SecureData - Redefining the new era of Anti-APT and Anti-malware Solution

SecureAge

Malware is always one step ahead!

Latest APT (Advanced Persistent Threats) attacks like Gauss, Flame and Stuxnet have once again proven that no business is impenetrable. Malware, whether general or advanced, thrives on ‘sniffing’ out sensitive information in current use or from an archive or shared across networks. It is a malicious threat that attacks not only valuable business information, but also business productivity and profitability. It can bypass whatever security measures in place and even render them completely powerless.

Yet enterprises remain completely oblivious despites of being hounded by last decade of cyber attacks. Most enterprises continue to search for the ‘best’ security solution against malwares by building greater perimeter defense or implementing multiple security layers to sniff and destroy malwares. But malware will always keep reinventing itself to stay one step ahead of security measures.

Cybercriminals’ ability to bypass antivirus protection is a daunting emerging trend. Even the most popular anti-virus solutions can be rendered completely useless. A recent security research has shown that 80% of Carberp infected computers were installed with anti-virus software but was either disabled or crippled by the Carberp malware. *(Source: ZDNet, 27 July 2012)*

Evidently, simply relying on a standard anti-malware solution gives enterprises a false sense of security as it only treats the symptoms but not the cause. Enterprises, very often, need to heavily invest in many other security solutions (like application whitelisting, Intrusion Detection Systems and audit logs) just to stop more symptoms of cyber attacks.

But enterprises can save such tremendous security investments with SecureAge’s one-stop solution, SecureData. *SecureAge SecureData redefines the new era of anti-APT and anti-malware solution.* It is the **ultimate application and data control** against data leakage, APT, rootkit, zero day attack, anti-malware disabler and other general malwares.

SecureAge SecureData – An integrated Application and Data Control (Patent Pending)

SecureAge SecureData is an integrated application and data control solution that detects, mitigates, wards off and kills malwares. It protects user data files from unintended data leaks at any points, saving enterprises from potential millions loss of revenue, brand damage, loss of intellectual property or national security threats.

1. Application Whitelisting

SecureAge SecureData is designed to combat APT and malware, especially the most sophisticated type of APT attacks. It is bundled with a complete Application Whitelisting component that creates a complete list of trusted applications in the user computer system and allows only trusted applications to run. All unknown software, including malware, will be blocked from executing in the system. It effectively blocks executable malware from running in the user machine and even prevents the existing malware from infecting the machine with more malwares.

Unlike SecureAge SecureData, most of the other application whitelisting solutions are unable to detect rootkits that can easily access user data and bypass detection. In the worst scenario, some deadly and advanced malwares may even disable anti-malware and whitelisting engines, leaving the user system completely defenceless and at the mercy of further execution of deadly malware codes.

SecureAge SecureData, on the other hand, tightly integrates Application Whitelisting with 3P (Proactive, Pervasive and Persistent) Data Protection capability. The Application Whitelisting component prevents unauthorized malware from damaging the user system, while the 3P data protection automatically encrypts all user data at rest and in motion. The difference is although rootkit is hidden from the whitelisting engine, it can only steal encrypted data that is useless when there is no key to decrypt it.

Similarly, when the tightly coupled Application Whitelisting and 3P Encryption Engines are disabled by malware, the user data will remain encrypted and no malware can access them. Hence, sensitive user data are protected from malware. Consequently, SecureData does not suffer the same inherent weakness as the other anti-malware solutions which can lead to sensitive data leak when they are disabled or crippled.

2. Application Binding

Application Binding is another application and data control component of SecureAge SecureData. It allows users to define the binding of specific type of data or data path with specific applications. For example, when .doc or .docx file format is bound with Microsoft Word application, no other applications, except Microsoft Word is able to access this file format. If other application like Adobe Reader, is compromised by a zero-day malware, it will not be able to access any Microsoft Word documents.

SecureAge SecureData combines Application Binding with 3P Data Protection capability to provide a complete data access control mechanism. It ensures data can be accessed only by specific authorized users and applications. Hence, sensitive data, regardless of where it goes to, remains securely protected from unauthorized access, malwares or insiders.

Application Binding can also restrict high risk application like web browser from accessing the user data file automatically without the user's consent. To enhance the protection of the underlying user system, an "Application Sandbox" can be created so that the application can read and write files only to a specific user directory.

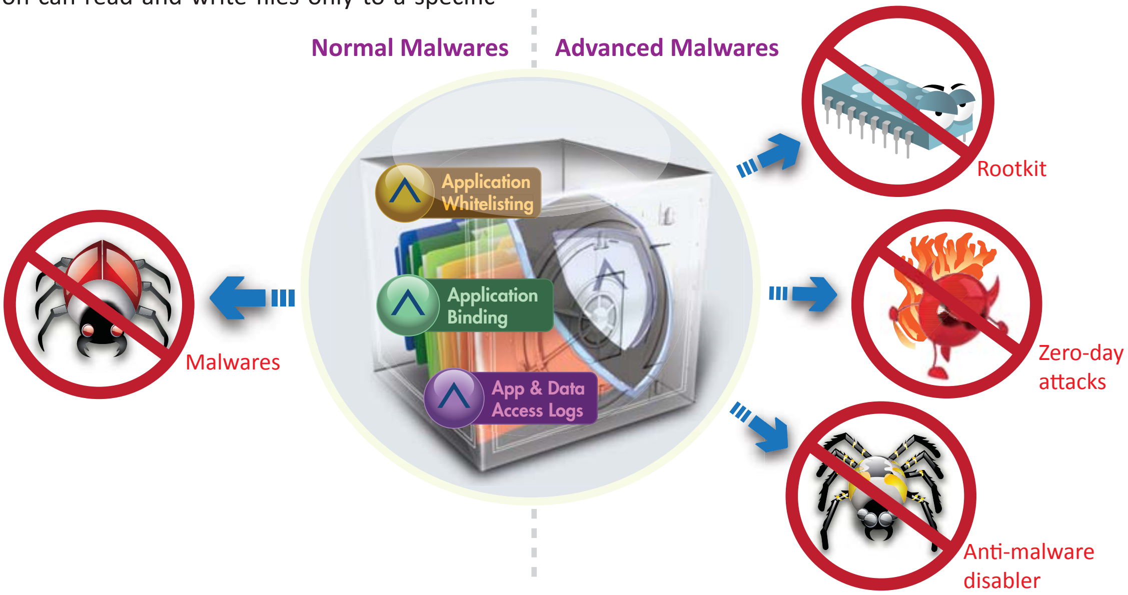
We cannot entirely remove the risk of zero-day attacks. But with Application Binding, the risk of zero-day attacks can be greatly mitigated and the damage can be reduced to the minimum in the worst case.

3. Application and Data Access Logs

SecureAge SecureData also provides a detailed log of application execution and data access activities. Entries pertaining to blocked application execution or abnormal user data access activities can help the system administrator to quickly identify potential threats that are happening in the enterprise systems. This will help to further mitigate the risk from malware and APT by enabling the easy identification of attacks that are in progress.

4. Anti-malware

The anti-malware component of SecureAge SecureData scans, detects and removes any known malware like rootkits, spywares, viruses, Trojans and other malicious codes that infect any user machine. It supports automatic / manual scanning capabilities as well as automatic updates of virus definition list.



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.