

Blaze Vault Online Backup
Whitepaper – Data Security

Version 5.x
Jun 2006

Table of Content

1	Introduction	3
2	Blaze Vault Offsite Backup Server – “Secure, Robust and Reliable”	4
2.1	Secure 256-bit SSL communication	4
2.2	Backup data are securely encrypted	4
2.3	Encrypting key are well protected	4
2.4	Best encryption algorithm is used	5
2.5	Require 2.05×10^{54} years to crack the 256-bit encryption	5
2.6	Restrict access to data by IP addresses	5
2.7	Data Centre Security	5

1 Introduction

This document describes the security measures available in Blaze Vault Online Backup software from the user's perspective. It serves as a reference for partners when addressing customers' queries on security.

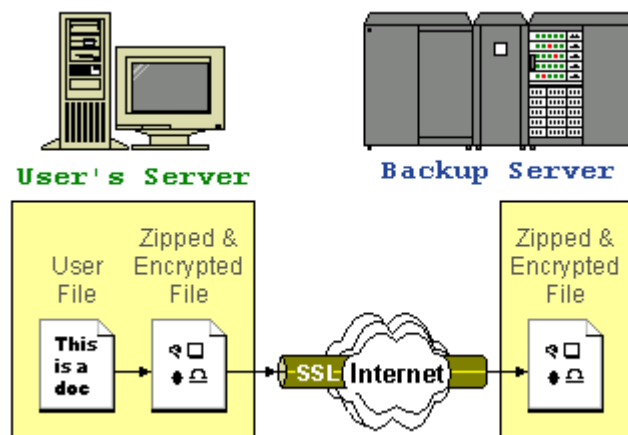
2 Blaze Vault Offsite Backup Server – “Secure, Robust and Reliable”

2.1 Secure 256-bit SSL communication



All communications between Blaze Vault Backup Server and your computer are transported in a 256-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.

2.2 Backup data are securely encrypted



All of your files are first compressed and encrypted with your defined encrypting key before they are sent to the Blaze Vault backup server. To all people but you, your files stored on the Blaze Vault backup server are no more than some garbage files with random content.

2.3 Encrypting key are well protected

The encrypting 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. Thus, even the system administrators will not be able to decrypt and view the content of your files stored on the backup server without your permission. This unfortunately means if the encrypting key is lost, you will never be able to recover your backup files.

Technical Details

The encrypting key for the different backup sets are stored the config.sys file, which is encoded by a proprietary algorithm:

(Windows)	C:\Documents and Settings\administrator\.obm\config\config.sys
(Linux)	~/.obm/config/config.sys
(Mac OS X)	~/.obm/config/config.sys

If client software cannot locate the config.sys (due to accidental deletion or logon to a new machine with the same account), it will prompt the user to re-enter the encrypting key for the backup set and then store it in the local config.sys.

2.4 Best encryption algorithm is used

Currently, the algorithm that we are using to encrypt your files is 256-bit AES. AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001 after a 5-year standardization process in which fifteen competing designs were presented and evaluated before Rijndael was selected as the most suitable (see Advanced Encryption Standard process for more details). It became effective as a standard May 26, 2002. As of 2009, AES is one of the most popular algorithms used in symmetric key cryptography. It is available in many different encryption packages. AES is the first publicly accessible and open cipher approved by the NSA for top secret information. For more information please visit [here](#).

2.5 Require 2.05×10^{54} years to crack the 256-bit encryption

A 256-bit key size has 1.1×10^{77} possible combinations. Even if you have the world best super computer, IBM's [Roadrunner](#), manufactured in 2008, it would take 2.05×10^{54} years to test all combinations. Assuming you have the super computer, Road Runner costing \$133 million, which totals a capability of 1.7 PFLOPS (trillions of operations/second), available to you. To use brute force attack (checking all combinations) on this encryption algorithm it would take:

$$\frac{1.1 * (10^{77})}{1.7 * (10^{15})} \quad \begin{array}{l} \text{(This is the possible number of AES 256-bit keys)} \\ \text{(This is how fast Roadrunner can calculate each possible combination)} \end{array}$$

$$= 64,705,882,352,941,200,000,000,000,000,000,000,000,000,000,000,000,000,000,000 \text{ Seconds}$$

or

$$= 2,051,810,069,537,710,000,000,000,000,000,000,000,000,000,000,000,000,000,000 \text{ Years}$$

or 2.05×10^{54}

to successfully try all combinations. You can be sure that your data stored on our server is 100% secured.

2.6 Restrict access to data by IP addresses

You can also restrict access to your backup files from the set of IP addresses you 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 backup files are not open to all locations, even if the username and password are known.

2.7 Data Centre Security

Trained security personnel maintain a 24/7/365 on site presence and carry out routine security checks. External Cameras and motion sensors cover the exterior perimeter of the data centre and are monitored by on site staff. Access to the data centre is protected by a sophisticated proximity fob system meaning all access events and movement within the data centre is logged and tracked. In addition security at the rack level can be enhanced by the addition of digital locks to rack doors.