Backup Software Solidifies Enterprise Backup and Recoverability of Microsoft Office 365 Data

by Jerome M Wendt

Many organizations globally have come to adopt Microsoft Office 365 thanks to its enterprise availability, management, and reliability features. Despite these benefits, organizations must still assume responsibility for protecting any data they store in Office 365. Only by using third party backup software can they confidently back up and recover all their Office 365 data.

Quest

COMPANY

Quest Software, Inc.
4 Polaris Way
Aliso Viejo, CA 92656
800.306.9329

Founded 1987

www.quest.com/netvault365/

INDUSTRY

Information Technology

MICROSOFT OFFICE 365 DATA PROTECTION SHORTCOMINGS

- All data stored in Microsoft Azure cloud
- Can only access and recover data when connected to Microsoft Office 365
- Malware may programmatically empty Deleted Mail folder or Recycle Bin
- Only stores deleted data in Deleted Mail folder or Recycle Bin
- Ransomware can encrypt deleted and production data

BENEFITS OF USING THIRD PARTY BACKUP SOFTWARE SUCH AS QUEST NETVAULT BACKUP

- Can access and recover data at any time
- Can store data on on-premises disk or tape or in other providers' clouds
- Recover data in the event of a ransomware attack
- Recover data even when Deleted Mail folder or Recycle Bin emptied
- Stores data outside of Microsoft Azure cloud

Microsoft Office 365 Protects My Organization's Data … Right???

Organizations of all sizes adopt Microsoft Office 365 for many viable reasons. It runs in the cloud. They no longer must buy hardware and software or retain staff to maintain it. They achieve higher levels of availability. It eliminates data migration challenges. Anyone can access their data anywhere using a variety of methods and devices (browser, desktop, or mobile.)

The many features Office 365 includes may lead some organizations to assume Microsoft includes backup and recovery among them. This is not completely accurate.

While Office 365 does include some basic data protection features, Microsoft does not assume full responsibility for any organization's data. It only provides a few tools for its customers to protect the data they store in Office 365. To fully protect their data, each organization must assume full responsibility for backing up and recovering any data that it stores in Office 365.

MS Office 365's Baseline Data Protection and Availability Features

Microsoft does provide organizations with basic tools to protect and retain data they store in Office 365. By default, Microsoft Exchange Online retains deleted folders and files for fourteen days in the Recycle Bin. In the cases of deleted emails and mailboxes, it retains them for 30 days.

Organizations may also set and apply policies that manage data deletion and retention based upon specific criteria across their Office 365 deployment. One can set policies to retain documents, emails, and instant messages for a minimum time. Then, once these items satisfy the minimum retention period, organizations may set separate policies to delete them.

Microsoft then hosts Office 365 and all its data in its Azure data centers to ensure their continuous availability. Microsoft places each Azure data center in an Availability Zone (AZ). Each AZ consists of three data centers. Each AZ replicates data stored in a data center to the other two data centers that make up the AZ. Configured this way, organizations can expect about 99.995% average uptime for applications running in a specific AZ.[1]

"Microsoft Office 365's native data protection features possess shortcomings that become the responsibility of organizations to remedy."

Backup Software Remedies Office 365's Shortcomings

Microsoft Azure's hosting of Office 365 provides these high levels of data availability and redundancy that meet or exceed the requirements of most organizations. However, Office 365's native data protection features possess shortcomings that become the responsibility of organizations to remedy. Using third party backup software, organizations may recover from data loss in the following ways:

- ***Recover data from malicious attacks.*** Malware attacks such as ransomware make the news almost weekly. Ransomware makes data inaccessible by encrypting any data it can access. In respect to Office 365, it may encrypt data stored in archives, email folders, file folders, and the Recycle Bin. The more data that it encrypts across these repositories, the more difficult it becomes for organizations to recover their data.

1. https://azure.microsoft.com/en-us/blog/advancing-microsoft-azure-reliability/

Using third party backup software, organizations can protect this data and store it outside of Office 365's domain. They can implement a 3-2-1 backup strategy (three copies of data, two different storage types, and one copy offsite) that shield their data from ransomware. This strategy diminishes or eliminates the possibility that ransomware can affect their data to ensure its availability for recovery.

- ***Recover accidentally or purposely deleted data.*** When individuals delete email messages or files, they can recover them from their Deleted Mailer folder or Recycle Bin. That works if the email messages or files still reside there. However, an individual may periodically empty his or her Deleted Mail folder or Recycle Bin to free up disk space. The organization may have policies set that delete aging email messages or files after a set time. Malware may even purposely empty these folders as part of an attack. Once emptied, Office 365 provides no means to recover this data.

  Third party backup software again addresses this Office 365 shortcoming. If someone or some software accidentally or purposely empties the Deleted Mail folder or Recycle Bin, an organization may still recover the data.

- ***Make data accessible outside of Office 365.*** Microsoft Office 365 offers extremely high levels of availability but that does not mean all the data is constantly accessible. Organizations may lose network connectivity to Office 365 for any number of reasons. During these times, organizations may need to access data stored in Office 365 for multiple reasons. These may include eDiscovery requests and urgent internal or external business demands, among others.

  Backup software gives organizations the flexibility to recover this data at any time regardless of Office 365's availability. Backup software also can lower storage costs by storing data on other storage targets. These may include software-defined deduplication solutions in Azure, local disk storage, other public storage, or even tape.

- ***Help satisfy long-term legal retention compliance requirements.*** Many organizations must retain data for a certain time to comply with various legal requirements. Using Microsoft Office 365, organizations may only apply a data retention policy that applies to all a user's data. Office 365 then stores this data on a single storage type.

  Using third party backup software, organizations obtain more management options for compliance. They gain the flexibility to store data on other storage targets such as Microsoft Azure Blob storage. Using Azure Blob, organizations ensure the immutability of their data.

  They also obtain more granular control over which data they retain and how long they retain it. Using backup software, they only need to retain the data that matches their specific compliance requirements.

"As more enterprises choose Microsoft Office 365, they also need to adopt and implement enterprise backup software to protect it."

Enterprise Backup Software Solidifies Office 365 as an Enterprise Ready App

Organizations continue to adopt Microsoft Office 365 for one big reason: they perceive it as enterprise ready. However, as more enterprises choose Microsoft Office 365, they also need to adopt and implement enterprise backup software to protect it.

Organizations that choose Microsoft Office 365 must also assume responsibility for protecting the data they store there. While Office 365 provides some base line methods for data protection, it does not scale to match enterprise requirements.

Using third party backup software, organizations may protect all data they store in Office 365 at scale. They may backup and store data outside of Microsoft's cloud, increase their accessibility to the data, and recover data anywhere. By implementing enterprise caliber data protection software, they deliver the type of solution that Office 365 needs and their organization requires. ■

CHI CORPORATION
Providing access, protection, and security for your data.

For more information please contact Chi Corporation.

John Thome, President
jthome@chicorporation.com
440-498-2310
ChiCorporation.com

About DCIG

DCIG empowers the IT industry with actionable analysis that equips individuals within organizations to conduct technology assessments. DCIG delivers informed, insightful, third party analysis and commentary on IT technology. DCIG independently develops and licenses access to DCIG Buyer's Guides and the DCIG Competitive Intelligence Platform. It also develops sponsored content in the form of blog entries, executive white papers, podcasts, special reports, webinars, white papers, and videos. More information is available at **www.dcig.com.**