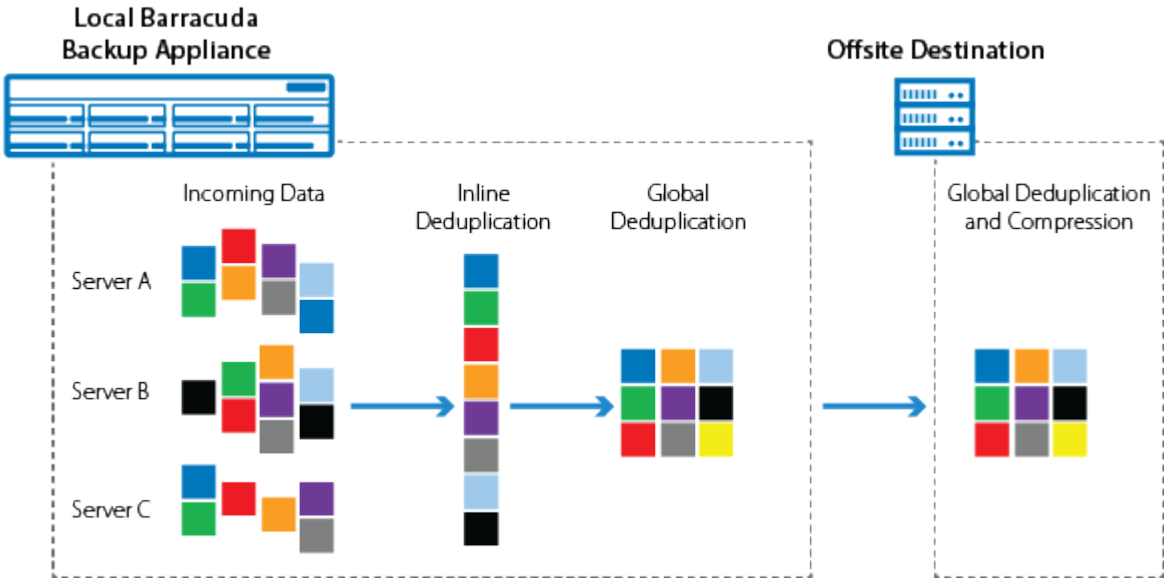
How Offsite Replication Works

All data selected for replication offsite is put in the offsite transfer queue on the local Barracuda Backup device. During the first initial full backup of a data source, all data is queued and transferred to the offsite replication destination. After each incremental backup, only the new or modified file parts are sent to the transfer queue and transferred to the offsite replication destination.

There are two types of data transferred offsite with every backup; metadata and binary data. Metadata contains information about the binary data, including how it is structured and when it was backed up. Metadata is very small, usually measuring in bytes, and is not included in any of the transfer graphs within the Barracuda Backup user interface. Binary data is the unique data that is written to disk after each backup. The binary data is what is reported in the transfer graphs in the Barracuda Backup user interface. Depending on how much data is backed up and put in the offsite transfer queue at once, the binary data size can range anywhere from a few gigabytes to tens of terabytes.

When data is transferred offsite, it is further deduplicated by checking to see if the file part already exists on the offsite replication destination. If the part does not exist, the part is compressed, encrypted using 256-bit AES encryption, and transferred to the replication destination. If the part already exists on the offsite replication destination, the part is simply dropped and not transferred offsite.

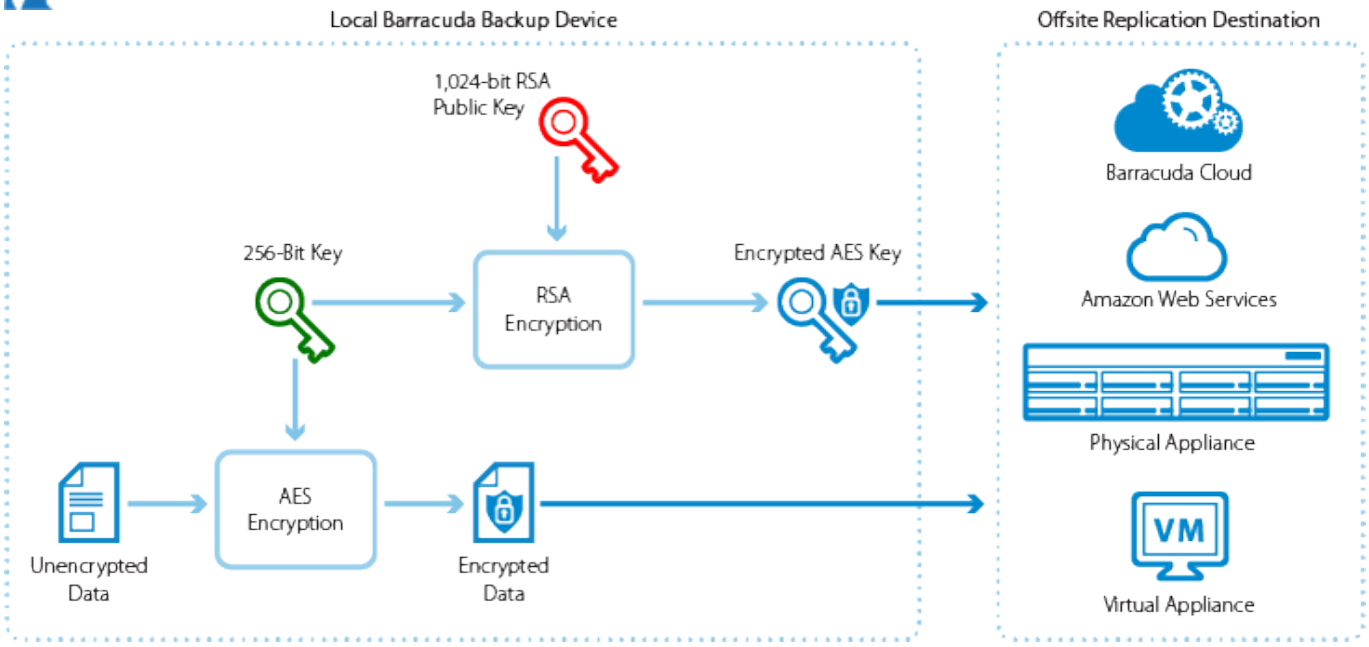
Figure 1. Data is Deduplicated and Replicated Offsite.



Encryption

Every piece of binary data is encrypted prior to being transferred offsite, to any offsite replication destination. Barracuda Backup uses a combination of Symmetrical (AES) and Asymmetrical (RSA) encryption to ensure that data transferred offsite is secure. For each binary data part or chunk, a unique AES 256-bit encryption key is generated, and the part is encrypted. To further protect the data, each unique AES key is encrypted using Asymmetrical 1,024-bit RSA encryption. The public key of the RSA key pair is used to encrypt the data locally and the private key, which is stored in the offsite replication destination, is used to decrypt the data upon recovery. Once each part and its associated key is encrypted, they are transferred to the offsite replication destination.

Figure 2. Offsite Replication Encryption Process.



For more information on Barracuda's cloud security and how encryption keys are managed, see Barracuda Security Policies.

The following data sources are encrypted during the offsite replication process:

- All binary data, which includes:
  - All data protected by the Barracuda Backup Agent for Windows, Linux, and macOS
  - VMware data
  - Network File Share data
  - Email attachments protected by the Exchange Message-Level backup

Data stored locally on a Barracuda Backup physical or virtual appliance is *not* stored encrypted. If encryption of data at-rest is a requirement, the Barracuda Encrypted Backup Appliances use encrypted hard disks and RAID controllers to secure data locally. Data transferred offsite, to any destination, is always transferred encrypted and stored encrypted at-rest on the target destination.

Cloud Data Private Encryption

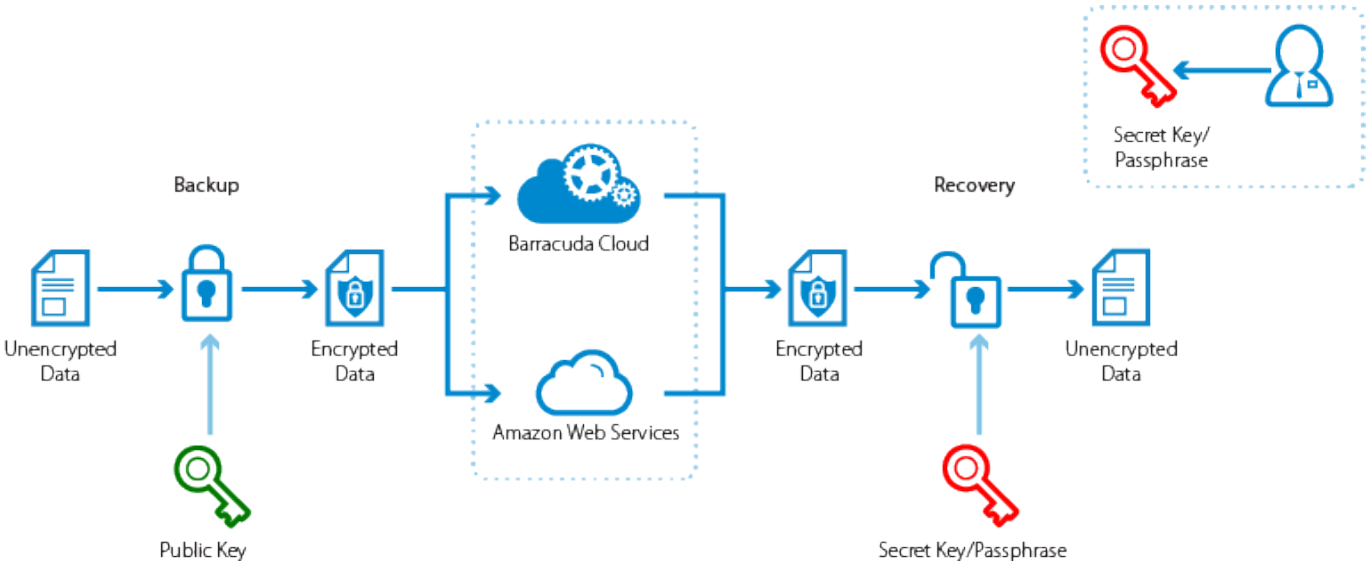
In Barracuda Backup version 6.5, Barracuda introduced a new feature enabling customers to create their own private encryption key for decrypting data that is replicated offsite to Barracuda Cloud Storage or Amazon Web Services (AWS). With this private encryption method, only Barracuda Backup users with the private encryption key passphrase can access and recover data. When configuring private encryption, it is recommended that the passphrase be kept using a password manager or stored in a secure location. If the passphrase is lost, the data stored in the cloud cannot be decrypted and is not retrievable, even by Barracuda personnel.

The customer-created passphrase is never stored on or written to disk on the local Barracuda Backup device or Barracuda datacenters in plain text. Private encryption of cloud data is configured in such a way that Barracuda has no ability to see the customer passphrase and interact with the privately encrypted data in any way.

The primary difference between the private encryption and the default, or Barracuda-managed, encryption method is that the RSA key pairs generated by the Barracuda Backup device are encrypted by the user passphrase when private encryption is enabled. Each Barracuda Backup device using private encryption has a unique 4,096-bit RSA key pair. The public RSA key is used to encrypt all the file parts prior to being transferred offsite, just like in the default Barracuda managed method. The private RSA key is still used to decrypt all the

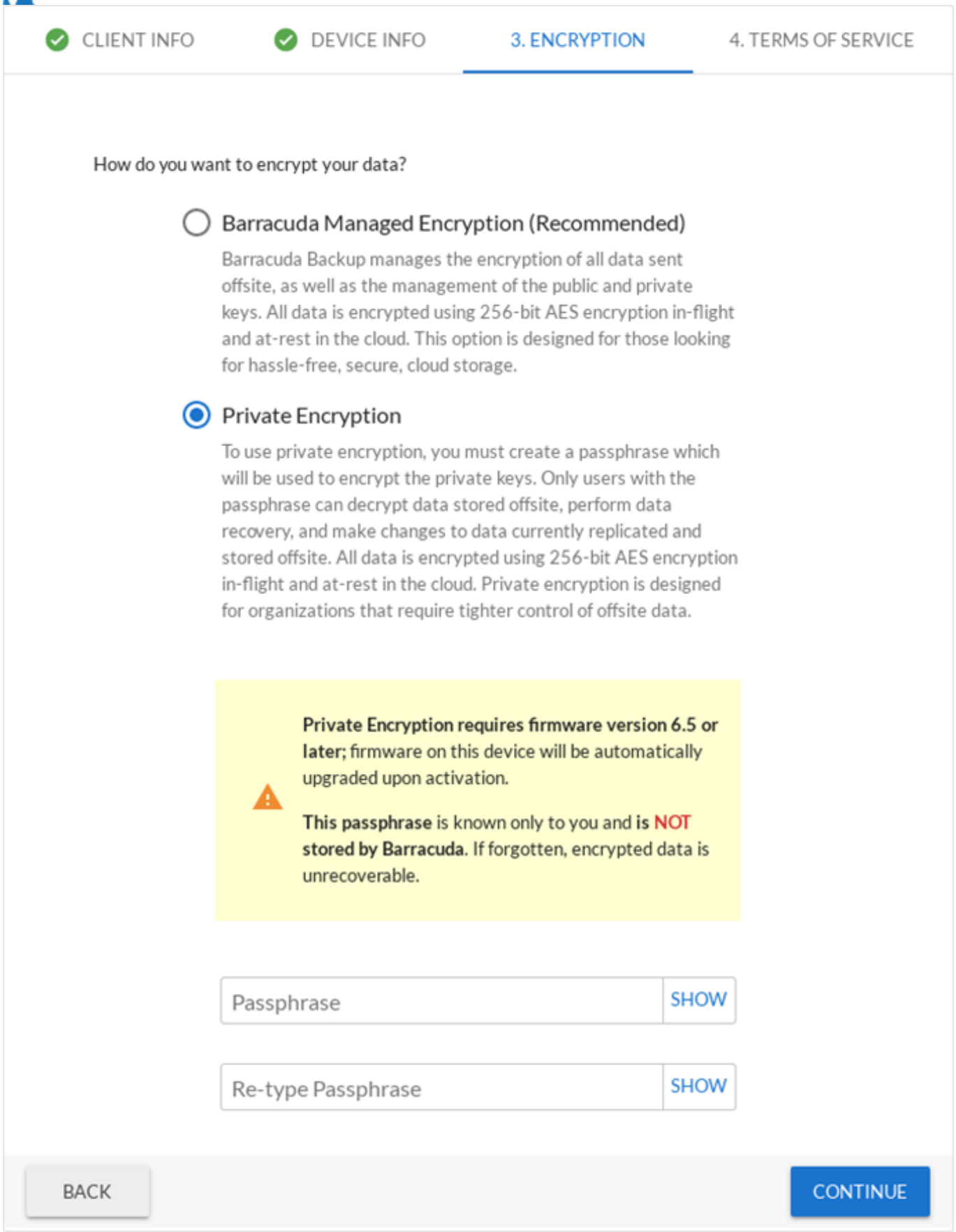
offsite data, however, only Barracuda Backup users with the configured passphrase can decrypt the data.

Figure 3. Private Encryption of Cloud Data.



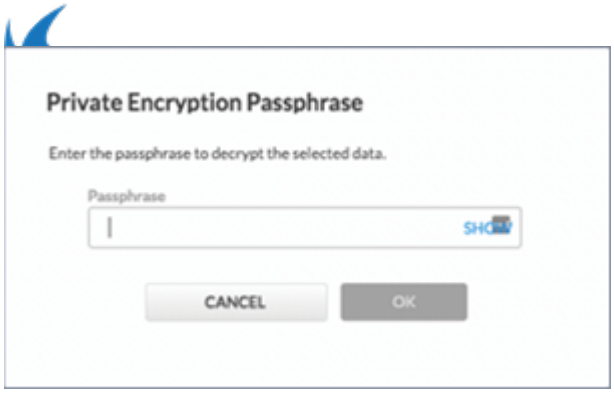
The private encryption feature can only be enabled in the activation wizard and therefore is only supported on new or newly linked Barracuda Backup devices. For existing customers that wish to use the private encryption feature, the Barracuda Backup device must first be wiped and re-activated. For more information on recovering privately encrypted data, see the Recovery section.

Figure 4. Configure Private Encryption.



Barracuda Backup devices with private encryption enabled display a prompt to enter the private encryption passphrase whenever any data recovery action is initiated by the user.

Figure 5. Private Encryption Passphrase Prompt.


Private Encryption Passphrase
Enter the passphrase to decrypt the selected data.
Passphrase
CANCEL
OK

Figures