Protecting Critical Data Starts with Microsoft 365 Data Resiliency and Recovery

Migrating to the cloud brings a host of benefits, beginning with anytime/anywhere data access. However, even in the cloud, organizations need to plan for business continuity and data recovery. The key to protecting information assets begins with understanding Microsoft 365 data resiliency and recovery.

While machine failures and natural disasters pose less of a threat in Microsoft 365 than with on-premises data, other risk scenarios exist. For instance, a disgruntled employee may delete critical files or emails. Likewise, an admin can mistakenly remove large portions of content. And cyber criminals always pose a threat.

Fortunately, Microsoft has implemented several layers of data retention features to help organizations preserve their data assets. Understanding these features and their limitations will help organizations make informed choices about their data.

Built-in Data Redundancy and Emergency Backup

To begin with, Microsoft mirrors your data in at least two separate data centers. This drastically reduces the possibility that a natural disaster or outage will render your data inaccessible.

Additionally, SharePoint Online keeps backups of all content for 14 days. If a large number of SharePoint files get deleted or corrupted, the organization can request a restore from Microsoft Support. However, keep in mind that this will restore an entire SharePoint document library to an earlier time. Any changes to folders or files after the recovery point will be wiped out.

Microsoft 365 Data Resiliency and Recovery in SharePoint and OneDrive

Microsoft 365 protects data in SharePoint and OneDrive in multiple ways. All plans enable versioning by default, storing 500 versions of each file. Users can revert back to an earlier version. And organizations can increase the limit to 50,000 versions if necessary.

Additionally, once a file or site collection has been deleted, a post-deletion retention period begins. That is, the deleted files stay in either the recycle bin or a second stage recycle bin for 93 days before the system deletes them permanently. The files can be recovered at any point during the 93 days.

Data Retention in Exchange Online

Microsoft also provides several features to protect mailbox data. For instance, Exchange retains deleted mailboxes for 30 days. And when an individual item is deleted, it remains in the Deleted Items folder until someone clears the folder. At that point, individual items are retained for another 14 days before being permanently deleted. That period can be lengthened to 30 days.

Finally, Microsoft 365 plans that include Exchange Online Archiving also offer the option of a litigation hold. When the litigation hold property is applied to a mailbox, the system retains all items in that mailbox indefinitely.

Compliance Retention

In addition to standard retention features, organizations with Microsoft 365 E3 or E5 plans can define data retention policies. These policies preserve data, deleted or not, for the time period specified in the policy. And because retention policies capture all versions of SharePoint items, they provide for a continuous backup.

Reasons to Implement a Third-Party Backup

With the combination of standard retention and compliance retention, Microsoft 365 offers robust features for preserving critical data. Many organizations find that these features offer all they need to recover lost data. However, there are a few reasons an organization might consider a third-party backup solution:

1. Research shows that in many cases, it takes organizations an average of 140 days to discover data loss. By that time, the standard retention period of 93 days for SharePoint would have already lapsed.
2. Restoring items retained through compliance retention can prove prohibitively time-consuming.
3. Microsoft applies storage limits, charging for storage over and above the allowed amount. Compliance retention and litigation holds, in particular, can quickly eat up the available storage.
4. When a Microsoft 365 account is deleted, as when an employee leaves, the system deletes all data in that account. Without a backup, the data will be lost.

Making Sense of the Options

While Microsoft takes good care of your data, it can prove confusing to sort through the various options and determine the need for additional backups. Likewise, effective implementation of compliance retention requires familiarity with Microsoft 365 administration.

With our longstanding Microsoft partnership and deep experience in data security and business continuity, the experts at eMazzanti can help you grow your business with Microsoft 365.