Data Sheet

Display-Only File Server (DOFS)

A Revolutionary Secure File Server Technology that Protects Enterprises from Information Theft by Insiders

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

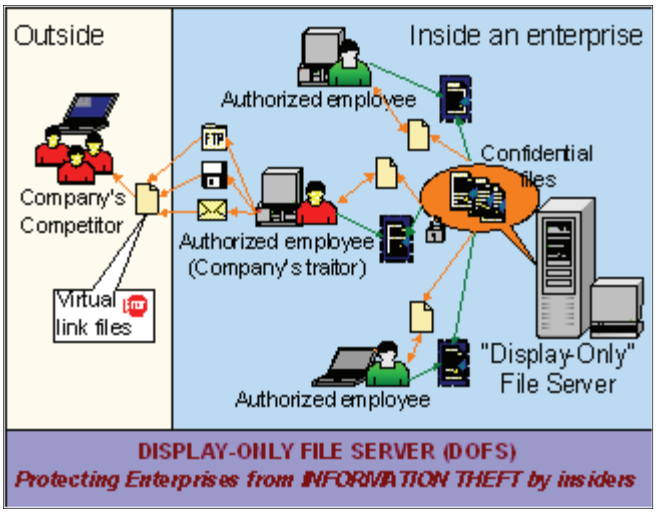
Stop unintentional or malicious data leakage in a centralized network environment.

Most existing solutions are based on either sophisticated access control mechanisms or Digital Rights Management (DRM) technologies, both of which have serious limitations in portability and effectiveness. In general, it is difficult to unify application-specific access control mechanisms into a uniform protection infrastructure that are 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 confidential information is stolen.

Prevents unauthorized:

- Printing
- Emailing
- Screen Capturing
- Saving to hard drive or removable device

of your sensitive data.



Display-Only File Server (DOFS) is the first secure file server that addresses the information theft problem by decoupling "display access" from other types of file access and guaranteeing that *even authorized insiders cannot have access to the bits of confidential files*. Moreover, DOFS 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
- Compliance Audit Trail

Recommended Requirements

DOFS Server

OS: Windows Server 2003 Standard and Enterprise with Terminal Server support, Windows Server 2008 R2 Standard and Enterprise with Terminal Server support

Hardware: Pentium-IV or better CPU, 1 GB RAM for 25+ users, with 15 MB per additional user

Applications: DOFS server program, MS Office Suite, Acrobat Reader, PostScript Viewer, and any application with Terminal Server support

DOFS Client

OS: Windows XP and Windows 7
Hardware: Pentium-IV, 256 RAM
Applications: DOFS client program and Terminal Server Client Access License

The key technology underlying the DOFS architecture is ***transparent remote execution***, which re-directs any operations on protected files to a DOFS server, forwards the display of execution results back to the user machine, and thus ensures that bits of a protected file never leave the DOFS server once it is checked in. At the same time, end users can still interact with confidential files stored in a DOFS server in exactly the same way as if they are stored locally.

Owing to the transparent remote execution architecture, DOFS is able to protect any company against information leakage by authorized insiders, regardless of whether the leakage is an accidental mistake or a malicious attack. In summary, the key features of DOFS include:

- Parts of a confidential file never leave a DOFS server after the file is checked in.
- Authorized users can interact with files containing enterprise confidential information in exactly the same way as if they are working on these files on their local machines, including copy-and-paste, attachment in an email, etc.
- DOFS interoperates seamlessly with the user authentication and file access control mechanisms of the underlying operating system.
- Clipboard operation such as cut and paste is unidirectional so that no information leakage from a DOFS server to a DOFS client is possible, but the other direction is allowed.
- Screen dump on a user machine is disallowed whenever the user is interacting with a confidential file.
- Digital watermarks are embedded into the print out automatically if printing from the secure file server is needed.
- An audit software, Access Tracker, is included with DOFS allowing you to track all DOFS file user activity on your DOFS server. It provides a file audit trail to help with any compliance needs.

Don't wait to protect your sensitive data, try DOFS at rether.com/DOFS or come visit us at www.rether.com

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

rnidofsds1011