



PROOFPOINT FOR OFFICE 365: ENABLES ADVANCED SECURITY AND COMPLIANCE FOR YOUR ENTERPRISE

UNDERSTAND THE SOLUTION BY ROLE: LEGAL

What eDiscovery challenges exist with Microsoft® Office 365™?

Native Microsoft® Office 365™ eDiscovery Capabilities

Microsoft® Office 365™ provides a number of native capabilities that help organizations with lightweight eDiscovery requirements. However, these capabilities depend on the package the organization has purchased. The SMB packages, for example, don't include eDiscovery capabilities. Only the higher-level enterprise SKUs, namely E3 and E4, come with eDiscovery features, but these features cost 2-4x more than comparable third-party packages. If your organization is infrequently involved in litigation, the capabilities built into Office 365 may meet your needs. These capabilities include:

- Message retention management (MRM)
- User-based retention through retention tags
- In-place legal hold
- eDiscovery search
- SharePoint eDiscovery Center

Microsoft® Office 365™ eDiscovery Challenges Overview

Although Microsoft® Office 365's™ eDiscovery capabilities may suffice for organizations that aren't frequently involved in litigation, those that have advanced requirements may require support from a third-party vendor. For example, some eDiscovery challenges with Office 365 include:

- **Retention management:** Office 365's retention capabilities, completed through Message Retention Management (MRM), don't actually ensure data retention. Per Microsoft's recommendation, the only means of ensuring that data stored in Office 365 is retained is to place the entire organization under legal hold.
- **Legal hold:** Legal hold with Office 365 can only be placed on content that exists within the Office 365 environment. In addition, BCCs and distribution lists cannot be placed under a legal hold.
- **eDiscovery search:** Search results within Office 365 aren't instantaneous. Processed in batch, there can be a substantial amount of wait time depending on the size, volume and scope of the search.
- **Content sources:** Office 365 only supports content types that exist within its environment, inclusive of email, SharePoint and Lync for example. However, it's not able to extend to social

media (e.g. Salesforce Chatter, Microsoft Yammer, Twitter, Facebook, etc.), nor files at rest on desktop endpoints.

Native Microsoft® Office 365™ Retention Capabilities

Microsoft® Office 365™ provides Message Retention Management (MRM) functionality designed to address the challenges of email volume and lifecycle management. As such, it's best used for disposition and not retention. Its primary purpose breaks into two key areas, including:

- Meeting business requirements by enabling end users to determine the importance of an email through retention tags
- Improved storage management through email disposition

MRM can also be used to apply retention policies for all messages belonging to specific users or an active directory group, but this doesn't ensure that messages are retained for eDiscovery and compliance purposes.

Microsoft® Office 365™ Retention Challenges Overview

Microsoft® Office 365™ provides end-user retention capabilities, effectively enabling users to make real-time retention decisions through folder-based tagging. For organizations in unregulated verticals that aren't concerned about ensuring retention of email, enforcing retention in this manner could work. Note that this will not mitigate the damage that could be done as a result of not retaining electronically stored information (ESI) that may be responsive to eDiscovery requests and ongoing litigation.

On the other hand, for organizations in regulated industries—or those with complex litigation requirements—ensuring data immutability is a firm business requirement. A workaround provided by Microsoft suggests that Office 365 users place the entire organization on a legal hold, as this is the only means of ensuring data retention. This isn't a best practice for a number of reasons, including:

- Microsoft contractually stipulates that only 15% of the organization can be placed under a legal hold concurrently.
- Data and legal hold management becomes burdensome and difficult to manage. More specifically, disposition is problematic and pushes the organization into the age-old 'never delete anything' information governance scenario. Simply put, you're keeping data that isn't valuable for the business while the risk increases year-over-year as you lose oversight.

How does Office 365 meet my data retention requirements?

Native Office 365 Retention Capabilities

Office 365 provides Message Retention Management (MRM) functionality designed to address the challenges of email volume and lifecycle management. As such, it's best used for disposition and not retention. Its primary purpose breaks into two key areas, including:

- Meeting business requirements by enabling end users to determine the importance of an email through retention tags
- Improved storage management through email disposition

MRM can also be used to apply retention policies for all messages belonging to specific users or an active directory group, but this doesn't ensure that messages are retained for eDiscovery and compliance purposes.

Office 365 Retention Challenges Overview

Office 365 provides end-user retention capabilities, effectively enabling users to make real-time retention decisions through folder-based tagging. For organizations in unregulated industries, enforcing retention in this manner could work assuming they aren't concerned about ensuring retention of email. Note that this will not mitigate the damage that could be done as a result of not retaining electronically stored information (ESI) that may be responsive to eDiscovery requests and ongoing litigation.

On the other hand, for organizations in regulated industries—or those with complex litigation requirements—ensuring data immutability is a firm business requirement. A workaround provided by Microsoft suggests that Office 365 users place the entire organization on a legal hold, as this is the only means of ensuring data retention. This isn't a best practice for a number of reasons, including:

- Microsoft contractually stipulates that only 15% of the organization can be placed under a legal hold concurrently.
- Data and legal hold management becomes burdensome and difficult to manage. More specifically, disposition is problematic and pushes the organization into the age-old 'never delete anything' information governance scenario. Simply put, you're keeping data that isn't valuable for the business while the risk increases year-over-year as you lose oversight.

How does Microsoft® Office 365™ meet legal hold requirements?

Native Microsoft® Office™ 365 Legal Hold Capabilities

In order to take advantage of legal hold capabilities, the customer must have either the E3 or E4 enterprise package. In the case of active litigation, an organization using Microsoft® Office 365™ can place litigation holds across content types stored within the multi-tenant Office 365 environment. This serves the purpose of ensuring preservation of electronically stored information, assuming it hasn't previously been deleted as a result of end-user deletion or content having hit a user-specified retention policy through MRM.

There are two primary legal hold types within Office 365 including people- and query-based. People-based legal hold can be applied to an individual as either a static or rolling legal hold, whereas query-based legal hold can be applied to a set of search terms. The holds can be placed either indefinitely, or for a specific number of days.

Microsoft® Office™ 365 Legal Hold Challenges

Numerous challenges exist with Microsoft® Office 365's™ native legal hold capabilities, including those of which are provided by its SharePoint eDiscovery Center. These challenges can be broken into the following key areas:

- **Complete capture:** Legal hold won't capture distribution list membership, nor recipients who were blind carbon copied. This is an issue because it signifies that a legal hold created within Office 365 does not represent all potentially relevant electronically stored information (ESI) for a specific matter.
- **Search scope:** The scope of legal hold search within the Office 365 email administrative console is limited to only 50 mailboxes at a time. If there are more than 50 custodians, the user will need to create multiple legal holds to support their matter.
- **Lack of immutable storage:** Office 365 storage isn't truly immutable. The only means of ensuring data retention is by placing the entire organization under legal hold. Not only is this not best practice and difficult to scale and manage, but contractually Microsoft stipulates that only a percentage of the organization can be placed under legal hold without additional cost.

Will Microsoft® Office 365™ safeguard critical data?

Microsoft® Office 365™ & Data Safeguarding

Although this doesn't directly address all data safeguarding measures including data residency and encryption methodology, Microsoft® Office 365™ is compliant with an impressive number of compliance standards. A sample of this list includes:

- Health Insurance Portability & Accountability Act (HIPAA)
- Federal Information Security Information Act (FISMA)
- ISO 27001
- EU Data Protection Directive
- U.S.-EU Safe Harbor
- Family Educational Rights and Privacy Act (FERPA)
- SSAE SOC Type I
- Gramm-Leach-Bliley Act (GLBA)

Microsoft® Office 365™ Data Safeguarding Challenges

Where Microsoft® Office 365™ will cause most organizations to pause is in how it handles data residency. Microsoft stores customer data spanning multiple datacenters, and contractually stipulates that they can move customer data without providing notification. This is of the utmost concern for organizations that have strict data residency requirements. Microsoft can even move data from one country to another, and Microsoft personnel or subcontractors may have direct access to customer data. These are process and architecture decisions that could prevent Office 365 from being a viable platform for complex multi-national enterprises.

Will Microsoft® Office 365's™ eDiscovery Center meet advanced litigation readiness needs?

Microsoft® Office 365™ eDiscovery Center Overview

Originally a feature that was built as a part of SharePoint™ Server 2010, the eDiscovery Center was extended to Office 365. Also embedded in Microsoft® Office 365's™ hosted SharePoint instance, the eDiscovery Center is a SharePoint site designed to manage preservation, search and export of content stored within Office 365.

Microsoft® Office 365™ eDiscovery Center Challenges

Because the eDiscovery Center embedded in Office 365 wasn't purpose-built, there are a great deal of challenges and inherent complexity that limit the system's ability to deliver substantial value to the user. First and foremost, the eDiscovery Center is itself a SharePoint site, and doesn't archive content. It simply acts as an overlay to search across content stored within Office 365. The same search limitations—such as support for only Microsoft file types—exist within the eDiscovery Center.

In addition, searches conducted within the eDiscovery Center carry their own limitations. For example, a search query can only be launched against 1,500 Exchange mailboxes or 100 SharePoint sites in a single search, for example. Plus, with support only for content stored within the Office 365 service itself, it's likely that an incomplete dataset will be provided to either internal or outside counsel.

Will Microsoft® Office 365™ meet eDiscovery search needs?

Native Microsoft® Office 365™ eDiscovery Search Capabilities

Microsoft® Office 365's™ E3 and E4 packages provide eDiscovery capabilities spanning the Exchange Administrative Console, as well as its SharePoint eDiscovery Center. The Exchange Administrative Console provides either an IT or eDiscovery user with the ability to search across either the entire organization, or select mailboxes. From there, the user is provided with the option to search across either a mailbox or filter based on select criteria, such as keywords, sender/recipient and date ranges.

The search functionality tends to meet the needs of smaller organizations, or those not frequently involved in litigation.

Microsoft® Office 365™ eDiscovery Search Challenges

Where the built-in search functionality falls short is in its inability to show the results of a complete result set. Given that journaling isn't used for message capture, which is an industry best practice, and retention is often dictated by end users. Consequently, the result set tends to paint an incomplete picture.

Other key concerns include:

- The in-place eDiscovery search capabilities don't provide instantaneous search results. This makes it challenging to quickly cull large datasets and determine relevancy. Additionally, users may discover that the search results weren't relevant and would be forced to re-run the search and then wait for it to process before beginning the review process.
- Office 365 doesn't index all file types, so it won't return search results inclusive of all criteria across non-Microsoft file types.
- The review process can often be arduous due to the lack of eDiscovery workflow. Search results are copied to an eDiscovery mailbox, which effectively looks and behaves like an online PST. This makes the review process time consuming and inexact.

Responding to eDiscovery events is more often than not a time-sensitive activity, making rapid response of paramount importance for legal teams. Bearing that in mind, Office 365 may not meet the needs of organizations that consider themselves part of a litigious environment.