Cloud Data Backup and Restore Essential for Business Continuity

As businesses move some or all their workloads to the cloud, many organizations assume that the need for data backup and restore has gone away. However, in an age of hybrid workplaces and increased cyber threats, the right backup strategy remains a critical component of business continuity.

For instance, with remote workers using a variety of devices to create and share data, the likelihood of cyber attack or data corruption increases. Without the ability to quickly restore clean data, companies risk losing critical data and taking a productivity hit.

Over one million companies use Microsoft 365. Yet the majority of those organizations do not have a backup system in place, instead depending on native Microsoft tools to protect against data loss. While built-in tools do provide important protections, they have significant limitations. Consequently, organizations need to implement a carefully designed backup strategy.

How Microsoft 365 Backs Up Your Data

Microsoft, like most cloud vendors, operates on a shared responsibility model for data cyber security. That means that, while Microsoft generally secures the infrastructure, customers retain primary responsibility for securing their data. That said, Microsoft 365 does include several key data protection features.

To begin with, Microsoft provides data redundancy by mirroring business data in at least two locations. Additionally, customers can restore data deleted from OneDrive and SharePoint within 93 days. Microsoft also retains deleted mailboxes for 30 days and keeps a 14-day backup of your Office 365 data.

In addition to these default protections, customers with at least a Microsoft 365 E3 license can set retention policies to preserve data even when someone deletes it. And organizations can create a litigation hold to preserve certain data indefinitely.

Limitations of Built-in Tools

However, these data protection features do not provide the same protection as a data backup plan. To begin with, the average time before a business discovers data loss is 140 days, well beyond the 93-day recycle bin period. And if a customer discovers data loss in time to restore from the recycle bin, they will need to restore file by file, recreating the structure.

Further, while Microsoft does create backups of your Office 365 data, they offer limited restoration options, with little granularity. For instance, they will conduct a full restore of a SharePoint site or mailbox upon request, but this will overwrite all existing data and can take a long time.

Powerful features like retention policies, litigation hold and DLP policies offer essential services. But they require proper configuration, and restoration requires a data search or eDiscovery, without the benefit of being able to view the file structure or mailbox.

Creating a Solid Backup and Restore Plan

Third-party backup solutions offer convenience and simplicity, as well as more granular options for restoring lost data. And by following data backup best practices organizations gain the peace of mind that comes with a solid insurance plan.

To choose the best backup solution, organizations need to consider what data needs to be backed up and where it lives. For instance, while backing up SharePoint, OneDrive and Exchange is straightforward, not all solutions back up data such as Teams chats. And backup plans need to account for all endpoints.

Additional key items to address in a backup and restore plan include:

- **Automate** – Automate regular backups for centralized data storage but also for team members.
- **Protect the backups** – To keep the backups safe and usable, employ encryption and keep multiple backups in different locations.
- **Create restore plans** – First, map out what needs to happen in a data restore. Then choose a vendor that offers the granular options you need for restoration.
- **Testing** – Regularly test both the backup and the restore process to ensure backups are clean and that the restoration happens as it should.
- **Back up structure and settings as well as data** – To ensure a seamless restoration, make sure to take data organization into account. For instance, in addition to preserving the files themselves, include the system of folders and subfolders. Additionally, backing up permissions and settings proves crucial in the event of a system rebuild.

Comprehensive Data Backup and Restore with eCare Cloud Backup

eCare Cloud Backup from eMazzanti Technologies delivers comprehensive backup coverage across Microsoft 365. Customers benefit from automatic backups up to six times daily, with no storage limits. Flexible restore options deliver full, granular, and point-in-time data restoration with one click.