

Automating Enterprise Rights Management (ERM)

How to Rapidly Close the Security Gaps in External Collaboration



Enterprise Rights Management – The Answer to Secure Collaboration

Enterprise Rights Management (ERM) offers organizations a way to persistently protect files wherever and however they are shared. At a time when more and more sensitive information is shared with third parties, the ability to apply persistent, granular usage rights to that information is critical to avoiding data leakage.

ERM goes beyond data loss prevention, file encryption and other traditional security technologies; it allows you to maintain constant control over a file while it is at rest, in transit and at work. That means you can control who can access the file, from which device or IP address, and for how long. Even more importantly, ERM allows you to control exactly what the recipient can do with the file: view, edit, copy/paste, print, run macros, and screen capture. With some advanced ERM systems, these 'usage controls' work within the native application such as Adobe, MS Word, MS Excel, Image Formats, Auto-CAD, and many more, ensuring links within the document remain viable and the user experience is seamless.

Ad-Hoc Versus Automated ERM

Most ERM systems are designed to only support the document creator or 'sender' manually protecting the file. These solutions are only viable in situations where very few sensitive documents are shared. The reason: If you are relying on your employees to manually protect files as they are created or shared, you will not close your collaboration security gap reliably or quickly.

To ensure the success of ERM projects, you need to look for the solution that will enable you to automatically 'attach' usage policies at the exact point where files are downloaded, shared, or discovered. To enable this automation, the ERM solution must have two primary capabilities: the ability to easily connect ERM with existing systems and the ability to easily leverage and augment existing access policies.

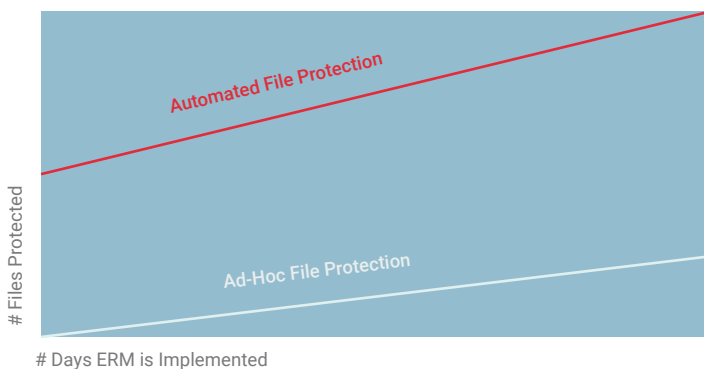


Figure 1: Automatically attaching usage policies to the files, you will protect 60% more of your sensitive files annually.

A Connecting ERM to Existing Systems

The first step to automating persistent file-centric security is getting close to the file storage, sharing, and discovery sources. To easily integrate ERM with your existing systems, you want a solution that provides a robust library of prebuilt connectors for Cloud Access Security Brokers (CASB), Enterprise File Sync and Share (EFSS), Enterprise Resource Planning (ERP), Data Loss Prevention (DLP), and Enterprise Content Management (ECM) solutions. These connectors will enable you to automatically attach the usage policies as documents are shared via EFSS, discovered by DLP and CASB, and downloaded from ERP and ECM systems.

By connecting directly with existing systems, you will dramatically accelerate the protection of sensitive information. Imagine turning on your ERM system and on day one, protecting hundreds of documents without employee intervention. That is the power of seamlessly connecting ERM with your existing systems.

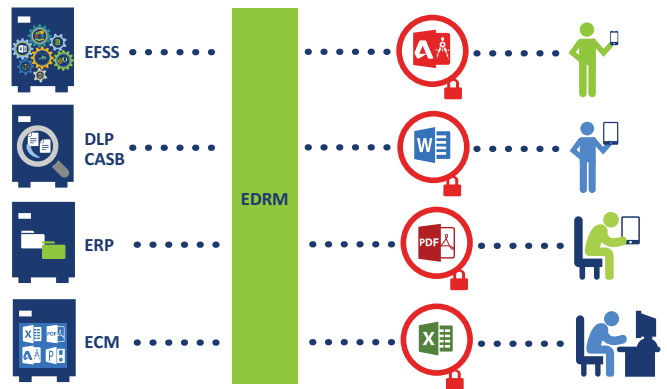


Figure 2: To automate file-centric security, you need to seamlessly connect ERM with existing systems.

Policy Federation: The Other Half of Automated ERM

The other half to 'automated ERM' is streamlining the process of defining and managing the granular usage policies. That's where Policy Federation comes into play. Policy Federation leverages the access policies already defined and managed in other Enterprise systems (DLP, ECM, ERP, CASB, and EFSS) and maps these existing access policies to the robust, granular usage policies that are controlled by the ERM solution.

By leveraging the existing access policies, and seamlessly syncing the access + usage policies (e.g. change made in ECM system automatically mapped to ERM usage policy) across systems, you can minimize the effort needed to manage your overall policies and significantly increase the consistency of your file-centric usage rights.

MS SharePoint Policies	Seclore Policies
amy.jones@gmail.com - View Only	View
kevin.smith@gmail.com - Edit	View + Edit
susan.morga@gmail.com - Contribute	View + Edit + Print
amit.gupta@gmail.com - Full Control	View + Lite View + Edit + Print + Secure Copy + Offline + Screen Capture

Figure 3: Policy Federation makes it easy to augment existing access policies with usage controls.

Seclore's ERM

Seclore's advanced Enterprise Rights Management solution enables organizations to control the usage of any type of file, wherever the file goes, both within and outside of organizations' boundaries. Featuring dozens of prebuilt connectors for leading enterprise applications (EFSS, CASB, DLP, ECM, ERP, and eMail), and an innovative Policy Federation capability, Seclore automates the protection of documents as they are downloaded, discovered, and shared to ensure rapid adoption.

The goal: to ensure secure collaboration and empower organizations to embrace BYOD, Cloud services, Enterprise File Synch and Share (EFSS) and all forms of external collaboration with confidence.

Summary

The combination of pre-built connectors + Policy Federation will enable you to automatically protect 60% more of the sensitive documents that are flowing around and shared outside your organization. Automation will enable you to rapidly close your collaboration security gaps and will ensure the overall success of your ERM deployment. If you'd like to learn more about how Seclore's ERM solution works, visit www.seclore.com or call us at 1-844-4SECLORE.

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 2000 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.

