Introduction.

Over the past 10 years, digital content has grown exponentially. Not only that, but the reliance organisations place on crucial electronic data has grown commensurately with the volume growth, and the incidence of data loss through technology failures, human error, human threat and natural disaster has also grown apace.

These three trends have thrown the issues of backing up and restoring data into stark relief, and whilst it is undoubtedly true that the costs of the hardware to support this have plummeted, the costs of the manpower to carry out the processes and manage the backup media have continued to soar alarmingly for organisations. However, even making these investments does not then guarantee secure outcomes (for example, a recent Gartner Group survey discovered that 71% attempts at restoring data from tape failed), but engaging with a trusted and secure data backup service company will provide a higher level of security for the storage of a mission-critical and regulatory compliant data, and straightforward restoration in the event of disaster striking.

Established since 1999, Datacenta is a professional hosting company, with two geographically –disperse hosting facilities in the UK providing a resilient and robust environment for all our services. Our data centres are fully-protected against intrusion and environmental disasters 24 x 7, offering safeguarding of your data both physically and legally, since as a UK Office of Government Commerce-approved Catalist Hosting Supplier, we abide by all the Council of Europe provisions for data protection and trans-border data flows.

The company holds BS7799 Information Security accreditation alongside ISO9001 Quality Management and ISO14001 environmental management systems.

Summary of Functionality.

Datacenta's Assured Restore On-Line Remote Backup service offers a number of features critical to a successful remote backup service, summarised below for a more detailed description of the functionality of the product set underlying our service, see https://www4.crashplan.com/business/learn.html):

1.1 Minimal infrastructure overhead

The service employs a compact item of client software loaded onto any machine that is to be backed up, which monitors that machine and sends your data over the Internet to our secure data centres - no further human intervention is required once the service has been configured (see Simple Service Configuration below), and multiple destinations may be specified as required (see Multiple Locations, below).

1.2 Secure handling and storage

By default, all data is encrypted on your machines before transmission to ours, using highly secure techniques (Blowfish with 448-bit keys). Not only can your data not be decrypted in transit, but Datacenta's staff are similarly unable to view your data in clear when at rest on our servers. However, encryption may be turned off if you wish.

1.3 Continuous data protection

Unlike some other services, which may schedule backups to start at certain times of the day or week, Datacenta's backup service may be always-on (although you may choose to prevent or throttle activity at undesirable times). Whenever a file has been updated, it is immediately made available for backup, captured with a new version number on our servers. (By virtue of Continuous Data Protection, it is undesirable to attempt directly to back up an open database. Therefore you are recommended periodically to dump open databases to a chosen location in your setup, using the database product's native tools, and we back up from there.)

1.4 Data compression

You choose whether to have data compressed or not. Data being transmitted to remote locations is automatically compressed.

1.5 Differential data transmission

A key aspect of our service is that only the bytes in a file that have changed are transmitted (in encrypted form). This aspect makes for both speedy and efficient transmission while keeping your storage requirements on our servers to a minimum, alongside de-duplication capabilities.

1.6 De-duplication

In the event that you have multiple copies of the same file on your machine(s), we store only one copy, with pointers to it from the duplicated files (a copy is detected in advance by our client software, based on recognising the identical nature of content rather than any considerations of file name or directory residence). This capability further minimises disk storage requirements.

1.7 Multiple platforms

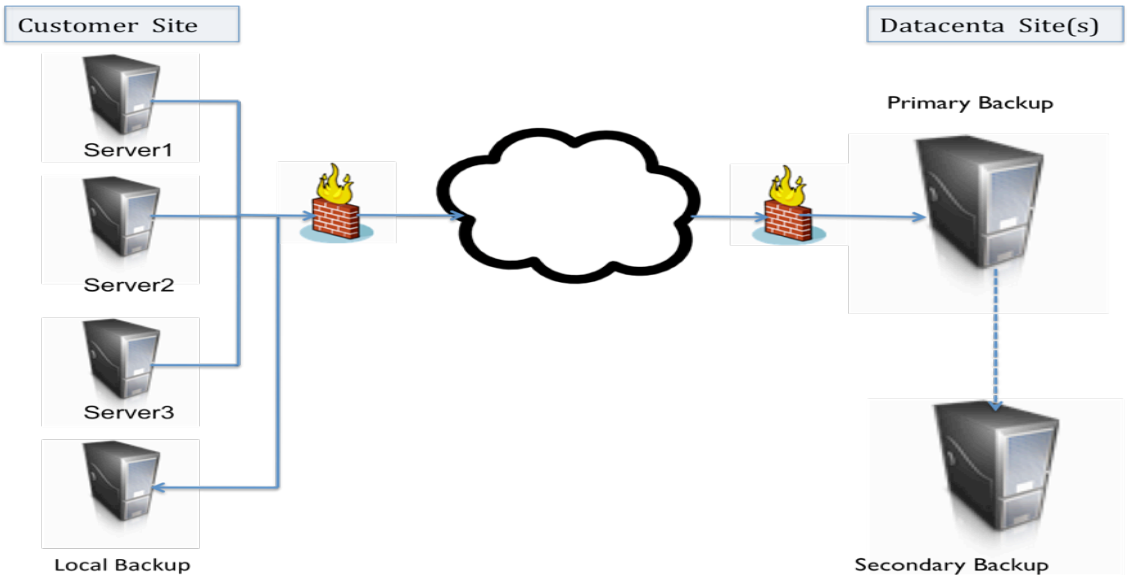
Our service can back up data stored on any of Windows, OSX, Linux, Solaris or VMWare platforms. We can handle any mix of these in the event that you wish to disaster-assure multiple machines and/or multiple sites.

1.8 Multiple locations

You may wish to employ our service to back your data up to both our remote data centre and also to a location in your local area, providing a facility for either rapid local restoration where circumstances permit (e.g. one disk has crashed but others are fine), or from our remote location when such local versions of files cannot be utilised or trusted. Datacenta's service may be configured to operate this way as a standard feature of all Service Plans (see the section of that name, below) at no additional cost. However, where an existing local backup capability is already in operation or is already otherwise planned, the remote backup service may be all that is required.

Finally, as an optional add-on, we can replicate your backed-up data to our secondary, remote data centre, providing the ultimate in redundant backup.

The following diagram illustrates an implementation comprising both local and remote backup:



1.9 Restoration of files

Files backed up are available online as soon as the backup has taken place, 24x 7, and are eligible for restoration either from the local backup or across the network via any normal web browser, depending upon the circumstances leading to the need for restoration (our engineers are available for consultation as to the best approach, where a managed service has been contracted for). You may restore a single file or a group of files in this manner, entirely at your discretion. However, where this is not possible (e.g. Internet access is impaired or out of commission), we are happy to copy selected files to appropriate media (specified by you) and despatch them to you, at a small additional cost per event. Our engineers are located in the very building that houses our primary data centre, to ensure the speediest response to restoration needs.

1.10 Built-in integrity

You are not buying a solution to provide backup – you are buying a solution to provide a capability of restoration. Automatic integrity checks built into our solution ensure backup data is always correct and ready when you need it, and in the unlikely event that data integrity issues are discovered they are automatically corrected via archive self-healing techniques. This process is completely transparent. It is however monitored by our engineers in the data centre, where you have contracted for a managed service (see below) and reported upon.

1.11 Simple service configuration

To set up the service from scratch is simplicity itself. Following order acceptance, the process is as follows:
We send you an email containing a URL from which to download the client to be installed on the machine(s) for which backup is contracted, a licence key, the URL of the server which will host your backups, Instructions regarding choice and deployment of username and password

You log into the download server, and follow the simple instructions therein to download and install the client, thereby creating an account (you will need to specify an email address and password)
You enter the license key provided; along with the name of the backup host server we supplied you above
Using the facilities of the User Interface that opens up, you can specify which files you wish to back up (there are a range of options: by folder, by file type, by wild-card file names et al), or you can simply elect to adopt the default, which backs up whole user accounts.

You specify any constraints you wish to apply regarding the amount of CPU used by the backup process (as a variable %), the extent of the available bandwidth you wish to allow (again as a %), times when backup is/is not to be running, how soon after saving it a file is to be backed up, how frequently data is to be integrity-checked, and for how long backups of deleted files are to be retained. Thereafter, the backup process simply runs according to these parameters without further human intervention, until you decide to change a parameter or wish to restore a file from backup.

The Managed Service

Self-Managed Service

The functional aspects of the are firmly state of the art, and for some, engaging with us to provide a remote, disaster-assured facility purely to host backups with automated weekly emailed reports, and event alerting of failures, fulfils a need. For such customers, we offer our Self-Managed Service. However, for many organizations, the overhead of managing backup and restore processes, managing media, handling alerts etc. is just not a realistic, affordable option in terms of manpower and cost. For such organisations, we offer range of Managed Backup services, at two levels:

Assisted Backup

In this variant, we provide assistance with your initial setup (e.g. how to configure local backup alongside remote, how to configure times when backup is not to run, etc.) and a monthly management report about when backups occurred, how much data was backed up, total storage currently in use and how many versions there are of each file on the server i.e. we relieve you of the burden of interpreting the weekly automated reporting and event alerting that is a feature of the Self-Managed service. In addition, if a scheduled backup fails to take place for whatever reason, we will take the appropriate action to rectify the situation in concert with your nominated representative.

Entrusted Backup

This service includes all the functions of the Assisted service, but additionally we work with you to develop a comprehensive plan for enterprise backup and restoration that reflects the particular imperatives of your business and IT environment, above and beyond just the restoration of data. This is reviewed with you annually. Thereafter, our engineers are actively and constantly monitoring your implementation. We telephone a named contact as soon as any irregularity is detected, and working with your own staff we participate in the processes of investigation and detection (remotely), for the providing advice and guidance on actions to be taken. Using our skills, and applying the potentially complex regime identified in your customised plan, restoration and recovery becomes a swifter and more certain process.

In both variants of the Managed Backup service, and at periods as defined below under Service Plans, we conduct with you a formal Service Review covering the period in question and examining all Incidents, Problems, Service Requests, Change Requests and any other related topics as are mutually agreed upon.

Plans for the Managed Services

All the standard functionality described above applies to all 3 plans, but with differential service levels as follows:

Component	Self-Managed	Assisted	Entrusted
Support Mode [Note 1] (all Incidents are logged and progressed via our Incident Management system, irrespective of mode)	Email	Email, Instant Messaging and/or telephone 0800-1800 Mon-Fri.	Email, Instant Messaging and/or telephone 0800-1800 Mon-Fri. [Note2]
Billing period	Monthly	Monthly or Quarterly as desired	Quarterly or Annually as desired
Service Review frequency	N/A	Annually	Quarterly
Backup/Restoration Plan creation and review	No	No	Annual
Active monitoring	N/A	N/A	Yes

Support Procedures

Datacenta's support is based on the principle that your communication will be dealt with by an Engineer, not a Call Centre Agent (we don't have them). Whether your chosen plan is based on email or telephone, contact with our Customer Support will require you to provide a summary of the Incident or Request as appropriate. The Engineer then captures the request in a return e-mail outlining the agreed scope, which is registered in our Incident Management system. Meeting the requirements specified in the email then forms the basis for later agreement that the case is closed. Of course, if you have contracted for Extended Managed Backup, it is Datacenta that will have detected the Incident, logged it and will already be working on the resolution as we contact you.

Resolution time for cases will vary depending on a number of factors, including but not limited to, complexity of the case, availability of customer data for analysis, availability of customer contacts etc. Service requests will be delivered during business hours 5 business days per week.

1. Support requests via email will be acknowledged and responded to within 8 working hours of receipt, and logged in our Incident Management system.

2. Customers of our Extended Service may also contact us outside of working hours, 24 x 7 x 52, but no commitment is provided that you will reach a Support Engineer directly. If this should be the case, an Engineer will call back within 2 hours.

3. The committed storage space is the accumulated space of all versions of files held. The differential data transmission feature makes for quite small increases in storage for each version, and you can configure the number of versions we hold for you.

4. As described under "Multiple Locations", we operate a secondary data centre some 20+ miles distant from the primary site and for an additional sum per month, we can replicate the backups to this second site, providing a 3-tiered backup of your data if so required

5. One-off add-ons will be billed at the end of the month in which the add-on service was delivered.

6. Initial Setup. Depending upon the volume of data to be loaded and the nature of your Internet connection, loading your initial data over the Internet could be a very lengthy process, and it may be preferable to conduct the initial load to a local additional server, to transfer the backed-up, encrypted files to portable media and to have them sent to us for loading. This process, often called "seeded backup", is configured and managed remotely by Datacenta, and the relevant fee as shown above is applied. We will jointly agree the media on which the backed-up data is to be transferred and the timing of the activity, to align with a quieter period in your schedule.

7. We will jointly agree the media upon which the restoration data is to be transferred and the means of despatch. We will then create the restoration data and despatch the media within 8 working hours of such agreement via the despatch method agreed. The costs of such despatch will be added to the next monthly bill.