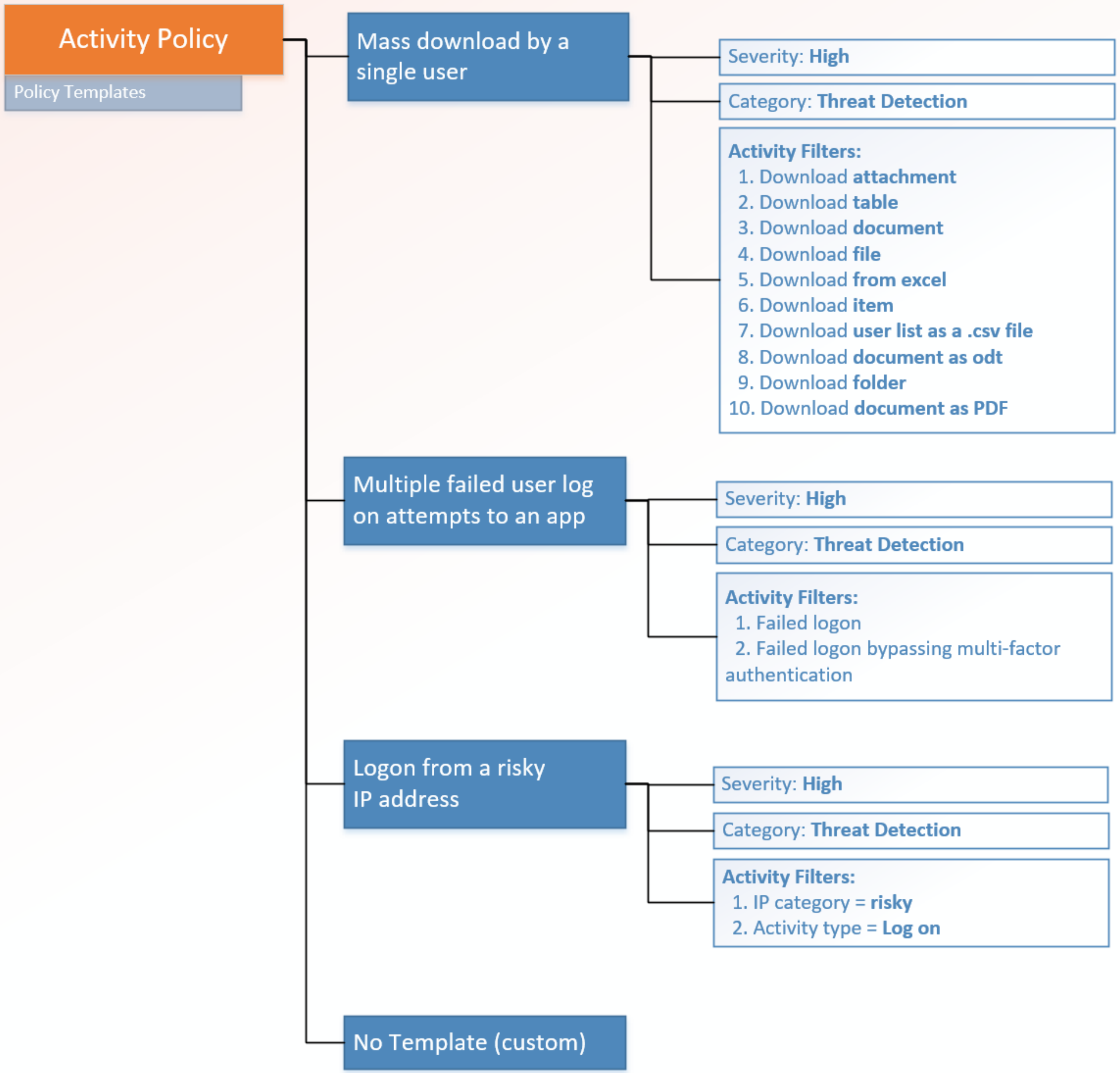
Cloud App Security

Manage advanced alerts

Your subscription allows you to use Advanced Security Management!

- Create alerts for user and admin activity
- Create alerts for anomalous and suspicious behaviour
- Respond to issues through actions like notifying or suspending users

Office 365 – Cloud App Security (**CAS**)



Activity Policy

Policy Templates

Mass download by a single user

- Severity: **High**
- Category: **Threat Detection**
- **Activity Filters:**
  1. Download **attachment**
  2. Download **table**
  3. Download **document**
  4. Download **file**
  5. Download **from excel**
  6. Download **item**
  7. Download **user list as a .csv file**
  8. Download **document as odt**
  9. Download **folder**
  10. Download **document as PDF**

Multiple failed user log on attempts to an app

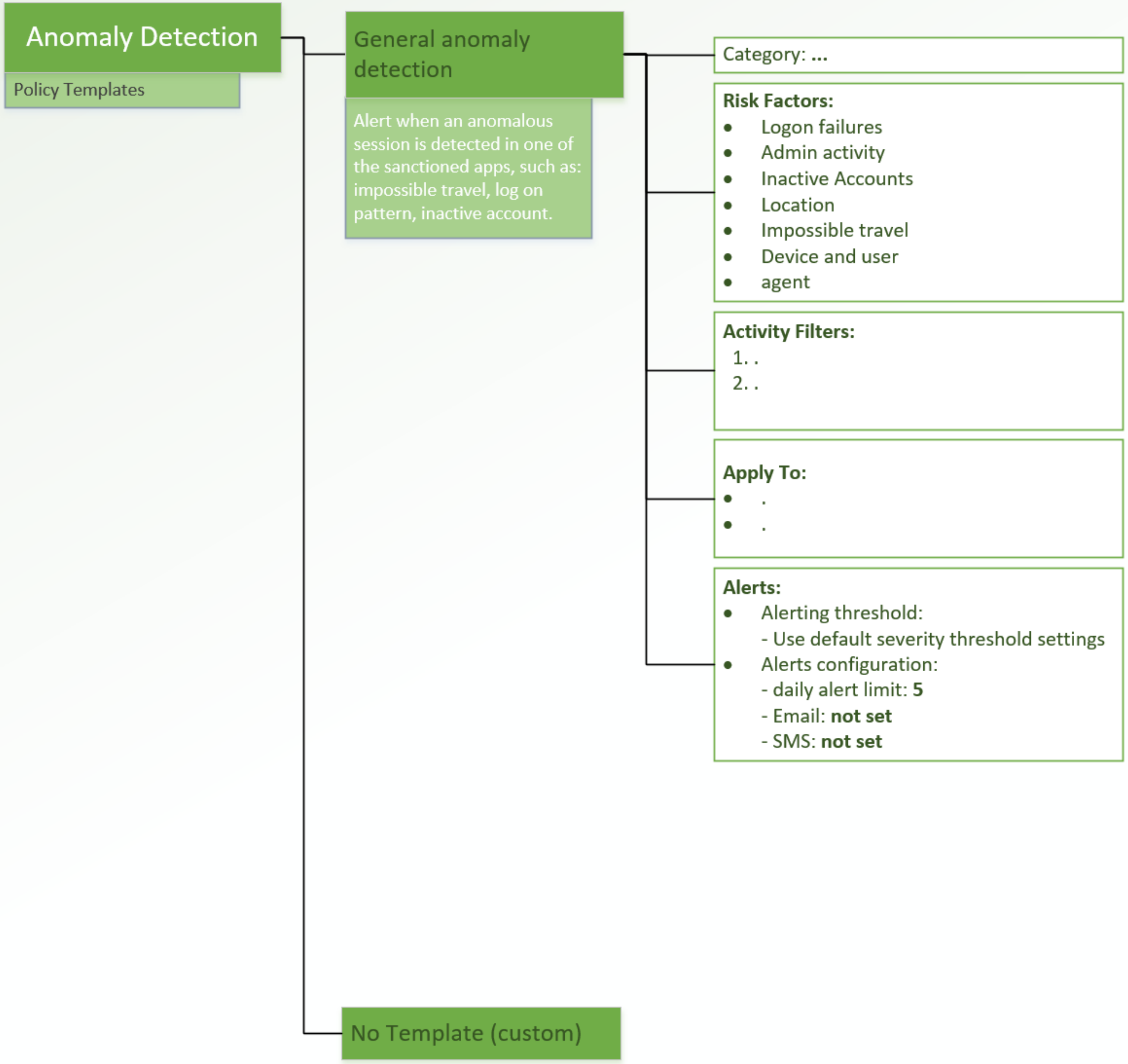
- Severity: **High**
- Category: **Threat Detection**
- **Activity Filters:**
  1. Failed logon
  2. Failed logon bypassing multi-factor authentication

Logon from a risky IP address

- Severity: **High**
- Category: **Threat Detection**
- **Activity Filters:**
  1. IP category = **risky**
  2. Activity type = **Log on**

No Template (custom)

Office 365 – Cloud App Security (**CAS**)



Anomaly Detection

Policy Templates

General anomaly detection

Alert when an anomalous session is detected in one of the sanctioned apps, such as: impossible travel, log on pattern, inactive account.

Category: **...**

Risk Factors:

- Logon failures
- Admin activity
- Inactive Accounts
- Location
- Impossible travel
- Device and user
- agent

Activity Filters:

1. .
2. .

Apply To:

- .
- .

Alerts:

- Alerting threshold:
  - Use default severity threshold settings
- Alerts configuration:
  - daily alert limit: **5**
  - Email: **not set**
  - SMS: **not set**

No Template (custom)

Questions

www.ignia.com.au

08 9365 8400

info@ignia.com.au

Perth | Melbourne | Sydney

ignia