



MICROSOFT 365 COPILOT SECURITY SCAN

ENSURE COPILOT SECURITY BEFORE, DURING,
AND AFTER DEPLOYMENT



“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 Europe

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 and 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 ticket complaints

Zero customer impact

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

MICROSOFT 365 COPILOT SECURITY SCAN

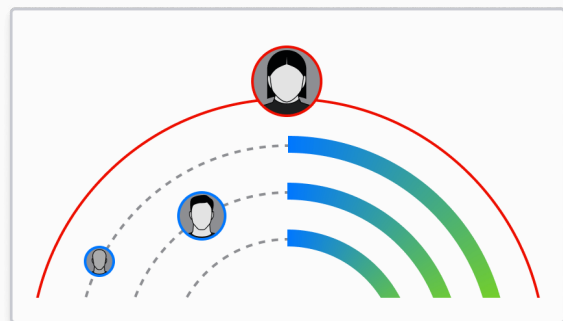


Classify and label data Copilot creates.

! 1.7K overexposed sensitive files

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

Reduce Copilot's blast radius.



Monitor Copilot activity in real-time.



3 alerts



Abnormal data access pattern via Copilot

Insider threat indication

David Johnson
djohnson@company.com

inactive entity orphaned user no mfa

Enable downstream DLP controls.

Records with org-wide exposure

All records Exposed

PCI
PII
GDPR
Finance

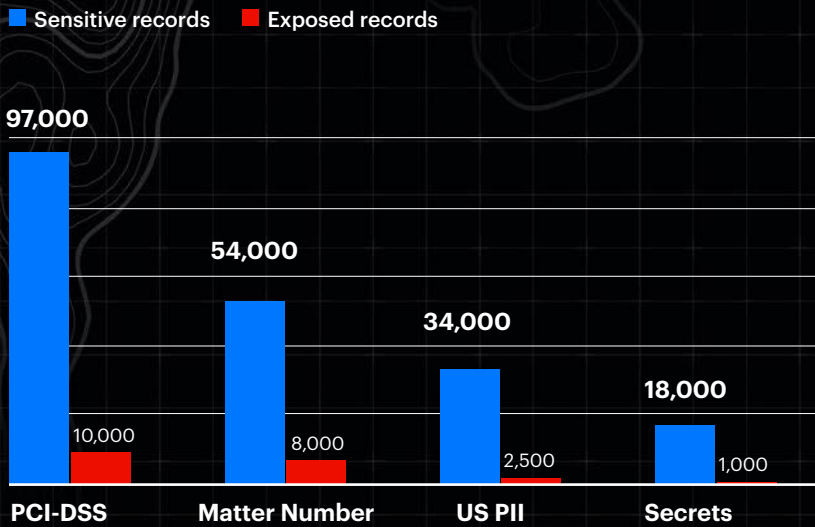
Sensitive data by exposure

Public Org-wide External

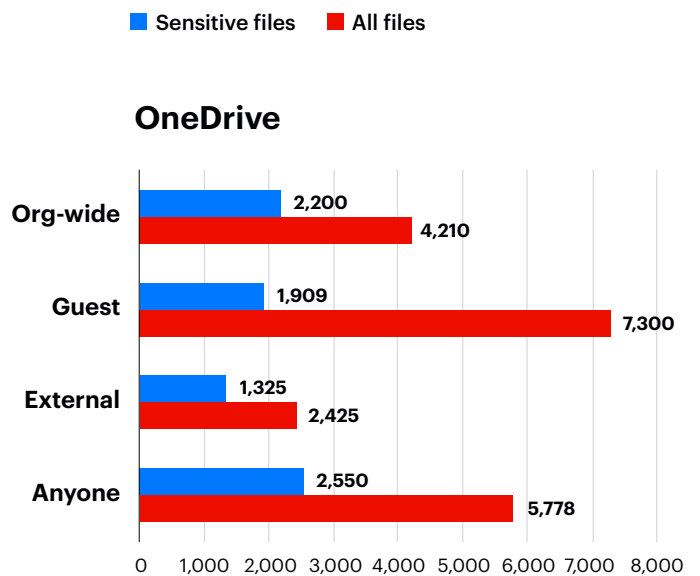
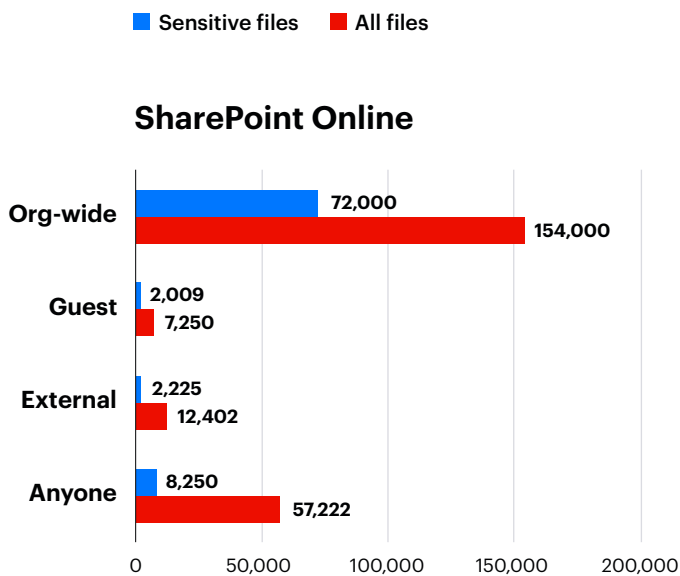


WHAT SENSITIVE DATA IS EXPOSED TO COPILOT?

Copilot posture dashboards help you decide if it's safe to deploy.



Copilot data exposure by level



HOW DOES COPILOT HAVE ACCESS TO SENSITIVE DATA?

Varonis shows you exactly how Copilot can access sensitive data by any method so you can fix issues before deploying.

- + Direct permissions
- + Group memberships (Teams, Azure, SharePoint, etc.)
- + Guest permissions
- + Anyone links
- + Org-wide links
- + Specific user links

The screenshot displays the 'Access Intelligence' interface. On the left, a file explorer view shows the file 'March 2006 billing.xls' under the root path 'https://varonistest226.sharepoint.com'. On the right, a detailed view of the file's permissions is shown. The file is titled 'March 2006 billing.xls' and has a path of '/sites/Finance/Documents/March 2006 billing.xls'. The permissions section lists several groups and users:

- Finance Mem...** (Group): Includes 'Elena Cabr...' (Elena Cabrera) and 'Erin Manni...' (Erin Manning).
- Specific People C...** (Group): Labeled 'Contribute', includes 'Zoey Caffrey' and 'mmathis138@...' (mmathis138@ou...).

Annotations with blue boxes and lines point to specific elements:

- A blue box on the left states: 'Elena is not on the finance team but joined the group via Teams. She should not have access to billing data.' A line points to the 'Elena Cabr...' entry in the 'Finance Mem...' group.
- Another blue box on the left states: 'Elena shared this file with a personal email account.' A line points to the 'Specific People C...' group, which is associated with the URL 'https://varonistest226...'.

Which sensitive files are mislabeled?

Copilot security relies heavily on accurate MPIP labels.
Varonis will find and fix MPIP labels.

We found 27,000+ sensitive files with no label applied. Copilot will not consider these files sensitive.

Path	Classification Results	Classification Labels	Name
C:\Share\Finance	US PII (0/43),HIPAA PHI Data - 2.0 US (0/...	GDPR Regulated Data (0/1)	Finance
C:\Share\Finance\Controllers	US PII (0/29),HIPAA PHI Data - 2.0 US (0/...		Controllers
C:\Share\Finance\Controllers\Finance repor...	US PII (2/7),HIPAA PHI Data - 2.0 US (12/...		Q1 2006
C:\Share\Finance\Controllers\Finance repor...	US PII (2/2),HIPAA PHI Data - 2.0 US (10/...		Inventory
C:\Share\Finance\Controllers\Finance repor...	US PII (3/3),HIPAA PHI Data - 2.0 US (15/...		Revenues
C:\Share\Finance\Controllers\Finance repor...	US PII (20/20),HIPAA PHI Data - 2.0 US (8...		SEC
C:\Share\Finance\data	Passwords (1/2),GDPR Greece (1/1),UK D...	GDPR Regulated Data (1/1)	data
C:\Share\Finance\DEMO94	Passwords (3/3),PCI Data Security Stand...		DEMO94
C:\Share\Finance\data\KolNet	Passwords (1/1),UK Data Protection Act ...		KolNet
C:\Share\Finance\Economics\Costing	[Preview] Document Passwords - 2.0 (6/...		Costing
C:\Share\Finance\Economics\Budget\2006\...	[Preview] Document Passwords - 2.0 (2/...		Final

Enable Copilot automation policies to quickly get M365 ready for deployment within days.

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

WHO IS ACCESSING SENSITIVE DATA VIA COPILOT PROMPTS?

Use Athena AI to ask questions like:

“Which users have accessed sensitive data via Copilot today?”

Marketing employee is surfacing finance data via Copilot interactions.

The screenshot shows a search interface with the query "Copilot references to sensitive files in the last 7 days". It displays 56 results, with 56 events on sensitive data and 56 events on data exposed to the whole organization. A table view shows the following data:

Drag here to set row groups			
<input type="checkbox"/>	Data Source Type	Event Time	Event Type
<input type="checkbox"/>	SharePoint Online	03/12/2024 6:10:30 PM	File referenced by Copilot Interaction
<input type="checkbox"/>	SharePoint Online	03/12/2024 6:10:30 PM	File referenced by Copilot Interaction

Who is abusing Copilot?

- + 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

COPILOT FLIGHT PLAN: STEP-BY-STEP

Before Copilot

- ✓ Deploy Varonis
- ✓ Complete initial scans
- ✓ Add and fix sensitivity labels
- ✓ Remediate high-risk exposure
- ✓ Review access to critical data
- ✓ Enable downstream DLP with Purview

After Copilot

- ✓ Monitor all Copilot usage and alert on suspicious behavior and sensitive data access
- ✓ Automate access control policies
- ✓ Automate DLP and data lifecycle policies



REDUCE YOUR RISK WITHOUT TAKING ANY.

Our free risk assessment takes minutes to set up and delivers immediate value. In less than 24 hours, you'll have a risk-based view of the data that matters most and a clear path to automated remediation.



Full access to the Varonis SaaS platform

Get full access to our Data Security Platform for the length of your assessment and get actionable insights for your most critical data.



Dedicated IR analyst

Being connected to the Varonis SaaS Data Security Platform means that our experts have eyes on your alerts and we'll call you if we see something alarming.



Key findings report

A detailed summary of your data security risks and an executive presentation to review the findings and recommendations. This report is yours to keep, even if you don't become a customer.

Get your free assessment today at Varonis.com.

Trusted by thousands of customers

