PREVENT DATA LOSS WITH REMOTE ONLINE BACKUP SERVICE

Prevent Data Loss with Remote Online Backup Service

The U.S. National Archives & Records Administration states that 50 percent of businesses that lose their critical data for 10 days or more end up filing for bankruptcy. Since one out of ten hard drives fails each year, and hard copies of data can be just as susceptible to damage as the original, having your company's important files stored with an off-site data backup service is simply good business sense.

In the event of a disaster, whether due to human error, theft, fire, defective components, or a system crash, having a remote online backup of all of your important information ensures that it is always safe, secure and easily accessible.

Remote online backup services have become more affordable and service providers are abundant. Many online backup vendors offer similar functionality but there are a number of variables, which can make selecting the right provider for your company a challenging task. This guide is designed to assist decision makers in determining the best remote backup solution for their company's needs.

What Are the Benefits Remote Online Backup?

There are two types of data backup systems; online and offline. An offline backup, or "cold" backup, is taken while the database is shut down. It includes all database files, a copy of the current control file and all online re-do log files. Online backup, known as a "hot" backup, is taken while the database is operating. It includes copies of all database files, a backup of the current control file and all re-do log files written during the period of the backup from the online archives. An online backup does not include online re-do log files.

Although remote online backup requires a fast Internet connection, this is usually not a problem since broadband access is common, especially among business users. Most likely, your connection will be fast enough to accommodate the traffic between your computer and the online backup server.

There are several advantages to remote online backup, including:

1. Your files will remain available and can be accessed remotely from any location with an Internet connection. Files stored locally, as on a hard drive, are not accessible remotely.
2. Remote online backup providers adhere to rigorous practices that virtually eliminate the possibility of your data being completely destroyed due to a disaster.
3. Your backups will be physically safe. Remote online backup protects your hardware and software against theft, failure, and natural disaster whereas backups kept on a hard drive, CD or DVD are still vulnerable to such occurrences.

4. Remote online backup services include such security measures as traffic encryption, password protection for stored files and secure file sharing.
5. Many remote online backup vendors offer real-time backup protection at no extra cost, a service that most businesses will want to take advantage of.
6. For many businesses, remote online backup can be much more cost-effective than the offline alternative.

Remote online backup systems are usually built around a client software program that collects your data then compresses it, encrypts it and transfers it to a server. Typically, this process is carried out on a daily basis. You will retain the ability to restore your data via the Internet or by purchasing a CD or USB drive containing all the data you have stored on the backup provider's server.

With a remote backup of all your important information, you can be assured that your information is safe and easily retrievable even in the event of a system crash, theft, natural disaster or user error.

How to Choose a Remote Online Backup Provider

With dozens of companies offering online backup service, how do you go about choosing the best provider? What are some common issues you will need to consider? And in what ways do the services of various providers differ? To begin your search, TechRepublic recommends looking for the following key features.

1. Reliable software

Make sure that the backup software works well with your operating system (OS). Some offsite backup services run best on Windows Vista, while others perform better on Windows XP, for example. The only way to be sure is to test a service’s application. Take advantage of the free trial offered by many companies in order to perform this test.

2. Storage plans that meet your needs

Some offsite backup services bill by the gigabyte. Others will charge a flat fee for an account containing a specific storage limit, such as 100MB, or 10GB. Such a plan can simplify budgeting for companies that do not anticipate exceeding these limits.
Look for a provider that offers a plan that is within your budget and flexible enough to meet your company’s needs.

3. Detailed reporting tools

A chief advantage of automated backup services is the knowledge that your critical data is being automatically backed up offsite. With vital data thus vigilantly protected, you can progress to tackling other responsibilities. Be sure you will have access to file-level reporting, including a daily list of every file that's backed up. Reporting tools should list file sizes, time of transfer, and error details.

4. A usable backup application

The backup application should be user-friendly and as infallible as possible. Make use of any trial period offered to work directly with the software. Verify that the service's backup application and interface are straightforward enough to avoid bewilderment but adaptable enough to meet your company's needs.

5. Simple recovery

When hard disks fail, system errors occur, IT professionals need the ability to recover files quickly. Test each backup provider's recovery capabilities to ensure that file recovery, if needed, will be simple, quick and secure. Also, make sure that unauthorized parties will be unable to perform this function.

6. Secure file transfer

Do not work with a provider who offers less than 128-bit AES encryption and SSL security. If you require the utmost in privacy and security you might opt for a much stronger encryption, such as the 448-bit encryption offered by some providers.

Whichever you choose, your data must remain secure once it reaches the destination server, which means the provider should have appropriate policies in place to ensure that employees cannot access client data unless authorized to do so. Be sure to protect account information (along with recovery hashes or passwords) vigilantly and change access information often.

7. Free trials

The best way to establish whether an offsite backup provider will be the right one for your company is to take advantage of the free trial period. Use this time to test the backup software application, support procedures, and reporting tools, and conduct a test recovery as well.Testing online backup tools on systems with similar configurations to those running in production environments will help eliminate any surprises and make you aware of potential incompatibilities.

8. Version tracking

Quite a few backup providers support the ability to retain multiple file versions. This can be a very useful feature if you ever need to refer to previous file versions. The typical daily backup schedule leaves little time to catch errors before each file is written over. Versioning file systems give you a means to review file history if the need should occur.

9. E-mail alerts

Some offsite backup providers will send you email alerts to make you aware when backups are failing or other concerns present themselves. This will ensure that your IT staff is aware of all backup operations and can deal with any problems as they arise.

Six Important Aspects to Consider When Making Your Selection

Security

Security should be a primary consideration when choosing a remote online backup provider. To ensure the safety of your company's data you will want to make certain the vendor you select provides substantial encryption and password protection for their clients.

This ensures that the only people who can access your company's stored data are those authorized by you, and to whom you have given the password. With proper encryption and password protection, even your backup service provider will not be able to access your information.

Support

Ensure that your backup service provider's tech support team will be available when you need them most. Many backup providers offer 24/7 support. Be certain you'll have access to support staff if you ever need troubleshooting assistance during off hours.

The best companies will offer 24/7 support via both telephone and email, and will gladly tell you how long it typically takes their support team to respond to requests. This should be true not only for their technical support, but also for general customer support and service.

Space Requirements

You should carefully consider how much space will be required to store your company's data. Find out whether the vendor will be able to support all the files that you need to have backed up. You don't want to sign up with a provider only to find that you have to choose which files to back up and which ones will be left vulnerable.

It’s important to note that the initial backup will require the most time and bandwidth since all the files you've selected for backup must be delivered to your service provider. If you need to prepare multiple computers for online backup, be sure to stagger the first few backups to prevent overburdening your Internet connection.

Archiving Period

It is vital that you know how long your data will be kept on the company’s servers if your account has not been accessed for a certain amount of time. Most companies do delete data after a designated period of account inactivity. If you anticipate a need for extended storage, find out if the provider will accommodate your needs, and what additional fees they might charge. You want to be sure that you can readily access your archived files from any computer whenever you wish.

Speed, Reliability and Up-time

These are three key factors to look at before making your final selection. Since backups are usually the only option for recovering data after a system failure or disaster, remote online backup services do not have a great margin for error. The data stored with them must be there when needed. Find out what steps the provider has taken to secure their clients’ data. Feel free to ask such questions as:

1. Does the center have a continuous, un-interruptible power supply, including a back-up generator in a secure location?
2. What is the up-time for the data center?
3. How many clicks are required to actually begin the online backup process?
4. When the backup is running, many disk resources or CPU does it consume?
5. Is the backup continuous?
6. How quickly can files be restored?

Pricing

The price you will pay for remote online backup service will naturally be one of your prime considerations. Many remote online backup providers offer unlimited storage for a very affordable price, either on a monthly or yearly basis. Some provide enough free storage to accommodate the needs of most smaller businesses.

Since pricing and features can vary greatly, it’s important to assess your needs before you begin the process of selecting a vendor. Your own company’s needs should be the determining factor when comparing prices. Remote online backup services designed for small businesses are very different from those intended for larger enterprises. For example, do you simply require a scheduled data backup at the lowest possible price or are you willing to pay more for real-time backup of email and database applications?

A lower priced service with basic features such as web access, scheduled backup and the ability to share files or send files by CD/DVD may be adequate for the needs of a smaller company. A larger business will require more complex features such as historical backup, live database, tighter encryption and the ability to back up operating system files.

Some key pricing details to ascertain from the company include:

1. Do they charge per computer or per account?
2. Is there a free trial period available?
3. What are their set-up fees, if any?
4. Will telephone technical support cost extra?
5. How much does the provider charge per GB per month?
6. Will I be charged if I exceed the allowable traffic and storage quota?
7. How frequently and what amount of data backup is allowed daily or monthly?
8. Can I cancel at any time or am I obligated for a minimum period?

Be sure to compare the services of a few different companies before settling on any one remote online backup provider. It will be worth your time to find a company that has the best reputation, price and storage space. InsideUp's online vendor comparison service can make your search much easier. Simply take a few minutes to tell us about your company's needs and you will receive custom quotes from up to five top remote online backup providers.

Glossary

Backup policy

The procedures and rules you currently use for ensuring adequate data backups are made. This includes the technology and methodology used and the process by which you restore system information from your backup copies.

Backup software

The software applications installed on computers that initiate a backup process. Usually described as the user interface (UI) that allows the person to control the backup procedure remotely.

Backup window

The time period required to complete a backup procedure. Normally, a backup procedure uses system resources that have detrimental effects on system and network performance. Backup windows can be managed to ensure business productivity is minimally affected.

Bandwidth resources
The amount of bandwidth available to facilitate an online backup process. Actual bandwidth needed depends on amount of data being protected, average daily change rate and determined Internet restore time objectives.

Bandwidth usage
Some solutions allow users to adjust how much bandwidth is used during a backup. This can be useful for different times of the day: more bandwidth for quieter times (such as in the evening) and less bandwidth during busy periods.

Block level backup
A backup that only contains the changes to files at a sub-file or block level. Block are smaller than files and therefore reduce the amount of change that needs to be sent to the vaults, but may require longer processing times to identify the changes.

Byte level backup
A backup that only contains the changed bytes of data. Bytes are smaller than blocks and therefore provide the smallest amount of change that can be sent to the vaults, but may require longer processing times to identify the changes.

Cache
A local store of recent backups left on site for fast access. A local cache avoids having to wait for bulk restores to be recovered over the Internet from the vaults.

CDP
Continual Data Protection, where the backup system logs every change to the host system in systematic intervals. This is generally enabled by saving byte or block-level differences rather than file-level differences.

Continual Data Protection
A process through which the backup system logs every change to the host system in systematic intervals. This is generally enabled by saving byte or block-level differences rather than file-level differences.

Data compression
In order to minimize the amount of bandwidth used during a backup, the data is compressed using what is known as a lossless compression algorithm. Essentially, data is packed into a smaller file size.

Data encryption
The process of encrypting data for restricted viewing. Only the person with the encryption key can decode the data and view it.

Disk to Disk
A backup that transfers data from the disks on the computers to disks in the vaults - as opposed to send the data to tapes. This method provides for rapid recovery, especially to older archives of data.

Delta backup
As differential backup, a backup that only contains the files that have changed since the most recent backup (either full or incremental). The advantage of this is quicker backup times, as only changed files need to be saved.

Differential backup
A cumulative backup of all changes made since the last full backup. The result is quicker recovery time, requiring only a full backup and the latest differential backup to restore the system.

Disaster recovery
Otherwise referred to as DR, its the process of recovering business operations after a disaster and restoring or recreating data. It is in any company's best interest to minimize its DR period.

Email Security
Anti-virus, spam and phishing service. Removes all emails containing malicious content before they reach the user's email server.

End-to-end encryption
Ideally, data should be encrypted before it leaves the source machine by a client generated key and stored, in an encrypted form at its destination.

Full backup
A backup of all (selected) files on any given system.

Full Disk Encryption
A method of encrypting data on a hard disk at a level below the operating system. Such a method does not rely on the operating system to manage the encryption and the disk cannot therefore be read if the disk is transferred to a new machine.

Hardware as a Service
HaaS - the provision of computer hardware on a pay-as-you-go basis - either in the 'Cloud' or on premise.

Hot backup
A backup of a database that is still running so that changes may be made to the data while it is being backed up. Some database engines keep a record of all entries changed, including the complete new value. This can be used to resolve changes made during the backup.

Incremental backup
A backup that only contains the files that have changed since the most recent backup (either full or incremental). The advantage of this is quicker backup times, as only changed files need to be saved.

Initial Backup
The first or seed backup of a set of data, usually directly to a data centre or vault. A seed backup can be done online over the Internet or using a media device such as a secure hard disk with encryption.

Latency
This is a measurement of the total time taken for data to be encoded and transferred between communicating devices. Poor latency causes lag, and is often responsible for transfer speeds that seem to fall short of advertised bandwidth figures.

Media spanning
The process of backing up data to multiple storage sites or mediums. This is normally conducted when there is a significant amount of data that needs protection.

Multi-platform
This term refers to software that works on both Macintosh and PC Operating System platforms. Some online backup software is capable of working on a variety of OS, while others will be specialized.

Multiplexing
A method of combining multiple backup data streams into a single stream that can be written to a single storage device.

Near store
Backing up data to a local staging backup device like a tape or hard drive. Typically located on-site for later archival restore.

Network backup
Many companies operate on a Network. The ability to back up multiple computers, servers or Network Attached Storage Appliances on the network from a centralized device is made available via this feature.

Off-site vault
Facility where data is stored away from normal place of operations. In professional online backup services, this is a sophisticated, disaster hardened, temperature controlled, high security bunker.

Online access to files
Online access allows you to access your backed up files via a normal web browser, usually through a secure web portal. This is useful if you are not at the physical machine.

Online backup
The backup of data and systems over the Internet to specialist storage vaults - as opposed to local backups to tape.

Open file backup
The ability to back up a file while it is in use. This is made possible by taking snapshot views of files even while they are open.

Recovery point objective (RPO)
The point in time that a restored data backup will represent. This is normally the point any system will be restored to upon recovery. The ultimate RPO is the point just prior to data loss. Optimization of RPO involves increasing the frequency of synchronization between source data and backup storage device.

Recovery time objective (RTO)
The amount of time elapsed between data loss event and restoration of full business activity. This relates to not only the time taken to retrieve files and systems but how long it takes to reinstate them and maintain normal business activity.

Remote backup
As online backup - the backup of data and systems over the Internet to specialist data centers

Remote store
Backing up data to an off-site backup facility, either directly from the live data source or from an intermediate near store device.

Reporting
Notifies the user on the efficiency of the backup process. Can be customized by the user to determine the frequency of updates.

Restore time
The amount of time it takes to restore data that has been backed up. This time varies depending on the amount of data being brought back.

Retention time
The length of time in which currently protected of data will remain available for restore.

SaaS
Software as a Service - the provision of standard software solutions provided over the Internet to customers on a pay-as-you-go, flat-fee basis.

Software as a Service
SaaS
The provision of standard software solutions provided over the Internet to customers on a pay-as-you-go, flat-fee basis.

Scheduling
The frequency with which backups of files and systems take place. Online backup allows full automation of scheduling removing the human element of this process.

Seeding
A term used to describe the process of uploading data to the data centre. Often this term is used with reference to the initial seeding of data, which can often be performed by uploading data onto a device and ‘seeding’ it directly to the storage vaults.

Site-to-site backup
Backing up data over the Internet to an off-site location under the user's control. Similar to remote backup except that the owner of the data maintains control of the storage location.

Snapshot
An instantaneous picture of a file system taken to preserve a ‘point in time’ static, read only view of the file system.

Synchronization
The process of ensuring that two or more locations contain the same up-to-date files. In online backup, initial synchronization is a one-time event to get the initial replica of a file under protection.

Tiered data centers
The tier of a data centre refers to how secure and reliable it is and ranges from the most basic at tier one with a 99.671% availability, to the most advanced tier four with 99.995% availability.

Transfer encryption
In order to prevent the interception of data between source and storage, data should be encrypted, normally via Secure Socket Layer (SSL) Encryption.

Versioning
Refers to how many versions of data are kept and is given as a number. How far back you can look will depend on how frequently data is changed.

Virtualization
The creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device or network resources.