

# SecureData Protects the Impossible

## Press Release

### SecureAge Technology Protects Data from Advanced Persistent Threats (APT) and Sophisticated Malware with Newly Released SecureData 5.0

*Innovative 3P Data Protection approach keeps valuable data safe anywhere*

**Singapore, 11 January 2012** – SecureAge Technology today announces SecureData 5.0, a new release that effectively protects data from malicious Advanced Persistent Threats (APT), rootkit, anti-malware disabler and zero-day attacks anywhere, whether those threats are transmitted over the network, or in cloud repositories.

#### SecureData

SecureData is an intelligent, policy-based encryption software that offers a reliable way to prevent unintended data leaks at any points, without the conventional management and user issues often associated with full disk encryption (FDE) methods. SecureData offers a proactive, pervasive and persistent (3P) Data Protection approach which differs from traditional data encryption as it is:

- 1. Proactive:** Smart and automatic encryption of all user data files without user involvement. It removes the weakest link, the end-user, thereby reducing the chances of data loss or leakage due to human error or ignorance.
- 2. Pervasive:** User data files are encrypted in all local, removable and network storage. Conventional data encryption is manually managed and restricted to specific file storage device while SecureData automatically encrypts all files regardless of the file storage system that it is moved to. This ensures that sensitive data cannot be accidentally leaked when they are move to different storage devices like CD/DVD, backup tapes or network storage devices.
- 3. Persistent:** All user data files are encrypted at rest and on the move. Conventional data encryption protects data only when it is within a “container”, e.g. a hard disk, but it does not protect data when it is transmitting from one endpoint to another. SecureData protects data at the file level, not just the “container” of the files. This means that even when data is transmitted from one endpoint to another in the network, the data is encrypted. This protects the data from anyone who is sniffing the network or stealing data from the computer by plugging in a thumb drive. No one can read the encrypted files anywhere except for the one who holds the key.

#### SecureData 5.0

With the release of SecureData 5.0, powerful new features are now available on the SecureAge platform. SecureData 5.0 tightly integrates Application Binding and Application Whitelisting with SecureAge’s 3P Data Protection solution. This single layer of “Integrated Defence” is a powerful and resilient data protection tool to ward off malicious APTs, low level rootkit, zero-day



attacks and anti-malware disabler.

### ***Protection against Rootkit and anti malware disabler***

Currently, Application Whitelisting has emerged to be the key solution to address APT. It creates a list of trusted applications in the user computer system and only these trusted applications are allowed to run in the system. It effectively prevents executable malware from running in the user machine and infecting the machine with more malwares.

However, Application Whitelisting, on its own, is not a fool-proof protection against malware. It is rendered completely ineffective in the face of zero-day attacks and low level rootkits. It does not prevent zero-day attacks from injecting malware code directly into trusted applications during run-time. It is unable to effectively detect rootkits that are staying at very low levels in the operating system and can easily hide from any anti-malware engines including the whitelisting engine. In the worst scenario, deadly and advanced malware can even disable anti-malware engines. This leaves the user system completely defenseless and at the mercy of further execution of deadly malware codes.

But SecureData, with its tightly integrated Application Whitelisting and 3P Data Protection, is able to mitigate low level rootkit and anti-malware disablers. The Application Whitelisting component prevents unauthorized malware from damaging the user's system. The 3P Data Protection, on the other hand, automatically encrypts all user data at rest and on the move in all storage devices and not just in "containers". When these two components are bundled together, the rootkit can still be hidden from the whitelisting engine but the difference is it can only steal encrypted data which is unreadable to the intruders. Hence, sensitive user data is protected since encrypted data is useless when the attacker has no key to decrypt it.

Similarly, when the tightly coupled Application Whitelisting and 3P encryption engine are disabled by malware, the user data will remain encrypted and no malware can access them. Once again, the user's data is securely protected from the malware.

### ***Safeguard data from zero-day attacks***

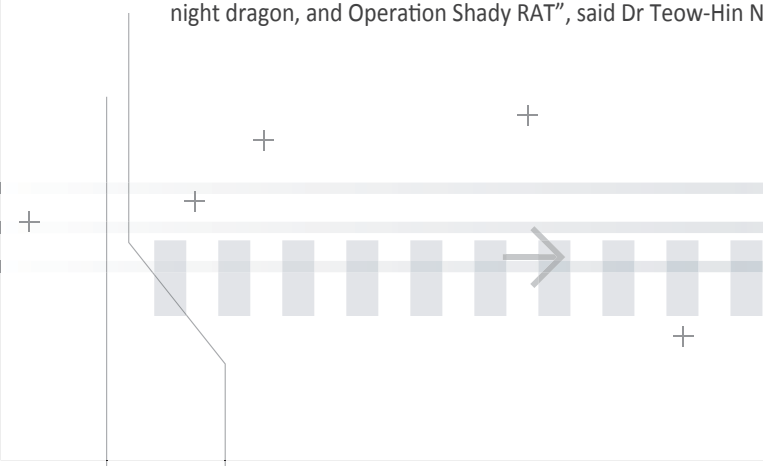
Application Binding, another integrated security component, allows users to define the binding of specific types of data or data paths with specific applications. For example, when the .doc or .docx file format is bound with Microsoft Word application, no other application, except Microsoft Word is able to access this file format. If another application, such as Adobe Reader is compromised by a zero-day malware, the compromised software will not be able to access any Microsoft Word document based on the pre-defined binding rules.

Application Binding can also restrict high risk applications like web browsers from accessing the user data file automatically without the user's consent. To enhance the protection of the underlying user system, a "Sandbox" can be created for the application so that it can read and write files only to a specific user directory, disallowing the potentially compromised software to breach other sensitive documents and system files in the user computer system.

### ***Advanced Persistent Attack Detection***

A detailed log file in SecureData 5.0 records every user activity in executing applications and file access. This provides the IT administrator with an avenue to quickly monitor and track any unusual activity that may potentially be due to the attacks by APT or other malware. Specific log entries like some applications were blocked from execution or from accessing specific data are good indications that the system may have already been compromised by malware.

"APT cannot be completely eradicated due to its sophisticated and persistent nature, but we can definitely mitigate the risks and minimize its damage. SecureData is developed with the ultimate aim to help organizations increase operational efficiencies by protecting their sensitive data against the treacherous malware and prevent disruptive episodes like Operation Aurora, Stuxnet, night dragon, and Operation Shady RAT", said Dr Teow-Hin Ngair, Chief Executive Officer and Founder of SecureAge Technology.



### **Reducing security risks of cloud computing**

By encrypting data at the file level, before it is transmitted over the network, SecureData 5.0 safeguards precious data and reduces security risk, without depending on the security of the storage infrastructure and devices, the integrity or diligence of the system administrator. In cloud computing, SecureData 5.0 ensures that the user data is always protected everywhere it is moved to, and blocks unauthorized malware from accessing the sensitive data even when the system is compromised. In the event that the data is leaked or exposed, it remains encrypted and safe. Only the person who holds the key can access it. With SecureData 5.0, mobile computing and cloud services users are less susceptible to data leaks and losses, which also minimizes the risk of enterprises and government getting astronomical fines due to violation of regulatory requirements like HIPAA and Sarbanes Oxley or serious compromises in national security.

### **Availability**

SecureData 5.0 is available immediately for purchase through SecureAge Technology at [biz@secureage.com](mailto:biz@secureage.com).

## **About SecureAge Technology**

SecureAge Technology is a developer of unique, innovative and military-grade enterprise data security solutions and secure mail solution (for Microsoft Outlook-Exchange and IBM Lotus Notes). Our unmatched and thought-leading 3P (Proactive, Pervasive and Persistent) encryption solutions ensure your precious data is secured – continuously, at rest, on the move, in all storage media and even when using our cloud services. They are now successfully deployed by numerous governments and large enterprises in the Asia Pacific region with each tens of thousands of users. SecureAge also developed the world's first and only secure cloud storage and back-up service LockCube (<https://www.lockcube.com>). Visit <http://www.secureage.com> for more information.

### **Media Contact:**

Priscilla Lim  
[pr@secureage.com](mailto:pr@secureage.com)

Ter Hui Peng  
McGallen & Bolden (for SecureAge Technology)  
[prsg@mccgallen.com](mailto:prsg@mccgallen.com)

## **→ Need More Information?**

**Channel / Sales :** [biz@secureage.com](mailto:biz@secureage.com)  
**Public Relations / Marketing:** [pr@secureage.com](mailto:pr@secureage.com)

**Technical Support:** [support@secureage.com](mailto:support@secureage.com)  
**General Enquiry:** [contactus@secureage.com](mailto:contactus@secureage.com)

[www.secureage.com](http://www.secureage.com)  
[www.lockcube.com](http://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.

