Microsoft 365 Copilot Readiness Assessment

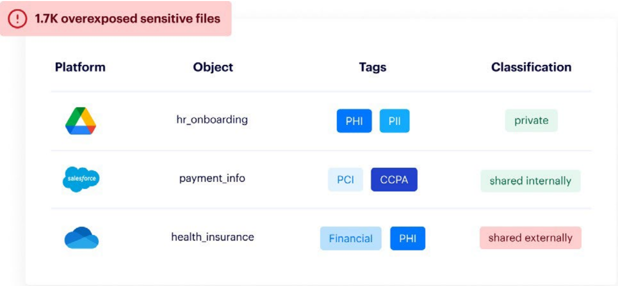
It's critical to improve your data security posture before your Copilot rollout. Varonis provides a free assessment that gives you a real-time view of gen AI risk in M365, automatically limits Copilot's data access, and alerts you to abnormal activity.

To help mitigate risk, Microsoft recommends securing sensitive data before rolling out Copilot by "making sure your organization has the right information access controls and policies in place."

Request your free assessment

Classify and label data Copilot creates.

Automatically discover, classify, and label sensitive and regulated data with extreme accuracy.



1.7K overexposed sensitive files

Platform	Object	Tags	Classification
	hr_onboarding	PHI PII	private
salesforce	payment_info	PCI CCPA	shared internally
	health_insurance	Financial PHI	shared externally

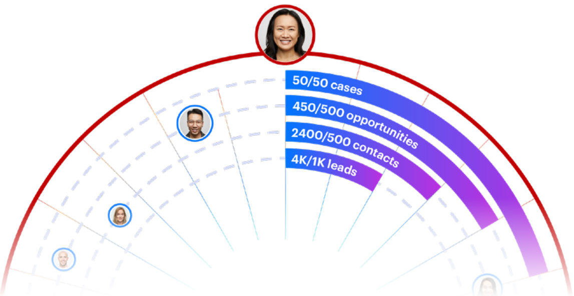
Enable downstream DLP controls.

Ensure AI-generated data is correctly labeled so your DLP policies work as intended.

Sensitive data exposure
Public
Org-wide
External
Records with org-wide exposure
All records
Exposed
PCI
PII
GDPR
Finance

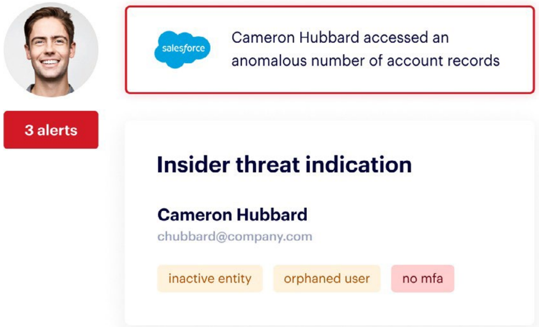
Reduce Copilot's blast radius.

Continually remediate data exposed to Copilot via excessive permissions with intelligent automation.



Monitor Copilot activity in real-time.

Get a searchable log with who, what, when, where, and how details. Alert on suspicious behavior.



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