Protecting Your Data in the Cloud with the Most Comprehensive Security and Encryption Measures

The MozyPro 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 Mozy

sales@mozy.com
877.669.9776
www.mozy.com/pro

It's more than just about backing up data

The growth of cloud-based backup solutions 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 cloud backup service, organizations need to take a close look at the security and encryption methods employed by the service provider. As one of the industry's leading cloud backup service providers, Mozy takes seriously the protection of your data in the cloud by utilizing the most comprehensive security and privacy measures.

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. EMC's 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 a SOC 1 SSAE 16 Type 2 audit and received ISO 27001 certification. 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 demonstrates its commitment to its client information and its preparation to face ongoing threats to digital information. Not only do many popular cloud-based backup services fail to implement such high standards of security, some fail to encrypt your data in a fully secure manner, and a few neglect encryption altogether. Later in this document, we detail the comprehensive measures and options that Mozy provides to ensure that your data is secured and encrypted properly.

Mozy encryption standards and options

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.

AES is a industry standard 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.

Types of encryption

Your use of AES or Blowfish encryption with the MozyPro service is determined by your choice in using one of the following three Mozy encryption options, with specific benefits for each type:

- **Mozy default encryption key:** Mozy assigns an encryption key to your users. This key is stored and managed by Mozy for the most seamless experience. Uses Blowfish encryption.
- **Personal encryption key:** The user enters a passphrase that is used to create the encryption key. Each user creates a unique personal encryption key. Uses AES encryption.
- **Corporate encryption key:** The administrator enters a passphrase that is used to create the encryption key. You can create a key for all users in the company or a unique one for each user group. The corporate key is sometimes referred to as the c-key. Uses AES encryption.

You determine the type of encryption key to use during the installation of the Mozy software, and that encryption is permanently associated with the files stored in the EMC cloud. MozyPro customers can configure the encryption type using a client configuration to assign the encryption key type for users. You can change the encryption type after you install the software. If you do change it, the software will re-upload all of your files to ensure that the stored files match your current encryption key.

Regardless of the type of encryption key used, files are encrypted in the first step of processing before they are sent to the EMC cloud. This ensures that the files are secure before ever leaving your computer and remain so during transit and at rest in the EMC cloud. If you are using personal encryption keys, Mozy cannot read and will not escrow your encryption key; therefore, the files are never decrypted until you restore them to your computer.

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 MozyPro 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.

Mozy default encryption key

The default encryption 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 encryption 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 of that for you, ensuring that your data is securely encrypted before it's ever transferred during the backup process.

Additionally, Mozy's mobility and web features have built-in support for the default encryption 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 encryption key will used by default unless you choose one of the other encryption options.

Personal encryption key

A personal encryption key is one of two options from Mozy for organizations or individuals who want to take advantage of AES encryption. Personal encryption keys allow individual users to manage their own encryption keys. When using a personal encryption 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 encryption 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've backed up, you'll be required to enter the appropriate passphrase.

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 encryption 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 encryption key option.

Corporate encryption key

The corporate encryption key (sometimes referred to as the 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 encryption 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 Admin 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. Because 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 encryption 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.

Similar to personal encryption keys, Mozy cannot assist you in decrypting files you have backed up, as we do not have access to your corporate encryption key. Corporate encryption keys are shared among all users in your organization or within a user group and can be distributed to the local computers or stored on a network server for users to access.

World-class data centers

EMC's state-of-the-art data centers are SSAE 16 audited and ISO 27001 certified and employ the following safety and security measures.

- **Onsite monitoring and security:** All of our data centers are surrounded by a secure perimeter and staffed 24x7x365 with technology professionals who maintain the highest standards in data protection. Both card and biometric security authentication are required to enter the facilities and access the Mozy server area.
- **Fire detection and suppression system:** EMC-managed data centers utilize a gas fire suppression system to extinguish fires in the event of an emergency without jeopardizing server functionality.
- **Redundant power and networks:** Power to our data centers is conditioned and protected by redundant systems. In addition, multiple network providers service each data center to ensure operation in the event a network carrier fails.
- **Temperature control:** All of our data center sites have cooling mechanisms in place to ensure that the servers are kept at optimal operating temperatures.

And because Mozy has multiple data centers located internationally, data can be stored locally within economic communities. For example, data can be retained within the United States or within the European Union. This ensures that it's possible to comply with local data-handling laws and principles.

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 these 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.

Protect your data, protect your business

When you back up information with Mozy, you remain in control of the data through the authentication schemes and encryption the system uses. Each file stored in the Mozy cloud 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.

Mozy is in the business of protecting your data and your business. You can count on Mozy's strict security policies, industry-standard encryption, and world-class data centers to deliver the availability, security, and privacy needed for optimal protection of your business data.

A company built to last

Mozy backs up data for more than 100,000 companies and more than 6 million individuals, and manages 90 petabytes of stored data. As a part of storage leader EMC, a Fortune 200 company, Mozy is a key component in EMC's mission of protecting your critical business data. EMC provides the infrastructure technology and solutions that enable organizations to compete and create value from their information. Through our heritage as one of the first cloud computing companies and our partnership with EMC, Mozy has the experience, infrastructure, and financial strength to ensure that your data is safe, secure, and available when you need it. From Fortune 500 to small businesses, Mozy by EMC is the most trusted name in cloud backup.