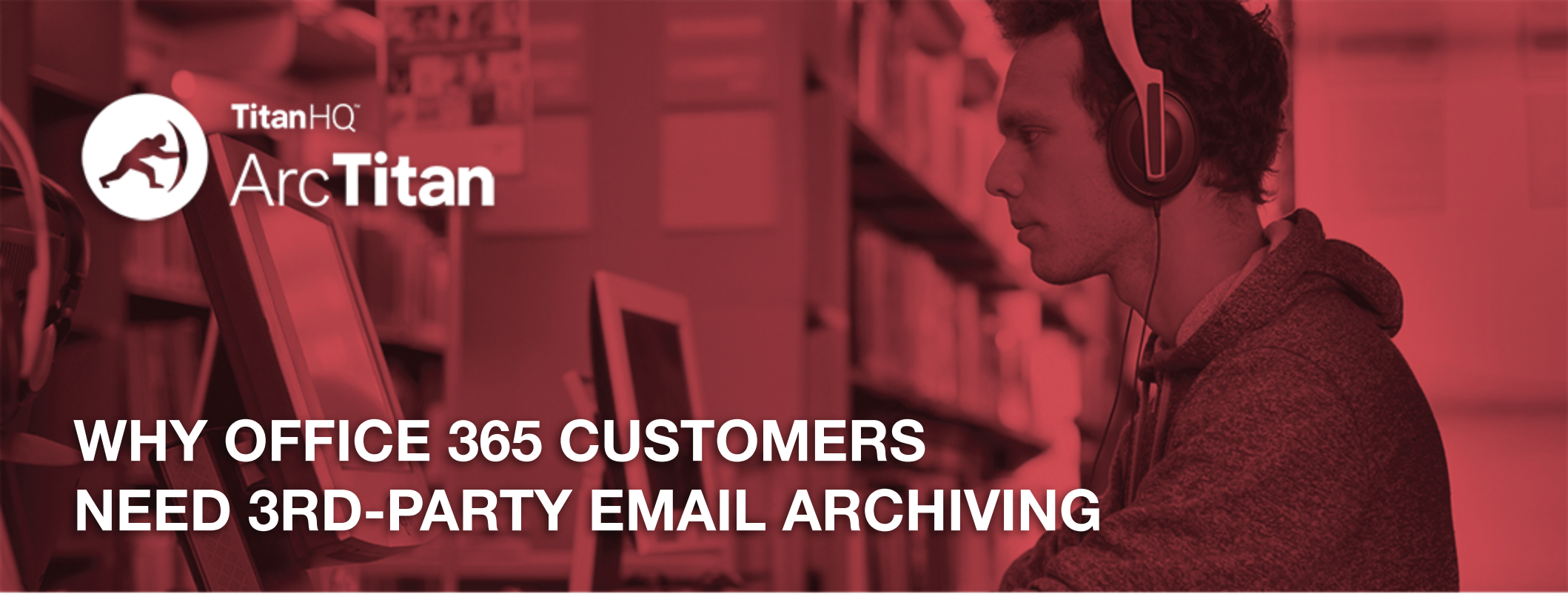


TitanHQ ArcTitan

WHY OFFICE 365 CUSTOMERS NEED 3RD-PARTY EMAIL ARCHIVING

1.0 Purpose of Document

Office 365 is changing the way businesses use IT. Microsoft have invested heavily in constructing their business case for organisations of all sizes to move into the cloud, and much of the IT community has listened.

The purpose of this white paper is to outline the archiving services that users can expect to find in Office 365 Email and consider the questions that businesses may be advised to ask to ensure their systems meet their needs. Finally, this document will also demonstrate some areas where Office 365 email archiving requires supplementation in order to be fully compliant.

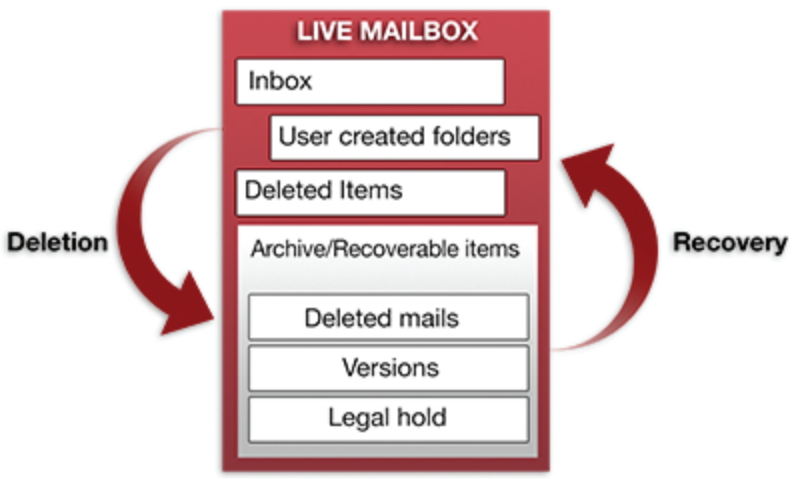
2.0 Email archiving in Office 365

Office 365 provides features and functionality that many users of on-premise Exchange email systems will be familiar with, such as the reminder to ‘archive your old items’ that Outlook suggests, especially when mailbox storage limits are approached. Like on-premise Exchange, Office 365 permits old copies of email to be moved from a user’s live mailbox to an archive.

Office 365 email archiving services offer to do this in three ways: the recoverable folders structure, the ability to export to .pst files and the use of legal hold (read on for explanation).

2.1 Deleted folder structure

Deleting mail from Office 365 either with or without Legal Hold enabled (see section 3.1) begins a process of passing the deleted email through the below folder structure. Once an email has been purged from deleted items the user can no longer retrieve them without the assistance of the IT department.



3.0 Compliance and email archiving in Office 365

The way in which organisations view compliance is changing. We have increasingly seen businesses focus on internal processes in equal measure to external audit. Business emails contain many critical documents, including contracts, intellectual property, purchase orders, invoices and other legally binding documents. Not only do your emails contain these kinds of attachments, but the body of the email is often extremely important in itself.

The IDC estimates that 60% of a business’ critical information is stored within its emails. From time to time businesses need to recover evidence of contractual and legally binding agreements, and Office 365 Email recognises this, offering a set of legal hold features and the compliance centre to manage them. The important difference between this type of archiving practice and the standard user archive is that, in the case of evidence requirements, the authenticity of the email needs to be demonstrated.

It is important to clearly be able to demonstrate that the emails returned from the archive are identical to the original emails.

3.1 Legal Hold

In order to guarantee the authenticity of an email, it must be identical to the original mail and be unedited. 'Legal Hold' was developed by Microsoft email in order to do this within Office 365 email services. Legal Hold can be activated by the admin, from the admin portal.

Legal hold ensures authenticity of the email from the date/time that legal hold is switched ON (emails that have been changed or edited since they were received can't revert to their original version). Once in legal hold, emails can still be edited or deleted as viewed from their mailboxes, but a copy of any changes is passed to the "recoverable items folder". Within that folder a copy of deleted emails and edited emails is maintained for as long as legal hold is switched on. This folder acts as the archive by creating a chain of all edited and deleted emails, which can be accessed via the Compliance Centre for the duration of the Legal Hold.

Once legal hold is removed then any deleted mail which is older than the retention period is purged. Any history of changes that has been tracked is removed. The only remaining copy of that email will be the most recent iteration (I.e. the last edited version) as well as anything which is in the primary user mailbox. In short, where anything is older than the retention period, its entry in the recoverable items folders will be deleted.

This means that the only way to ensure that the original copy of an email is never deleted is to have indefinite legal hold from the day you go live with Exchange or Office 365. It is important to note also that only active mail boxes can be placed on Legal hold (see section 5.4).

Microsoft offer two types of legal hold:

3.2 Litigation hold

When Litigation Hold is enabled, all mailbox items are placed on hold. Once Litigation Hold is disabled, you can no longer prove that an accurate copy of an email has been retained. If Litigation Hold is disabled, then any previously deleted emails which were being stored will be purged. In order to keep all emails, Litigation Hold must be enabled permanently for the entire company.

3.3 In-Place hold

In-Place Hold preserves only those items that meet the criteria of a search query, defined by using the In-Place eDiscovery tool, it can be set by the admin. If In-Place Hold is turned on and the user deletes an email not covered by the query defining the hold, that email will be purged from recoverable items after 14 days.

It is therefore important to note In-Place hold cannot be used to prove an email wasn't sent, since the absence of an email in an archive based on In-Place hold could simply mean it did not meet the criteria of the search.

3.4 Hold duration

When you set up hold duration in either Litigation Hold or In-Place Hold, it is possible to base the period on either a date range, or an infinite time period.The duration which the mailbox is held for begins on the day the item is created or received. For example: if you're using a retention period of 5 years, using time-based hold, then all items will be kept for 5 years from the point which they arrived or were created on your mail server. If you delete something from the Office 365 primary mailbox after 1 year, that item will be held for a further 4 years in the archive before being purged in order to meet the full 5 year time-based hold period.

If your Legal Hold period and retention period are different then preserving a mailbox is more likely to have risks associated with it. Tech net (June, 2016) states:
"If you set every mailbox to legal hold for 7 years then you cannot delete the mailbox. If you delete a user account that has a mailbox, the Exchange Information store will eventually detect that the mailbox is no longer connected to a user account and mark that mailbox for deletion, even if the mailbox is on hold."

If you want to preserve the mailbox it is important that you follow proper procedure; disabling the user, changing selected properties and retaining the mailbox until all data has been removed, or until preserving the data is no longer required.

3.5 Compliance Centre

The Compliance Centre is an admin area available within Office 365 Email which is designed to provide a control panel. In order for the Compliance Centre to be made available to multiple users the admin must undergo a series of steps (which can be found here).

Compliance Centre provides functionality to manage compliance and allows users to do the following:

- Enable or disable users' mailbox archiving after a specified period
- Undertake eDiscovery cases to identify, hold, search, and export content from Office 365 mailboxes. Results can be sorted /previewed in the details pane on the Compliance search page. Previews are opened in a new Outlook Web App window.

  *Note: If you preview the search results for a search that was last run more than 2 days ago, a new search will be run to refresh the search results.
- Preview search results (up to 200 recent results)
- Export email to a .pst file (A Personal Folders file (.pst) is an Outlook data file that stores your messages and other items on your computer, the mail in a .pst doesn't count towards mailbox quota and is therefore often used for storage savings)
- De-duplicate search results to copy only one instance of each unique message to the discovery mailbox.

There is no mechanism to tag and comment on email or share with other authorised users such as auditors. After a search you may preview the results, up to 200 at a time. Beyond that number you must export to a .pst file in order to view the results of your search. Please note – At the time of writing, Microsoft have retracted version 2 of the Compliance Centre in favour of reverting to version 1.

4.0 What is Journaling?

Journaling email refers to the process of taking copies of all email (either all emails for selective users or globally for all users) that pass through your Office 365 server, in real-time. A journal message contains the content of the actual email message and all related metadata (e.g. date, time, recipients). Journaling is a key stage in the email archiving process which 3rd party email archive solutions like ArcTitan use to capture email.

The ArcTitan Definition:
The process of collecting all emails, complete with all attachments and associated metadata, which have been sent from or received by your mail server, on a continuous basis, from a temporary store on the mail server. ArcTitan, as an external archiving solution, makes use of the journaling process. In the case of ArcTitan we can either receive a journal feed via SMTP directly to our dedicated SMTP service, or Office 365 can journal directly to a mailbox from ArcTitan to collect via POP/IMAP/EWS. Please note - Office 365 cannot journal to a mailbox which is on Office 365, it can only journal to a third party mailbox, or on-premise Exchange mailbox.

5.0 Limitations of Office 365 Email Services

5.1 Journaling

Office 365 can only Journal to an External Address, for the purposes of enabling use of 3rd party journal archive technology.
Using Office 365 email services without 3rd party Journal archive, you cannot:

- Find more than 200 results in any one eDiscovery search using the Compliance Centre
- Search more than 10,000 mailboxes in any one search
- Have tamper evident email (without Litigation hold set permanently on for ALL mailboxes that have ever existed in your organisation)
- Run more than 2 eDiscovery searches at the same time within the same company
- Access any of your email on Litigation Hold and/or Live email if service goes down
- Prove that your email are original copies if you turn off Litigation/In-Place hold
- Prove that an email has NOT been sent or received
  (without Litigation hold set permanently on for ALL mailboxes that have ever existed in your organisation)
- Retain or archive email for leavers without maintaining their mailbox

5.2 Exporting mail to .pst file

Some organisations choose to copy email into a .pst file. However, Microsoft state that .pst files "… are not meant to be a long-term, continuous-use method of storing messages". Due to the fact that .pst files can be edited, any use of them as evidence is easily questioned. Not only that but as the .pst file grows it is likely to become corrupt.

5.3 Searching

Office 365 offers benefits in terms of large storage limits and cloud-based email, however searching facilities are limited to the familiar Outlook search bar.

5.3.1 Types of Search

When searching for email in Office 365, access (including searches) to Office 365 email occurs via a remote cloud service and the Office 365 email service encourages large storage allowances. These two factors can, and do, combine to cause slower searching than in an on-premise Exchange.

The complexity of the search running on Office 365 is a large factor affecting search times. The number of mailboxes searched has a larger effect, however Microsoft doesn't provide a Service Level Agreement for search times. The following table lists average search times for a content search based on the number of mailboxes included in the search. The reference can be found here:

5.3.2 Search Speed

There is little point in keeping emails in an archive if you can't find them again quickly and easily when you need them. Searching in Office 365 lacks functionality that can be found in third party archives that specialise in fast search and retrieval. Whilst the standard Outlook interface does support Boolean searching, it is not intuitive, which creates issues for users finding mail, especially those in non-technical roles.

In addition to the actual search query it is important to note that searches across multiple folders will become much slower, and less reliable within Office 365, than searches within a specific folder. If a user wishes to search for information within an attachment, or to use an attachment in order to locate an email, this complicates the search further.

Once the search is returned, locating the term you searched for within that email becomes a manual process. All these considerations pose even more issues when you begin to combine search criteria, or require your users to conduct searches themselves.

NUMBER OF MAILBOXES	AVERAGE SEARCH TIME
100	30 seconds
1,000	45 seconds
10,000	4 minutes
25,000	10 minutes
50,000	20 minutes
100,000	25 minutes

5.4 Licencing considerations

Office 365 email licenses on a per user subscription basis, which poses issues when employees leave an organisation. In order to maintain an employee's email, either in or out of Legal Hold, once they leave your organisation the mailbox must remain live. Therefore that user's license must be retained once they have left, plus any replacement would also require a mailbox license at full price, meaning you pay for two licenses for just one job role.

For this reason, an organisation with 50 employees, where the employees stay for an average of two years, would be paying for 200 licenses after four years. An archive which licensed per live user would only charge for 50 licenses total during that time.

Not only will permanent users create more license fees in Office 365 than with archiving solutions like ArcTitan, but temporary users will require new licenses too. For example, if your business is adding temporary access to an employee's archive for maternity leave, then any users with access to that archive would require a new license purchase.

5.5 Migration issues

Migrating to Office 365 can be challenging. In particular, getting legacy email into the cloud so that users can see their current and historical email, and allowing the on-premise Exchange server to be decommissioned. Migrating legacy email creates a period of limbo, where users are uncertain of where to go to retrieve their email from at that point. This migration of legacy email will require time in management, plus additional tools or services.

Email data typically includes the users' current mailbox contents and can include .pst files, too. Therefore the IT department will have to construct a plan that caters for all forms of legacy email. Some organisations will need to research where and how .pst files are in use across their business, and retrospectively address issues with best practice and the prevention of corrupt data in .pst files.

During the migration there is a risk of data loss. The limbo transition period for users whilst mailboxes are spread across two (or more) environments can cause problems. All of this management means time taken to move the data in and out. This issue is only exacerbated by throttling on the import to reduce network impact on the Office 365 environment that can't be remedied by the organisation without the help of Microsoft.

5.6 Future Proofing

When moving into the cloud it is important to insure against future risks. Organisations must explore exit clauses for any cloud service if they want to remain safe when the time comes to end their contract. Such exit clauses need to consider both the cost of recovering data, any penalties applied and also the ease of extracting data. Data that is free to recover might still cause issues if download speeds are limited or restricted.

Switching provider brings a lot of work for the IT department; it can be time-consuming as well as complicated and (typically) expensive too. Those reasons alone can be enough to put you off switching provider, even if it's the right thing for your business in the long term. Therefore it is important to protect against them.

6.0 And finally…

By adding a third party archive like ArcTitan your entire company is able to search through your archive at any time, quickly and without limits like the short list of preview pane results. Not only that but you will be able to restore email to a mailbox rather than creating large problematic .pst files.

Augmenting the Compliance Centre with a more powerful search and retrieval tool allows for increased efficiency and unlocks the real potential of a cloud archive. The issues discussed in this report are easily countered with the installation of ArcTitan.

Our customers have had great success pairing ArcTitan with Office 365 so that they can get the most out of both email archiving and a cloud-based Exchange. In particular, being able to supplement Office 365 by implementing the ArcTitan solution alongside Office 365 (a process which requires only one step).

If you'd like to learn more about ArcTitan email archiving, contact us at info@TitanHQ.com or by telephone USA +1 813 304 2544
OR IRL +353 91 54 55 00