VARONIS

Remediating Risk and Securing Data in Shared DoD Microsoft 365 Tenants

Table of contents

Securing Data in DoD IL5 Microsoft 365

The unmanaged risk of command consolidation

The Department of Defense (DoD) recently migrated its sub-organizations into consolidated Microsoft 365 tenants — each containing hundreds of thousands of users. Previously, data for each sub-organization was stored in a silo, so users in one command could not access data belonging to another command.

In Microsoft 365, Microsoft's primary mission is to facilitate productivity and collaboration. All security and administrative controls are managed at the tenant level. Individual commands have no visibility into who can access their data, where mission-critical data is stored, or even how that data is used. No administrative boundaries in place means users can access sensitive data within an unrelated command.

The result: individual commands cannot protect data stored in consolidated tenants, comply with Executive Order (EO) 14028, or implement the DoD's Zero-Trust requirements.

The capacity to create, share, and expose data has far exceeded the ability to protect it. With Varonis, DoD commands can close the visibility and protection gap and secure data stored in OneDrive, SharePoint Online, and Teams.

Why can Microsoft 365 be hard to protect?

Before the cloud, the security model for on-premises data was managed by administrators who determined which users should or should not have access to data. In Microsoft 365, the security model is controlled by end users. The capacity to create, share, and expose data has far exceeded the ability to protect it. End users can easily break the data security model with a few clicks from any number of applications. Collaboration workflows allow any user to share sensitive data with everyone in the tenant — including guest users.

The resulting complexity makes it extremely difficult for administrators to understand who has access to sensitive data. Without a way to centrally visualize, manage, and remediate risks to their data in a Microsoft 365 consolidated tenant, administrators must:

- Manually search Teams or Azure AD to identify Teams members and data owners
- Manually search SharePoint Online (advanced view) to see who has received links to files, folders, sites, and where permissions have been granted directly through SharePoint Online
- Manually review individual permissions on files stored in OneDrive

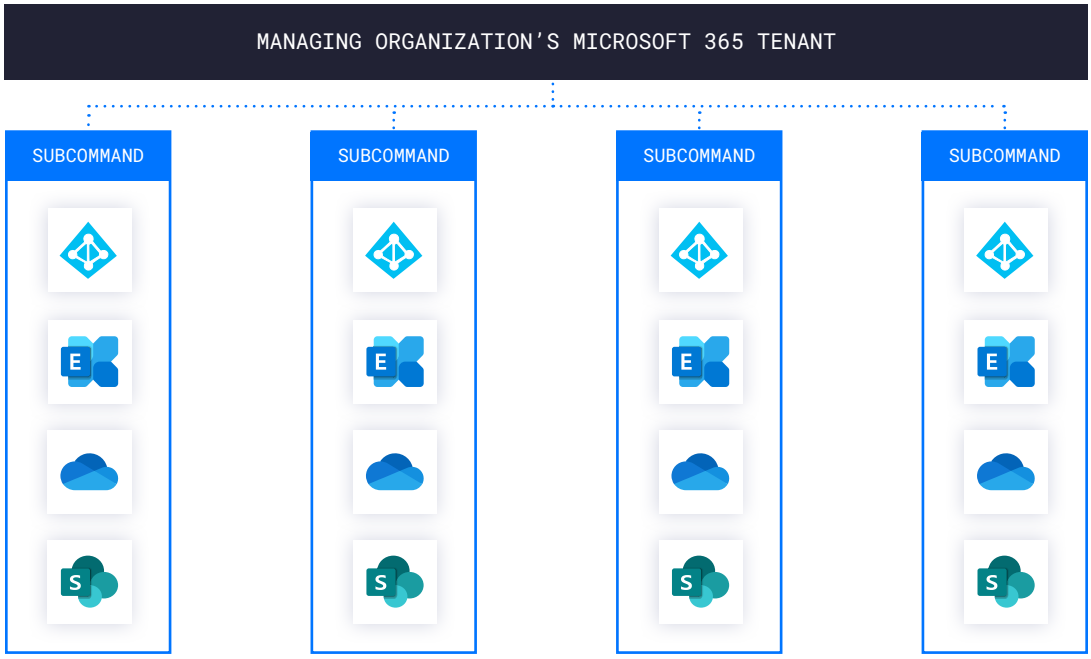
Content classification can also be challenging for individual commands, given the scale and amount of data stored on the DoD's consolidated tenants. Data stored in Microsoft 365 is growing exponentially, and each tenant already contains millions of files. Microsoft Information Protection (MIP) — Microsoft's native classification solution — limits automatic classification in each tenant to roughly 25,000 files per day. Commands that rely on these native tools cannot visualize risk, protect sensitive information, or remediate data spillages without automatic data classification.

Varonis segmentation solution for consolidated DoD tenants

Varonis provides a unique solution to empower suborganizations and individual commands whose data is stored in a consolidated tenant. Suborganizations can visualize and remediate risks to their data; classify CUI, classified, and top-secret data at scale; and prevent attacks on their data.

Varonis fills the solution gap and enables individual commands to protect and secure their data hosted in large, consolidated Microsoft tenants. This flexible solution allows for data segmentation for Teams, SharePoint Online, and OneDrive through many different mechanisms, including:

- Site owner/site creator
- Azure Active Directory group membership and attributes
- Site naming convention
- User permissions



Varonis will automatically detect and monitor the users, Teams sites, SharePoint sites, and OneDrive sites that are in-scope for the DoD suborganization. Data protection is maintained as new Teams sites are created and new users are onboarded. Varonis also grants Microsoft 365 program owners at the parent organization the ability to protect and secure data tenant-wide while giving visibility and control to individual commands.

Varonis empowers commands to independently secure Microsoft 365 data

With the ability to manage their own data, individual commands can protect Microsoft 365 data from threats. Varonis empowers commands to independently implement the controls required for EO 14028 and the DoD CIO Zero-Trust mandates.

Visualize and reduce the blast radius	**Automatically classify** sensitive data with pinpoint accuracy	**Alert** on insider threats, APTs, and supply-chain attacks

Varonis helps visualize and reduce the risk inherent in collaboration tools by continually crawling and analyzing permissions. Varonis scans group memberships, direct permissions, and sharing-links for overexposed data — leaving no stone unturned. Varonis unravels the complexity of collaboration in Microsoft 365 and provides quick answers to questions like:

- Which sensitive files are exposed to everyone in the organization?
- Which sites, Teams, and OneDrive accounts contain the most sensitive data?
- Can I detect a data breach and prevent unauthorized access to sensitive data?

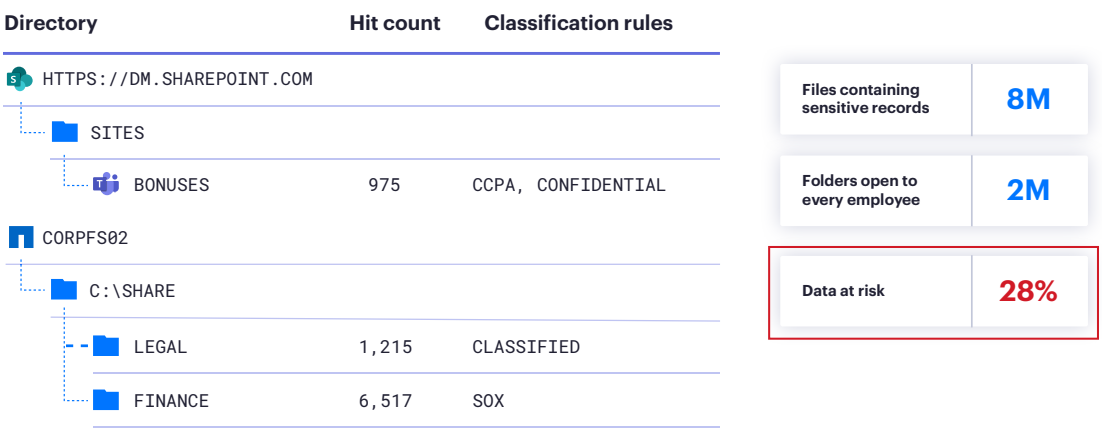
Varonis provides a unified interface for understanding collaboration risks and managing permissions — instead of siloed admin portals that provide inconsistent views. Varonis gives quick, at-a-glance insight into where sensitive data is exposed. Centralized permissions management enables organizations to enforce least privilege. Varonis puts Microsoft 365 risks and user behavior in context with on-premises data and infrastructure, enabling more comprehensive alerting and faster investigations than with Microsoft native tools alone.

Advanced content classification and risk visualization

Varonis gives organizations the ability to automatically classify and label all sensitive data through sophisticated, out-of-the-box rules that have been proven and battle-tested by numerous federal agencies and DoD missions:

- PII/PHI
- CUI
- Sensitive government forms
- Secret and top-secret information

Varonis correlates content classification information with access rights and user activity to help organizations quantify risk. Through a hierarchical view, Varonis unravels the complexity of collaboration and enables organizations to prioritize remediation efforts.



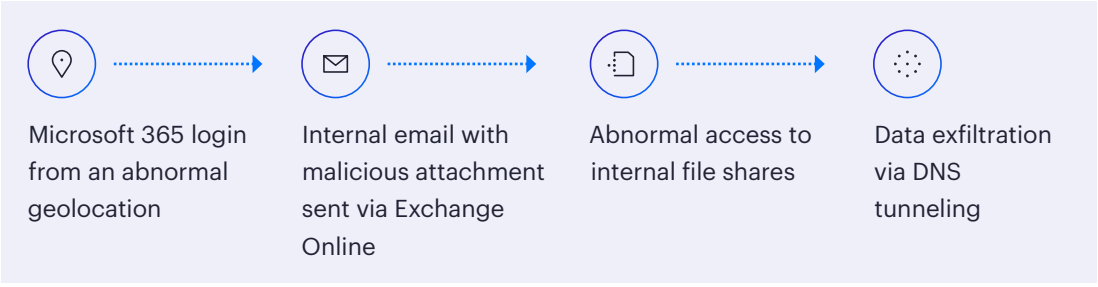
Reducing the attack surface through automation

Risk visualization enables commands to ensure that the right people have access to the right data. Varonis' modeling and simulation capabilities allow commands to quickly implement a least-privilege model without removing data from those who need access — and without impacting the mission.

User collaboration and guest links are tightly controlled to prevent unauthorized access to sensitive data and to remediate data breaches.

Visibility and context to detect threats

Varonis provides unprecedented visibility into insider threats, APTs, and supply-chain attacks. User activity from both on-premises and cloud resources is combined to build sophisticated threat models that detect user anomalies. Behavioral-based policies detect suspicious activity, while enriched log information makes investigations quick and conclusive.



Summary

Varonis is a Microsoft-certified partner for a reason — we deliver added capabilities to secure DoD hybrid environment. We provide a holistic view of what's happening with data on-premises and in the cloud to help eliminate risks and stop threat actors. Varonis brings Microsoft 365 data into context with other data sources — all through one interface — making it easier for IT and security teams to make fast and informed decisions about what happened and what to do about it.

Our segmentation solution empowers individual commands to take back control over their data and implement the administrative controls required to secure Microsoft 365.

Varonis bolsters our customers with world-class support, which includes our complimentary Incident Response team. Our security analysts will help customers, and trial users investigate incidents and take necessary steps to prevent future issues.

Varonis Risk Assessment in Microsoft 365 and Teams

A Varonis complimentary Risk Assessment quantifies and visualizes Microsoft 365 data exposure, detects abnormal access, and provides a roadmap to compliance with EO 14028 and the DoD CIO Zero-Trust mandates.

It's hard to protect what you can't see.

Varonis highlights the collaboration risk that is impossible to pinpoint using native Microsoft tools.

A Risk Assessment will help you:

- Quantify your Microsoft Teams risks and visualize your Microsoft 365 attack surface
- Uncover backdoor Teams access
- Identify folders and files shared with guest users or external accounts
- Alert on suspicious activity in Teams, SharePoint, OneDrive, Exchange Online, SharePoint Online, and Azure AD

Sample findings

479K

sensitive records found in Microsoft 365 Teams sites

73%

of records open to every user on the shared tenant

21

users storing PII in their personal OneDrive

Ready to experience the Varonis difference?

Reduce your risk without taking any. Contact our team to learn what will be covered in your **free** Data Risk Assessment.

Contact us

About Varonis

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data on premises and in the cloud: sensitive files and emails; confidential customer, patient and employee data; financial records; strategic and product plans; and other intellectual property.

The Varonis Data Security Platform detects insider threats and cyberattacks by analyzing data, account activity and user behavior; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation. With a focus on data security, Varonis serves a variety of use cases including governance, compliance, classification, and threat analytics. Varonis started operations in 2005 and has thousands of customers worldwide — comprised of industry leaders in many sectors including technology, consumer, retail, financial services, healthcare, manufacturing, energy, media, and education.