

restoreVault with PRE-RECOVERY

...pre-recovery keeps your business running even when your servers fail

As more and more data fills up larger and larger discs, a simple failure can cause vital systems like email and data servers to take hours or even days to come back online - crippling business and causing inconvenience to both clients and staff alike.

With its **Pre-Recovery** function the oobu restoreVault appliance brings failed servers back online straight away, and for total protection, it also backs up and then replicates your data to secure remote Data silo(s).

www.partner.net

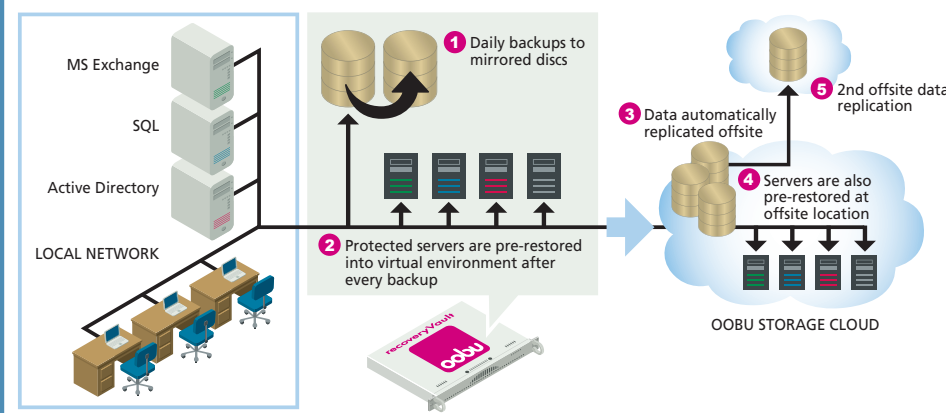
Partner Name Here
address
phone, etc.



restoreVault appliance summary:

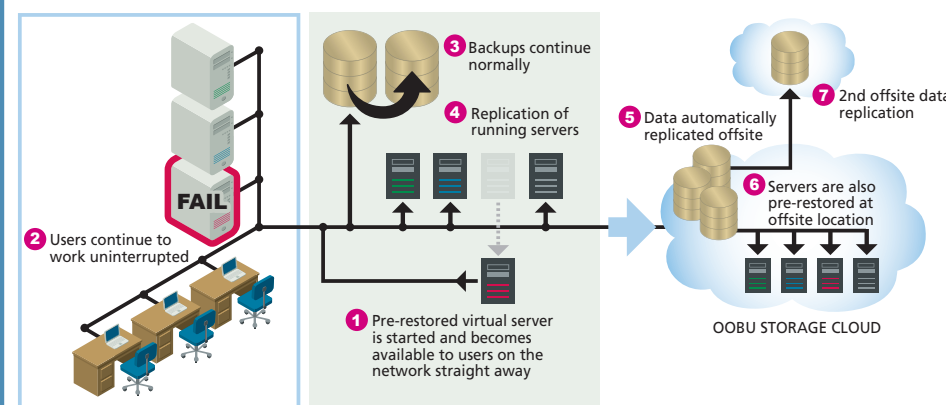
- inbuilt pre-recovered servers - immediate recovery of failed servers
- local disc backup - LAN speed restores of protected data
- auto-replication - data automatically replicated offsite
- one appliance solution - simple remote administration
- fully automated - no staff management issues

Normal (daily) operation



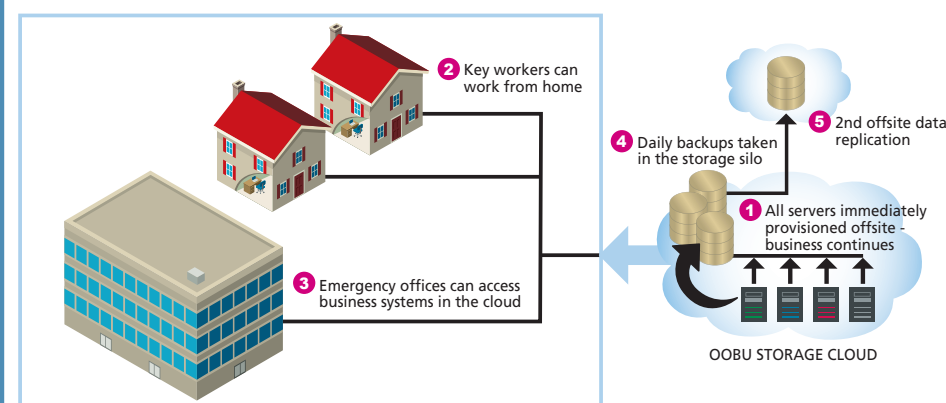
1. Daily backups are encrypted and made to internal, mirrored discs giving two backup copies of the protected data inside the appliance.
2. Also inside of the appliance, after every backup protected servers are then **pre-restored** in to their respective virtual servers, which are then ready to be switched on at a moments notice in the event of the protected server failing.
3. All protected data is then replicated to an offsite secure data silo.
4. Protected servers are then pre-restored again to provide disaster tolerance (optional).
5. All remotely protected data is replicated to a secondary data silo (optional).

Failed server - emergency operation



1. The pre-restored virtual server is started and this appears on the network almost straight away.
2. Within a couple of minutes or so, all network users will be working as before the failure.
3. All backup jobs to the local discs continue normally (including backing up the virtual server).
4. The unaffected servers are virtualised as before.
5. All protected data is then replicated to an offsite secure data silo.
6. Protected servers are then pre-restored again to provide disaster tolerance (optional).
7. All remotely protected data is replicated to a secondary data silo (optional).

Lost site - emergency DR mode



1. The pre-restored virtual servers located at the offsite silo are started and provisioned to be accessed remotely.
2. Users at home access remotely.
3. Users based in Temporary offices access remotely.
4. Daily backups taken in the storage silo.
5. All data is replicated to a secondary data silo (optional).

To re-instate the data, a restoreVault is shipped to the new customer site containing all data ready to run in Failed server mode. When the new infrastructure is ready, data is then simply restored.