YOTTA SAFE

4 COMMON DATA PROTECTION MYTHS DEBUNKED

4 Common Data Protection Myths Debunked

Hybrid workforce and distributed business have resulted in increased vulnerability of endpoints to cyberattacks exponentially. Imagine a scenario where the valuable data of your employees and clients is on the loose and you have no control. Or a ransom is being sought to release your data, and still, there is no guarantee of the data being released to you even after paying the hefty ransom! Or the system crashes during an important project due to a power failure! Or the endpoint device itself is lost due to a natural disaster! Sounds scary?

According to an IDC report, with today's hybrid workforce, 70% of all breaches still originate on the endpoint. This makes it even more essential for the IT teams to increase their visibility and control of endpoint data remotely.

When we speak of data backup, many of us believe that cloud storage is good enough and can be banked upon in case of a data breach or loss of a device. This belief is unfounded.

Read more to find out as we debunk the top and most common data protection myths.

Is Cloud storage & Cloud endpoint backup the same?

While they sound similar, think of Cloud storage as an additional storage device. If you are low on physical storage or want to share some files with an outsider, you will generally use a Cloud storage service.
Let's dive into the comparison.

Cloud storage

Cloud storage allows you to store files outside of your primary devices. Cloud storage services are good for storing files, photos and videos in one centralised location – the cloud. You can access your files from any device and easily share them with friends and family, allowing easy syncing. Cloud storage refers to tools that let you free up space on your device by having copies of the files saved on the cloud or using it as an extension of your local storage.

Cloud endpoint backup

While Cloud endpoint backup refers to tools that protect your data, files and system from catastrophic events like ransomware or theft by collecting and transmitting data residing on endpoint devices like desktops or laptops, Endpoint backup solutions can protect users' data by automatically and securely backing up data copies offsite to a cloud storage location.

Common myths on Data Protection

Myth 1

Employees/users will perform manual endpoint backups proactively.

- **Cloud storage:** Users must manually upload files (drag & drop) into the cloud storage.
- **Myth Buster 1**: It's observed that only few users back up data proactively. An ideal solution is one which syncs data at regular intervals without hampering the ongoing work of the users.

Yotta Safe: Syncing happens automatically at regular intervals without hampering the user's work.

Myth 2

Cloud Storage offers the best protection for files.

- **Cloud storage:** They use encryption like the 128-bit or 256-bit AES keys to protect files at rest and encrypt data in motion with 128-bit AES SSL/TLS encryption or better. Some providers use 256-bit SSL/TLS encryption in motion to protect files.
- **Myth Buster 2**: Cloud storage providers have a lower level of encryption than Yotta Safe to secure data.

Yotta Safe: Data is encrypted in transit and at rest. It is protected with a 256-bit level AES encryption wherever your data resides. It also supports file-level encryption and has the ability to support external KMS like Gemalto, SafeNet, KeySafe, etc. for complete backup data encryption at the destination.

Myth 3

Files can be recovered once deleted from a Cloud Storage

Cloud storage: It helps in file-sharing with single or multiple users. However, if the file/s are deleted (accidentally or otherwise) by any of the users, it is lost forever and for everyone. No backups are available.

Myth Buster 3: Backups are absent in Cloud storage in the event of deletion of the file.

Yotta Safe: In an inadvertent event of deletion of a file by any user, the last backed up copy can be restored easily by the user.

Myth 4

Users assume backup solutions are costly.

Cloud storage: Prices vary and are based on storage space. They start from approximately. Rs. 9,000 per year for a 2TB storage per user. While others can be cheap, the storage space offered is also low.

Myth Buster 4: Yotta Safe comes at a highly competitive price and offers many added benefits than a cloud storage solution.

Yotta Safe: Most endpoint backup solutions are costlier vis-à-vis cloud storage. Also, they give limited storage space. However, Yotta Safe offers unlimited backup storage at just Rs.1800 per year per user device.

YOTTA SAFE

Secure your endpoint data with Yotta Safe

Yotta Safe, powered by Commvault, offers endpoint backup without worrying about storage limitations and high costs. Relieve your IT Team and protect workforce data wherever they are with this scalable, secure and cost-efficient endpoint backup solution.

Additionally, your data is secured and stored at a failsafe location at Yotta NM1 - Uptime Institute Tier-IV certified data center. It meets the compliance and regulatory requirements of storing data in India. Other features include minimised network usage with source-side deduplication, network throttling, incremental backups with self-service recovery options, device refresh, and an integrated dashboard for easy management.

Schedule a demo today, or contact us for more information.

www.yotta.com