Seclore FileSecure IRM for Symantec DLP

Complete data governance and protection – both inside and outside your network

Symantec™ COMPATIBLE

SECLORE

Symantec DLP Endpoint significantly enhances your security, risk, and compliance requirements. It discovers and protects data lying on your employees' laptops and desktops, and prevents data leakage from these endpoints.

However, while the scope of DLP Endpoint ends at the endpoint, your confidential information doesn't. In today's flat, perimeter-less, and hyper-connected world of outsourcing, cloud computing, file sharing, BYOD, and Mobility - it is not enough to secure your organizational boundary.

Securing Information Wherever it Goes

Every single day, you send sensitive information to third parties (board members, sub-contractors, vendors, partners, auditors and lawyers) as part of regular business processes. This may include merger and acquisition information, intellectual property, engineering designs and drawings, customer information, financial data, engineering standards and designs, and more. Your employees are also likely sharing – officially or unofficially - sensitive documents over cloud-based file-sharing environments. Cloud computing, BYOD, and the use of mobile devices have further blurred the line between your organization and the 'outside world'.

All this highly sensitive information is being sent outside without any security or controls. It is sent to potential data leakage points- smaller organizations that may not have the same security infrastructure as yours, to a disgruntled vendor employee, or to a sub-contractor, without any protection whatsoever.

While most security initiatives are focused on securing the enterprise perimeter and the information inside it, there is a dire need today for an information-centric security solution. A solution that can enable data governance, risk mitigation, and data protection even outside your corporate firewall.

The security offered by DLP is applicable only within your organization's boundaries. That's great as far as it goes. But if you regularly need to send your confidential data outside your network perimeter – that doesn't go very far. And neither does your security.

Symantec DLP and Seclore FileSecure Integration: Extending Your Security Reach

Seclore FileSecure Information Rights Management (IRM) can be easily integrated with Symantec DLP to extend your security reach to information traveling outside of your perimeter. Here are some advantages of the combined offerings:

Extending Security and Compliance Beyond the Firewall: The integration of Symantec DLP and Seclore FileSecure IRM provides end-to-end protection of information and keeps your data in your control – even when it leaves your DLP's control. Seclore FileSecure IRM can seamlessly take over where Symantec DLP Endpoint protection ends – and then stay with the file wherever it travels. IRM policies can be mapped to information flow and data usage patterns – thus ensuring that your critical assets remain secure even when they are shared with vendors or partners. Thus, your security and risk infrastructure gets extended to wherever your confidential information travels –anywhere in the world.

Reduced Incident Lists: IRM-protected files can be detected by the DLP system. DLP can then be configured to not generate alerts and incidents for information that is already IRM protected. This will lead to significantly reduced incident logging, which in turn leads to less overhead.

Reduced False Positives: Innocent data triggering rules can frustrate day-to-day business processes – not to mention end users. Using Symantec DLP in combination with Seclore FileSecure's data classification capabilities, the chances of false positives are virtually eliminated. Since files can be classified by user-based inputs, there are fewer chances of the file classification being incorrect – compared to the chances of innocent information being flagged by DLP as sensitive. DLP rules can then be triggered based on this classification, thus virtually eliminating the risk of false positives.

http://www.Symantec.com/apps/partners/partnerlisting.aspx?region=us#seclore

Increased Business Agility: DLP-IRM integration enables you to implement document distribution control (DLP) as well as document usage control (IRM). The freedom to secure your information that travels beyond your corporate borders makes your business more agile and enables you to achieve business objectives, while significantly reducing enterprise risk – whether it is for outsourcing, working with new partners, or for adopting new cloud storage solutions.

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

End-to-End Auditing and Regulatory Compliance: IRM gives you complete visibility over who accessed the file, at what time, for what purpose (viewing, editing, copying content and printing) and in what location. With DLP-IRM integration, you can now fulfill your regulatory obligations for confidential information during its entire lifecycle – both within and outside your enterprise boundary.

Granular Security to Maximize Control: DLP actions can be categorized under two broad umbrellas – allowing or blocking data distribution. Using IRM in conjunction with DLP, you can send files out to intended recipients with restricted access and usage controls. Unintended recipients won't be able to access the information at all – even if they get hold of the file.

Automated Data Protection: The integration of Symantec DLP and Seclore FileSecure IRM presents a way to automate the process of classification, protection, access management, and auditing. Users do not need to protect files manually; a file is protected as soon as confidential data is discovered. The act of protection is completely transparent to the end user.

Minimum IT Overhead: Once DLP and IRM rules are mapped configured and mapped, there is hardly any need for any IT involvement. Files get protected during normal discovery scans or DLP rules get triggered based on the Seclore FileSecure classifications on metadata for the file.

Content-Aware IRM and Boundary-Independent DLP

Important features of Seclore FileSecure IRM:

Boundary Independence: *Equally effective security both within and outside the enterprise network*

Persistent Protection: *Secures information regardless of where and how it is stored, transmitted, or accessed*

Remote-Control: *Retain control of the information, even after it is shared, copied, or forwarded*

DLP solutions are content-aware: they can read the content of a document and take appropriate actions on it when a DLP policy is violated or a rule is triggered. On the other hand, IRM solutions cannot read inside a document, but can block and enforce granular access and usage controls (viewing, editing, printing, re-distribution) to it for different users. An effective DLP and IRM combination can allow an organization unprecedented control over its digital assets – by ensuring both distribution control and access/usage control of information.

Seclore FileSecure IRM has the ability to:

a) Build an ***intelligent firewall around the file itself*** – so that IRM protection is applied to all copies of the document – regardless of mode of transfer – email, USB, shared folders, and more. This firewall allows or blocks access depending on predefined access permissions.

b) ***Enforce granular access permissions on*** *files and emails based on action (viewing, editing, printing, screen captures, macros), time (number of days or a date range), and location (specific computer, IP addresses) for every user or team - and any combination of these.*

Monitoring and Auditing: *Track and audit information at all times or in all locations*

Instant Information Expiry: *Immediately revoke access to information at any time, regardless of where the information actually resides*

Time-based Controls: *Send documents out with in-built time-based controls*

Location-based Controls: *Restrict file access to specific computers, specific IP addresses and networks*

Mobile Support: *Support for iOS and Android devices*

Agentless Access: *No agent required to view protected content*

Single-agent Access: *One desktop agent for all file formats and applications for performing advanced operations (editing, printing, copying)*

File Format and Application Support: *Support for over 140 file formats and numerous applications*

Centralized Usage Policy Lists: *Centralized and easy access to usage permission policies.*

c) ***Monitor and audit*** access to documents and maintain a complete audit trail of the time, location and other details of the activities performed on the content.

WHO can access it — Users, Teams, Groups.

WHAT they can do it — Read Only, Edit, Print, Copy, Re-Distribute, Take Screenshots.

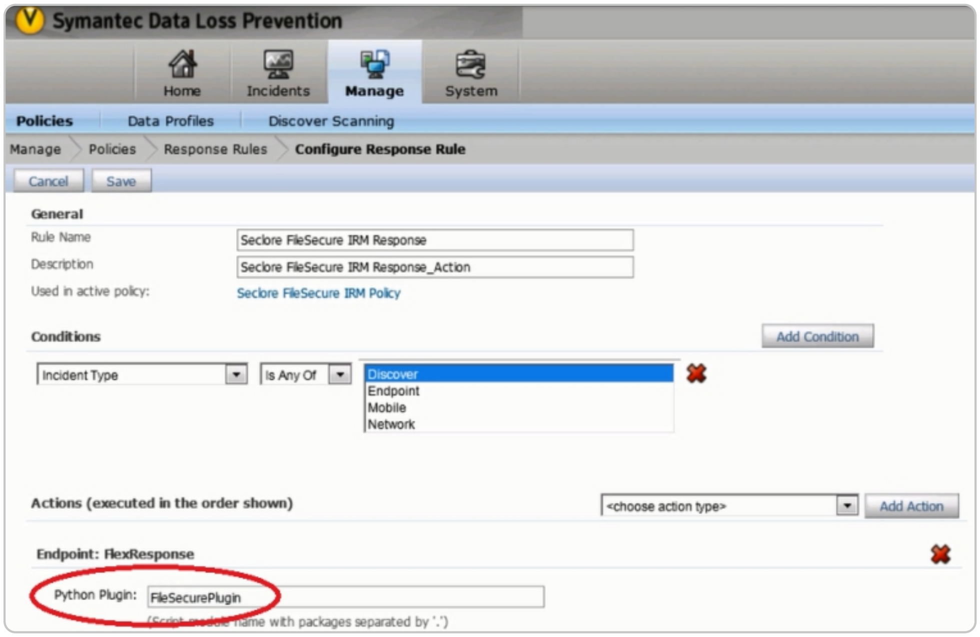
WHEN they can do it — Specific Days, Dates and Times, a Date Range.

WHERE they can do it — IP Addresses, a Specific Device only, a Specific Computer Only.

d) ***Dynamically update access permissions*** applied on a document: you can change (or revoke) access levels on a document for any user at anytime from anywhere.

Applying IRM Policies on Discovered Information

A DLP discovery rule can discover a file with a particular sensitive keyword or tag - and can then apply the appropriate IRM policies to the file. These policies persist with the document even when it travels beyond the endpoint. When defining a DLP Discovery Rule, you can now choose the relevant Seclore FileSecure policy for the file.



General

Rule Name: Seclore FileSecure IRM Response

Description: Seclore FileSecure IRM Response_Action

Used in active policy: Seclore FileSecure IRM Policy

Conditions

Incident Type | Is Any Of | Discover, Endpoint, Mobile, Network

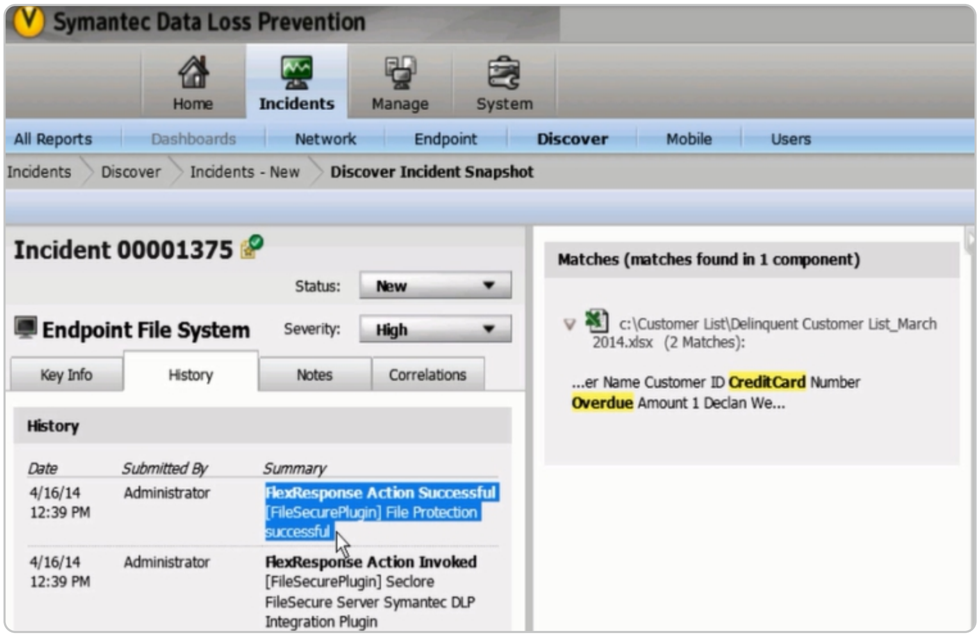
Actions (executed in the order shown) <choose action type>

Endpoint: FlexResponse

Python Plugin: FileSecurePlugin

(Script module name with packages separated by '.')

For example, all files with sensitive information (e.g. a credit card number) can be discovered and automatically encrypted and protected with Seclore FileSecure IRM. All confidential data discovery is logged.



Incident 00001375

Status: New

Endpoint File System

Severity: High

History

Date	Submitted By	Summary
4/16/14 12:39 PM	Administrator	FlexResponse Action Successful [FileSecurePlugin] File Protection successful
4/16/14 12:39 PM	Administrator	FlexResponse Action Invoked [FileSecurePlugin] Seclore FileSecure Server Symantec DLP Integration Plugin

Matches (matches found in 1 component)

c:\Customer List\Delinquent Customer List_March 2014.xlsx (2 Matches):

...er Name Customer ID CreditCard Number Overdue Amount 1 Declan We...

Reading Seclore FileSecure Classification Metadata

DLP rules can be triggered based on the Seclore FileSecure classification of the file. The Seclore FileSecure classification is stored in file metadata in plain text form.

A New Way Forward: Not Just a Technology Integration, but a Business Enabler

While most organizations have been investing in solutions that stop information from leaving the organization and protecting the perimeter from attack, the truth is that your organization is likely sending sensitive information, unprotected, beyond the boundary of your enterprise every day.

The seamless integration of Symantec DLP with Seclore FileSecure IRM will enable your organization to protect information wherever it goes, enabling you to embrace external collaboration, mobile devices and the Cloud with confidence.

About Seclore

Seclore offers an innovative solution, FileSecure, which enables organizations to control access to information wherever it goes, both within and outside of the organization's boundaries. The ability to remotely control who can view, edit, copy, and distribute unstructured information empowers organizations to embrace mobility, Cloud, and external collaboration with confidence. The most integration-friendly solution on the market, Seclore FileSecure extends and enhances the security of information detected and downloaded from DLP, ECM, ERP systems and attached to Mail/Messaging solutions through pre-built connectors. With nearly 4 million users across 420 companies in 22 countries and rapidly growing, Seclore is helping organizations achieve their security, privacy and compliance objectives.

SECLORE

Securing Information Wherever it Goes

www.seclore.com | info@seclore.com | blog.seclore.com

USA

USA
560 S. Winchester Blvd., San Jose, CA 95128
1-650-619-7801

INDIA

Mumbai
Corporate Office
Excom House Ground Floor, Plot No. 7 & 8
Off. Saki Vihar Road Sakinaka, Mumbai – 400 072
+91 22 6130 4200 | +91 22 6143 4800

Bengaluru
Regional Office
5th Floor, Vakil Square, Bannerghatta Road
Opp. Jayadeva Hospital. Bengaluru – 560 076
+91 97425 11179

Gurgaon
Regional Office
OCUS Technopolis, Golf Course Road
Sector 54, Gurgaon - 122 001
+91 0124 4626 161