SecureAge

Secure Cloud Storage for Small and Medium Enterprises

LockCube
Whitepaper

Data Security in the Cloud

Cloud storage is a matter of choice and trust to enterprises. Data breach is a matter of redefining data protection. 3P encryption will be the key to redefine data protection and reinstate a culture of choice and trust in the cloud.

The challenges of data backup faced by enterprises

More and more enterprises are grappling with one common problem – where and how to store their critical data securely?

Some enterprises may store their critical data in their computer hard disk or file server or back up to a removable media. But accidents like crashed hard disk, lost USB flash drive or damaged external hard disk do happen. Disasters like flood, fire or earthquake do strike and will destroy all critical data alongside with the storage devices in no time. There is no way you can recover these critical data stored in the ruined devices. Furthermore, loss of important data may affect a company's business continuity and progress. In a worst scenario, it may even cause the company to shut down.

What about those mobile business professionals who need to access sensitive data on the go? It is extremely cumbersome for them to carry portable storage devices (like USB flash drive and external hard disk) wherever they go. What if they lose the devices? It means that the unprotected sensitive data in the lost devices may run the danger of being accessed by someone else. Since they are always on the move, they need the convenience of accessing the data anytime, anywhere with their laptop, smart phone and tablet. How to solve their problems?

Cloud Storage Solution

Cloud storage is a more efficient and cost effective backup solution for small and medium enterprises, as compared to setting up a file server in the company or hosted in a remote data center. They can store tons and tons of data in the cloud without having to purchase expensive storage equipments. They can cut down on IT expenses and reduce unnecessary overheads by embracing pay-per-use Infrastructure-as-a-Service (IaaS) or Software-as-a-Service (Saas) solutions. They can also enjoy great scalability and cost savings by scaling their cloud storage according to their requirements and pay only for what they use.

Since data is stored in the cloud, enterprises no longer have to worry about unrecoverable data due to crashed hard disks or misplaced USB flash drives or natural disasters. With an Internet connection, they can access the data anytime, anywhere with their laptop, smart phone and tablet.

Cloud storage definitely offers numerous benefits to enterprises, but they are still hesitant to use it. Why?

Data Security in the Cloud - A Top Concern for Enterprises

Numerous industry surveys have cited data security as users' key concern when putting their data in the cloud. Recent news report on hacking activities targeted at big corporation, government sites and social media increase

Security Infrastructure

enterprises' concern over data security in the cloud. Their worries over data integrity, privacy and reliability have deterred them from exploiting the true advantages of cloud storage solution.

Since anyone can access the data stored in the cloud anytime and anywhere, there is a possibility that their privacy may be compromised. They are worried that sensitive data in transit may be compromised by potential intruders or stolen by their adversaries.

Most enterprises are used to storing their information in their own premises. They may feel uneasy to entrust their critical data to another company for storage. They are concerned that a disgruntled employee of the cloud service provider may potentially commit an insider attack.

In fact, such data security concerns are not unfounded especially with a data breach incident by a renowned cloud storage provider in June 2011. It accidentally allowed anyone to access any user's account without user's knowledge.

Massive data breaches are beyond any user's control. They will ultimately make or break an enterprise's choice in utilizing a cloud storage solution. But we shouldn't resign to this fact. There is a way to store your data securely in the cloud without worrying about security breaches. But you must do it right.

What does a good security infrastructure entail?

Data security can be a great stumbling block to users' easy access to the cloud data anytime, anywhere. To make security process less painful, most of the cloud storage providers usually allow the encryption and decryption process to be done at the server. In order to perform this encryption and decryption process at the server, a single server encryption key stored at the server is used for encrypting the storage system. Unfortunately, anyone with access to the server system can then easily access user's data wantonly.

Hence, a good and robust data security should cover up such vulnerability by removing all possibilities of exposing the user's key to unauthorized personnel. Every single user has to create, own and safe-keep his/her own unique key that authenticates his/her identity. Data encryption and decryption process should be performed only at the client side and with a user's encryption and decryption key. Unauthorized intruders to the cloud storage server are unable to access the encrypted data without the proper decryption key. But such sophisticated security infrastructure encompasses extremely complicated technical architecture which requires many years of intensive development and testing effort.

SecureAge Technology started off by developing security solutions specifically for the militaries and governments based on stringent security policies. Our cumulative years of experience have helped us to develop a robust security infrastructure which has been widely deployed by the militaries and governments in the Asia Pacific region. LockCube, developed based on the same security implementation, is the reliable cloud storage service that genuinely keeps your confidential data safe in the cloud.

LockCube reinvents data security in the cloud. It armours every single data with an invisible cloak of encryption – transparent and automatic to users yet unfathomable to hackers, sniffers and insiders.

What is LockCube?

What is LockCube?

LockCube provides business users a smart and secure way to backup, restore and share any file in the cloud, anytime, anywhere, on any device like desktop, laptop, smart phone and tablet. It is the perfect cloud storage service for small and medium enterprises because:

i. It is highly affordable as users need to pay only for the storage they use with unlimited access,

ii. It fulfills a company's business continuity and disaster recovery plan by providing a secure and regular offsite backup.

iii. It provides company with a cost-effective backup alternative to costly hardware, servers and databases.

iv. It provides company with a simple, reliable and secure way of storing their voluminous data, instead of relying on storage media (like backup tape, external hard disk and USB flash drive) with limited life span.

v. It provides company with unlimited scalability of storage space without needing to plan ahead

vi. It allows secure business collaboration whereby confidential information can be shared among co-workers, counterparts or customers.

vii. It helps company with limited IT resources by cutting down on the IT support in server maintenance.

viii. It provides mobile business professionals an easy and unlimited access to the data anytime and anywhere.

ix. It provides multiple access methods via web, direct disk mounting and dedicated LockCube App.

LockCube's Infrastructure with Proven Military-grade Security

1) User's Encryption Key

LockCube is built on a security infrastructure that is proven to be military-grade due to its successful deployment for more than 20,000 militaries and governments in the Asia Pacific region. It eliminates data security concerns by using a comprehensive authentication and encryption technique to ensure that only authorized user is privy to the content of the data. Each and every authorized user creates and safe-keeps his/her own unique encryption key that is not shared with anyone else.

Unlike other cloud storage operators, the user's encryption key is not stored at the LockCube server, as stated in LockCube Terms of Service. There is no way anyone, including the LockCube operator, can access the user's data without the key.

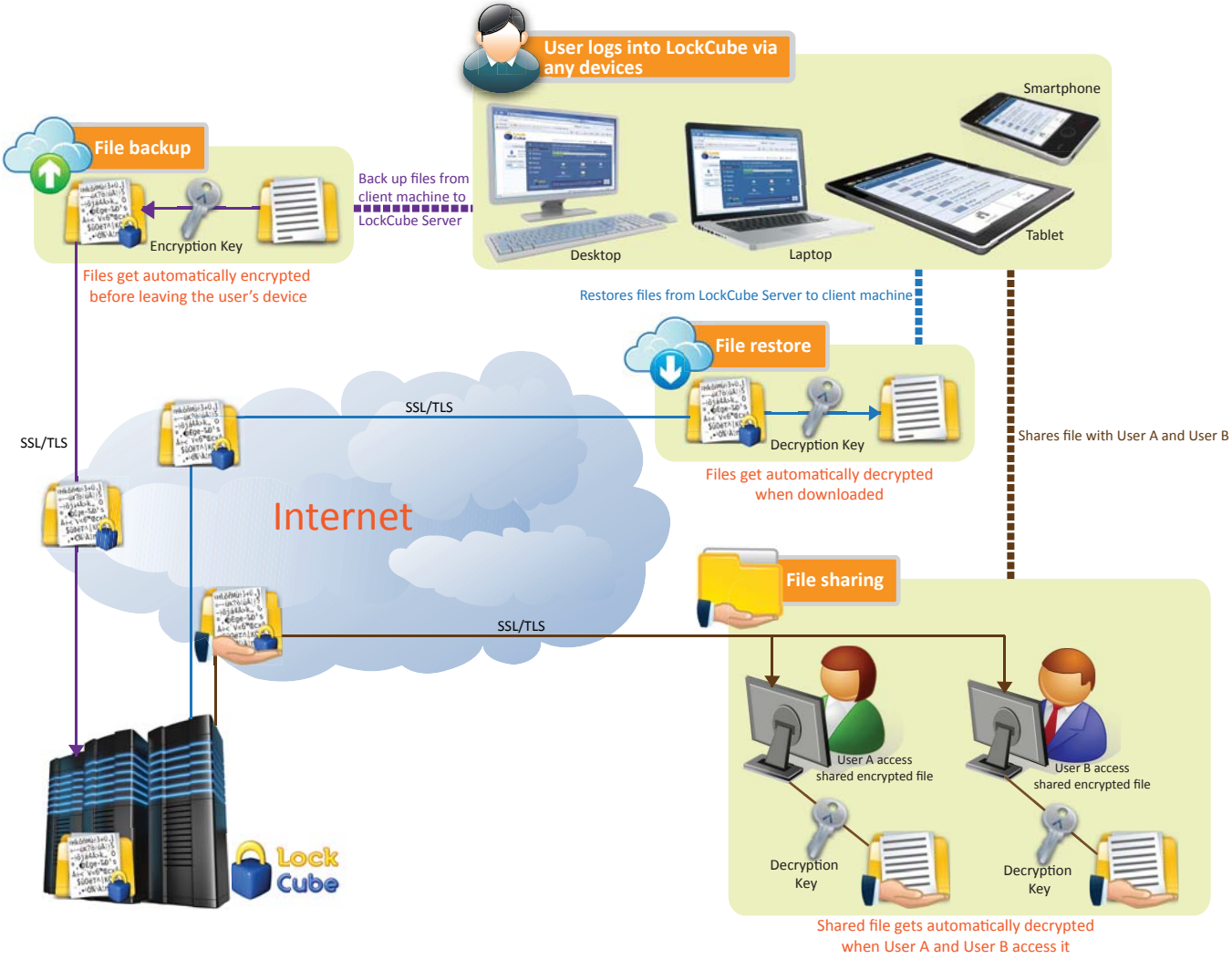
On the other hand, many other cloud storage providers, using a single server encryption key, may claim to impose stringent policy to restrain their internal staff from accessing the users' data. But human is the weakest link in data security. Any of their disgruntled employees can simply ignore this policy and choose to sabotage the users' data.

Since only authorized users safe-keep their own encryption key, there is no way any insider, sniffer and hacker can compromise the security of the user's data stored at the LockCube cloud storage. Even when a government subpoena orders the surrender of the user's data, it will only expose files with unreadable content.

2) Two Layers of Security

Like all the other cloud storage operators, LockCube secures the network transmission between the user machine and LockCube server with SSL/TLS (Secure Socket Layer/Transport Layer Security) technology. But the difference is LockCube uses SecureAge's proprietary SSL VPN solution to protect the network transmission.

How Does LockCube Work?



SecureAge SSL VPN secures all remote access to the network by using SSL as the underlying security protocol to prevent access by unauthorized users. SSL enables secure HTTPS sessions by securing data above the transport layer without interfering with the lower layer network services.

But SSL only protects the network transmission and the data in motion is still vulnerable to potential sniffers using man-in-the-middle attacks. Hence, LockCube fortifies the security by providing another layer of protection - data encryption based on SecureAge's proprietary 3P (Proactive, Persistent and Pervasive) technology. With 3P technology, files get automatically encrypted at the client machine, remain continuously encrypted before, during and after they travel over the Internet and even when residing at the LockCube server. In short, 3P technology provides end-to-end data protection that forbids any unauthorized intermediary party from accessing the data.

LockCube's two layers of security give users a complete peace of mind knowing that it will be a more secured storage option than their own local network storage as it fully protects user's data against malicious attacks.

LockCube Infrastructure

3) Encryption at File-level – Secures Data in Motion and at Rest

LockCube leverages on AES (Advanced Encryption Standard) to encrypt each file with 256-bit unique session key. 256-bit AES is the strongest encryption standard in the world today against brute-force attack. It is certified to be used for protecting secret level data by the US government and 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 $3x10^{51}$ years to exhaust the 256-bit key space.'

Unlike other cloud storage operators, LockCube provides file-level encryption that encrypts individual file with the user's encryption key at the client machine. These files, when accessed, will be decrypted automatically via the authorized user's corresponding decryption key. Since individual file remains persistently encrypted before, during and after travelling over the Internet, there is no way any hacker, sniffer and insider can access the encrypted files without the user's decryption key.

Many other cloud storage operators also claim that they provide data encryption to secure user's data. Before jumping straight into their service, it is advisable to always step back and truly study their security architecture. In fact, most of them encrypt the data only at the server via full disk encryption. Full disk encryption uses the same encryption key to encrypt the entire disk or server but not the individual file. Once the system has started up, it can read every single file as plain data. Hence, full disk encryption is like a bank vault with the door wide open, and once the users' data travel out of this bank vault, it will be unprotected and vulnerable to intruder attacks. It is an adequate protection for laptop and portable storage device when they are lost. But it is definitely not a foolproof data protection in the cloud since any of the cloud storage operator's employees and hackers can easily access the user's data.

3) On-the-fly Encryption - Automatic and Transparent

LockCube enables automatic data encryption and decryption without a user's conscious effort to manually encrypt and decrypt every single file. The data encryption and decryption process is so transparent that the users are not even aware of it. It is as if each and every data is armoured with an invisible cloak of encryption that does not disrupt a user's routine access to the data in LockCube cloud storage. Acknowledging that human is the weakest link in data security, sophisticated security technologies are incorporated into LockCube to provide users a secure but convenient mean of accessing the data without requiring their conscious involvement in protecting their data.

5) Mobile Device Data Encryption

LockCube provides LockCube App for mobile device to allow users to securely store and access any files in the cloud with any mobile device like Android smartphone, Android tablet, iPhone and iPad. It leverages on 256-bit AES encryption and TLS (Transport Layer Security) technology to securely upload and download any files (such as Microsoft Office documents, PDFs, Contacts, videos, photos and songs) anytime and anywhere.

During any upload, the data are automatically encrypted before leaving the mobile device and remain continuously encrypted as they transmit over the Internet right up to the LockCube server. Likewise, when the data is downloaded from the LockCube server to the mobile device, the data remain encrypted on the smartphone or tablet repositories. The data will be decrypted only when user access them via LockCube App for mobile device.

This is known as end-to-end security technology that ensures only authorized users with the right encryption key are privy to the content of the data. Any intruder or trespasser will not have an avenue to sniff for valuable

data around the public network, from the cloud storage or from the mobile device. Therefore, users no longer have to worry about other people accessing their sensitive data when they lost their mobile device.

6) Flexible Customization

SecureAge Technology has accumulated years of experience in customizing additional security capabilities for large enterprises, particularly for the government. We can custom-built additional security features into LockCube in order to meet your corporate policies and security requirements. We provide the option of incorporating two-factor authentication into LockCube. So apart from the usual login and encryption authentication, companies can also provide a second layer of authentication via either mobile phones or smart card or USB token.

Key Features

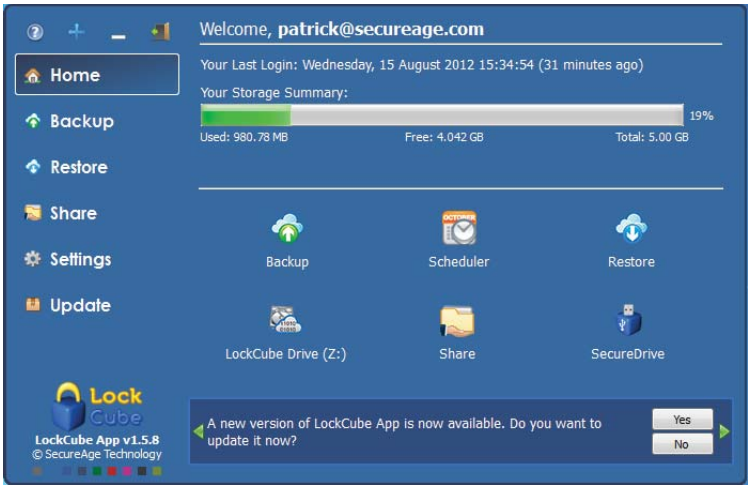
To start using LockCube, users need to download a LockCube App via Java applet. LockCube App offers many useful functions like backup, restore, share and LockCube account and session management.

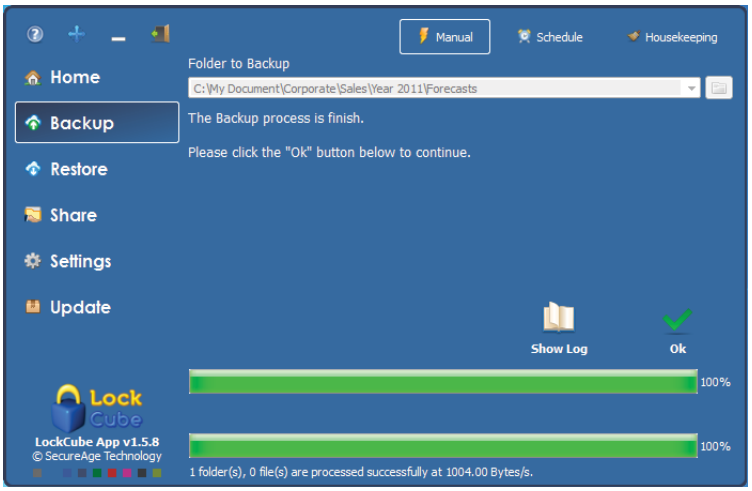
1) A Total Backup Solution with In-file Delta Technology

LockCube comes with a powerful backup functionality that prevents data loss and helps enterprises to fulfil their disaster recovery and business continuity plan. It supports both manual and scheduler options. Scheduler gives users the flexibility of defining a recurring backup date and time that will not disrupt their work routines.

LockCube enables a highly efficient incremental backup of voluminous files by using in-file delta technology. During the backup process, the in-file delta technology will check and compare the entire backup files with those stored in the cloud storage. It will then identify and automatically backup only those modified data within a file but not the entire file. Hence, it reduces subsequent backup time and network bandwidth usage significantly. Users, who have access to high speed fibre network will get the most benefits out of this smart technology. They can enjoy daily backup of huge data size of up to 500 GB (Gigabytes) at a very high speed.

LockCube also caters for data backup with unlimited versioning using in-file delta technology. The smart versioning feature supports time-stamping capability that creates versioning of backup folders by specific date and time. It allows users to salvage the original file even when the current version is corrupted or accidentally deleted. It also saves the user's storage space since the unmodified files are not replicated.



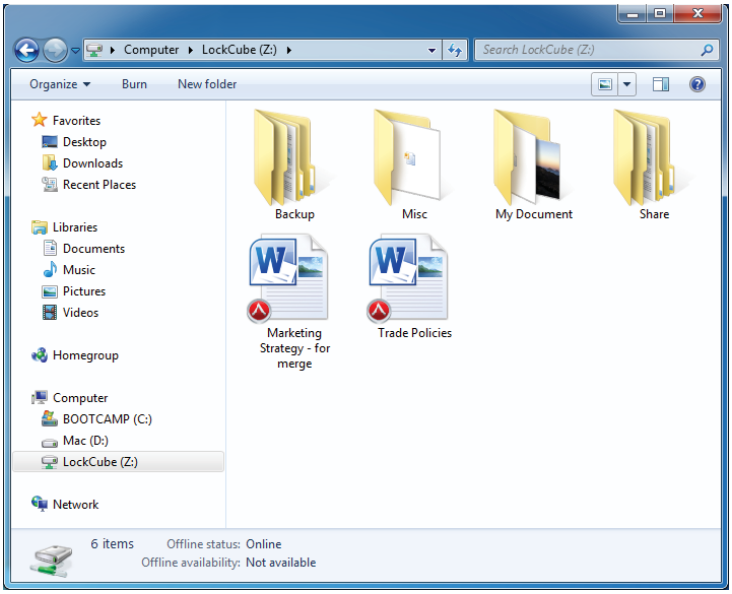


Key Features

2) LockCube as a Network Access Storage (NAS)

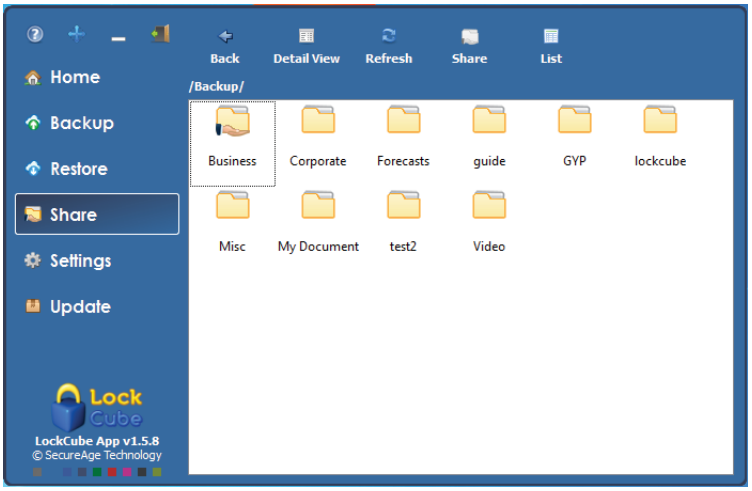
LockCube attaches the cloud storage to the user's machine as a network drive known as LockCube drive (usually Z:\). It works like a normal NAS drive that provides users with a direct access mechanism to their data in LockCube cloud storage. Users can view their files using file explorer, drag and drop their files for copying, using any application to access their files directly, and even execute program stored on LockCube cloud storage. In short, it gives users the convenience to store, open, edit, save, copy and paste any file just like a computer local drive.

Since editing and saving of the files are done directly on the LockCube drive, traces of temporary files will only be created on this LockCube drive and not on the computer local drive. Hence, users do not have to worry about leaving trails of sensitive data in their computer.



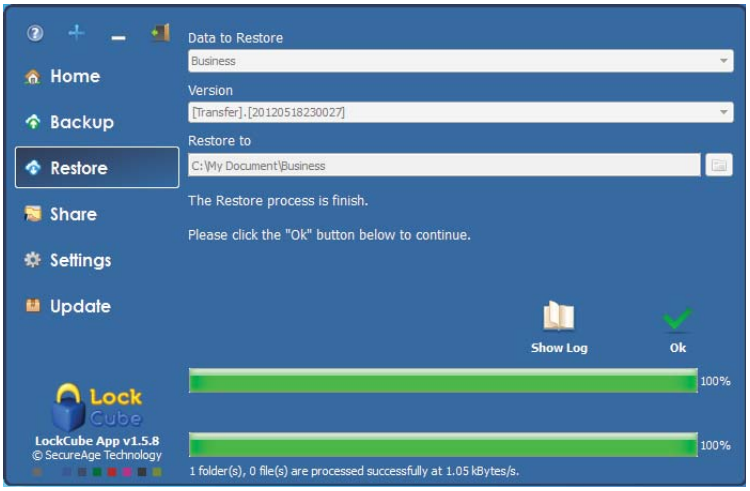
3) Secure File Sharing

LockCube is built with a sophisticated PKI based technology that is transparent to the end users. It uses RSA public key cryptography to enable a user to securely share file with his/her designated recipient(s). A file, when shared, is encrypted specifically for the chosen recipient(s). Only the authorized recipient(s) can decrypt the shared file with their corresponding decryption key.



4) Restores any File Securely

LockCube allows users to restore their files securely from the LockCube cloud storage to their client machine. This is an extremely useful feature for users to recover all their critical data when their computer hard disks crash, when their handheld devices are lost, or when disasters strike. During the restoration process, files get automatically decrypted via the user's corresponding decryption key on their local machine. The entire decryption process is seamless and invisible to the users.



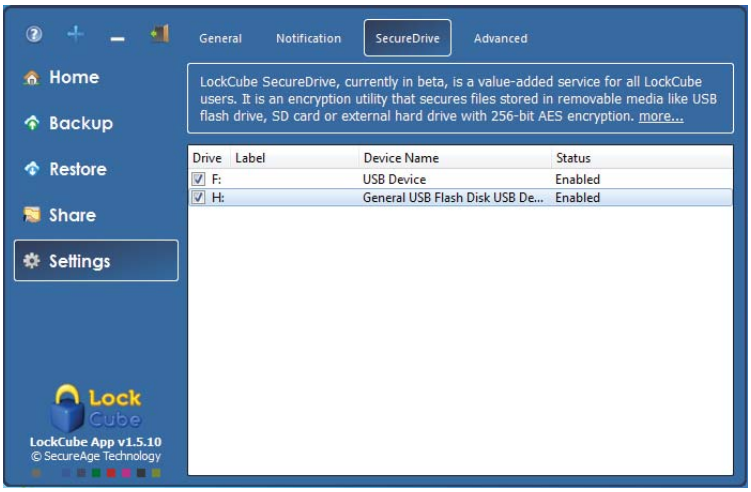
Technical Features

5) SecureDrive – An encryption Utility

LockCube is the world's first cloud storage service to provide an encryption utility, SecureDrive. SecureDrive is a value-added option for users to either rapidly backup voluminous data or promptly restore critical data during disaster recovery via a removable media (eg USB flash drive and external hard disk), with the help of the LockCube Team. It uses 256-bit AES to automatically encrypt/decrypt files with user's encryption/decryption key. Hence, users will have peace of mind knowing that the LockCube Team, when performing file backup or restore, is unable to view the encrypted files without the user's decryption key.

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. The LockCube Team will then help users to copy the encrypted files from the removable media directly to LockCube cloud storage.

SecureDrive also allows users to salvage their critical data. The LockCube Team helps users to restore all encrypted files from LockCube cloud storage to user's removable media. The user will, in turn, use Secure-Drive to copy and decrypt the encrypted files from the removable media back to their local hard drive or file server.



Technical Features

- Military grade security implementation
- 256-bit AES data encryption
- Unique session key for each encrypted files
- Full RSA public key encryption support
- Master encryption key is owned by the user and not accessible by the server
- SSL VPN tunnel between user machine and LockCube server for double layer security protection
- A total backup solution that provides secure remote data backup support
- Unlimited versioning of backup data with file level deduplication support
- Secure disk mounting of LockCube Storage as network attached storage (NAS)
- Mobile support for iOS and Android devices
- Easy access to user's cloud data using web, mobile device, restore tool and direct disk access
- Optional direct access service to LockCube storage server for quick backup and restore operations
- Optional 2FA authentication support

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.