Seclore FileSecure

IBM FileNet and Seclore FileSecure Join Forces to Enable Secure Internal & External Collaboration in a Leading Manufacturing Company

SECLORE

"People leaving our company carried a lot of confidential and significant business information with them on their laptops. Hence, we felt the need to protect our knowhow with strong controls like Seclore FileSecure offers."

~ Director of Information Security

Background Of The Organization

This organization is the second largest chemical manufacturer 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 Seclore FileSecure

In an effort to reduce process cycle times and increase productivity and accountability, the organization had invested in the IBM FileNet Electronic Content Management (ECM) system.

To enable collaboration to flow freely, access to IBM FileNet was 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 were automated using IBM FileNet's BPM capabilities.

IBM FileNet's content and business process management capabilities have enabled the organization to automate and control the flow of confidential information (related to different internal and external business processes). However, once information was downloaded from IBM FileNet and even sent to external partners or internal employees in the course of doing business, it could easily be viewed, forwarded, and exploited by unauthorized users.

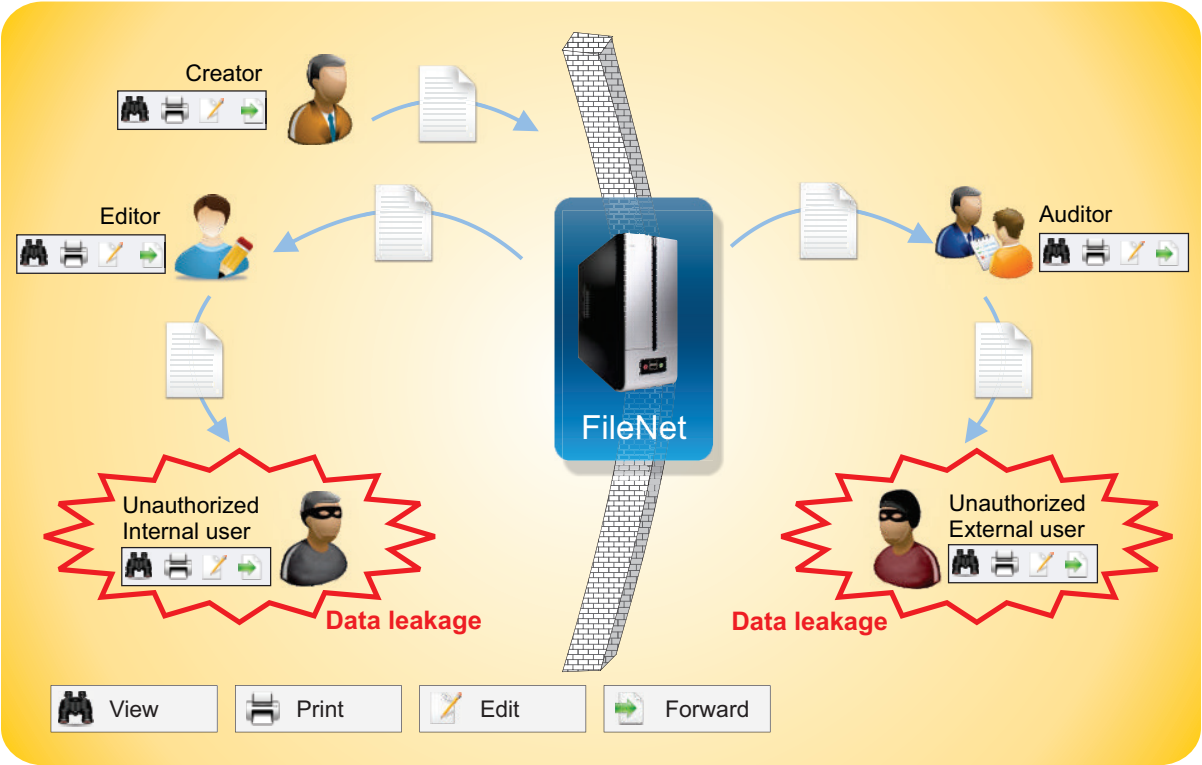

Figure 1. Process before FileSecure

Extending the Security of IBM FileNet With Persistent Usage Controls

All security measures that were implemented prevented unauthorized access to information and documents inside IBM FileNet. However, there were still risks of information breaches from unauthorized access to this information once it was checked out of IBM FileNet and distributed via emails and removable media.

Some of the key business processes and areas where security risks were identified include:

- Audit information was stored in IBM FileNet. External auditors were given access to IBM FileNet to audit the organization's books and update them. One of the risks identified was that when the information was "checked out" from FileNet, it could be misused intentionally or unintentionally.

"Among all of the solutions evaluated, Seclore FileSecure provided us with the maximum flexibility and integration capabilities."

~ Chief Information Officer

- Documents edited by employee groups should be privy to employees within the group only. However, these documents once downloaded from IBM FileNet can find their way to an un-intended audience through various medium like email, removable media, etc.

- Confidential joint venture, partner, vendor agreements are stored in silos within IBM FileNet. Access to these confidential silos was restricted. But these documents, once downloaded by authorized users, could be easily distributed to other unauthorized users or accessed from a stolen device.

- The organization has selective pricing offered to different vendors depending on their geographic location. This information is stored in IBM FileNet and each vendor has access to their selective pricing which is only enforced by a paper-based Non-Disclosure. The "selective" pricing is easily flowing across geographies, leaving the organization vulnerable.

- Employees constantly downloaded confidential documents from IBM FileNet onto their laptops. These sensitive documents are leaving the organization when an employee terminates employment or when a laptop is lost.

- Market survey reports containing data about usage and preference of different products are regularly generated and shared. These reports are extremely valuable. Because they are unprotected, they end up in competitors' hands.

- Transporters upload their freight rates to IBM FileNet so that any branch office and plant can download the information 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, because, once downloaded, information is unprotected and can be easily forwarded and viewed by others.

- Legal documents stored within IBM FileNet were 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 IBM 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 not being addressed. For example, the organization had to adhere to certification on documents after they are downloaded from the IBM FileNet system that they were unable to meet.

A thorough analysis identified the basic problem: once authorized users download the information from IBM FileNet, IBM FileNet cannot control the information from being viewed, edited, printed, forwarded, etc. The organization recognized that they needed the ability to attach “information-centric” access and usage policies to information being downloaded from the IBM FileNet system. These policies needed to stay with the file wherever it went, both internally and externally to third party partners. A key success requirement: the usage policies needed to be automatically attached and couldn’t change the work flow.

Other identified requirements for the information security system included:

- The system needed to easily integrate the with the IBM FileNet system and automatically attach policies as documents were downloaded from IBM FileNet.

- Granular control on usage rights needed to be 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	Revoke Rights
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 IBM FileNet for regulatory compliance.

- Ability to modify the usage rights of downloaded information in real time and anytime.

Seclore FileSecure and IBM FileNet Integration

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.

Seclore FileSecure Connector would allow IBM FileNet to attach usage rights on information before the information is downloaded onto the user's device (desktop, laptop, mobile). 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 the IBM FileNet workflow process. Documents could also be "expired" as soon as a business process was over, thereby enabling access to documents only when it is 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.

IBM FileNet Plus Seclore FileSecure: Protecting Information Wherever It Goes

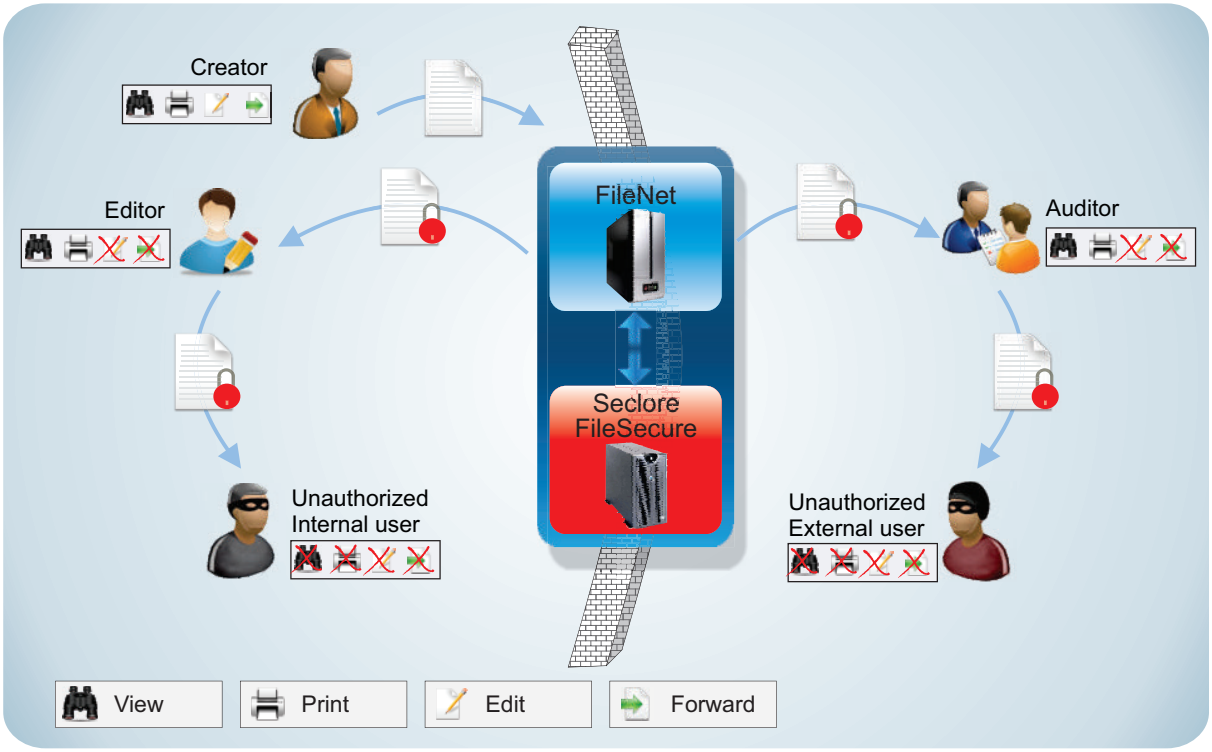

Figure 2. Process after FileSecure

Benefits and ROI Factors

All the above mentioned requirements were directly addressed when Seclore FileSecure was integrated with IBM FileNet.

In additional to addressing the organization's key requirements, the integration of Seclore FileSecure with IBM FileNet also provided additional benefits and value including:

- ***Information security outside of the "walls" of IBM FileNet*** – Persistent security of information inside and outside of FileNet and even beyond the organization's perimeter reduced the risk of security breaches. And because content stored in IBM FileNet has usage policies applied automatically as content is downloaded, the content can be distributed safely, locking out access from unauthorized users regardless of how it's distributed outside of IBM FileNet.

- ***Secure 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 IBM FileNet are automatically encrypted with the correct policies governing their usage, making the system easy to implement and use. Support for native applications (like MS Office, Adobe PDF reader etc.) to access protected documents and single sign-on functionality with IBM FileNet meant users experienced no change in how they worked.

- ***Meeting compliance requirements*** – Seclore FileSecure's audit trail provided comprehensive tracking of information. This audit trails provided proof of compliance with regulatory frameworks and reduced associated reporting costs.

- ***Low IT administration overheads*** – Seclore FileSecure's "integration-friendly" API's provided the capability to integrate with the organization's existing identity management system, existing storage system and existing web application infrastructure which lowered IT administration overheads.

About Seclore

Seclore offers an innovative solution, FileSecure, which enables organizations to control access to information wherever it goes, both within and outside of the organization's boundaries. The ability to remotely control who can view, edit, copy, and distribute unstructured information empowers organizations to embrace mobility, Cloud, and external collaboration with confidence. The most integration-friendly solution on the market, Seclore FileSecure extends and enhances the security of information detected and downloaded from DLP, ECM, ERP systems and attached to Mail/Messaging solutions through pre-built connectors. With nearly 4 million users across 350 companies in 22 countries and rapidly growing, Seclore is helping organizations achieve their security, privacy and compliance objectives.

Visit us at www.seclore.com for more information.

Contact Us

For more information on FileSecure or a live demo, please contact sales@selcore.com

SECLORE

Securing Information Wherever it Goes

www.seclore.com | info@seclore.com | blog.seclore.com