Secure Cloud Storage.
Backup, Share and Restore Any File, Anytime, Anywhere, with Any Devices

SecureAge

What is **LockCube** ?

LockCube is a cloud storage service with a proven military-grade security. It allows users to securely back up, restore and share any file – Microsoft Office documents, zipped files, pdf, videos, photos, songs and more – in the cloud with any device.

What can LockCube do?

Secures Data at Rest and in Motion

- Uses proven military-grade data security trusted and deployed by governments in Asia Pacific.
- Uses 256-bit AES encryption client to encrypt individual data with the user's encryption key automatically and transparently. Users do not have to consciously remember to encrypt each and every file.
- Individual file remains encrypted before, during and after it is transmitted over the network to the LockCube server.
- Only authorized users can use their decryption keys to decrypt and view the encrypted files. Hence, hackers, sniffers or insiders are unable to view them without the user keys.

Backup of any File with Smart and Unlimited Versioning

- Allows secure backup of any file to prevent data loss.
- Provides users with scheduler to define specific backup date and time without disrupting their work routines. This saves them the hassle of backing up their data manually.
- Detects and backs up only modified data automatically, reducing subsequent backup time and network bandwidth usage significantly.
- Creates versioning of backup folders by specific date and time, enabling users to recover their original file when the current version is corrupted or accidentally deleted.

Restores any File Securely

- Allows users to salvage all their critical data when

their computer hard disks crash, when their handheld devices are lost, or when disasters strike.

Secure File Sharing

- Allows users to share encrypted files with one another.
- Only authorized recipients are privy to the content of the shared encrypted files.

Direct Access to LockCube Drive

- LockCube drive (usually Z: drive) is automatically mounted on the computer and works like a normal drive in the computer. Users can access, open, edit, save, copy and paste any file by using any existing application, such as Microsoft Word.
- All data stored in the LockCube drive are automatically encrypted without user's conscious involvement.

SecureDrive - An Encryption Utility

- LockCube is the world's first cloud storage service that provides an encryption utility, SecureDrive.
- Users can enjoy a hassle-free backup of more than 50GB of data by using SecureDrive to copy and encrypt all files from the local hard drive, file server, or even the LockCube drive to any removable media like USB flash drive or external hard drive. The LockCube Team can then provide the service to copy the encrypted files from the removable media directly to LockCube cloud storage.
- Helps users restore critical data for disaster recovery quickly. The LockCube Team can restore all encrypted files to users' removable media, allowing them to recover lost files by using SecureDrive to copy and

decrypt the encrypted files from the removable media back to their hard drive or file server.

Secure and Easy Access via Handheld Devices
- Allows users to securely store and access any files in the cloud with Android smartphone, Android Tablet, iPhone and iPad.
- Ensures all data is encrypted on mobile devices, when shared and when uploaded.
- No more worries about anyone viewing their encrypted data when the mobile device is lost.

Who needs LockCube?

LockCube is for small and medium enterprises that need to:
- Perform a secure and regular offsite backup as part of the company's business continuity and disaster recovery plan.
- Reduce capital outlay in hardware, servers and databases.
- Actively share confidential information with their co-workers, counterparts or customers.
- Cut down on their IT support in server maintenance.
- Access sensitive data anytime, anywhere.

Why Choose LockCube?

LockCube is different from other cloud storage providers for its proven military-grade data security. It leverages on 256-bit AES encryption, the world's strongest encryption standard today. It is certified for use in protecting secret level data by the US government and the Department of Defense. As cited in Wikipedia's Brute-force attack, 'Breaking a symmetric 256-bit key by brute force requires 2^{128} times more computational power than a 128-bit key. A device that could check a billion billion (10^{18}) AES keys per second would in theory require about 3×10^{51} years to exhaust the 256-bit key space.'

LockCube in comparison with other cloud storage offerings

LockCube	Other Cloud Storage Offerings
File level encryption – Each file gets automatically encrypted at the client machine (computer). **Benefits:** • Data is automatically encrypted at the client machine using the user's encryption and decryption key. • This ensures that individual file will not be compromised by intruders even if it leaves the client machine, travels over the Internet and residing in the servers.	**Full disk encryption** – Users' data get encrypted only at the server. **Threats:** • Data is encrypted and decrypted at the server using the same encryption and decryption server key. • Full disk encryption only encrypts the entire disk or server but not the individual file. It is like a bank vault with the door wide open, and once the users' data travel out of this bank vault, it becomes unprotected and vulnerable to intruder attacks.
User's encryption key is not stored in the server **Benefits:** • Users safe-keep their own key. Hence, only the authorized user and no one else can decrypt and access the encrypted data. • Any attempts by the hackers or even the employees of LockCube to open the encrypted data, are unable to do so without the authorized key. • A government subpoena that orders the surrender of the users' data, will not be able to access the data without the proper key.	**Encryption key is stored in the server** **Threats:** • Other cloud providers may self-profess to impose stringent policy to restrain their internal staff from accessing the users' data. But policies can be disregarded by their unhappy employees any time. • Any disgruntled employees of the cloud storage providers can easily sabotage the users' data. • Hackers who hack into the servers can access all the users' data. • A government subpoena can order the cloud storage providers to surrender all the users' data stored in the server.
Genuine protection of data in motion via Encryption **Benefit:** • Truly protects / encrypts individual file with the authorized user's key. Since the file remains encrypted even when it is travelling over the Internet, sniffers will not be able to access it without the authorized key.	**Claim to protect users' data via SSL (Secure Socket Layer)** **Threat:** • SSL is a cryptographic protocol that can only secure communications / transmissions on the Internet. It does not truly protect / encrypt the individual file that is travelling over the Internet. Hence, the data in transmission is still vulnerable to potential sniffers using man-in-the-middle attacks.

→ Need More Information?

General Enquiry: contactus@secureage.com
Public Relations / Marketing: pr@secureage.com

LockCube Technical Support: ask-lockcube@secureage.com

www.lockcube.com
www.secureage.com

Asia Pacific
SecureAge Technology Pte Ltd
3, Fusionopolis Way
#05-21, Symbiosis
Singapore 138633

Japan
SecureAge K.K.
Barbizon 18, 7F
5-18-18 Shirokanedai
Minato-ku, Tokyo 108-0071
Japan

North America
SecureAge Technology Inc
3 Twin Dolphin Drive Suite 150
Redwood City CA 94065
U.S.A.