



Safely Enabling Copilot with Varonis

Scott Leach | Vice President, Asia Pacific & Japan

12 August 2024

Flight Plan

- + Microsoft Copilot
- + What are the security risks?
- + Why are they hard to solve?
- + How to safely enable Copilot with Varonis



The image is a promotional collage for Microsoft Copilot. It features a large, central, stylized logo in shades of blue and purple. Surrounding this logo are several overlapping, semi-transparent windows that showcase the Copilot interface in various contexts:

- Top Left Window:** Displays the Copilot logo and the text "Your Copilot for work". Below it, a chat interface shows the prompt "A whole new way to work" and a video call window with participants "Sandra Davis" and "Joshua Williams".
- Top Right Window:** Shows a chat window with the prompt "What issues are unresolved?" and a list of tasks.
- Middle Right Window:** Displays a chat window with the prompt "What new trends are we seeing in this month's sales data?". It includes a table of sales data and a "Smart table" button.
- Bottom Right Window:** Shows a chat window with the prompt "Create a 10 slide presentation from the press release". It displays a list of slides and a "Break the content up into bullet points" button.

At the bottom of the collage, a large white quote is centered over a dark background:

**“The most powerful productivity tool on the planet.”
— Microsoft**



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.



Microsoft 365 Copilot



Microsoft's approach to AI security:

- ❑ User inputs a prompt in an app like Word, Outlook, or PowerPoint
- ❑ Microsoft gathers business content **based on their M365 permissions**
- ❑ Prompt is sent to the LLM to create a response
- ❑ Microsoft performs post-processing responsible AI checks

How to prepare for Microsoft 365 Copilot

Technical requirements and onboarding guide for IT admins

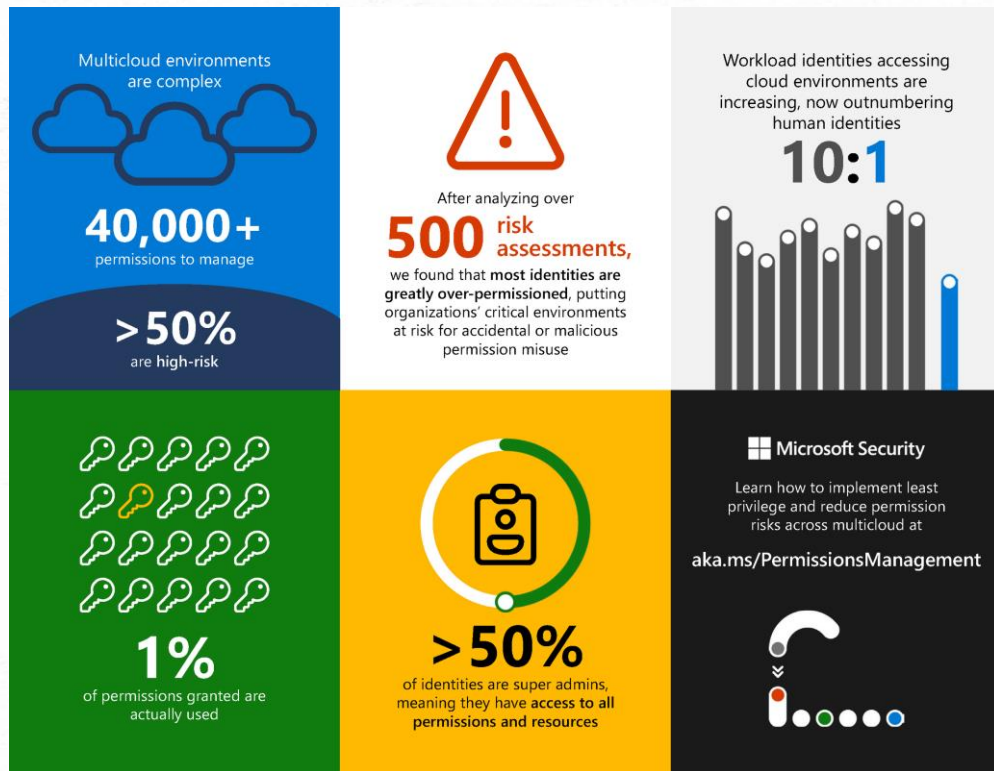


Permissions and content management best practices

Microsoft 365 Copilot uses your existing permissions and policies to deliver the most relevant information, building on top of our existing commitments to data security and data privacy in the enterprise. This means it is important to have good content management practices in the first place. For many organizations, content oversharing, and data governance can be a challenge. Content oversharing is when content is shared beyond the needed audience either intentionally or accidentally. Learn about some of the things your organization can do to detect and prevent oversharing in the [new era in content 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.

Microsoft's Cloud Permissions Report

- + Most identities are greatly over-permissioned
- + More than half of permissions are high risk
- + 99% of user permissions are unused





**What can someone
really do?**



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.

The background is dark with several diagonal stripes in shades of gray. In the corners, there are faint, dashed white lines forming brackets or corner markers.

Why, though?

Access Intelligence

File server = All

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.sharepoint.com Org-wide	Edit
	Everyone Abstract Org-wide	
	HR Members varonistest226.onmicrosoft.com (Azure)	

[View Full Table](#)

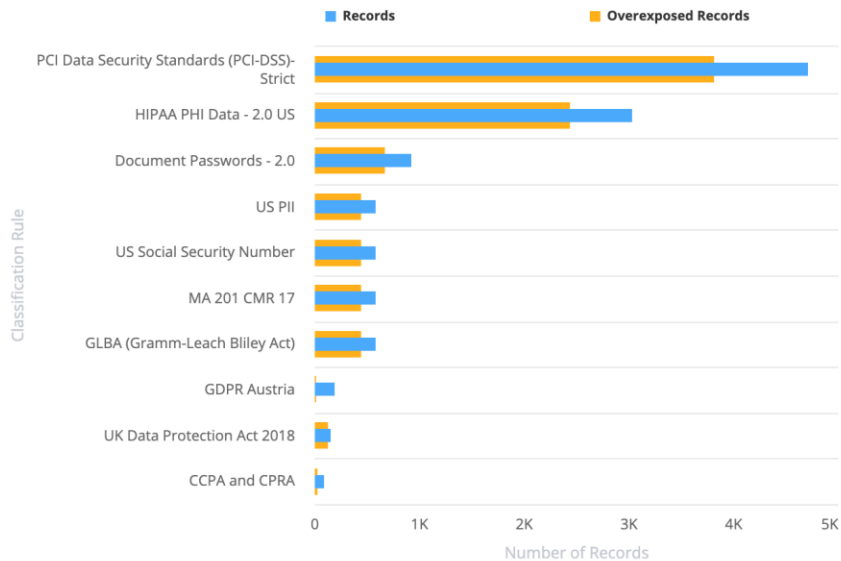
Compliance

File server = All

Compare over time

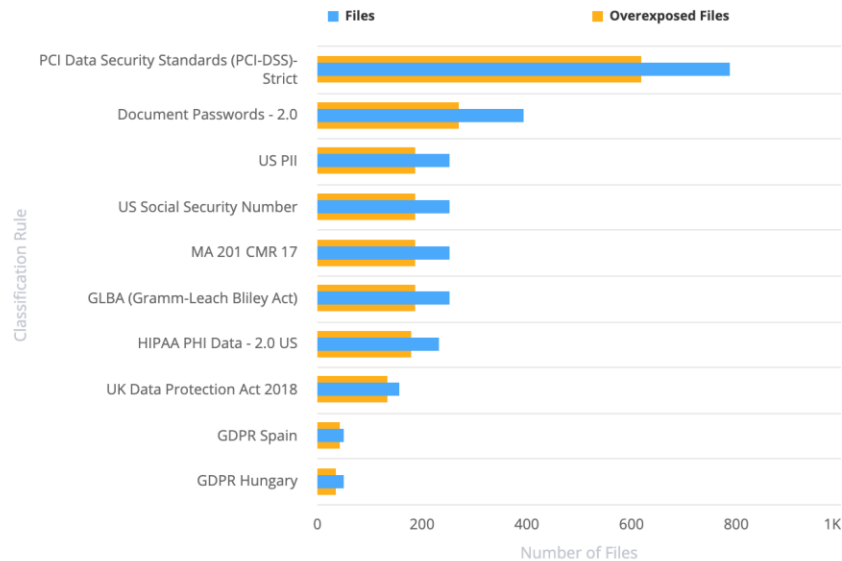
Overexposed Records by Rule

Rules All



Overexposed Files by Rule

Rules All



Overexposed Sensitive Files

786

No change

Misabeled Files

159

No change

Resolved Misabeled Files

52

No change

Files with Label Downgraded by User

0

No change

Copilot security Challenges

- Employees have access to far too much data
- Sensitive data is often not labeled or mislabeled
- Insiders can quickly find and exfiltrate data
- Attackers can find secrets for privilege escalation and lateral movement
- Right-sizing access and enforcing least privilege is impossible to do manually
- Generative AI can create net new sensitive data extremely fast



These are the **same**
problems we've had for
years!

- Everyone



Safely Enabling Copilot with Varonis





Varonis' integration gives customers the added security and compliance controls necessary to quickly and confidently adopt Microsoft Copilot for M365.

Anat Gil, Partners Lead, Microsoft



Varonis delivers real outcomes.



Real-time understanding of risk



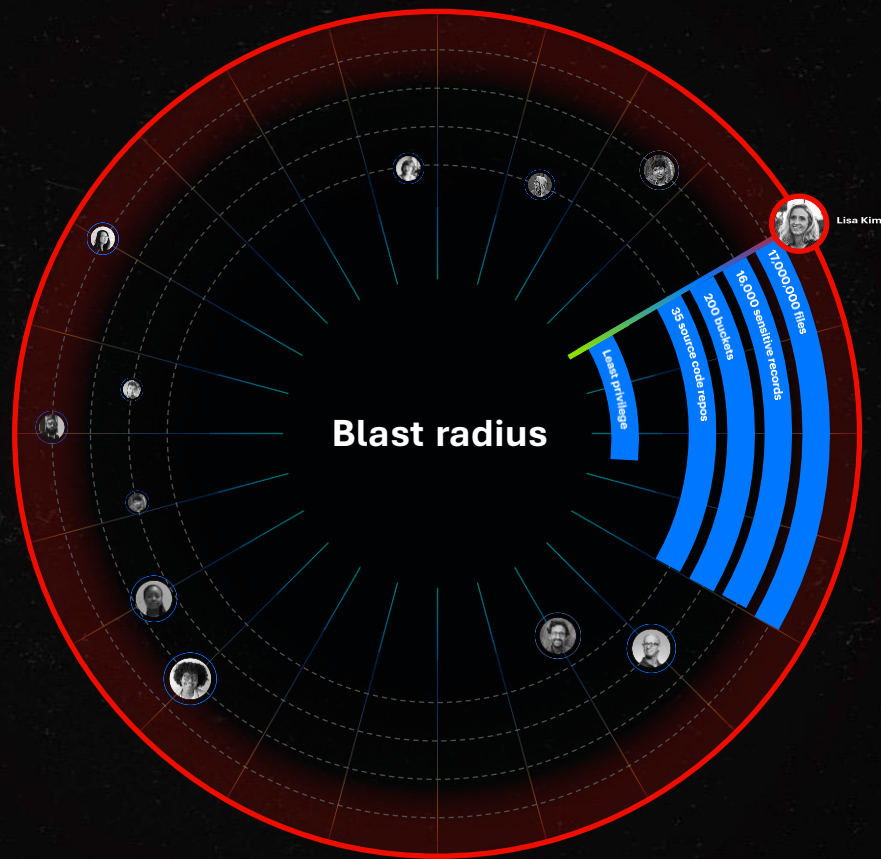
Continuously reduced blast radius



Data-centric detection



Simplified compliance, labeling



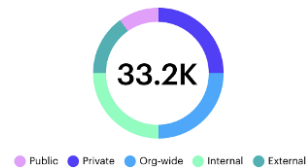


Phase 1: Before Copilot

1. Deploy and Complete Initial Scans

- ✓ Data sensitivity
- ✓ Configuration and security posture
- ✓ Access controls and shared links
- ✓ Connected third-party apps
- ✓ Existing labels

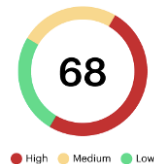
Overall data security posture



Sensitive data by exposure











Open misconfigurations



2. Add/Fix Purview Sensitivity Labels

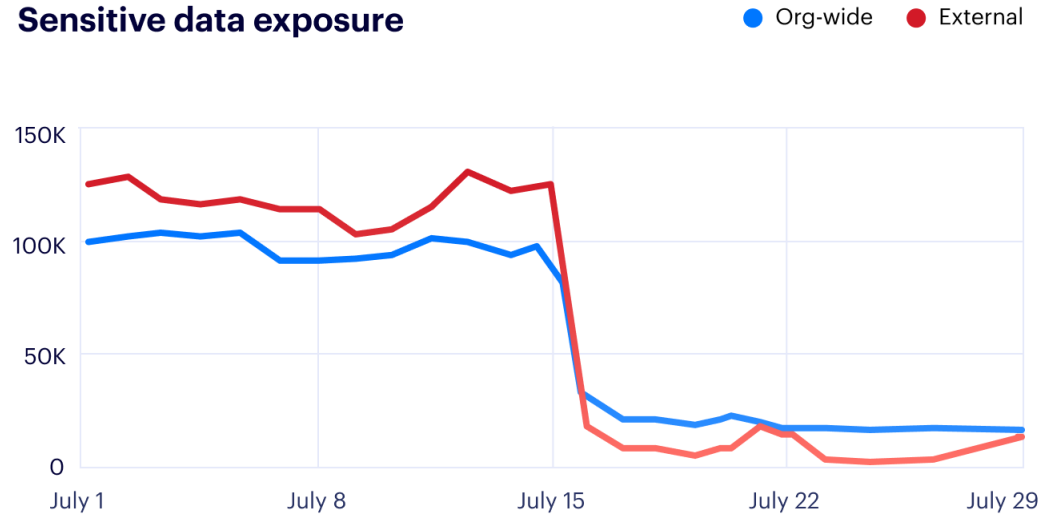
- + Automatically identify files that are missing or don't have accurate labels
- + Automatically identify and fix misapplied labels
- + Automatically identify and fix files with missing labels

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

3. Remediate High Risk Exposure

Type	Remove collaboration link
Policy name	Remove "Anyone in the
Description	This policy removes collaboration links with the link" type.
State	<input checked="" type="checkbox"/> Enabled

Sensitive data exposure



4. Review Access to Critical Data

Resources

display sensitive files available to large numbers of users in 365 Cancel Saved searches

379 Results

51 Unique resources | 51 Protected resources | 322 Direct sensitive resources | 17 Resources with anyone exposure | 56 Resources with org-wide exposure | 314 Resources with stale access

<< Refine Attributes Actions Export Items per page 100 1 2 3 4 >

Resource

Classification categories... (6)

Classification labels (dir... (1)

Classification rules (dir... (44)

Exposure level (3)

File servers (3)

Mailbox type (1)

Platforms (3)

Protected (13.5%)

Resource types (7)

Sensitive (direct) (85.0%)

Site types (3)

Stale (69.7%)

Drag here to set row groups

	Sensiti...	Path	New	Total Record Count (...)	Modify Date	Classification Results
<input type="checkbox"/>	Yes	/sites/HR/Documents/Salary and Compensation/UK		522	11/01/2022 5:46 PM	UK Data Protection Act 1998 (204/2
<input type="checkbox"/>	Yes	/sites/HR/Documents/Salary and Compensation/Cyprus		520	11/01/2022 5:46 PM	PCI Data Security Standards (PCI-D
<input type="checkbox"/>	Yes	/sites/HR/Documents/Salary and Compensation/UK/UsersUK.csv		488	11/01/2022 5:47 PM	UK Data Protection Act 1998 (190/1
<input type="checkbox"/>	Yes	/sites/HR/Documents/Salary and Compensation/Cyprus/UsersUK.csv		488	11/01/2022 5:47 PM	UK Data Protection Act 1998 (190/1
<input type="checkbox"/>	Yes	/personal/elenacabrera_varonistest226_onmicrosoft_com/Documents/SEC R...		256	12/07/2022 2:29 PM	California SB-1386 (18/18),HIPAA P
<input type="checkbox"/>	Yes	/sites/Legal/Documents/Corporate/Web stuff		246	11/01/2022 5:44 PM	PCI Data Security Standards (PCI-D
<input type="checkbox"/>	Yes	/personal/margaretcoakley_varonistest226_onmicrosoft_com/Documents/A...		231	12/07/2022 2:51 PM	MA 201 CMR 17 (33/33),GLBA (Grap
<input type="checkbox"/>	Yes	/sites/Finance/Documents/Controllers/Finance reports/Corporate/2006/Q1 ...		202	11/01/2022 5:43 PM	US Social Security Number (16
<input type="checkbox"/>	Yes	/sites/Finance/Documents/Financial Reports/alice/Billing MTIL01		168	11/01/2022 5:43 PM	Document Passwords - 2.0 (18/18),I

5. Enable Downstream DLP

- ✓ Encrypt sensitive data
- ✓ Prevent risky sharing
- ✓ Block attempted exfiltration
- ✓ Apply file-level controls
- ✓ Enforce residency and retention

The screenshot shows the 'Microsoft 365 compliance' interface, specifically the 'Data Loss Prevention > Create a policy' section. On the left, a vertical navigation pane lists the steps: '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. The table lists several locations with their respective status and options for inclusion or exclusion.

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



Microsoft 365 Copilot

Enable Copilot



Phase 2: After Copilot

6. Ongoing Monitoring and Alerting

- + Detect inappropriate or risky interactions
- + Detect sharing of confidential information
- + Track files accessed and relevant labels
- + Apply labels as a response to alerts



3 alerts



Abnormal data access pattern
via Copilot

Insider threat indication

David Johnson

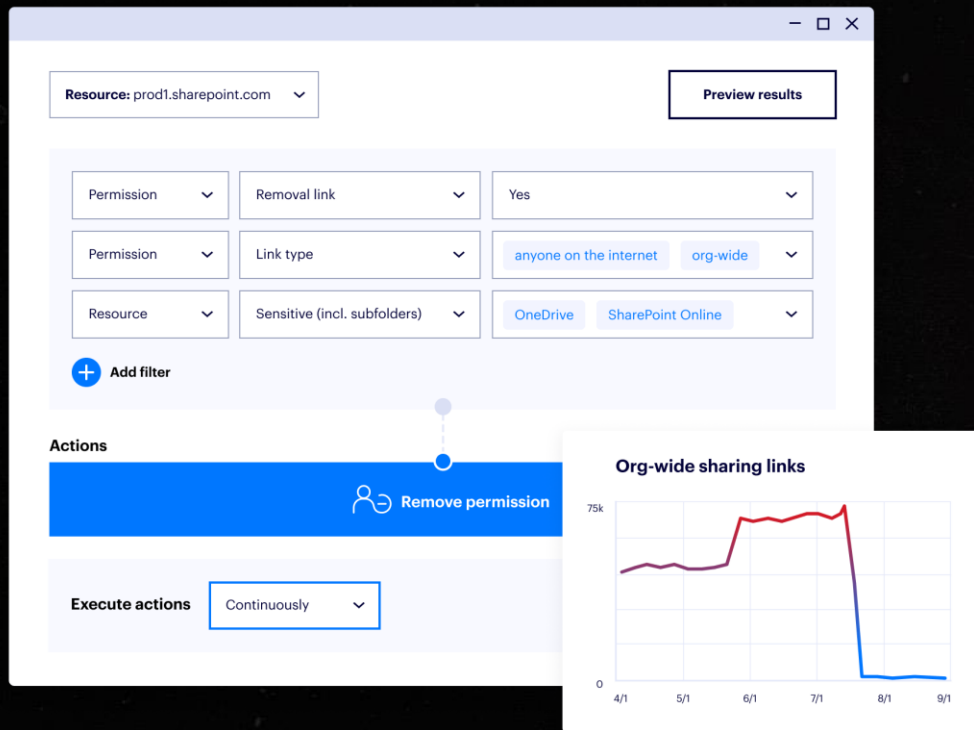
djohnson@company.com

inactive entity

orphaned user

no mfa

7. Automate Policies for Access Control



- ✓ Revoke excessive access
- ✓ Fix misconfigurations
- ✓ Fix labels
- ✓ Disable third-party apps
- ✓ Data lifecycle
- ✓ Data residency

Operational Plan Summary

Before Copilot:

- + Deploy Varonis
- + Complete Initial Scans
- + Add/Fix Data Labels
- + Remediate High-Risk Exposure
- + Review Access to Critical Data
- + Enable Downstream DLP with Purview

After Copilot:

- + Ongoing Monitoring and Alerting
- + Automate Access Control Policies



CoPilot Live

Prompts Today

4,242

Sensitive File References Today

895

Copilot

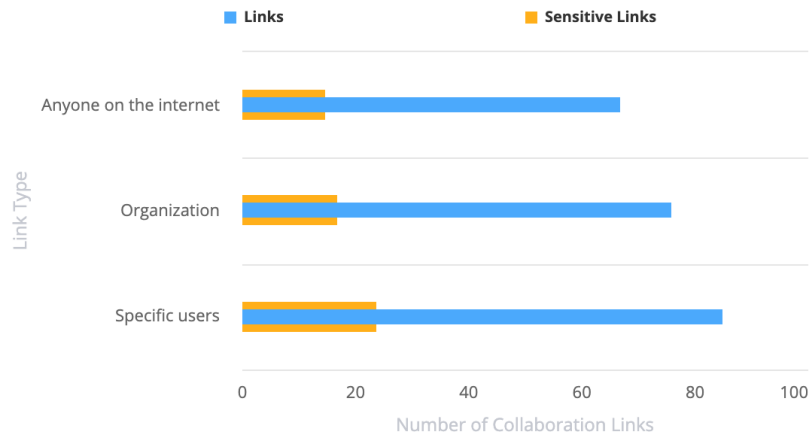
Data source = All

Compare over time

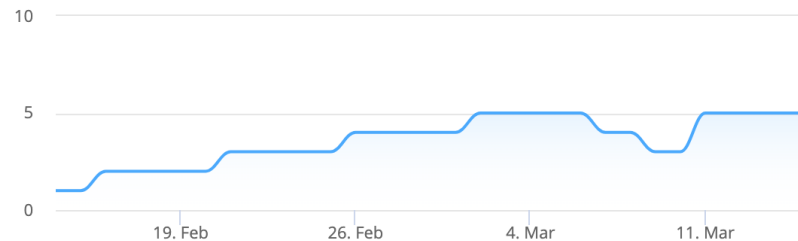


Collaboration Links by Type

Copilot Remediation



Overexposed Sensitive File References



Sensitive File References by Category

Categories All

Financial



Copilot Readiness in 10 days

Varonis reduced a financial institution's Copilot exposure by 99.8% in 10 days.
Zero impact on the business using 20 automation policies to lock down ~1 million files.

992K
files

Starting point

~1M files across the org's SharePoint, Teams, and OneDrive. Varonis quickly classified 120K sensitive files.

57K
exposed
files

Identifying Copilot risk

Used Varonis to identify exposed PHI, PII, credentials at risk of being exposed via Copilot.

99.8%
exposure
reduction

10-Day Difference

Automatically eliminated ~2K sharing links and right-sized access to 57K files with Varonis policies.

0
tickets
complaints

Zero customer impact

Proactively notified M365 admins of the remediation plan. The team heard zero complaints.

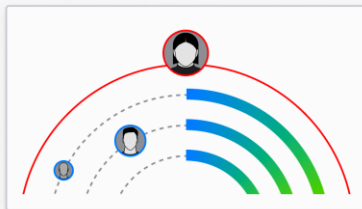


Microsoft 365 Copilot Readiness Assessment

🚨 1.7K overexposed sensitive files

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

Classify and label data Copilot creates.



Reduce Copilot's blast radius.



3 alerts

Cameron Hubbard accessed an anomalous number of account records

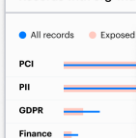
Insider threat indication

Cameron Hubbard
chubbard@company.com

inactive entity orphaned user no mfa

Monitor Copilot activity in real-time.

Records with org-wide exposure



Sensitive data by exposure



Enable downstream DLP controls.



Questions?



Thank you.

 VARONIS