

IT-BLOCKS

FilesCare

Microsoft[®]
CERTIFIED

Partner

MS Azure Information Protection & FilesCare



FilesCare

The evolution of Information Protection

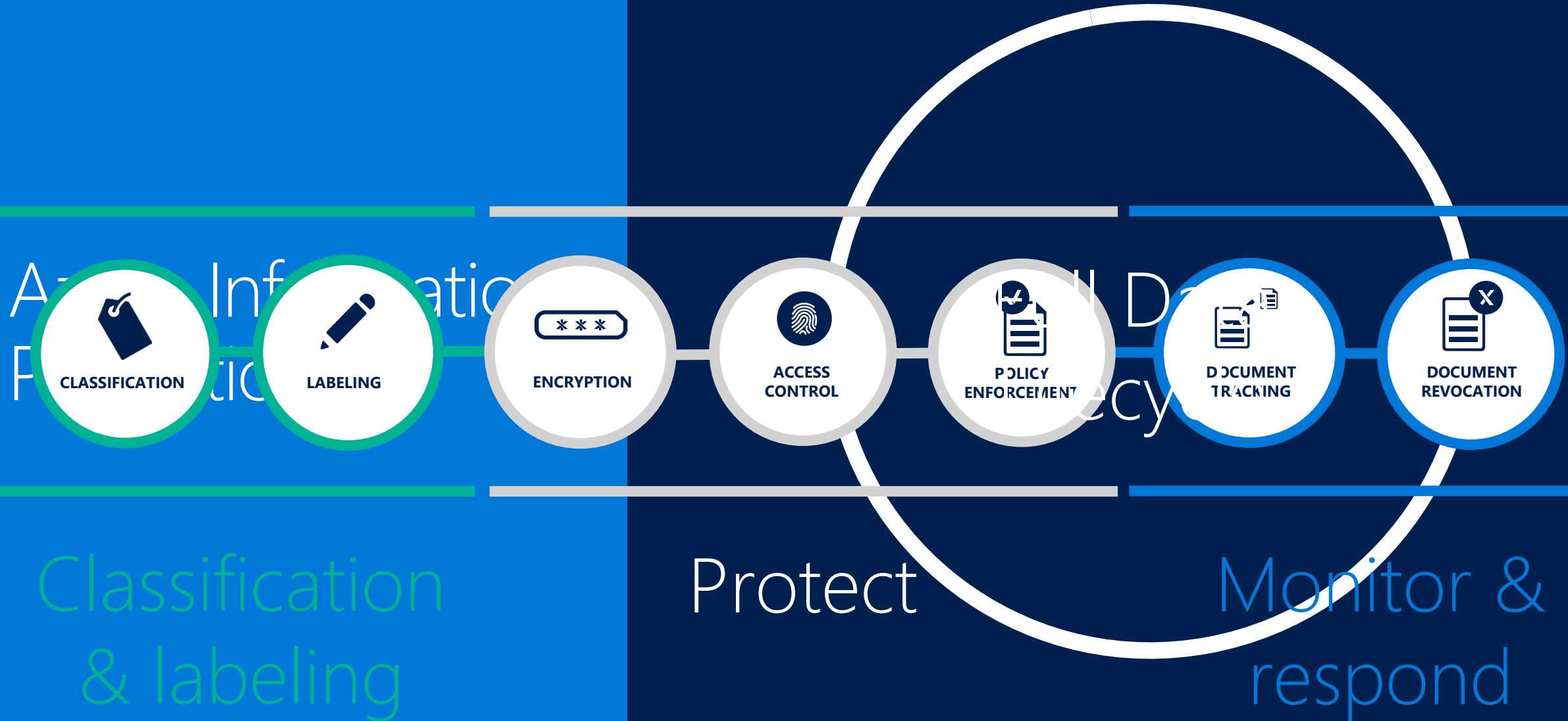


Classification
& labeling

Protect

Monitor &
respond

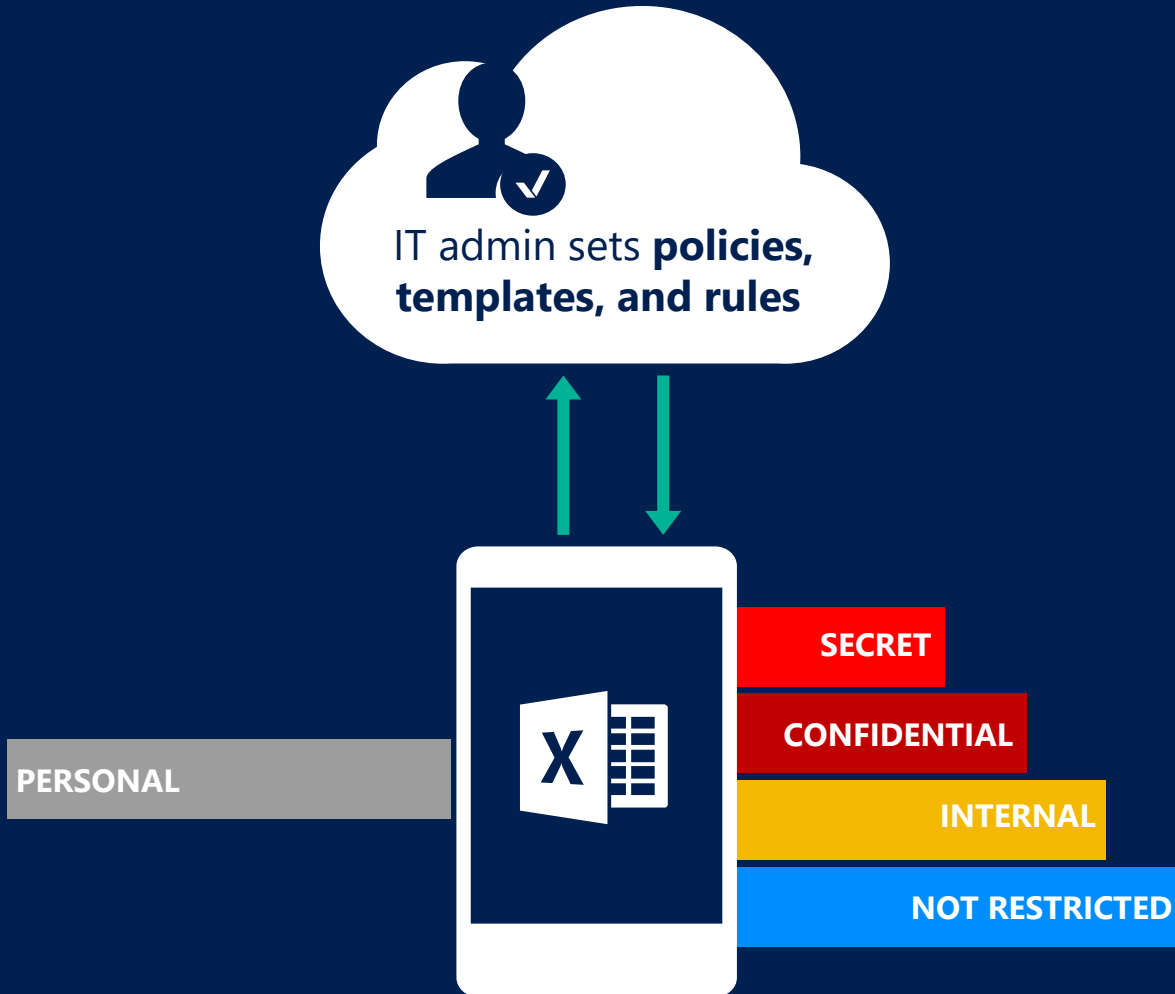
The evolution of Information Protection



Classify Data – Begin the Journey



Classify data based on sensitivity



- ▶ Start with the data that is most sensitive
- ▶ IT can set automatic rules; users can complement it
- ▶ Associate actions such as visual markings and protection

Scoped Policies

* Policy name

Finance Policy ✓

Policy description

Policy for Finance - including confidential/finance label + default finance label

Select which users/groups get this policy ⓘ

1 Group >

Configure labels for this policy and order them by sensitivity level

LABEL NAME	TOOLTIP	POLICY	MAR... P.
Public	This information is not restricted, can be used by everyone in	Global	...
Internal Use	This information includes a wide spectrum of internal busine	Global	✓ ...
Restricted	This information contains highly sensitive data for Microsoft	Global	✓ ...
Finance		Finance Policy	...
Critical Handling	This information contains highly sensitive data. Exposing this	Global	...

+ Add a new label

- ▶ Policies for specific groups/departments
- ▶ Can be viewed and applied only by the members of that group
- ▶ Customization options for labels, sub-labels, and settings like mandatory labeling, default label, and justifications

How Classification Works



Automatic

Policies can be set by IT Admins for automatically applying classification and protection to data



Recommended

Based on the content you're working on, you can be prompted with suggested classification



Reclassification

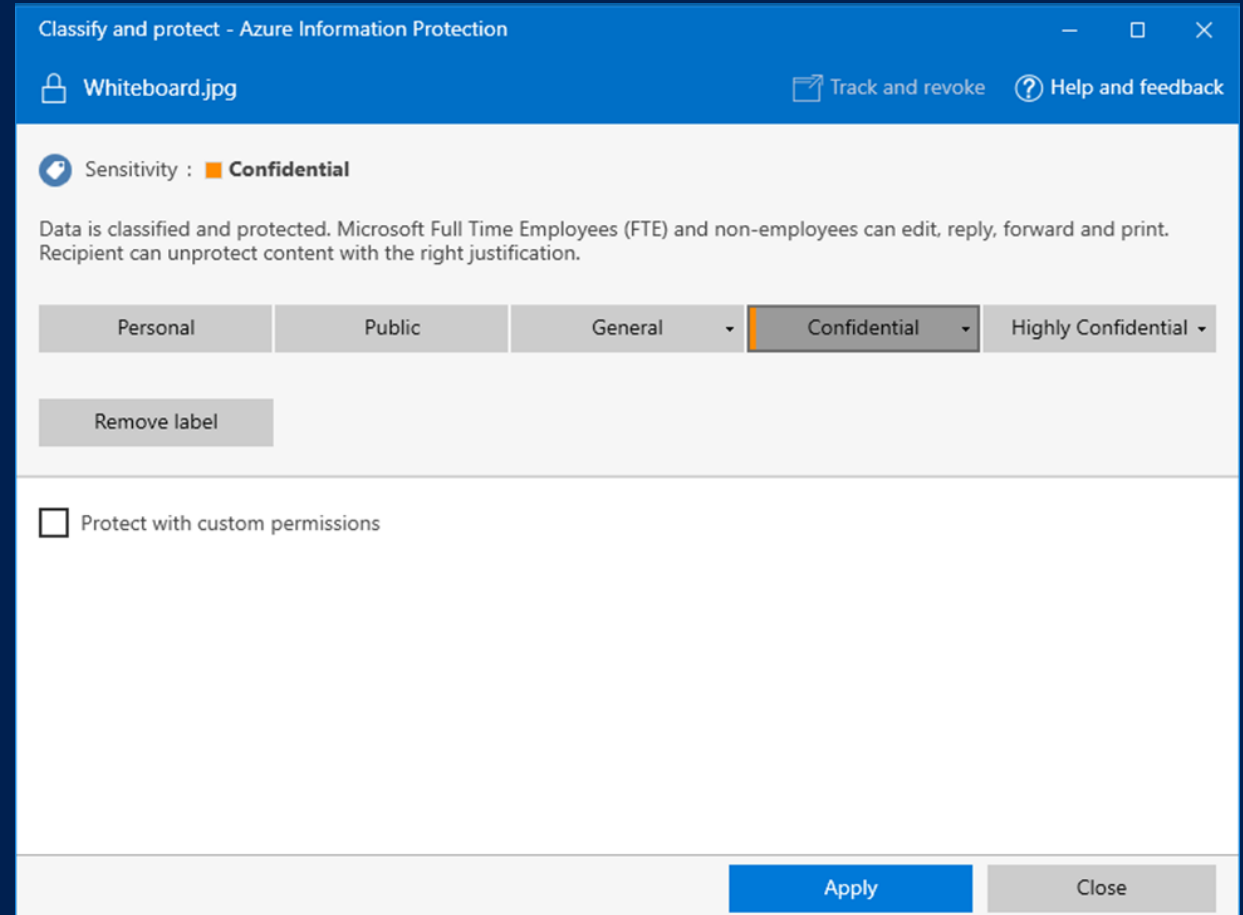
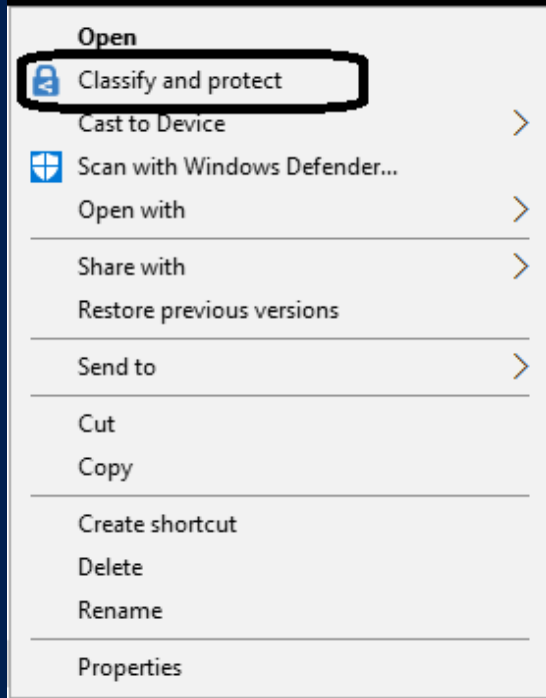
You can override a classification and optionally be required to provide a justification



User set

Users can choose to apply a sensitivity label to the email or file they are working on with a single click

Manual (right-click) labeling and protection for non-Office files



- ▶ Label and protect any file through the windows shell-explorer
- ▶ Select either one file, multiple files or a folder and apply a label

Apply labels based on classification

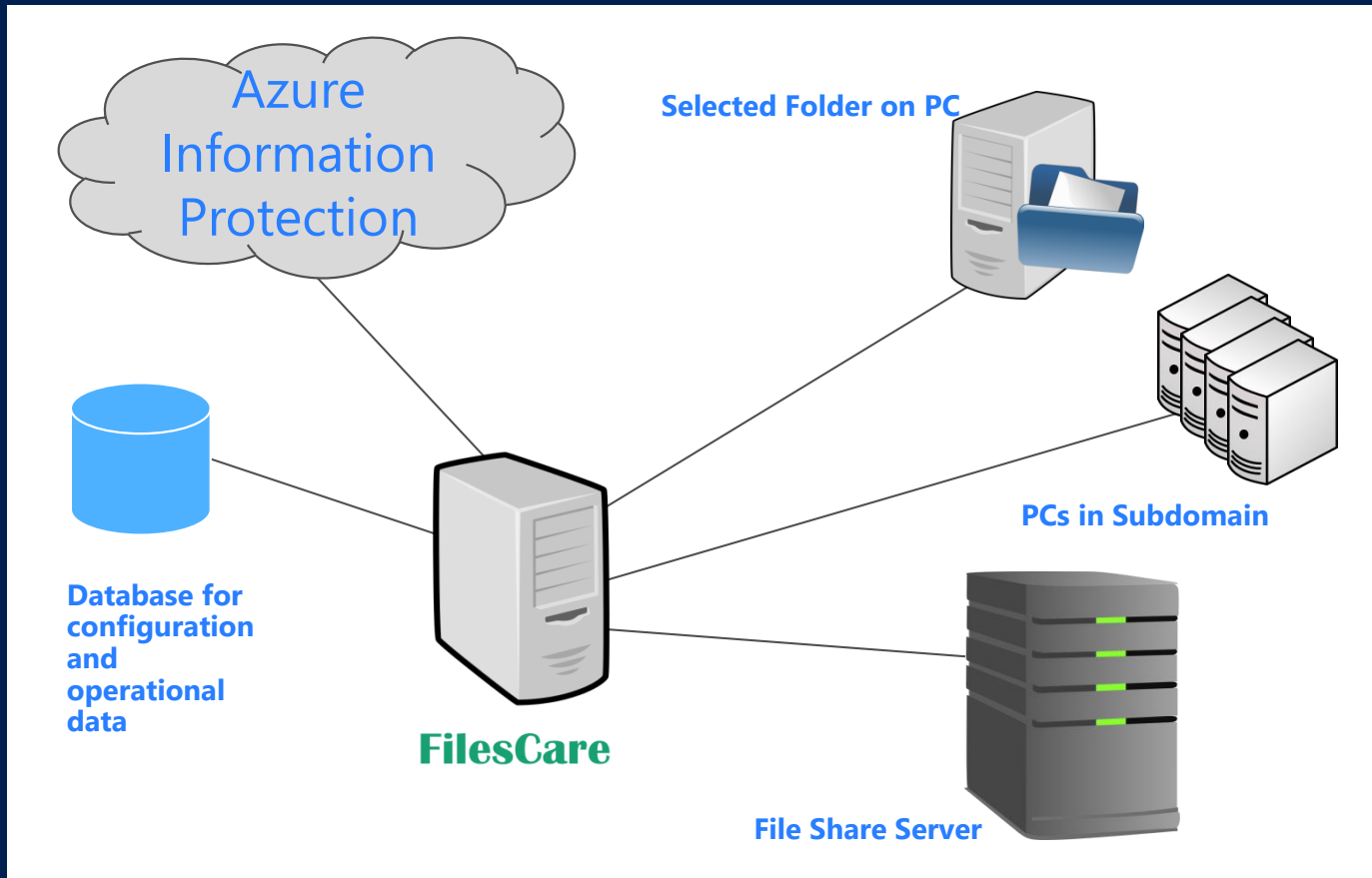


Persistent labels that travel with the document



- ▶ Labels are metadata written to documents
- ▶ Labels are in clear text so that other systems such as a DLP engine can read it

Bulk classification for files at rest using FilesCare

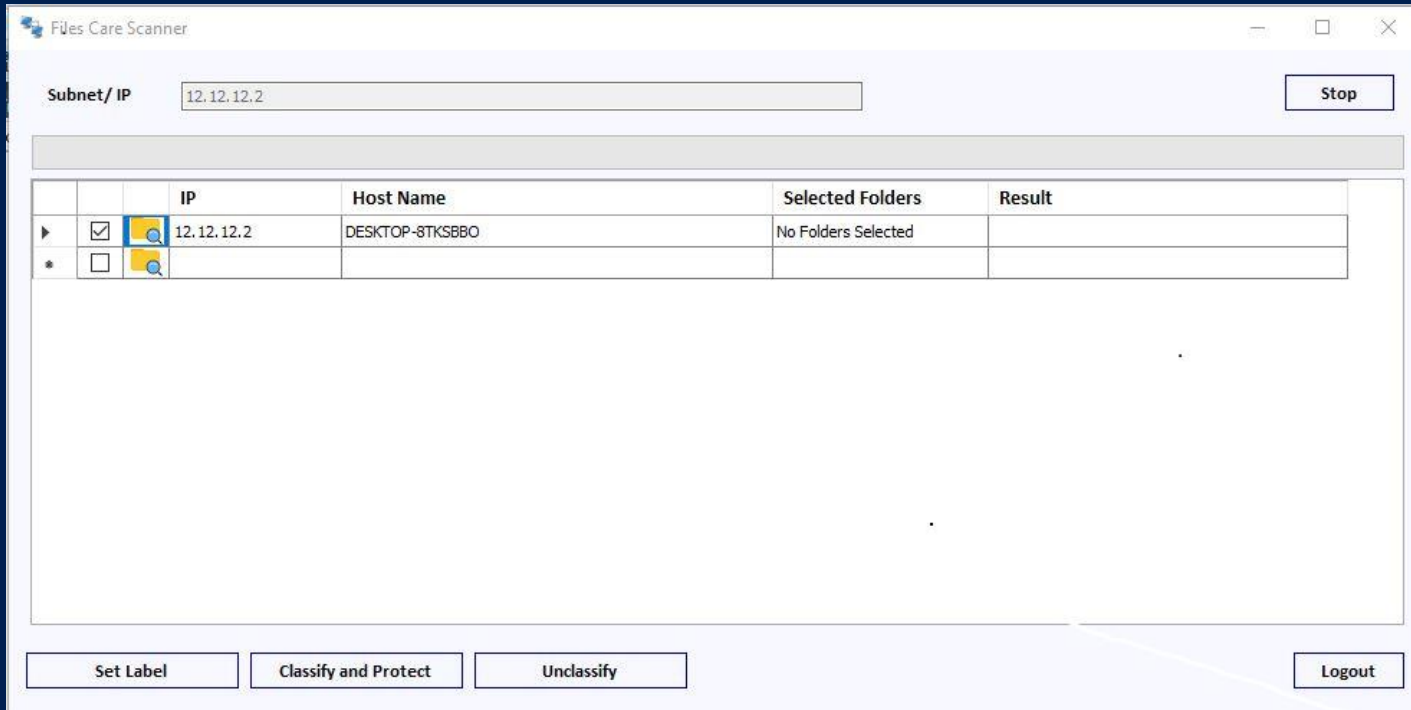


- ▶ Query for file labels and protection attributes
- ▶ Apply policy by setting a label and/or protection for files stored locally or on file shares
- ▶ Remove labels and/or protection from files

FilesCare

Automatically discover, classify, label & protect older files

FilesCare protects your legacy files

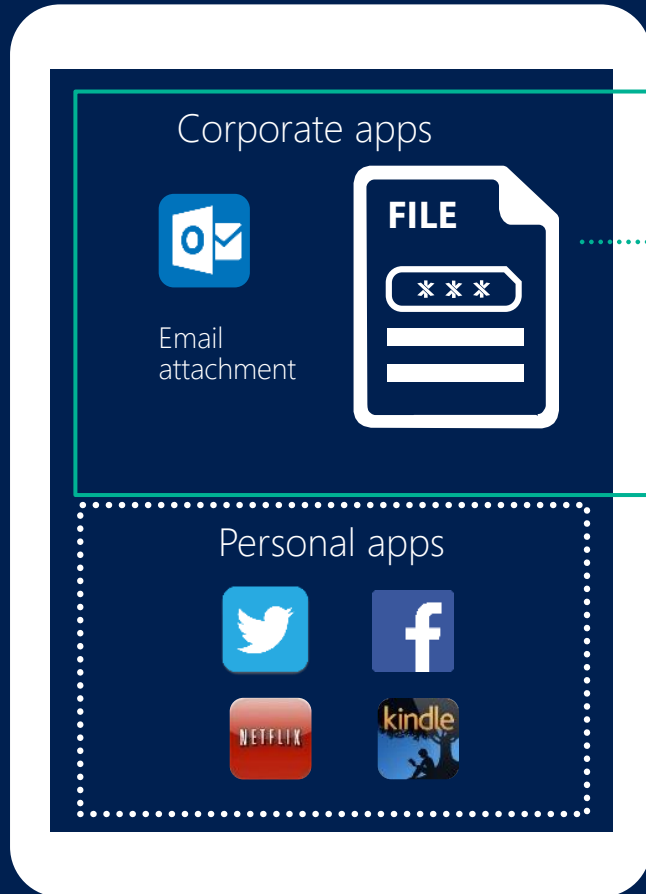


- ▶ Select Subnet to list PCs
- ▶ Select PCs and/or folders to scan
- ▶ Scan, discover, classify, label and protect files on selected PCs and/or folders
- ▶ Set a unique label on all files
- ▶ Remove labels from all files

Critical for migration scenarios and compliance with regulations such as GDPR



Protect data against unauthorized use



VIEW



EDIT



COPY



PASTE



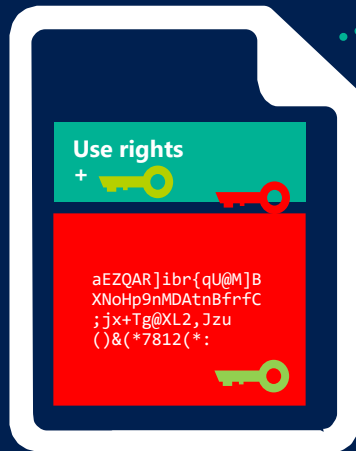
Protect data needing protection by:

- ▶ Encrypting data
- ▶ Including authentication requirement and a definition of use rights (permissions) to the data
- ▶ Providing protection that is persistent and travels with the data

How Protection Works



LOCAL PROCESSING ON PCS/DEVICES



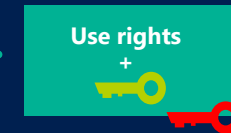
File content is **never** sent to the RMS server/service



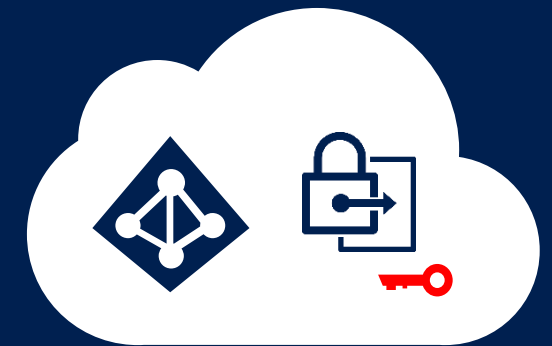
Apps protected with RMS **enforce rights**



Apps use the **SDK** to communicate with the RMS service/servers



Azure RMS never sees the file content, only the license

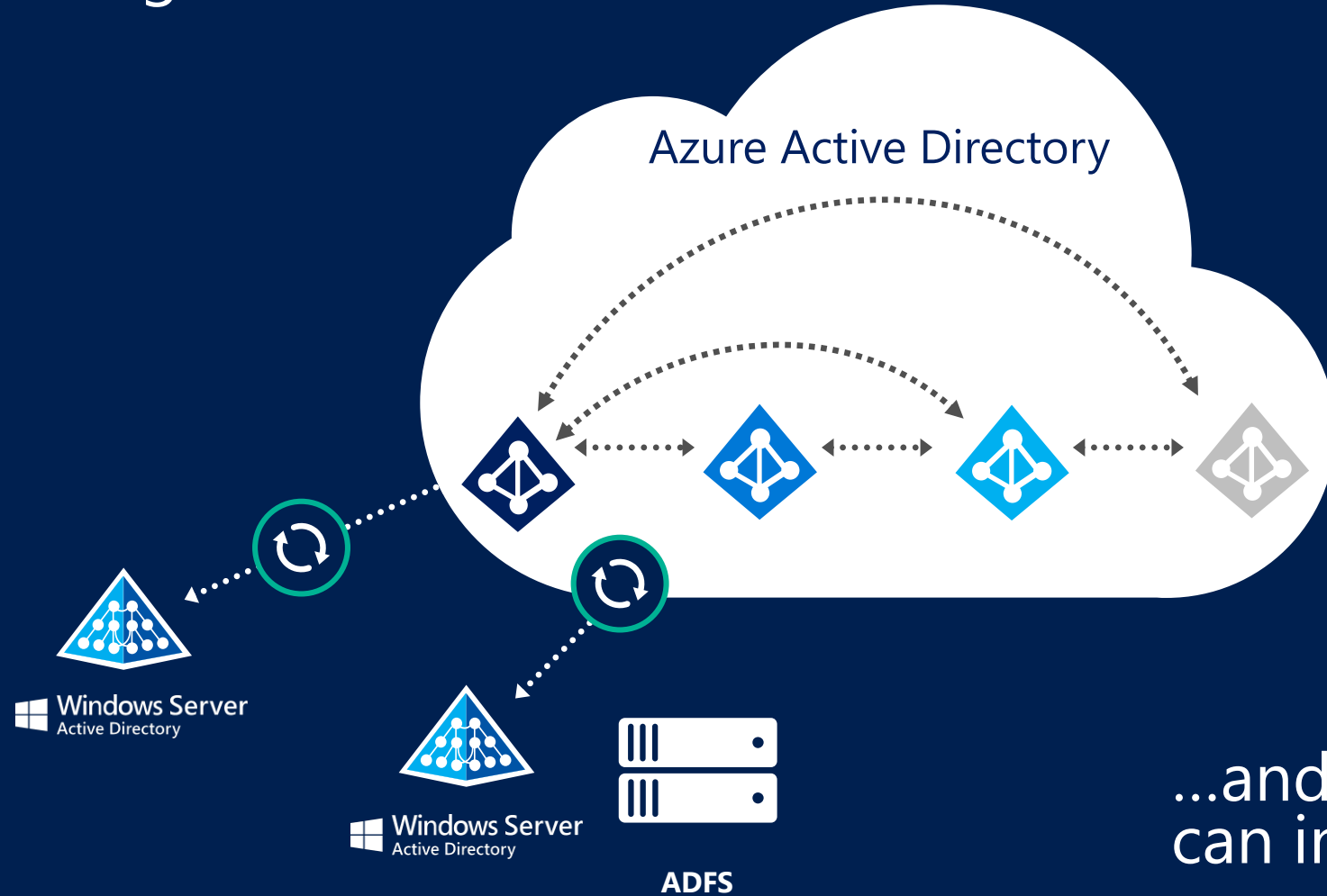





Microsoft Azure
Rights Management
Active Directory
Key Vault

How Sharing Works



Using Azure AD for authentication



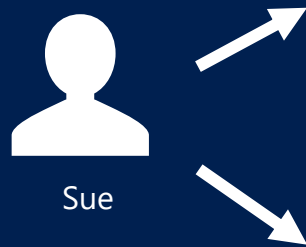
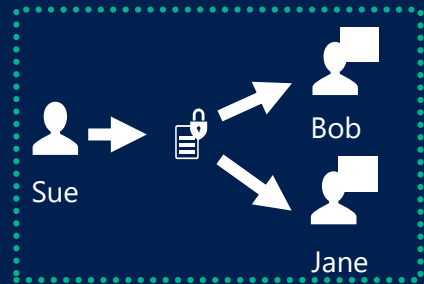
-  On-premises organizations doing full sync
-  On-premises organizations doing partial sync
-  Organizations completely in cloud
-  Organizations created through ad-hoc signup

...and all of these organizations can interact with each other.

Monitor and Respond



Monitor use, control and block abuse



MAP VIEW

A globe with four location pins. The pins are: South America (green, 2), India (green, 11), North America (red, 8), and Africa (red, 8).

2	Bob accessed from South America
11	Jane accessed from India
8	Joe blocked in North America
8	Jane blocked in Africa





WHY AZURE INFORMATION PROTECTION?

Persistent
protection

Safe
sharing

Intuitive
experience

Greater
control

FilesCare

We help you protect your legacy files

IT-BLOCKS

Microsoft
CERTIFIED
Partner