SECLORE

Combining the Power of DLP and Rights Management: How to Streamline and Extend Your Data Security

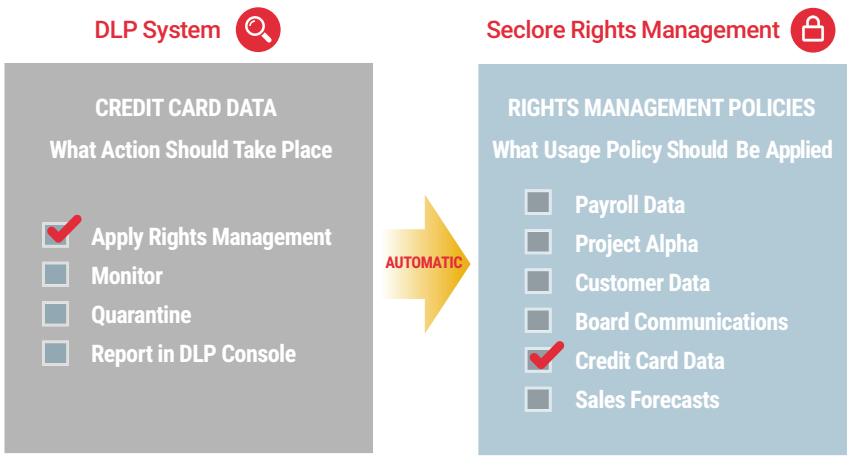
By combing the power of DLP and Rights Management, organizations can automate the detection and protection process to ensure data is secure, revokable, and tracked while it is being utilized and wherever it travels.

Extending DLP Jurisdiction Beyond Organizational Borders

DLP technology can detect and monitor sensitive data and prevent it from leaking outside your enterprise. DLP can also apply basic file encryption to files. However, once your confidential data is shared outside your enterprise for genuine business reasons – with numerous contractors, vendors, and partners – you have lost control.

By adding Seclore Rights Management to your DLP solution, you can control who can access a file, what they can do with it (view, edit, cut/paste, screen share, print), when, and from which device or IP address. You can also revoke access after a file is shared and track all usage of the file, no matter where it is located.

How DLP and Rights Management Work Together



DLP + Rights Management integration enables you to implement document distribution control (DLP) as well as document usage control and tracking (Rights Management).

The combination of DLP + Rights Management gives you full control of files as they travel through public and partner networks, are stored on the cloud or file-sharing services, or as they are accessed on personal laptops and mobile devices.

Automatically Apply Granular Usage Controls on Information Discovered by DLP

Confidential files discovered by a DLP solution can be automatically protected by Seclore Rights Management. When defining a DLP discovery rule, you can choose the relevant Seclore Rights Management policy that will be applied to the discovered file.

A unique Seclore Policy Federation capability enables you to easily map and synchronize DLP and Rights Management policies to ease on-going administration.

Reducing False Positives During Discovery

Files can be easily classified (manually or automatically) using Seclore's Data Classification. DLP rules can be triggered based on this classification label which drastically reduces false positives during data discovery.

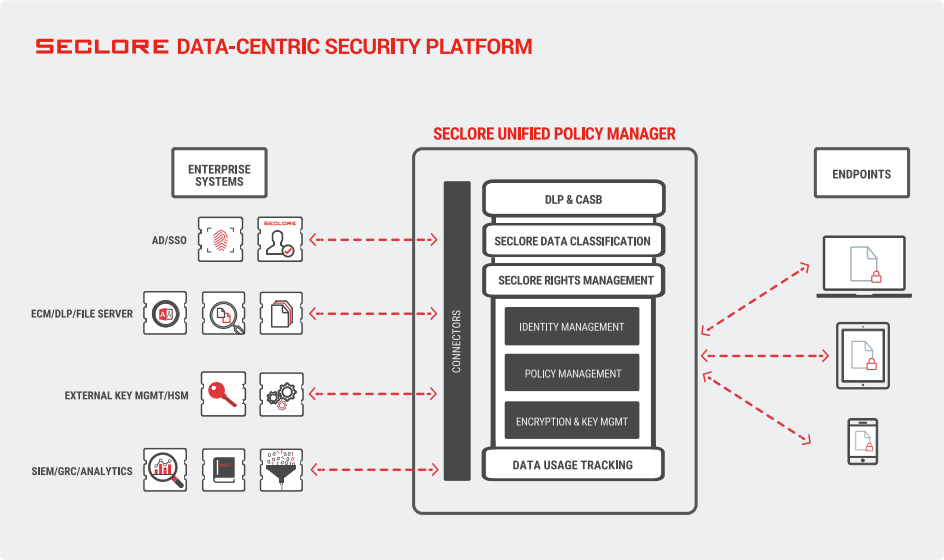
Pre-Built Connectors for DLP

Seclore's Data-Centric Security platform features pre-built connectors for McAfee, Symantic, Forcepoint, and other leading DLP providers. The pre-built Seclore Connectors for DLP and Policy Federation capabilities make it easy to add automatically add granular usage controls and tracking to a DLP solution.

Secure Decryption of Seclore Protected Emails

Seclore Decrypter for Email enables secure access to Seclore protected emails and attachments. Decrypting the email or attachment allows email security solutions like DLP, CASB, SEG, and other email content inspection solutions to inspect content and patterns to make appropriate decisions (Allow / Block / Protect) before sending. The Seclore decrypter is universal and works with any email security solution.

Through the decryption feature, organizations can claim compliance to regulations as their discovery solutions can now discover, track, and audit all files now – both unprotected and protected documents.



Seclore Data-Centric Security Platform

Key Business Benefits

Security and Compliance Beyond the Firewall

DLP and Rights Management integration allows you to secure and audit data everywhere it goes: to vendor and partner networks, to public networks, to the cloud, or to mobile devices.

Reduced False Positives

DLP rules being triggered by innocent data can frustrate day-to-day business processes – and end users too. The integration of Seclore Data Classification and your DLP system drastically reduces the chances of false positives during data discovery.

Reduced Incident Lists

DLP can be configured to treat Rights Management–protected files as safe– and not generate alerts for such files. Automated detection and protection of files leads to significantly reduced incident logging.

Reduced Insider Threats

The ability to automatically revoke information wherever it is stored means you can remove access to sensitive information on employees' personal devices when they leave.

Protect Data-at-Work

File encryption only protects data in transit and storage. Rights Management will enable you to control the use of a file even while it is being utilized by an authorized recipient.

End-To-End Auditing and Regulatory Compliance

DLP and Rights Management integration enables you to track the usage and comply comply with regulatory obligations for the entire lifecycle of unstructured data – both within and outside your enterprise network.

Automated Data-Centric Protection

DLP and Rights Management integration automates the entire process of discovering, classifying, protecting, controlling usage, and auditing. The process of Rights Management protection and tracking is completely transparent to the end user to ensure security gaps are closed.

Enforcing IT Policies on Third Parties

DLP and Rights Management integration lets you enforce your data governance and corporate IT policies on your contractors, vendors, partners, and other third parties.

The Power of Data-Centric Security

By combing the power of Data Classification, DLP, and Rights Management, you will achieve unprecedented control and monitoring of your sensitive information assets wherever they travel and even while they are being utilized within other applications.

Adding Seclore Rights Management and Seclore Data Classification to your DLP solution will enable you to reduce data leakage, engage in secure external collaboration, rapidly address regulatory compliance, and gain the confidence to fully embrace the cloud, BYOD and outsourcing.

SECLORE