SecureData for Cloud Computing

SecureData is the ideal cloud data security solution that prevents data leakages by continuously protecting user data at rest and on the move. It is an end-to-end data protection solution that single-handedly safeguards organizations' critical information without having to combine a host of different solutions. Its unified policy can be configured and imposed to protect sensitive data from being compromised regardless of where the data is stored; be it in local hard drive, network file server, tape backups and so on.

How does SecureData works?

1. 3P Technology

The basic design principle of SecureData is built on 3P (Proactive, Pervasive and Persistent) technology to provide transparent encryption of any data files, which will remain encrypted, whether at rest, in-transit or in any storage systems. It prevents anyone sniffing the network from obtaining any useful information.

Proactive
Data is automatically and transparently encrypted from the instant it is first created. Users do not have to consciously remember to encrypt data that the system is processing.

Pervasive
Data will remain protected when it is stored in any storage media like local hard drives, external hard disks, network file servers, tape backups and cloud storage. Any unauthorized copying of the sensitive documents from a machine or fileserver will only expose encrypted data file and the risk of sensitive information leaking is thus mitigated.

Persistent
The data will be securely encrypted before leaving the client machine and remains continuously encrypted as it travels over the network to the server.

2. Data Protection for Cloud Storage

Organizations that store sensitive data in the cloud storage should implement SecureData because its 3P technology protects their data from possible insider attacks by cloud operator and network traffic sniffers.

Any data uploaded to the cloud storage will be automatically encrypted before leaving the client machine and will remain encrypted as it travels from the Internet to the cloud server. Any attempts by network traffic sniffers and the cloud operator to steal this data will only expose encrypted data that cannot be deciphered without the user encryption key.

3. Data Protection for Cloud Computing

Similarly, organizations that are running application in the cloud should install SecureData to securely protect data that is residing on their Virtual Machine (VM) server. The data will then stay protected when stored in the VM and cloud storage and continue to be protected when travelling between the VM servers and the cloud storage.

Since the data is always encrypted in the cloud computing environment, there is no way the cloud operator is able to decrypt it without proper encryption key. Hence, any insiders from the cloud operator will not be able to see all your confidential data even when they are managing, moving, copying, backing up, or inspecting them. This gives user peace of mind to leverage on the affordability and scalability of the cloud infrastructure without compromising the security and privacy of their sensitive data.

4. Security Architectures

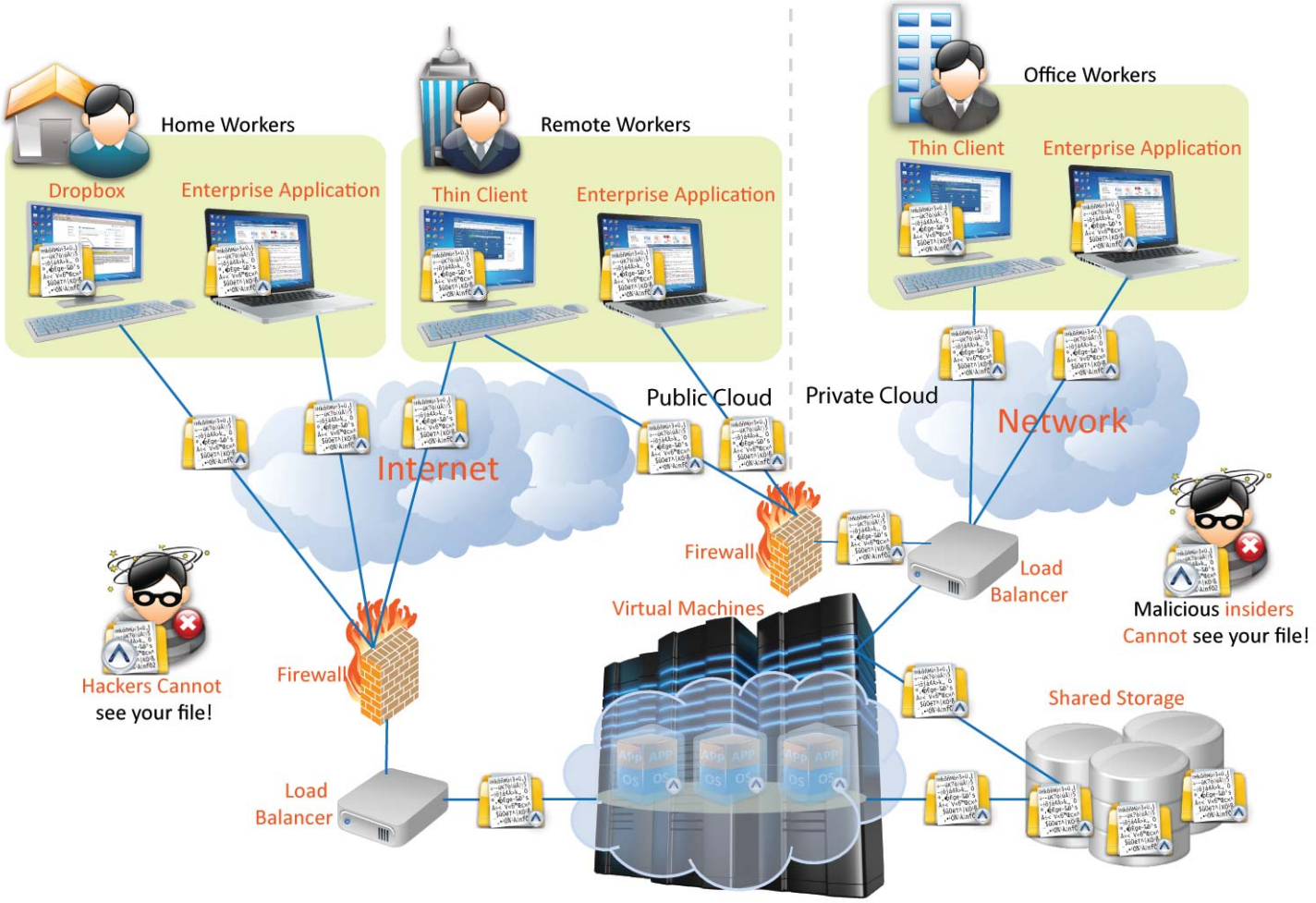
SecureData encryption is based on the strongest AES algorithm with each data file protected by a different randomly generated 256-bit AES session key. The session key is in turn protected by the user's RSA public key with key strength of 1024, 2048, 4096 or

higher bit length. Advanced user could also opt for Elliptic Curve (ECC) public key system instead of RSA to improve the cryptographic efficiency. The usage of public key cryptography also allows sensitive data files to be easily shared by any dynamic group of authorized users without having to put in place a complex key management system.

The user's public and private keys can be stored on any PKCS#11-compliance smart card, USB token or HSM to provide strong two factor protection. These two factor authentication devices are located in user's environment, away from the cloud infrastructure so that the user can retain control of which cloud server can access the key when performing the data encryption and decryption operations.

5. Integrated Defence: 3P Technology, Application Whitelisting and Application Binding

Apart from 3P encryption engine, SecureData also uniquely combines with two other security components, Application Whitelisting and Application Binding. These three security components, when tightly integrated, will provide a highly secure environment to protect sensitive user data from any accidental or intentional leakages. Organizations can thus increase operational efficiencies and achieve comprehensive protection in the face of sophisticated Advanced Persistent Threats, low level rootkit, zero-day attack, anti-malware disabler and other malwares.



Need More Information?

Sales: biz@secureage.com
Public Relations / Marketing: pr@secureage.com
General Enquiry: contactus@secureage.com
Technical Support: support@secureage.com

www.secureage.com
www.lockcube.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.