VARONIS

Varonis for Microsoft 365

Protect your critical Microsoft 365 data with least privilege automation, data-centric UEBA, and world-class data classification.

Challenge

Collaboration features in Microsoft 365 can make it very difficult to protect data. In just a few clicks, users share information and create new permissions sets, all without the help of IT. Microsoft's built-in security tools are limited in their ability to know which sharing links are in use, and which ones aren't needed anymore — that's where Varonis comes in.

Solution

As a Microsoft Silver Partner, Varonis augments Microsoft's native security capabilities, helping collaboration flourish without compromising security. Varonis provides a single control point for securing cloud and on-prem data, simplifying the many admin portals that security teams would have to navigate within Microsoft. Varonis lowers your risk of data exposure by providing real-time visibility and control over your critical data, automatically remediating risk while you sleep.
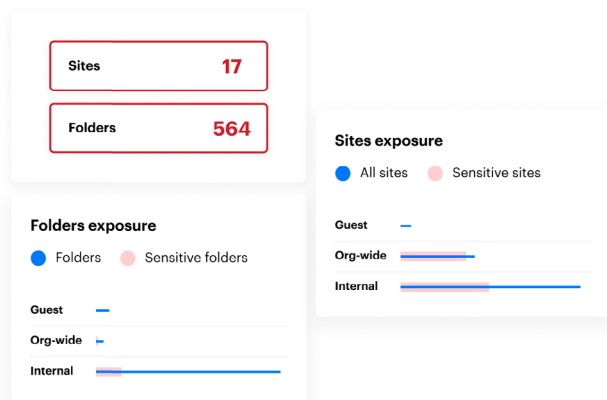
Key benefits

Hybrid visibility into cloud and on-prem activity

Sensitive data monitoring and alerting

Intelligent automation to achieve Zero Trust

Sites	17
Folders	564

Folders exposure
● Folders ● Sensitive folders

Guest
Org-wide
Internal

Sites exposure
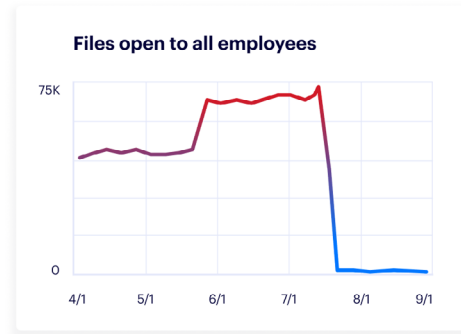● All sites ● Sensitive sites

Guest
Org-wide
Internal

> "The move to Microsoft 365 enabled our business to be more collaborative, but it's a dual-edged sword. Varonis is the crossguard that stops us from getting cut."

CIO, Leading Automotive Manufacturer

Read the case study →

Least privilege automation

Effortlessly eliminate data exposure from shared links and excessive permissions. Varonis makes intelligent decisions about who needs access to data and who doesn't, based on how sharing links are used (and not just based on a specific expiry time). With Varonis, you can enforce Zero Trust without an army of admins and without breaking the business.

Files open to all employees

Data classification and labeling

Varonis' vast library of policies uses sophisticated logic to generate accurate classification results that go beyond what Microsoft can find natively. We pair classification results with permissions to reveal where sensitive data is overexposed, providing a clear picture of risk. Use our labeling engine to apply persistent MPIP labels to sensitive files for encryption, DRM, and more.

Directory	Hit count	Classification rules
https://dm.sharepoint.com		
Sites		
Bonuses	975	CCPA, Confidential
CorpFSO2		
C:\share		
Legal	1,215	Classified
Finance	6,517	SOX

Files containing sensitive records	**8M**
Folders open to every employee	**2M**
Data at risk	**28%**

Data-centric threat detection and forensics

Varonis expands your field of vision by combining activity from Microsoft 365 and Azure AD with on-premises and perimeter telemetry to build more complete threat models.

Our behavior-based detections deliver only alerts that matter. Enriched logs viewable from a single interface make investigations fast and comprehensive.

Abnormal behavior: activity from new geolocation to the organization	3
Abnormal behavior: an unusual amount of data was uploaded	3
GDPR data was shared publicly	2
Abnormal behavior: activity from new geolocation to the organization	2
Encryption of multiple files	2

Try Varonis for free.

Varonis takes just minutes to install and provides data security insights instantly. Get started today at **varonis.com/trial.**

Available on the Azure and AWS marketplaces.

VARONIS