

A large, glowing blue shield icon with a white outline, centered on the left side of the slide. The shield is surrounded by a circular, glowing blue ring. The background of the entire slide is a dark blue circuit board pattern with glowing blue lines and nodes.

# Microsoft Azure Information Protection

Prenez le contrôle de vos données

A horizontal bar at the bottom of the slide, divided into several colored segments: green, red, blue, orange, yellow, and grey.

# Agenda.

1. Présentation de Bechtle Suisse SA
2. Introduction à Microsoft Azure Information Protection
3. Classification des données et « Sensitivity Labels »
4. Paramètres et « politiques »
5. Protection et chiffrement
6. AIP Scanner
7. Monitoring et administration
8. Expérience utilisateur
9. Modèles de licences et fonctionnalités AIP P1 et P2
10. Questions/Réponses et conclusion

# Présentation de Bechtle Suisse SA

---

# Bechtle Suisse SA.

**>1000**  
EMPLOYEES

**>30**  
PARTENAIRES

**NOS PROPRES  
(SUISSE)  
DATA CENTERS**

**Top-level  
certifications**

PME,  
ENTERPRISE  
ET PUBLIC

11 SITES REPARTIS EN  
SUISSE:

- Baar
- Bâle
- Berne
- Mägenwil
- Morges
- Petit-Lancy
- Plan-les-Ouates
- Pratteln
- Regensdorf
- Rotkreuz
- St Gall



**30**

ANNEES  
D' EXPERIENCE

ORGANISATION  
CENTRALE  
AVEC **SPOC**

**CONSEILS  
PERSONNALISES**

Global IT Alliance –  
Un réseau de  
partenaires triés  
sur le volet dans le  
monde entier

CUSTOM  
**bios shops**

**End-to-end  
IT services**

**>2500 CLIENTS**



# Azure Information Protection

---

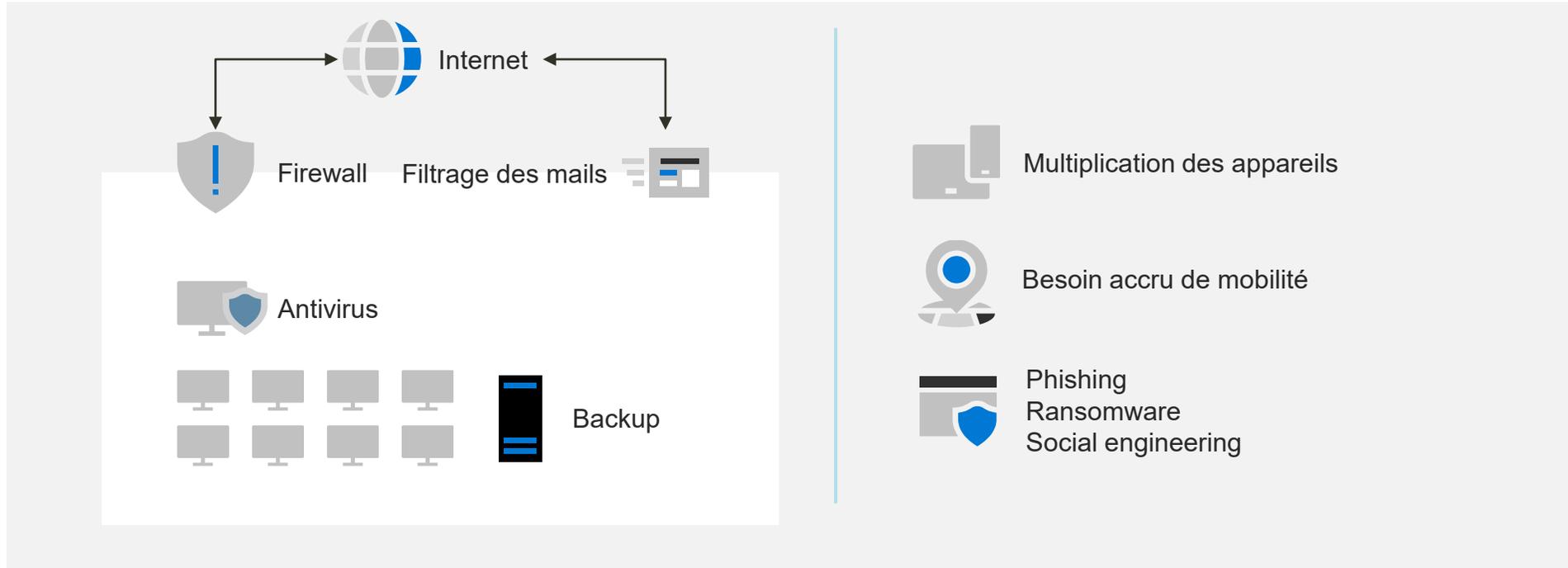
# Introduction à Microsoft Azure Information Protection

Le cloud Microsoft



# Introduction à Microsoft Azure Information Protection

Un nouveau contexte sécuritaire à appréhender



Les données migrant vers le Cloud et les utilisateurs étant de plus en plus mobiles, de nouveaux challenges nécessitent de nouvelles réponses.

# Introduction à Microsoft Azure Information Protection

Les réponses de Microsoft 365 à cette nouvelle situation



La défense globale contre les cyber-attaques



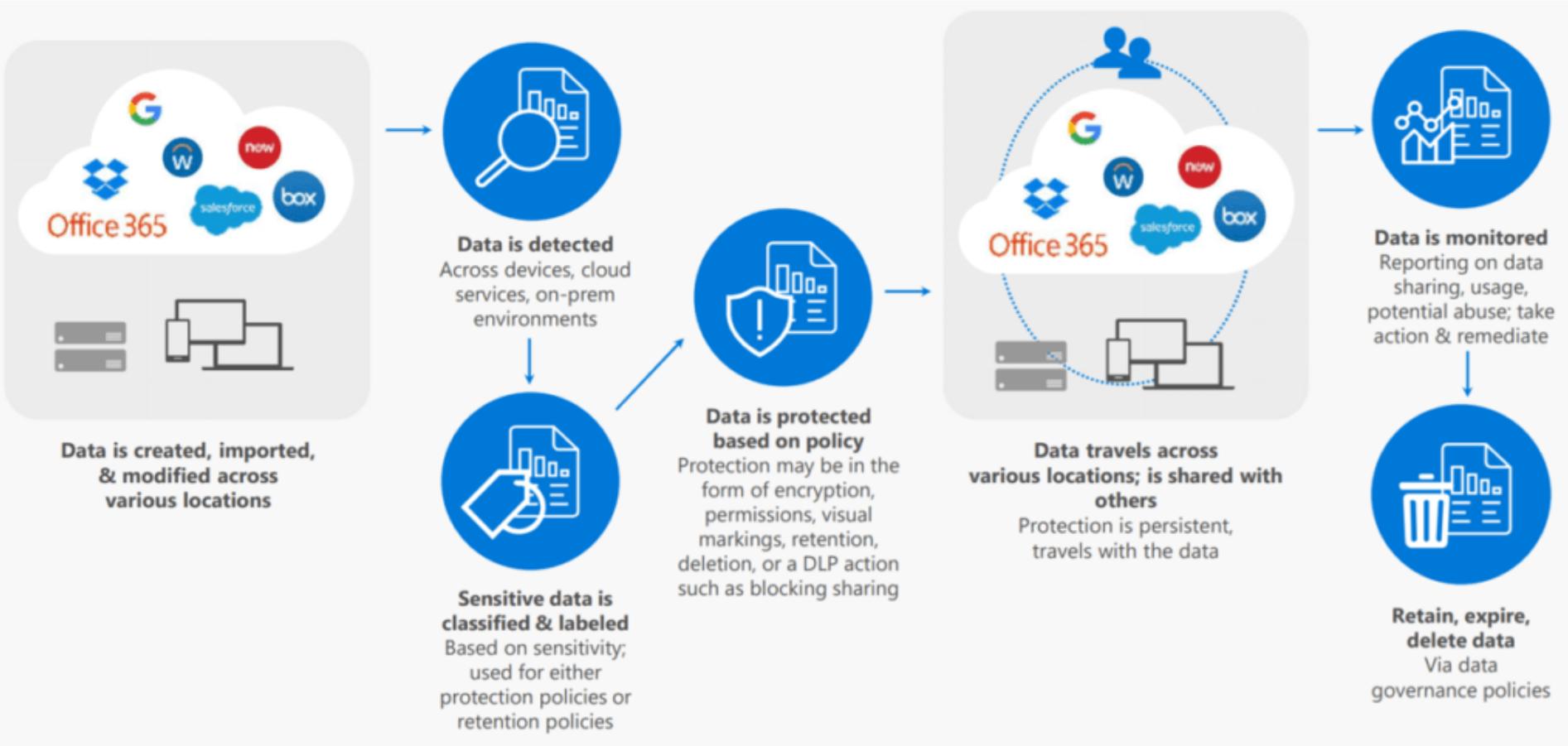
La protection centrée sur la donnée



Le contrôle des appareils et de leurs accès

# Introduction à Microsoft Azure Information Protection

## Concept Microsoft AIP



# Introduction à Microsoft Azure Information Protection

## Protéger et suivre la donnée



### Discover

Detect sensitive data across a variety of locations, based on the rules you define.



### Classify and label

Classify sensitive data and apply labels to documents and emails – automatically or manually.



### Protect and control sharing

Apply flexible protection actions, such as encryption, access restrictions and visual markings.



### Monitor and remediate

See what's happening with your sensitive data to gain more control over it.

# Classification des données et « Sensitivity Labels »

Protéger et suivre la donnée

Name		Order	Scope
Public	...	0 - lowest	File, Email
Interne	...	1	File, Email
— Confidentiel	...	2	File, Email
Pas de protection	...	3	File, Email
Protection avec chiffrement	...	4	File, Email
— Secret	...	5	File, Email
Pas de protection	...	6	File, Email
Protection avec chiffrement	...	7 - highest	File, Email

# Paramètres et « politiques »

Protéger et suivre la donnée

## Policy settings

You can choose to have a default label, mandatory label, or require users to justify actions on their end.

### Apply this label by default to documents and email

Interne



- Users must provide justification to remove a label or lower classification label
- Requires users to apply a label to their email or documents
- Provide users with a link to a custom help page

<https://intranet/AIP/Help.aspx>

# Protection et chiffrement

## Protéger et suivre la donnée

### Encryption

Control who can access files and email messages that have this label applied. [Learn more about encryption settings](#)

Remove encryption if the file or email is encrypted

Configure encryption settings

**Assign permissions now or let users decide?**

Assign permissions now

The encryption 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** ⓘ

Always

### Assign permissions

Only the users or groups you choose will be assigned permissions to use the content that has this label applied. You can choose from existing permissions (such as Co-Owner, Co-Author, and Reviewer) or customize them to meet your needs.

- + Add all users and groups in your organization
- + Add any authenticated users ⓘ
- + Add users or groups
- + Add specific email addresses or domains ⓘ



# Protection et chiffrement

Protéger et suivre la donnée

Assign permissions now or let users decide?

Let users assign permissions when they apply the label

---

Microsoft Azure Information Protection

Sensitivity	Test Encryption
Select permissions	Only for me
Select users, groups, or organizations	Example: John@contoso.com ;...
Expire access	Never (Click to set an expiration date)

Apply Cancel

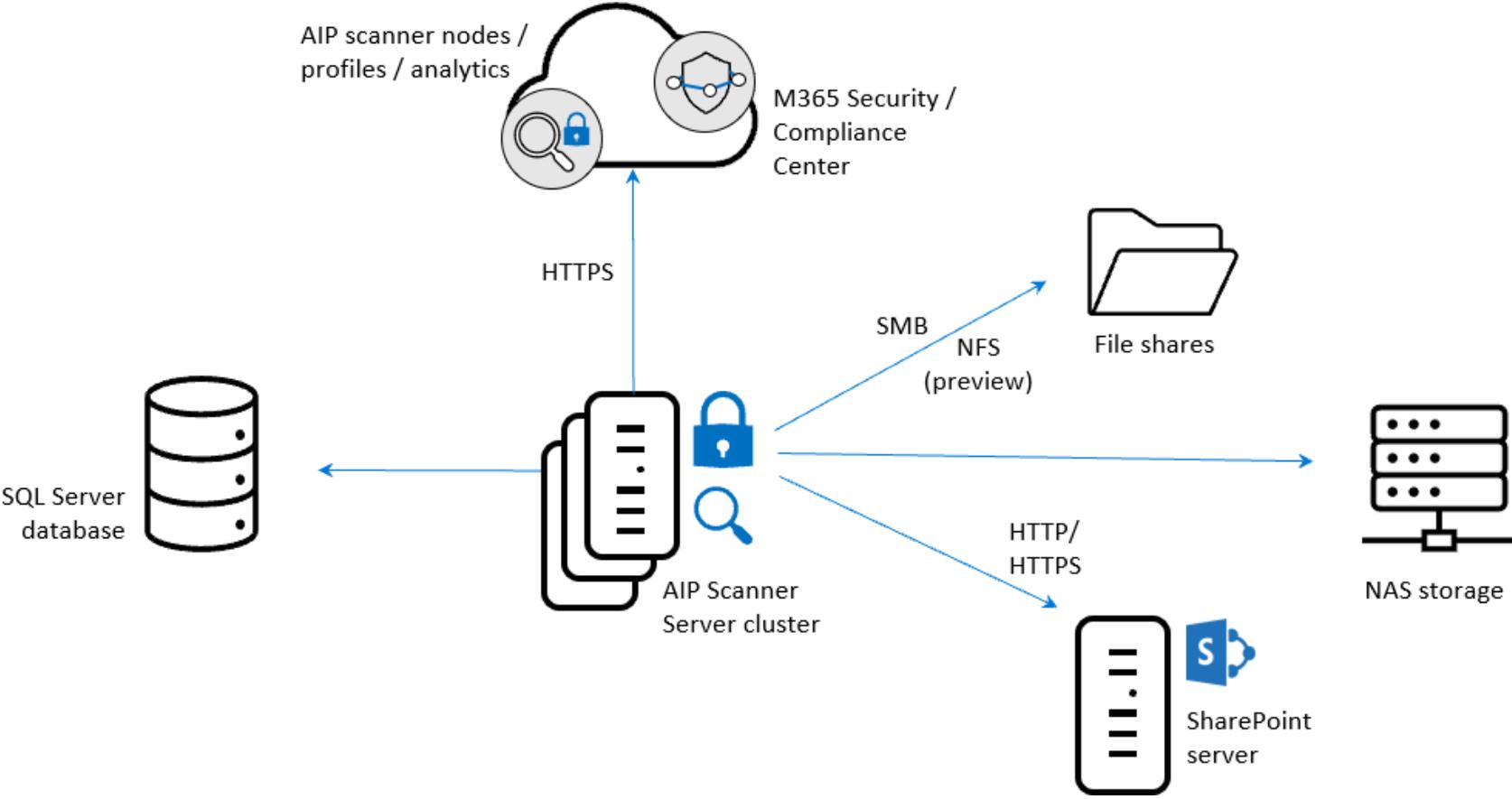
Select Permission

- Viewer - View Only
- Reviewer - View, Edit
- Co-Author - View, Edit, Copy, Print
- Co-Owner - All Permissions
- Only for me



# AIP Scanner

## Découverte et labélisation des données on-premise



# Monitoring et administration

## Analytics Workspace

Columns Log Analytics

Activity date: **Last 31 days** Information types == **None** Label == **Any** Result status == **Succeeded** [Add Filter](#) [Filter](#)

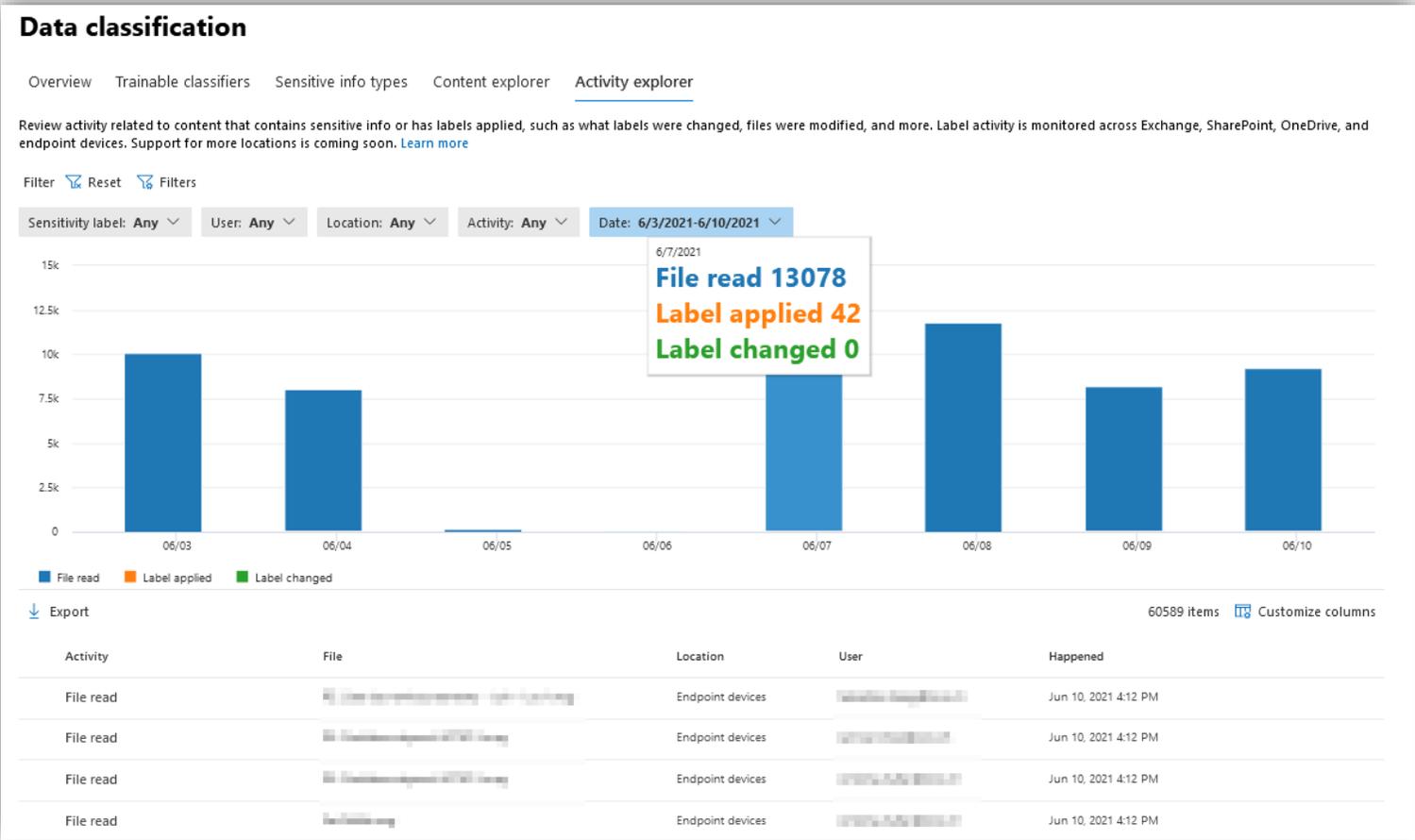
Date	Time	User	Item name	Activity	Label	Protection	Device name	Application name	Result status
6/10/2021	3:30:51 PM	[redacted]	[redacted]	Access	Public	No	[redacted]	Outlook	✔ Succeeded
6/10/2021	3:29:27 PM	[redacted]	[redacted]	Access	Public	No	[redacted]	Outlook	✔ Succeeded
6/10/2021	3:29:16 PM	[redacted]	[redacted]	Access	Public	No	[redacted]	Outlook	✔ Succeeded
6/10/2021	3:29:07 PM	[redacted]	[redacted]	Access	Public	No	[redacted]	Outlook	✔ Succeeded
6/10/2021	3:28:56 PM	[redacted]	[redacted]	Access	Public	No	[redacted]	Outlook	✔ Succeeded
6/10/2021	3:28:22 PM	[redacted]	[redacted]	Access	Public	No	[redacted]	Outlook	✔ Succeeded
6/10/2021	3:27:09 PM	[redacted]	[redacted]	Access	Public	No	[redacted]	Outlook	✔ Succeeded
6/10/2021	3:26:48 PM	[redacted]	[redacted]	Access	Public	No	[redacted]	Outlook	✔ Succeeded
6/10/2021	3:26:46 PM	[redacted]	[redacted]	Access	Public	No	[redacted]	Outlook	✔ Succeeded
6/10/2021	3:26:44 PM	[redacted]	[redacted]	Access	Public	No	[redacted]	Outlook	✔ Succeeded
6/10/2021	3:26:37 PM	[redacted]	[redacted]	Access	Interne	No	[redacted]	Outlook	✔ Succeeded
6/10/2021	3:26:26 PM	[redacted]	[redacted]	Access	Public	No	[redacted]	Outlook	✔ Succeeded
6/10/2021	3:25:51 PM	[redacted]	[redacted]	Access	Public	No	[redacted]	Outlook	✔ Succeeded
6/10/2021	3:25:38 PM	[redacted]	[redacted]	Access	Interne	No	[redacted]	Outlook	✔ Succeeded
6/10/2021	3:24:58 PM	[redacted]	[redacted]	Access	Public	No	[redacted]	Outlook	✔ Succeeded

1 67 < >

\* Displaying first 1000 records

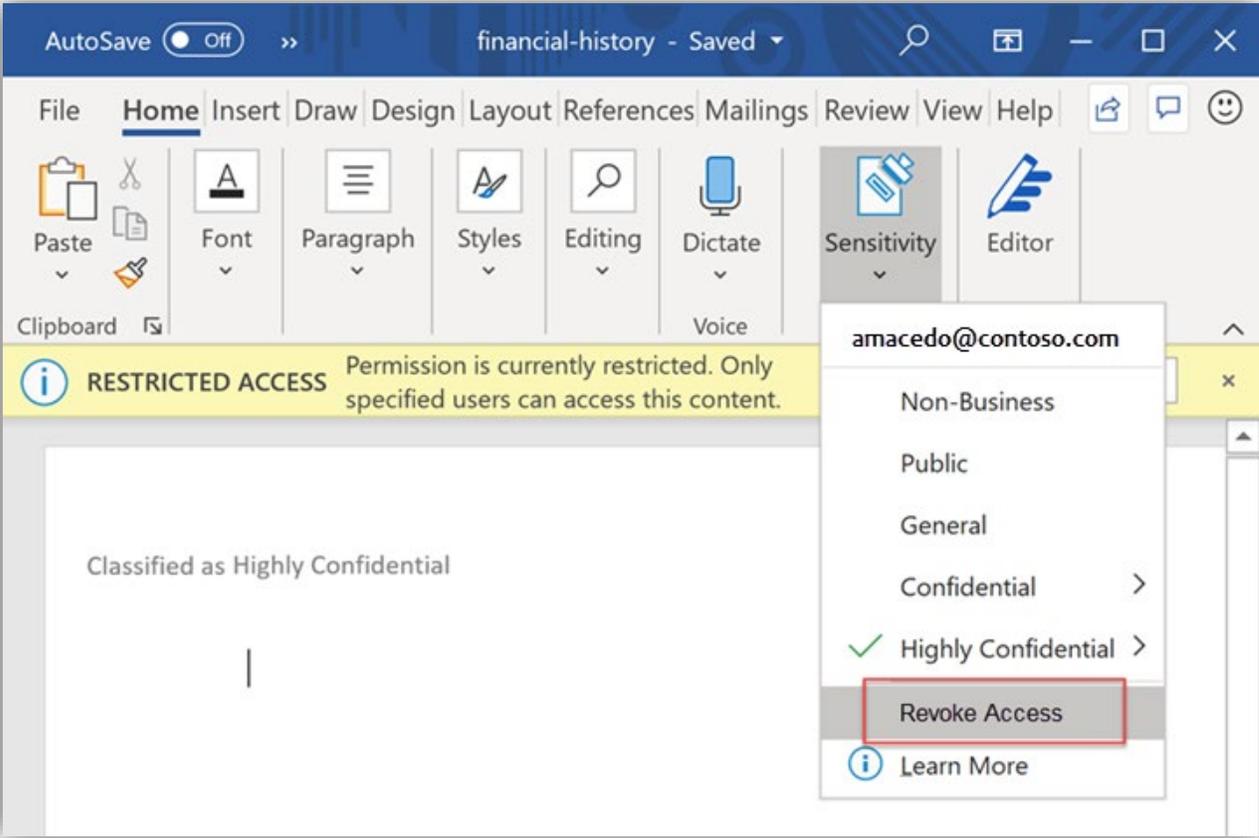
# Monitoring et administration

## Activity Explorer



# Monitoring et administration

## Track & Revoke



# Monitoring et administration

## Super User et garantie d'accès aux contenus chiffrés

Home > Groups | All groups (Preview) >

**AIP Super Users | Privileged access (Preview)** ×

Group

« + Add assignments Settings Refresh Export

Overview (Preview)  
Diagnose and solve problems

Manage

Properties  
Members (Preview)  
Owners (Preview)  
Administrative units (Preview)  
Group memberships (Preview)  
Assigned roles (Preview)  
Applications  
Licenses  
Azure role assignments

Activity  
Privileged access (Preview)  
Access reviews

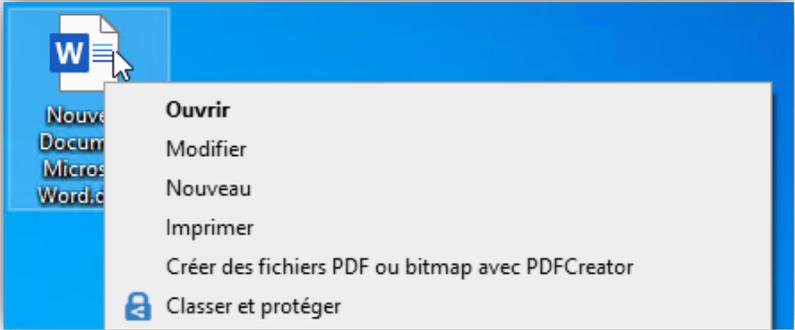
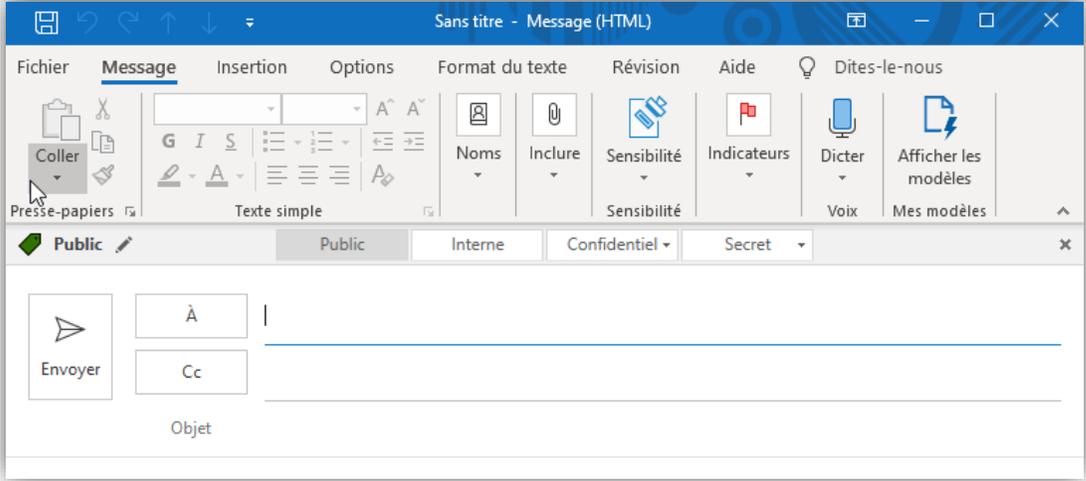
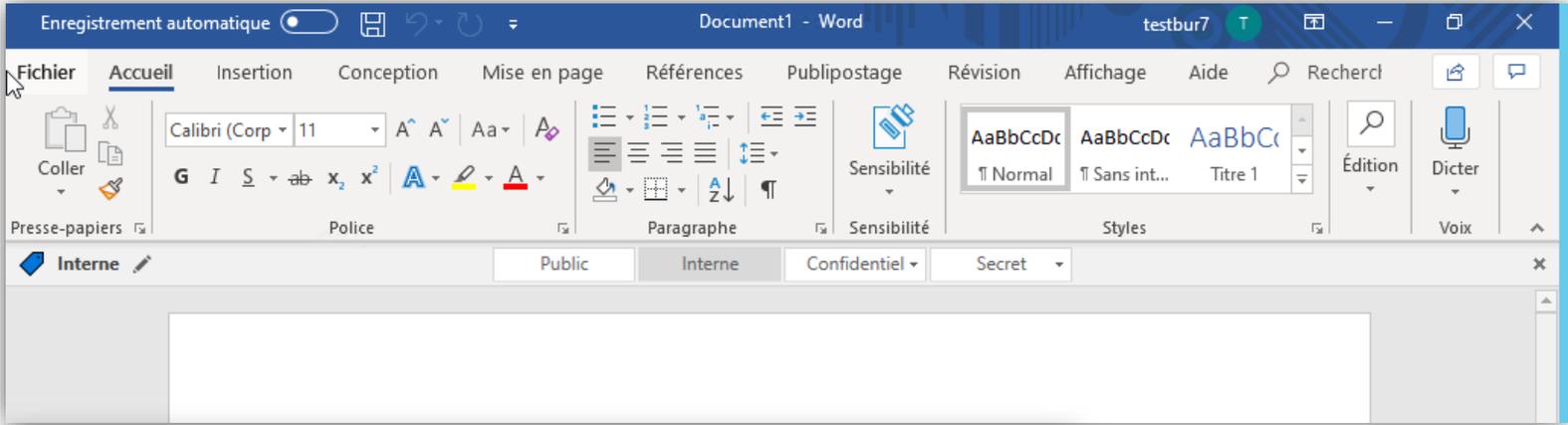
Eligible assignments Active assignments Expired assignments

Search by member name or principal name

Name	Principal name	Type	Membership	Start time	End time	Action
<b>Member</b>						
James Madison	james@...onmicr	User	Direct	8/12/2020, 1:53:01 PM	8/12/2021, 1:51:17 PM	Remove   Update   Extend
George Washington	george@...onmic	User	Direct	8/12/2020, 1:53:03 PM	8/12/2021, 1:51:17 PM	Remove   Update   Extend
John Adams	john@...micro	User	Direct	8/12/2020, 1:53:05 PM	8/12/2021, 1:51:17 PM	Remove   Update   Extend

# Expérience utilisateur

## Client AIP et intégration



# Expérience utilisateur

## Intégration Teams et Sharepoint Online

The image shows two overlapping screenshots from Microsoft Teams. The top-left screenshot is a dialog box titled "What kind of team will this be?". It features a "Sensitivity" dropdown menu with "Confidential" selected. A note below the dropdown states: "Teams with this sensitivity must be private." Below this, the "Privacy" section shows two options: "Private" (with a lock icon) and "Public" (with a globe icon). The "Private" option is highlighted, with the text "People need permission to join". The bottom-right screenshot shows a team page with a "Welcome to the team!" message. The page includes navigation tabs for "General", "Posts", "Files", and "Wiki". In the top right corner, a yellow box highlights the "Team" icon, the word "Confidential", and a help icon. The main content area contains three action buttons: "Add more people", "Create more channels", and "Open the FAQ".

# Expérience utilisateur

## Contenu chiffré et utilisateurs externes

Reply Reply All Forward IM

Tue 5/26/2020 2:19 PM

Financeuser <Financeuser@[redacted]@microsoft.com>  
[External] Test

To Kopalle, Kartik

If there are problems with how this message is displayed, click here to view it in a web browser.

message.rpmsg  
108 KB

Financeuser ([Financeuser@\[redacted\]@microsoft.com](mailto:Financeuser@[redacted]@microsoft.com)) has sent you a protected message.

[Read the message](#)

[Learn about messages protected by Office 365 Message Encryption.](#)

We sent a one-time passcode to [kartik@gmail.com](mailto:kartik@gmail.com).

Please check your email, enter the one-time passcode and click continue. The one-time passcode will expire in 15 minutes.

One-time passcode

This is a private computer. Keep me signed in for 12 hours.

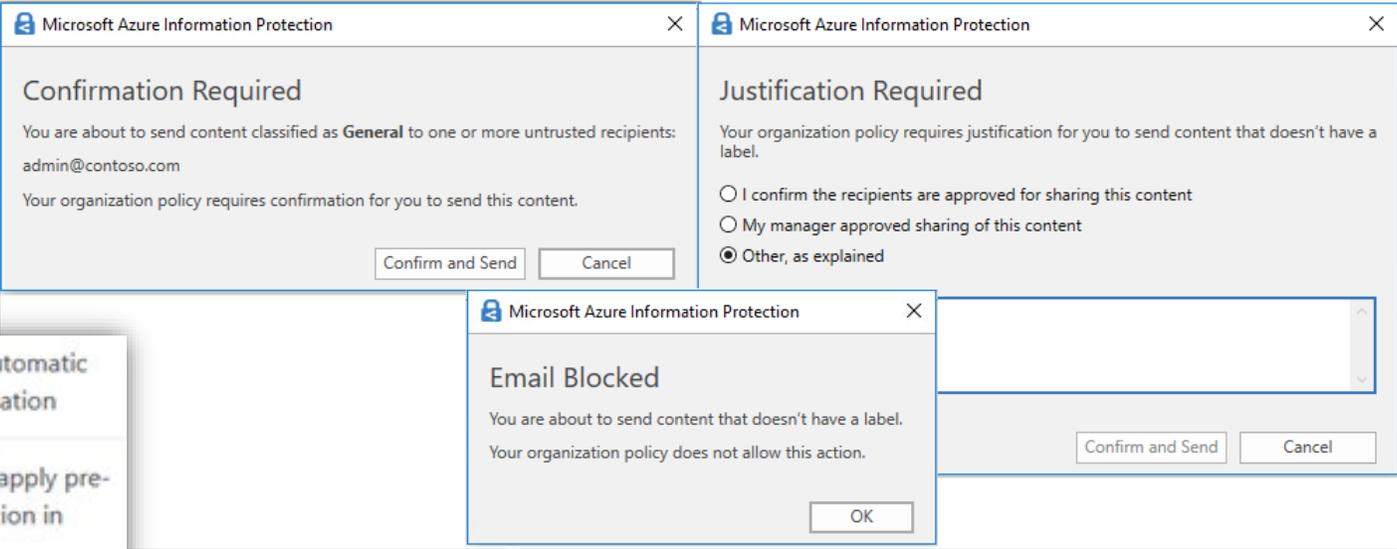
[Continue](#)

Didn't receive the one-time passcode? Check your spam folder or [get another one-time passcode](#).



# Modèles de licences et fonctionnalités AIP P1 et P2

## Azure Information Protection Premium P1 et P2



- Configure conditions for automatic and recommended classification
- Set labels to automatically apply pre-configured S/MIME protection in Outlook
- Control oversharing of information when using Outlook (warn, justify or block emails).
- Azure Information Protection scanner for automated classification, labeling, and protection of supported on-premises files

# Modèles de licences et fonctionnalités AIP P1 et P2

## AIP P2 Automatic classification and labelling

### Sensitive info types

Search

Select all

- Japan Bank Account Number Microsoft Corporation
- German Driver's License Number Microsoft Corporation
- U.K. National Insurance Number (NIN... Microsoft Corporation
- Japan Passport Number Microsoft Corporation
- France Passport Number Microsoft Corporation
- Singapore National Registration Ident... Microsoft Corporation
- Canada Driver's License Number Microsoft Corporation
- U.S. / U.K. Passport Number Microsoft Corporation
- Australia Tax File Number Microsoft Corporation
- India Unique Identification (Aadhaar) ... Microsoft Corporation
- SWIFT Code Microsoft Corporation
- Israel National ID Microsoft Corporation
- ABA Routing Number Microsoft Corporation
- New Zealand Ministry of Health Num... Microsoft Corporation
- Spain Social Security Number (SSN) Microsoft Corporation

**Add** Cancel

### Trainable classifiers

Trainable classifiers are used to identify categories of content specific to your organization, like contracts or employee agreements. [Learn more](#)

Search

Select all

- Offensive Language Microsoft
- Resumes Microsoft
- Source Code Microsoft
- Targeted Harassment Microsoft
- Profanity Microsoft
- Threat Microsoft

File Home Insert Design Layout References Mailings Review View Help **Share** **Comments**

AutoSave  Off

**POLICY TIP** Your organization recommends that you apply the sensitivity: All Employees. Confidential data that requires protection, which allows all employees full permissions. Data owners can track and revoke content. **Apply sensitivity**

Credit card: 4242-4242-4242-4242

# Des questions ?

