

Four Must-Have Rights Management Capabilities



Four Must-Have Rights Management Capabilities

If you are currently using an Information or Enterprise Rights Management system, or you have checked out Rights Management in the past and found it lacking, the newest entrants in this market are creating a dramatic change in terms of what the technology can do and how easily it can be adopted.

These technical advances, combined with the surge in use of mobile devices, file-sharing services, outsourcing, and the general upswing in the need to collaborate externally, are creating the perfect storm for Rights Management.

If you have information that needs to leave your organization to support collaboration, and are looking for better ways to secure mobile devices, outsourcing and file-sharing, you need to take a look at the next generation of Rights Management solutions.

The Past Challenges of Rights Management

Previous versions (and many current versions) of Information and Enterprise Rights Management solutions face several key challenges that have hindered adoption:

- Bulky and intrusive agents to access protected information
- A user unfriendly application requiring significant enablement and support
- Limitations in file types and applications that could be protected
- Lack of access to protected information on mobile devices
- Lack of automation made the act of protecting files time-consuming and difficult
- Authentication of the user was cumbersome; systems lacked federation and connectivity with identity portals

Let's take a look at what's changed in the new generation of solutions to make Rights Management a compelling technology for protecting information that travels outside of your secured perimeter.

Four Key Rights Management Solution Capabilities

Here are four key capabilities that you should look for in a Rights Management solution:

1) Easy, Non-Intrusive Adoption for Users Who Protect Files

Rights Management thrives in an organization when it is easy to use and adopt. Ease of use ensures that users will secure information while collaborating with third parties, further reducing your security risks. Ease-of-use is a key criterion when choosing a Rights Management system as it affects project success and overhead costs of training and enablement. With the newer generation of Rights Management, user adoption requires very little training and assumes little-to-no knowledge of enterprise security controls. Some of the "easy adoption" features of the new generation of solutions that are offered by Seclore's Enterprise Rights Management capabilities are:

1. Native Rights Management support in current productivity tools (MS Word, Excel, AutoCAD, email, etc.) means that users do not need to utilize or learn a new system.
2. Availability on both desktop and mobile platform means that users can utilize the same Rights Management process across all computing platforms.
3. Streamlined user interfaces and processes make it much easier to attach the right usage policies to the right files.
4. Seamless identity federation and single-sign-on capabilities remove the need for end users to remember or input their authentication information.
5. Granular controls enable end users to graduate and become "power-users" quickly.

Seclore has carefully analyzed user behavior around rights management and has optimized its technology for easy adoption and minimal overheads.

2) Ease-of-Use for Recipients of Protected Files

On-boarding and enabling external users to utilize rights-protected content is also key to the use and adoption of Rights Management. Making it easy to access protected documents is also important to reduce support calls! In some solutions, the ability to access and utilize rights-protected documents requires an external user management process, which does not exist in most enterprises. If you require the external recipient to install an agent, that is also a problem because it will involve the external entity's IT team to accept the software before secure external collaboration can begin.

To eliminate the challenges faced by enterprises engaged in secure external collaboration, the next generation of Rights Management such as Seclore's ERM solution has introduced many features to simplify the recipient's experience:

1. Seamless identity federation and single-sign-on for external users enables recipients of protected documents to leverage the existing credentials found in on-premise systems (vendor portal, client portal) as well as SAML based cloud identity brokers.
2. Automated identity creation, approval, and management for external users enables external users to be easily on-boarded without any IT administration overhead.
3. Agentless access to protected content enables external users to utilize a browser to consume protected content, eliminating the hassles of downloading and installing an agent.
4. "Lite" versions of agents which can be installed without administrative rights by recipients, removing the involvement of the external agencies' IT teams.
5. Ability to access protected documents through a desktop or mobile device.

3) Automating and Expanding How Rights Are Applied to Files

Educating users on the appropriate usage policies for a given document and ensuring confidential content that leaves the organization is properly secured has traditionally been a huge challenge.

The new generation of Rights Management offers several automated methods for the "attachment" of usage policies to files. These automated methods reduce the dependency on end users to define and apply usage policies to files.

1. Single-click protection: Users can drag/drop a file into a "secure folder" where it will automatically assume the correct usage policies.
2. Ready integrations with ECM systems such as MS SharePoint, IBM FileNet, EMC Documentum and file-shares provide centralized usage policy definition and management. As files are extracted from these systems, the appropriate usage policies are automatically attached.
3. Ready integration with mail and messaging systems such as Outlook and Lotus Notes gives the user an in-app experience and a "single click" process for protecting email text and attached files.
4. Ready integrations with leading DLP systems like McAfee DLP and Symantec (Vontu) DLP automates the application of rights to a given file without dependence on people.
5. Rich APIs offer easy integration of Rights Management with proprietary and third-party systems such as ERP, BI, and Legacy Systems. The connectivity of these core systems with Rights Management allows the security policies that are defined in the core systems to be inherited by the sensitive information that is extracted and distributed.

Seclore has built the most integration-friendly Rights Management system in the world. Through integrations with identity, content, security and transaction management systems, user involvement in policy definition and implementation is significantly reduced.

4) Agnostic, Comprehensive Rights Management

Most Rights Management solutions are tied to a particular document management solution, DLP system, EFSS, or a particular vendor infrastructure, inhibiting the full potential for protecting sensitive information. As well, the controls that can be enforced in some Rights Management solutions are limited, leaving security gaps. Here are some of the capabilities you will want to look for in a Rights Management system:

1. The ability to control macros, prohibit screen captures, and watermark documents gives organizations deeper control and security over sensitive information.
2. The expansion to protecting a full array of file types, including AutoCAD, image files, and more, increases the security coverage.
3. The ability to control access to a given file down to the exact device and location enables organizations to address compliance requirements.
4. The ability to control application-to-application data sharing can eliminate any human intervention on the files that are shared with outsourcers and other third parties.
5. The ability to extend and add usage control enforcement to any EFSS, ECM, DLP, ERP, BI system gives the organization a common infrastructure for information-centric security and full flexibility in where you utilize rights management.

Seclore – Enterprise Rights Management 3.0

As a global leader in the space, Seclore has been designing and delivering innovative Rights Management solutions for several years. After extensive research in usability and how people are exchanging information, Seclore has introduced the next-generation of Rights Management solutions. Seclore's Enterprise Rights Management 3.0 solves the adoption and usability issues found in other Rights Management solutions, and dramatically expands how well documents can be secured.

Summary

With external collaboration and the use of mobile devices, cloud services, outsourcing and file-sharing on the rise, more and more sensitive information needs to be shared outside of the organization. In fact, every 49 minutes, a sensitive file is sent outside of your organization's perimeter unprotected.

Rights Management has been the answer to enabling secure external collaboration for quite a while, but the technology was lacking. Now, with the new technical advances in the latest generation of offerings, Rights Management is at exactly the right place. Whether you are a new comer to the technology, or an early adopter, it's time to take a look at what Seclore's Enterprise Rights Management 3.0 can do for you.

About Seclore

Seclore offers the market's first fully browser-based data-centric security solution, which enables organizations to control the usage of files wherever they go, both within and outside of the organization's boundaries. The ability to remotely enforce and audit who can view, edit, copy, screen share, and redistribute files empowers organizations to embrace mobility, file-sharing, and external collaboration with confidence. With over 6000 companies in 29 countries using Seclore to protect 10 petabytes of data, Seclore is helping organizations achieve their data security, governance, and compliance objectives.

Learn how easy it now is to keep your most sensitive data safe, and compliant.

Contact us at: info@seclore.com or CALL 1-844-4-SECLORE.

USA – West Coast

157 S. Murphy Avenue
Sunnyvale, CA 94086
1-844-473-2567

USA – East Coast

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

India

Excom House Ground 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

Bengaluru

+91 080 46586900

Singapore

Seclore Asia Pte. Ltd.
#08 -01
80, Robinson Road
Singapore – 068898
+65 8292 1930
+65 9180 2700

Europe

United Kingdom
Suite 4B, Linwood Point
Paisley, PA1 2FB
+44 141 433 7902

UAE

Seclore Technologies FZ-LLC
Executive Office 14, DIC
Building 1 FirstSteps@DIC
Dubai Internet City, PO Box
73030, Dubai, UAE
+97155-990-1570
+9714-440-1348

Saudi Arabia

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

