Microsoft Purview
- Four steps to data protection

Jukka Outinen 15.1.2026

MSUGFI #14

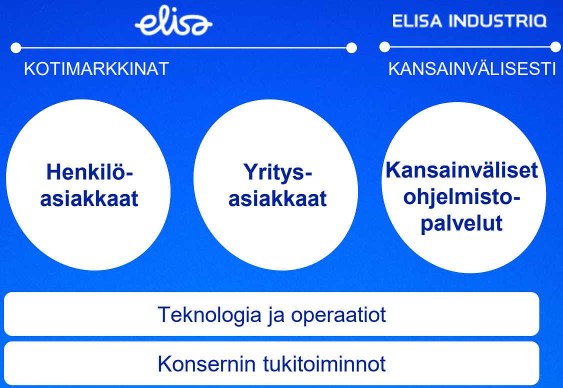
A SUSTAINABLE
FUTURE THROUGH
DIGITALISATION

Elisa lyhyesti

2,8 milj.
asiakasta

2,2 mrd €
liikevaihto 2024

6 700 elisalaista yli 20 maassa



Markkina-asema:

#1 Suomessa

#2 Virossa

Yli 140 vuoden osaamisella

Päämarkkinoillemme

- IT-palvelut
- Kyberturvapalvelut
- Tietoliikennepalvelut
- Viihtymisen palvelut

Kansainvälisille markkinoille

- Telecom-ohjelmistot
- Teollisuuden ohjelmistot
- Energianhallintaohjelmistot

- 25 years with IT
  - 10+ years as entrepreneur
  - 10 years at Elisa – Consultant & team manager
- Focus on Microsoft 365
  - Data protection, cyber security, tenant-to-tenant migrations
  - Technical workshops for Purview and Defender Suites

Jukka Outinen

Lead Technical Consultant

Microsoft 365 Certified: (Enterprise) Administrator Expert
Microsoft Certified: Information Security Administrator Associate

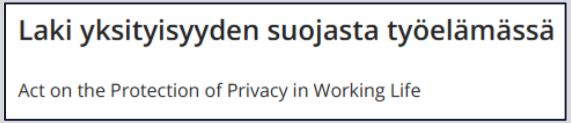
Microsoft 365 ~~Certified~~ Retired: Security Administrator Associate
Microsoft ~~Certified~~ Retired: Information Protection and Compliance Administrator Associate

https://www.linkedin.com/in/jukkaoutinen/

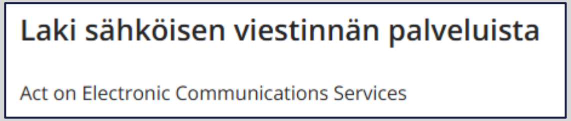
Cyber security vs. data security

Cyber Security	Data Security
Protects identities, systems and networks	Protects information
Evaluates threat actor	Evaluates data sensitivity
Common best practices are available	Industry-based implementation
Dynamic threat landscape	Assets are relatively static
Tools operate in real time	Protection policies are based on processes and data lifecycle
Requires constant monitoring	Alerting can be enabled for certain applications
Ownership = SecOps	Ownership = ?
Microsoft Defender	**Microsoft Purview**

How to plan data security controls?


Laki yksityisyyden suojasta työelämässä

Act on the Protection of Privacy in Working Life


Laki sähköisen viestinnän palveluista

Act on Electronic Communications Services

1. **Data discovery**
   - **What** you need to protect
   - **Where** it is located
2. **Risk assessment**
   - Evaluate the impact of data loss or data leak
3. **Governance policies**
   - Define user policies for data handling and sharing.

     Arrange end user training
   - Define administrative roles and responsibilities
4. **Data Classification**
   - Tag sensitive files
5. **Deployment of preventative controls**
   - Access control, DLP, encryption, backup, alerting, lifecycle management
6. **Regulatory requirements**
   - Stay compliant with GDPR / NIS2 / DORA, etc.
   - Don’t forget the local legislation

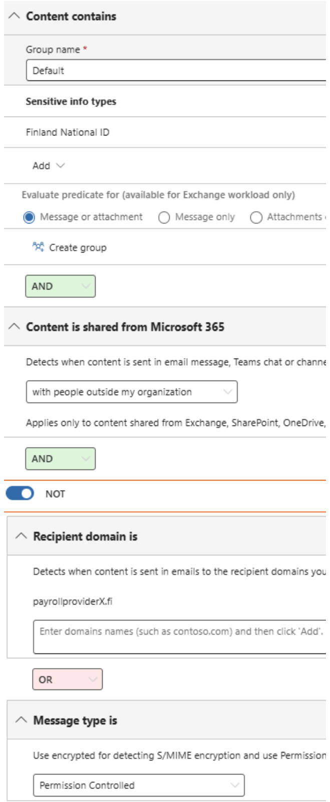
Step 1: My first DLP

- Prevent oversharing of business / personal data
- Deploy Data Loss Prevention using pre-defined information types

DEMO: create a basic DLP policy

- Prevent sending Finnish National ID to external recipients by email
- But
  - Allow sending as encrypted to anyone
  - Encrypt automatically if sent to payroll provider

DEMO: create a basic DLP policy



Content contains

Group name *

Default

Sensitive info types

Finland National ID

Add

Evaluate predicate for (available for Exchange workload only)

● Message or attachment ○ Message only ○ Attachments

Create group

AND

Content is shared from Microsoft 365

Detects when content is sent in email message, Teams chat or channe

with people outside my organization

Applies only to content shared from Exchange, SharePoint, OneDrive,

AND

NOT: On

Recipient domain is

Detects when content is sent in emails to the recipient domains you

payrollproviderX.fi

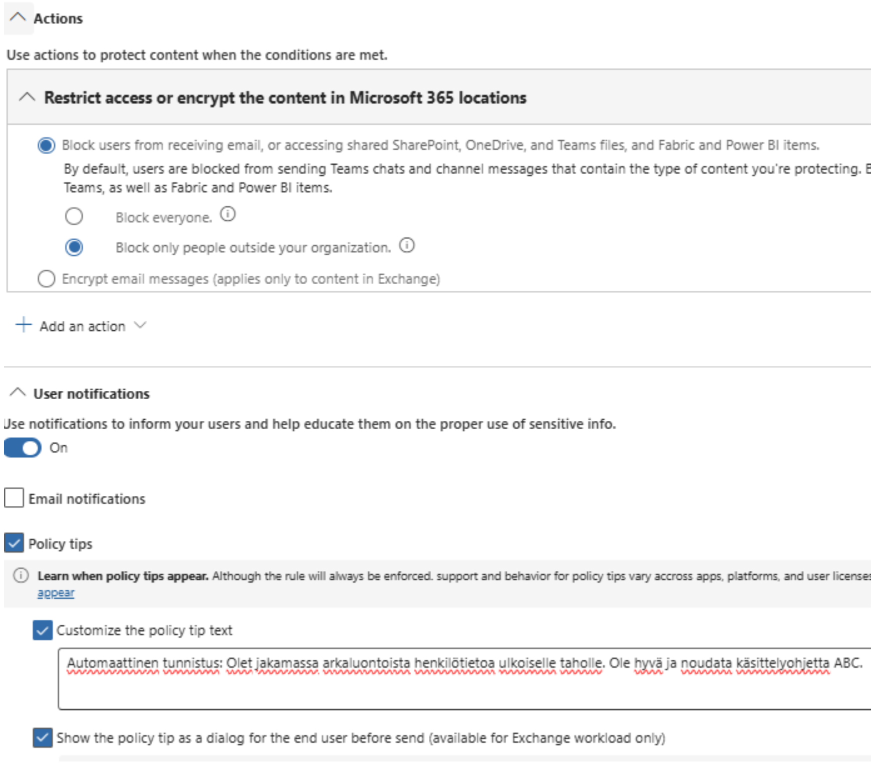
Enter domains names (such as contoso.com) and then click 'Add'.

OR

Message type is

Use encrypted for detecting S/MIME encryption and use Permission

Permission Controlled



Actions

Use actions to protect content when the conditions are met.

Restrict access or encrypt the content in Microsoft 365 locations

● Block users from receiving email, or accessing shared SharePoint, OneDrive, and Teams files, and Fabric and Power BI items.

By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. E Teams, as well as Fabric and Power BI items.

○ Block everyone.

● Block only people outside your organization.

○ Encrypt email messages (applies only to content in Exchange)

Add an action

User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

On

□ Email notifications

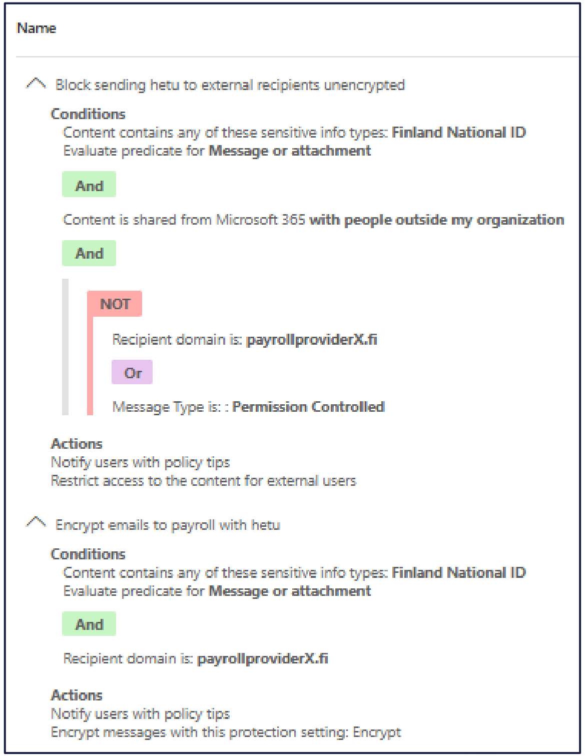
☑ Policy tips

Learn when policy tips appear. Although the rule will always be enforced. support and behavior for policy tips vary accross apps, platforms, and user license appear

☑ Customize the policy tip text

Automaattinen tunnistus: Olet jakamassa arkaluontoista henkilötietoa ulkoiselle taholle. Ole hyvä ja noudata käsittelyohjetta ABC.

☑ Show the policy tip as a dialog for the end user before send (available for Exchange workload only)



Name

Block sending hetu to external recipients unencrypted

Conditions

Content contains any of these sensitive info types: **Finland National ID**
Evaluate predicate for **Message or attachment**

And

Content is shared from Microsoft 365 **with people outside my organization**

And

NOT

Recipient domain is: **payrollproviderX.fi**

Or

Message Type is: : **Permission Controlled**

Actions

Notify users with policy tips
Restrict access to the content for external users

Encrypt emails to payroll with hetu

Conditions

Content contains any of these sensitive info types: **Finland National ID**
Evaluate predicate for **Message or attachment**

And

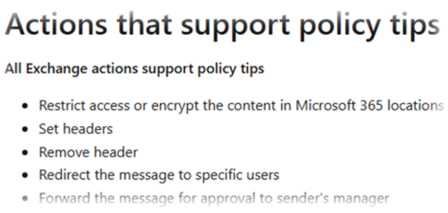
Recipient domain is: **payrollproviderX.fi**

Actions

Notify users with policy tips
Encrypt messages with this protection setting: Encrypt

Where are my DLP policy tips?

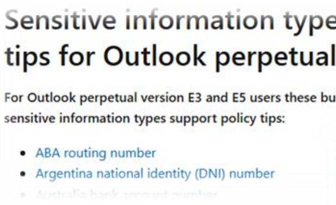
Policy Tips will not be displayed in the classic Outlook client for DLP policies scoped to non-mail enabled security groups but rule actions will be enforced.



Actions that support policy tips

All Exchange actions support policy tips

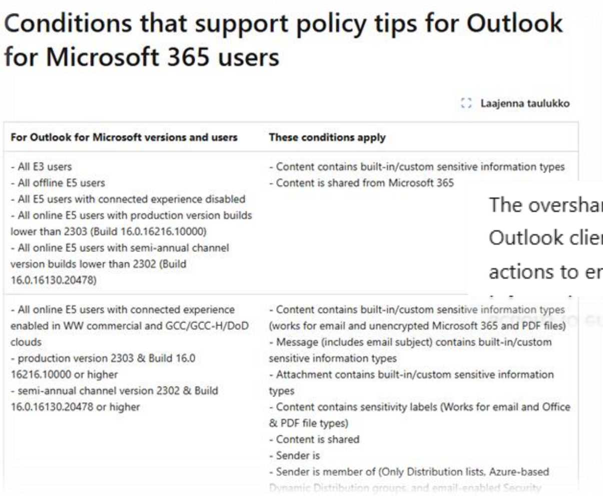
- Restrict access or encrypt the content in Microsoft 365 locations
- Set headers
- Remove header
- Redirect the message to specific users
- Forward the message for approval to sender's manager



Sensitive information types that support policy tips for Outlook perpetual users

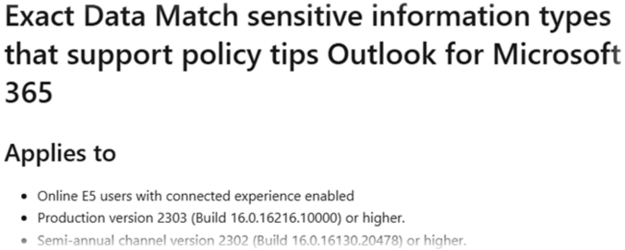
For Outlook perpetual version E3 and E5 users these built-in sensitive information types and custom sensitive information types support policy tips:

- ABA routing number
- Argentina national identity (DNI) number
- Australia bank account number



Conditions that support policy tips for Outlook for Microsoft 365 users

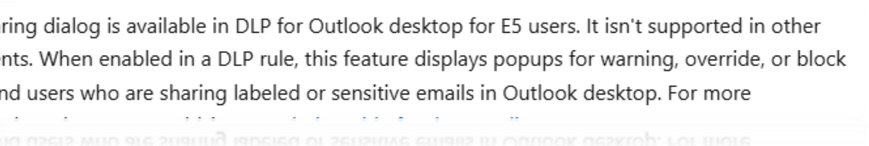
For Outlook for Microsoft versions and users	These conditions apply
- All E3 users - All offline E5 users - All E5 users with connected experience disabled - All online E5 users with production version builds lower than 2303 (Build 16.0.16216.10000) - All online E5 users with semi-annual channel version builds lower than 2302 (Build 16.0.16130.20478)	- Content contains built-in/custom sensitive information types - Content is shared from Microsoft 365
- All online E5 users with connected experience enabled in WW commercial and GCC/GCC-H/DoD clouds - production version 2303 & Build 16.0 16216.10000 or higher - semi-annual channel version 2302 & Build 16.0.16130.20478 or higher	- Content contains built-in/custom sensitive information types (works for email and unencrypted Microsoft 365 and PDF files) - Message (includes email subject) contains built-in/custom sensitive information types - Attachment contains built-in/custom sensitive information types - Content contains sensitivity labels (Works for email and Office & PDF file types) - Content is shared - Sender is - Sender is member of (Only Distribution lists, Azure-based Dynamic Distribution groups, and email-enabled Security



Exact Data Match sensitive information types that support policy tips Outlook for Microsoft 365

Applies to

- Online E5 users with connected experience enabled
- Production version 2303 (Build 16.0.16216.10000) or higher.
- Semi-annual channel version 2302 (Build 16.0.16130.20478) or higher.



The oversharing dialog is available in DLP for Outlook desktop for E5 users. It isn't supported in other Outlook clients. When enabled in a DLP rule, this feature displays popups for warning, override, or block actions to end users who are sharing labeled or sensitive emails in Outlook desktop. For more

https://learn.microsoft.com/fi-fi/purview/dlp-ol365-win32-policy-tips

Step 2: Custom SIT and data classification

- Customize Sensitive Information types per organization requirements and enhance DLP protection
- Plan and deploy data classification model using sensitivity labels
- Integrate DLP policies with classification information

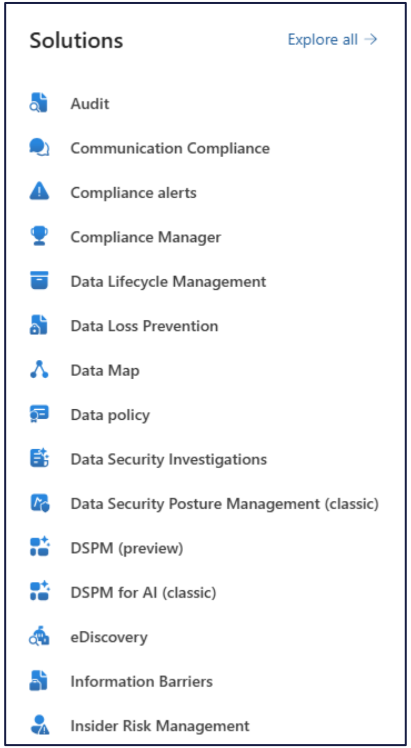
What are Sensitive Information Types (SIT)?

- Pattern-based classifier
- Used for defining certain content in a file or email message
- Several formats available depending on licenses

https://learn.microsoft.com/en-us/purview/sit-sensitive-information-type-learn-about

Single SIT → Used in different Purview solutions

- Information Protection (MIP)
- Data Loss Prevention (DLP)
- Data lifecycle management
- Insider Risk Management (IRM)
- eDiscovery
- Communication Compliance



Solutions Explore all →

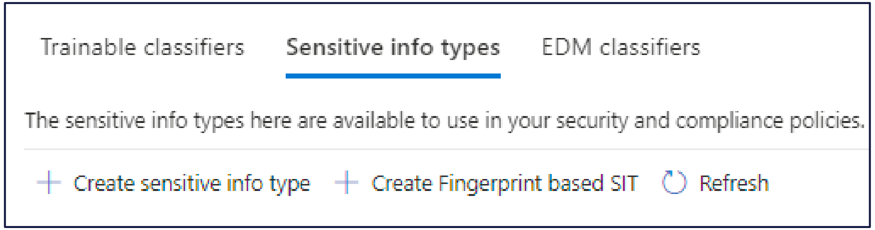
- Audit
- Communication Compliance
- Compliance alerts
- Compliance Manager
- Data Lifecycle Management
- Data Loss Prevention
- Data Map
- Data policy
- Data Security Investigations
- Data Security Posture Management (classic)
- DSPM (preview)
- DSPM for AI (classic)
- eDiscovery
- Information Barriers
- Insider Risk Management

M365 – Different info types

- Built-in sensitive info type
- Custom sensitive info type
- Trainable classifier
- Document fingerprint
- Exact data match

Pre-configured data models

- National ID
- Credit card number
- Postal addresses
- Full names
- Passwords and credentials (app secret, S3 storage ym.)



The sensitive info types here are available to use in your security and compliance policies.

M365 - Different info types

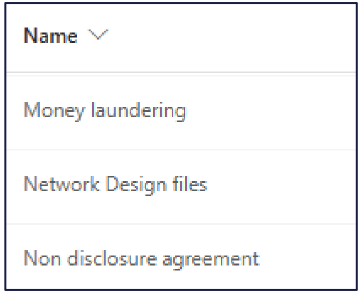
- Built-in sensitive info type
- Custom sensitive info type
- Trainable classifier
- Document fingerprint
- Exact data match

Custom data models

- Customer number
- Project code
- keywords

M365 - Different info types

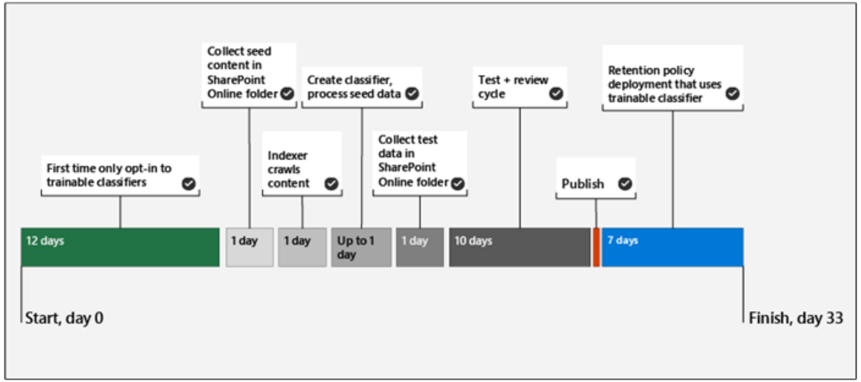
- Built-in sensitive info type
- Custom sensitive info type
- Trainable classifier
- Document fingerprint
- Exact data match



Name
Money laundering
Network Design files
Non disclosure agreement

Identify items of different categories

- Machine learning
- Feed with 50-500 sample documents
- Test the logic and give feedback for getting better results



First time only opt-in to trainable classifiers ✓
Collect seed content in SharePoint Online folder ✓
Indexer crawls content ✓
Create classifier, process seed data ✓
Collect test data in SharePoint Online folder ✓
Test + review cycle ✓
Publish ✓
Retention policy deployment that uses trainable classifier ✓
12 days
1 day
1 day
Up to 1 day
1 day
10 days
7 days
Start, day 0
Finish, day 33

M365 - Different info types

- Built-in sensitive info type
- Custom sensitive info type
- Trainable classifier
- Document fingerprint
- Exact data match

Based on document template

- Patent applications
- Patient records
- HR documents
- Health documents
- Partial or complete match

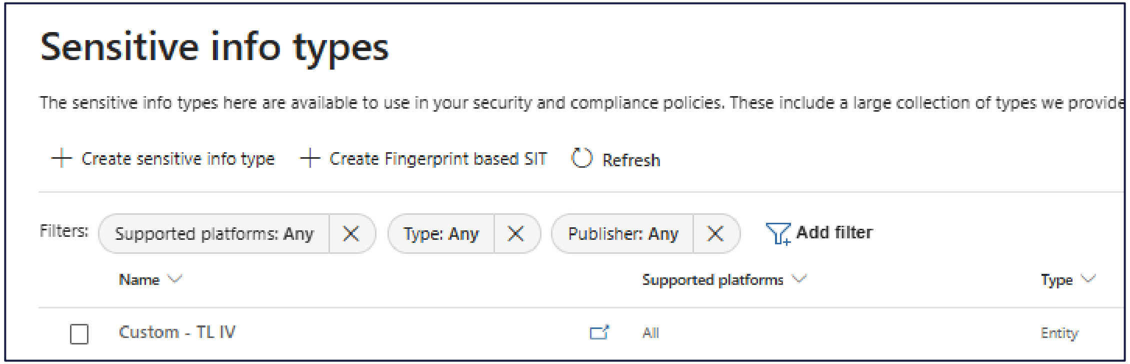
M365 - Different info types

- Built-in sensitive info type
- Custom sensitive info type
- Trainable classifier
- Document fingerprint
- Exact data match →

Comparison with master database

- Patient register
- Customer register
- Personnel list
- List of patents or inventions
- Property list

DEMO: create a custom SIT



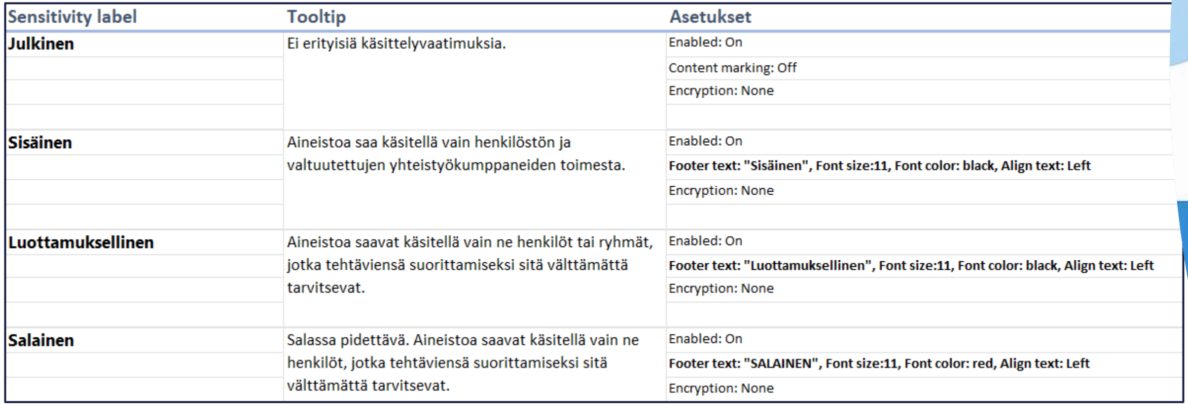
Sensitive info types

The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we provide

Filters: Supported platforms: Any ✕ Type: Any ✕ Publisher: Any ✕

	Name	Supported platforms	Type
□	Custom - TL IV	All	Entity

DEMO: create a sensitivity label

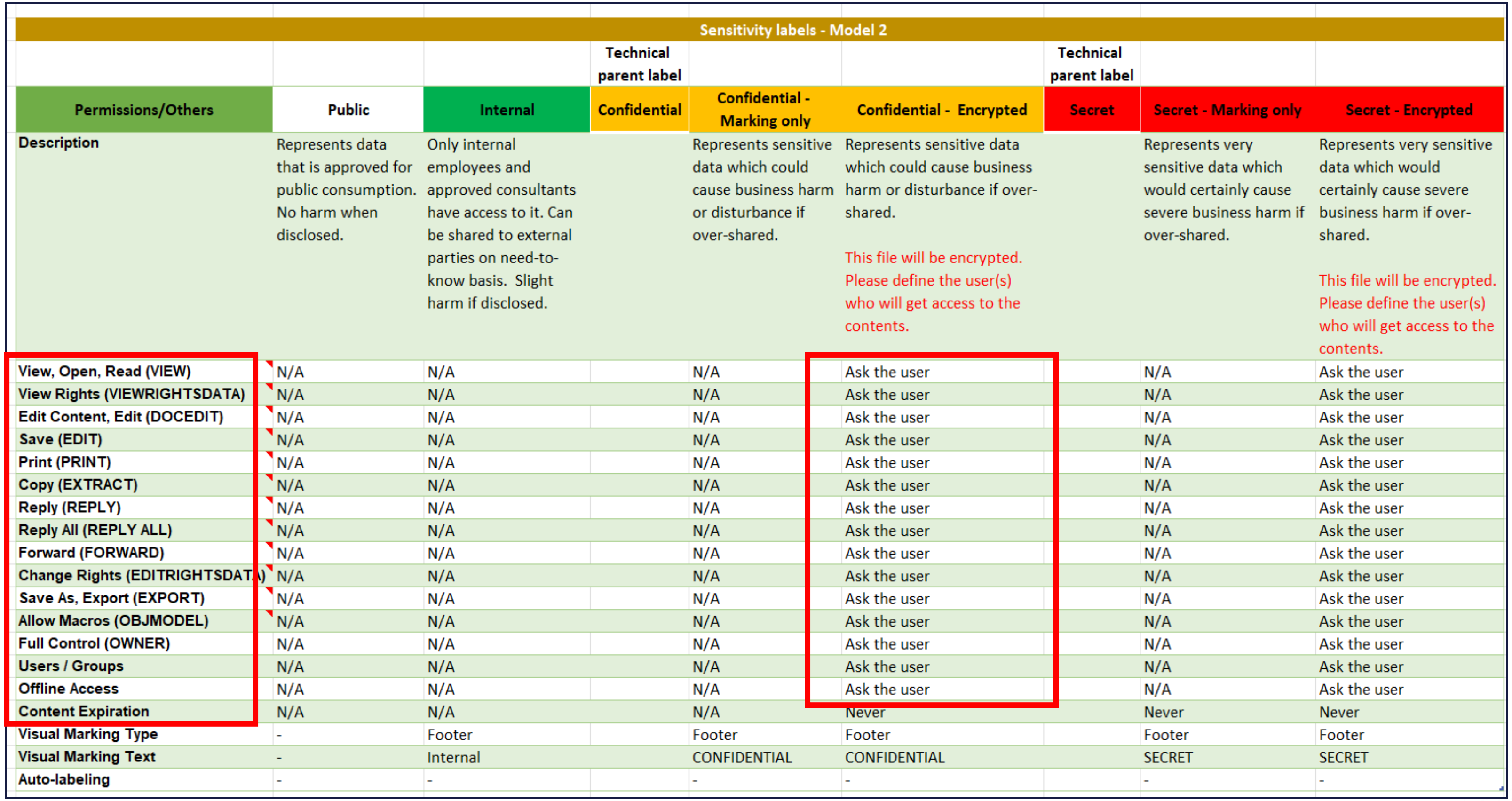


Sensitivity label	Tooltip	Asetukset
Julkinen	Ei erityisiä käsittelyvaatimuksia.	Enabled: On Content marking: Off Encryption: None
Sisäinen	Aineistoa saa käsitellä vain henkilöstön ja valtuutettujen yhteistyökumppaneiden toimesta.	Enabled: On **Footer text: "Sisäinen", Font size:11, Font color: black, Align text: Left** Encryption: None
Luottamuksellinen	Aineistoa saavat käsitellä vain ne henkilöt tai ryhmät, jotka tehtäviensä suorittamiseksi sitä välttämättä tarvitsevat.	Enabled: On **Footer text: "Luottamuksellinen", Font size:11, Font color: black, Align text: Left** Encryption: None
Salainen	Salassa pidettävä. Aineistoa saavat käsitellä vain ne henkilöt, jotka tehtäviensä suorittamiseksi sitä välttämättä tarvitsevat.	Enabled: On **Footer text: "SALAINEN", Font size:11, Font color: red, Align text: Left** Encryption: None

Step 3: Enable encryption

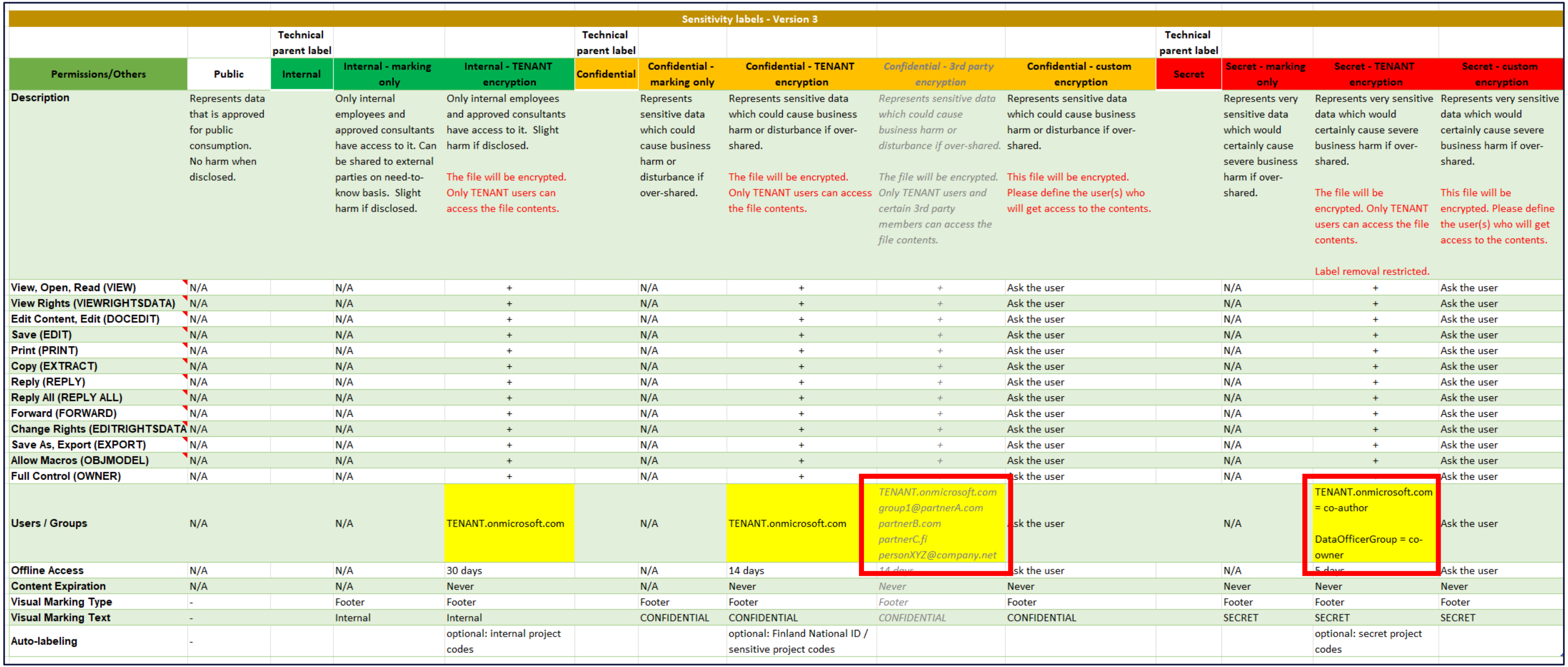
- Deploy fine-grained sensitivity labels
- Activate encryption for most sensitive data using auto-labeling

First step to encryption



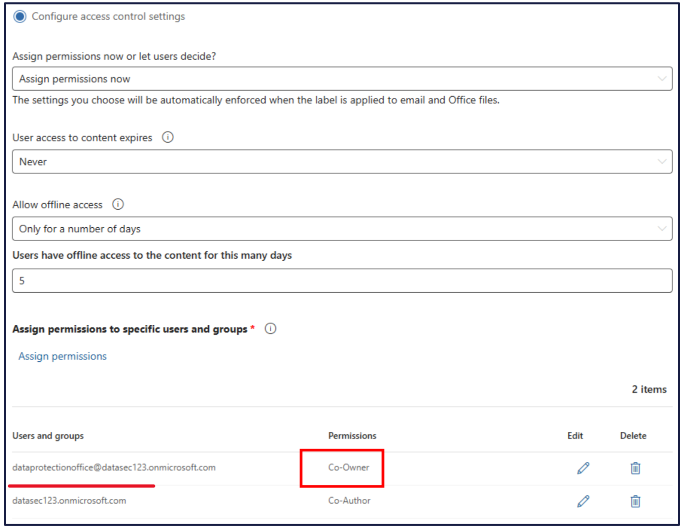
Sensitivity labels - Model 2								
			Technical parent label			Technical parent label		
Permissions/Others	Public	Internal	Confidential	Confidential - Marking only	Confidential - Encrypted	Secret	Secret - Marking only	Secret - Encrypted
Description	Represents data that is approved for public consumption. No harm when disclosed.	Only internal employees and approved consultants have access to it. Can be shared to external parties on need-to-know basis. Slight harm if disclosed.		Represents sensitive data which could cause business harm or disturbance if over-shared.	Represents sensitive data which could cause business harm or disturbance if over-shared. This file will be encrypted. Please define the user(s) who will get access to the contents.		Represents very sensitive data which would certainly cause severe business harm if over-shared.	Represents very sensitive data which would certainly cause severe business harm if over-shared. This file will be encrypted. Please define the user(s) who will get access to the contents.
View, Open, Read (VIEW)	N/A	N/A		N/A	Ask the user		N/A	Ask the user
View Rights (VIEWRIGHTSDATA)	N/A	N/A		N/A	Ask the user		N/A	Ask the user
Edit Content, Edit (DOCEDIT)	N/A	N/A		N/A	Ask the user		N/A	Ask the user
Save (EDIT)	N/A	N/A		N/A	Ask the user		N/A	Ask the user
Print (PRINT)	N/A	N/A		N/A	Ask the user		N/A	Ask the user
Copy (EXTRACT)	N/A	N/A		N/A	Ask the user		N/A	Ask the user
Reply (REPLY)	N/A	N/A		N/A	Ask the user		N/A	Ask the user
Reply All (REPLY ALL)	N/A	N/A		N/A	Ask the user		N/A	Ask the user
Forward (FORWARD)	N/A	N/A		N/A	Ask the user		N/A	Ask the user
Change Rights (EDITRIGHTSDATA)	N/A	N/A		N/A	Ask the user		N/A	Ask the user
Save As, Export (EXPORT)	N/A	N/A		N/A	Ask the user		N/A	Ask the user
Allow Macros (OBJMODEL)	N/A	N/A		N/A	Ask the user		N/A	Ask the user
Full Control (OWNER)	N/A	N/A		N/A	Ask the user		N/A	Ask the user
Users / Groups	N/A	N/A		N/A	Ask the user		N/A	Ask the user
Offline Access	N/A	N/A		N/A	Ask the user		N/A	Ask the user
Content Expiration	N/A	N/A		N/A	Never		Never	Never
Visual Marking Type	-	Footer		Footer	Footer		Footer	Footer
Visual Marking Text	-	Internal		CONFIDENTIAL	CONFIDENTIAL		SECRET	SECRET
Auto-labeling	-	-		-	-		-	-

Still trying to keep it simple…



Sensitivity labels - Version 3													
		Technical parent label			Technical parent label					Technical parent label			
Permissions/Others	Public	Internal	Internal - marking only	Internal - TENANT encryption	Confidential	Confidential - marking only	Confidential - TENANT encryption	*Confidential - 3rd party encryption*	Confidential - custom encryption	Secret	Secret - marking only	Secret - TENANT encryption	Secret - custom encryption
Description	Represents data that is approved for public consumption. No harm when disclosed.		Only internal employees and approved consultants have access to it. Can be shared to external parties on need-to-know basis. Slight harm if disclosed.	Only internal employees and approved consultants have access to it. Slight harm if disclosed. The file will be encrypted. Only TENANT users can access the file contents.		Represents sensitive data which could cause business harm or disturbance if over-shared.	Represents sensitive data which could cause business harm or disturbance if over-shared. The file will be encrypted. Only TENANT users can access the file contents.	*Represents sensitive data which could cause business harm or disturbance if over-shared.* *The file will be encrypted. Only TENANT users and certain 3rd party members can access the file contents.*	Represents sensitive data which could cause business harm or disturbance if over-shared. This file will be encrypted. Please define the user(s) who will get access to the contents.		Represents very sensitive data which would certainly cause severe business harm if over-shared.	Represents very sensitive data which would certainly cause severe business harm if over-shared. The file will be encrypted. Only TENANT users can access the file contents. Label removal restricted.	Represents very sensitive data which would certainly cause severe business harm if over-shared. This file will be encrypted. Please define the user(s) who will get access to the contents.
View, Open, Read (VIEW)	N/A		N/A	+		N/A	+	+	Ask the user		N/A	+	Ask the user
View Rights (VIEWRIGHTSDATA)	N/A		N/A	+		N/A	+	+	Ask the user		N/A	+	Ask the user
Edit Content, Edit (DOCEDIT)	N/A		N/A	+		N/A	+	+	Ask the user		N/A	+	Ask the user
Save (EDIT)	N/A		N/A	+		N/A	+	+	Ask the user		N/A	+	Ask the user
Print (PRINT)	N/A		N/A	+		N/A	+	+	Ask the user		N/A	+	Ask the user
Copy (EXTRACT)	N/A		N/A	+		N/A	+	+	Ask the user		N/A	+	Ask the user
Reply (REPLY)	N/A		N/A	+		N/A	+	+	Ask the user		N/A	+	Ask the user
Reply All (REPLY ALL)	N/A		N/A	+		N/A	+	+	Ask the user		N/A	+	Ask the user
Forward (FORWARD)	N/A		N/A	+		N/A	+	+	Ask the user		N/A	+	Ask the user
Change Rights (EDITRIGHTSDATA	N/A		N/A	+		N/A	+	+	Ask the user		N/A	+	Ask the user
Save As, Export (EXPORT)	N/A		N/A	+		N/A	+	+	Ask the user		N/A	+	Ask the user
Allow Macros (OBJMODEL)	N/A		N/A	+		N/A	+	+	Ask the user		N/A	+	Ask the user
Full Control (OWNER)	N/A		N/A	+		N/A	+		Ask the user		N/A		Ask the user
Users / Groups	N/A		N/A	TENANT.onmicrosoft.com		N/A	TENANT.onmicrosoft.com	*TENANT.onmicrosoft.com* *group1@partnerA.com* *partnerB.com* *partnerC.fi* *personXYZ@company.net*	Ask the user		N/A	TENANT.onmicrosoft.com = co-author DataOfficerGroup = co-owner	Ask the user
Offline Access	N/A		N/A	30 days		N/A	14 days	*14 days*	Ask the user		N/A	5 days	Ask the user
Content Expiration	N/A		N/A	Never		N/A	Never	*Never*	Never		Never	Never	Never
Visual Marking Type	-		Footer	Footer		Footer	Footer	*Footer*	Footer		Footer	Footer	Footer
Visual Marking Text	-		Internal	Internal		CONFIDENTIAL	CONFIDENTIAL	*CONFIDENTIAL*	CONFIDENTIAL		SECRET	SECRET	SECRET
Auto-labeling	-			optional: internal project codes			optional: Finland National ID / sensitive project codes					optional: secret project codes	

Option: restrict label downgrading



● Configure access control settings

Assign permissions now or let users decide?

Assign permissions now

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

Never

Allow offline access ⓘ

Only for a number of days

Users have offline access to the content for this many days

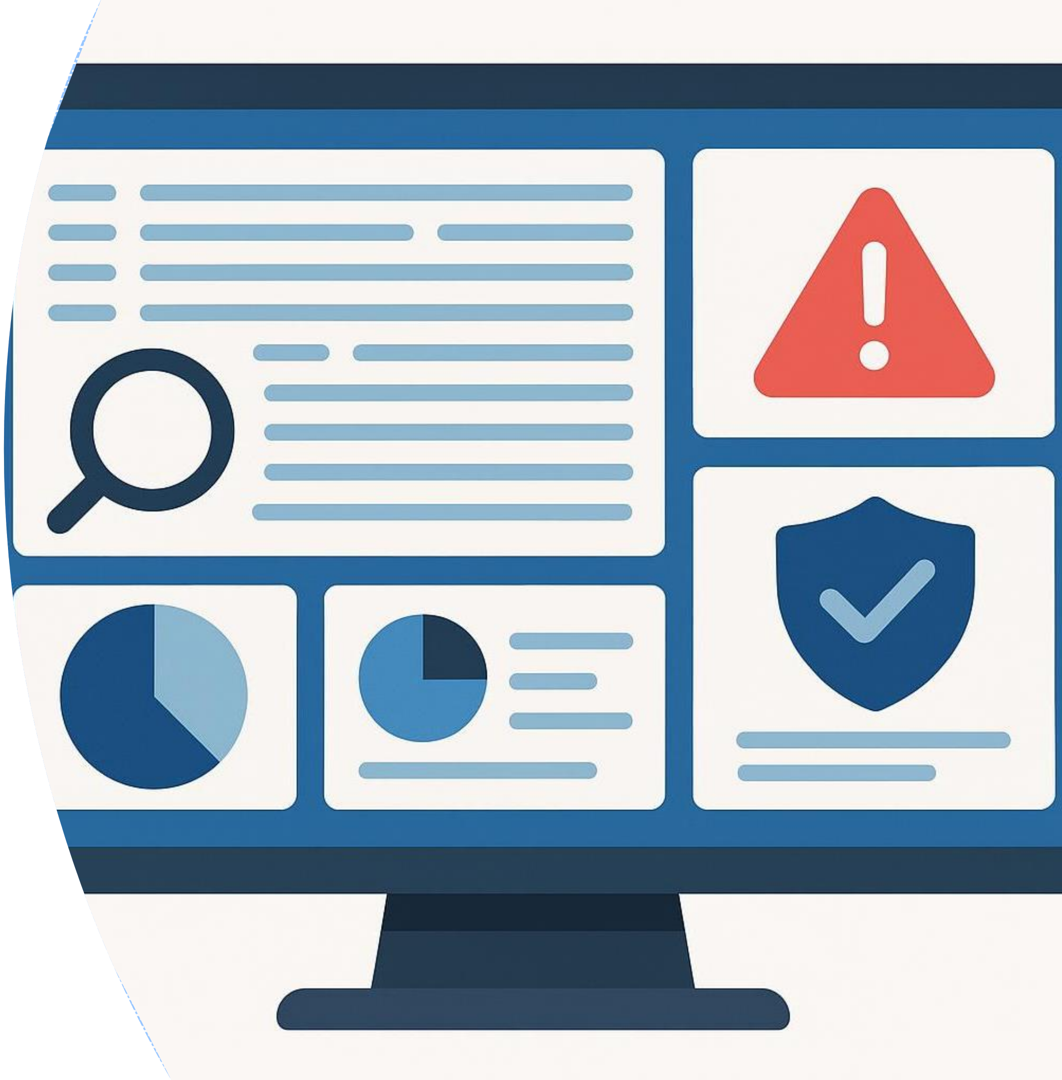
5

Assign permissions to specific users and groups * ⓘ

Assign permissions

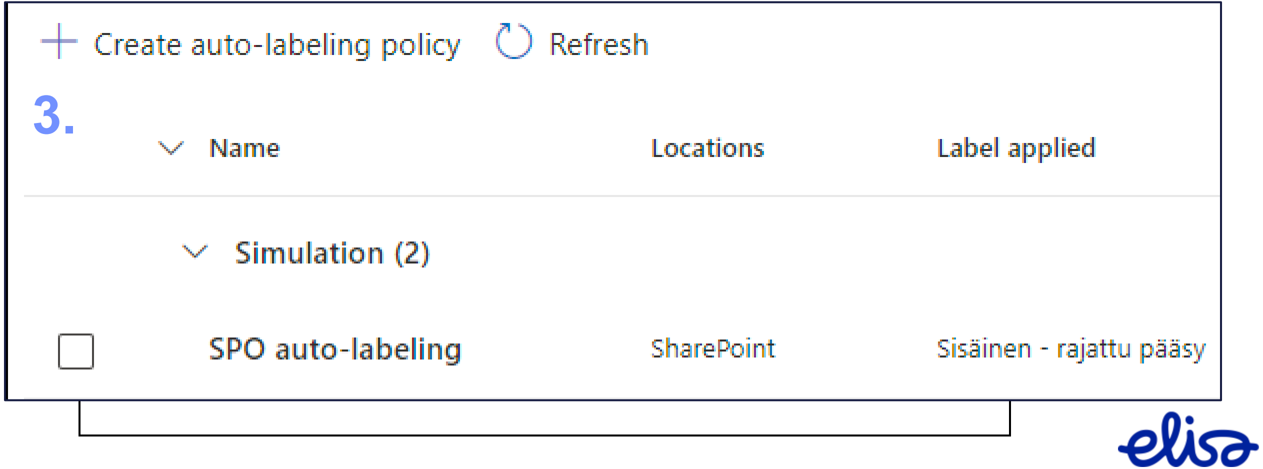
2 items

Users and groups	Permissions	Edit	Delete
dataprotectionoffice@datasec123.onmicrosoft.com	Co-Owner	✎	🗑
datasec123.onmicrosoft.com	Co-Author	✎	🗑



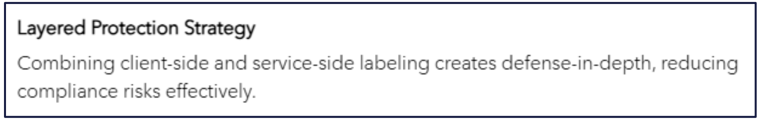
How to label automatically?

- Files can be labeled automatically based on their contents
  1. By instructing the user to choose a certain label
  2. Choosing the label for the end user
  3. Targeting the policy to a certain location
     - Sharepoint sites
     - Teams



	Name	Locations	Label applied
	Simulation (2)		
□	SPO auto-labeling	SharePoint	Sisäinen - rajattu pääsy

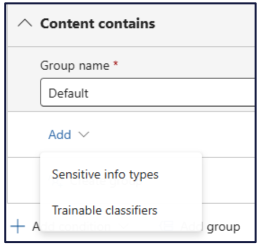
Auto-labeling comparison



Layered Protection Strategy

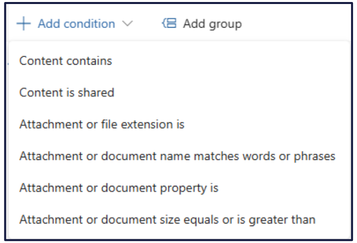
Combining client-side and service-side labeling creates defense-in-depth, reducing compliance risks effectively.

ASPECT	CLIENT-SIDE AUTO-LABELING	SERVICE-SIDE AUTO-LABELING
Where It Runs	Office apps on endpoint devices	SharePoint, OneDrive and Exchange Online for data at rest
Timing	Real-time during content creation	Asynchronous after upload/send
User Interaction	Prompts and recommendations. User has full control	Silent, no user prompts. Simulation mode for admins
Coverage	Office documents and email	Emails, SPO/OD files, Teams messages
Policy scoping	By label (for user or group)	By site, group or user



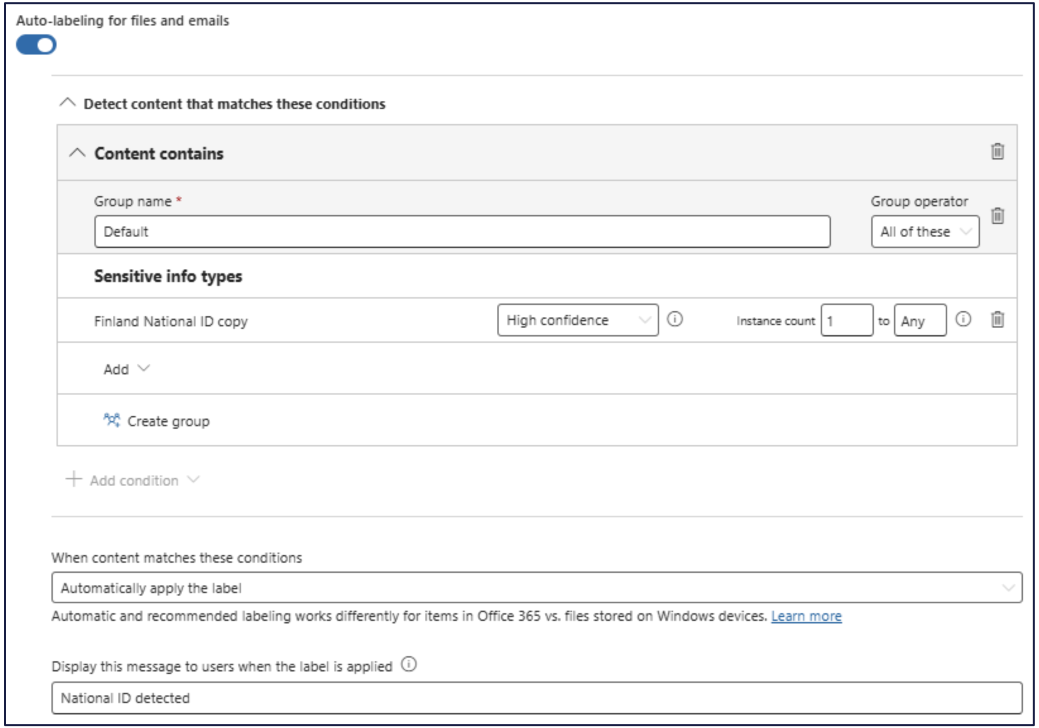
Content contains

Group name * Default



Add condition
Add group
Content contains
Content is shared
Attachment or file extension is
Attachment or document name matches words or phrases
Attachment or document property is
Attachment or document size equals or is greater than

DEMO: add client-side autolabeling



Auto-labeling for files and emails

Detect content that matches these conditions

Content contains

Group name * Default

Group operator All of these

Sensitive info types

Finland National ID copy — High confidence — Instance count 1 to Any

When content matches these conditions

Automatically apply the label

Automatic and recommended labeling works differently for items in Office 365 vs. files stored on Windows devices. Learn more

Display this message to users when the label is applied

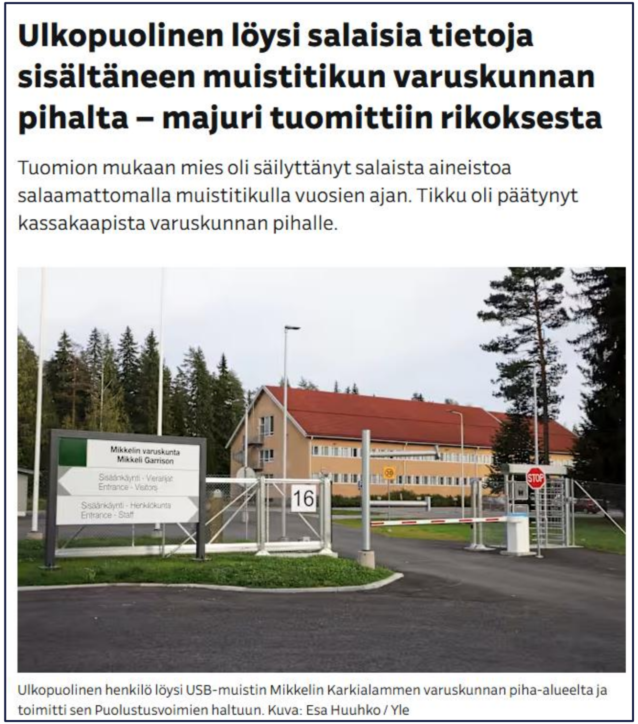
National ID detected

Step 4: Control endpoints

- Add endpoints to DLP scope

Why does it matter?

How could this have been prevented?

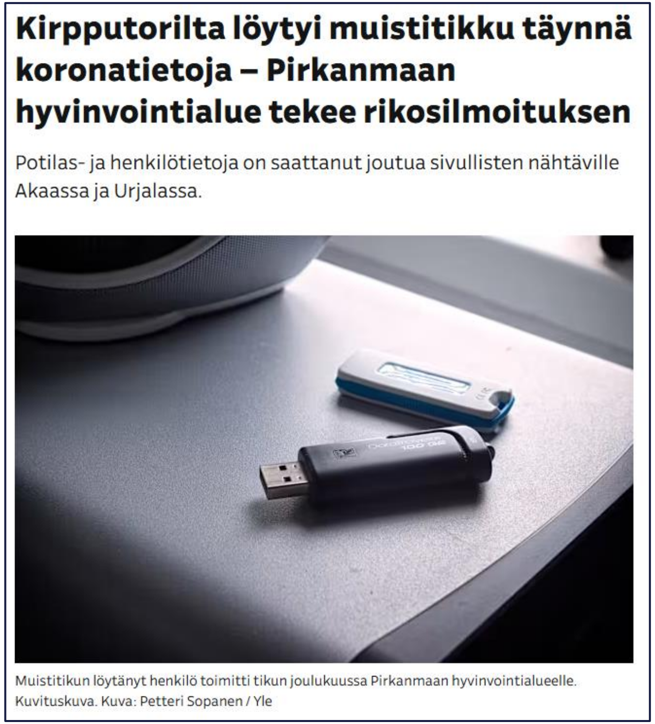


Ulkopuolinen löysi salaisia tietoja sisältäneen muistitikun varuskunnan pihalta – majuri tuomittiin rikoksesta

Tuomion mukaan mies oli säilyttänyt salaista aineistoa salaamattomalla muistitikulla vuosien ajan. Tikku oli päätynyt kassakaapista varuskunnan pihalle.

Ulkopuolinen henkilö löysi USB-muistin Mikkelin Karkialammen varuskunnan piha-alueelta ja toimitti sen Puolustusvoimien haltuun. Kuva: Esa Huuhko / Yle

https://yle.fi/a/74-20167616



Kirpputorilta löytyi muistitikku täynnä koronatietoja – Pirkanmaan hyvinvointialue tekee rikosilmoituksen

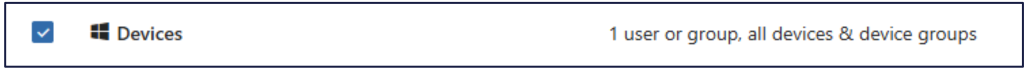
Potilas- ja henkilötietoja on saattanut joutua sivullisten nähtäville Akaassa ja Urjalassa.

Muistitikun löytänyt henkilö toimitti tikun joulukuussa Pirkanmaan hyvinvointialueelle. Kuvituskuva. Kuva: Petteri Sopanen / Yle

https://yle.fi/a/74-20204051

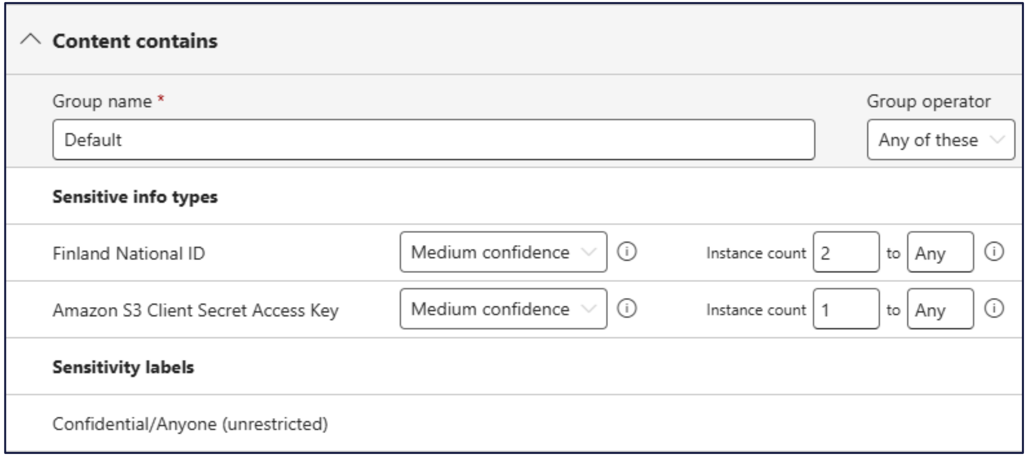
DEMO: Create endpoint DLP policy

Scope



☑ Devices — 1 user or group, all devices & device groups

Conditions



Content contains

Group name * : Default

Group operator: Any of these

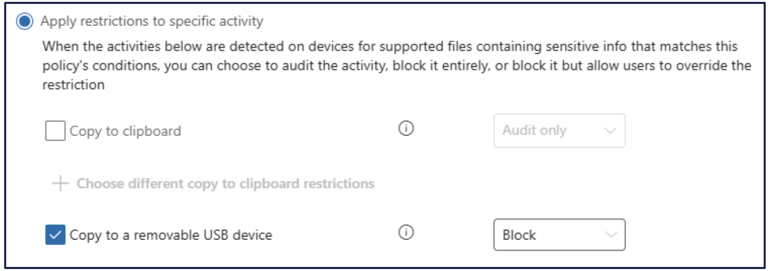
Sensitive info types

Finland National ID	Medium confidence	Instance count	2	to	Any
Amazon S3 Client Secret Access Key	Medium confidence	Instance count	1	to	Any

Sensitivity labels

Confidential/Anyone (unrestricted)

Actions



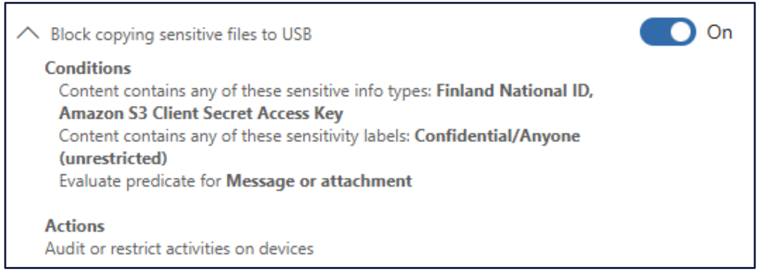
● Apply restrictions to specific activity

When the activities below are detected on devices for supported files containing sensitive info that matches this policy's conditions, you can choose to audit the activity, block it entirely, or block it but allow users to override the restriction

□ Copy to clipboard — Audit only

+ Choose different copy to clipboard restrictions

☑ Copy to a removable USB device — Block



Block copying sensitive files to USB — On

Conditions

Content contains any of these sensitive info types: **Finland National ID, Amazon S3 Client Secret Access Key**

Content contains any of these sensitivity labels: **Confidential/Anyone (unrestricted)**

Evaluate predicate for **Message or attachment**

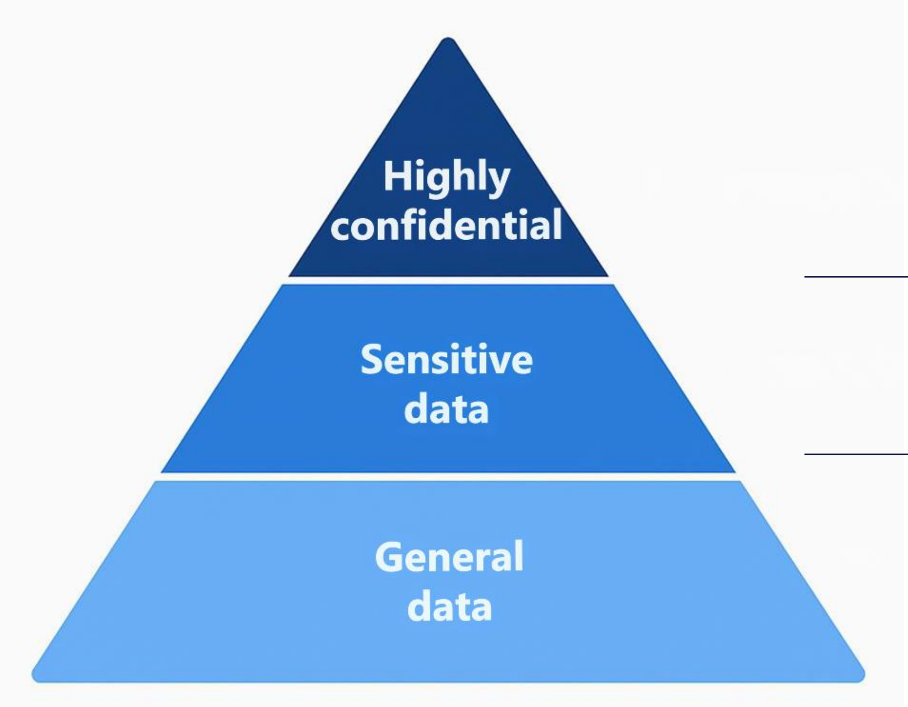
Actions

Audit or restrict activities on devices

Summary

- Don’t rush the planning phase
- Get knowledge of business requirements for data protection but also their sharing needs
- Implement custom SIT if needed
- Combine labeling and DLP

Protection per data sensitivity



- Always encrypt
- Enable DLP alerting

- Implement DKE? IRM?

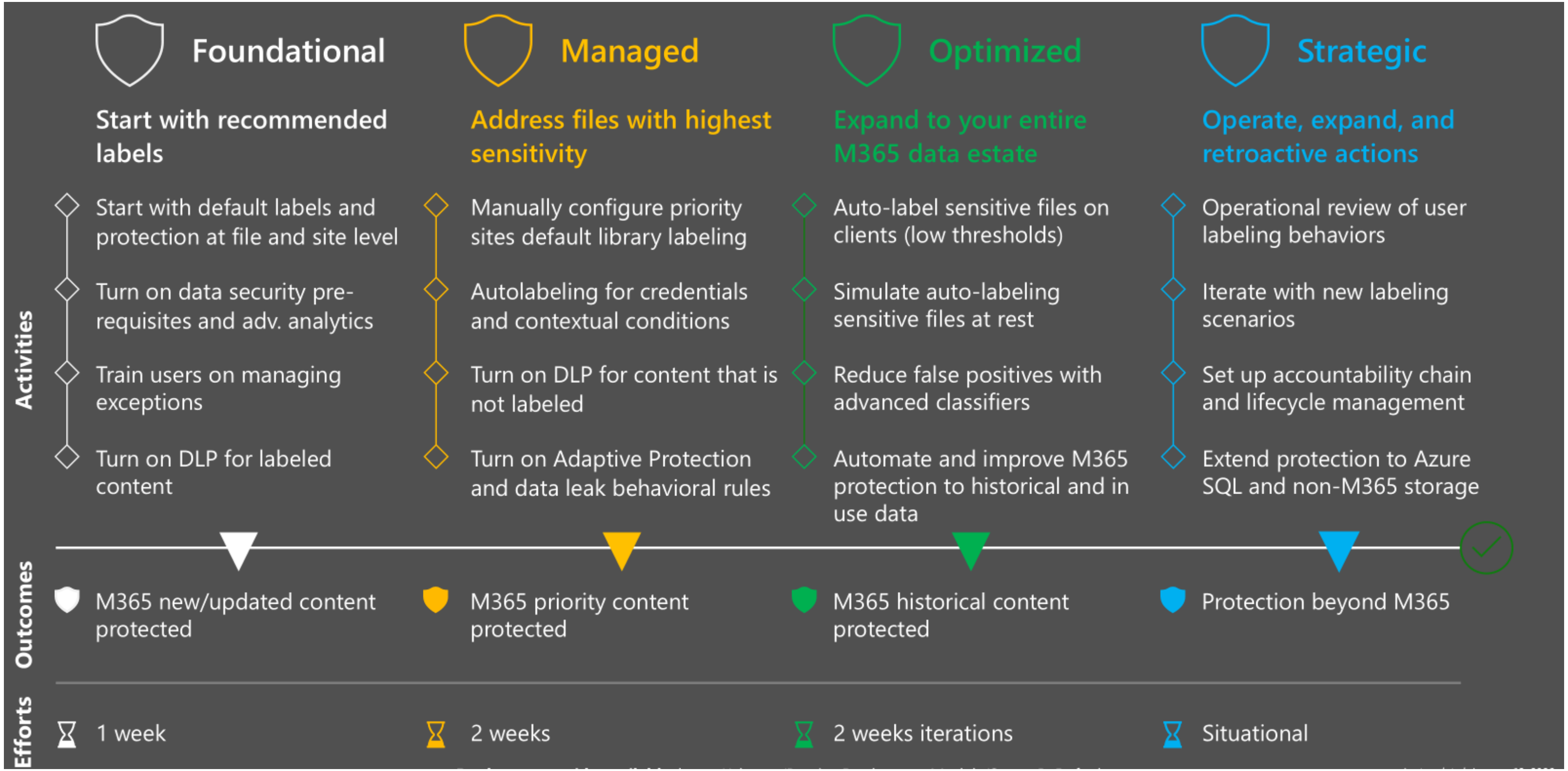
↑

- Customize sensitive information types
- Implement automatic labeling
- Protect data with DLP and/or encryption

↑

- Determine data handling rules. Arrange training for end users
- Activate lifecycle policies
  - Automate retention and deletion
  - *Data can't leak if it doesn't exist anymore*
  - Records management and backup
- Allow manual classification for new files
- Maintain access control

Secure by default with Microsoft Purview



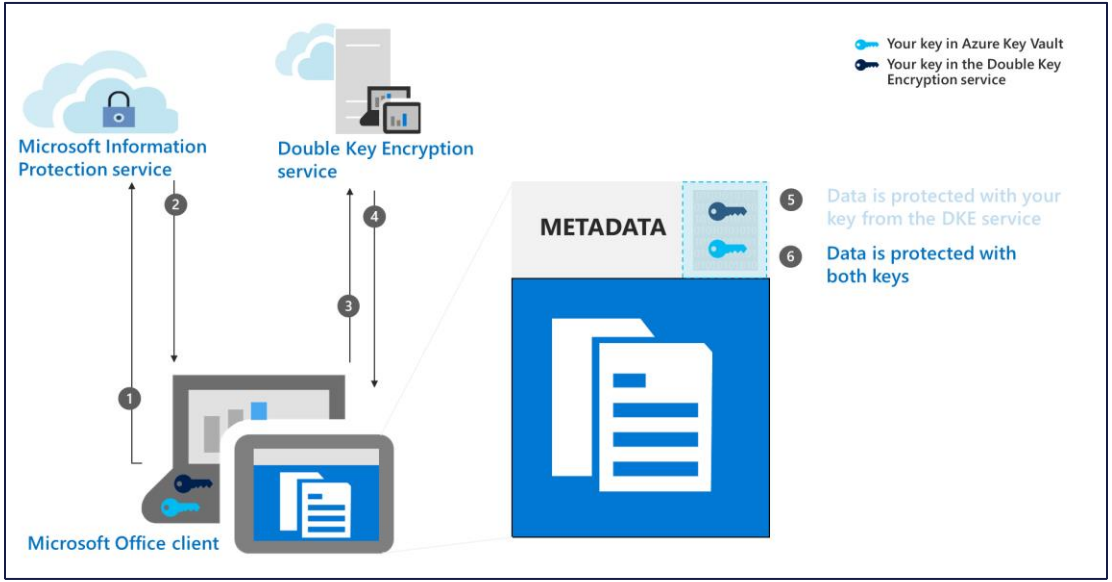
	Foundational	Managed	Optimized	Strategic
	Start with recommended labels	Address files with highest sensitivity	Expand to your entire M365 data estate	Operate, expand, and retroactive actions
Activities	Start with default labels and protection at file and site level Turn on data security pre-requisites and adv. analytics Train users on managing exceptions Turn on DLP for labeled content	Manually configure priority sites default library labeling Autolabeling for credentials and contextual conditions Turn on DLP for content that is not labeled Turn on Adaptive Protection and data leak behavioral rules	Auto-label sensitive files on clients (low thresholds) Simulate auto-labeling sensitive files at rest Reduce false positives with advanced classifiers Automate and improve M365 protection to historical and in use data	Operational review of user labeling behaviors Iterate with new labeling scenarios Set up accountability chain and lifecycle management Extend protection to Azure SQL and non-M365 storage
Outcomes	M365 new/updated content protected	M365 priority content protected	M365 historical content protected	Protection beyond M365
Efforts	1 week	2 weeks	2 weeks iterations	Situational

https://aka.ms/PurviewDeploymentModels/SecureByDefault

+ Step 5: DKE

- Double Key Encryption: encrypt the most sensitive data using your own key

DKE = Double key encryption

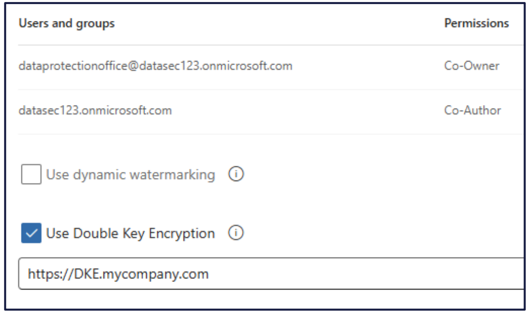

Your key in Azure Key Vault
Your key in the Double Key Encryption service
Microsoft Information Protection service
Double Key Encryption service
2
4
3
1
METADATA
5
Data is protected with your key from the DKE service
6
Data is protected with both keys
Microsoft Office client

https://learn.microsoft.com/en-us/purview/double-key-encryption

Plan & implement

- *Which data needs DKE?*
- *Which users or groups will apply these labels?*
- *What business processes require DKE-protected documents?*

Use only with content where it's truly needed



Users and groups	Permissions
dataprotectionoffice@datasec123.onmicrosoft.com	Co-Owner
datasec123.onmicrosoft.com	Co-Author

☐ Use dynamic watermarking ⓘ

☑ Use Double Key Encryption ⓘ

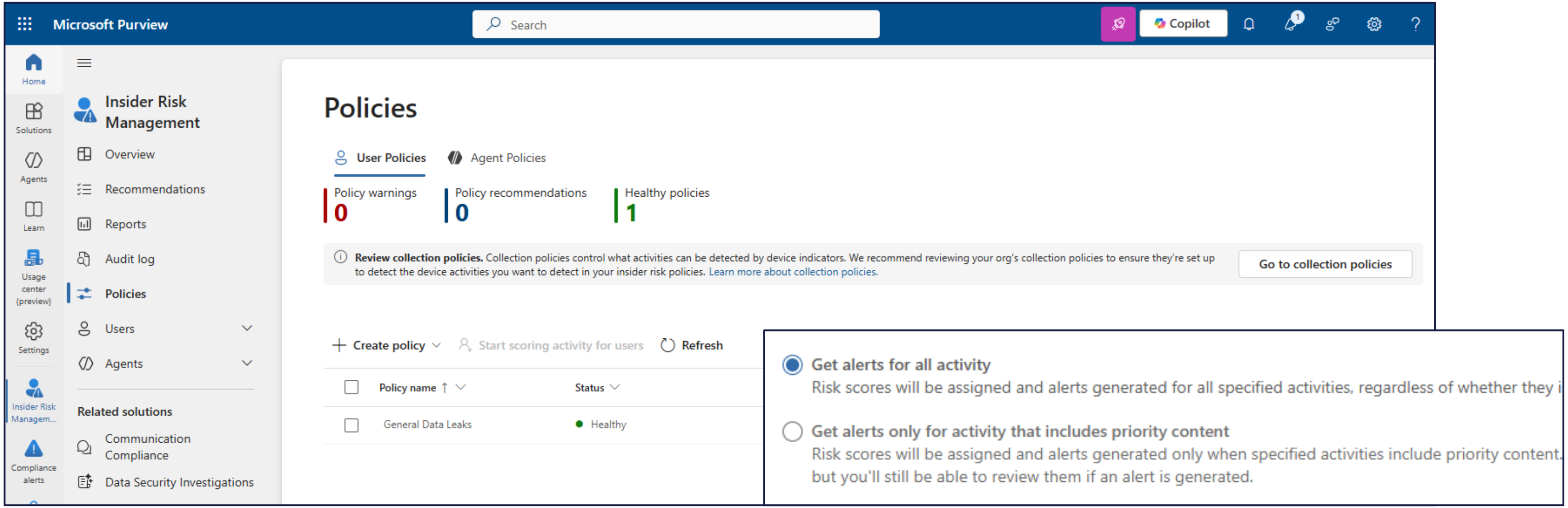
https://DKE.mycompany.com

1. Setup key store
   - On-premises IIS servers with load balancing will do
   - Generate and backup the key
2. Register DKE service
3. Maintain ACL for DKE key
4. Create new sensitivity label with DKE
5. Test and start encrypting

option: IRM

- Activate and monitor Insider Risk Management alerts
- Detect both inadvertent oversharing and malicious data theft

Detect data leak incidents with IRM



Policies

User Policies | Agent Policies

Policy warnings	Policy recommendations	Healthy policies
0	0	1

ⓘ **Review collection policies.** Collection policies control what activities can be detected by device indicators. We recommend reviewing your org's collection policies to ensure they're set up to detect the device activities you want to detect in your insider risk policies. Learn more about collection policies.

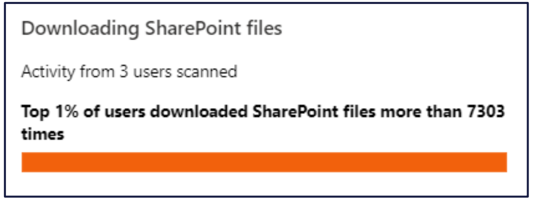
Go to collection policies

+ Create policy ⌄ | Start scoring activity for users | Refresh

□	Policy name ↑ ⌄	Status ⌄
□	General Data Leaks	● Healthy

● Get alerts for all activity
Risk scores will be assigned and alerts generated for all specified activities, regardless of whether they i

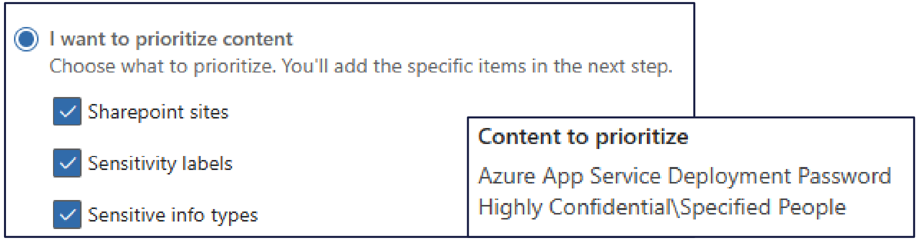
○ Get alerts only for activity that includes priority content
Risk scores will be assigned and alerts generated only when specified activities include priority content.
but you'll still be able to review them if an alert is generated.



Downloading SharePoint files

Activity from 3 users scanned

Top 1% of users downloaded SharePoint files more than 7303 times



● I want to prioritize content
Choose what to prioritize. You'll add the specific items in the next step.

☑ Sharepoint sites

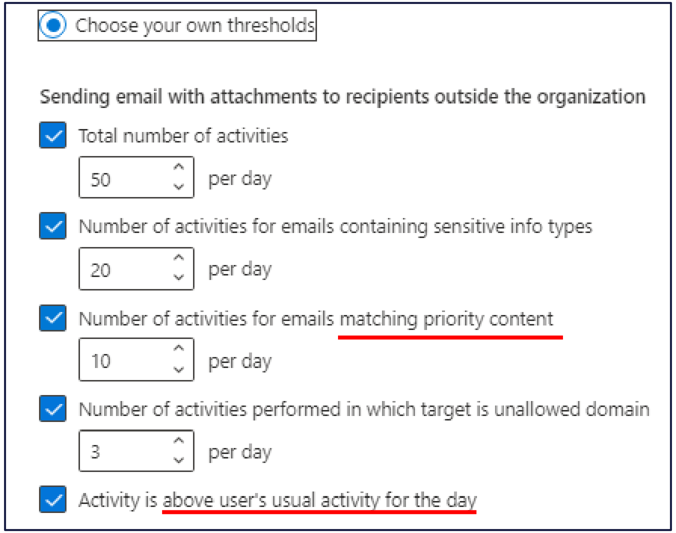
☑ Sensitivity labels

☑ Sensitive info types

Content to prioritize

Azure App Service Deployment Password
Highly Confidential\Specified People

Insider Risk Management policy



● Choose your own thresholds

Sending email with attachments to recipients outside the organization

☑ Total number of activities

50 per day

☑ Number of activities for emails containing sensitive info types

20 per day

☑ Number of activities for emails matching priority content

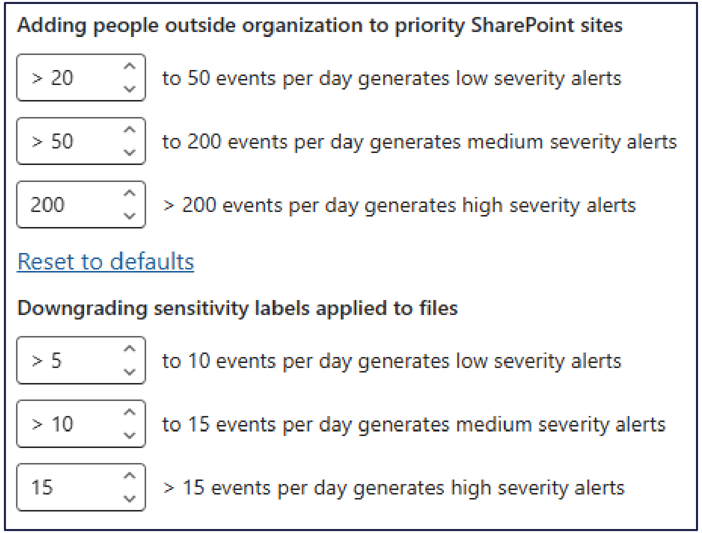
10 per day

☑ Number of activities performed in which target is unallowed domain

3 per day

☑ Activity is above user's usual activity for the day

1. Triggering thresholds



Adding people outside organization to priority SharePoint sites

> 20 to 50 events per day generates low severity alerts

> 50 to 200 events per day generates medium severity alerts

200 > 200 events per day generates high severity alerts

Downgrading sensitivity labels applied to files

> 5 to 10 events per day generates low severity alerts

> 10 to 15 events per day generates medium severity alerts

15 > 15 events per day generates high severity alerts

2. Indicator (alert) thresholds

elisa

A SUSTAINABLE FUTURE THROUGH DIGITALISATION

Thank you!
Have a great day!