PARABLU

Can you use Microsoft OneDrive for Business to back-up your Endpoints?

I get this question a lot – especially from Microsoft customers who have recently purchased Office 365. Several of them receive up to 1TB of cloud storage per employee, in the form of OneDrive for Business – and they think they've solved their Endpoint Backup problem. There was one CTO who I recently spoke with that said "Isn't the whole point of having a cloud file storage service, that people don't need backup software anymore?".

The answer is a little complicated. So, let's break it down.

Most file storage services (OneDrive for Business included), broadly provide the following things:

1. Storage in the cloud
2. A means to view, upload and download files using a web browser
3. An optional client which allows for an automatic sync of the files into a specific folder on your endpoint computer
4. Features like 'sharing' – which allows you to share a file or set of files with other users.

While file storage services can perform some of the functions a backup requires, they fall short in some critical areas. Importantly:

1. The ability to identify files on your endpoint computer that are eligible for backup (preferably based on a policy you can set), and copy them to the cloud. Not simply in one folder, but across your entire computer.
2. Keep the copy of data in the cloud insulated from actions on the client. For example, deleting a file on the cloud in response to a deletion on the client. Or allowing a file that infected by ransomware to be deleted on the cloud and replaced by its encrypted version. These would defeat the purpose of having a backup in the first place.
3. Ensuring that the data in the cloud is safe from prying eyes, by encrypting it with keys known only to the organization, but not to anybody else.

So, going back to the original question of whether file storage services can still be used for effective endpoint backups – the answer is still YES, if you can do the following:

1. Make sure you're not relying on the sync client that is provided by the file storage service or using a manual / scripted method to upload or copy files to the cloud.

2. Invest in reliable backup software that can utilize the cloud storage as a backup target. Look for software that can minimally do the following:

    i. Allows you to set policies which define what files/folder you'd like to backup across your endpoints. You should be able to specify file and folder paths, select files by extension or MIME type, and also specify what types of files and folders you want to exclude.

    ii. Perform incremental backups – i.e. identify files that have been modified and move only those to the cloud. Or even better, maybe even move only portions of the files that have changed – this could be especially useful for very large files like PSTs that change very little every day.

    iii. Schedule backup operations that can be controlled via policy over several hundred or even several thousand computers.

    iv. Be able to resume a failed backup from the point of failure.

    v. Be able to backup files in use or that are 'locked'.

    vi. Be resource sensitive and use techniques like compression and de-duplication to save network bandwidth and storage space.

    vii. Allows you to manage data retentions by file versions – so you can get back data from a previous day or even a previous week.

3. And of course, make sure that your organization's privacy is protected by ensuring that the data is sent to the cloud after it is encrypted using **your** keys.

Until now, Endpoint backups have tended to be low on the list of priorities for IT organizations. But with recent incidences of high profile data losses, increased regulation and ransomware attacks, they've become unavoidable. A clean backup every day is still the best defense against ransomware.

Endpoint backup strategies through the years have tended to be of the form of “we ask our users to copy their important data to the file server” or more recently “we’re asking users to copy important data to their OneDrive folder”.   But user behavior is hard to change and it is common to find critical files under “My Documents” or some other folders on a user endpoint.

If you haven’t considered a professional approach to endpoint backup, it is time to do so.

What I have listed above is only a small subset of features which are important for good backup software – but these are particularly important when backing up to a cloud target. And of course, make sure that the vendor you pick supports the cloud target of your choice.