SECLORE

# Data-Centric Security: Combining the Power of DLP, ERM & Classification

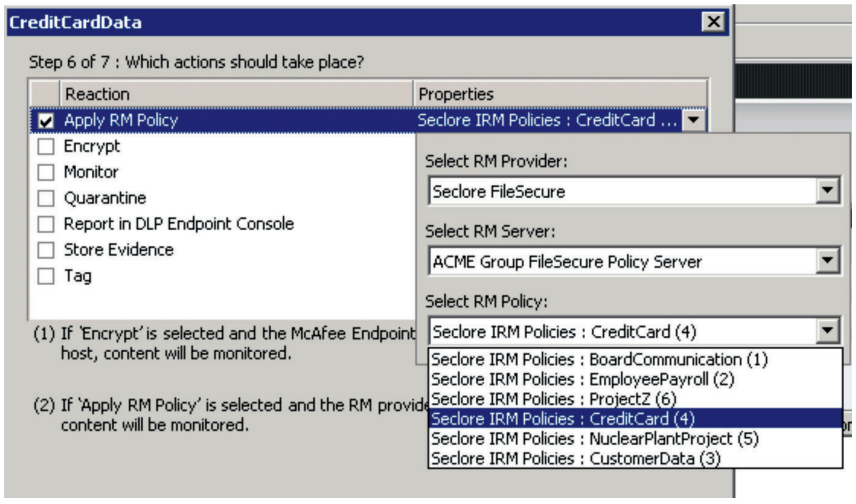
**Neil MacDonald**
**VP and Gartner Fellow**

*The need to place and enforce EDRM policies on information (e.g. can I print this? copy it to USB? email it?) must expand to include contextual awareness of the content being protected – the realm of DLP. These are not separate problems and should be integrated, ideally from a single solution.*

## Extending DLP jurisdiction beyond organizational borders

DLP 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 even revoke access after a file is shared.




*DLP-ERM integration enables you to implement document distribution control (DLP) as well as document usage control (ERM).*

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 filesharing 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 ERM 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 which drastically reduces

## Pre-Built Connectors for DLP

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

## Key Business Benefits

### Security and Compliance Beyond the Firewall

DLP-ERM 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 Classification and your DLP system drastically reduces the chances of false positives during data discovery.

### Reduced Incident Lists

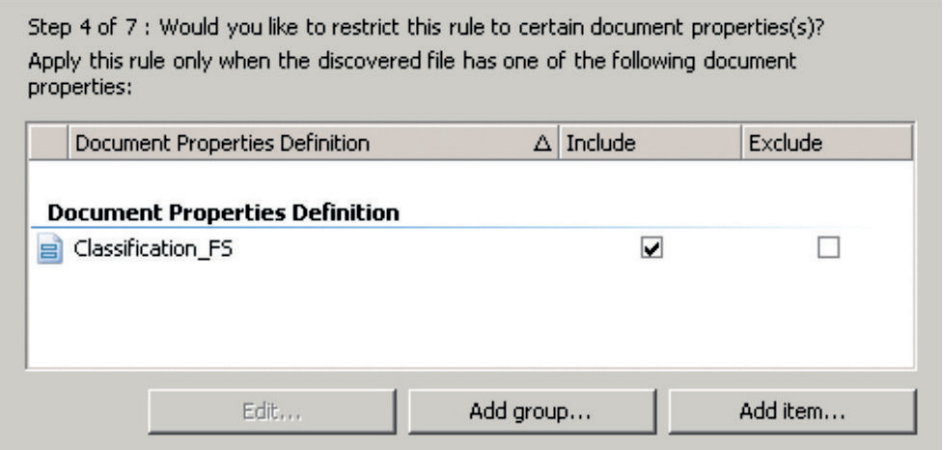
DLP can be configured to treat ERM-protected files as safe - and not generate alerts for such files. This leads to significantly reduced incident logging.

### 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. ERM 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-ERM integration enables you to comply with regulatory obligations for the entire lifecycle of unstructured data – both within and outside your enterprise network.

### Automated Data-Centric Protection

DLP-ERM integration automates the entire process of classifying, protecting, controlling usage, and auditing. The process of ERM protection is completely transparent to the end user.

### Enforcing IT Policies on Third Parties

DLP-ERM 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 combining the power of Data Classification, DLP and ERM, 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 Classification to your data-centric infrastructure will enable you to reap the full benefits from DLP, rapidly address regulatory compliance, and gain the confidence to fully embrace the cloud, BYOD and outsourcing.



SECLORE