

REDUCE FALSE POSITIVES WITH DLP in CGSaaS CONFIG

December 2018

Brian Heffner
bheffner@checkpoint.com

OVERVIEW	2
ASSUMPTIONS & REQUIREMENTS.....	2
DLP CONFIGURATION.....	3
VIEW EVENTS BY GOING TO THE EVENTS TAB	7
ADDITIONAL RESOURCES	7

Overview

- The purpose of this white paper is to reduce DLP false positives. This document is written to help you reduce the number of false positives in the DLP config of Cloud Guard SaaS. With Check Point's powerful DLP engine, can come a high amount of false positives. False positives are the result of the strength and depth of Check Point's DLP engine. We have a large amount of DLP power. As with any power, it must be controlled. As a result, of this DLP noise it is important to configure your DLP rules correctly.
- CLOUDGUARD SAAS - SAAS SECURITY IS ONE CLICK AWAY
 - To protect from SaaS threats, Check Point offers Cloud Guard SaaS – a new cloud service that prevents attacks on enterprise SaaS applications, within minutes' deployment.
 - Prevent malware and zero-day threats from getting into SaaS apps
 - Blocks cybercriminals from taking over employee SaaS accounts with ID-Guard technology
 - Keeps data protected by blocking sensitive data sharing and forcing its encryption
 - Provides full security coverage with synced policies and unified management across gateways, endpoints, and cloud

Assumptions & Requirements

This guide makes the following assumptions:

- Your Check Point Cloud portal at <https://portal.checkpoint.com> is already provisioned and you have your login name and password.
- You have already configured the API connection for your SaaS application.

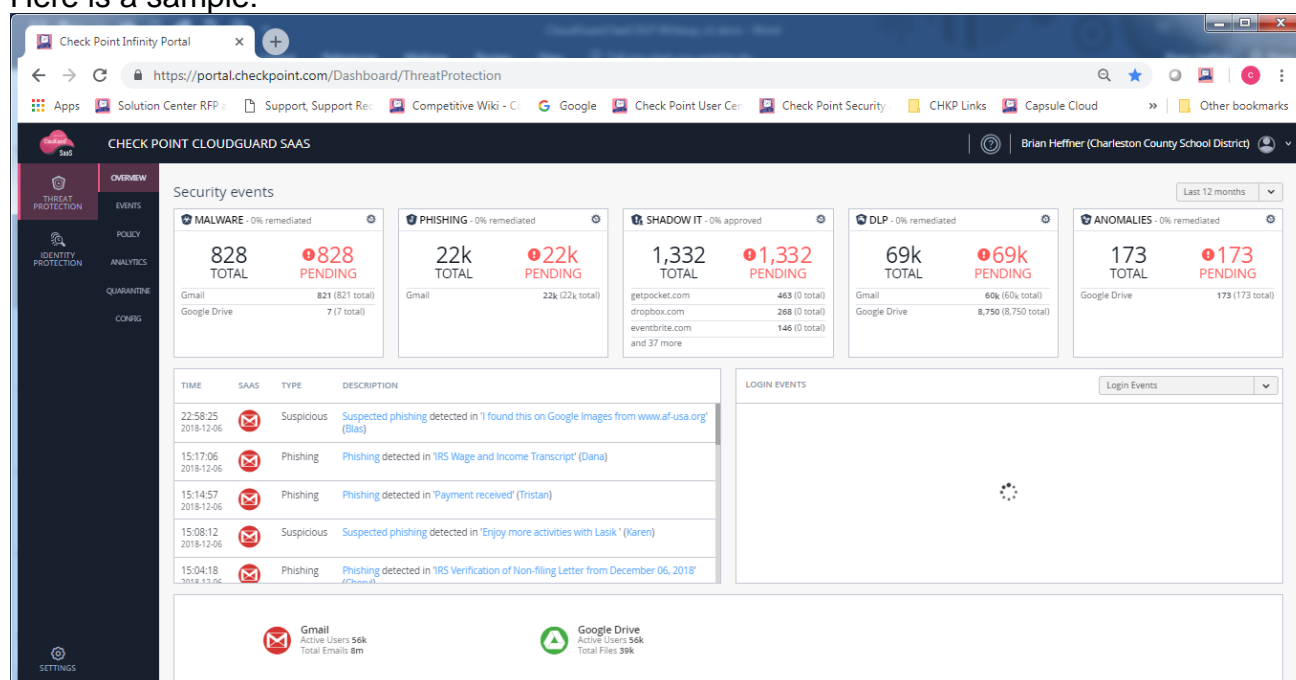
DLP Configuration

The necessary important steps are below to configure your DLP correctly. These steps are critical for **both** a high catch rate and to eliminate false positives.

IMPORTANT: AT THIS TIME DLP IS MONITOR ONLY AND NOT PREVENT!!!

After you login to <https://portal.checkpoint.com>, you will see the overview page.

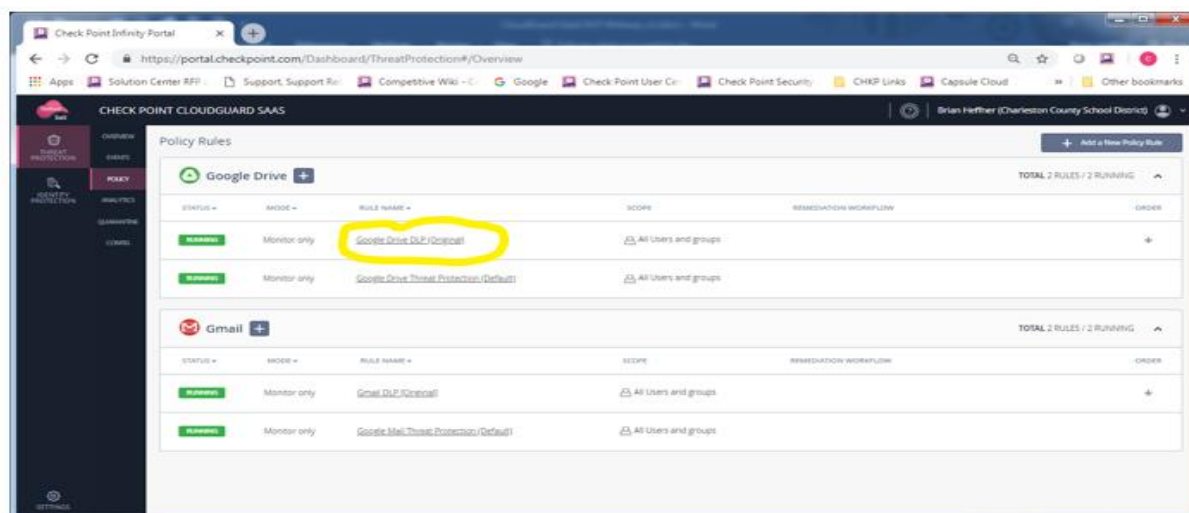
Here is a sample:



Next, choose Policy from the menu on the left side of the overview page.

We will start by configuring DLP policy for Google Drive

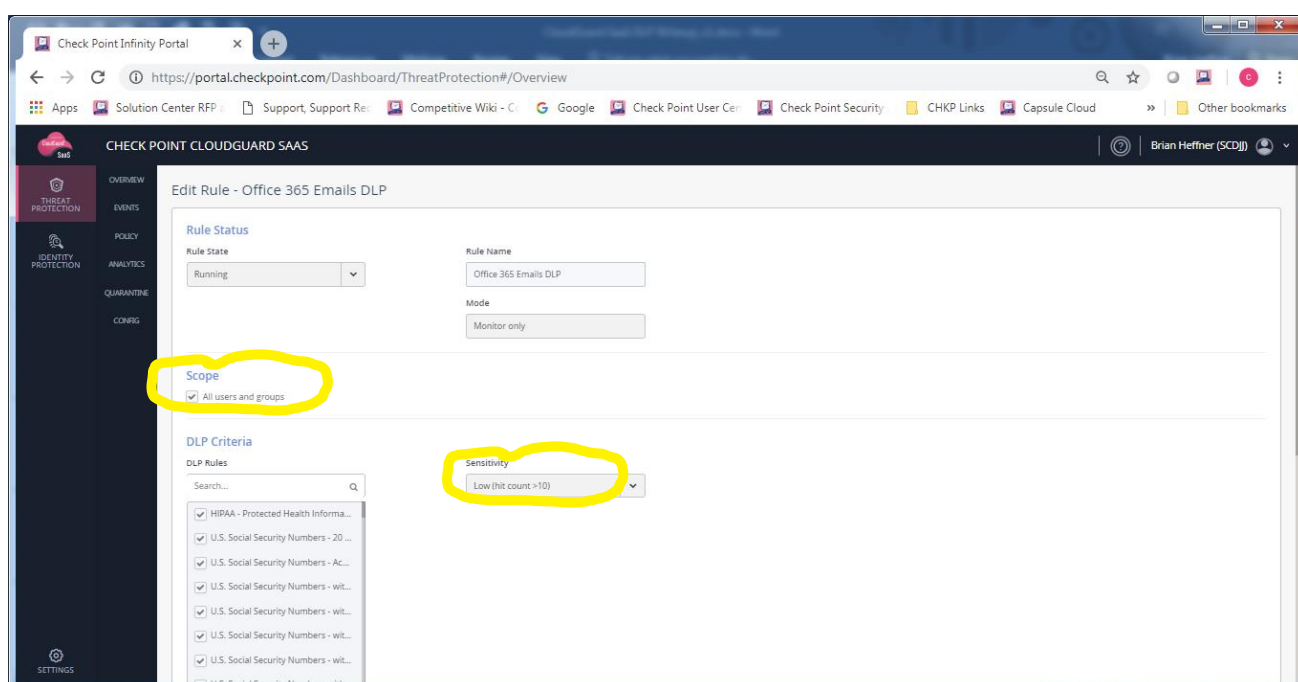
Here is a sample screen of the policy:



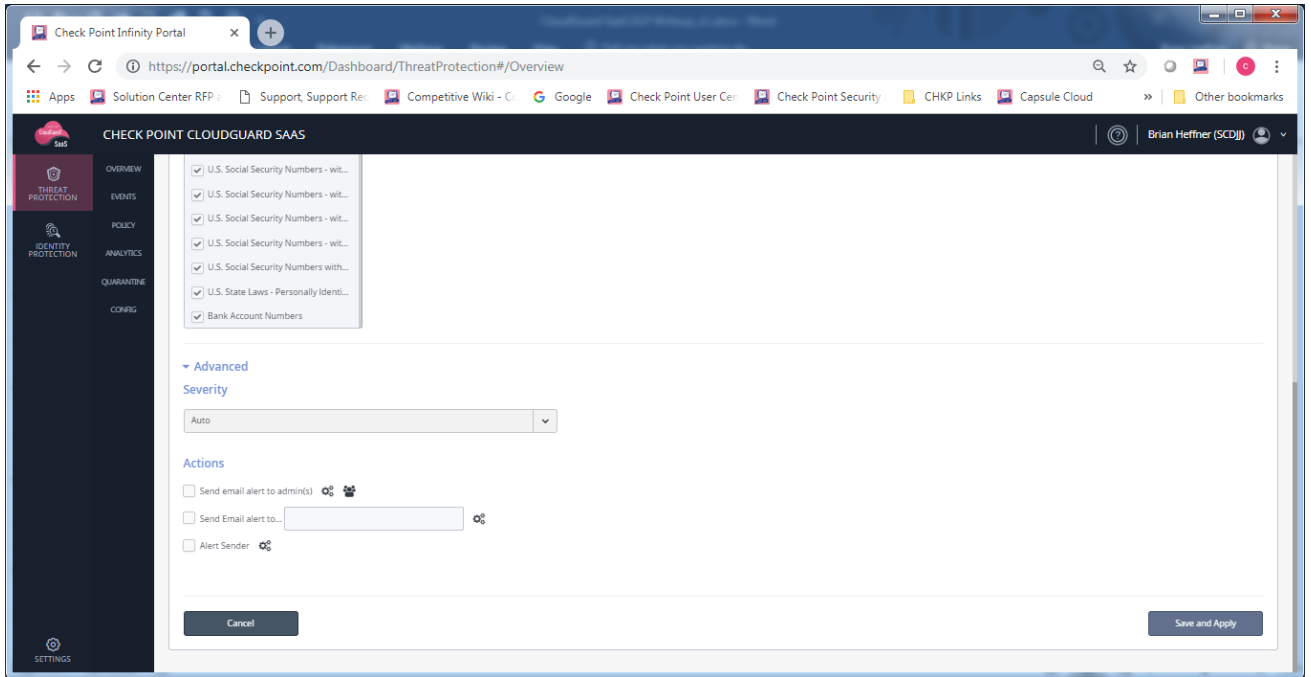
Next click on the first DLP rule for Google Drive and match this setup. The most important parameter below is the “sensitivity” parameter. If you select all of the DLP protections and

set the sensitivity to very high (hit count >2), you will of course get many false positives. Therefore the best approach is to adjust the data types to be specific to the customer's needs and set the sensitivity to Very low (hit count >20) initially. For example, there is a DLP data type that is just 9 digits long for social security numbers, which by enabling can cause high false positives. (Note: You can leverage the 77.30 data type library as a guide since the data types used in Cloud Guard SaaS are similar.) The data types are listed under the DLP criteria box at bottom left. You should be as granular as possible.

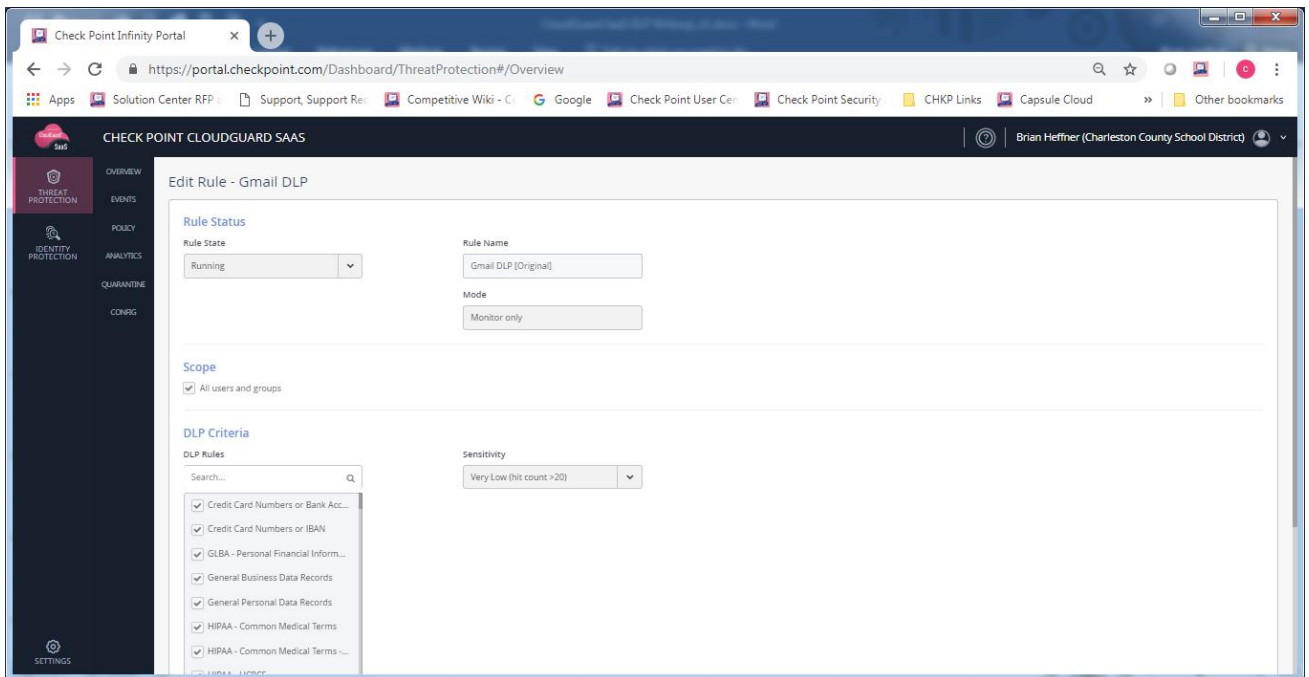
The next important piece highlighted is the scope. When you create the rule, you are able to select the scope for that rule. You cannot make exclusions on DLP at this time. Therefore, make sure to only select the users needed in the scope when you create the rule.



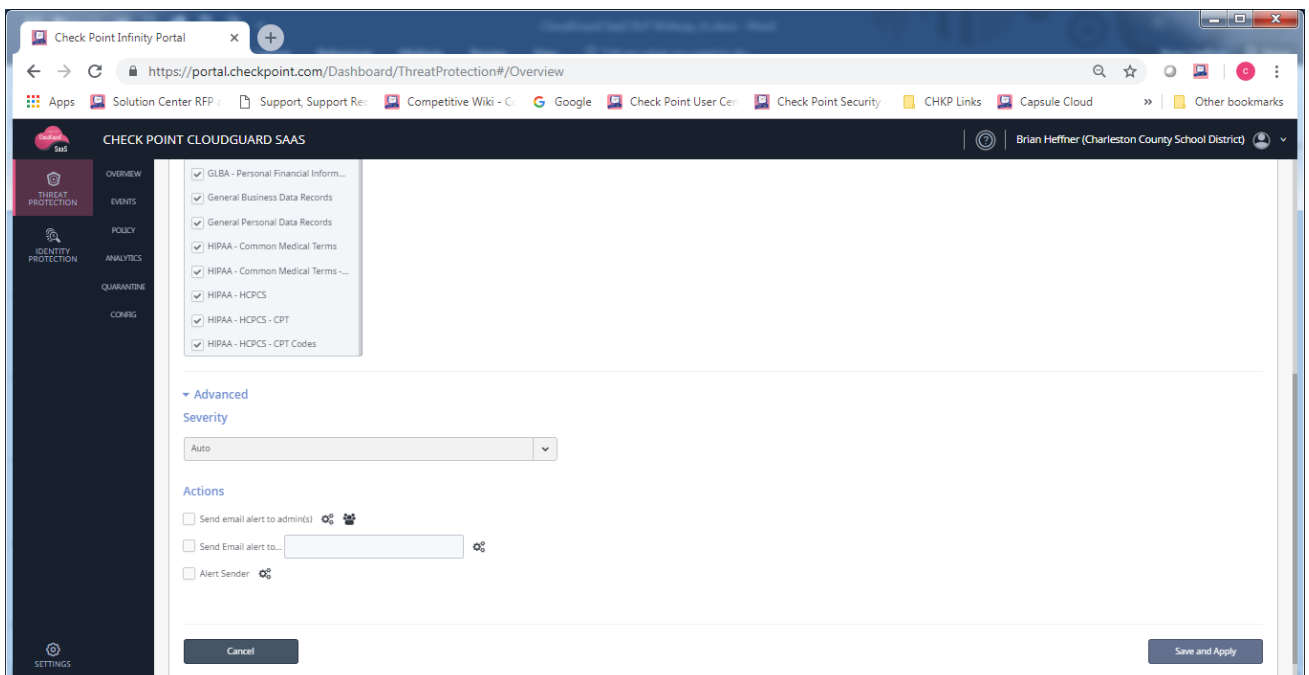
Next, Make sure to click “Save and Apply.”



Next, go back to the policy page, click on the first DLP rule for Gmail and duplicate the setup you did above for file storage. In most environments, the same DLP settings will match between file storage and email communications. Of course, you can customize where necessary. In regards to DLP, Microsoft and Google settings would be the same, so you can apply this information to both environments.



And



Make sure to click "Save and Apply."

View events by going to the EVENTS TAB

On the events tab you have the capability to filter by type, either on all threat protection or just DLP events. On DLP events, as the ones listed below, you will see a dismiss option. The dismiss option when clicked only removes the event from the overview page. It does not do anything else.

The screenshot shows the Check Point Infinity Portal interface. The top navigation bar includes 'CHECK POINT CLOUDGUARD SaaS' and the user 'Brian Heffner (SCDJ)'. The left sidebar has tabs for 'THREAT PROTECTION', 'POLICY', 'IDENTITY PROTECTION', 'ANALYTICS', 'QUARANTINE', and 'CONFIG'. The main content area is titled 'EVENTS' and features three donut charts: 'Events by Severity' (4688 MEDIUM), 'Events by State' (4688 NEW), and 'Events by SaaS' (135 OFFICE 365 ONEDRIVE, 44410 OFFICE 365 EMAILS, 88 OFFICE 365 SHAREPOINT). Below the charts is a 'Security Events' section with a search bar and filters. The table below shows a list of events with columns for Time, State, Severity, SaaS, Type, Event Description, Workflow, and History. The 'Workflow' column for several events contains a link labeled 'Alert Sender Dismiss', which is highlighted with a yellow circle.

TIME	STATE	SEVERITY	SaaS	TYPE	EVENT DESCRIPTION	WORKFLOW	HISTORY
11:02:07 2018-12-28	NEW	MEDIUM		DLP	Check Point DLP has detected U.S. Social Security Numbers - without Delimiters leak in 'Drug Screen Receipt' (KRALLE@SCDJ.net's mailbox)	Alert Sender Dismiss	
11:02:04 2018-12-28	NEW	MEDIUM		DLP	Check Point DLP has detected U.S. Social Security Numbers - without Delimiters leak in 'Drug Screen Receipt' (KRALLE@SCDJ.net's mailbox)	Alert Sender Dismiss	
10:38:56 2018-12-28	NEW	MEDIUM		DLP	Check Point DLP has detected U.S. Social Security Numbers - without Delimiters leak in 'Drug Screen Receipt' (KRALLE@SCDJ.net's mailbox)	Alert Sender Dismiss	
10:38:55 2018-12-28	NEW	MEDIUM		DLP	Check Point DLP has detected U.S. Social Security Numbers - without Delimiters leak in 'Drug Screen Receipt' (KRALLE@SCDJ.net's mailbox)	Alert Sender Dismiss	
10:28:02 2018-12-28	NEW	MEDIUM		DLP	Check Point DLP has detected U.S. Social Security Numbers - without Delimiters leak in 'Drug Screen Receipt' (KRALLE@SCDJ.net's mailbox)	Alert Sender Dismiss	
10:28:01 2018-12-28	NEW	MEDIUM		DLP	Check Point DLP has detected U.S. Social Security Numbers - without Delimiters leak in 'Drug Screen Receipt' (KRALLE@SCDJ.net's mailbox)	Alert Sender Dismiss	

Additional Resources

1. Check Point Cloud Guard SaaS Getting Started Guide
2. Check Point Cloud Guard SaaS Identity Protection Guide
3. Check Point Cloud Guard SaaS Manual Configuration with Office 365
4. Check Point Cloud Guard SaaS Threat Protection Admin Guide
5. Check Point Infinity Portal Admin Guide

All documents above available from this link:

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doShowproductpage&product=495