Data Sheet

Data Paladin

An Effective and Easy-to-Deploy Solution to Protect Enterprises from Insider Information Theft

Business-critical information and intellectual property stored in standard enterprise file servers are vulnerable to information theft by insiders, which is generally considered the most damaging form of cyber threats in terms of potential financial loss. Moreover, it is difficult to detect and prevent insider theft of confidential information because in many cases the inside attacker had the proper authority to access the stolen information.

Stop unintentional or malicious data leakage in a decentralized network environment.

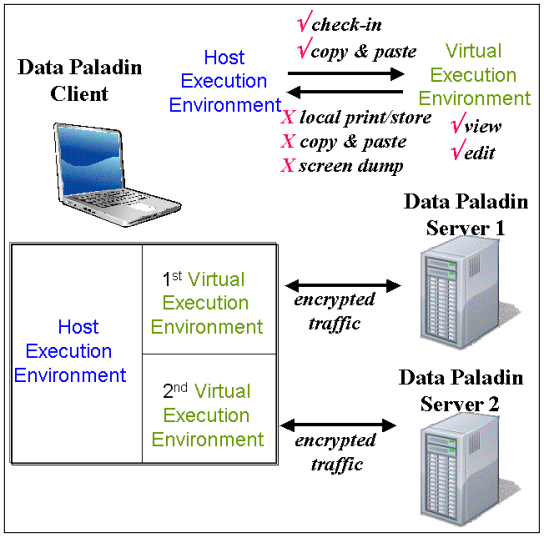
Most existing solutions to the insider information theft problem are based on either sophisticated access control mechanisms or Digital Rights Management (DRM) technologies, both of which have serious limitations in portability and effectiveness. These limitations stem from the fact that it is difficult to embed application-specific access control mechanisms into a general data protection infrastructure that is applicable to a wide variety of file types. Moreover, they are unable to stop information theft by authorized users because there is simply no access control violation when they access the protected information.

Prevent unauthorized:

- Printing
- Emailing
- Screen capturing
- Saving to hard drives or removable devices

of your sensitive data.

Data Paladin is the leading secure file server using OS virtualization technology to guarantee that *even authorized users cannot take out protected files after they are deposited.* Moreover, Data Paladin is able to thwart most information theft attacks without being disruptive to the end users or requiring significant changes to the existing IT infrastructure.



Benefits

- Protects Sensitive Data
- Cost Effective
- Easy to Deploy
- Ease of Use
- Application Agnostic

Recommended Requirements

Data Paladin Server
OS: Win 2003 Server Standard and Enterprise
Hardware: Pentium-IV or better CPU, 512MB

Data Paladin Client
OS: Windows XP

The enabling technology underlying Data Paladin is ***Feather-Weight Virtual Machine*** **(FVM)**, which allows the creation of a virtual execution environment on the user's machine that is isolated from the host execution environment and logically part of the central secure file server. Users view and edit protected files in this isolated virtual execution environment as if the files are stored locally on their machines, but protected files can never be removed from this virtual execution environment and thus logically staying within the control of the central Data Paladin secure file server.

Because of its isolated virtual execution environment architecture, Data Paladin is able to protect an enterprise against information leakage by authorized insiders, regardless of whether the leakage is an unintentional error or a malicious attack. The key features of Data Paladin are:

- **Scalability**: Since document viewer execution is on the local machine, the load on the central server is greatly reduced and a large number of users can be supported concurrently.
- **Ease of deployment**: Authorized users can interact with protected files in exactly the same way as if these files are stored on their local machines, including copy-and-paste, including and viewing attachment in an email, etc.
- **Seamless**: Data Paladin interoperates seamlessly with the user authentication and file access control mechanisms of the underlying operating system, for example, user authentication based on Active Directory credentials and Windows discretionary file access control mechanism.
- **One-way communication:** Clipboard operation such as cut and paste is unidirectional so that no information leakage from a Data Paladin server to a Data Paladin client is possible, but the other direction is allowed.
- **Screen dump protection**: A user machine is forbids screen dumps whenever the user is interacting with a confidential file.

Protect your confidential data, test DP at rether.com/DP or come visit us at rether.com.

Rether Networks Inc.
25 Health Sciences Drive, Suite 206
Stony Brook, NY 11790
Tel: 631.638.1043 Fax: 631.444.8825