mozyenterprise®

Securing and Encrypting Mozy Cloud Backup

The MozyEnterprise® advantage

Simple

Seamlessly manage backup, sync, and mobile access for multi-user and server environments from a single web-based console.

Secure

Your data is safe with military-grade encryption, world-class data centers, and EMC—a company built to last.

Affordable

Keep costs low with no hardware to purchase and minimal overhead required.

Contact us

corporatesales@mozy.com
866.950.6699
www.mozy.com/enterprise

According to IDC, cloud backup services have become the largest and most popular segment of advanced services among cloud-based storage services ("The Benefits of Cloud-Based Backup," IDC, September 2011). The growth of cloud-based backups can be attributed to their ability to deliver effective data protection and business continuity in a manner that increases reliability and consistency, while significantly reducing IT costs and ongoing maintenance and support efforts. However, before taking advantage of any online backup service, organizations need to take a close look at the security and encryption methods employed by the service's provider. As one of the industry's leading online backup service providers, Mozy takes seriously the protection of your data by addressing three main areas of concern for protecting data in the cloud: security, privacy and compliance.

Security

Mozy encrypts your data before it ever leaves your machine, during the transfer process across the wire, and while at rest in our data centers. The data centers employ state-of-the-art physical and technical security practices and where applicable, adhere to European Union Safe Harbor Privacy Principles. Additionally, Mozy has successfully completed the SSAE-16 audit and is ISO-27001 certified. These independent verifications certify that Mozy's processes and procedures meet or exceed the strictest control objectives in the industry. By voluntarily submitting to the SSAE-16 audit and obtaining ISO 27001 certification, Mozy shows its commitment to its client information and its preparation to face the growing threats to digital information. Not only do many popular cloud-based backup services fail to implement such high standards of security, but some fail to encrypt your data in a fully secure manner with a few entirely neglecting encryption. Later in this document, we detail the comprehensive measures and options that Mozy provides to ensure your data is secured and encrypted properly.

Mozy encryption options and standards

Before your backup data ever leaves your computer, Mozy first encrypts it using either AES or Blowfish encryption. Blowfish is a public-domain algorithm created in 1993 by a renowned cryptographer, Bruce Schneier. The algorithm was designed as a fast, general purpose algorithm that employs a secure variable-length keyed symmetric block cipher. Mozy utilizes the maximum 448-bit key length when employing the Blowfish encryption algorithm.

mozy BY EMC Copyright © 2014 Mozy, Inc. All Rights Reserved.

AES is a military-grade 256-bit encryption algorithm that has become the de-facto standard for the U.S. government in encrypting both Secret and Top Secret information. AES is also the standard encryption algorithm used by the National Security Agency and has become one of the most widely supported and utilized algorithms for encryption. Additionally, the AES algorithm is accepted by the Federal Information Processing Standard (FIPS) 140-2 for cryptography. As a result, the use of AES encryption enables an organization to be in full compliance with government data protection standards, enabling all government agencies and regulated subsidiaries to use Mozy AES encryption options to protect their data.

While AES is considered to be more secure or stronger than Blowfish, both algorithms are deemed as very secure. Additionally, while AES can achieve fast encryption rates, they are not quite as fast as Blowfish encryption rates.

Even though the Blowfish algorithm is considered secure, a publicly available cryptanalysis of the algorithm is not available. This doesn't indicate that the algorithm itself is broken, but simply that if it has weaknesses, they are not yet known. It also suggests that other algorithms that have received more attention might have greater longevity in terms of industry use and widespread support. On the other hand, AES has gone through multiple iterations of serious review. The first of such was a five-year review process as part of its adoption as the Advanced Encryption Standard itself. Since the year 2000, a number of other publicly available cryptanalyses have been conducted on AES, which has led to its wide acceptance and distinction as one of the most secure encryption algorithms available.

Your use of AES or Blowfish encryption with the MozyEnterprise service is determined by your choice in using one of the following three Mozy encryption options:

- **Default key:** Uses Blowfish
- **Personal key:** Uses AES
- **Corporate key (c-key):** Uses AES

In addition to the AES or Blowfish encryption of your data, during the transfer of your data Mozy uses a certified SSL connection with two-way certificate verification to communicate between your computers and the MozyEnterprise service. This is the same technology used by banks to secure online transactions. Furthermore, all users must authenticate to Mozy with a registered username and password.

Default key for encryption

The default key uses the Blowfish algorithm to encrypt your data. In addition to using a very secure and fast encryption algorithm, one of the main benefits of using the default key is that Mozy maintains that key for you. You don't have to worry about remembering the passphrase for that key in order to encrypt or decrypt your data. Mozy automatically takes care of all that for you, ensuring that your data is securely encrypted before it's ever transferred during the backup process.

Additionally, the mobility and web features in Mozy have built-in support for the default key. This means that you can seamlessly and securely view, search, or download backup files from your mobile device or a web browser. The default key delivers out-of-the box, ease-of-use encryption for all of your backups. Even though the default key offers secure, ease-of-use encryption, some organizations prefer to manage their own encryption passphrase rather than allowing Mozy to have knowledge of that key. As the name suggests, the default key will used by default unless you choose one of the other encryption options.

Personal keys for encryption

A personal key is one of two options from Mozy for organizations or individuals that want to take advantage of AES encryption. Personal keys allow individual users to manage their own encryption keys. When using a personal key, every user specifies their own unique encryption key for the data on their computer. In addition to having the stronger security that AES provides, security is further heightened by having a unique key that is known only by the individual user. The Mozy service does not maintain or have any knowledge of that key. So, even under force of law, Mozy cannot decrypt your files if you choose personal encryption.

To establish their unique personal key, users will be prompted to enter a passphrase that can consist of characters, symbols, or numbers. The passphrase can be any length. To keep the key secure, the Mozy client software uses a cryptographic hash of the passphrase stored on the user's machine.

Because the Mozy service does not store your personal encryption key and cannot decrypt them, in order to use Mozy's web and mobile capabilities to preview, search, or directly download files that you have backed up, you'll be required to enter the appropriate passphrase.

mozy BY EMC Copyright © 2014 Mozy, Inc. All Rights Reserved.

Additionally, if you're a Mozy administrator, in order to perform a restore on behalf of your users or to restore the files of users that have left the company, you will need to know or have access to those users' personal keys.

Likewise, if individual users forget their passphrase keys, they won't be able to decrypt or restore their data to a workstation. To protect against forgotten passphrases, Mozy provides the export option. The export option allows the user to save the encryption passphrase as a plain text file on a network share or removable USB drive. It can also be saved on the local computer's hard drive, but this is not recommended because that file will not be accessible if the computer encounters a system failure. When using the export option, we recommend that organizations establish a security policy in regard to where such passphrase files should be stored.

For organizations that want to take advantage of AES encryption but don't want users managing their own passphrases, Mozy offers the corporate key option.

Corporate key for encryption

The corporate key (or c-key) option enables enterprises to take advantage of the strength of the AES algorithm to encrypt their data, while significantly simplifying and strengthening passphrase management. With the corporate key option, one individual establishes the passphrase key for the entire organization. This individual could be anyone you choose, such as an IT or security director, manager or administrator. From within the Mozy administration console you set the corporate key passphrase and where it will be stored, such as a network share, web server, or as part of a package for installing Mozy on client machines. As Mozy is employed on different machines, each machine will access that location to use the encryption key for encrypting and decrypting files.

Because the corporate key passphrase will likely be stored on a network share or web server, to protect against unauthorized access of that key Mozy employs a Shared Secret capability that encrypts the passphrase. As you install Mozy on your client machines, the encryption of that passphrase will automatically be programmed into each client. As a result, your workstations running the Mozy backup client will be able to seamlessly leverage that passphrase to encrypt or decrypt files as needed.

To perform a web restore when using the corporate key, you will need to the use the Mozy crypto utility to decrypt files to be restored. The Mozy crypto utility will prompt you to enter a path to the corporate key file, the shared secret, and the files downloaded from the web restore to perform the decryption of the files and restore them on your local machine.

Similar to personal keys, because you maintain and store the corporate key passphrase, Mozy has no knowledge of it. Unlike other online backup providers, Mozy does not require that the key be uploaded or escrowed to Mozy's system. As a result, Mozy does not have the ability to decrypt your files if you choose the corporate key option. Likewise, since neither the Mozy service nor most users in your organization will have access to your corporate key passphrase, you are able to ensure your company's data remains safe from unauthorized access, even from employees who might attempt to download files to a home computer.

Privacy

To protect the privacy of your data, Mozy incorporates a combination of industry standard technical, administrative, and physical controls that safeguard your personal Information. Additionally, Mozy has established its own privacy commitment, operating our business on the following principles:

- Your information is your information, not our information
- We never sell your information to anyone nor do we sell information about you
- We never sift through your information in order to create a profile of you or target advertising
- You can always get your information back. We have no rights to your information if you leave the service
- Compliance

Compliance

Mozy views compliance as critical to the protection of your data. Our customers often want to know if they can remain compliant with a wide variety of international, U.S. and European Standards, including PCI DSS, SOX, HIPAA, GLBA, 95/46/EC Data Protection Directive, 2002/58/EC Privacy & Electronic Communications Directive, and SafeHarbor Listed while using our backup solutions. The principles behind each

mozy BY EMC Copyright © 2014 Mozy, Inc. All Rights Reserved.

of these standards are for the data owner to retain control of sensitive data and ensure that only authorized parties can view that data.

When you back up information to Mozy, you remain in control of the data through the authentication schemes and encryption the system uses. Each file stored within the Mozy infrastructure is encrypted prior to transmission to our infrastructure, meaning that private and sensitive information remains private while we store it for you. We do not compromise the internal security controls our customers maintain to meet compliance with various regulations. Mozy also takes proactive steps to protect against attacks, hazards, or unauthorized access that could threaten the security, privacy and integrity of your data.

Protect your data, protect your business

Mozy is in the business of protecting your data and your business. You can count on Mozy's strict security policies, military-grade encryption, and world-class data centers to deliver the availability, security, privacy, and compliance needed for optimal protection of your business data. From Fortune 500 to small businesses, Mozy is the most trusted name in online backup. As a part of storage giant EMC, Mozy has the experience and infrastructure to keep your data safe and secure.

mozy BY EMC Copyright © 2014 Mozy, Inc. All Rights Reserved.