What is Cloud Backup?

Cloud backup is a method of backing up your data into a storage facility held in the cloud.



Cloud computing is defined in detail [here](http://www.managedserviceexpert.com/blog/2012/05/22/11-what-is-cloud-computing-how-does-cloud-computing-work). A working definition is that cloud computing results in software, information and shared resources being delivered over a network, usually the Internet to computers and devices such as smartphones, dumb terminals etc. as a quantified utility, comparable to the way electricity is delivered over the grid. This is a loose term covering a number of technologies which together result in the delivery of computing as a metered service rather than a finite product.

Backup should be a key constituent of an organisation’s Disaster Recovery Plan; if you need to know what this is and why you need one there are ideas on this [here](http://www.managedserviceexpert.com/blog/2012/05/23/19-making-a-disaster-recovery-plan).

The data that needs to be backed up is, at the very least, the organisation’s critical data which should be held offsite, well separated from the main site so as to survive any disaster that overtakes the main site. In this way, a good plan will include backup to a data centre which is separated from the main site by 10’s of miles, meaning fire or flood does not destroy the backup as well as the main data.

This can be achieved in a number of ways which include providing your own equipment in racks rented in a chosen suitable data centre. However here we focus on managed backup services, also known as cloud backup which we define as a service providing users with a system for backup and storage of computer files.

Such online backup systems are typically built around a software program deployed on a per client basis, running to a schedule, normally once a day, and usually at night while users are idle. This program collects, compresses, encrypts, then transfers the data to service provider's servers or off-site hardware.

There are many of these service products available, which target specific market segments with a variety of feature sets, service levels, types of encryption etc.

In an industry as young as IT, we need be careful when using the term “traditionally” but to date backup has been provided using tape. However, as bandwidth and disk storage capacity have increased and the internet has gained in acceptance so disk to disk storage across the web has been adopted now traversing most sectors with a large number of vendors emerging with products built to suit requirements. Early years were spent capturing market share with most providers of online backup services now positioning their services using the SaaS (software as a service) model. The relevance of these is predicted to increase exponentially in the next few years as personal and enterprise data storage needs rise.



# What Should The Service Deliver?

## Critical Features:

* Backed up data must be recoverable whenever required.
* Recoverability is vital so integrity validation is required.
* Services must be flexible enough to fit with requirements imposed by clients and their applications.
* Back end storage management must be transparent to the client!
* Interface provided so allowing clients to select the data they wish to protect/recover, retention times, destruction dates and scheduling etc.
* Cloud backup does not need data to be copied using a specific appliance from collection point prior to transmission to and storage in the service provider's data centre.
* Ubiquitous access.
* Cloud backup must use standard networking protocols to transfer data between the customer and the service provider.
* Service providers’ storage facilities must be available 24x7x366 guaranteeing data restore to any location connected to the service provider’s cloud via the client’s chosen network.
* Storage capacity must be elastic and scalable ensuring customers’ data is allocated on demand and without limit then re-allocated as customers delete backup sets as they age. Service provider allocates storage capacity to a customer, when the customer deletes data or no longer needs that capacity, the service automatically releases and reallocates that capacity to a different customer.
* Cloud backup is a metered by use service.
* Cloud backup is bought and sold on a per-gigabyte per month basis, prices are based on age of data, type of data (email, databases, files etc.), number of backup copies, volume and recovery time objective. This enables clients to align the value of data with the cost of protecting it.
* Cloud backup service is shared and secure.
* Cloud backup service utilises a full stack native cloud multitenant platform (shared everything).
* Provider lock-in should be prevented and data mobility/portability guaranteed ensuring clients can move their data from one service provider to another and/or move entirely into a dedicated private cloud/hybrid cloud.
* Security in the cloud is critical and cloud backup services are no exception. Thus, one client should never have access to another’s data and service providers must not be able to access client data without the client’s permission.



# Cost factors

Online backup services are typically priced based on:

1. Total amount of data.

2. Number of machines.

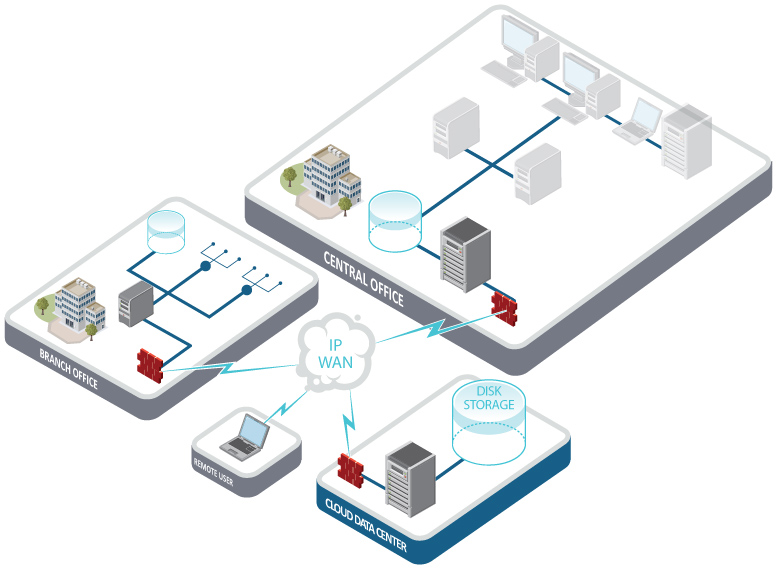
3. The number of versions of each file kept.

4. Data retention and archiving period options.

5. Managed vs. unmanaged backups.

6. Service levels and features.

# Enterprise-class Cloud Backup



An enterprise-class cloud backup solution will include an on-premise cache, to ameliorate the effects of any inconsistent Internet connectivity.

Hybrid cloud backup is a backup approach combining local backup for fast backup and restore, plus off-site backup to mitigate against local disasters. This hybrid cloud backup works by storing data to local disk for the high speed backup, followed by disk to disk to cloud appliance with the backup software encrypting ten transmitting data to a service provider. In this way recent backups are retained locally, so speeding data recovery operations.

## Features

### Continuous backup/continuous data protection

These are 2 methods allowing a service to back up continuously or on a predefined schedule. Most backup services are scheduled with backups performed at predetermined times alternatively other services provide continuous data backups which are typically used by large online retailers and large financial institutions. However such systems typically have a trade-off with performance and system resources.

#### File-by-file restore

Under this system users restore files identified by them by name and/or folder themselves, without the intervention from the service provider. Services vary and some may feature search files by searching for filenames and folder names, by dates, by file type, by backup set, and by tags.

#### Online access to files

This is rarely offered but some services allow the user access to backed-up files via a web browser.

### Encryption

Again all data must be encrypted prior to being sent across the internet and then stored in its encrypted state. Encryption level must be at least 256 bits, with the user having the option of using their own encryption key, which should never be sent to the server.

### Network backup

Supporting network backup enables a cloud backup service that provides for multiple computers, servers or network attached storage appliances on a LAN (local area network) to be backed up from a single computer or device.

### Data compression

Self-evidently data is compressed with a lossless algorithm to minimize bandwidth used.

### Differential data compression

Again to minimize network traffic this method allows for the transfer only of the binary data that has changed from one day to the next. This is a feature some of the more advanced online backup services that use this method rather than transfer entire files.

### Bandwidth usage

Again it may be advantageous to use bandwidth at certain times of the day and some services include a user-selectable option to allow this.

### Off-Line Backup

Under this type of service a part of the backup is taken to a local device (tape drive/disk/disk array/another server) when the network connection is down or otherwise being used and once the network connection is available, the remote backup software updates the datacentre with the changes from the off-line backup media.

### Synchronization

Optional on a number of services is data synchronization which allows users to keep a consistent library of all their files across many machines so augmenting productivity by increasing access to data.

# Features for business users



Business users must review their connectivity arrangements as some home broadband connections impose restrictions on data upload.

## Bulk restore

Using a portable storage device to restore data when a full restore over the Internet would take too long; a technique once known as “sneakerware”.

### Centralized management console

IT department/staff member use this feature to monitor backups for the user.

### File retention policies

Clients needs vary across their business and so need to create flexible file retention policies applied to an unlimited number of groups of files called "sets".

# Fully managed services



These are intrinsically higher levels of support which command commensurately higher price tags. As ever, levels of support vary from provider to provider with some delivering things such as immediate assistance, proactive monitoring, personal visits, telephone support etc.

### Redundancy

Under this type of service, multiple copies of data are backed up to different locations, usually achieved with two or more mirrored data centres and/or keeping a copy locally of the latest version of backed up data on site with the business.

### Seed loading

This is analogous to “sneakerware” as above where the first large backup is delivered on a portable storage device rather than over the web

### Server backup

These are services specifically designed to backup servers running special databases such as groupware, SQL, and directory services.

### Versioning

Under this type of service, multiple past versions of files are kept to facilitate for rollback to or restoration from a specific point in time.

### Regulatory compliance

Government and industry bodies require that some organisations must comply with regulations relating to privacy, disclosure, legal discovery etc. Service providers differentiate themselves by delivering an understanding of and proper compliance with these laws.



# Advantages of cloud backup over traditional methods:

* Backups are stored in a different location from the original data where traditional backup requires manually taking the backup media offsite.
* User intervention is not required; the user does not have to change tapes, label CDs or other manual steps.
* Unlimited data retention.
* Automatic backups to a specified routine.
* Backup services may offer the option to work continuously, so files are backed up files as changed.
* Backup services may offer the option to maintain a list of versions of your files.
* Backup services typically use a 128 - 448 bit encryption to send data over unsecured links (the internet)
* Some backup services are able to reduce backup by only transmitting changed binary data bits

# Disadvantages of cloud backup over traditional methods:

* Restoration of data can be slow; speed is contingent on available network bandwidth. Said data can be recovered using either the Internet or shipped on a disk from the service provider.
* Some backup service providers may not guarantee stored data will be kept private from for example, employees. Consequently most recommend files are encrypted.
* The service provider could go out of business or be purchased, which may affect the accessibility of one's data and/or the cost to continue using the service.
* Should the encryption password be lost, data recovery will be impossible. Using managed services should mean this is not be a problem.

# Managed vs. unmanaged

Some services provide backup management services expertise as part of their offering which may include:

* Assistance with the initial backup
* Continuous monitoring of the backup processes on the client machines to ensuring backups succeed.
* Proactive alerting should backups fail
* Assistance restoring and recovering data