Whitepaper

BOBcloud

AHSAY™

BOBcloud Data Encryption

www.BOBcloud.net

Summary

A core feature of BOBcloud's Cloud Backup Suite v7 is the focus on data confidentiality and security by using the most secure encryption methods and standards. By default the encryption is enabled with the highest encryption settings. Along with strong data protection capabilities, we provide our partners or MSP (Managed Service Providers) with tools for easy encryption key management (protecting encryption keys from loss, corruption, and unauthorised access) and the recovery of encryption keys.

What Is Data Encryption?

Data Encryption is

"The process of completely re-writing a file using an algorithm so that the data itself is obscured from being read"

unless a secret key or password is provided to decrypt the data back into its original form.

How Does BOBcloud Use Encryption To Protect Data?

This is how BOBcloud backs up your sensitive client data to our service or cloud storage. Clients need to be confident their data is totally secure from unauthorised access.

The purpose of data encryption is to protect the confidentiality and security of your data during backup, transit, rest and restore.

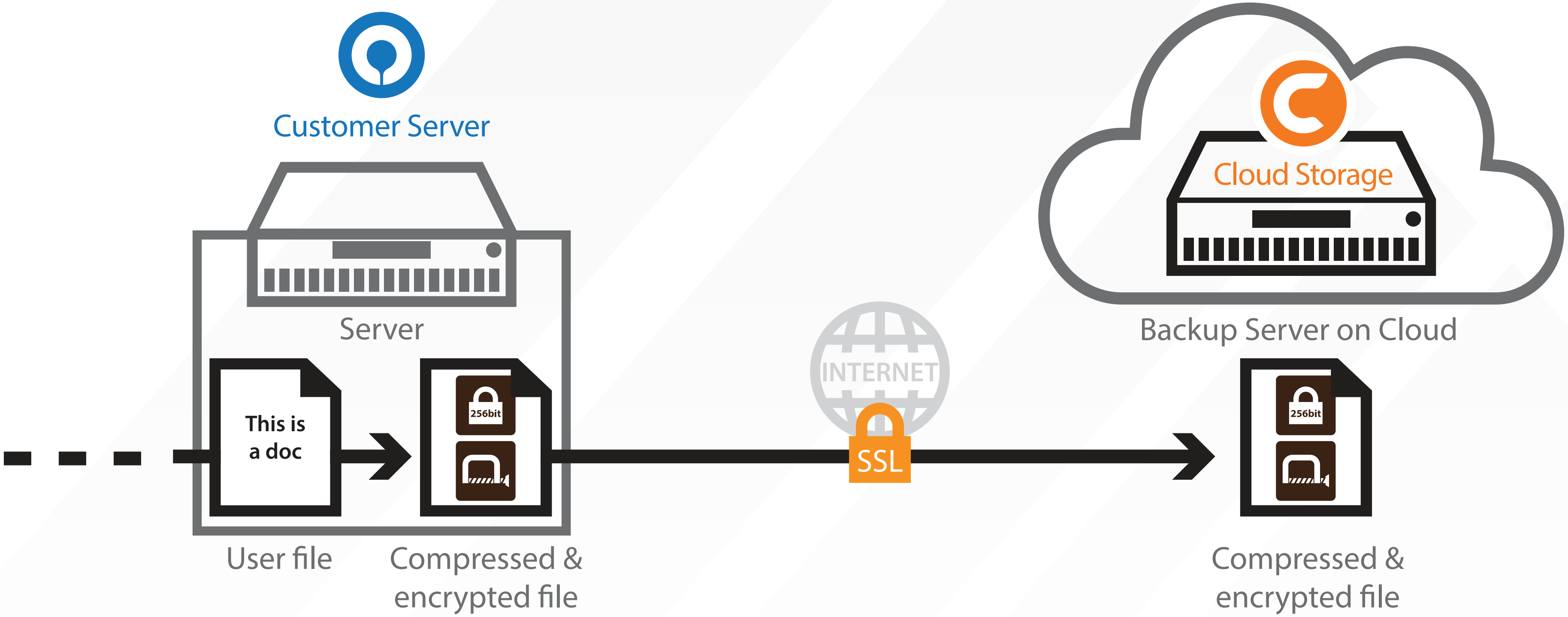
1 When it's transmitted via the Internet or other networks during backup/restore or replication.

Backup / Restore

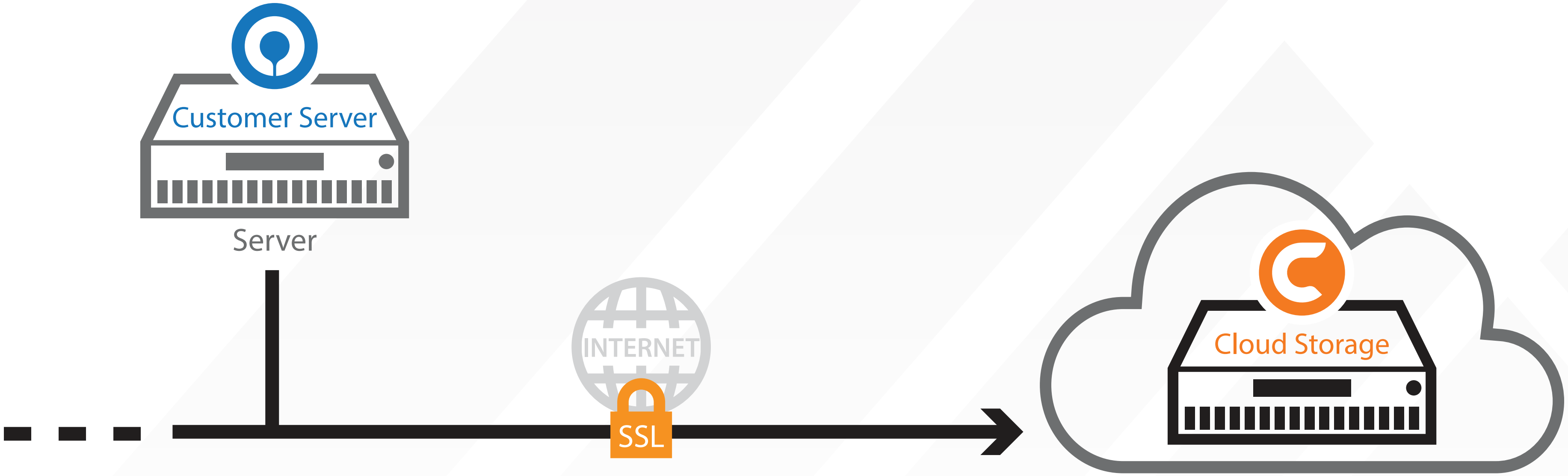
2 When it is stored in the backup destination(s), i.e. on the BOBcloud server or public cloud storage.

Backup Server on Cloud

All files are encrypted before they are transmitted to the BOBcloud server or public cloud storage. In the unlikely event the data is intercepted it would be useless to the unauthorised recipient. The backup data is stored in an encrypted format on the backup destination.



All communications between the Server and Desktop backup agents and the BOBcloud server or public cloud storage is via 256 bit SSL (Secure Socket Layer) channel. This uses TLS (Transport Layer Security) v1.2 protocol to ensure that your data is transmitted securely.



Backup Server on Cloud

256-bit SSL communication (TLS v1.2)

Authentication parameters & encrypted files
are further encrypted within an SSL channel

Encryption Algorithm

BOBcloud provides **three encryption options**:

AES, Twofish or DESede,

with AES providing the highest level of protection and DESede the lowest. Different levels of encryption allows you to protect your backup sets at varying levels, as there is a tradeoff between backup/restore performance and data security. When encrypting data using an AES algorithm the backup speed may be affected verses DESede algorithm. Therefore, you may want to use AES for sensitive data such as client information, commercial secrets, and financial records. While for less sensitive data, you may consider using a lower encryption option such as Twofish or DESede.

In addition, **two encryption methods** are available:

ECB (Electronic Cook Book) and CBC (Cypher Block Chaining),

where CBC is the stronger method, along with support for 128 bit and 256 bit key lengths.

The default encryption algorithm provides the highest level of protection and is the industry standard AES (Advanced Encryption Standard) encryption algorithm. It has a 256 bit key length and CBC mode. This is the only publicly available encryption algorithm approved by the US government for securing top secret information.

Can AES Algorithm Be Cracked?

Given enough time and processing power, any known encryption algorithm can be cracked using a brute force attack, i.e. systematically checking through all possible combinations.

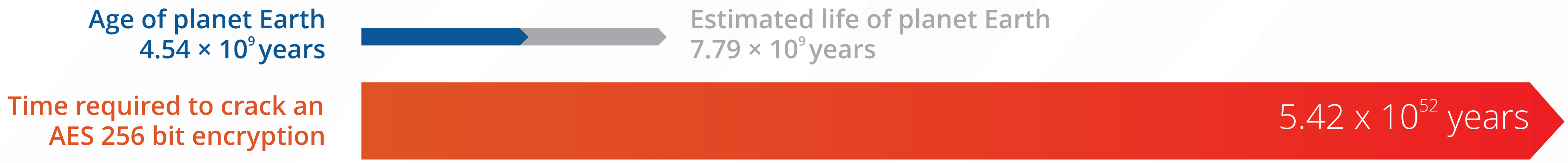
To put things into perspective,

AES 256 bit encryption algorithm has $1.1\mathrm{x}10^{77}(2^{256})$ possible combinations.

This would require approximately

$5.42 \mathrm{~x~} 10^{52}$ years to crack

with a brute force attack using a Tianhe-2 Supercomputer @ 33.86 petaflops. Therefore, the practical feasibility of a successful brute force attack is limited.



Encryption Key

The encryption key is used by BOBcloud to encrypt and protect your backup sets and data from unauthorised access. Once an encryption key is confirmed for a backup set, it cannot be removed or changed later.

If the encryption key on a backup sets needs to be removed or changed then:

- A new backup set will need to be created with the new encryption key.
- The data will have to be backed up again from scratch.

Encryption Type

BOBcloud offers three different options for generating the encryption key depending on the security level required by the customer; Default, User password, and Custom.

Type	Encryption Key Strength	Encryption Level
Default	The default option and is the most secure as the encryption key is a randomly generated 44 character key string with; upper case (A-Z) and lower case (a-z) characters, numbers (0-9), and other characters (/,\,=,+..).	AES, 256 bit, CBC
User password	Dependent on login password complexity	AES, 256 bit, CBC
Custom	Dependent on client preference	Client preference

Although different encryption options are available, BOBcloud provides partners and MSPs with an easy way to customise which encryption options clients can select. This will encourage good practices in data security via BOBcloud group policy.

⚠ **Note:** If the "User password" option is selected for generating the encryption key:

- BOBcloud Server / BOBcloud Desktop will use the current login password as the encryption key.
- The encryption key will not change, even when the login password is updated later.

Where Is the Encryption Key Saved and How Is It Protected?

The encryption key which protects the backup data is stored in a special file (settings.sys) encrypted using AES 256 bit algorithm. This is stored on the machine where the Server or Desktop backup agent is installed.

Depending of the operating system of the machine the **settings.sys** file is located in the following folder:

Operating System	BOBcloudServer	BOBcloudDesktop
Windows	%USERPROFILE%\.Server\config	%USERPROFILE%\.Desktop\config
Linux / UNIX	/root/.Server/config	--
Mac OS X	/Users/%username%/.Server/config	/Users/%username%/.Desktop/config
Synology NAS	/volume1/@appstore/BOBcloudServer/.Server/config	--

When Do I Need To Enter My Encryption Key?

The common situations where the Server or Desktop backup agent will require you to enter the encryption key:

The original machine has suffered a fatal outage and you need install Server or Desktop on a new machine to restore the files.

When accessing a backup set originally created on another machine.

The .server or .desktop folder on the machine is deleted.

The settings.sys file is accidentally deleted or corrupted.

When using BOBcloud to restore files (Service Providers only)

When using BOBcloud to restore files.

⚠ **Note:** If you do not have the correct encryption key you will not be able access the backup set and data or perform any backup/restore jobs.

Encryption Key Best Practices

For backup sets protected with “User password” or “Custom” encryption setting it is very important to make sure the encryption key will not be easily cracked or guessed. Please consider the following recommendations when creating an encryption key for your backup set.

Do not use an encryption key containing personal information, i.e. name, birthday, qwerty, login name, abc123, 123456 etc.

Ab1@$%

The encryption key should contain both uppercase (A-Z) & lowercase (a-z) characters, numbers (0-9), and other characters (+/-\=@#$%^&*())

≥8

The encryption key should be at least 8 characters long.

Keep a copy of the encryption key.

The encryption key is the password that allows access to your data, without the correct encryption key your data will not be recoverable. It is highly recommended that you keep a separate copy of your encryption keys and store them in a secure place. Clients are prompted to do this during the creation of each new backup set on BOBcloud Server / BOBcloud Desktop.

How To Manage Encryption Keys?

To meet both the needs of your clients and to satisfy any contractual, legal, or regulatory requirements related to data confidentiality and security, BOBcloud allows partners flexibility on how they choose to manage their clients' encryption key:

Allow their clients manage their own encryption keys.

The client encryption key is not uploaded and stored on the BOBcloud backup Server. Clients managing their own encryption keys provides the highest level of protection. The downside is, if a client loses or forgets their encryption key they will not be able to access their backup sets or recover data from their backup sets.

Manage their client encryption keys.

A copy of the encryption key is uploaded and stored on the BOBcloud backup server in a special file (EncryptionKeys-YYYY-MM-DD.json.rgz) for each backup set. This is encrypted using an AES 256 bit algorithm to maintain the confidentiality and security of the client data. Even the partner or the BOBcloud server administrator cannot access the encryption keys in this file.

The **EncryptionKeys-YYYY-MM-DD.json.rgz** file located in BOBcloud user home path: **%_USERHOME%\{%username%}\%backupset_id%\settings** folder.

If a client ever loses their encryption key then BOBcloud can request an encryption key recovery direct from the Ahsay web management console using our "Self Service Encryption Key Recovery Service".

	Partner/MSP	Client
Security Level	The keys are stored in a file protected by AES 256 bit encryption on the BOBcloud server (BOBcloud staff cannot access this password). The partner/MSP does not have access to keys.	The client only knows the encryption key.
Recovery	Encryption keys can be recovered by contacting BOBcloud. We will open the request with Ahsay and they will send the password to our customer and not us.	⚠ If the encryption key is lost or forgotten, the backup data is lost forever.

Encryption Key Recovery

People unfortunately make mistakes, and as a result passwords or encryption keys are lost or forgotten over time. This causes serious problems as the data you have invested time and money into protecting is no longer accessible.

To provide partners with peace of mind, BOBcloud has introduced the Self Service Encryption Key Recovery. Partners can now perform a recovery of client encryption keys directly from BOBcloud. The recovered encryption key is emailed directly to the contact email on the backup user account.

During the whole process the recovered encryption is only disclosed to the authorised recipient.

⚠ To use the Self Service Encryption Key Recovery Service partners must have:

- A valid maintenance contract.
- BOBcloud version must be on v7.9.2.0 or above.
- BOBcloud Server / BOBcloud Desktop must be on v7.5.0.0 or above.
- The "Upload encryption key after running backup for recovery" setting is enabled on the backup user account on the BOBcloud backup server.
- The "Encryption Recovery" option must be enabled on BOBcloud Server / BOBcloud Desktop backup client.
- BOBcloud Server / BOBcloud Desktop v7 must have successfully uploaded the encryption key details to the BOBcloud after a backup job.

  Which is saved in the **EncryptionKeys-YYYY-MM-DD.json.rgz** file located in BOBcloud user home path: **%CBS_USERHOME%\{%username%}\%backupset_id%\settings**
- The contact email address in the backup user account must be valid.