Dr.Backup™
online backup service

Cloud Sync Backup Service Description

http://drbackup.net

GUARANTEED 100% Customer Satisfaction GUARANTEED

If for any reason you are not absolutely delighted with the ease-of-use, safety or convenience of our service -- please let us know immediately. We will either fix the issue or refund 100 percent of your monthly service fee.

Backup of mission critical data to a secure offsite server is essential. It protects against virtually all threats that might cause loss of a critical business asset. However, within any organization, not all data is of equal importance. Sometimes, there's a need to economically perform "bulk" backup of images, audio, video, archives and other (static) data not critical to day-to-day operation of the business.

The Cloud Sync Backup Service* is an add-on to the Dr.Backup S.M.A.R.T. Online Backup Service. It provides the mechanism to send secure encrypted backup data to a local drive containing a cloud sync folder – rather than sending data to a secure online storage server. When this add-on is paired with a customer-provided cloud sync offering such as Dropbox® Pro, Microsoft® OneDrive or Google® Drive, the organization can take advantage of the economies of bulk priced public cloud storage without compromising the security content of the data.

In addition to adding security, the Cloud Sync Backup Service also provides for data compression, version control, and customized data retention. The combination of secure online backup, local image backup and cloud sync backup enables organizations to achieve maximum data backup protection at an optimized price point consistent with a customer's risk tolerance.

*Customer must provide and maintain a functioning third party cloud sync service. While the Dr.Backup Cloud Sync Backup Service will transfer encrypted file content to the designated local cloud sync folder, the ultimate transmission of this data offsite is constrained by the operation of the third-party cloud storage service the customer uses.

Service Description	Per Month	Per Month 1-YR Prepaid*
Cloud Sync Backup Service for Microsoft Windows (optional add on) - RBS-CS-001 Allows local cloud sync folder to function as target repository for secure (encrypted) data backup files. *Note:* Mission critical data should always be backed up offsite to a Dr.Backup secure server. Purchase and ongoing maintenance of compatible public cloud sync service is the sole responsibility of the customer. If this service is not operating correctly, encrypted backup data placed in the sync folder may not be transferred offsite. **You must subscribe to a qualifying Dr.Backup online backup service to purchase this add-on.**	**$9.95**	**$8.95**
Additional PC (sub-account) (RBS-ID-001) Add PCs by purchasing additional software licenses. Online backup disk storage 'pool' is shared by all systems in the plan.	**$5.00**	**$4.50**
* Includes a 10% prepaid annual contract discount.		

Frequently Asked Questions

Cloud Sync Backup Service for Microsoft Windows

1. Why do I need a cloud sync backup when I already have online backup?

Online backup provides the ultimate in mission critical data protection. It helps you to avoid loss from threats such as fire, flood, lightning/electrical surges, theft, viruses and more. However, within any organization, not all data is of equal importance. Sometimes, there's a need to economically perform "bulk" offsite backup of images, audio, video, archives and other (static) data not critical to day-to-day operation of the business.

The Dr.Backup Cloud Sync Backup Service permits an organization to use **inexpensive public cloud storage** as a repository for secure file backups. This creates a two-tiered approach to backing up data files which is useful in defeating many physical threats.

Mission critical data should always stored on secure offsite servers maintained and operated by Dr.Backup offering the highest level of protection, reliability, availability, service and support. Less critical data can now optionally be secured in public cloud storage using a file sync service operated by a third party provider. This offers the potential for reduced storage costs as the amount of non-critical data grows.

WARNING: Cloud sync backups may not provide protection from certain viruses or malware (ransomware) due to the security model used in cloud sync products. If your public cloud sync folder is compromised, you may not be able to recover any of the data.

Note: If your public cloud storage is breached, any data placed in this storage by Dr.Backup will be fully secured by a high-level of encryption. This breach therefore may not need to be reported under current HIPAA guidelines if no other data in the sync folder contained patient information.

2. How does the cloud sync backup process actually work?

The Dr.Backup version 11.17 (or higher) backup agent software includes support for the optional Cloud Sync backup feature. There is no additional software required after the service feature is enabled by customer support.

Cloud Sync backups are configured very similar to online file backups. But, instead of selecting the backup destination to be a Dr.Backup secure online storage server, a local "cloud sync" folder is targeted. Files, folders and other data objects are selected, compressed and encrypted before being copied into the local cloud sync folder structure. It is then the responsibility of the customer's local cloud sync provider to transfer this data to public cloud storage as time and bandwidth constraints permit.

3. How much storage do I need for the local cloud sync backups?

Prior to being copied to the cloud sync folder, all data files are compressed and encrypted. In many cases this will make them ~25% smaller than their original size on the local disk. You will therefore need enough local storage (on the local cloud sync volume) to hold all the compressed data backup files – usually about 75% of the size prior to compression. In addition, you **MUST PURCHASE SUFFICIENT PUBLIC CLOUD STORAGE** from your designated provider to serve as an offsite repository for the data.

Notes: Failure to monitor public cloud storage utilization may result in inability of data to be transferred offsite. Payment for public cloud storage is NOT included in your Dr.Backup service fees. You alone are responsible for establishing and maintaining an active public cloud storage account.

4. How often do I need to run a cloud sync backup?

The frequency of data backup will depend on the volatility of data designated as non mission critical. If you are backing up archives that only rarely change, then a weekly cloud sync backup is likely sufficient. However, if you are constantly adding content to your repository of non critical data, than perhaps nightly cloud sync backup runs are more appropriate.

5. Do I still get business-class service and support with the local backup service?

Absolutely. Technical support hours are M-F from 8am to 6pm eastern time. Emergency after-hours data restore assistance is available from an on-call technician.

Dr.Backup technicians will work with you or your local technical contact to install and configure your cloud sync backups – targeting the backup output of non mission critical files to a dedicated subfolder of your cloud sync.

Should a restore from the public cloud be required, you will first need to recover all files from the Dr.Backup cloud subfolder and synchronize them down to a local PC. Once that is completed, the Dr.Backup restore function can be used to decrypt and decompress the data prior to restoring it to a location on your local computer.

Note: We recommend that you **SUPPRESS** synchronization of the dedicated Dr.Backup cloud sync subfolder to all devices participating in the cloud sync network unless you intend for a specific device to function as a hot-standby from which a recovery operation could be immediately initiated.