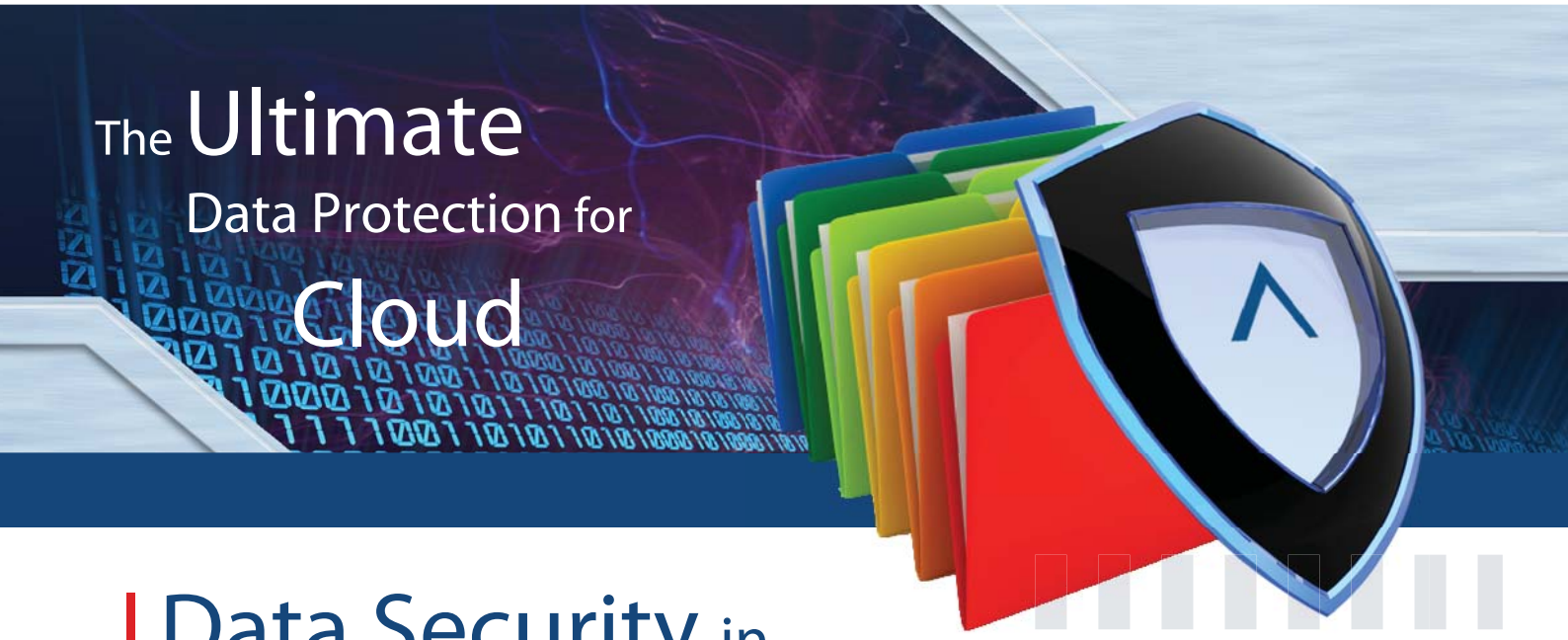
SecureAge



Data Security in the Cloud

SecureData
Whitepaper

Cloud Data Security

Why is Data Security in the Cloud Necessary?

Many surveys have cited data security as organizations' prime concern when embarking on cloud computing services. News on detrimental data losses and leakages are also frequently being reported, like government agencies being compromised in Shady RAT attack, Sony and Sega losing their users' personal and financial information, and IT security companies like RSA having their two-factor authentication token secret compromised by hackers. Even cloud service providers like Dropbox could accidentally allow anyone to access any user's account without the user's knowledge. This would potentially lead to massive data breaches which are beyond the user's control. How can we prevent such data breaches?

To fortify the security for cloud computing, most organizations adopt standard enterprise security solutions like firewall, IPS and anti-virus. Since users can now access cloud services from anywhere in the world, some organizations may implement strong user authentication and access control solutions as a defense against identity fraud. Unfortunately, these solutions do not really protect the user's data in the cloud.

Security measures like full disk encryption, DLP and USB port control are most commonly adopted by enterprises to secure user data. But are these good enough measures to truly secure data in the cloud? Such solutions are not effective especially for systems that are up and running all the time. They also cannot protect user data against insider attacks. However, the insiders in this case are no longer your own employees. In fact, you need to be more wary of the employees from the cloud service providers who are operating your compute and storage servers. There is no way you will know who actually have direct access to your compute and storage servers. There is no way you can trust or even prevent them from accessing and leaking your sensitive information.

How can we prevent data breaches, data loss and data leakages?

A robust data protection solution must be able to secure data for both enterprise end-points and computer servers running in the cloud. This is made possible with an end-to-end data protection solution, SecureAge SecureData. SecureData single-handedly safeguards organizations' critical information and stops data leakages from different channels without having to combine a host of different solutions. It entails a unified policy which can be configured and imposed to protect sensitive data from being compromised regardless of where the data is stored - be it in the local hard drive, network file server, tape backups and so on.

How does SecureData works?

1) 3P Encryption Technology

The basic design principle of SecureData is built on 3P (Proactive, Pervasive and Persistent) encryption technology to provide transparent encryption of any data files, which will remain encrypted, whether at rest, in-transit or in any storage media.

Proactive – All data files are automatically encrypted when they are created, edited, moved, or copied to any local, external or network storage devices based on pre-defined policy. It is so seamless that users do not have to consciously and manually encrypt the data.

Pervasive – All data files remain encrypted when they are stored in any storage media like local hard drive, external hard disk, USB flash drive, network file server, tape backups and even cloud storage. Hence, SecureData transparently ensures all important documents and data files are stored in encrypted format without changing the way the users make use of their computers. Any unauthorized copying of the sensitive documents from a machine or fileserver will only expose encrypted data files and the risk of sensitive information leaking is thus mitigated.

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

In short, the end-to-end architecture of SecureData is built on the 3P encryption technology that prevents anyone sniffing the network from obtaining any useful information.

2) Data Protection for Cloud Storage

Organizations that store sensitive data in the cloud storage should implement SecureData because its 3P encryption technology protects their data from possible insider attacks by the cloud operator and network traffic sniffer. Any data files, when being uploaded to the cloud storage, will be automatically encrypted before leaving the client machine and will remain encrypted as they travel all the way from the Internet to the cloud server. Hence, any attempts by the network traffic sniffers and the cloud operator to steal such information will only expose encrypted data files that can only be deciphered with the user encryption key.

3) Data Protection for Cloud Computing

Similarly, organizations that are running applications in the cloud should install SecureData to securely protect data that is residing on the Virtual Machine (VM) server. It will stay protected when stored in the cloud storage and continue to be protected when travelling between the VM server and the cloud storage. Most of the time, the data will remain encrypted when at rest or on-the-move. But it will only appear as plain data when it is processed in memory by the server applications.

Since the data is always encrypted in the cloud computing environment, there is no way the cloud operator is able to decrypt it without the 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 it. 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-compliant smart card, USB token or HSM to provide strong two factor protection. These two factor authentication devices are located in the 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) Data Access Audit Log

Besides protecting data by encryption, SecureData also provides a complete data access audit log. It can be configured to provide different levels of detail on data access entries to fit the user requirements. The audit trail could provide detailed information of every file being accessed by different applications, moving of information to external devices, file ownership information, and blocked operations. These logs can be automatically uploaded to the SecureAge central management server to provide a consolidated view of user activities. Entries pertaining to blocked application execution or abnormal user data access activities can help the system adminstrator to quickly identify potential threats that are happening in the enterprise systems.

6) Data Protection Against APT, rootkit, zero-day attack and anti-malware disabler

What about malware? Can it steal your data even when the data is encrypted? Unfortunately, malware, running in a system with transparent encryption, can access all the data files and then send them out in plain via proprietary network protocol to the attacker's server. Malware and especially Advanced Persistent Threats (APT), frequently target company servers, including those that run in the Cloud in order to steal sensitive corporate information.

In order to prevent such attacks, SecureData is bundled with two anti-malware modules: application whitelisting and application binding. Application whitelisting is an anti-malware engine that allows only trusted applications to run in an operating system. All unknown applications are automatically considered not trusted and will not be allowed to run in the system. Consequently, malware executables will be unable to run without authorization.

a) Threat of Malware

However, application whitelisting on its own cannot prevent all malware like zero-day attacks. A zero-day attack can infiltrate the system easily with just a document containing malicious code. When such a document is loaded by a trusted application, the malicious code can infect the trusted application process in memory. Such attacks could be carried out by sending the document to a user via email or over a web link.

Another form of malware that can evade detection by application whitelisting is low level rootkit. Rootkit is usually very stealthy and is able to avoid detection by a standard anti-malware engine. Low level rootkits are loaded during system boot up and normally before the running of the anti-malware engine. Hence, they cannot be detected at load time because the anti-malware engine is not running yet.

Finally, there are 'anti-malware disablers' which can disable a standard commercial anti-malware engine, thus rendering the protection solution ineffective. They then allow attackers to inject additional malware to steal sensitive information from the user machine.

b) Integrated Defense: 3P Encryption Engine, Applica -tion Whitelisting and Application Binding:

SecureData combines the 3P encryption engine with the application whitelisting and application binding engines. Together, they provide an integrated defense that can effectively prevent rootkits and anti-malware disablers from causing any harm to user sensitive data.

A low level rootkit stays at very low layers in the operating system stack. It can read the data without passing it through the SecureData engine to avoid detection. However, the data is encrypted and will appear as garbage when received by the rootkit. In order for the rootkit to read the data properly, it will need to send the data through the

SecureData Features

SecureData engine. But in this case, the request will pass through the application whitelisting engine as well and will automatically be blocked since the rootkit is not a trusted application.

For the anti-malware disabler, if it disables the SecureData application whitelisting engine, it will also disable the SecureData encryption engine. Consequently, all the malware in the system can no longer access the plain data because there is no longer a decryption engine running in the system. Hence, the integrated defense of SecureData can effectively prevent low level rootkits and anti-malware disablers from compromising sensitive user data.

What about zero-day attacks? This is where the Application Binding feature of SecureData comes into play. Application binding allows users to specify rules that bind specific data to specific applications. The flexible rule system allows users to configure their systems based on their own security risk matrix. One generic application binding rule is to create an application sandbox for high risk applications like web browsers so that even when these applications are injected with malicious code, they cannot compromise sensitive user data in the system. Another control using the application binding rule is to create a data sandbox which bind sensitive data to a specific application. For instance, one can configure all Microsoft Word documents (*.doc, *.docx) to be accessible only by the Microsoft Word program. In this case, other applications that are compromised by a zero-day attack will not be able to access the Word documents. Hence, zero-day attacks can be fully mitigated without affecting the system functions, and security of sensitive data can be protected.

In SecureData, application whitelisting and application binding also provide detailed log for abnormal activities including all unauthorized execution of applications (application whitelisting) and blocked access to data files by an application (application binding). Such log entries should immediately raise an alarm to the users that their systems are probably under attack and urgent action should be taken to prevent malware or attackers from inflicting more damage on their systems.

Highlights of SecureData Features

1. Protects Data Privacy

- Complete and automatic file encryption, including all temporary files and system page file.
- End-to-end data encryption with data remaining encrypted when transferred over network.
- Supports multiple users using different keys on a single operating system.
- Supports secure sharing of encrypted data with multiple users.

2. Stops Data Breach

- No change in computer usage by authorized users.
- One-stop transparent encryption for all storage devices.
- Transparently encrypts all documents copied to network file servers and network disks.
- Protection against worms and trojans from stealing sensitive documents.
- Stop unauthorized users and processes from accessing sensitive data.

SecureData Features

3. Protect Against Malware

- Application whitelisting to prevent malware execution.
- Application binding to mitigate the risk of zero-day attacks.
- Integrated defense to prevent low level rootkit and anti-malware disabler.
- Active logging to immediately alert user to system under attack.

4. Achieve Regulatory Compliance

- Payment Card Industry (PCI), Data Security Standard
- Data Privacy Bill (e.g. California SB 1386)
- Protection of Sensitive Agency Info (White House OMB)
- Sarbanes-Oxley(SOX)
- Health Insurance Portability & Accountability Act (HIPPA)
- Gramm-Leach-Bliley Act (GLBA)

5. State-of-the-art Security Solution

- Supports default 256-bit AES and 168-bit triple-DES encryption.
- Supports unlimited key length RSA, DSA, ECDH & ECDSA.

6. Two-Factor Security with Smart Card / USB Token

- PKCS#11 standard compliance.
- Supports smart card, USB token, TPM chip and HSM.
- Supports password protected soft key.

7. Complete PKI Support

- Comprehensive certificate, CRL and OCSP support.
- Multiple user profiles management with unlimited user key history support.
- PKI optimization with local management of peer certificates.
- User created self-signed certificate.

Need More Information?

Sales Enquiry: 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.