Email Security User Guide

Check Point Harmony Email & Collaboration

Sentry Management • Information Security

FOR SENTRY EMPLOYEE AND REMOTE TEAMMATE USE ONLY

Overview

Sentry has deployed Check Point Harmony Email & Collaboration to protect your inbox from spam, phishing, malware, and other email-based threats. This system works silently in the background — most of the time you won't notice it. This guide explains the features that are visible to you and how to get the most out of them.

What This System Does

- Blocks malicious emails before they reach your inbox
- Quarantines suspicious messages for your review
- Sends you a daily digest so you never miss a quarantined message
- Labels promotional and marketing email so you can manage your inbox
- Lets you report spam or phishing with a single click

Email Labeling & Greymail Filtering

Not all unwanted email is dangerous — some of it is just clutter. "Greymail" refers to legitimate but promotional email: newsletters, marketing messages, sale announcements, and similar content you may have subscribed to at some point. Check Point Harmony identifies this email and treats it differently from genuine threats.

How It Works: Two Phases

Phase 1 — Grace Period (First 45 Days)

During the first 45 days after rollout, promotional email will be delivered normally to your inbox but will be labeled with a "[Promotional]" tag in the subject line.

This gives you time to identify senders you want to hear from and take action before filtering begins.

Phase 2 — Promotions Folder (After Day 45)

After the 45-day grace period, email identified as promotional will automatically be moved to a dedicated "Promotions" folder in your mailbox — similar to how Gmail's Promotions tab works.

Your main inbox will be reserved for messages that matter most.

You can check the Promotions folder at any time to review and act on those messages.

What Gets Labeled as Promotional?

The system identifies email as promotional based on signals such as:

- Bulk sending patterns (email sent to many recipients at once)
- Marketing headers embedded by the sender's email platform
- Unsubscribe links or list-serve indicators
- Commercial language and formatting typical of marketing messages

What You Should Do During the Grace Period

We recommend taking the following steps while promotional email is still appearing in your inbox:

1. Review any email tagged “[Promotional]” that you want to continue receiving.
2. If you want to ensure a sender reaches your inbox going forward, add them to your Contacts or mark them as “Not Junk” in Outlook.
3. Unsubscribe from any promotional senders you no longer want to hear from — this is a great opportunity to clean up your inbox.

Important

If a legitimate business email is incorrectly labeled as promotional, please report it to the IT Helpdesk at the contact below. We can whitelist the sender.

Email Quarantine

When Check Point Harmony identifies an email as potentially dangerous — such as a phishing attempt, a message with a malicious attachment, or suspected spam — it will not deliver that email to your inbox. Instead, it places the message in quarantine where it can’t cause harm.

How Quarantine Works

- Quarantined messages are held securely and are not visible in your regular inbox or Junk folder.
- You will receive a daily Quarantine Digest email (described in the next section) listing any messages that have been held.
- From the digest, you can review quarantined messages and release any that are legitimate.
- Messages that remain in quarantine are automatically deleted after 30 days.

Releasing a Quarantined Message

If you receive a quarantine notification and believe a held message is legitimate:

1. Open your daily Quarantine Digest email.
2. Sign in to Check Point Email Security Quarantine Portal. (refer to quarantine user guide)
3. Locate the message you want to release.
4. Click “Request Release” next to the message.
5. After Admin Review, the message will be delivered to your inbox within a few minutes.

A Note on Safety

If you are unsure whether a quarantined message is legitimate, do not release it. Contact the IT Helpdesk and we can review it for you.

Releasing a malicious email can put your computer and our network at risk.

Quarantine Categories

Messages can be quarantined for several reasons. Understanding the category can help you decide whether to release a message:

Quarantine Reason	What It Means
Spam	High-confidence unsolicited commercial email. Usually safe to release if you recognize the sender.
Phishing	Suspected attempt to steal credentials or personal information. Do NOT release unless confirmed legitimate by IT.
Malware	Email contains an attachment or link identified as malicious. Do NOT release.
Suspicious Link	The email contains a link that could not be verified as safe. Contact IT before releasing.

Quarantine Digest Email

To keep you informed about messages being held on your behalf, Check Point Harmony sends a daily Quarantine Digest email. This is a legitimate system-generated email — it is not spam.

What to Expect

- You will receive the digest once per day, typically in the morning.
- The digest will only be sent if there are messages waiting in your quarantine. If your quarantine is empty, you will not receive a digest that day.
- The digest comes from do-not-reply@portal.checkpoint.com — do not reply to it directly.

What's in the Digest

Each digest email includes:

- A list of quarantined messages showing the sender, subject, date, and quarantine reason
- Action buttons next to each message: Release, Release & Allow, or Delete
- A link to view your full quarantine portal for more detail

Actions Available in the Digest

Action	What It Does
View in Portal	Opens the quarantine portal where you can see full message content before deciding.

Tip
If you did not receive a quarantine digest and you expected to, check your Junk email folder first, if not found no messages have been quarantined.

Reporting Spam or Phishing

If a suspicious or unwanted email makes it into your inbox, you should report it rather than simply deleting it. Reporting helps our IT team improve filtering and protect everyone at Sentry.

How to Report an Email

Check Point Harmony adds a “Report” button directly in your Outlook toolbar. Here’s how to use it:

1. Select the suspicious email in your inbox (do not open attachments or click any links).
2. Click the “Report” button in the Outlook ribbon at the top of the screen or by right clicking on the message.
3. Choose the type of report: Spam or Phishing.
4. The email will be submitted to our IT team and removed from your inbox automatically.

Spam vs. Phishing: Which Should I Choose?

Report Type	Use When…
Spam	The email is unwanted or unsolicited but does not appear to be trying to steal information or credentials. Examples: unsolicited advertising, mass marketing emails you didn’t ask for.
Phishing	The email appears to be trying to trick you into clicking a link, providing a password, or sharing personal/financial information. Examples: fake Microsoft login pages, “urgent” requests from executives, fake package delivery notices.

Suspected Phishing? Stop and Report.

Do not click any links, open any attachments, or reply to the sender.
Do not forward the email to colleagues to “show them.”
Use the Report button or call the IT Helpdesk immediately at [HELPDESK PHONE].
If you accidentally clicked a link or provided credentials, call IT immediately.

What Happens After You Report

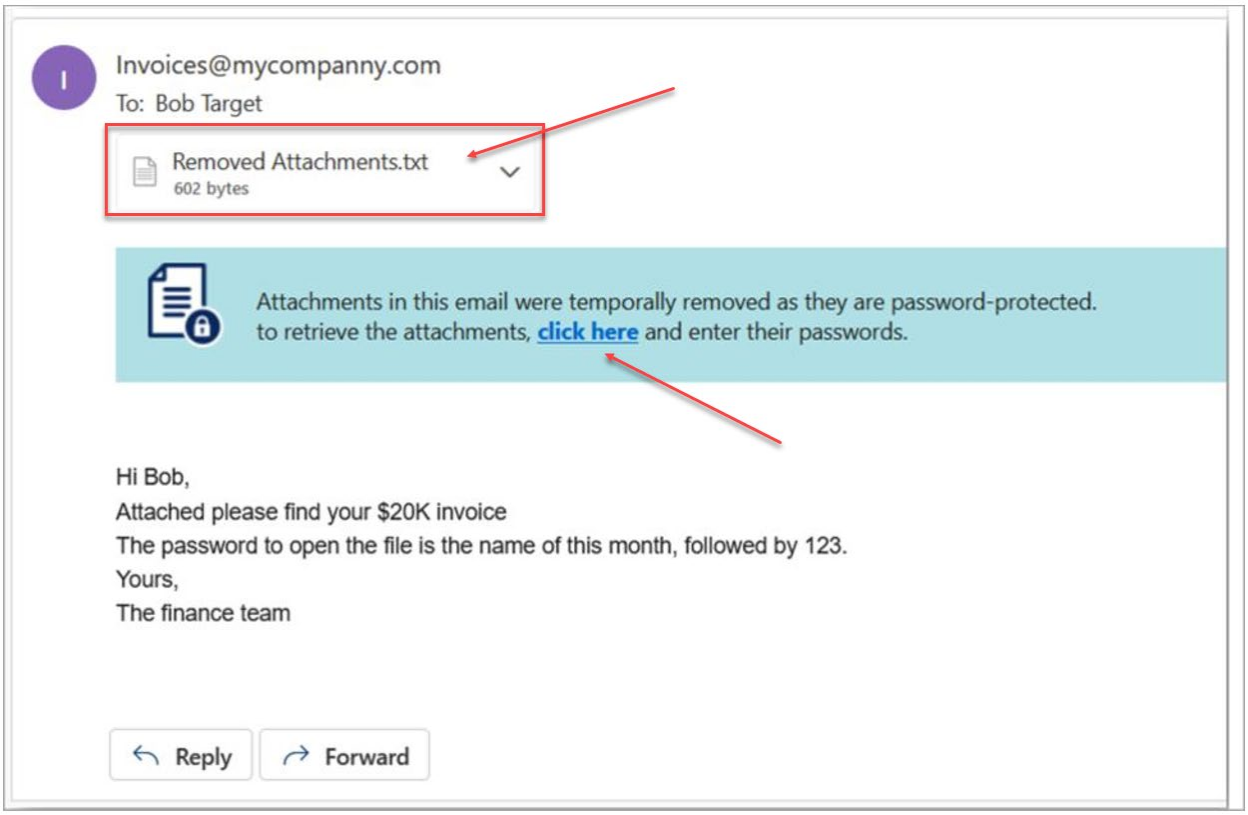
- Your report is submitted to the Check Point threat intelligence platform and to the Sentry IT team.
- The email is automatically removed from your inbox.
- If the email is confirmed malicious, additional protective actions may be taken across the organization.
- You do not need to take any additional steps. IT will contact you if follow-up is needed.

Requesting Passwords for password protected attachment(s)

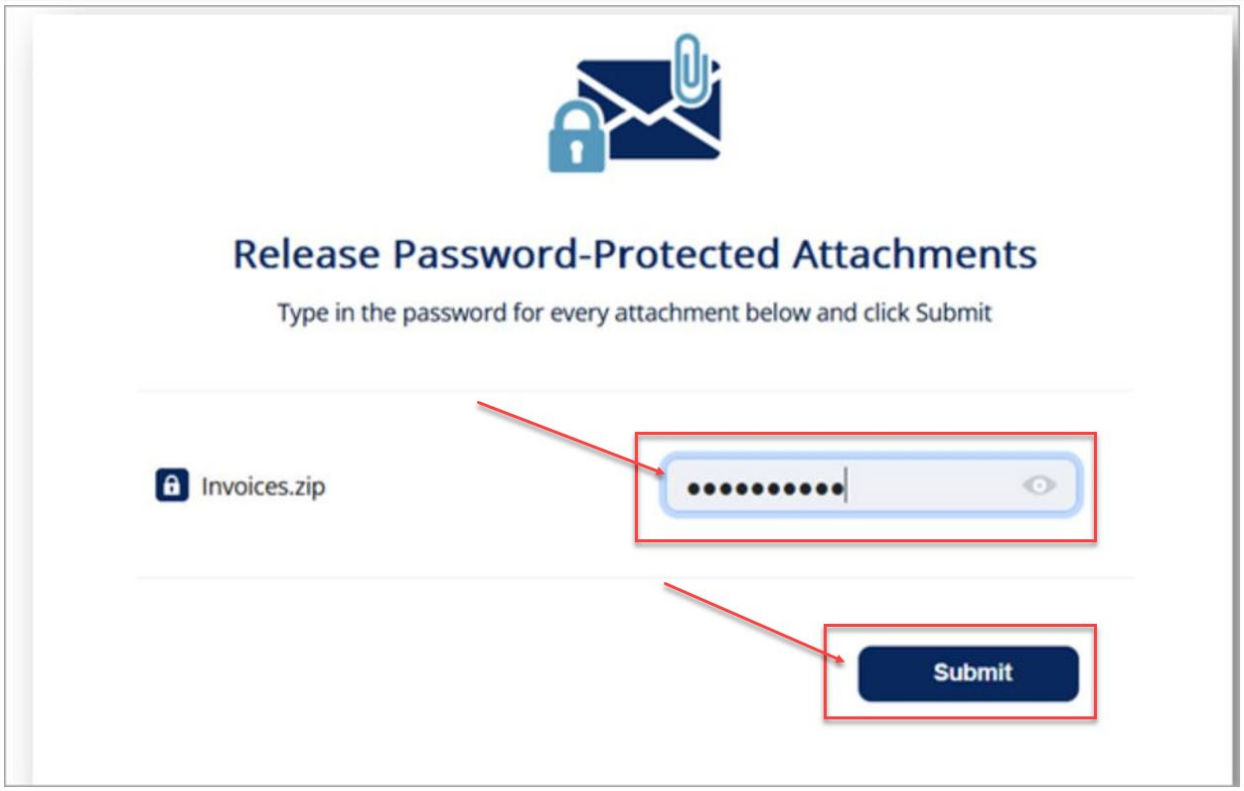
For Example Word, Excel, PDF, etc.

To secure sensitive data transmitted via email, Check Point uses Email Security with password-protected attachments, adding an extra layer of protection against unauthorized access and data breaches.

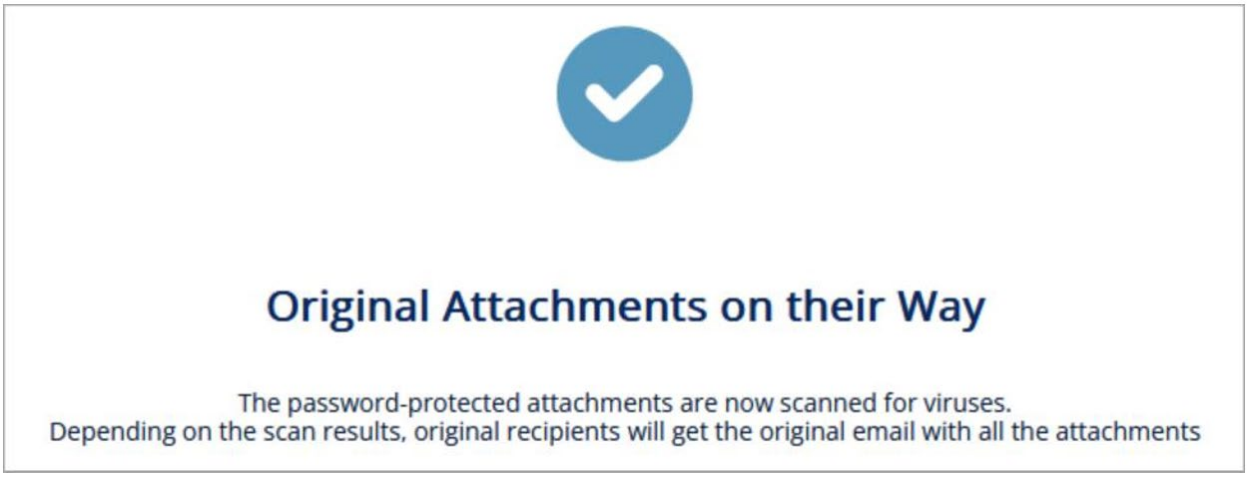
Check Point has configured the policy to require users to enter the **protected attachment password**, **(NOT your Sentry email password)** the system temporarily removes the attachment and adds a warning banner to the email. This banner includes a **click here** link where you can securely enter the "**attachment**" password to access the attachment.



Enter the password for the attachment and click **submit**.



After you submit, the Anti-Malware engine scans the attachment for malicious content.

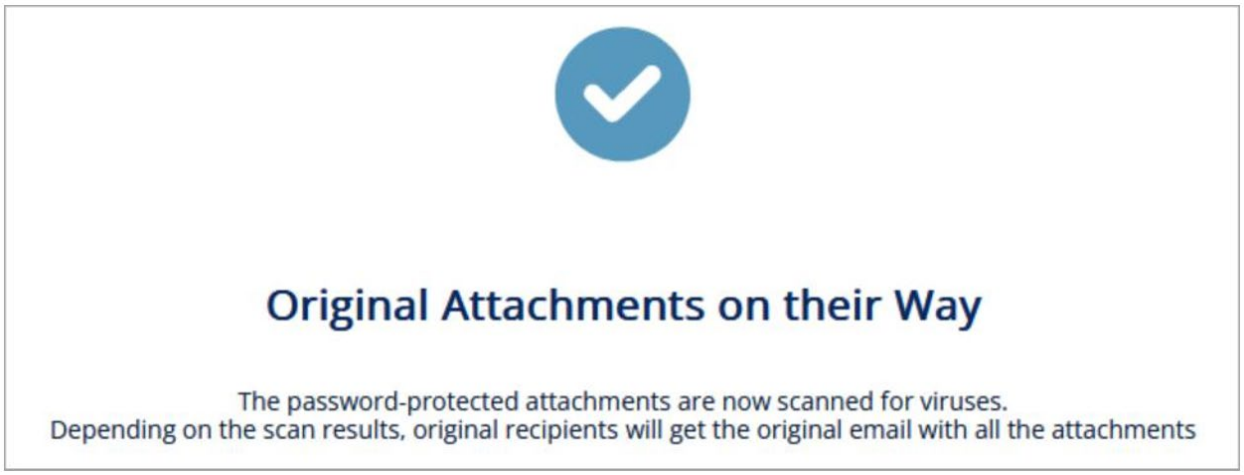


If the Anti-Malware engine finds the attachment as clean, the original email with password-protected attachment gets delivered to the original recipients of the email.

Getting Help

If you have questions about your email security or need assistance with any of the features described in this guide, submit a Help Center ticket.

If the email was already released, this message appears:



IT Helpdesk Contact Information

💻 Portal: Sentry Employee Help Center

Please include as much detail as possible when reporting an issue, such as the sender's email address, the subject line, and any error messages you received.