

# Technical Overview

## Contents:

- 1 System Overview
- 2 Onsite – The Appliance
- 3 Onsite – Connectivity
- 4 Onsite – Software Agents
- 5 Onsite – Configuration
- 6 Offsite – Storage & Security
- 7 Offsite – Web Access
- 8 Monitoring & Recovery
- 9 Data Encryption
- 10 Controlling User Access

## System Overview

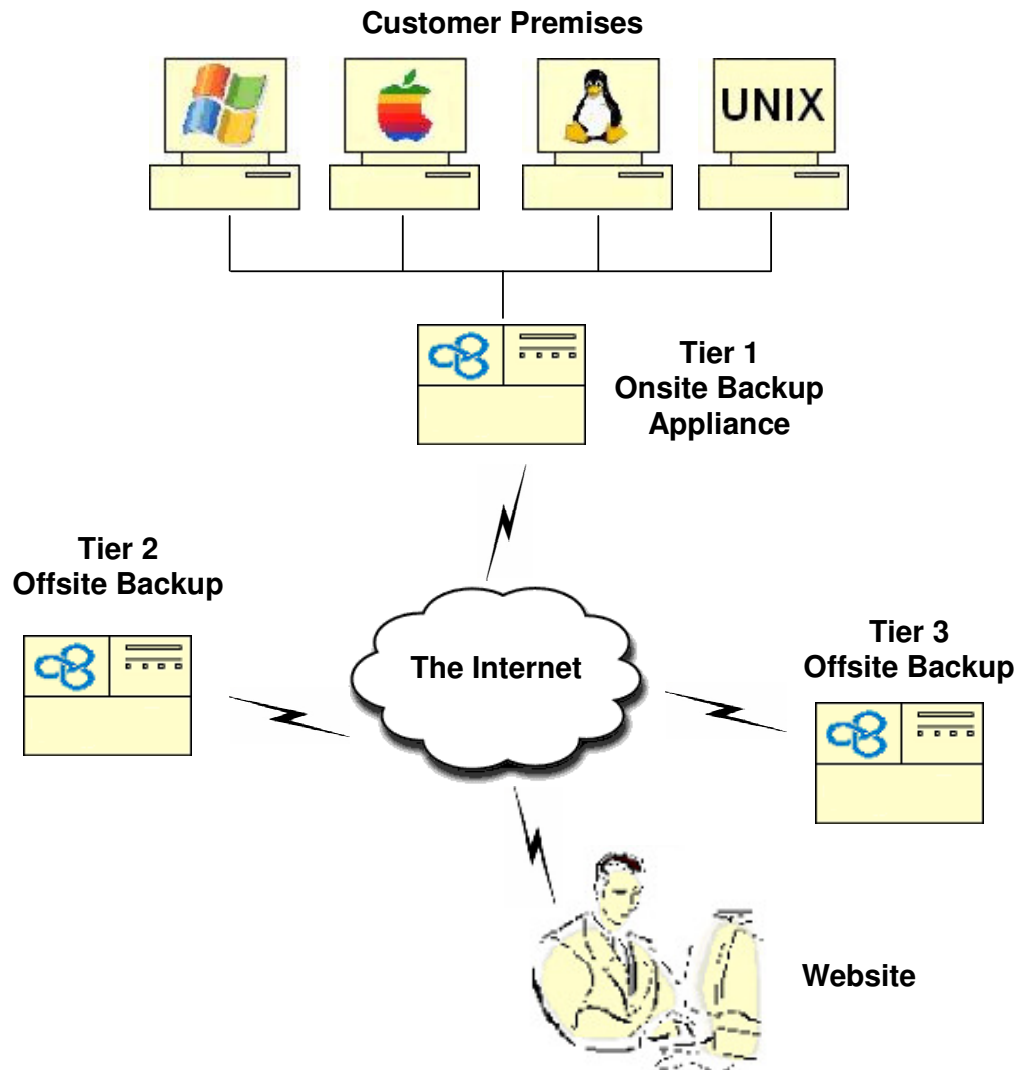
The system backs up the customer's computers during the day and sends the data offsite overnight.

An appliance is installed at the customer's premises to host the backup data and provide hardware redundancy.

One month of revisions are kept onsite, users can instantly see the directory tree and files as they were on any given day. Access to the backups is over the customer's local network and is very fast.

The data is stored at two secure offsite locations. One year of revisions are kept offsite. The offsite data is accessible via a website.

Backup Systems monitor the system, proactively contacting the customer and/or reseller if some aspect of the backup process failed.



## Onsite – The Appliance

The appliance is installed on the customer's premises and holds the onsite backup. It holds one month's worth of revisions.

It is a PC running Linux with custom backup software. The precise hardware build will vary depending on the customer's requirements.

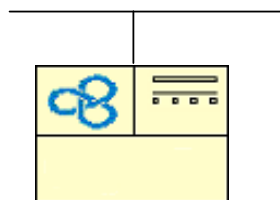
Typically the appliance is a small form-factor computer, measuring 20cm height x 20cm x 32cm length. It is quiet and power efficient, has 512MB ram, a Intel Celeron-R 3Ghz processor and a 100mbps network port. If required it can have a 1gbps network connection. If it needs to connect to a wireless only network it will have a wifi card.

We typically use RAID to protect the appliance. The maximum amount of data we can backup with a single appliance is 500GB. For larger amounts of data, we can either use multiple appliances or a larger appliance such as a tower computer.

The unit is owned and maintained by Backup Systems.

There are a number of pre-requisites that need to be met before the appliance can be installed;

- A broadband connection, sufficient to offsite the daily changes.
- A regular or UPS power supply.
- A network port with a static or DHCP allocated IP address.
- Customer firewall must allow http and ssh traffic for the appliance.
- Must setup a user with read access to all files that are to be backed up.



**Tier 1  
The Appliance**



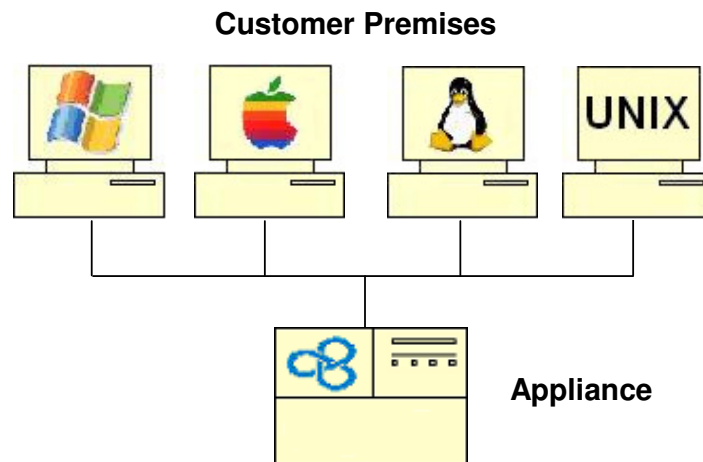
## Onsite – Connectivity

The appliance connects to the customer's computers using the Server Message Block (SMB) protocol. This is the standard networking protocol for Microsoft Windows machines.

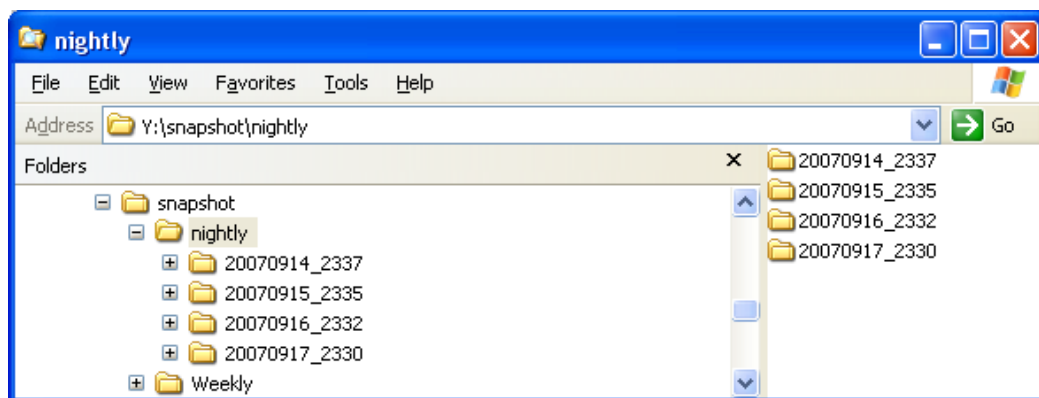
The customer must set up a read only share on the computers that require a backup to be taken and a user who has access to all the files that need to be backed up.

If for some reason SMB is unavailable, NFS can be used.

Laptops will be backed when they connect to the network. Remote sites on a WAN may be backed up from a central appliance provided the WAN is sufficiently fast, otherwise a second appliance will be required at the site.



The users also access the backup via read only SMB shares. Therefore the user can use their normal file browser to drag and drop backed up files from the appliance. For example, a Microsoft Windows user will simply map a drive using the standard Windows Explorer utility.



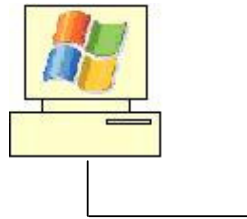
## Onsite – Software Agents



A software agent is a piece of software that needs to be installed on a customer's computer to allow certain applications to be backed up.

This is necessary where copying the files is not possible, e.g. they are always locked by the operating system. Or the application uses various files that need to be copied at the same moment of time.

### Customer Computer



We currently have to install an agent to backup the .pst files used by Microsoft Outlook, each computer with Outlook requires the piece of software. We need to buy this and so will pass the cost on to the customer.

Databases like Microsoft SQL Server or Sybase need to be scheduled to create a database dump to a file, we then offsite the file.

## Onsite – Configuration

The main tasks that the appliance carries out are;

- Backing up a share on a computer.
- Encrypting and sending the data offsite.

Typically all computers are backed up at the end of the day and are offsite during the night.

However the scheduling and frequency are soft coded.

For example;

- It would be possible to take an hourly backup of a particular directory tree on a computer, while only taking an end of day backup of another area on the same computer.

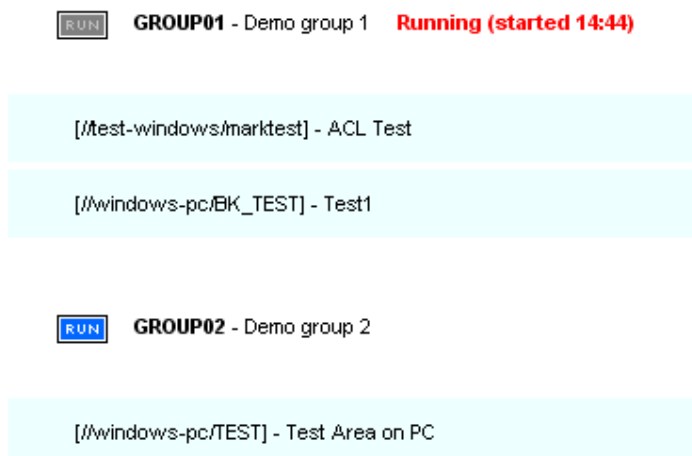
- It would be possible to group the backing up of various computers so they take place together at a certain time while other computers are backed up at a different time

- The offsiteing of data could be scheduled to run at a different time.

- The monthly limit of data can be extended.

The appliance is initially set up and configured by Backup Systems depending on the customer's requirements. At the present time further configuration changes are also done by Backup Systems.

The appliance has a password protected web page that allows the administrator to kick off an adhoc backup of a group. Here is a partial screenshot.



## Offsite – Storage & Security



The data is sent offsite during the night using the customer's broadband.

A delta blocking algorithm means that only the changes to files are sent offsite, this helps keep bandwidth usage down.

The files are sent to a server at a secure data centre.

Once the new version of the files have been reconstituted on the server a version control process takes place creating a "checkpoint" of the files for that date.

Later changes are replicated to another server at a separate location, the "Third Tier"

Customers share space on the same server. A "jail" ensures each customer's data is completely protected and cannot be accessed by another customer.

We may change data centre from time to time, however we always insist on the following features;

- 24 hour access, in the event that we need to do a full restore.
- A security patrol in the building with ID check on entry.
- A locked cabinet for the server.
- An Emergency generator.



## Offsite – Web Access

The offsite copy of the data can be accessed via a website.

Once the user has logged in, they are presented with a tree view of directories and files. Any file can be opened by left clicking on it's name. Or it can be saved to the users computer by right clicking and selecting "Save Target".

### Offsite Backup




There is a drop-down that allows the user to select which backed up share they want to view.

There is also a Date field. The field defaults to the date of the most recent checkpoint, by changing this the user can look at the directory tree and files as they were on any particular date. Normally one year of revisions are available.




To the right of each file is the date the file was last changed. Clicking on this will give a history of dates on which the file was changed.

A partial screenshot of the website is given below;






#### Account

<b>Login</b>	Emma Stuart
<b>Share</b>	My Documents <input type="button" value="v"/>
<b>Date</b>	 18th September 2007 <a href="#">Display Calendar</a>

#### File Name

<b>Spreadsheets</b>	
	Holidays
	2005-Sales.xls
	2006-Projections.xls

#### Directory Tree

- [-]  My Documents
  - [+]  Customers
  - [-]  **Spreadsheets**
  - [+]  Holidays
  - [+]  Year-End Files

## Monitoring & Recovery



Backup Systems monitor all appliances to ensure they are functioning correctly and backups are being taken. We proactively call customers if there is a problem.

Logs from the appliances are uploaded and automatically parsed; errors persisting over certain tolerances are automatically reported to us via emails.

The check-pointing process on the server is similarly monitored.



In the event of a total failure, for example a failure of the appliance or building burnt down, we would supply the customer with a new appliance with the most recent version of the data on it.

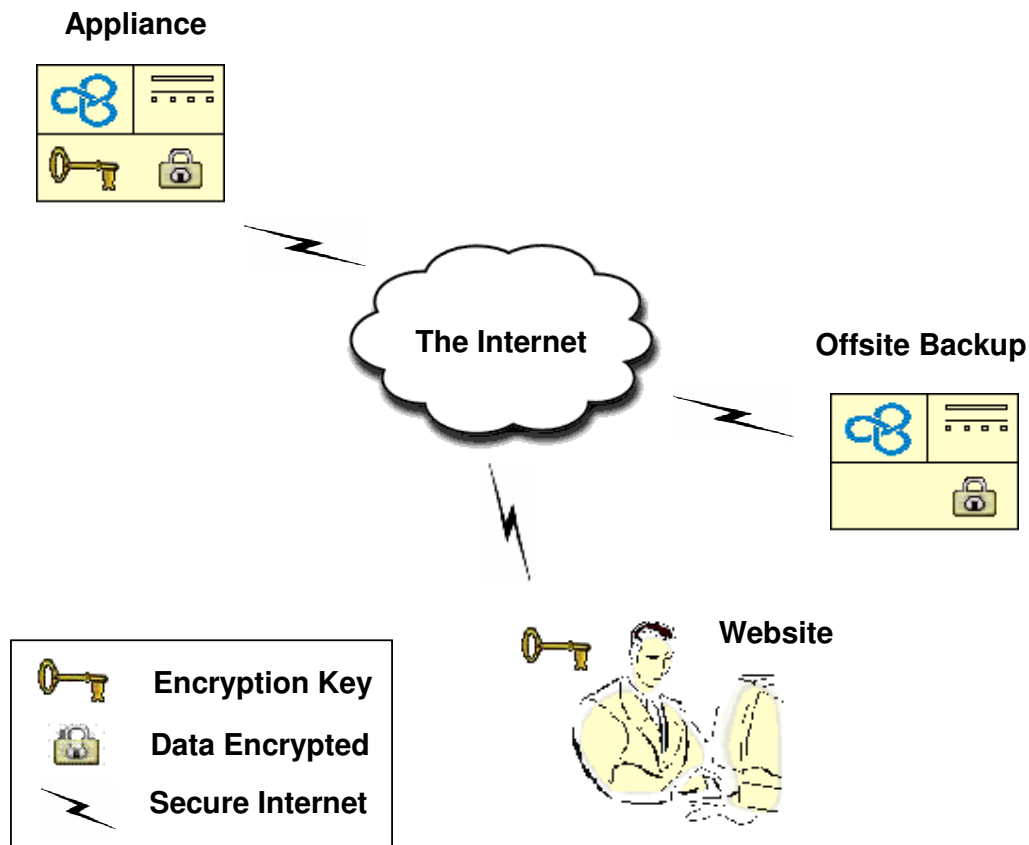
In any lesser failure, for example, one of the customer's servers is broken; the data will already be available on the appliance. This is the advantage of independent hardware.

# Data Encryption

All data sent across the Internet, between the onsite appliance and the offsite storage, or between the offsite storage and the website uses 128-bit encryption.

Additionally if the client has requested “offsite file encryption”, the data is encrypted on the local appliance prior to being sent. The data remains encrypted offsite and the key must be supplied when accessing the data via the website.

Therefore in this model the key is only stored on the appliance and the data is always encrypted when away from the customer’s premises. Backup Systems will not keep a record of the key, the customer needs to keep the key safe as they must supply it in the event of a full restore.

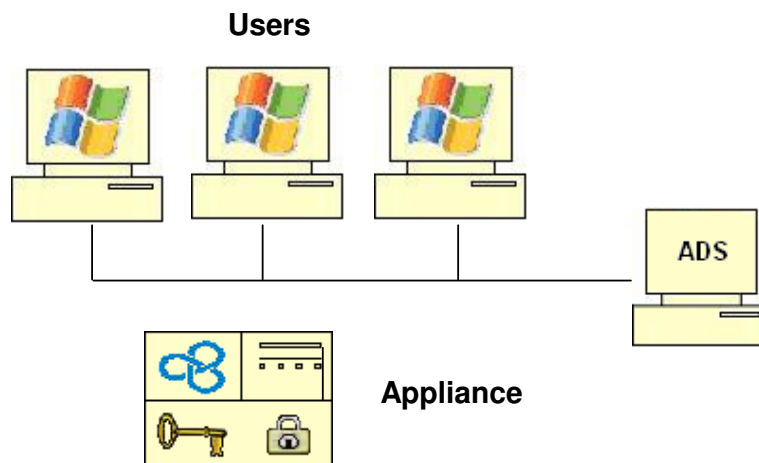


## Controlling User Access

Access to the local backup on the appliance is via read only network shares. The data can be split across any number of shares, with different users having access to different shares.

For example: The backup of payroll data may be accessed via a separate share from the marketing data. Some users would only be able to see payroll data others only marketing data.

If available the appliance can be integrated with Active Directory. In this model the AD administrator controls a user's access to the backups by adding/removing them from groups.



Access to the offsite backup is via a website, the user is required to supply a password to sign in. The data a user has access to can be configured based on their login.

