Cloud Data Backup Tips to Protect Essential Business Data

As the majority of businesses migrate data to the cloud, many assume they no longer need to back up their data. However, cloud storage does not take the place of data backup. In fact, hybrid work increases the likelihood of cyber attack and data corruption, making it even more important to put a cloud data backup strategy in place.

Consider that over one million organizations use Microsoft 365. However, although Microsoft itself suggests using a third-party backup solution, most of these companies do not have a backup system in place. Additionally, most organizations store data in a combination of on premises and multiple cloud locations. Protecting data from multiple platforms and thousands of devices requires a strategic approach.

Native Tools from Cloud Vendors Have Limitations

Cloud vendors like Microsoft include native tools for backup and recovery of data stored in their platforms. These backup options deliver cost savings, but they come with significant limitations and little flexibility. In the first place, native retention applies only to certain types of content and caps out at 93 days, insufficient to meet regulatory requirements for retention.

Additionally, native Microsoft backups offer little granularity in their restoration options. Conducting a full restore of a SharePoint Site or a mailbox, for example, will overwrite existing data and take a long time. And while powerful features like retention polices play an important role, these features require proper configuration.

Essential Components of Backup Plan

When choosing a backup solution, the organization first needs to determine what data needs to be backed up and where that data lives. For instance, data in Teams chats requires a more complex approach than backing up SharePoint sites or Outlook mailboxes. Also, the prevalence of remote work and BYOD policies greatly increases the number of endpoints to back up.

Address the following essential items when implementing a backup solution:

- **Automation** – Automate backups to streamline the process and reduce the risk of human error.
- **Multiple backups** – Even in the cloud, organizations still need to create multiple, separate copies of essential data. This can include storing copies in different regions or separate data centers. Thus, a regional disaster or corruption from ransomware will not make backup data inaccessible.
- **Testing** – Test both the backup and the restore processes regularly to ensure backups are clean and restoration occurs as it should.
- **Back up data structure and settings** – In addition to backing up the data itself, consider how that data is organized. This involves backing up the system of folders and subfolders as well as the data. Backing up permissions and other data settings will also prove critical if the system needs to be rebuilt after ransomware.
- **Capture endpoints** – A single organization can have data stored in thousands of endpoints, from the cloud to PCs, servers, and mobile devices. A reliable backup solution will need to address all these endpoints.

- **Ensure regulatory compliance** – As privacy regulations grow increasingly complex, be sure that backup policies take into account data retention and security mandates. For instance, regulations can affect what data needs to be backed up and how long to retain backup copies.

Advantages of Cloud Data Backup

Cloud backups involve backing up data directly to a public cloud, to a service provider's private cloud or from one cloud to another. Cloud backups offer several key advantages. In the first place, users and administrators can access backed up data from any internet-connected device. Administrators can also monitor and manage data backup and storage using web-based tools.

In addition to accessibility, cloud backups offer scalability. Traditional backup solutions require purchasing expensive servers and guessing at future data needs. On the other hand, adding additional cloud storage requires just a couple of clicks.

What to Look for in a Cloud Backup Service

While all cloud backup providers provide general backup services, the specific options can differ greatly from vendor to vendor. Therefore, organizations should look closely at their own needs and at the services each cloud provider offers.

For instance, look for comprehensive data security options including end-to-end encryption. Ensure that the provider can handle all the various operating systems and applications in your data environment. And verify that they offer the desired degree of granularity in recovery options.

As you examine your data environment and backup needs, reach out to the consultants at Messaging Architects. With deep understanding of the challenges of a hybrid environment, we can help you find the right cloud backup solution to protect your business data.