ARCHIVE360

Journal Archiving with Office 365:

Do I need it and does it work?

Table of Contents

Chapter 1:
Overview

You're looking to move your on-premise email infrastructure to an Office 365/Cloud Exchange for better cost efficiency, higher security and increased scalability. Before you begin such a migration, you should identify if your organization requires to journal and archive emails, for compliance, legal or another business requirement.

If your company does, then read on.

Before we get into the meat of this topic, it is important to identify what we mean by certain phrases.

What do we mean by "Journaling"?

The term 'Journaling' is defined as the ability to record all communications for use in the company retention or archiving policy. This is generally implemented as part of a legal or compliancy regulation on behalf of the organization. In short, the email is copied from the mailbox into a dedicated sandbox for storing. It creates an exact copy (including Metadata) of the email original. Microsoft invented the "Journal Mailbox" during the mid-90s for on-premise Exchange solution, specifically aimed at the newly implemented SEC requirements for brokers and traders in the finance sector. This strategy ensured that all communications have a full audit trail and can be retrieved without having been tampered with or edited in any way.

What is the difference with "Archiving"?

The term 'Archiving' refers to the physical moving of files (email) from their native location, i.e., an Exchange server/Office 365, and storing them elsewhere for ongoing management, retrieval and backup storage. There is a physical storage of any content (edited or otherwise) that is placed in a location other than that of the live mailbox. Archiving is generally perceived to be a strategy of backup and restore in a Disaster Recovery Framework, whereas Journaling is more of an ongoing audit of communications.

Journaling is used as a company-wide email management strategy to demonstrate compliance and facilitate eDiscovery.

Regulatory requirements launch journaling

To date, at least two government regulatory bodies specify a journaling strategy for electronic communications. As we have discussed previously, Journaling ensures that an email conversation and string of metadata is captured immediately, registered for auditable purposes and allows the organization to use this communications and immutable properties in a legally defensible position. Many companies believe that journaling of a mailbox was, in fact, simply to archive the mailbox via backup procedures. This is false; a mailbox backup would overwrite any data that had been edited, removed or placed in the 'trash' folder during any previous archives or backups taken, ultimately leaving the data useless or overwritten.

A perfect example of this precise issue occurred circa 2009 when the White House IT department set up journaling on a mailbox for the Vice President's office email server to meet U.S. National Archives and Records Administration (NARA) archiving regulations. This regulation ensures that all governmental agencies archive all email communication and conversations via their email infrastructure. The IT department set up a journaled mailbox to capture the office's incoming and outgoing communications. One area they forgot to focus on however, was that they chose to rely on a manual process of transferring journaled data to file servers, instead of utilizing any automated email archiving system that would have archived and transferred the auditable content to a separate archive server. Later, the Vice President's office was served with a Freedom of Information Request (FOIA request).

During the investigation, it was revealed that large amounts of email data were missing. During a Congressional hearing, it was identified that the IT department had not only failed to implement a stable journaling strategy, but also failed to monitor the manual transfer of mailboxes which resulted in large amounts of data being overwritten (de facto deleted).

Standards and Best Practices

Prescriptive communication journaling requirements are included in the SEC Rule 17a-4 and in MiFID II (Markets in Financial Instruments Directive 2004).

There are several other regulations, where journaling can assist in compliance:

- Sarbanes-Oxley Act of 2002 (SOX)
- Security Exchange Commission Rule 17a-4 (SEC Rule 17 A-4)
- National Association of Securities Dealers 3010 & 3110 (NASD 3010 & 3110)
- Gramm-Leach-Bliley Act (Financial Modernization Act)
- Financial Institution Privacy Protection Act of 2003
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act)
- European Union Data Protection Directive (EUDPD – EU 2016/A29)
- Japan's Personal Information Protection Act (PPC 2016)

Litigation hold and journaling

Other reasons companies utilize email journaling is for litigation purposes; when a lawsuit is filed (or anticipated), the companies affected are required to locate and place a litigation hold on all **potentially relevant data** in the expectation of a later eDiscovery order. In many cases, the opposing counsel will ask for required data between two specific dates – such as all email from or to target employees between specific dates. In some circumstances however, the date range could be open-ended requiring a litigation hold on all past, current, and future email dialogue.

The easiest way to ensure all affected email is captured and placed on a litigation hold is to begin immediately journaling the target employee's mailbox. In fact, many companies will automatically journal their C-Level employee's email and hold it for 2 or more years simply because their GC expects that those employees have a higher risk of being named in lawsuits.

Chapter 2:

Journaling workarounds

Since Office 365 archiving doesn't support journal capture, customers have devised many workarounds:

1. **Utilizing shared mailboxes for journal data.** – This is a valid option for smaller organizations, however communications that go "off piste" via individual email addresses will not get picked up in the archiving sweep, meaning that the conversation is incomplete, thus non-compliant.
2. **"Exploding" legacy journals so they can migrate the journaled individual emails into the associated custodian mailboxes.** – Again, a valid solution, but takes up far too much physical storage and is not efficient in an investigation.
3. **Keeping your on-premise Exchange server active.** – Increases your costs.
4. **Using a proprietary third-party journal archive vendor.** – A great option which we will discuss in more detail following.

Journaling and Office 365.

If your company does journal email, the question you should ask is can Office 365 archiving work with journaling? The simple answer is no. Instead, Microsoft suggests an on-premise or third-party cloud archive to be used as the journal mailbox. There are a couple of issues with this suggestion.

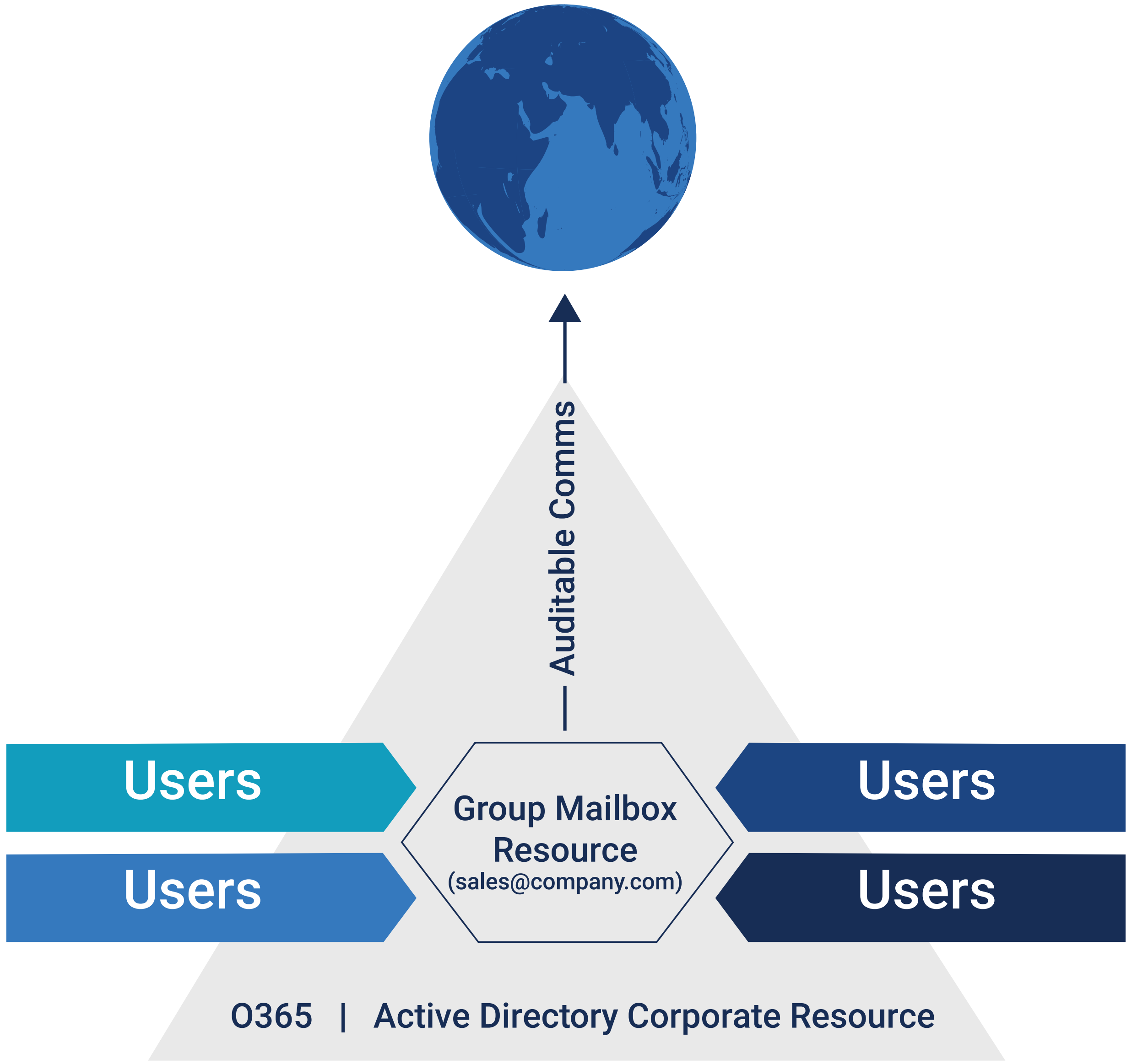
Keeping an on-premise email archive active to act as a journaled mailbox is expensive and ultimately defeats the purpose of moving your live email on-prem to Office 365 – it will cost more than staying with your current on premise Exchange system.

Relying on a third-party cloud archive can be costly and ultimately leads to vendor lock-in issues. Vendor lock-in occurs when a third-party archive vendor controls data access and converts your journal data into a “more convenient” format to make way for an even harder exit strategy, should you wish to change later on. The issues are compounded financially, when the proprietary archive vendor will charge you an exorbitant amount to “re-convert” your data back into its original format – sometimes as much as $10 + per GB. This situation is referred to as “data ransom” and depending on the amount of data in the archive, can cost millions of dollars / euros.

Another tactic used by proprietary archives is to throttle data extraction speeds, should you try to move too much data away from their proprietary infrastructure. Throttling creates roadblocks to force you into changing your mind on leaving their services. Some customers have told us of third-party vendors drastically limiting the data extraction speeds to draw out their move to another cloud archive – in some cases estimating it would take a year or more to get their data back.

Journaling to an Office 365 Shared Mailbox

So, what is a shared mailbox? A shared mailbox is a common Office 365 mailbox that can be used by many employees in a group - for example a mailbox such as groupname@companydomain,com Many employees can have access rights to it and can send emails to anyone, all from the common email address.


Auditable Comms
Users
Users
Group Mailbox Resource (sales@company.com)
Users
Users
O365 | Active Directory Corporate Resource

The problem is Microsoft has lowered the storage limit of an Office 365 shared mailboxes to 50 GB, which is much lower than what a corporate customer would expect. This move is important because many companies use a shared mailbox for more than its intended use, for example as a journaling mailbox.

Also, many companies move mailbox contents from exited employees, to a shared mailbox. This is because it remains in Office 365, doesn't use an Office 365 license, and its free. However, Microsoft best practice dictate that ex-employee mailbox contents should be declared as inactive - this keeps the mailbox intact and separate and also frees up an Office 365 license. There are some downsides to using inactive mailboxes - which is why some companies have adopted the shared mailbox strategy, creating a shared mailbox that all contains all previous employee content.

What to do with Legacy On-Premise Journals

Many companies, particularly those in regulated industries such as financial services (Finserv or FinTech), have a requirement to journal content from select mailboxes, for example, brokers and traders, and retain the data for 3-7 years.

The issue Finserv companies face is the fact that Office 365 does not have, nor does it allow, mailboxes to be designated as journaling mailboxes. So, what can Finserv organizations do with their existing archived journals? Microsoft recommends companies either keep an on-premise Exchange server as the journaling repository or work with a third-party cloud provider to supply the journaling repository – neither which is considered ideal due to the impact of cost, as well as complexity.

Several third-party data migration companies have come up with a scheme of exploding an on-premise archived journal (usually a huge amount of data) and migrating the exploded emails into individual custodian's mailboxes.

An issue with this strategy is what happens to departed employee journaled email – there is usually no Office 365 mailbox to migrate it to. Another issue is that because journaled email can have 2 or more recipients, **each** email with multiple recipients must be duplicated so that the journaled individual email can be placed into each custodian's mailbox. This means that one on-premise 10 TB journal, when exploded and migrated into individual Office 365 mailboxes can grow to many times the original size in Office 365 – 20 TB, 40 TB, or more. Microsoft has let it be known that they do not want their customers following this process and again, suggest using an on-premise Exchange server or a third-party cloud provider.

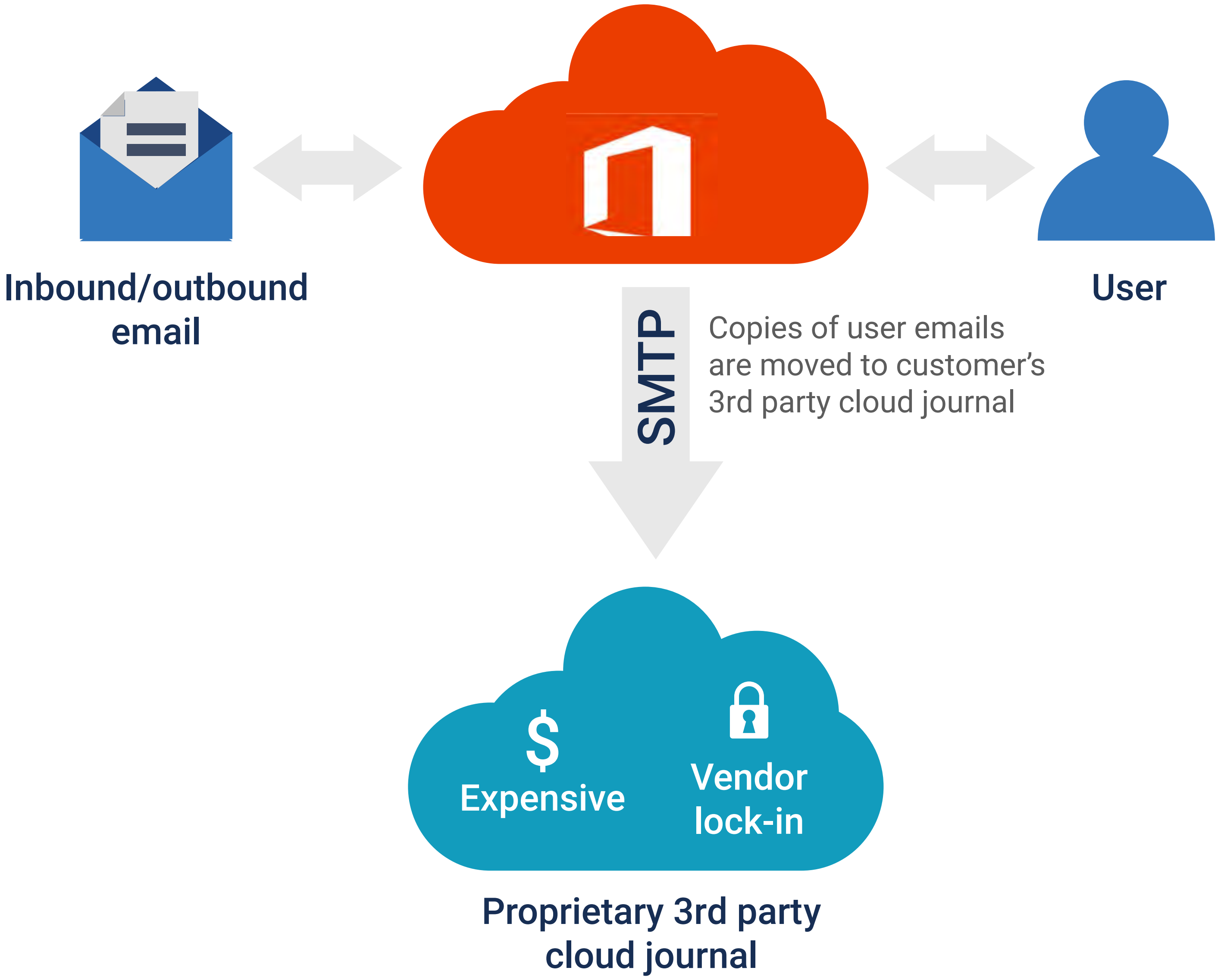

Inbound/outbound email
User
SMTP
Copies of user emails are moved to customer's 3rd party cloud journal
$
Expensive
Vendor lock-in
Proprietary 3rd party cloud journal

Fig 1: Using a third-party cloud as the Journal is expensive and risks being sentenced to data prison

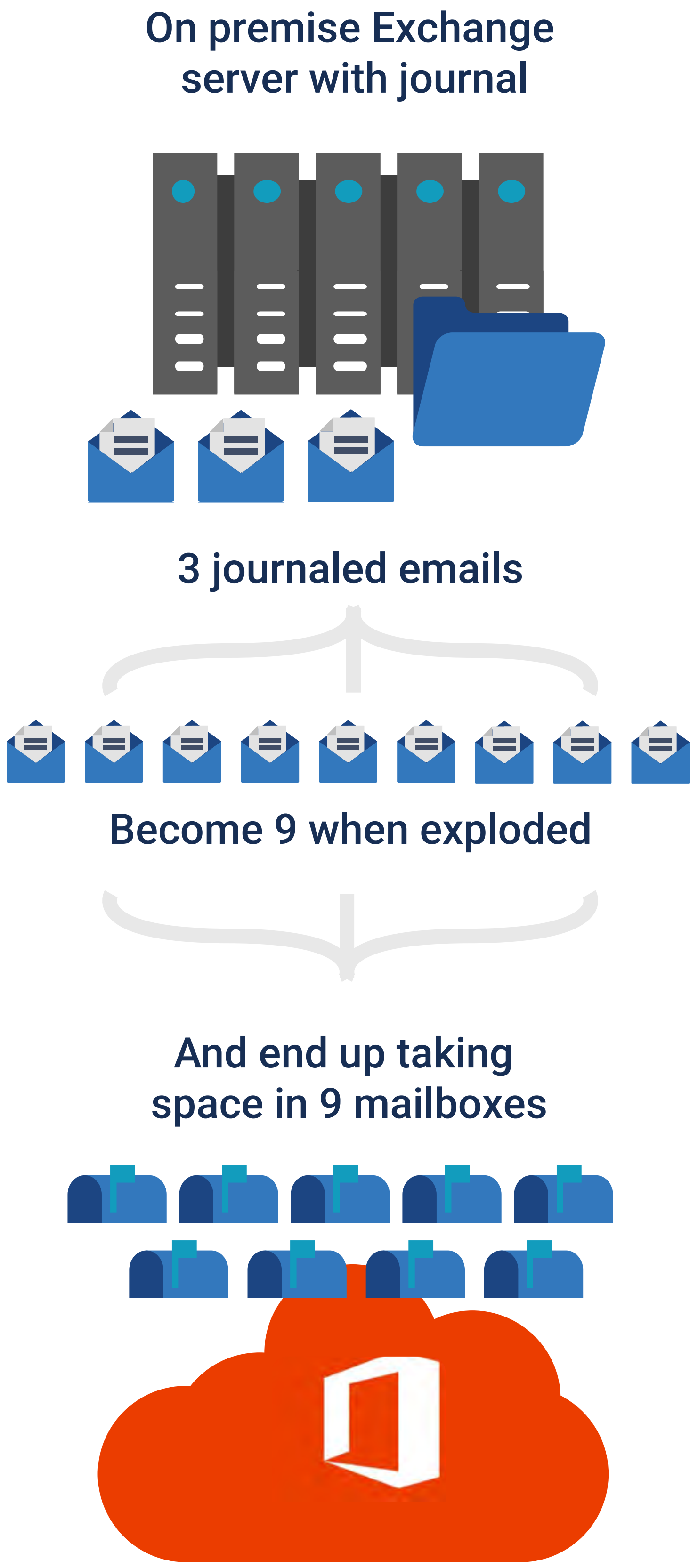
Another strategy some companies use is to migrate legacy archived journals into a shared Office 365 mailbox, accessing it when needed to respond to a regulatory information request or to perform eDiscovery. Again, because the new shared mailbox storage limit is now 50 GB, most legacy journals would not fit. Of course, you can split the journal among several shared mailboxes, but this complicates regulatory and eDiscovery searches. Also, for companies in the Finserv sector, shared mailboxes journals would not meet the SEC 17 regulations, including the requirement to store data in a truly immutable or WORM format.

The other challenge Finserv organizations face when moving to Office 365 is what to do with their on-going, live email journaling requirements.

Some companies began using an Office 365 shared mailbox as a live journaling repository (because its free) to save the expense of keeping an on-premise Exchange server active or paying the high prices for a proprietary third-party cloud.

Again, the problem with this strategy is, depending on the size of the organization, live journaling into a shared mailbox will need to be migrated regularly (raising regulatory or legal risk if not done) as the shared mailbox fills up. Let's not forget the new shared mailbox storage limit is now 50 GB. In reality, the 50 GB limit is driving companies back to the existing costly and complex journaling solutions by keeping an on-premise Exchange server active or using a third-party cloud, rather than reducing any cost and resource from their dilemma.

Fig 2: Exploding a journal can take up a great deal of space (and cost) in Office 365


On premise Exchange server with journal
3 journaled emails
Become 9 when exploded
And end up taking space in 9 mailboxes

Chapter 3:
Journaling for eDiscovery

Does your organization utilize Office 365 for email? Is your organization required to journal email for compliance, legal, or business requirements? Do your Attorneys complain about the time it takes to find information for an eDiscovery request? If the answer is yes to any of these questions, then keep reading.

A journal ensures "Golden Copy" status

As mentioned above, journaling was originally developed for capturing email from financial brokers and traders and has become an important legal requirement through the SEC regulation. But as companies moved from on-premise email systems to Office 365 (which is cloud based),journaling became more difficult. As Office 365 does not provide journaling capability, companies have been forced to adopted 3rd-party cloud solutions to act as the journaling folder. We will cover this in a later chapter.

Isn’t journaling just for financial services compliance?

Journaling is used extensively for litigation preparedness and eDiscovery and today is used just as much in any sector business, regardless of legal or compliance requirements. To capture and retain the email contents, some companies still utilize the email journaling feature in their on-premise Microsoft Exchange server. For many companies however, the 3rd-party journaling cloud option is too complex, too expensive, has potential security issues, as well as introducing vendor lock-in challenges.

Other companies using the Office 365 cloud, employ a 3rd-party cloud archive to journal from Office 365 infrastructure to their 3rd-party cloud archive. This may become costly due to the high cost of 3rd-party cloud archives, as well as vendor lock-in issues (if they exist). It’s important to note that not all Vendor have a lock-in, but you must be vigilant in order to ensure that you do not succumb to pitfalls when you sign-up with a partner.

Also, be careful about relying on journaling for eDiscovery without fully understanding the technical complexities of the implementation. Journals can be configured in several ways, some of them do not capture all message data (or metadata). Some configurations, for example, don’t capture the BCC recipient, a potential issue for eDiscovery response and dialogue inclusion. Best practice is to ensure you document what your journaling capabilities are (the specific method you use) for your “meet and confer” meeting and inform legal counsel of its use for preservation and collection purposes.

Chapter 4:
A better solution

Journaling to your cloud

So if keeping an on-premise archive active is inefficient and costly, and relying on a third-party vendor to keep your data in proprietary archives locks you into their contract, what possible solution is available to make this easier for your organization?

Many CIOs looked into the extremely low cost, security, and unlimited scalability of public cloud systems, such as Microsoft Azure, and gave feedback that if they could simply journal from their Office 365 email system to their own Azure tenancy, this would solve the O365/Journaling challenges. By taking advantage of the company's own low-cost cloud infrastructure, they could mitigate several issues.

Ideal Journal Archiving Solution

Legally defensible onboarding migration

- Accelerated onboarding from leading ECMs
- Guaranteed validation and immutability
- AI-powered autoclassification and tagging

Stay in control of your data

- Retain control and ownership of your data—store everything in YOUR Azure tenant
- Capture and maintain your information in fully-portable format
- Secure your data with your keys
- Control costs via policy-driven tiered storage and WORM

Flexible and global data insight

- On-demand data analytics and intelligent search to help with cost control
- Identify and investigate data trends, expose risks, mitigate fraud and liability
- AI-driven predictive records classification and sensitive data identification
- Meet complex eDiscovery and records management requirements

Preserve legal chain of custody with full audit trails

- Apply advanced retention policies
- Implement and enforce defensible disposition policies
- Secure and audited data access and RBAC
- Ensure records immutability

Is there a better solution for journaling in Office 365?

Wouldn't it be better to keep your legacy and live journal data within the same Microsoft Cloud while retaining full regulatory compliance, security, and control over your sensitive data?

Archive360's Archive2Azure platform enables customers to onboard their legacy journal data and stream live journal data while keeping the journal contents completely intact with zero metadata loss or data conversion. Archive2Azure is the first intelligent information management and archiving platform built for the Azure Cloud. This means that your sensitive legacy and live journal data always stays in **your** Microsoft Cloud under your direct control. Archive2Azure provides full data migration and cloud management of **your** journal data, all in one solution without the need to pay for and rely on a proprietary third-party cloud provider.

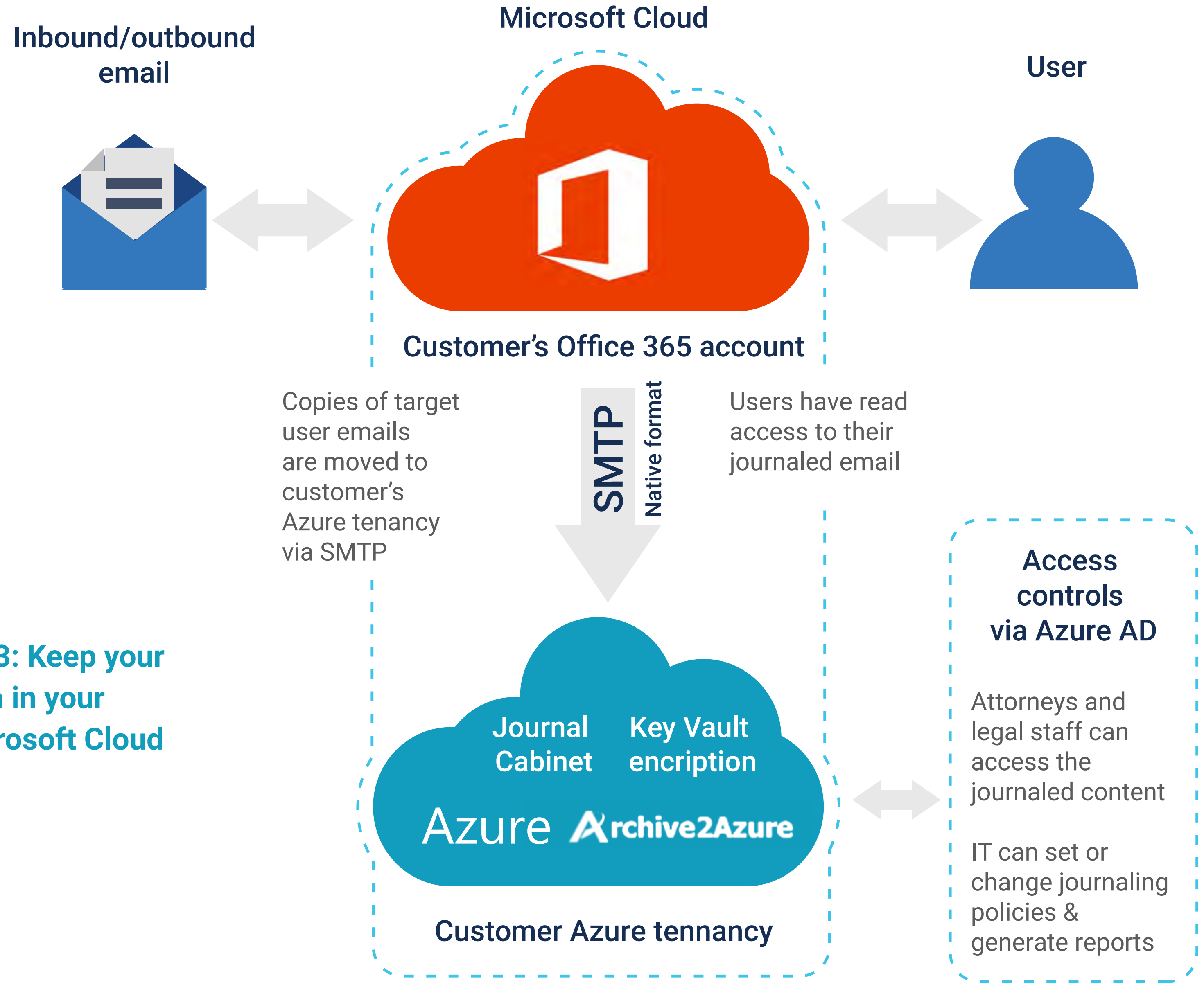

Inbound/outbound email
Microsoft Cloud
User
Customer's Office 365 account
Copies of target user emails are moved to customer's Azure tenancy via SMTP
SMTP
Native format
Users have read access to their journaled email
Journal Cabinet
Key Vault encription
Azure
Archive2Azure
Customer Azure tennancy
Access controls via Azure AD
Attorneys and legal staff can access the journaled content
IT can set or change journaling policies & generate reports

Fig 3: Keep your data in your Microsoft Cloud

Companies can now take advantage of their Azure tenancy to store and manage their legacy journal data as well as take live journal data from Office 365. With this solution, you no longer need to worry about being locked into a contract with a third party vendor, manage additional issues with shared O365 mailboxes, or the extra expense of keeping an on-premise Exchange server active.

With the “storage stress” of exploding your legacy journals, multiple times its original size, directing your live journal stream to an expensive third-party proprietary cloud (risking vendor lock-in), or keeping a costly on-premise Exchange server active, it would appear to be a less than ideal practice when you have the option of keeping your sensitive journal data within your same Microsoft cloud tenancy, but with the additional benefits of using your own encryption keys, infinite scalability and storage with a significantly lower cost it makes sense to give Archive2Azure a try.

For companies wondering what to do with their legacy and live journal data when migrating to Office 365, please keep the following in mind:

- Exploding legacy journals so you can migrate the individual emails into custodian mailboxes is not supported by Microsoft and for financial services companies, may put you at risk for SEC 17 non-compliance.
- Utilizing shared mailboxes for journal data no longer is possible due to the reduced storage limit of 50 GB.
- Keeping your on-premise Exchange server active is costly.
- Using a proprietary third-party cloud can be expensive and risks the issue of vendor lock-in.

Additionally, each of the above strategies increases the complexity and risk of regulatory non-compliance and litigation support.

ARCHIVE360

I help our enterprise and government customers translate compliance, privacy, and data sovereignty regulations into actionable solutions and I assist with modern eDiscovery best practices. I'm available to answer any questions about journaling, GDPR, or any emerging regulation impacting human-generated data in your business.

To schedule time with me, just send me an email:
bill.tolson@archive360.com

Bill Tolson | Vice President, Compliance & eDiscovery

Learn more at:
archive360.com/live-messaging-journaling

Back to top