Top Five Reasons to Switch from Your Current Cloud Collaboration Platform

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

1

Connecting with multiple repositories is either expensive or impossible with other platforms. 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, other platforms on the market focus on data stored in their own workloads and contained in specific supported file types. For a higher price tag, organizations can use data discovery capabilities for multiple cloud services and on-prem 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 the platform but is out of luck for ongoing analysis. Other platforms are focused on storing everything in—surprise—their own platforms, bumping ROT removal down the priority list.

2

Emphasis on redundant, obsolete, or trivia (ROT) data is not a priority for other platforms. 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.

Other platforms' 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 other platforms 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 Fritschit
Director
FCP Fritsch, Chiari & PartnerZT 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.

Other platforms approach data access analysis across applications where identity and access are managed through their own platform and requires 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. Other platforms assume a thorough access approach to the platform 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 other platforms force a re-indexing of all selected data locations by a custodian. This adds time and slows the process of data discovery. Other platforms do 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 workloads and multiple legal holds can be applied to the same workload.

5 **Secure endpoint backup is limited to platform-specific cloud storage.** 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.

Start exploring how OpenText information management and governance solutions can support your organizational initiatives today and deliver where other platforms can't.

Learn more about these OpenText cloud collaboration alternatives:

- OpenText Enterprise Messaging
- OpenText GroupWise
- Secure file sync and share
- Unified endpoint management
- Data backup and resiliency
- Email, social, and team collaboration

Content in other platforms can be synchronized to an endpoint for simple access and collaboration. Users can avoid data retention requirements easily by storing documents outside the alternative platform's folder hierarchy. Data stored on endpoints outside the platform is excluded from eDiscovery, creating dark data. Additionally, other platforms scan data stored in their cloud storage and will delete files sporadically they deem potentially dangerous if they aren't set to retention policies. Other platforms automatically capture 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 other platforms.

Alternative platforms can provide organizations with enhanced collaboration and teamwork but lacks many of the security features enterprise organizations need for proper data management and retention.

Learn more at opentext.com ›

"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

opentext™