SECLORE

DATASHEET
Seclore FileSecure IRM for Symantec DLP

Symantec

Seclore FileSecure IRM for Symantec DLP

Neil MacDonald
VP and Gartner Fellow

> “*The need to place and enforce DRM 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 technology can detect and monitor sensitive data and prevent it from leaking outside your enterprise. However, your confidential data is sent outside your enterprise for genuine business reasons – to numerous contractors, vendors, and partners – without any security or controls. Seclore FileSecure IRM for Symantec DLP enables you to extend your data security capabilities to wherever your information travels.

You can control who can access a file, what they can do with it, when, and from which computer or device. With such persistent, file-centric controls, the scope of Symantec DLP can be extended to files travelling through public and partner networks, stored on the cloud or file-sharing services, or accessed on mobile devices.

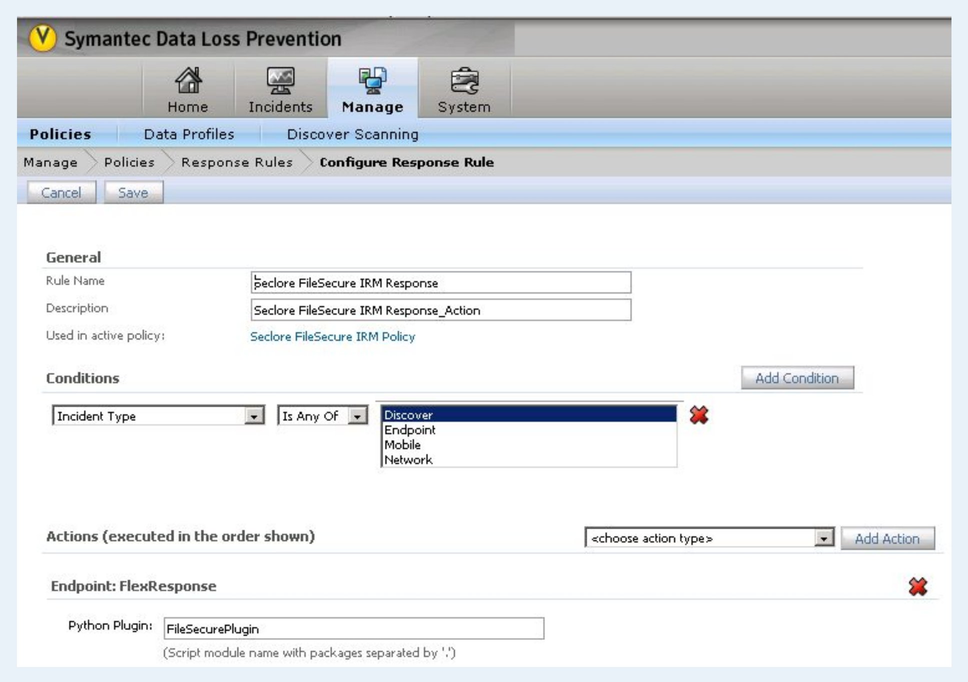
Applying Seclore FileSecure IRM Policies on Information Discovered by Symantec DLP

Confidential files discovered by Symantec DLP can be automatically protected by Seclore FileSecure IRM. When defining a DLP discovery rule in the Symantec Enforce console, you can choose the relevant Seclore FileSecure IRM policy that will be applied to the discovered file.

If disgruntled employees find it so easy to leak data (most data leaks occur from within), imagine how much higher the risk is in case of disgruntled vendors or partners, who lie outside your DLP jurisdiction and are not restrained by your security infrastructure in any way.

Seclore FileSecure IRM for Symantec DLP actually enforce your corporate IT policies on your vendors, partners, lawyers – anyone who access your information.

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



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

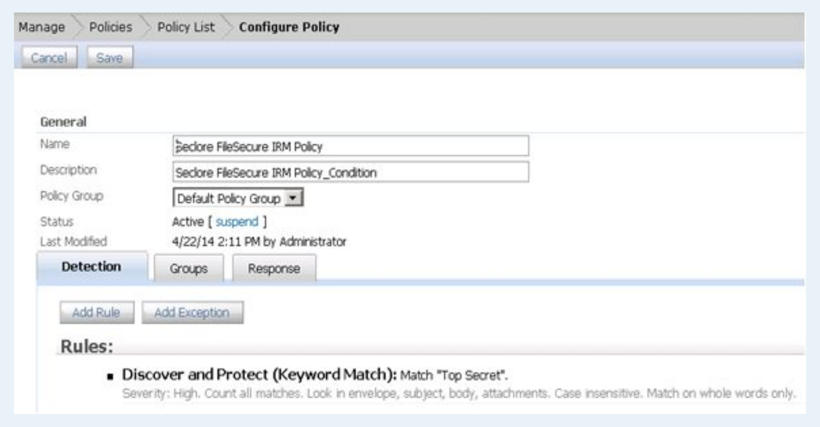
Actions (executed in the order shown) <choose action type>

Endpoint: FlexResponse

Python Plugin: FileSecurePlugin
(Script module name with packages separated by '.')

Reading Seclore FileSecure Classification Metadata

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



General

Name	Seclore FileSecure IRM Policy
Description	Seclore FileSecure IRM Policy_Condition
Policy Group	Default Policy Group
Status	Active [suspend]
Last Modified	4/22/14 2:11 PM by Administrator

Rules:

- Discover and Protect (Keyword Match): Match "Top Secret".
  Severity: High. Count all matches. Look in envelope, subject, body, attachments. Case insensitive. Match on whole words only.

Supported Symantec components:

- *Symantec DLP Endpoint Discover 11.5 and above*
- *Python 2.6 and above*

Key Business Benefits

Security and Compliance Beyond the Firewall

DLP-IRM 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 FileSecure Data Classification and Symantec DLP drastically reduces the chances of false positives during data discovery.

Reduced Incident Lists

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

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

Automated Data Protection

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

Enforcing IT Policies on Third Parties

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

Making DLP Boundary-Independent and IRM Content-Aware

DLP solutions are content-aware but are constrained inside your corporate boundary. IRM solutions are not content-aware, but can enforce persistent security that is independent of boundaries. By combing Symantec DLP with Seclore FileSecure IRM, you will achieve unprecedented control over your unstructured information assets – with security that is both content-aware and boundary-independent. Seclore FileSecure IRM allows you to reap the full benefits out of Symantec DLP and extend its jurisdiction to external collaborators, the cloud, and mobile devices.