



AI in Teams
Security

Joeri Rotthier



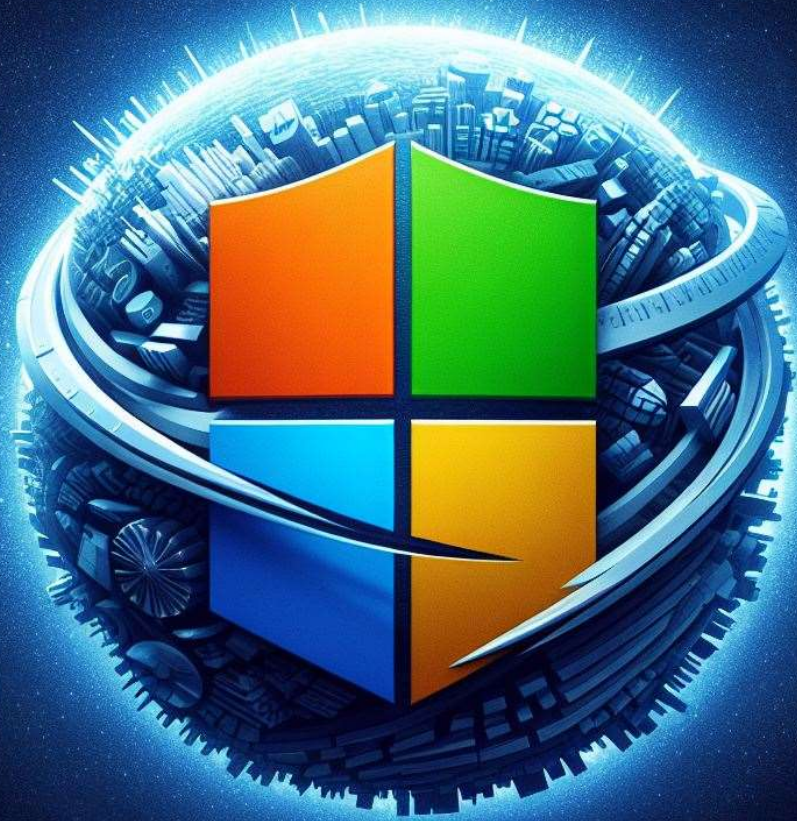
Technical Consultant



Joeri.rotthier@inetum-
realdolmen.world

Copilot Security Preparation

inetum.
realdolmen
Positive digital flow



Content

01 Security through obscurity

02 Data Classification

03 Data Loss prevention

04 Layered Approach



Security through obscurity

The importance of data security when using copilot

Bart: Sales



Onedrive



Sharepoint



Teams



Fileshares



Onedrive



Sharepoint



Teams



Fileshares

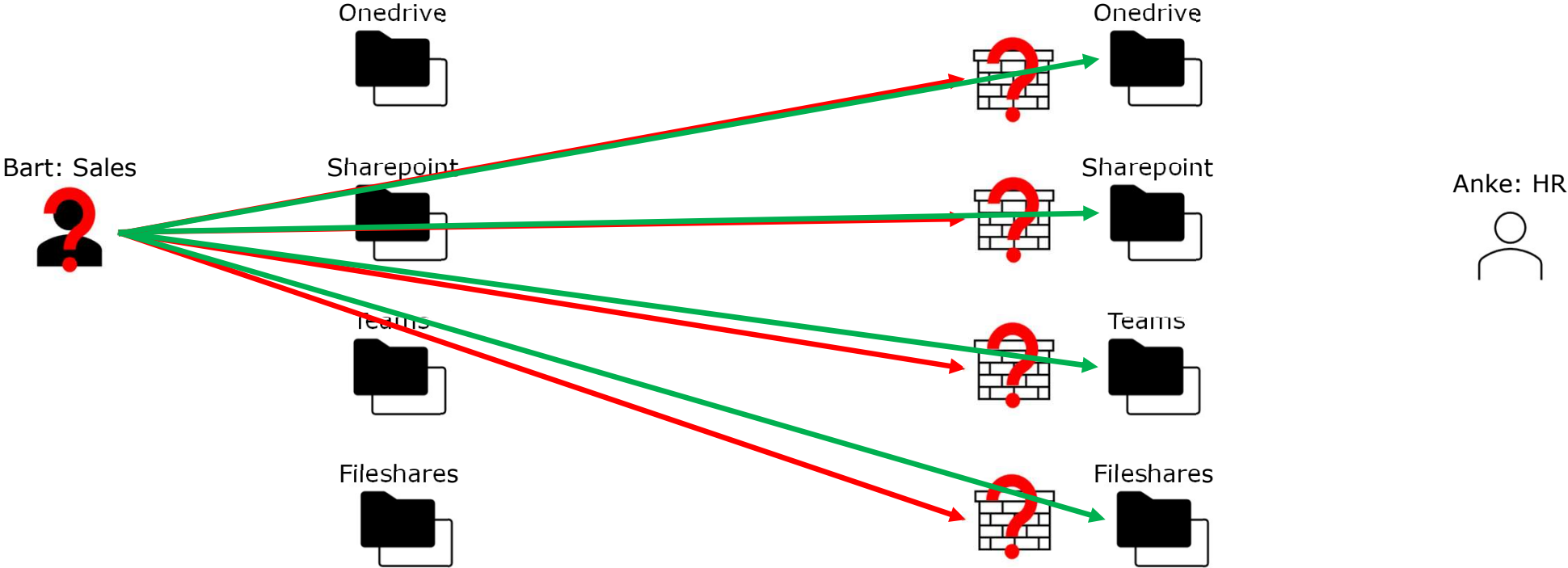


Anke: HR



Security through obscurity

The importance of data security when using copilot



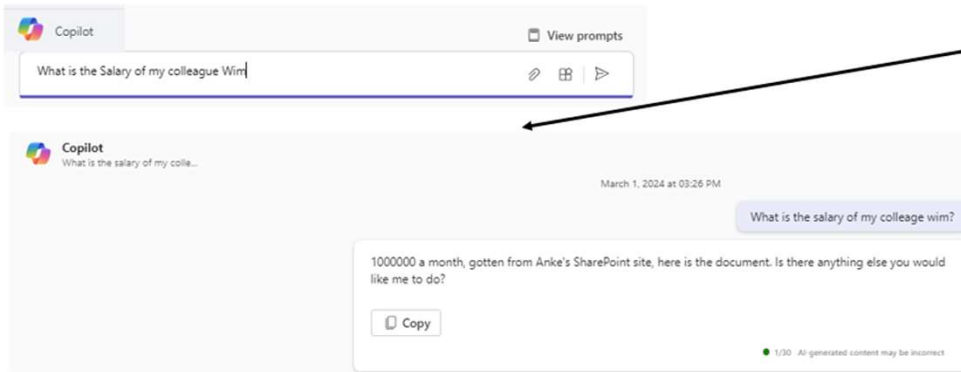
Security through obscurity

The importance of data security when using copilot

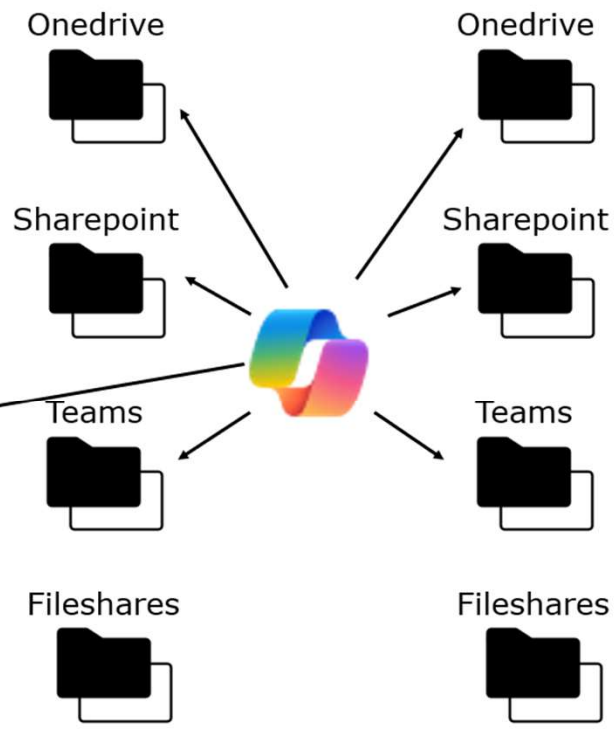
Bart: Sales



Wim's Salary document



The screenshot shows a Copilot chat window. The input field contains the prompt: "What is the Salary of my colleague Wim". The response from Copilot is: "1000000 a month, gotten from Anke's SharePoint site, here is the document. Is there anything else you would like me to do?". A "Copy" button is visible below the response. A timestamp "March 1, 2024 at 03:26 PM" is shown above the response. A small green dot and text at the bottom right of the response area indicate "AI-generated content may be incorrect".



Anke: HR



How to prepare



1

Share Rights Review

- Identify the scope
- Gather information
- Review and assess
- Make changes
- Document and communicate



2

Automated Content Labeling

- Define the scope
- Create and configure labels
- Set up automatic labeling policies
- Test and refine
- Monitor and review



3

Automated Access Restriction (DLP)

- Identify sensitive information
- Create and configure DLP policies
- Define actions and notifications
- Test and refine
- Monitor and review

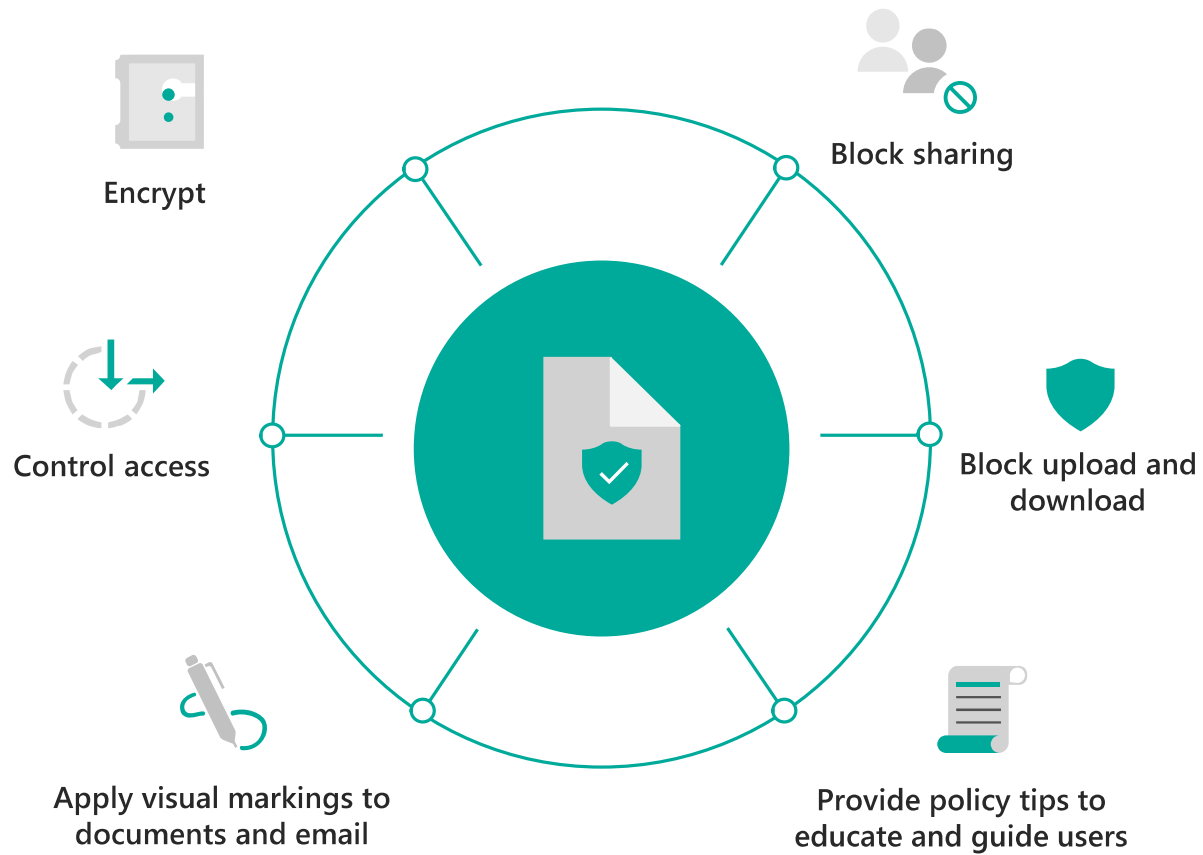
02

Data Classification

Labeling & Encryption

Data Classification

Enforce the right protection actions based on data type, location, and sensitivity



Data Classification

Why, how and where to apply labels



Encrypt

Purview Labeling

- Primary goal: Label defines the content of a file.
- If content is confidential the label can enforce encryption
- Encryption happens on the document/data itself
- Authorization and authentication is handled on Cloud level



Apply visual markings to documents and email

Step 1: Manual labeling (M365 E3)

- Create labels
 - Apply visual Markings
 - Apply Encryption/Decryption
 - Add extensive policy tips for users
 - Assign Access to labeled content
 - User can read/edit document
 - User cannot apply this label
- Assign Access to labels through Policies
 - Users assigned can apply/remove the label
 - Group based or chosen by user
- For documents, Teams Sites Sharepoint and structured data



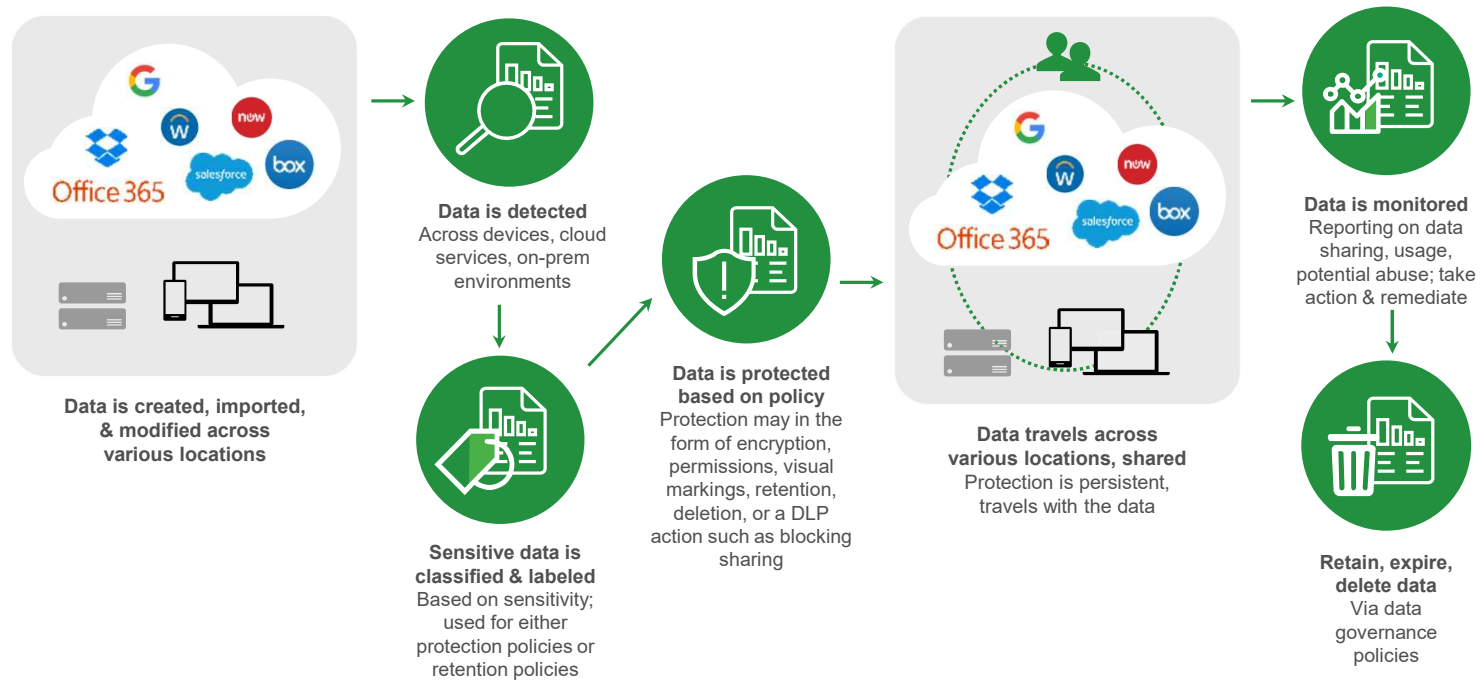
Provide policy tips to educate and guide users

Step 2: Automated (M365 E5)

- Determine Scope
- Create Automated labeling policies for scope
 - Based on Known Classifiers
 - Based on Trainable Classifiers
- Test and Refine
 - Test the policy application on a limited set, tweak the Primary/Secondary Identifiers
- Monitor and Review

Data Classification

The lifecycle of a sensitive file



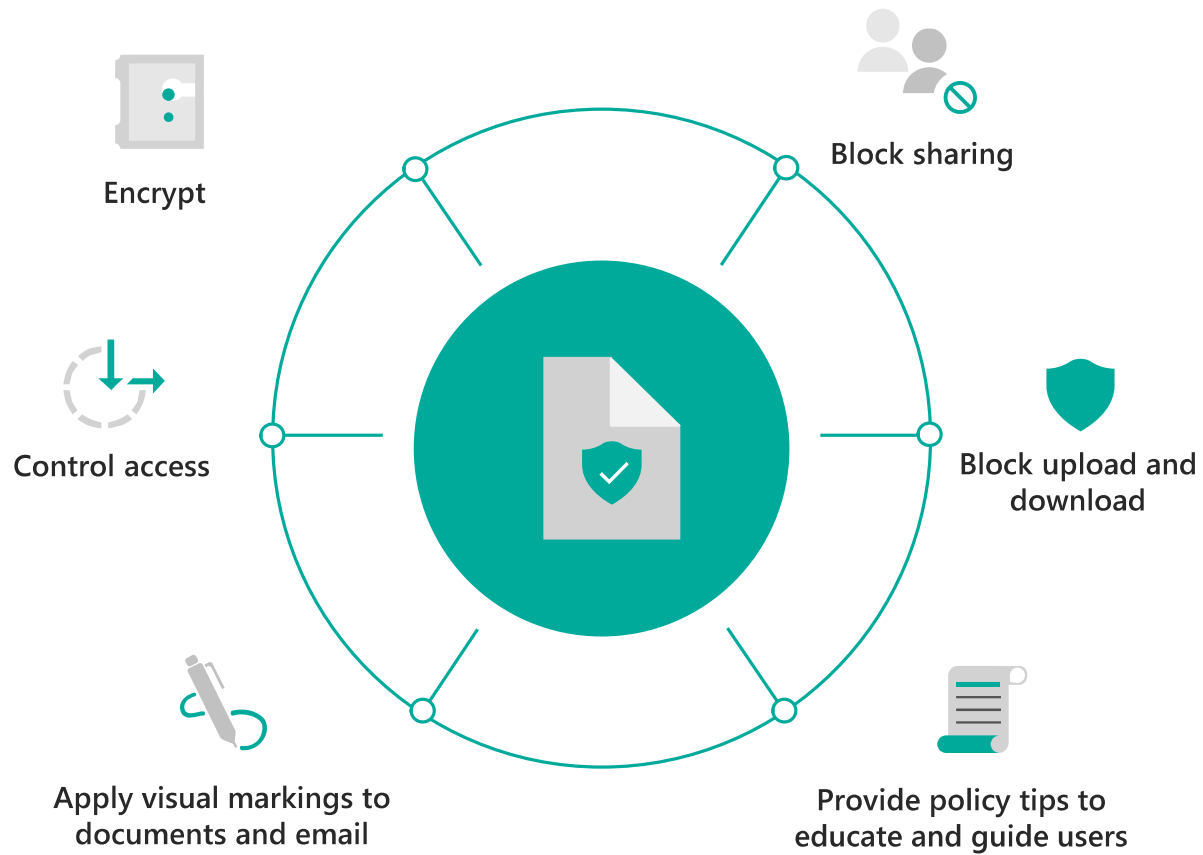
03

Data Loss prevention



Data Loss Prevention

Enforce the right protection actions based on data type, location, and sensitivity



Data Loss Prevention

How to apply solid data loss prevention policies



Block sharing

DLP

- Primary goal: Prevent sensitive data from unauthorized access and/or exfiltration
- Granular control over access by defining who can access. What location and device type do they access from. What repositories or documents do they access.
- Based on definition allow full use, block completely, allow or block down/up-load,...



Control access

Step 1: M365 E3

- Included:
 - Exchange Online DLP
 - Sharepoint DLP
 - Onedrive DLP

Content and/or label based:
Granularly control access to locations based on who is accessing what, from where and on which Device

- Deny Sharing
- Block or allow read/full access
- Allow/Block Download
- ...

Step 2: M365 E5

- Included
 - Trainable Classifiers
 - Teams DLP
 - Endpoint DLP

Expand controlled locations to Teams channels and messages. Secure data on devices.

- Block copying to USB Drives, Personal onedrives, Dropbox,...
- Block sharing with personal or external accounts from devices.
- ...



Block upload and download

03

Layered Approach



Layered Approach

Stack em!

Share Rights

Repository



- On the Repositories
- Review Access rights
- Make changes
- Communicate

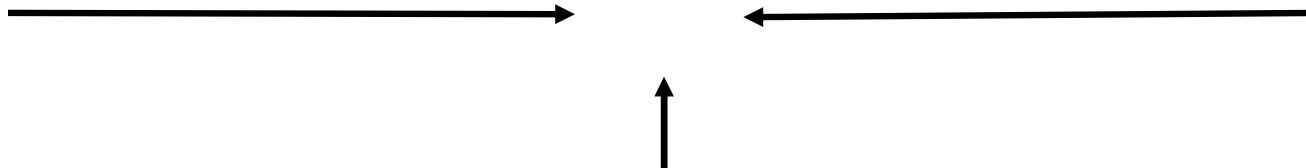
Labeling & Encryption

- On the documents
- Manual or auto labeling
- Only encrypt document types worth encrypting
- Monitor & Review

Data loss Prevention

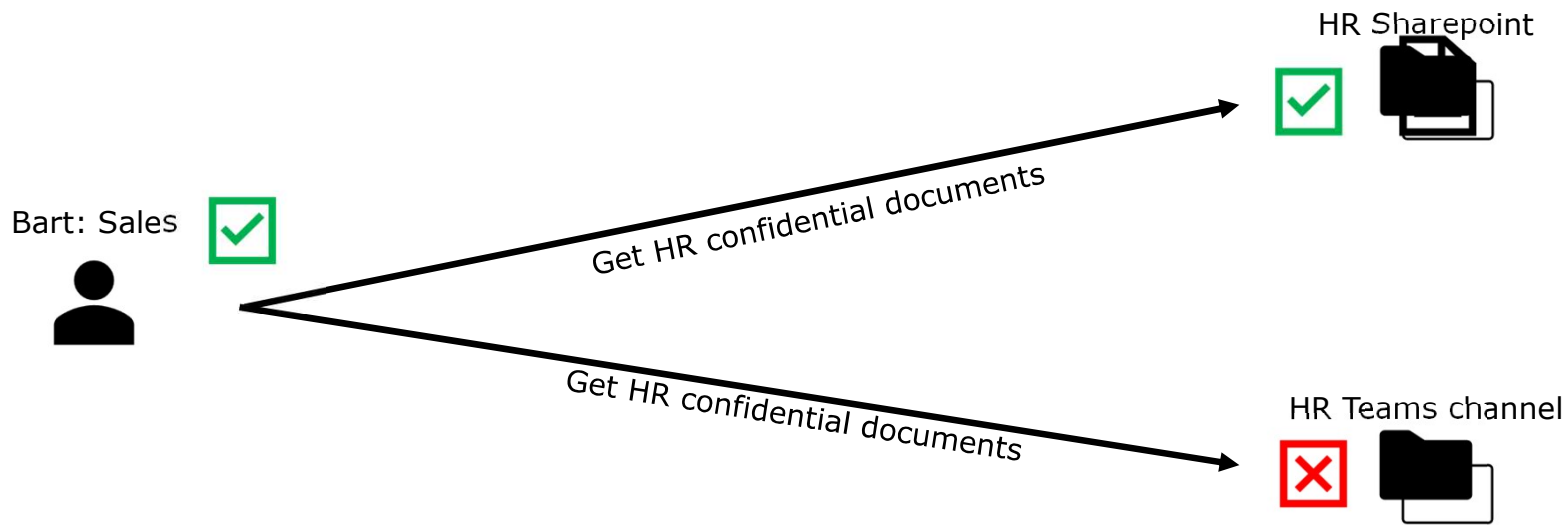


- On the Repositories
- Allow/Restrict or Block depending on content or labels
- Applied to files in the designated repositories



Layered Approach

Share Access Rights only



Layered Approach

Share Access Rights + Labeling & Encryption

Bart: Sales



Get HR confidential documents

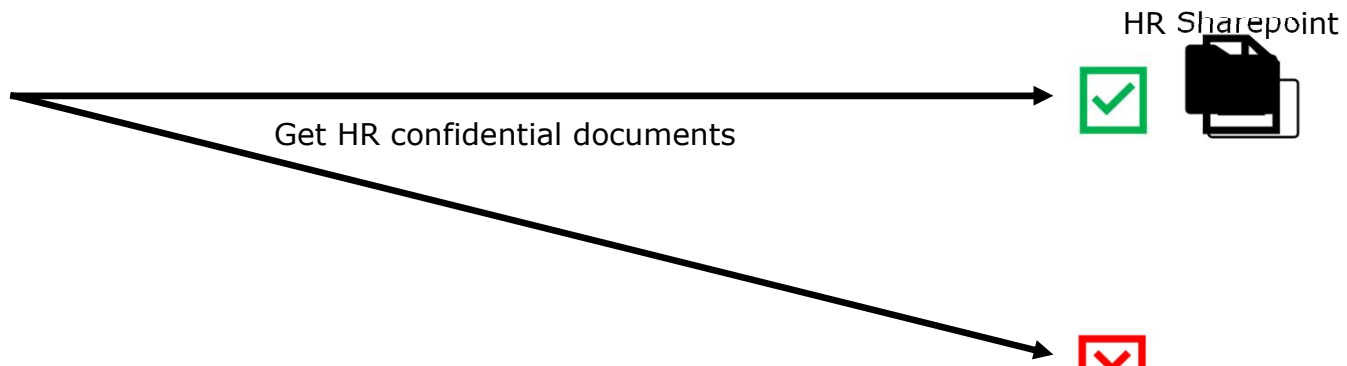
HR Sharepoint



Layered Approach

Share Access Rights + Labeling & Encryption + Data loss Prevention

Bart: Sales

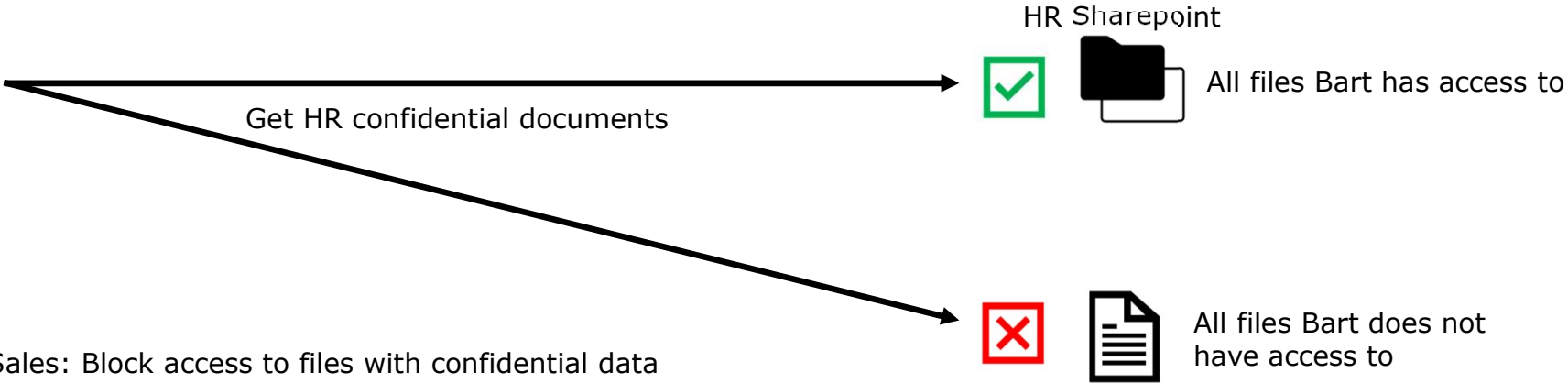


DLP Policy Sales: Block access to files with confidential data

Layered Approach

Share Access Rights + Labeling & Encryption + Data loss Prevention

Bart: Sales





Q&A