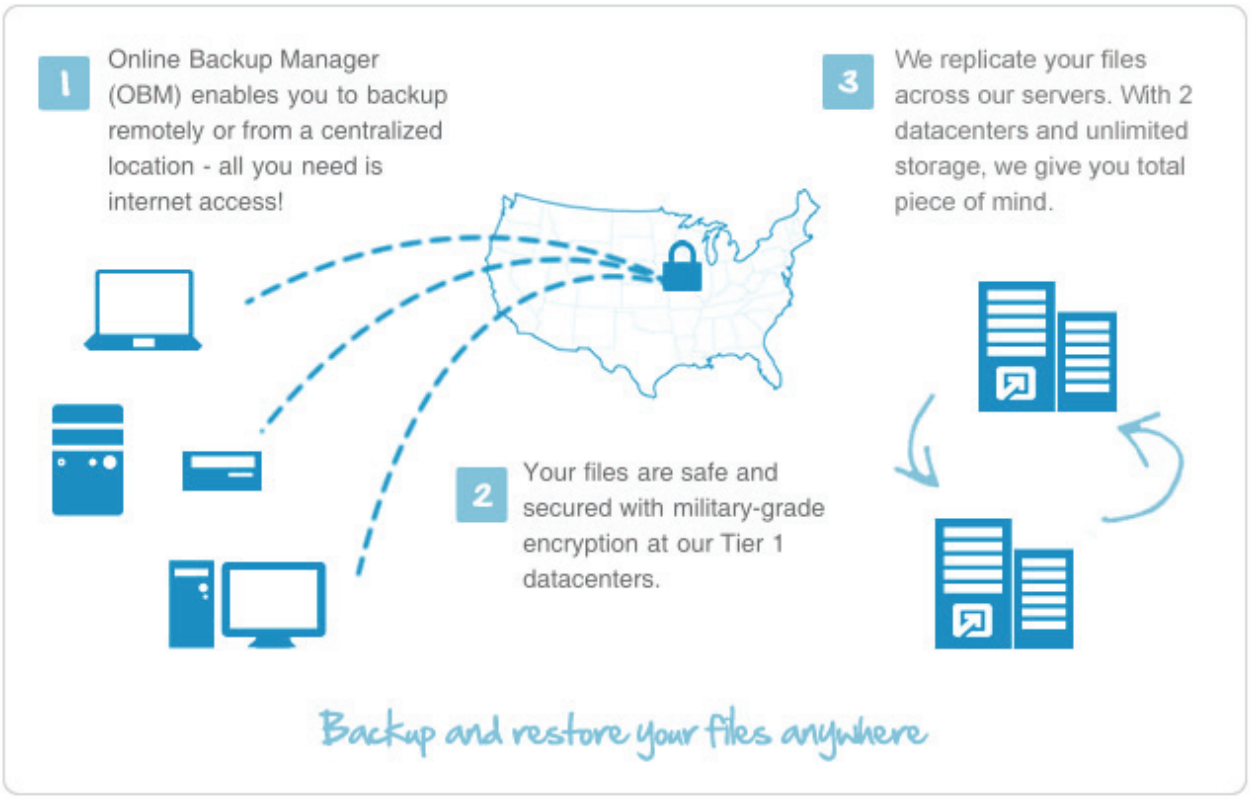
ONLINE BACKUP MANAGER

HOW IT WORKS

ONLINE BACKUP MANAGER HOW IT WORKS



1. Secure 128-Bit SSL Communication

All communications between Offsite Backup Server and your computer are transported in a 128-bit SSL (Secure Socket Layer) channel. Although all your backup files travel through a public network (internet), eavesdroppers have no knowledge of what has been exchanged.

2. Backups Are Securely Encrypted

All of your files are first zipped and encrypted with a user-defined encrypting key before they are sent to the Offsite Backup Server. To all people but you, your files stored on the Offsite Backup Server are no more than some trashed files with random content.

3. We Don't Keep Your Encryption Key

The encryption key used to encrypt your files resides only on your computer and is known only to you. It is never transmitted anywhere across the network. If this key is lost, all backup files can never be recovered. Therefore, although we have access to all files you stored on our Backup Server, we have no knowledge of the content of the files you stored.

VERY IMPORTANT : Please make sure you write down your encryption key and keep it in a safe place where it will never be forgotten. Otherwise, you will never be able to recover your backup files.

4. The Best Encryption Algorithm Is Used

Currently, the algorithm that we use to encrypt your files is 128-bit Twofish. It is a block cipher designed by Counterpane Labs. It was also one of the five Advanced Encryption Standard (AES) finalists chosen by National Institute of Standard and Technology (NIST). It subjects to frequent public reviews but no known attack against this algorithm has been reported.

5. It Would Require 8.77 x 1,017 Years To Crack Our 128-Bit Encryption

A 128-bit key size has 2,128 or around 3.4 x 1,038 possible combinations. Even if you have the world's best super computer, ASCI White, SP Power3 375 MHz manufactured by IBM as of November 2000, it would take 8.77 x 1,017 years to test all combinations. Assuming you have this super computer, the ASCI White, SP Power3 375 MHz has 8,192 processors which totals a capability of 12.3 teraflops (trillions of operations/second), available to you. Also it just needs one computer operation to test a possible combination (which is already faster than what it can do). To use brute force attack (checking all combinations) on this encryption algorithm. It would take:

3.4 x 1,038 possible combinations / 12.3 x 1,012 seconds (approximately 2.76 x 1,025 seconds)

(i.e. 876530835323573935 years or 8.77 x 1,017 years) to successfully try all combinations. Let alone the ASCI White cannot process as fast as what is described here. You can be sure that your data stored on our server is 100% secure!

6. Restricted Access To Your Data By IP Address

You can also restrict access to your backup files from the set of IP addresses you have defined. If someone tries to access your data from an IP address not on your defined list, their access will be denied. This additional security ensures that backup files are not open to all locations, even if the username and password are known.