



Solution Brief

Archiving from Office 365 for Compliance and eDiscovery

Barracuda Message Archiver and the Barracuda Cloud Archiving Service enhance Office 365 with the additional functionality needed to support sound information governance practices. Both enable organizations to meet demanding compliance regulations and address information discovery requests easily and effectively.

Requirements for Compliance and eDiscovery will vary based on the industry in which each organization operates. For example, heavily regulated industries such as financial services, healthcare and government have very specific requirements that have to be complied with, and the penalties for non compliance can be severe. However, all organizations need to implement sound information governance practices.

Microsoft has improved the compliance features within Office 365, and also provides an archive mailbox within Exchange Online. However, several key archiving and compliance capabilities are still either limited or missing. This means that Office 365 is unlikely to meet the wider needs of those organizations that have specific data retention, policy enforcement and eDiscovery requirements.

In this Solution Brief, we identify a number of key areas for Compliance and eDiscovery, as well as show how the Barracuda Message Archiver or the Barracuda Cloud Archiving Service can enhance Office 365 in those areas. We also highlight some additional points to consider when implementing Office 365.

Capture Everything

Organizations need to make sure they capture and secure a copy of every email message sent or received, and to do this before users have time to amend or delete those messages.

What Office 365 Provides

Microsoft's Messaging Records Management (MRM) within Office 365 doesn't provide this as a native capability. The way to ensure every email is captured is to place every mailbox across the organization on a permanent In-Place Hold as described in the next section. This is also the only way within Office 365 to capture an accurate list of all recipients for emails that have been sent to distribution lists.

This conflicts with the subsequent use of In-Place Hold functionality for its original purpose of supporting individual eDiscovery searches and responding to legal requests.

How Barracuda Helps

Barracuda takes an alternate approach and uses the Office 365 journal function to capture and secure a copy of each email "in motion" at the time it is sent or received. Unlike other solutions that involve "pulling" delivered mail from individual Office 365 mailboxes using POP or IMAP, Barracuda will not be susceptible to throttling or any other Office 365 performance restrictions.

The Barracuda approach ensures that an accurate and unmodified copy of every email sent or received, including details of all recipients, will be captured and stored securely.



Keep Everything Securely

For an extended period of time, organizations will need to securely keep all emails they have captured in order to respond to eDiscovery and other information requests.

What Office 365 Provides

Office 365 uses an “in-place” approach to retain an original copy of every email that every user has ever sent or received within that user’s mailbox. The user is still able amend or delete their email at any time, even if it has been moved into the their archive mailbox. To ensure an original copy is kept, all messages must be put on In-Place Hold.

In-Place Hold operates at the individual message level using the Recoverable Items folder (which is not visible to end users), as follows:

- When an email is deleted by the user, it is moved into the Discovery Hold subfolder within Recoverable Items and kept there for the duration of the hold.
- Each time an email is amended by the user, a copy of the email before amendment is added to the Versions subfolder within Recoverable Items.
- All emails that have not been amended or deleted are simply retained in the user’s mailbox for the duration of the hold.

This is a complex process to understand and manage since it operates within the production email environment. The original copies within each mailbox will be spread across multiple folders and there can be multiple versions of an email within a mailbox. A similarly complex process is followed for emails in public folders.

As the Recoverable Items folder is also used for a number of other processes (such as audit and calendar logging), it can be difficult for organizations to guarantee and demonstrate—for compliance purposes—that they are actually retaining a complete and accurate copy of every email sent or received.

How Barracuda Helps

Barracuda takes an alternative approach by capturing a single immutable copy of every email. It minimizes risk by storing this copy outside the production email environment in a separate secure archive repository, either in a dedicated hardware or virtual appliance, or in the Barracuda Cloud.

This straightforward approach ensures that original email data will be stored securely for as long as needed without risk of corruption or deletion. Compliance is easy to demonstrate, and end users can have read-only access to search and retrieve email themselves at any time from any device.

Keep Everything for as Long as Needed

After capturing email and storing it securely, organizations then have to make sure they retain it for as long as it is needed. An increasing number of organizations are implementing compliance policies for message retention and deletion to ensure all relevant information remains available to support eDiscovery and other information requests. This may be driven by specific industry or legal requirements, or as part of an overall information governance strategy.

What Office 365 Provides

Retention policies in Office 365, despite the name, do not ensure that email is retained for as long as required. Their purpose is to ensure that data is deleted after a specified period, and they are not able to prevent users from deleting or amending email at any time before that.

Retention policies are limited to selection based on age or location, and may not provide the flexibility or granularity many organizations require to meet their individual compliance policies.

In order to ensure that all data is retained for the specified period, once again, mailboxes must be placed on In-Place Hold for that duration.

It is also useful to note that although data stored in public folders can be placed on hold, it is not possible to apply retention policies to these folders. Therefore, there is a risk of this data being retained indefinitely.

How Barracuda Helps

Retention policies within Barracuda manage both the retention and deletion of each message. They will ensure that an original copy of every email sent or received will be retained in the archive for the entire specified period, and then deleted at the end of that period.

These policies are highly configurable and cover a wide range of criteria, such as message type, content, source, addresses, age, and attachments. Therefore, they can meet the most complex compliance and business needs.

Barracuda can also manage the retention and deletion of data that has been captured and archived from public folders.

Respond to Information Requests

When responding to eDiscovery and other similar information requests, organizations will start by identifying an initial set of relevant data. This set must be put on legal hold to prevent it from being amended or deleted for as long as it takes them to refine and complete that request, regardless of any other retention rules that may apply to the data concerned.

What Office 365 Provides

The In-Place Hold facility in Office 365 can be used with In-Place eDiscovery or the Office 365 Compliance Center to support individual search or discovery exercises. It can identify and secure the specific set of data that is relevant to each particular investigation for as long as is needed.

However, as we have seen earlier, many customers may have already applied a blanket In-Place Hold to every mailbox as a means of ensuring they capture and retain an accurate record of all data sent and received. This will conflict with the subsequent use of In-Place Hold functionality for its original purpose of supporting individual eDiscovery searches and responding to legal requests. This conflict can cause confusion and lack of clarity, particularly with demonstrating chain of custody.

The use of In-Place Hold can result in multiple versions of an email being stored in the Recoverable Items Versions subfolder, so customers must ensure their search only returns original versions from this location.

How Barracuda Helps

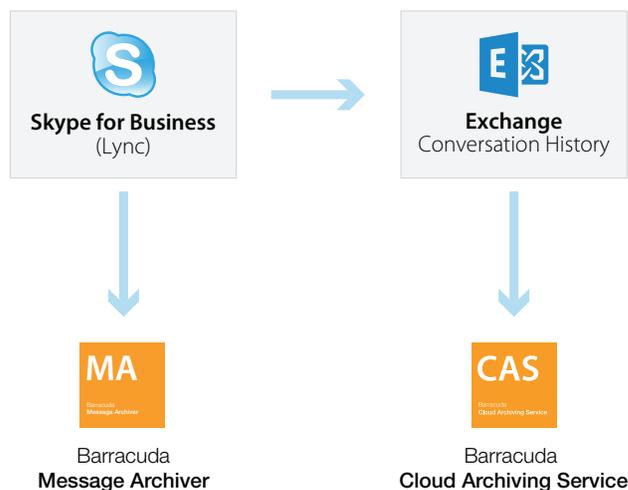
Barracuda also provides extensive search and discovery capabilities, and can apply legal holds to selected data on an individual case-by-case basis. However, it differs from Office 365 by managing this outside the operational environment on a separate secure archive copy of the data.

This “best practice” approach means that there is no conflict between data retention for operational compliance and legal hold for search and discovery exercises. As a result, it is easy to demonstrate the accuracy and completeness of data returned for each case, and to provide the chain of custody for that data.

Don't Forget Instant Messaging

Instant messaging (IM) is increasingly becoming adopted for communicating internally within an organization, as well as being used externally between organizations. In many cases, it is now used as an alternative to more traditional email communication, so just as with email there is a need to retain all IM content and make it available for search and retrieval.

Industry and business regulations are recognizing this trend, and many are now requiring organizations to accurately capture and preserve all instant message conversations for legal and compliance purposes. They may need to respond to eDiscovery requests on this data, as well as comply with the existing range of laws and regulations, such as FOIA, that



require message archiving and retrieval.

What Office 365 Provides

Skype for Business is Microsoft's Office 365 solution for providing instant messaging and conferencing to businesses of all sizes, and is a central component in many Office 365 plans. However, it does not include the ability to capture, archive or retain a copy of these conversations securely.

Office 365 can be configured to store IM conversation history within the Conversation History folder in each end user's Exchange Online mailbox, but this has the same limitations we have already discussed for email for retention and secure storage. Users are able to modify or delete data if the entire history folder is placed on "In-Place Hold."

How Barracuda Helps

Barracuda captures and archives a copy of all IM conversations, conferences and other content from the Conversation History folder. This data is then kept securely alongside other archived content such as email messages and attachments, meaning that all message data is available in one place for end users to search and retrieve. It also provides a single solution for organizations to meet their compliance and eDiscovery requirements for both email and IM.

Don't Forget to Keep Costs Under Control

What Office 365 Provides

As we have seen, in order to fully meet compliance and eDiscovery requirements using Office 365 all mailboxes across the organization must be placed on In-Place Hold.

The In-Place Hold capability is only available for mailboxes that are on the Office 365 E3 plan or above, or on Exchange Online Plan 2.

Providing an E3 or a P2 license for every user in an organization can represent a considerable additional cost, especially if they do not need the other advanced features enabled with these licenses. To put this into context, the cost of Exchange Online Plan 2 is double that of Plan 1, and the Office 365 E3 plan is three times the cost of the E1 plan.

How Barracuda Helps

Barracuda can provide all archiving, retention, compliance and eDiscovery functionality for all users within an organization at a single price. Because it does not require all users to be on higher level Office 365 licenses, it can be a very cost effective solution.

Conclusion

Compliance and eDiscovery capabilities provided within Office 365 may be adequate for some organizations, but the "in-place" approach Microsoft takes for long term email retention and preservation means these capabilities have inherent limitations. They can be complex and expensive to operate, and are unlikely to meet the needs of organizations with more demanding compliance and discovery requirements.

Barracuda Message Archiver and the Barracuda Cloud Archiving Service both enhance Office 365 with the additional functionality customers will need to meet demanding business and legal requirements. They follow the accepted "best practice approach for compliance by archiving an original copy of every email into a separate immutable store for long-term retention and preservation. Comprehensive retention and discovery capabilities, combined with ease of operation and use make either one a cost effective solution.

