



# CLOUDGUARD SAAS THREAT EXTRACTION

December 2018

**Brian Heffner**  
bheffner@checkpoint.com

**OVERVIEW ..... 2**

**ASSUMPTIONS & REQUIREMENTS..... 2**

**ENVIRONMENT PROBLEM..... 3**

**RESOLUTION ..... 5**

**ADDITIONAL RESOURCES ..... 6**

## Overview

- The purpose of this whitepaper is to explain a confusing Threat Extraction “scan details” action within CloudGuard SaaS. I will be focusing on something called “**should replace.**” We will be focused on the Threat Protection portion of the portal and not the Identity Protection portion. In addition, we will NOT be reviewing DLP.
- CLOUDGUARD SAAS - SAAS SECURITY IS ONE CLICK AWAY
  - To protect from SaaS threats, Check Point offers CloudGuard 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

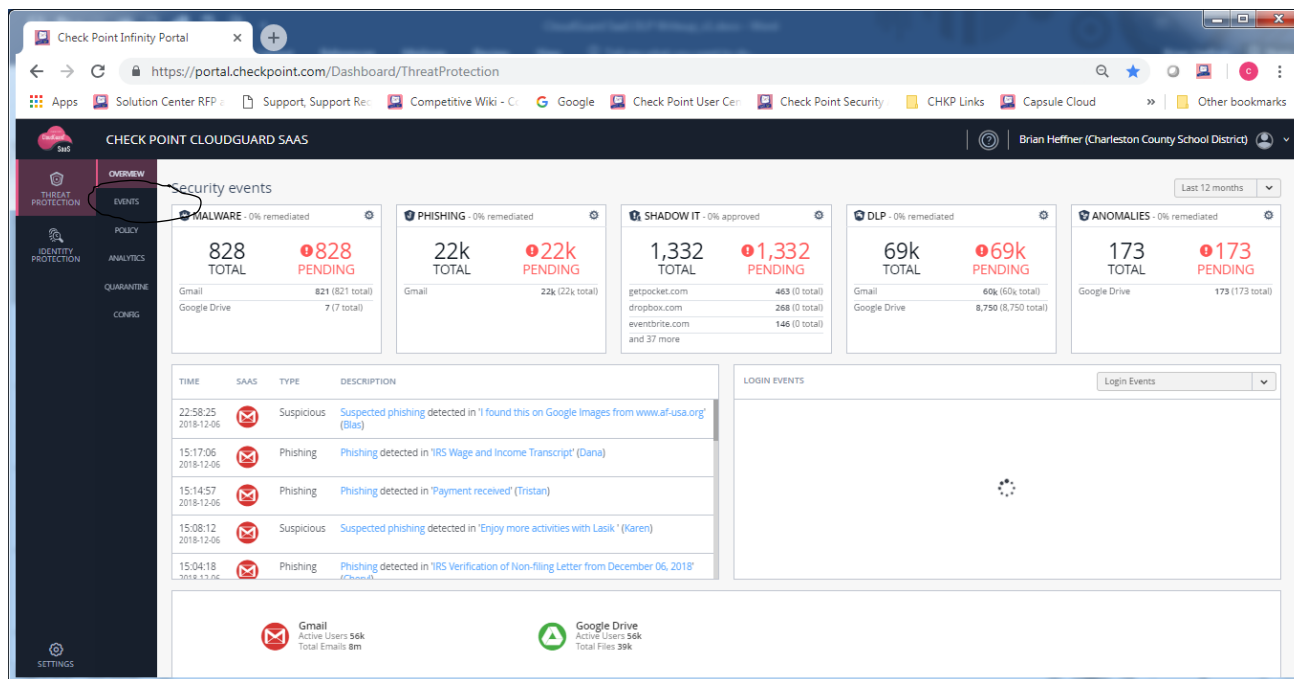
## Assumptions & Requirements

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.

# ENVIRONMENT PROBLEM

CloudGuard SaaS portal already setup against Microsoft or Google email.  
After you login to <https://portal.checkpoint.com>, you will see the overview page.  
Here is a sample:



Next, you would choose EVENTS from the menu on the left side of the overview page.

Here is a sample screen of an event you would normally see:

The screenshot displays the 'Security Stack' interface. The top section is the 'Email Profile' for an email from 'SCEIS Business Objects Report (bu.bobj@admin.sc.gov)' to 'Roger A. Muir (RAMUIR@scdj.net)'. The subject is 'Invoice 11272018/KB19913964-586 from SCEIS Business Objects Report / Job 2000576'. The email received at is 'Tue, 27 Nov 2018 17:43:40 GMT'. The content type is 'Text'. The email is marked as 'Deleted'. The user mailbox is 'RAMUIR@scdj.net' and the user aliases are 'ramuir@scdj.net' and 'ramuir@scdj.onmicrosoft.com'. The email is marked as 'Unread'. The sender is external and the recipient is not external. There are links for 'Recheck', 'Show headers from raw email', and 'Show body from raw email'.

The 'Anti Phishing' section shows 'Anti-phishing' with a green checkmark. Below it, 'Insecure attachments found' is highlighted with a red exclamation mark. A Word document icon and the filename 'INV-KB19913964-586.doc' are shown next to the exclamation mark.

The 'Email attachments' table has two columns: 'NAME' and 'SIZE'. It lists one attachment: 'INV-KB19913964-586.doc' with a size of '189.2 Kilobytes' and a red exclamation mark icon.

The 'Conversation' table has two columns: 'TIME' and 'SUBJECT'. It is currently empty.

The 'Live event log' table has four columns: 'DATE/TIME', 'OBJECT', 'USER', and 'EVENT'. It lists two events:

DATE/TIME	OBJECT	USER	EVENT
12:44:37 2018-11-27	INV-KB19913964-586.doc	Check Point Security	Inspected by Antivirus <span style="color: green;">✔</span>
12:44:12 2018-11-27	INV-KB19913964-586.doc	Check Point Security	Inspected by Threat Extraction <span style="color: red;">!</span>

You will see from screen shot above, a typical alert that anti-phishing says the email is fine. However, the exclamation point for the attachment will stand out to you. When you dive deeper into the threat extraction exclamation for more details you will get this screen:

The 'THREAT EXTRACTION SCAN DETAILS' dialog box shows the following information:

- Action Taken: Should Replace
- Action Taken for clean method: Should Replace
- Action Taken for convert method: Should Replace
- Not Supported By Capsule: false
- Replaced Date: Tue, 27 Nov 2018 17:44:11 GMT
- Status Code: 0

A 'Close' button is located at the bottom right of the dialog box.

Here is the problem. What exactly is an action taken of “**should replace?**” If the action was really “taken” then there is no “should” because it would be done. However, my customer wanted an explanation and so did I. I was unable to find any details about this anywhere. Therefore, it was time for R&D help.

## RESOLUTION

When you see this confusing status it means that “**IF**” you had threat extraction enabled then threat extraction would have replaced the attachment with a clean PDF. So in my situation, since TE was not enabled, then the malicious file was not converted. Therefore, leaving the mailbox vulnerable. To protect yourself from this confusing situation with your customer and to help them be better protected, TE must be enabled.

The steps to enable TE are very easy. You simply create a new threat protection rule as below with the highlighted mode and advanced settings.

NEW CHECK POINT CLOUDGUARD SAAS

### New Policy Rule - Office 365 Emails Threat Detection

Rule Name: Office 365 Emails Threat Detection

Mode: Protect (inline)

Scope:  All users and groups

**Advanced**

Enable Sandblast Threat Extraction for attachments

Clean: None

Convert: None

Blades:  All the running threat detection blades

Specific tools

Alerts

Send email alert to admin(s) about phishing

Send Email alert to...

SETTINGS

Needs to be Protect (Inline)

After Protect Inline is Enabled, You have the two options of Clean and Covert to PDF. Use the supported Threat Extraction SK to configure file types extensions. sk101553

## Additional Resources

1. Check Point CloudGuard SaaS Getting Started Guide
2. Check Point CloudGuard SaaS Identity Protection Guide
3. Check Point CloudGuard SaaS Manual Configuration with Office 365
4. Check Point CloudGuard 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](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doShowproductpage&product=495)