# Top Five Reasons to Replace Your Microsoft 365 Platform

Whether government restrictions or security issues have forced or encouraged you to look outside Microsoft for your information management and governance needs, OpenText has you covered.

**1.** **Connecting with multiple repositories is either expensive or impossible with Microsoft.** When an organization begins the information governance journey, an early step in the process involves identifying, storing, and categorizing the information that exists in its repositories. A comprehensive solution would connect with multiple repositories, whether on-prem or in the cloud. It should work across data repositories, services, and file formats. Machine learning algorithms can be used to identify sensitive information like PHI, PII, and PCI.

Unfortunately, Microsoft 365 focuses on data stored in Microsoft 365 workloads and contained in supported Microsoft file types. For a higher price tag, organizations can use data discovery capabilities for multiple cloud services and on-prem Microsoft data repositories. About 100 sensitive information types are used to analyze and label content in files. The types rely on keyword and regex matching. Identifying ROT data is supported when an organization migrates its data to Microsoft 365 but is out of luck for ongoing analysis. Microsoft is focused on storing everything in—surprise—Microsoft 365, bumping ROT removal down the priority list.

**2.** **Emphasis on redundant, obsolete, or trivial (ROT) data is not a priority for Microsoft.** Identifying what information should be kept and what information should be thrown out is vital for any organization, especially those in regulated industries. A complete solution would place an emphasis on the removal of ROT data. This streamlines what data is retained, reducing the risk of litigation, the vulnerability of sensitive data to an attack, and storage costs. Reporting can support collaborative decision-making. It is also best practice to create a separate backup of email, document, and file data for long-term storage and archival.

Microsoft 365's data governance capabilities focus on applying retention labels to content that must be kept for a pre-scheduled duration, but largely ignores the rest of the organization's data. (Much of this is ROT.) Users are then expected to select the correct retention label. A single source architecture in Microsoft 365 for current and archived data means that incorrect classification of pertinent email, document, and file data leads to indefensibly early deletion.

**"We were recently faced with the effects of the global COVID-19 virus outbreak. We were told on Friday that the vast majority of our staff needed to work remotely from the following Monday… with the Micro Focus (now a part of OpenText) collaboration tools… we had 95 percent of our staff remotely working within mere minutes."**

**GEORG FRITSCH**
IT Director, FCP Fritsch, Chiari & Partner ZT GmbH

**3.** **You need a user-centric analysis of your data and who can access it.** The threat of insider data breaches is high when organizations don't have a strong approach to access governance with their data. Many organizations have poorly organized files servers with decades-worth of unstructured data that isn't managed. A good information governance approach involves scoping the data access analysis across data repositories for on-prem and cloud-based. It offers a user-centric analysis of the data people are trying to access with automated remediation of inappropriate access privileges.

Microsoft scopes data access analysis across applications where identity and access are managed through Azure AD and requires Azure AD Premium P2 licensing. There are no provisions to prevent "sharing" of content with users who shouldn't have it and it's not possible to validate the reason someone has access to data. Microsoft assumes a thorough access approach to Microsoft 365 already exists and it provides the tools to keep it that way.

**4.** **Quick access to company data is essential for legal holds.** Organizations are likely to face litigation over the course of their existence, but without proper and comprehensive eDiscovery capabilities in their information governance solution(s), trouble could be lurking. If the data can be quickly attained, cases can be closed faster with much higher success rates. Content searches should use standard indexing processes for the quick and responsive presentation of search results. Only responsive content is assembled for external legal review, to substantially decrease the cost of the external review process. Legal holds for the content in question are created by guarding data in a separate repository for each case, allowing for multiple legal holds to be applied to the same content.

Content searches for eDiscovery in Microsoft 365 force a re-indexing of all selected data locations by a custodian. This adds time and slows the process of data discovery. Microsoft 365 does not offer the ability to pre-process potentially responsive content and search results must be exported before they can be viewed. Legal holds can be put on responsive content wherever it is stored in production Microsoft 365 workloads and multiple legal holds can be applied to the same workload.

**5.** **Secure endpoint backup is limited to OneDrive in Microsoft.** With remote work being commonplace, proper management of corporate- and employee-owned endpoint devices is crucial. Endpoints also serve as an organizational risk. Endpoints contain corporate data and can be costly or difficult to obtain crucial data from. Proper policy-based enterprise endpoint backup solutions safeguard all data on an endpoint in the network. Data retention on enrolled endpoints is a policy-based decision. All endpoint data is captured and preserved to support eDiscovery and enterprise search requirements. Organizations can define how long files should be kept available in an archive.

Content searches for eDiscovery in Microsoft 365 force a re-indexing of all selected data locations by a custodian. This adds time and slows the process of data discovery. Microsoft 365 does not offer the ability to pre-process potentially responsive content and search results must be exported before they can be viewed. Legal holds can be put on responsive content wherever it is stored in production Microsoft 365 workloads and multiple legal holds can be applied to the same workload.

Content in OneDrive and SharePoint can be synchronized to an endpoint for simple access and collaboration. Users can avoid data retention requirements easily by storing documents outside the OneDrive folder hierarchy. Data stored on endpoints outside OneDrive is excluded from eDiscovery, creating dark data. Additionally, Microsoft scans data stored in OneDrive and will delete files sporadically it deems potentially dangerous if it isn't set to retention policies. OneDrive automatically captures deleted files in a couple of recycle bins, but when a file is removed from the second storage bin, it is gone forever. The ability to verify if an endpoint has been patched or updated is a key component of an endpoint management solution and is lacking in Microsoft.

Microsoft OneDrive is a great platform for collaboration and teamwork but lacks many of the security features enterprise organizations need for proper data management and retention. OneDrive isn't quite a complete backup platform, content management platform, or secure file sharing platform.

Start exploring how OpenText Information Management and Governance solutions can support your organizational initiatives today and deliver where Microsoft can't.

"We like the roadmap of the products and the new functionality on the horizon plays to an increasingly mobile workforce, which is something we all have to manage."

**ANTONIO PARRINELLO**
CEO
Nakoma

Learn more about these OpenText alternatives to Microsoft:

- Enterprise Messaging
  - Alternative for Outlook, Exchange, or Teams.
- Unified Endpoint Management
  - Alternatives for Autopilot, Endpoint Configuration Manager, Untune, or Defender for Endpoint.
- Secure Content Management
  - Alternatives for OneDrive, Stream, Sway, Lists, Forms, or Visio.
- Data Protection
  - Alternatives for Defender, Azure Information Protection, or Advanced Threat Analytics.
- Collaboration
  - Alternatives for Teams, SharePoint, Yammer, or Viva Connections.
- GroupWise
  - Alternative for Outlook, Exchange, or Bookings.
- Enterprise File Sync and Share
  - Alternatives for OneDrive or Teams.

Learn more at
**www.microfocus.com/en-us/microsoft-365-alternative**
**www.microfocus.com/opentext**

269-000028-001 | O | 04/23 | © 2023 Open Text

opentext™