Seclore for McAfee DLP

Data Loss Prevention (DLP) can discover sensitive data and prevent it from leaking outside your network. However, what happens after data discovery? How can you secure the confidential documents that need to be sent outside your network to support timely collaboration with numerous contractors, vendors, and partners? And how do you protect sensitive data shared via the cloud, or accessed by third parties on their mobile devices?

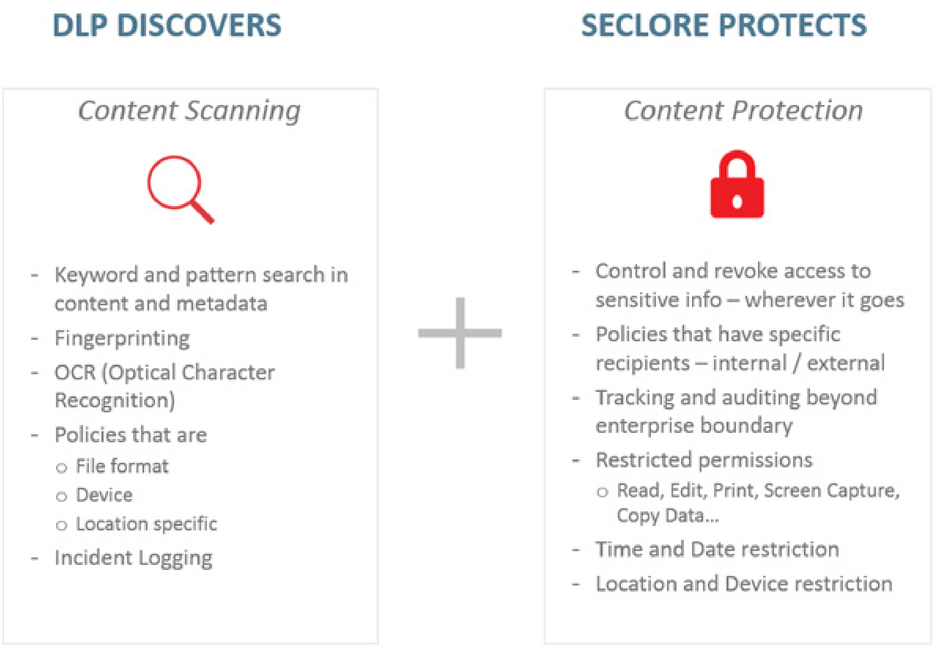
McAfee DLP + Seclore

DLP can inspect content in documents and discover sensitive data. This can help you identify where your sensitive documents are stored and their classification levels. The discovery in turn can help you determine the appropriate usage policies (rights) to apply on the document.

Most organizations find it difficult to go beyond the discovery phase to the 'persistent protection' phase. Reviewing the reams and reams of logs is challenging enough – and is only reactive. Stopping discovered documents hampers workflow. And applying the correct usage policies to fully protect discovered data wherever it travels is beyond the scope of DLP.

By adding Seclore to your McAfee DLP system, you have complete control over the use of your information – including the power to revoke access entirely – even when documents travel beyond your enterprise boundaries to support collaboration. As soon as sensitive data is discovered by McAfee DLP, Seclore can instantly protect it with the appropriate usage policy. These granular rights will always stick with the document wherever and however it travels.

Seclore enables you to automatically classify documents and apply the control that will enforce who can access the document, what they can do with it, when, and from which computer or device. By adding persistent, data-centric controls, the scope of McAfee DLP can be extended to control the use of documents travelling through public and partner networks, stored on the cloud or file-sharing services, or accessed on mobile devices.



DLP DISCOVERS

Content Scanning

- Keyword and pattern search in content and metadata
- Fingerprinting
- OCR (Optical Character Recognition)
- Policies that are
    - File format
    - Device
    - Location specific
- Incident Logging

+

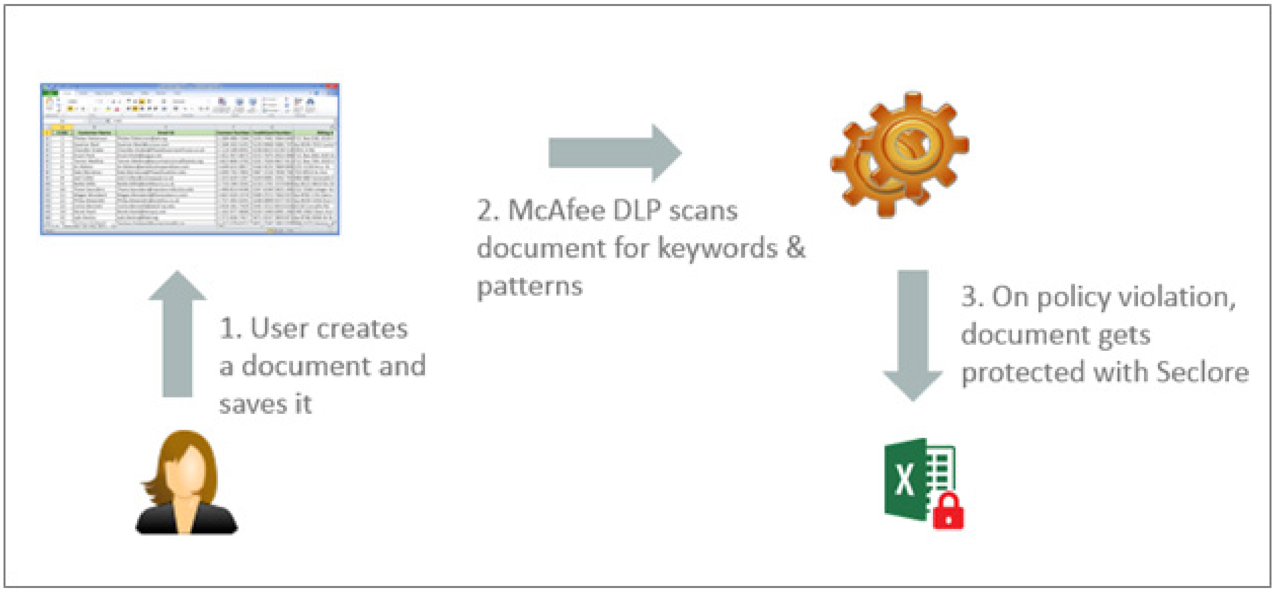
SECLORE PROTECTS

Content Protection

- Control and revoke access to sensitive info – wherever it goes
- Policies that have specific recipients – internal / external
- Tracking and auditing beyond enterprise boundary
- Restricted permissions
    - Read, Edit, Print, Screen Capture, Copy Data...
- Time and Date restriction
- Location and Device restriction

Seclore Rights Management and McAfee DLP Endpoint Discovery

McAfee DLP can scan documents and sniff out confidential data lying on endpoints. It can match keywords (e.g. “revenue projections”), patterns, and regular expressions (e.g. credit card numbers) - and also look into specific folders or search for documents of specific formats. After discovery, Seclore Rights Management can automatically secure this sensitive information to prevent its leakage or misuse.



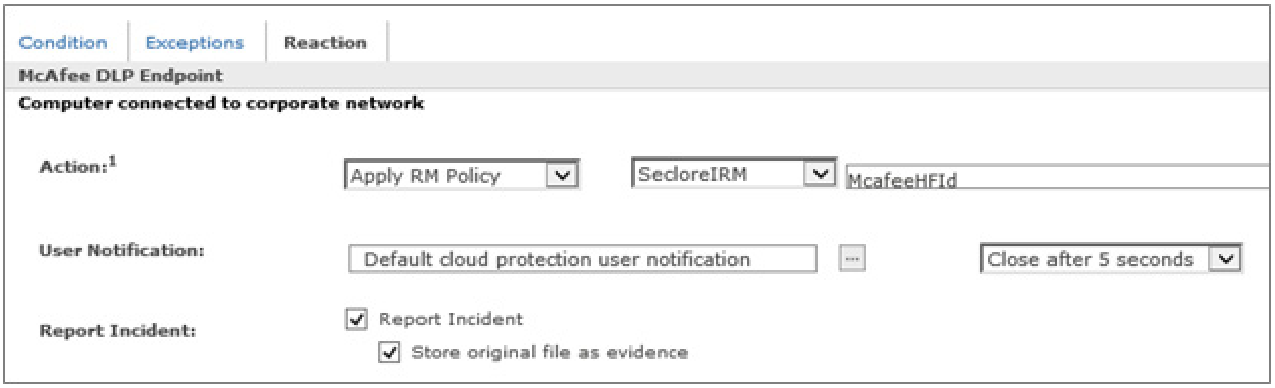
1. User creates a document and saves it

2. McAfee DLP scans document for keywords & patterns

3. On policy violation, document gets protected with Seclore

- A user saves or copies a document (containing sensitive data) on their local computer.
- McAfee DLP discovers sensitive data in a document on the endpoint – either during a scheduled or a real-time scan.
- McAfee DLP applies the relevant Seclore Rights Management policy and the document is protected.
- Whenever the document is opened anywhere in the world, Seclore’s usage controls remain in effect.
- All activities performed on the document are centrally logged in real time.

When defining a discovery rule, you can choose the relevant Seclore Rights Management policy that will be automatically applied on the discovered document – without employee intervention – to ensure your information is fully secured.



McAfee DLP Endpoint

Computer connected to corporate network

Action:[1] Apply RM Policy | SecloreIRM | McafeeHFId

User Notification: Default cloud protection user notification | ... | Close after 5 seconds

Report Incident: ☑ Report Incident
☑ Store original file as evidence

ADVANTAGES OF DLP + RIGHTS MANAGEMENT

- Sensitive data sitting on users' laptops and desktops can be automatically protected through DLP scans.
- No dependence on the end user to protect sensitive information with granular usage controls.
- Once protected with Seclore Rights Management, the information stays protected with granular usage controls wherever it goes – within or outside the enterprise.
- Workflows are not interrupted to ensure timely external collaboration.
- All actions on the document, both authorized and unauthorized, are tracked for simplified audit and compliance reporting.

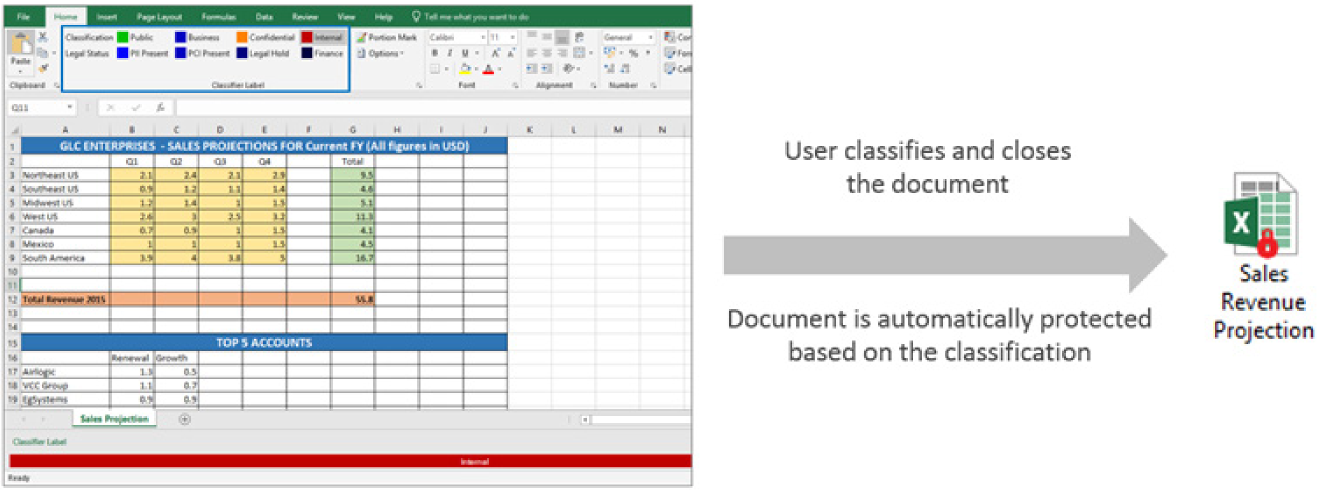
Sensitive data discovered during DLP discovery scans at endpoints can be instantly protected by Seclore. For example, Seclore protection policies can be mapped to the discovery of sensitive keywords or regular expressions (e.g. credit card numbers). These granular usage policies will control exactly who can do what with the document no matter where or how it travels.

Moreover, the attachment of the granular usage controls to the document are completely automatic. This means less effort for your end users; they don't need to do anything to add protection to the document. Automated protection in turn means less training overhead and less change management. Most importantly, you will be sure your information is properly secured and tracked - even during external collaboration.

Adding Seclore Data Classification to the Mix

Data Classification is often the first step towards data protection. Seclore Data Classification – powered by Boldon James – provides users with easy ways to classify documents with a single click. Since the documents are classified by the users themselves, chances of false positives are reduced.

- A user classifies an Office document by simply clicking on a classification in the Office ribbon.
- McAfee DLP tags the document based on the chosen classification – or can 'override' the classification if a sensitive keyword is found as a form of 'checks and balances.'
- Seclore Rights Management automatically protects the document with the appropriate usage policy based on the classification label.
- Whenever the document is opened anywhere in the world, Seclore protection remains in effect.
- All activities performed on the document are centrally logged in real time.



	GLC ENTERPRISES - SALES PROJECTIONS FOR Current FY (All figures in USD)					
	Q1	Q2	Q3	Q4		Total
Northeast US	2.1	2.4	2.1	2.9		9.5
Southeast US	0.9	1.2	1.1	1.4		4.6
Midwest US	1.2	1.4	1	1.5		5.1
West US	2.6	3	2.5	3.2		11.3
Canada	0.7	0.9	1	1.5		4.1
Mexico	1	1	1	1.5		4.5
South America	3.9	4	3.8	5		16.7
Total Revenue 2015						55.8

	TOP 5 ACCOUNTS	
	Renewal	Growth
Airlogic	1.3	0.5
VCC Group	1.1	0.7
EgSystems	0.9	0.9

User classifies and closes the document

Document is automatically protected based on the classification

KEY BUSINESS BENEFITS OF DATA-CENTRIC SECURITY

- **Automated, Granular Data Protection:** DLP-Seclore integration automates the entire process of classifying, protecting, controlling usage, and auditing. The 'handover' from detection to protection is seamless. The process of Seclore protection is completely transparent to the end user and even governs actions taken on documents while they are being utilized.
- **Security and Compliance Beyond the Firewall:** DLP-Seclore integration allows you to secure and audit data everywhere it goes without interrupting workflows: to vendor and partner networks, to public networks, to the cloud, or to mobile devices.
- **Reduced Incident Lists:** DLP can be configured to treat Seclore-protected files as safe - and not generate alerts for such files. This leads to significantly reduced incident logging.
- **Minimum Training Overhead:** There is almost zero training required for end users, since protection is automatic, and a protected document opens in the native application just like any other document.
- **Increased Business Agility:** The ability to secure your information that travels beyond your corporate borders solves a thorny compliance challenge, significantly reduces your security risks, and enables you to adopt file-sharing services, BYOD, and Cloud Computing safely and securely.
- **End-To-End Auditing and Regulatory Compliance:** DLP-Seclore integration enables you to comply with regulatory obligations for the entire lifecycle of unstructured data – both within and outside your enterprise network.
- **Enforcing Data Security Policies on Third Parties:** DLP-Seclore integration lets you enforce your data governance and corporate security policies on your contractors, vendors, partners, and other third parties.

Seclore and McAfee DLP: The Complete Data-Centric Security Solution

By combining McAfee DLP with Seclore, you will achieve unprecedented control over your unstructured information assets – with security that is content-aware, boundary-independent, and completely automated. Seclore also allows you to reap the full benefits out of McAfee DLP and extend its jurisdiction to external collaborators, the cloud, and mobile devices.

SECLORE