Solution Brief

Integrated Box Security Classification with Symantec CloudSOC and Symantec DLP

Automatically identify, classify and govern your sensitive data in Box with native Box Governance Security Classification using industry-leading Symantec CloudSOC CASB[1] and Symantec Cloud DLP[2]. Get the advantage of using native Box capabilities with the automation of CASB policy controls and the fine-tuned, enterprise-wide content policies of DLP.

Symantec™

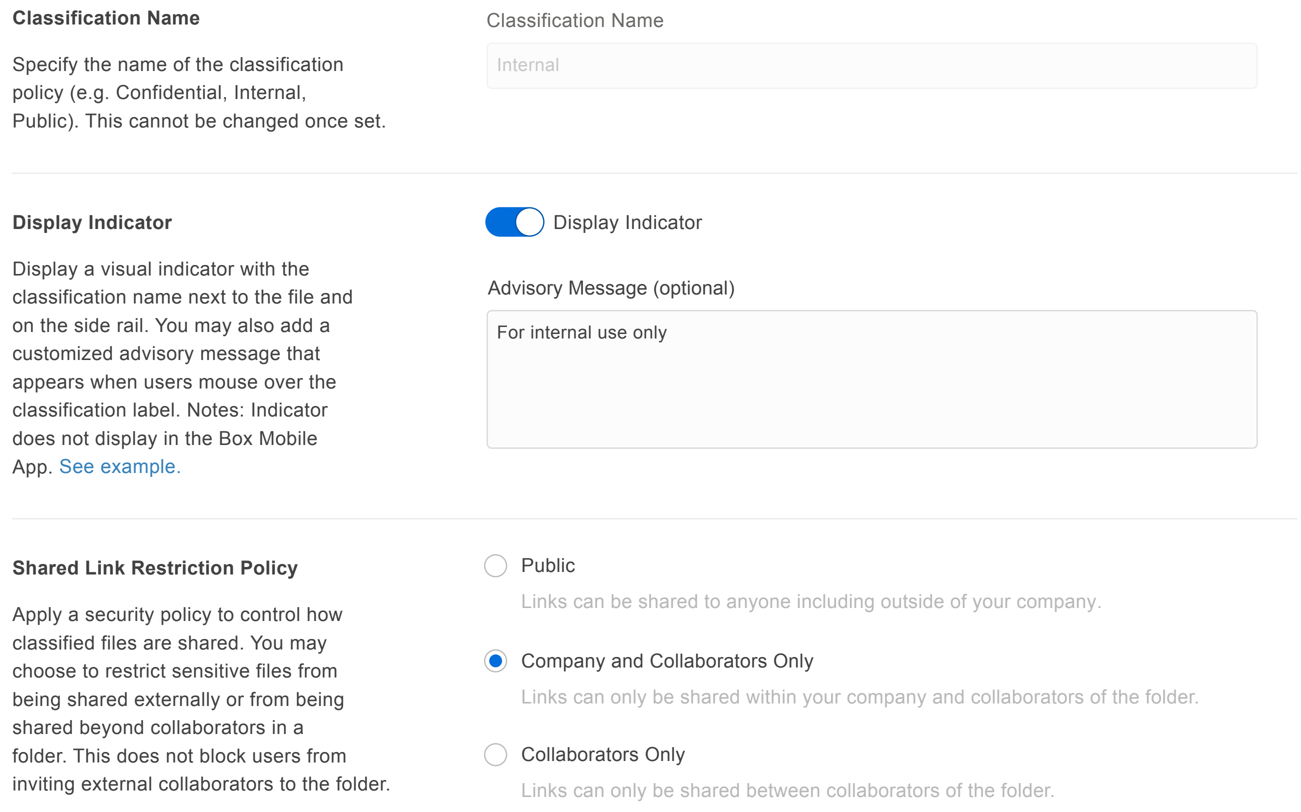
1. Forrester Wave™: Cloud Security Gateways, Q4 2016
2. Gartner Magic Quadrant for Enterprise Data Loss Prevention, 16 February 2017

Get Started

Once you have a Box Governance subscription and Symantec CloudSOC you can easily classify content types based on the security criteria you want and control how those files are shared.

1 Set up security classification in box governance

Start by setting up file classification labels in Box Governance Content Controls. Here you name the classification; set up visual cues for end users to identify types of content and provide additional information on what to do with this type of file; and specify the Box sharing policy for this type of data.



Classification Name

Specify the name of the classification policy (e.g. Confidential, Internal, Public). This cannot be changed once set.

Classification Name

Internal

Display Indicator

Display a visual indicator with the classification name next to the file and on the side rail. You may also add a customized advisory message that appears when users mouse over the classification label. Notes: Indicator does not display in the Box Mobile App. See example.

● Display Indicator

Advisory Message (optional)

For internal use only

Shared Link Restriction Policy

Apply a security policy to control how classified files are shared. You may choose to restrict sensitive files from being shared externally or from being shared beyond collaborators in a folder. This does not block users from inviting external collaborators to the folder.

○ Public

Links can be shared to anyone including outside of your company.

● Company and Collaborators Only

Links can only be shared within your company and collaborators of the folder.

○ Collaborators Only

Links can only be shared between collaborators of the folder.

Setup Screen on Box

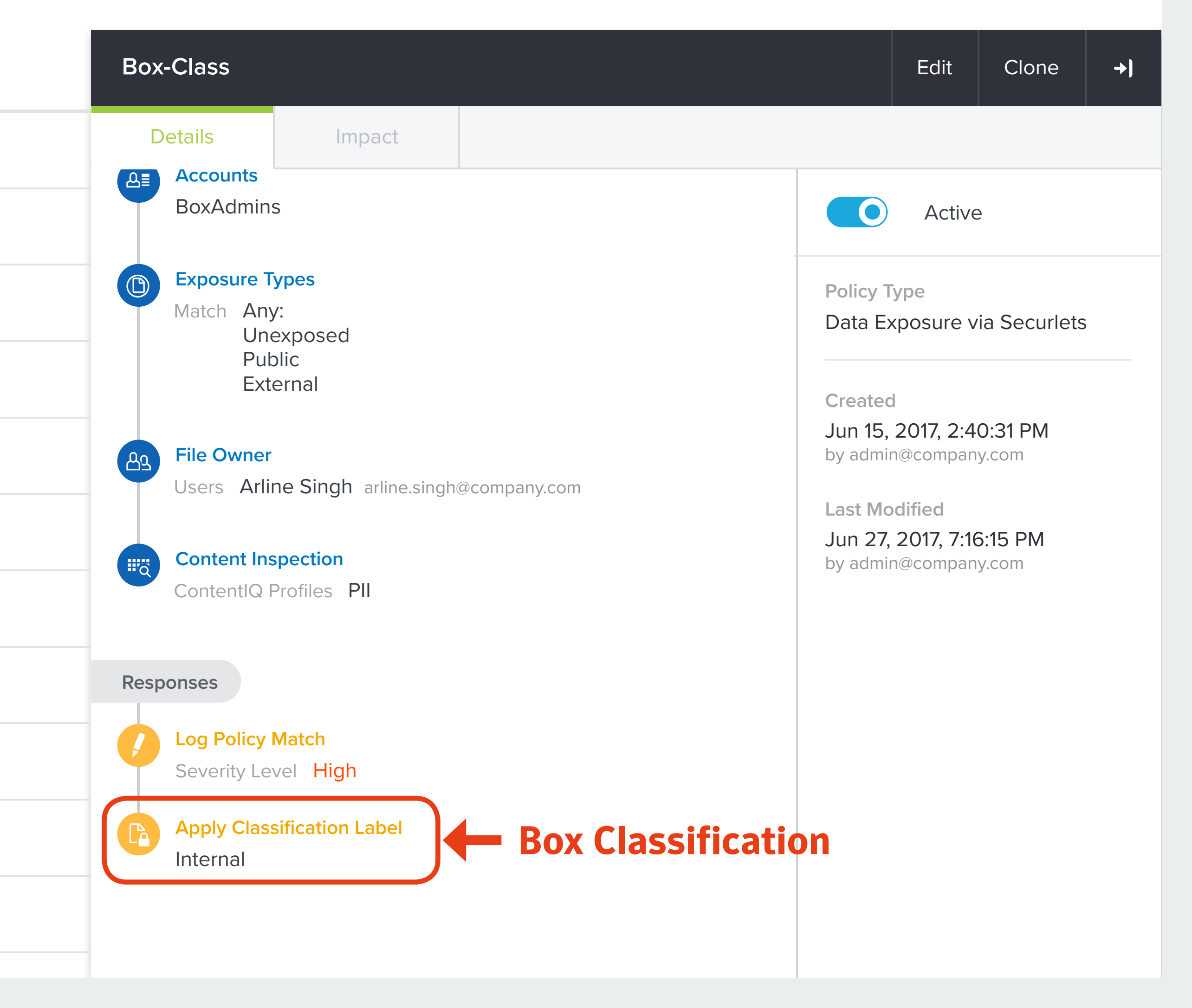
2 Accurately Identify File Content

Since Symantec DLP is the industry-leading enterprise DLP solution in the market, you may already have a Symantec DLP policy tuned to identify specific classes of data for your organization. If so, just leverage the policies you already have for Box. If you don't already have a matching content policy in place, you will want to create one. Symantec DLP offers an extensive array of content identification technologies to help you accurately identify what type of content is in a file – one of the reasons we think it does so well in Gartner's Magic Quadrant.

If you are not using Symantec DLP, you can create a ContentIQ profile directly in CloudSOC. ContentIQ profiles are easy to set up and are highly accurate thanks to the machine-learning in the ContentIQ DLP engine native to CloudSOC. In addition to automated classifications, ContentIQ can apply data science that learns to identify forms specific to your organization. And if you want to add custom dictionaries and regular expressions, that's available too.

3 Activate Automated Classification Policy Control

Put all the pieces together with a CloudSOC policy that will automatically inspect file content based on your DLP policies and apply the appropriate Box Security Classification.



Box-Class

Accounts
BoxAdmins

Exposure Types
Match Any:
Unexposed
Public
External

File Owner
Users Arline Singh arline.singh@company.com

Content Inspection
ContentIQ Profiles PII

Responses

Log Policy Match
Severity Level High

Apply Classification Label
Internal

Active

Policy Type
Data Exposure via Securlets

Created
Jun 15, 2017, 2:40:31 PM
by admin@company.com

Last Modified
Jun 27, 2017, 7:16:15 PM
by admin@company.com

Box Classification

Policy Details on CloudSOC

An Integrated Solution in Action

Once you've completed the above setup, here's how it will operate:

1. A user uploads or modifies a file in Box.
2. CloudSOC is alerted of a new file to inspect in Box through an API integration.
3. CloudSOC inspects that file using either a native ContentIQ profile or integrated Symantec DLP Cloud.
4. If the file matches content inspection criteria, CloudSOC triggers the Box API to apply the security classification label.
5. Box tags that file with the appropriate classification label and enforces the established permissions for file sharing.

Strong security
protects today's business

Our tightly integrated information-centric security gives you the confidence to do business in today's environment of always-on data sharing.

Contact your local Symantec sales representative or business partner ❯ **www.symantec.com**

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit **www.symantec.com** or connect with us on **Facebook**, **Twitter**, and **LinkedIn**.

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com