



Sécuriser Microsoft Copilot

Prévenir le prompt hacking et l'exposition des données avec Varonis

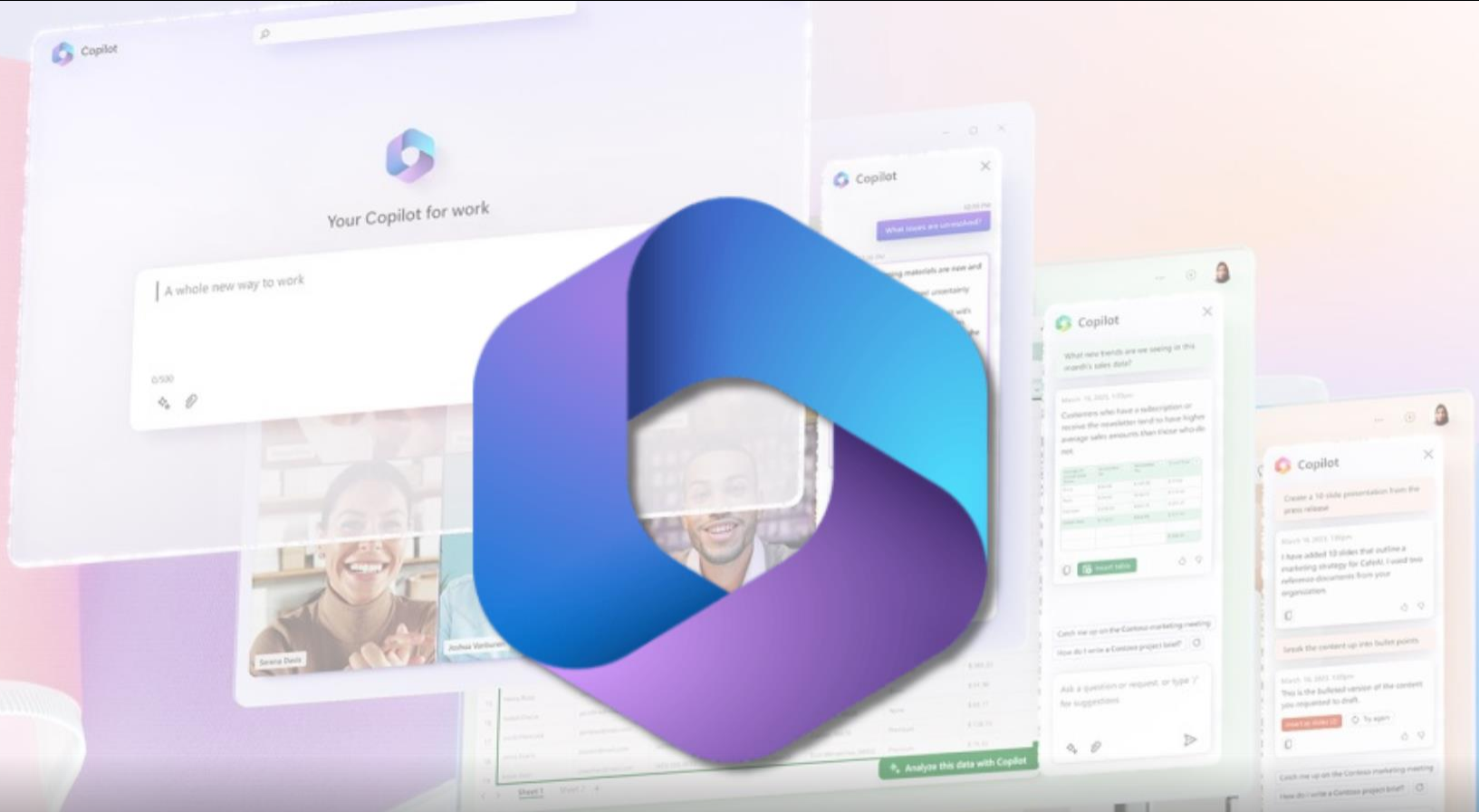
19 Septembre 2024



Programme

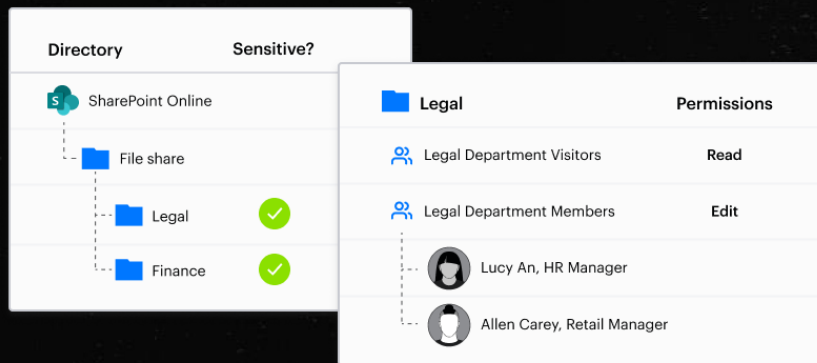
- + Qu'est-ce que Microsoft Copilot et comment fonctionne-t-il ?
- + Quels sont les risques pour la sécurité ?
- + Pourquoi ces défis sont-ils difficiles à relever ?
- + Comment activer Copilot en toute sécurité avec Varonis ?

**Qu'est-ce que
Microsoft Copilot et
comment
fonctionne-t-il ?**



« L'outil de productivité le plus puissant au monde. »
— Microsoft





Comment fonctionnent les contrôles de sécurité Copilot ?

+ Un utilisateur saisit un prompt dans une application comme Word, Outlook ou PowerPoint.

+ Microsoft recueille le contexte métier **en fonction des autorisations M365 de l'utilisateur.**

+ Le prompt modifié est envoyé au LLM pour générer une réponse.

+ Microsoft effectue des contrôles d'IA responsables post-traitement.



ON A DÉPLOYÉ COPILOT



**LES PERMISSIONS/LABELS
SONT ALIGNÉS ?**



N'EST-CE PAS ?

Quelles sont les recommandations de Microsoft ?

The following capabilities from Microsoft Purview strengthen your data security and compliance for Microsoft 365 Copilot:

- Sensitivity labels and content encrypted by Microsoft Purview Information Protection
- Data classification
- Customer Key
- Communication compliance
- Auditing
- Content search
- eDiscovery
- Retention and deletion
- Customer Lockbox

[management and security in SharePoint, OneDrive, and Teams](#), watch [this video](#), and read [this article](#) to get details on how to adopt content management best practices.

**Quels sont les
risques pour la
sécurité ?**



Copilot

For Microsoft 365

What's new?

What's the latest from **person**, organized by emails, chats, and files?

Get the gist

Give me a bullet list of key points from **file**

Draft an FAQ

Create an FAQ based on **file**

How to

How do I write a request for proposal?

Generate ideas

List ideas for a fun remote team building event

Help me write

Write an email to my team about our top priorities for next quarter from **file**

OK, what can I help with? Try one of the examples or enter your own prompt.



Copilot

For Microsoft 365

What's new?

What's the latest from `person`, organized by emails, chats, and files?

Get the gist

Give me a bullet list of key points from `file`

Draft an FAQ

Create an FAQ based on `file`

How to

How do I write a request for proposal?

Generate ideas

List ideas for a fun remote team building event

Help me write

Write an email to my team about our top priorities for next quarter from `file`

OK, what can I help with? Try one of the examples or enter your own prompt.



Copilot

For Microsoft 365

What's new?

What's the latest from **person**, organized by emails, chats, and files?

Get the gist

Give me a bullet list of key points from **file**

Draft an FAQ

Create an FAQ based on **file**

How to

How do I write a request for proposal?

Generate ideas

List ideas for a fun remote team building event

Help me write

Write an email to my team about our top priorities for next quarter from **file**

OK, what can I help with? Try one of the examples or enter your own prompt.



Copilot

For Microsoft 365

What's new?

What's the latest from `person`, organized by emails, chats, and files?

Get the gist

Give me a bullet list of key points from `file`

Draft an FAQ

Create an FAQ based on `file`

How to

How do I write a request for proposal?

Generate ideas

List ideas for a fun remote team building event

Help me write

Write an email to my team about our top priorities for next quarter from `file`

OK, what can I help with? Try one of the examples or enter your own prompt.

Access Intelligence

File server = All

Attributes

https://varonistest226.sharepoint.com > \ > sites > HR > Documents > **Salary and Compensation**

Name	Size of F...	Stale (incl. su
Employee Heaitncare.csv	0.004	Yes
> HR - Documents	0	Yes
> Interview Summary	3.427	Yes
> Job Descriptions	1.437	Yes
> NewEmployees	0.352	Yes
> Salary and Compensation	93.064	No
> Temp CVs	1.287	Yes
> Training	0.014	No
Site Assets	0.011	No
Site Pages	0.001	Yes
> Legal	8.851	No
> Marketing	0.014	No
> Operations	3.402	No
> RD	0.013	No
> RemoteWorkforceSupport	0.018	Yes
> Sales	3.401	No

Salary and Compensation

SharePoint Online | Created: 11/01/2022 5:46 PM | Modified: 11/01/2022 5:48 PM

Path: /sites/HR/Documents/Salary and Compensation

Anyone Org-wide Sensitive Protected

Permissions Statistics Compliance Info

Affiliation All

ANONYMOUS LOGON Abstract	Guest Link (Edit)
Anyone in the organization with the li... varonistest226.onmicrosoft... Org-wide	Contribute
Anyone in the organization with the li... varonistest226.onmicrosoft... Org-wide	Read
Site collection Administrators 3/38 https://varonistest226.sharepoint.com	Full Control
HR Owners 2/3 https://varonistest226.sharepoint.com	Full Control
HR Visitors https://varonistest226.sharepoint.com	Read
HR Members 2/5 https://varonistest226.sharepoint.com	Edit

View Full Table

Attributes

https://varonistest226.sharepoint.com > \> sites > HR

Name	Permission
> ChannelManagement	⊖
> Demo	⊖
> FederalSales	⊖
> Finance	⊖
▼ HR	✔ Edit
> Documents	✔ Edit
Site Assets	✔ Edit
Site Pages	✔ Edit
> Legal	⊖
> Marketing	⊖
> Operations	⊖
> RD	⊖
> RemoteWorkforceSupport	⊖
> Sales	⊖
> https://varonistest226-my.sharepoint.com	
> psg6cae7fs01	

HR

SharePoint Online | Created: 10/31/2022 4:08 PM | Modified: 03/06/2024 5:18 PM

Path: /sites/HR

Org-wide Sensitive Protected

Permissions Statistics Compliance Info

Affiliation All

- Site collection Administrators | https://varonistest226.sharepoint.com | Full Control
- HR Owners | https://varonistest226.sharepoint.com | Full Control
- HR Visitors | https://varonistest226.sharepoint.com | Read
- HR Members | https://varonistest226.share... | Org-wide | Edit
- Everyone | Abstract | Org-wide
- HR Members | varonistest226.onmicrosoft.com (Azure)

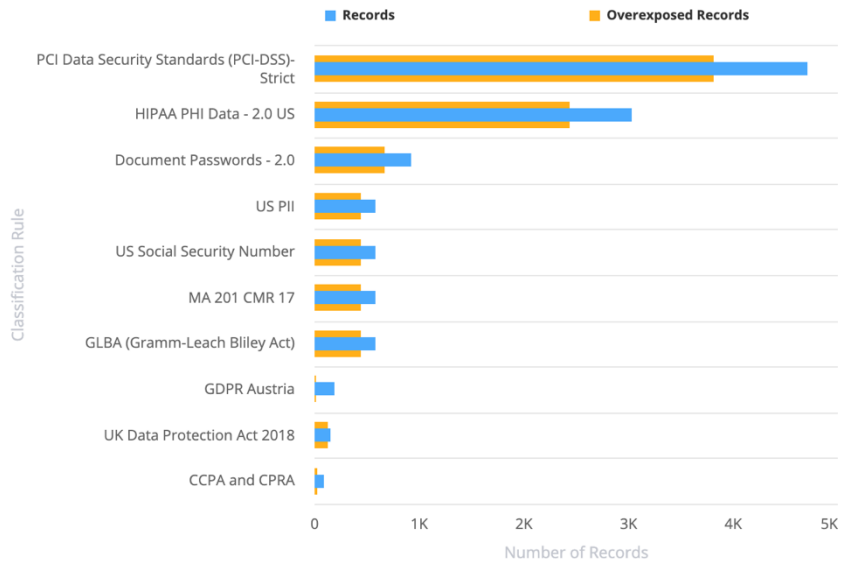
Compliance

File server = All

Compare over time

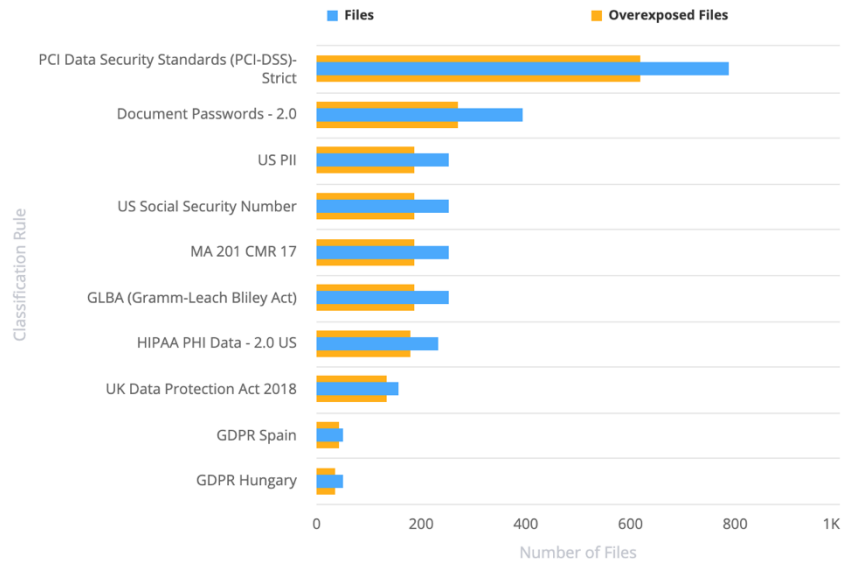
Overexposed Records by Rule

Rules All



Overexposed Files by Rule

Rules All



Overexposed Sensitive Files

786
No change

Mislabeled Files

159
No change

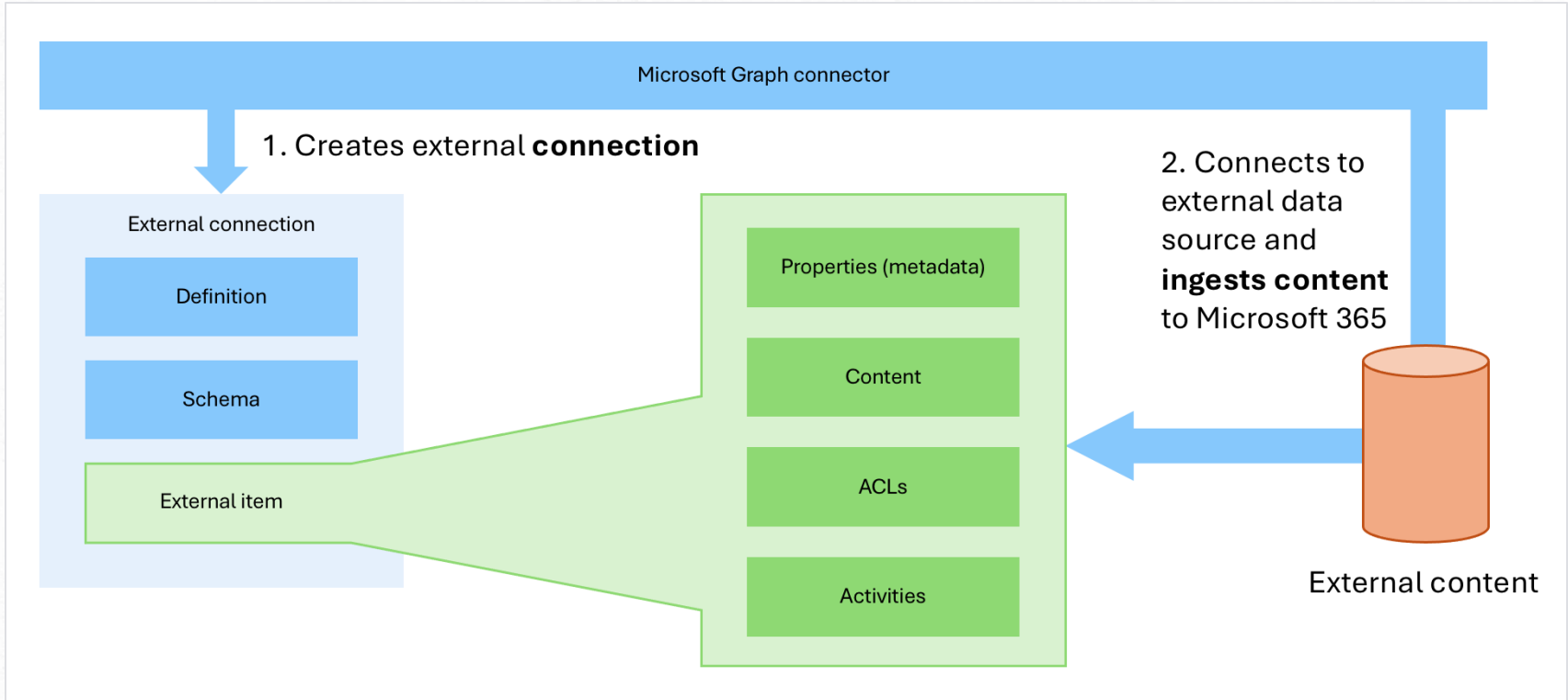
Resolved Mislabeled Files

52
No change

Files with Label Downgraded by User

0
No change

Comment fonctionnent les Graph Connectors ?



Vos autorisations externes doivent également être correctes.

Item Id
ACL
Properties
Content

```
{  
  "@odata.type": "microsoft.graph.externalItem",  
  "acl": [{  
    "type": "User",  
    "value": "c3a8d94d-f807-4785-b1c0-f0f4dbc9f54"  
    "accessType": "deny",  
    "identitySource": "azureActiveDirectory"  
  }, {  
    "type": "Group",  
    "value": "contosoEscalations"  
    "accessType": "grant",  
    "identitySource": "External"  
  }, {  
    "type": "Everyone",  
    "value": "07ea6043-dab2-4448-9d7f-70dba909a9c"  
    "accessType": "grant",  
    "identitySource": "azureActiveDirectory"  
  }  
],  
}
```

**Pourquoi ces défis
sont-ils difficiles à
relever ?**

Sécurité de Copilot

Les challenges

- Les employés ont accès à beaucoup trop de données
- Les données sensibles ne comportent souvent aucun label ou un mauvais niveau
- Les personnes internes peuvent rapidement identifier et exfiltrer des données
- Les attaquants peuvent découvrir des secrets à des fins d'escalade aux privilèges et/ou de mouvements latéraux
- Il est impossible de modifier tous les accès et d'appliquer le principe de moindre privilège manuellement
- L'IA générative peut créer de nouvelles données sensibles très rapidement

The background is a solid blue color with several diagonal stripes of varying shades of blue running from the top-left to the bottom-right. In each of the four corners, there is a white dashed-line bracket shape, resembling a corner of a square frame.

**Activer Copilot en
toute sécurité avec
Varonis**



Nasdaq Market Activity News + Insights Solutions About Nasdaq+ 🔍 🌐

Varonis Accelerates Secure Adoption of Microsoft Copilot for Microsoft 365

PUBLISHED
JAN 23, 2024 9:00AM EST

f Integration lays the foundation for secure and compliant deployment of Microsoft Copilot for Microsoft 365

in NEW YORK, Jan. 23, 2024 (GLOBE NEWSWIRE) -- [Varonis Systems, Inc.](#) (Nasdaq: VRNS), a leader in data security, today announced a strategic collaboration with Microsoft to help companies safely harness the power of AI. The integration helps joint customers continually assess and improve their Microsoft 365 data security posture before, during, and after they deploy Microsoft Copilot for Microsoft 365.

t

e



« L'intégration de Varonis fournit aux clients les contrôles de sécurité et de conformité supplémentaires nécessaires pour adopter rapidement et en toute confiance Microsoft Copilot pour Microsoft 365. »

Anat Gil, responsable des partenaires, Microsoft Europe

FORRESTER®

WAVE
LEADER 2023

Data Security Platforms



Varonis est une **solution idéale** pour les entreprises qui souhaitent visualiser précisément leurs données, exploiter les fonctionnalités de classification et bénéficier d'une remédiation automatisée pour l'accès aux données.

Forrester Wave™ : Plateformes de sécurité des données, 1er trimestre 2023

Sécurité des données entièrement automatisée



Visibilité en temps réel

Déterminez le véritable niveau de sécurité de vos données en temps réel.



Prévention automatisée

Réduisez continuellement votre rayon d'exposition, appliquez des labels et mettez en œuvre des politiques.



Détection proactive

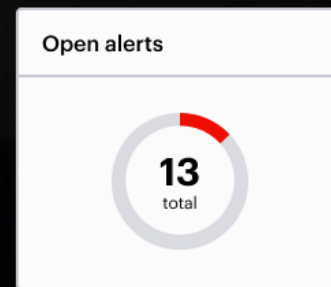
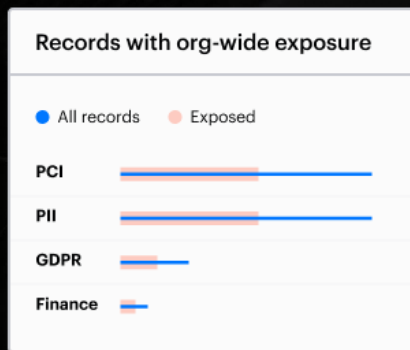
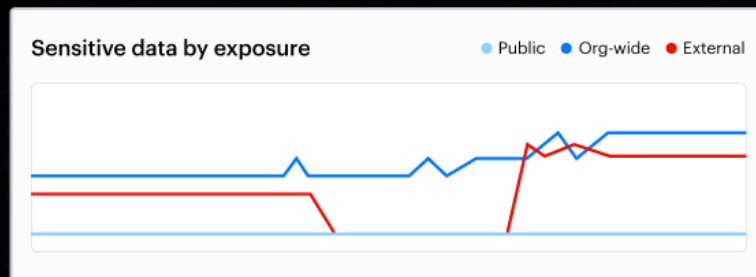
Always-on, UEBA centrée sur les données + l'équipe de réponse à incident de Varonis.

Phase 1

**Avant le déploiement de
Copilot**









1. Déployer la solution et effectuer les analyses initiales

- ✓ Recherche et classification des données
- ✓ Configuration et posture de sécurité
- ✓ Contrôles d'accès et liens partagés
- ✓ Applications tierces connectées
- ✓ Labels existants



2. Ajouter et corriger les labels de confidentialité de Purview

- + Identifiez automatiquement les fichiers manquants ou qui n'ont pas de label précis
- + Identifiez et corrigez automatiquement les labels erronés
- + Identifiez et corrigez automatiquement les fichiers dont les labels sont manquantes
- + Utilisez le **droit d'utilisation EXTRACT** pour marquer les fichiers et **prévenir l'accès à Copilot**.

File	Classification results	Classification labels
	PCI	
	GDPR, PII	 
	CCPA, PII	 

3. Remédier à une exposition à haut risque

Par exemple, appliquez une politique visant à supprimer les liens de partage de données sensibles dans l'ensemble de l'entreprise.

The screenshot displays a configuration interface for a security policy. At the top, the resource is set to 'prod1.sharepoint.com'. Below this, there are several filter criteria: 'Permission' (set to 'anyone on the internet'), 'Removal link' (set to 'Yes'), 'Link type' (set to 'org'), and 'Sensitive (incl. subfolders)' (set to 'OneDrive' and 'SharePoint Online'). An 'Add filter' button is also present. Under the 'Actions' section, the 'Remove permission' action is selected. The 'Execute actions' dropdown is set to 'Continuously'. A 'Preview results' button is located at the top right.

The line graph, titled 'Org-wide sharing links', shows the number of sharing links over time from 4/1 to 9/1. The y-axis ranges from 0 to 75K. The number of links starts at approximately 40K in April, rises to about 60K in May, then spikes to nearly 75K in June. It remains high through July, then drops sharply to near zero by late July, and stays low through September.

Month	Number of Links (Approximate)
4/1	40,000
5/1	55,000
6/1	70,000
7/1	72,000
8/1	5,000
9/1	5,000



Copilot

For Microsoft 365

What's new?

What's the latest from `person`, organized by emails, chats, and files?

Get the gist

Give me a bullet list of key points from `file`

Draft an FAQ

Create an FAQ based on `file`

How to

How do I write a request for proposal?

Generate ideas



List ideas for a fun remote team building event

Help me write

Write an email to my team about our top priorities for next quarter from `file`






OK, what can I help with? Try one of the examples or enter your own prompt.

4. Vérifier l'accès aux données critiques

 Display sensitive files available to large number of users in 365 

379 Results Resources with anyone exposure **17** Resources with org-wide exposure **56** Resources with stale access **314**

[Attributes](#) [Actions](#) ▾ [Export](#)

Sensitive	Path	Total record count	Classification
	/HR/Documents/Salary and Compensation/UK	522	*PCI (18). *PHI (2). *PPI (3)
	/HR/Documents/Salary and Compensation/Cyprus	520	*PCI (18). *PHI (2). *PPI (3)
	/HR/Documents/Salary and Compensation/UK/UsersUK.csv	488	*PCI (18). *PHI (2). *PPI (3)
	/HR/Documents/Salary and Compensation/Cyprus/UsersUK.csv	256	*PCI (18). *PHI (2). *PPI (3)
	/Legal/Documents/Corporate/Web	246	*PCI (18). *PHI (2). *PPI (3)

5. Activer les contrôles DLP en aval

- ✓ Chiffrer les données sensibles
- ✓ Empêcher les partages risqués
- ✓ Bloquer les tentatives d'exfiltration
- ✓ Appliquer des contrôles au niveau des fichiers
- ✓ Appliquer la résidence et la rétention

The screenshot shows the 'Microsoft 365 compliance' interface. The breadcrumb is 'Data Loss Prevention > Create a policy'. A progress bar on the left indicates the current step: 'Choose the information to protect' (checked), 'Name your policy' (checked), 'Locations to apply the policy' (active), 'Policy settings', 'Test or turn on the policy', and 'Review your settings'. The main content area is titled 'Choose locations to apply the policy' and includes a sub-header: 'We'll apply the policy to data that's stored in the locations you choose.' Below this is a table with columns for Status, Location, Included, and Excluded. A note above the table states: 'Protecting sensitive info on Windows devices is now in preview. Learn more about the capabilities'.

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> On	Exchange email	All Choose distribution group	None Exclude
<input checked="" type="checkbox"/> On	SharePoint sites	All Choose site	None Exclude
<input checked="" type="checkbox"/> On	OneDrive accounts	All Choose account	None Exclude
<input checked="" type="checkbox"/> On	Teams chat and channel messages	All Choose account	None Exclude
<input checked="" type="checkbox"/> On	Devices	All Choose user or group	None Exclude
<input checked="" type="checkbox"/> On	Microsoft Cloud App Security	All Choose instance	None Exclude

- Home
- Copilot
- Create
- My Content
- Feed
- Apps

Create a SWOT analysis in loop based on this info

SWOT Analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> Offers sustainable building materials, a growing market Good reputation for quality products Strong gross profit margin in Q1 2023 	<ul style="list-style-type: none"> Production and supply chain Inefficient cost management Quality control problems
Opportunities	Threats
<ul style="list-style-type: none"> Growing demand for sustainable materials Expansion of product line Investment in supply chain efficiency 	<ul style="list-style-type: none"> Fluctuations in raw material prices Changes in government policies or regulations Price sensitivity in a sagging market

+ Add a row

Copy
 Open in Word

1 reference

AI-generated content may be incorrect.



What are some additional threats?

What were our gross profits in Q1?



Ask a work question or make a request



Activer Copilot











Phase 2

**Après l'onboarding
de Copilot**

6. Surveiller l'activité de Copilot

- + Collecter et enrichir les sources d'audit de Copilot
 - + Journal d'audit de conformité
 - + Recherche de contenu
 - + e-Discovery
 - + Conformité en matière de communication
- + Collecter et analyser toutes les interactions de Copilot : prompts et réponses

Platform	Event type	Object name	Is sensitive?	Prompt
	file accessed	schema_map.xml		Find admin passwords
	file accessed	10-K Report.docx		Find social security ...
	file deleted	bonuses.xlsx		Show bonuses given
	file created	Admin		Find admin passwords
	file accessed	commissions.pdf		Show commissions ...

7. Alerter en cas de comportement anormal via Copilot

- + Détecter les interactions inappropriées ou risquées
- + Détecter le partage d'informations confidentielles
- + Suivre les fichiers consultés et les labels pertinents
- + Appliquer des labels en réponse à des alertes



3 alerts



Abnormal data access pattern
via Copilot

Insider threat indication

David Johnson

djohnson@company.com

inactive entity

orphaned user

no mfa

8. Automatiser les politiques de sécurité des données

- ✓ Révoquer un accès superflu
- ✓ Corriger les erreurs de configuration
- ✓ Aligner les labels
- ✓ Désactiver les applications tierces
- ✓ Respecter le cycle de vie des données
- ✓ Résidence des données

The screenshot shows a configuration interface for a data security policy. At the top, there is a dropdown menu for 'Resource' set to 'prod1.sharepoint.com' and a 'Preview results' button. Below this is a grid of filter options:






Permission	Removal link	Yes
Permission	Link type	anyone on the internet org-wide
Resource	Sensitive (incl. subfolders)	OneDrive SharePoint Online

There is an '+ Add filter' button below the grid. Underneath the filters is an 'Actions' section with a blue bar containing a 'Remove permission' button. At the bottom, there is an 'Execute actions' dropdown menu set to 'Continuously'.

Type = All

24 Automations | [+ New Automation](#) | [Export](#)

Items per page 20 | < 1 2 >

Name	Category	Type	Approval	State
Disable stale users 	Remediation	Disable stale users	Yes	<input checked="" type="checkbox"/> Enabled
Remediate inconsistent permissions	Remediation	Remediate inconsistent per...	Yes	<input type="checkbox"/> Disabled
Remediate Org-wide exposure for Windows	Remediation	Remediate org-wide exposure	Yes	<input type="checkbox"/> Disabled
Remove "Anyone in the organization with the link" collaboration links 	Remediation	Remove collaboration links	Yes	<input type="checkbox"/> Disabled
Remove "Anyone on the internet with the link" collaboration links 	Remediation	Remove collaboration links	Yes	<input type="checkbox"/> Disabled
Remove "Specific people" collaboration links in OneDrive 	Remediation	Remove collaboration links	Yes	<input type="checkbox"/> Disabled
Remove collaboration links that over-expose sensitive data 	Remediation	Remove collaboration links	Yes	<input type="checkbox"/> Disabled
Remove direct permissions for disabled users	Remediation	Remove direct permissions f...	Yes	<input type="checkbox"/> Disabled
Remove direct permissions for dynamic groups	Remediation	Remove direct permissions f...	Yes	<input type="checkbox"/> Disabled
Remove direct permissions for non-org users	Remediation	Remove direct permissions f...	Yes	<input type="checkbox"/> Disabled
Remove direct permissions for org-wide groups	Remediation	Remove direct permissions f...	Yes	<input type="checkbox"/> Disabled
Remove direct permissions for public groups	Remediation	Remove direct permissions f...	Yes	<input type="checkbox"/> Disabled
Remove direct permissions for stale users	Remediation	Remove direct permissions f...	Yes	<input type="checkbox"/> Disabled
Remove memberships of disabled users	Remediation	Remove memberships of dis...	Yes	<input type="checkbox"/> Disabled
Remove memberships of disabled users from "Specific people" collaboration links	Remediation	Remove memberships of dis...	Yes	<input type="checkbox"/> Disabled
Remove memberships of dynamic groups	Remediation	Remove memberships of dy...	Yes	<input type="checkbox"/> Disabled
Remove memberships of non-org users	Remediation	Remove memberships of no...	Yes	<input type="checkbox"/> Disabled

Plan de vol de Copilot

Avant Copilot :

- + Déployer Varonis
- + Effectuer les analyses initiales
- + Ajouter et corriger des labels de confidentialité
- + Remédier à une exposition à haut risque
- + Vérifier l'accès aux données critiques
- + Activez la DLP en aval avec Purview

Après Copilot :

- + Surveillance, UBA et alertes continues
- + Automatiser les politiques de contrôle d'accès, de DLP et de cycle de vie des données

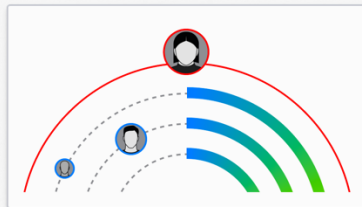


Évaluation de l'état de préparation de M365 Copilot

1.7K overexposed sensitive files

Platform	Classification	Exposure
	PII, PI	share externally
	PCI, CCPA	share externally
	PII	share externally

Classification et labeling des données créées par Copilot.



Réduction du rayon d'exposition de Copilot.



3 alerts

Cameron Hubbard accessed an anomalous number of account records

Insider threat indication

Cameron Hubbard

chubbard@company.com

inactive entity orphanded user no mfa

Surveillance de l'activité de Copilot en temps réel.

Records with org-wide exposure

All records Exposed

PCI
PII
GDPR
Finance

Sensitive data by exposure

Public Org-wide External



Activation des contrôles DLP en aval.

MERCI DE VOTRE ATTENTION !

Simon FAVRE

sfavre@varonis.com

Sondage de satisfaction
Merci de votre feedback



Scannez-moi