

Chemical Manufacturer



AT A GLANCE

Company:

- A leading manufacturing company with operations in 17 countries
- Manages 23 manufacturing plants serving customers in 65 countries
- Employs more than 2000 employees and has more than 5 million retail and enterprise customers

Challenges:

- IBM ECM security policies are removed once a document is downloaded from the system
- Loss of control over business-critical information shared inside and outside the organization or when an employee leaves
- External partners have access to IBM ECM; once a document is downloaded, the Manufacturer loses control over that content
- Regulatory compliance laws need to be met and show proof of compliance

Solution:

Seclore's Rights Management

How IBM Enterprise Content Management (ECM) and Seclore's Enterprise Digital Rights Management joined forces to enable secure internal and external collaboration in a leading manufacturing company.

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

To enable collaboration to flow freely, access to IBM ECM was provided to employees and also to some outside business partners such as vendors and independent auditors. To improve productivity, efficiency and interaction, a large number of business processes and associated document management were automated using IBM ECM's business process management capabilities.

Challenges

IBM ECM'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 process. However, once information was downloaded from IBM ECM to a desktop, removable media, or emailed to external partners or internal employees, it could easily be viewed, forwarded and exploited by unauthorized users.

Multiple Security Risks Identified in the Manufacturer's Business Processes
The security measures that were implemented did a great job of preventing unauthorized access to documents inside

IBM ECM. Once content was downloaded, the policies no longer applied. The company identified several key business processes that were creating a security risk:

- Documents edited by employee groups could be distributed to unintended audiences once the document is downloaded from IBM ECM.
- Employees constantly download confidential documents from the ECM system to their laptops. If the laptop is stolen or the employee left the organization, the data would be lost.
- External auditors have access to IBM ECM to audit and update the organization's books. When information is checked out from IBM ECM, the content could be misused intentionally or unintentionally.
- Confidential data such as joint ventures, partner and vendor agreements, legal documents, technical specifications, and survey reports could be freely distributed and could potentially end up in competitors' hands.
- Selective pricing offered to different vendors based on geographic location was vulnerable to being shared across geographies although paper-based non-disclosures were signed.

- An international online library in IBM ECM is available to employees from around the world. The library contains confidential documents such as specifications and patents. Although the library is a convenience, it poses a risk of information being leaked.

Apart from all the above security concerns, there are numerous regulatory and compliance norms not being addressed. For example, the organization has to adhere to regulations around certification documents after they are downloaded from the IBM ECM system that they were unable to meet.

A thorough analysis identified the basic problem: once authorized users download the information from IBM ECM, the 'usage rights' do not travel with the information. The organization recognized that they needed the ability to attach persistent "information-centric" access and usage policies to content being extracted from the IBM ECM system. A key success requirement: the usage policies needed to be automatically attached without changing the work flow.



People leaving our company carried a lot of confidential business information with them on their laptops. Hence, we felt the need to protect our intellectual property with persistent, strong controls such as Seclore's EDRM offers.

Director of Information Security



The Solution: Seclore's Enterprise Digital Rights Management (EDRM)

The Seclore EDRM Connector for IBM ECM enables the organization to enforce security policies on information even after it has been downloaded from IBM ECM.

Seclore's EDRM Connector enables IBM ECM to automatically attach persistent usage rights on information as it leaves the IBM system. The usage rights defined WHO (people, groups) can use the document, WHAT (view, edit, print, screen capture, print) can the person do with the document, WHEN (specific dates, time spans) can this be done and from WHERE (which device or IP address) can the document be used. These usage rights can be defined for employees and external users depending on their role and responsibility and the current state of the IBM ECM workflow process.

Documents can 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 proved compliance to regulatory standards but also helped in doing forensics whenever there was any unauthorized activity attempt on information. The Seclore IBM ECM Connector also provides a "remote control" feature to change the usage rights on documents post download, providing complete control of distributed documents.

Business Benefits and Results

The company is now able to automatically attach usage policies as documents are downloaded from IBM ECM. This allows the organization to enforce granular usage rights based on roles and tasks assigned to employees and partners. The persistent, end-to-end usage control on information throughout its lifecycle ensures complete security over sensitive information even during external collaboration.

In addition to rigorous enforcement of content usage wherever information travels, the complete audit trail of authorized activities and unauthorized attempts is also helping the organization address their compliance requirements. With Seclore's Rights Management solution, the company is able to have secure collaboration within and outside the company without comprising the security of information that is vital to the company's business.

USA – West Coast

691 S. Milpitas
Blvd.#217
Milpitas CA 95035
1-844-473-2567

USA – East Coast

420 Lexington Avenue
Suite 300,
Graybar Building
New York City
NY 10170

India

Excom House Second Floor
Plot No. 7 & 8,
Off. Saki Vihar Road
Sakinaka, Mumbai
400 072
+91 22 6130 4200
+91 22 6143 4800

Gurugram

+91 124 475 0600

Singapore

Seclore Asia Pte. Ltd.
AXA Tower, 8 Shenton
Way
Level 34-01
Singapore – 068811
+65 8292 1930
+65 9180 2700

Europe

Seclore GmbH
Marie-Curie-Straße 8
D-79539 Lörrach
Germany
+49 151 1918 5673

UAE

Seclore Technologies FZ-LLC
Executive Office 14, DIC
Building 1 FirstSteps@DIC
Dubai Internet City, PO Box
73030, Dubai, UAE
+9714-440-1348
+97150-909-5650
+97155-792-3262

Saudi Arabia

5th Floor, Altamyo Tower
Olaya Street
P.O. Box. 8374
Riyadh 11482
+966-11-212-1346
+966-504-339-765

