



SECLORE FILESECURE

Share with Confidence !



Financial Services

CASE STUDY

Background Of The Organization

The client is one India's leading financial conglomerates, offering end-to-end financial solutions. The products and services offered by the client include commercial banking, stock broking, mutual funds, life insurance and investment banking. The client employs more than 20,000 people, has presence in more than 350 cities across the world and excess of 3.5 million retail and enterprise customers.

Process Before

The client has its 20,000 employees that operate out of multiple locations spread over many cities. All confidential client information as well as internal sales and distribution documents were stored on a central file server. To protect these documents and other information, stringent access control mechanisms were implemented on the files and folders within the central file server. There was also some information which was circulated to different members of the senior management that operated across various locations. Such custom reports were prepared by the MIS department for circulation. All such confidential documents were password protected before circulation.

Issues And Information Leakage Scenarios

While many methods were employed for information security, all were centered around access control of information. In other words, the main focus of the security methods was prevention of unauthorized users gaining access to the documents. However, most of the information leakages were detected to occur when authorized users shared information intentionally or accidentally, with others who may have required not having access to the same. In many cases, information leakages were traced back to ex-employees who had left the organization, but had access to the information when they were part of the organization, and had made copies of the same. All of these had resulted in serious information security compromises, which posed a huge threat to ongoing business and market position of the organization. This called for an in-depth study of the document and information usage in the company to be able to identify a suitable method to address the issues caused due to information leakages.

Need For A Document Usage Control System With Persistent Security

A thorough analysis by the internal information security team identified the need for an information usage control system that would allow:

- Centralized control of rights for documents coming in and going out of the file server
- Granular control of usage rights (view / print / edit /forward) per document
- Usage rights to be persistent i.e. the rights should not be dependent on the location of the information.

- Possibility to modify usage rights for the documents remotely, without the need to re-send the document.
- Document security without the need to have document specific passwords.
- Full audit trail of access and usages of documents whether accessed from within the enterprise network or from outside.

The Seclore Solution

The Seclore FileSecure Solution for file server provided to the client allowed rights protected documents to be shared across the enterprise without the need to manually password protect documents. A central administrator is able to associate rights with each folder on the file server. Documents are protected as soon as they are copied on the folder and the protection is persistent and independent of location. The rights allow specific users, using their windows domain credentials to view, print, edit or forward documents. Dynamic rights management allow the rights to be revoked based on events like resignations and transfers.

Control

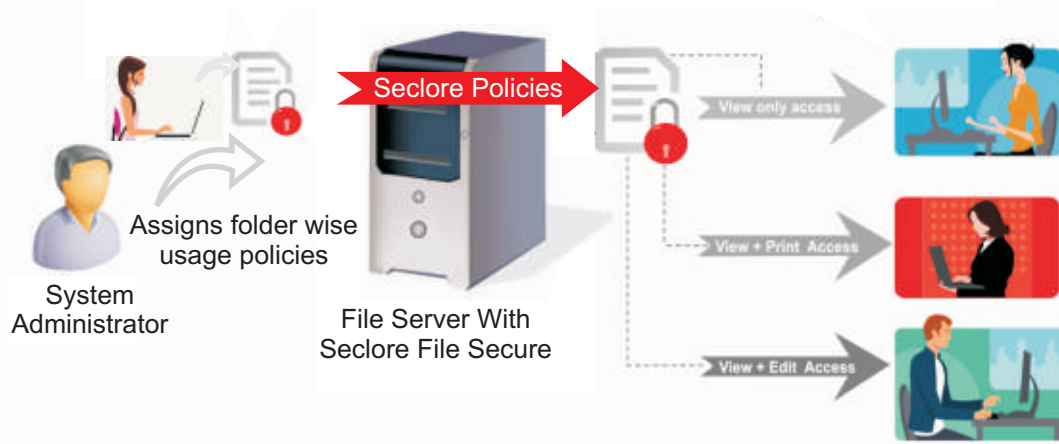
Who: Only specified users with rights associated with the specific folder on the file server

What: Only a specified set of actions, view / edit / print / reclassify for each user

When: Only till the time the specified policy is in force

Where: Only within computers within the domain

Seclore File Secure



Benefits And ROI Drivers

Seclore FileSecure for file Server provided the client with persistent end-to-end control over its information through the life cycle of creation, storage, transmission, usage and destruction. Automated protection of files within the file server as well as administrator controlled rights for each folder meant no change in existing processes and systems. Dynamic rights management allowed for centralized revocation of rights based on status changes.

About Seclore

Incubated and promoted by IIT Bombay, Seclore Technology develops innovative solutions in the area of information usage control. Seclore has achieved industry leadership in the area of information usage control, information rights management, enterprise DRM through its range of products. Some of the largest corporations in financial services, engineering and education use Seclore products for information usage control.



SECLORE

Tel: +91 22 4015 5252

Email: info@seclore.com

Blog: <http://blog.seclore.com>

www.seclore.com