



SECLORE FILESECURE

Share with Confidence !

Manufacturing and R&D

CASE STUDY

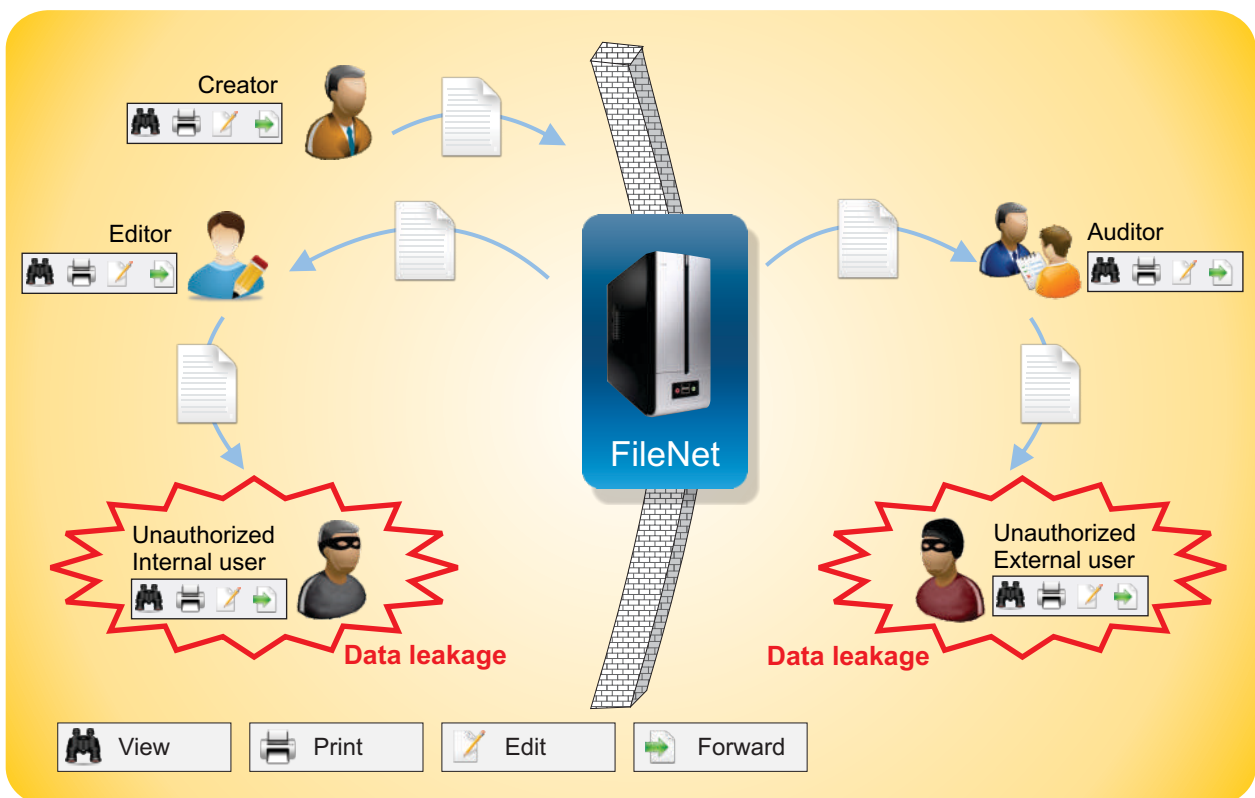
Background Of The Organization

The organization is India's largest paint manufacturing company and ranked among the top ten decorative coatings companies in the world. The company has operations in 17 countries across the world with 23 paint manufacturing facilities, servicing consumers in 65 countries. The organization employs more than 2000 employees and has more than 5 million retail and enterprise customers.

Process Before

In an effort to reduce process cycle times and increase productivity and accountability, the organization has invested in IBM FileNet Electronic Content Management (ECM) system. To enable collaboration to flow freely, access to FileNet is provided to employees and also to some outside business partners (like vendors and independent auditors). To improve productivity, efficiency and interaction, a large number of business processes and associated document handling are automated using FileNet's BPM solution. This has resulted in a lot of confidential information (related to different internal and external business processes) being handled by the FileNet system. To protect this information, stringent process and object store level access control have been implemented in FileNet.

Process Before



Information risk and need for persistent security and usage control around FileNet

All security measures that were implemented prevented unauthorized access to information and documents inside FileNet. However, there were still risks of information breaches from unauthorized distribution of this information outside of FileNet i.e. via emails & removable media.

Some of the key business processes and areas where security breaches were identified are:

- Audit information was stored in FileNet. External auditors were given access to FileNet to audit the organization's books and update them. One of the risks identified was that of this information being misused intentionally or otherwise.
- Documents edited by employee groups should be privy to employees within the group only. However, these documents once downloaded from FileNet found its way to un-intentented audience through various medium like email, removable media, etc.
- Confidential joint venture, partner, vendor agreements are stored in silos within FileNet. Access to these confidential silos was restricted. But, these documents after downloading by authorized users could end up in the wrong hands.
- The organization has selective pricing offered to different vendors depending on their geographic location. This information is stored in FileNet and each vendor has access to their selective pricing only which was enforced by the NDA. However, these “selective” pricing used to circulate across geographies, resulting in a price arbitrage and a cause of worry for the organization.
- Employees constantly downloaded confidential documents from FileNet on their laptops to work on them. These documents suffered from a risk of breach in case employees carried them as a part of “memorabilia” after leaving the organization or lost their laptops.
- Market survey reports containing data about usage and preference of different products are regularly generated and shared. These reports are extremely valuable. These research reports used to land up on competitors desk through unknown sources.
- Transporters upload their fright rates to FileNet so that any branch office and plant can download the freight rate for processing. Different transporters should not have access to other transporters freight rate documents. However, it was noticed that transporters managed to get each others freight rate documents.

- Legal documents stored within FileNet was made accessible to the legal team only, but there was a risk of these sensitive documents finding their way to other un-intended employee and sometimes even competitors.
- The organization has made an International online library in FileNet. Employees from all parts of the world can access this library. The library contains confidential documents like research reports and patents. Though this feature provides convenience to users it also provided an avenue to easy and bulk leakage of information.

Apart from all the above security concerns, there were numerous regulatory and compliance norms that the organization had to adhere to for certification on documents after they are downloaded from the FileNet system.

A thorough analysis identified that the basic problem was that once authorized users download the information from FileNet, FileNet cannot control the information from being viewed, edited, printed, forwarded, etc. Enabling security policies configured in FileNet to be implemented even for information downloaded from FileNet without any change to employees workflow was identified as a key success factor for the deployment of any security system.

The following requirements were identified as key to achieving this:

- The system should be least intrusive with capability to automatically protect document when they are downloaded from FileNet.
- Granular control on usage rights based on the role and task that is assigned to an employee.

E.g.- A simple workflow consisting of a document creator (A) -> document editor (B) -> and document auditor(C) should possibly have the following rights for usage control

User	View Rights	Edit Rights	Print Rights	Distribute Rights	Date Embargo
Creator (A)	✓	✓	✓	✓	X
Editor (B)	✓	✓	X	X	X
Auditor (C)	✓	X	X	X	✓ _(only after a certain date)

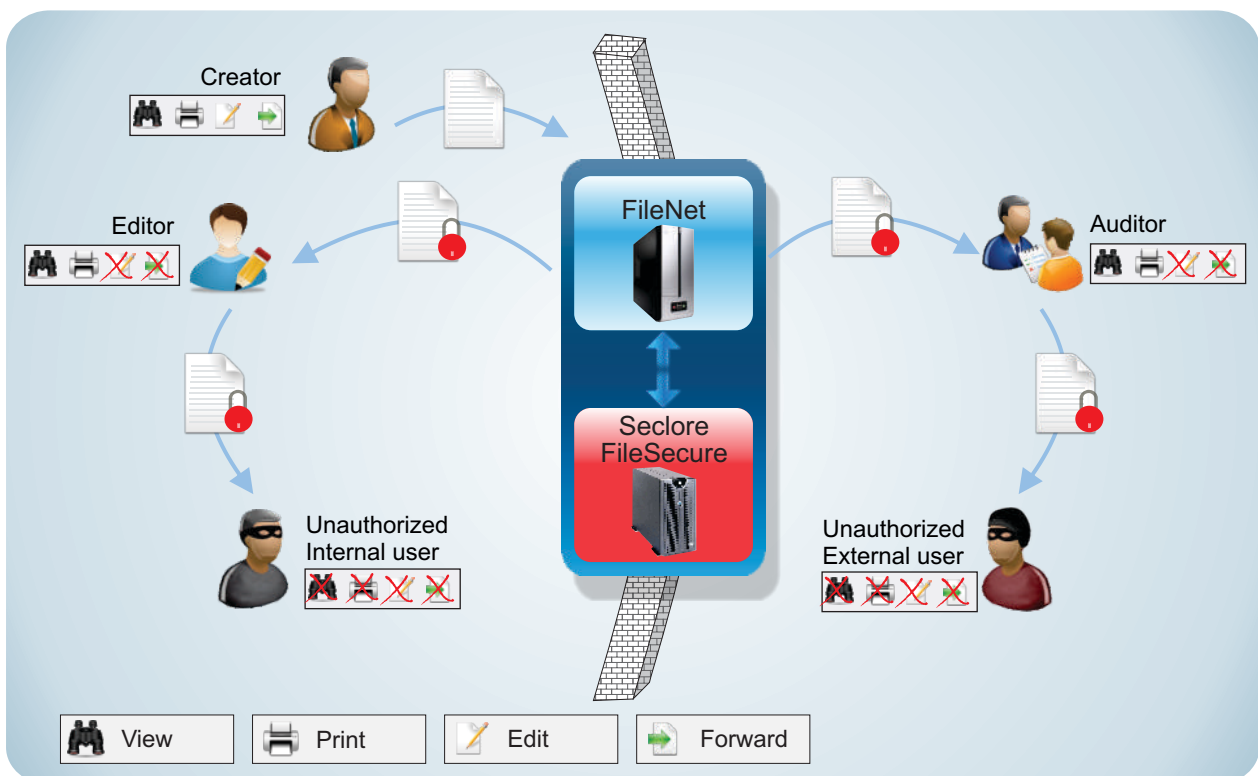
- Persistent end-to-end usage control on information throughout its lifecycle of creation, storage, versioning, updating archival and deletion.
- Complete audit trail of authorized activities and unauthorized attempts performed on the information when it is inside and outside of FileNet for regulatory compliance.
- Ability to modify the usage rights of downloaded information in real time and anytime.

The Seclore FileSecure connector for FileNet

The Seclore FileSecure connector for IBM FileNet enabled the organization to enforce security policies on information even after it has been downloaded from IBM FileNet. With the connector, security policies defined within FileNet extended to information within and outside of FileNet.

The connector would allow FileNet to put usage rights on information before download on to user's computer. The usage rights would define **WHO** (people, groups) could use the document, **WHAT** (view, edit, print, forward, full control) can the person do with the document, **WHEN** (specific dates, time spans) can this be done & from **WHERE** (within the office, at business partner) can the document be used. These usage rights could be given to employees and external users like auditors and vendors depending on their role and responsibility and the current state of FileNet workflow process. Documents could also be "deprecated" as soon as a business process was over, thereby enabling access to documents only when they are required. The "audit trail" feature not only guaranteed compliance to regulatory standards but also helped in doing forensics whenever there was any unauthorized activity on information. The Seclore FileSecure connector also provided "remote control" feature to change the usage rights on documents post download and/or distribution thereby providing complete control of distributed documents.

Process After



Benefits and ROI Drivers

All the above mentioned requirements were directly inherited when Seclore FileSecure connector for FileNet was implemented.

Besides that a few other key benefits which gave exponential ROI were:

- Information security outside of the “walls” of FileNet – Persistent security of information inside and outside of FileNet and even beyond the organization made sure that information breaches don't happen. And because content stored in FileNet has policies applied to it automatically, the content can be distributed safely, locking out access from unauthorized users regardless of how it's distributed outside of FileNet.
- Collaboration – By providing seamless security, Seclore FileSecure enhanced collaboration as information could now be shared with colleagues and business partners without worry.
- “Intrusion-less” security - Documents downloaded from FileNet are automatically encrypted with the correct policy governing their usage, thus enabling easy use of the security system. The use of native applications (like MS Office, Adobe PDF reader etc.) to access protected documents and single sign-on functionality with FileNet meant no change in the existing way of working for users.
- Compliance – Seclore FileSecure's audit trail provided comprehensive tracking of information. This audit trails provided compliance to regulatory frameworks and reduced associated costs.
- Low IT administration overheads – Seclore FileSecure's “integration friendly” API's provided the capability to integrate with existing identity management system, existing storage system and existing web application infrastructure which eventually lowered IT administration overheads.

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