The Ultimate Data Protection for Enterprise Servers

SecureAge

SecureData for Enterprise Servers

SecureData, an end-to-end data protection solution, secures critical servers within the enterprise network from data leakages. Without having to combine a host of different solutions, it single-handedly safeguards organizations' sensitive data that is stored on file server, enterprise database, Microsoft SharePoint, proprietary Enterprise App servers, FTP servers and backup tapes. It ensures data stored in such servers to be continuously protected at all time, be it at rest or in motion.

How to protect data in the Enterprise Servers?

1. 3P Technology

SecureData is built on 3P (Proactive, Pervasive and Persistent) technology to protect organizations' mission critical data that is stored in their enterprise servers from potential insider attacks and malwares. Any data stored in the servers will be automatically encrypted and remains continuously encrypted as the data is moved between servers or between server and client machines. Hence, any attempts by network sniffers to steal this data will only expose encrypted content that cannot be deciphered without the system encryption key.

Since the data in the enterprise servers always stays encrypted, there are no ways malicious users and malwares can decrypt it without proper encryption key. To further enhance security, access to certain sensitive data can be restricted by encrypting them with keys belonging to authorized users. This prevents system administrator, who is not the authorized user, from accessing the data. Even if the system administrator's admin privilege has been compromised, users can have peace of mind that security and privacy of their sensitive data remains fully protected.

2. Application Whitelisting

SecureData tightly integrates Application Whitelisting with 3P technology to protect sensitive user's data from normal malwares and advanced malwares like low level rootkit and anti-malware disabler.

Application whitelisting controls the server system to ensure that only "trusted applications" can be executed. All unknown applications, including malwares, will be blocked from running in the systems. Nevertheless, Application Whitelisting, on its own, is unable to detect rootkits that are staying at very low level in the operating system. Deadly and advanced malware can even disable anti-malware engines, leaving the user system completely defenceless and at the mercy of further execution of deadly malware codes. But once it is tightly integrated with 3P technology, it is able to mitigate low level rootkit and anti-malware disabler. The rootkit can still be hidden from the whitelisting engine and both the 3P encryption and whitelisting engines can be disabled, but the sensitive user's data remain encrypted and no malicious malwares can access them.

3. Application Binding

Application Binding, another SecureData's security component, binds specific type of data, files or directories to specific applications. For instance, webpages can only be accessed by the web server and upload processes, and database files can only be accessed by the database server and backup processes. Any attempts by users to copy the files or malwares to modify the files will be blocked. With application binding, even advance zero-day attacks on trusted applications can also be blocked from accessing sensitive system data. Furthermore, application binding could also be used to send encrypted data to application like FTP server and proprietary application servers to ensure that data are automatically transmitted in encrypted format, providing end-to-end data protection.

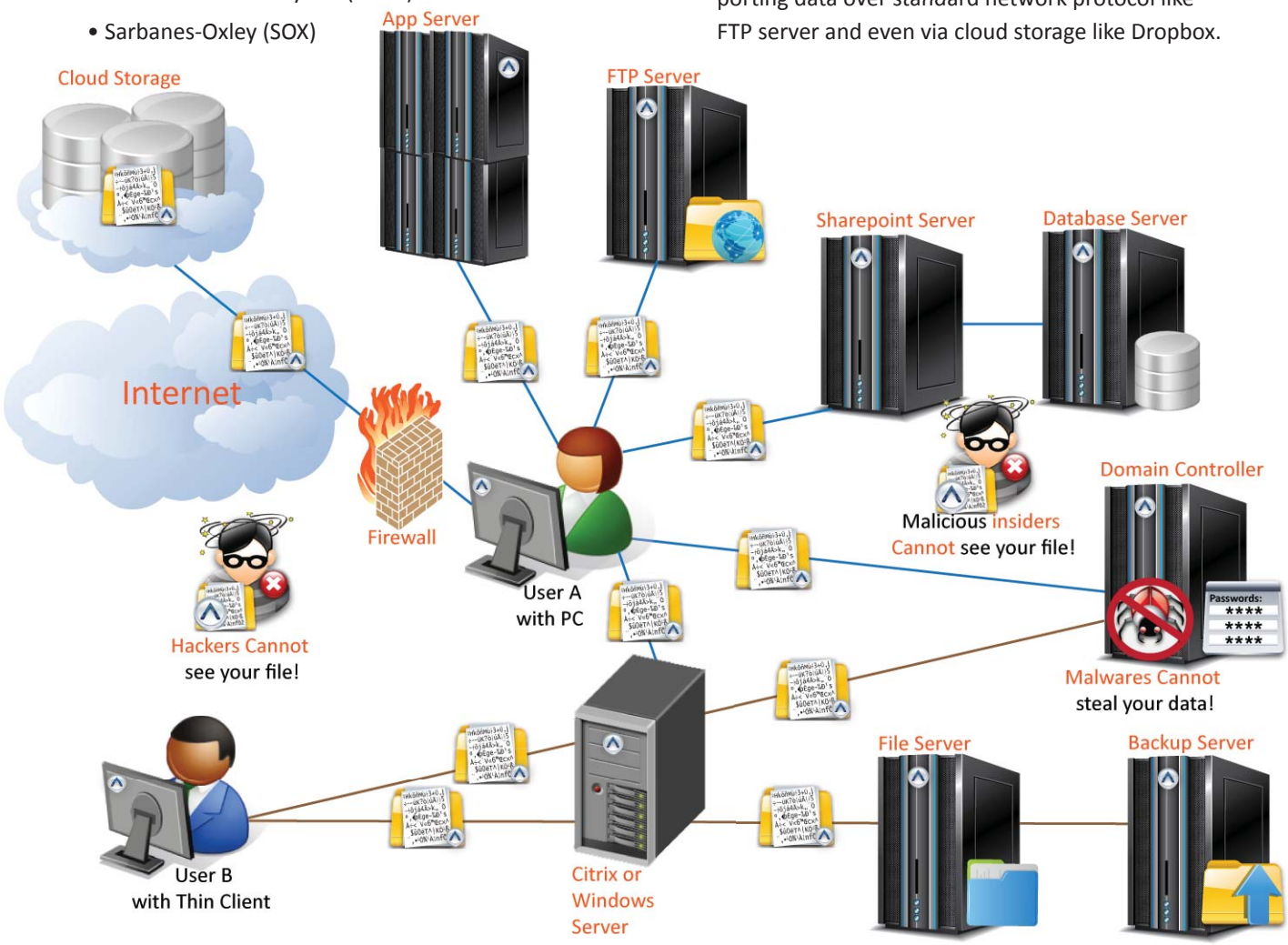
4. Regulatory Compliance

SecureData helps organizations to achieve regulatory compliances like

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

5. Key Benefits

- Ensures all sensitive data stored on file server, enterprise database, SharePoint and proprietary enterprise App servers remain encrypted at all time.
- Ensures sensitive data on tape backup remains encrypted at all time without having to pay for an expensive upgrade.
- Stops advanced malware from compromising your webpages on your web server and user's accounts on the Domain controller.
- Ensures end-to-end data protection when transporting data over standard network protocol like FTP server and even via cloud storage like Dropbox.



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.