Extending IBM FileNet Security with Seclore FileSecure

You apply access control on IBM FileNet folders. With the addition of Seclore FileSecure, that security will remain with downloaded files, keeping your information protected wherever it travels.

SECLORE

To limit the audience for any given pieces of information, access permissions are defined on the relevant IBM FileNet folders. This security is applicable only within the confines of IBM FileNet. The information however, often travels outside the IBM FileNet system and organizational perimeter, especially in today's world where mobile devices, Cloud services and external collaboration are the norm. Once a document is downloaded by an authorized user, it is free to travel anywhere in the world with no restrictions or control whatsoever.

The Problem with a Stand-alone Document Management System

Enterprises today invest in sophisticated collaboration tools to manage document flow, sharing, and storage. These systems include electronic content management (ECM) systems, business process management (BPM) systems, and Document Management systems (DMS). One of the most popular such tools is IBM FileNet. It has proven extremely successful for organizations looking to streamline document management, collaboration, and storage.

End-to-End Security is the New Requirement

Most documents stored in IBM FileNet are proprietary to the organization. Many are confidential in nature and contain sensitive information and can include everything from invoices to intellectual property.

IBM FileNet implements the first level of access control policies, which dictate whether or not a user can download information from IBM FileNet. After the document is downloaded, IBM FileNet, and the original document owner, do not have any understanding or control over what is being done with the document and where it is. To obtain end-to-end security, organizations now need to add access and usage policies that will stay with the information wherever it goes.

New Requirement: "Everywhere" Information Usage Tracking

The act of downloading a document from IBM FileNet is logged against the user. However, that is where the tracking ends. Once a document is downloaded, IBM FileNet cannot track distribution and usage of the information thereafter. Organizations have a growing need to control, and track documents after they are removed from the confines of the IBM FileNet solution.

Wanted: The Ability to Change Access Controls After the Document is Downloaded

With traditional DMS offerings, all changes made to access control policies will only go into effect for subsequent downloads and use of the content. Subsequent changes (revoke access rights e.g.) cannot be enforced by IBM FileNet for content that has already been downloaded and distributed.

External Collaboration - The New Normal

There is nothing in a DMS system that stops an authorized user from downloading a folder or library and using them as they wish. And with most organizations now needing to share information with a growing number of business partners, vendors, prospects and outsourcers, the lack of control over information is even greater.

Due to these factors and by virtue of its perimeter-centric nature, information in IBM FileNet frequently gets breached - intentionally or unintentionally. Depending on the nature of the business, this may lead to loss of revenue, consumer confidence and intellectual property.

Seclore FileSecure + IBM FileNet = Super Power Information Security

Security that Goes Beyond IBM FileNet

Seclore FileSecure, an information-centric security solution, extends the control of a DMS system to wherever the actual information travels. A security blanket is applied around the document itself, just before it is downloaded. This security then “sticks” to the document and stays with it wherever it travels. This means that the information is secure even after it is taken out of IBM FileNet and distributed within and outside of the organization.

Seclore FileSecure enables ‘owners’ of information to control the actions that are performed on the information after it has been downloaded. These controls are applied to the content itself without any constraint on the computer, network, storage or transmission technology used. The controls are also dynamic, for example if the ‘owner’

wants to change the controls to provide usage to a different set of people, or different set of actions, it is possible for him/her to remotely change the rights to all copies of the downloaded information. The owner can even "revoke" anyone from access the information after distribution.

Securing Information with Seclore FileSecure

Securing information with Seclore FileSecure involves manually or automatically defining "usage rights" for the information as it leaves IBM FileNet. These usage rights can be a combination of the following controls:

- **WHO** can access the information: You can readily define who is allowed to access the information in conjunction with current user repository (e.g. LDAP) and can also map to the organization hierarchy of users, groups & organization units. FileSecure can leverage Federated Identity Management systems (non-LDAP) repositories as well.

- **WHAT** can each user do with the information: This typically relates to individual actions allowed on the information by a specific user. Individual actions which can be controlled are viewing, editing, printing, forwarding/ sharing, copy/paste of content & un-protecting.

- **WHEN** can each user access the information: This control can limit users to access the information within a specific date range or time-span. A document could thus have "August 19 at 4 pm TO August 23rd at midnight" as a specific date range or "two days from first access" as the specific time span within which the document is available.

- **WHERE** can the information be used: This is useful in cases of information with extreme confidentiality. The WHERE control can restrict usage of the information to only a pre-specified list of computers identified by the hardware or to a specific range of IP addresses or networks.

Benefits of a Combined IBM FileNet and Seclore FileSecure Solution

Seclore FileSecure used with IBM FileNet provides complete and persistent usage control on information throughout its lifecycle. A pre-built connector makes it very easy to integrate the two solutions. Organizations can embrace the use of mobile devices, external collaboration and outsourcing with confidence. And security can be ensured without compromising on the natural collaboration capabilities of IBM FileNet.

Security that Stays with the File Reduces the Risk of a Breach

Once a file is downloaded from IBM FileNet, it remains protected. The security blanket travels with the file. FileSecure builds an intelligent firewall around the file itself – so that information-centric protection is applied to all copies of the document – regardless of mode of transfer – email, USB, mobile device, shared folders, etc. The security will also persist when the file is transformed from one format to another (eg. saving a docx file as a PDF file).

Automated Usage Tracking Simplifies Audits

Seclore FileSecure's auditing capabilities, combined with IBM FileNet's, provides a complete view of document usage at all times and in all locations – within and beyond IBM FileNet and the organization's perimeter. All activities performed on protected files by authenticated users – whether inside or outside the enterprise network - are centrally logged in the system. These logs are updated in real time and are easily accessible to the information owner. When integrated with SIEM systems, alerts can be sent to the information owner for a particular activity – such as an unauthorized attempt.

User	Activity	Date and Time	Authorized?
John	View	5th Jan 2013 12:10 PM	Yes
Richard	Edit	5th Jan 2013 12:15 PM	Yes
Mary	View	5th Jan 2013 4:10 PM	Yes
Stephen	Print	5th Jan 2013 4:12 PM	No

Authorized actions as well as unauthorized attempts to access information can be tracked across enterprise boundaries. This can help enterprises adhere to regulatory and compliance frameworks such as ISO, Sarbanes-Oxley & HIPAA for "unstructured" data control. Seclore FileSecure can also significantly lower costs and process delays associated with version control and document retention policies. With Seclore FileSecure, information can be safely and securely shared with employees and business partners with no large additional investment in security systems.

Remote-Control Facilitates External Collaboration

The document owner can control access to the information even after it has been shared. The owner can change access levels to it at any time – including revoking all access from the desired users. He can also deactivate the file – so that it instantly becomes inaccessible to everyone.

Independence on Device, Transmission and Storage Mediums Enhances Agility

Seclore FileSecure information-centric protection and encryption is completely independent of both the transmission and storage mediums. For example, there is absolutely no risk in sending the file over a public network. A FileSecure-protected file remains as secure when travelling over a public network as it is while inside a VPN (Virtual Private Network) tunnel. Files shared on the Cloud are also perfectly secure, giving your employees and partners great freedom in how they collaborate and work.

Granular Security Promotes Flexibility in Information Control

FileSecure allows an information owner to specify access levels to documents (View-only, View+Edit, View+Edit+Print etc.) for different users, at different times, and for different locations - and any combination of these, as discussed above.

Complete Automation Maximizes Security Without Impacting Productivity

The process of using Seclore FileSecure capabilities with IBM FileNet is completely automatic. Files get automatically protected when they are downloaded from IBM FileNet. The entire process is transparent to the end user.

No Impact on Existing IBM FileNet Functionality Speeds ROI

Files get protected just before they are downloaded from a configured IBM FileNet folder. As long as the files are within the folder, they are not encrypted and can be indexed and searched as usual. The integration of Seclore FileSecure with IBM FileNet makes information-centric security for all confidential content an achievable aim. The minimal cost and effort of having such capabilities far outweighs the risks of losing sensitive information.

Summary

The security offered by Document Management Systems contains a major drawback – it extends only until the DMS boundary. Sadly, however, the information doesn't stop at the DMS border. With the addition of Seclore FileSecure, security and audit control can extend to wherever the information travels, offering organizations a simple way to extend IBM FileNet security with minimal extra investment.

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