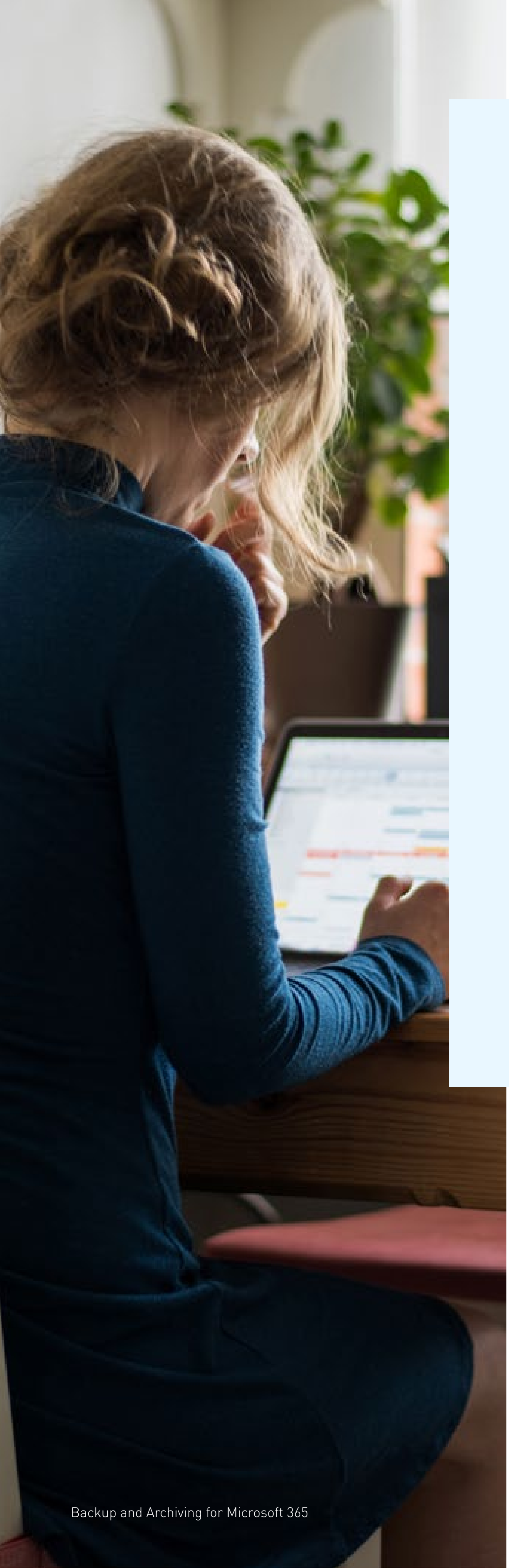
Hammer Technical Services

WHITEPAPER

Backup and Archiving for Microsoft 365

Contents



SUMMARY

Business leaders and even IT staff sometimes struggle with articulating the difference between backup and archival, and often conflate their operational use.

The purpose of this paper is to compare and contrast how these services work to support a Microsoft 365 environment and the specific problems they address. This can help organizations more effectively map their business and technical requirements to backup and archiving, and have a better understanding of how these services should be used together for maximum protection of operational data and ultimately, the business.

2 COMPARING BACKUP AND ARCHIVING

Backup and archive retain copies of production data, but the way they capture, store, structure, index and retrieve that data is very different because they address different operational requirements. Equally important, email archiving addresses Exchange email messages and attachments while backup for Microsoft 365 addresses workspaces like SharePoint and Teams, files stored in OneDrive, Exchange email and other Microsoft 365 operational data such as calendars and Office 365 Groups.

BACKUP

A backup enables recovery from a situation where data has been lost, corrupted or becomes inaccessible, so it's primarily a safeguard to facilitate data recovery.

A backup stores multiple copies that are each associated with a specific revision of data, and it provides recovery back to a known good state from a specific point of time.

ARCHIVING

An archive enables compliance with legal and business data retention policies, as well as supporting eDiscovery.

An archive preserves a single copy in secure immutable storage for a finite time period and provides ongoing end user access to historical business information.

This Table Summarizes Some of the Key Differences Between Backup and Archiving:

FUNCTION	BACKUP	ARCHIVING
Primary Purpose	Protect current and revision data	Preserve historical data
What It Enables	Point in time data recovery	Data retention and discovery
Business Needs	Restore data after loss, corruption or unintentional deletion, to a specific point in time	Produce complete and accurate evidence to meet legal, regulatory, and policy obligations
Who Uses It	Administrators (IT)	Business Users (Legal, HR, etc...)
What It Stores	Multiple point in time copies of data revisions	A single fully indexed copy of all data
Optimized For	Point in time restore of production environment	Item level preservation, search, retrieval, analysis, and export
Data Disposition	Source data is left in place	Source data may be deleted
Search	Point in time revision and basic metadata search	Full-text search of files, attachments and metadata (custodians, keywords, etc.) plus eDiscovery capability
Retention Polices	Primarily based on the age of data that would need to be restored	Primarily based on age, location, content and metadata. Includes overriding Legal Hold capability

For effective data protection and preservation, organizations need both a backup and an archiving strategy. They may attempt to use a backup solution as an archive (and vice versa), but as will be discussed below, there are significant limitations and deficiencies with this approach that make it inadvisable.

3 BACKUP IS FOR RECOVERY

The primary purpose of backup is to allow recovery from the situation where the original version of data is lost due to unintentional or accidental deletion, or where files have been corrupted in some way to make it unusable.

A backup system achieves this by taking copies of the data on a regular basis to create a series of revisions. Each one of these revisions reflects the data at a specified point in time and can be restored back as needed.

A backup system is critical to addressing the risks of data loss because the Microsoft 365 cloud does not provide comprehensive protection and recovery from data loss due to human action or other events that can compromise data.

- Users may accidentally delete an email, file, or folder. In some cases, a user may intentionally delete a file, simply because they don't realize it might be needed later. And in remote work environments, computers shared with or accessible by other users are more vulnerable to unintentional deletions or accidents.
- Employee turnover creates opportunities for a disgruntled employee to maliciously delete valuable contact information, or an entire mailbox or OneDrive account. A SharePoint admin can actually permanently delete an entire SharePoint site collection, making it immediately unrecoverable.
- Malware and ransomware are constant and growing threats in corrupting your data, and making it unrecoverable. Ransomware is such a common threat that it is incumbent to not just protect data, but also to minimize downtime for users when this occurs.
- Even secure clouds are vulnerable to variety of software issues that contribute to data loss events. These include over-writing data, license changes or other changes with software or hardware that can make data unrecoverable.

A backup system is critical to addressing the risks of data loss because the Microsoft 365 cloud does not provide comprehensive protection and recovery from data loss due to human action or other events that can compromise data.

WHY YOU NEED TO BACK UP MICROSOFT 365

While Microsoft 365 does include a range of features that offer some level of data protection, it is important to know that these don't offer the complete data protection and recovery that businesses need, which is why Microsoft recommends businesses use third-party services to regularly backup their content and data.

Microsoft 365 covers the availability of your data 'as-is' across multiple data centers in the event of a data center outage, but it doesn't cover the state of your data as it was before a data loss. If data is deleted, that deletion is replicated across data centers.

Data that is deleted in Microsoft 365 is retained for a limited time, depending on the application, license limits, and configurations for specific plans. In many cases, data can be recovered if data loss or corruption is identified in a timely fashion. But unfortunately, if you don't realize what data was lost before the retention expires, it will be unrecoverable.

Also, retention periods and data capacity differ across Microsoft 365 services. While the details vary from plan to plan, the most common data recovery capabilities are:

MICROSOFT 365 SERVICE	RETENTION PERIOD	DATA CAPACITY
Exchange Email	14 days	50-100 GB
Microsoft Teams/Office 365 Groups	30 days	50GB
SharePoint and OneDrive	186 days	1TB

Retaining data when an employee leaves an organization is another problem area with Microsoft 365. All data stored by a user in Exchange Online will be permanently deleted 30 days after their account is deleted, so this data must be backed up first. Email data may be retained for a longer period if a retention policy is applied before their account is deleted, but this is a premium feature only available in Office 365 E3 plans and above.

To address this, organizations use third-party backup with Microsoft 365 to provide much more complete protection, as well as much longer retention periods and more comprehensive recovery options.

PROBLEMS WITH USING A BACKUP AS AN ARCHIVE

There are a number of issues using backup as an archiving solution:

- A backup will capture all data that exists at a specific point in time, but it will not capture volatile data such as new email messages that may be amended or deleted before the next backup is taken. This means that a backup cannot support fully compliant data retention and eDiscovery for an organization.

- Legal requirements and business regulations mean that organizations typically need to enforce a set of retention policies covering different types of information, and these are often based on the data content itself or the metadata associated with each data item. Indexing allows archiving to support a wide range of policy-based retention rules to meet the most demanding of requirements, whereas the retention policies within backup solutions do not usually provide this granular level of control.

- Archive solutions are designed to support search and retrieval, so all data content and metadata will be indexed, and advanced techniques such as full-text search and data tagging are provided to enable business users to undertake discovery exercises easily without IT involvement. In contrast, backup solutions are designed for use by administrators working at the file level or higher, and as data is typically not fully indexed, attempting to use a backup for eDiscovery can be an extremely complex and time-consuming task for the IT department.

- Backup solutions retain multiple point-in-time revisions to enable organizations to meet recovery point objectives. But searching across multiple revisions will return multiple versions of individual data items which then need to be reconciled in order to provide a single set of accurate and verifiable results for eDiscovery. In contrast, an archive provides a single verifiable copy of each data item.

- As backup solutions are not accessible by end users, meeting the needs of end users for access to their historical data can be a significant ongoing overhead for the IT department. In contrast, archive solutions provide the ability for end users to search and retrieve their own archived data, and allow them to restore individual items as needed, all without the involvement of their IT department.

4 | ARCHIVING IS FOR DISCOVERY

The primary purpose of archiving is the long-term preservation and retention of current and historical data, to enable the organization to undertake legal and other eDiscovery requests on this data as well as meeting their compliance and business requirements for data retention and deletion.

An archiving system achieves this by capturing and securing a copy of every item of data as it is created. In the case of email, this must be captured as soon as the message is sent or received, and before an end user has time to amend or delete the message.

The archive builds up over time to reflect every item of data that has ever existed during that time, even if it has since been deleted from the original location. Retention policies ensure that the archive copy of each item of data is retained for as long as required, and deleted after that time.

End users are able to search and retrieve their own archived data whenever needed, while auditors and other administrative users are provided with a range of advanced search and export features to enable them to undertake complex organization-wide eDiscovery requests.

WHY YOU NEED TO ARCHIVE FROM MICROSOFT 365

Microsoft has improved the compliance features within Microsoft 365, and also provides an archive mailbox within Exchange Online, but there are still a number of limitations. Together with the use of "In-Place Archiving" instead of a separate dedicated archive, this means Microsoft 365 is unlikely to meet the wider needs of those organizations with specific data retention, policy enforcement, and e-discovery requirements. It's also important to note that archiving and compliance features require the more expensive Office 365 E3 and E5 plans.

DATA SECURITY

Microsoft 365 retains all data (including archived data) in the operational environment where it co-exists with more transient data and is at risk of amendment or deletion. This contrasts with third-party solutions that take the accepted "best practice" approach to retaining a separate immutable copy of every email outside the operational email environment in a separate secure repository.

DATA RETENTION

Retention policies for email in Microsoft 365 are limited to just age or location, and do not provide the flexibility or granularity many organizations require to meet their compliance requirements, such as rules pertaining to custodians or content.

DATA PRESERVATION

Retention policies within Microsoft 365 use a complex process with multiple folders to secure email data against modification or deletion. The Discovery Hold and Versions subfolders within the Recoverable Items folder are used to store original copies of items that have been deleted or modified, whereas unmodified items remain in the user's Inbox or Archive Mailbox. This means that the original copies of emails can be spread across multiple folders and there can be multiple versions of the same email within a mailbox, so it is not easy to ensure and demonstrate you are retaining a complete and accurate copy of every email sent or received.

These and other limitations mean that Microsoft 365 is unlikely to meet the wider needs of organizations that have specific data retention, policy enforcement and eDiscovery requirements, and many are now implementing third party archiving solutions to enhance Microsoft 365.

PROBLEMS WITH USING AN ARCHIVE FOR RECOVERY

Some organizations may be tempted to use data stored in their archive as a backup solution, but this approach has a number of limitations that make it unsuitable and problematic:

- An archive captures a copy of all data items created over a period of time in a single version, compared to a backup where each revision captures each data item within its current context at that specific point in time. It may not be feasible to do a point in time data restore from an archive without considerable additional processing.
- The directory structure for each user's data in the archive will be based on historical information and possibly not reflect their current live usage, making it difficult to restore data back to the correct location.
- An archive will retain (subject to organizational retention policies) a copy of all data that a user has ever owned over the period of time. This will include items that have been intentionally deleted and that should not be restored unless specifically requested.
- An archive is optimized for search and retrieval, and may be appropriate for end users to recover individual items. However, it is likely to be inefficient when used for the recovery of larger quantities of data such as entire folders or mailboxes.

5 BACKUP AND ARCHIVE SHOULD WORK TOGETHER

As we have seen, backup and archiving perform separate functions for different reasons, but they are complementary, and the capabilities of each one can help the other work more effectively.

Storing data within an archive is the best way to retain a secure copy of all historical information, and will enable an organization to meet its business requirements for compliance and discovery.

Archiving older or inactive data and removing it from operational storage will also improve the operation of backup processes. By reducing the volume of data to be backed up, backups will run more quickly, and with less data to manage, it will be easier to restore data when needed.

6 BACKUP & ARCHIVING SERVICES FOR MICROSOFT 365

BACKUP FOR MICROSOFT 365

Backup for Microsoft 365 provides simple and complete protection for your Microsoft 365 users with regular backups with unlimited capacity and retention for your Microsoft 365 tenant, including Exchange, OneDrive, Microsoft Teams, SharePoint, and Office 365 Groups. Backup for Microsoft 365 can be turned on in seconds with up to 6 daily backups, with no data limits or overages using a full cloud to cloud backup, so there is no impact on your business or any requirements for additional hardware or software.

EMAIL ARCHIVING FOR EXCHANGE ONLINE

Email archiving preserves Microsoft 365 Exchange email to facilitate compliance, and speed eDiscovery with a service that’s fast, scalable and secure. This set-and-forget service captures all sent and received email and stores them securely in a separate archive repository for as long as needed without risk of amendment or deletion.

CONCLUSION

Businesses that have adopted Microsoft 365 need to protect their investment in productivity and intellectual property by ensuring they are adequately protected from the challenges of both recovery, and discovery. They are ultimately responsible for protection, backup and compliance for the data in Microsoft 365. Having effective backup and archiving in place is critical to meeting these goals.

Although backup and archiving sound similar, they address different operational requirements, and are not adequate substitutes for each other. Comprehensive recovery and discovery requires both services.

We are an industry leader in providing cloud services for businesses and can help you deploy these services quickly to meet your business requirements.

QUESTIONS? CONTACT US TODAY!

Hammer Technical Services, Inc.
Kerry Hammer, CEO

(830) 765-2812
www.hammertechservices.com

service@hammertechservices.com