

Email Quarantine User Guide

Overview

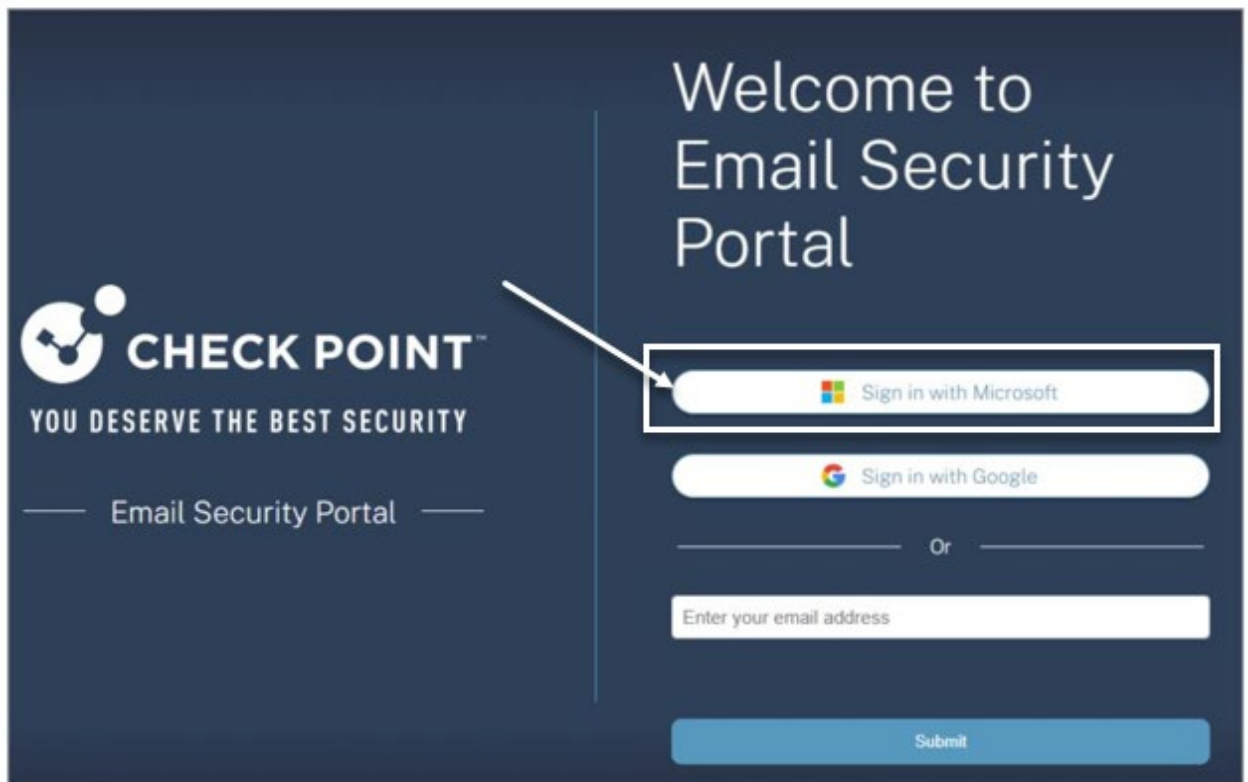
When Check Point Harmony identifies an email as potentially dangerous — such as a phishing attempt, a message with a malicious attachment, or suspected spam — it will not deliver that email to your inbox. Instead, it places the message in quarantine where it can't cause harm.

How to Sign in to the Check Point Email Quarantine

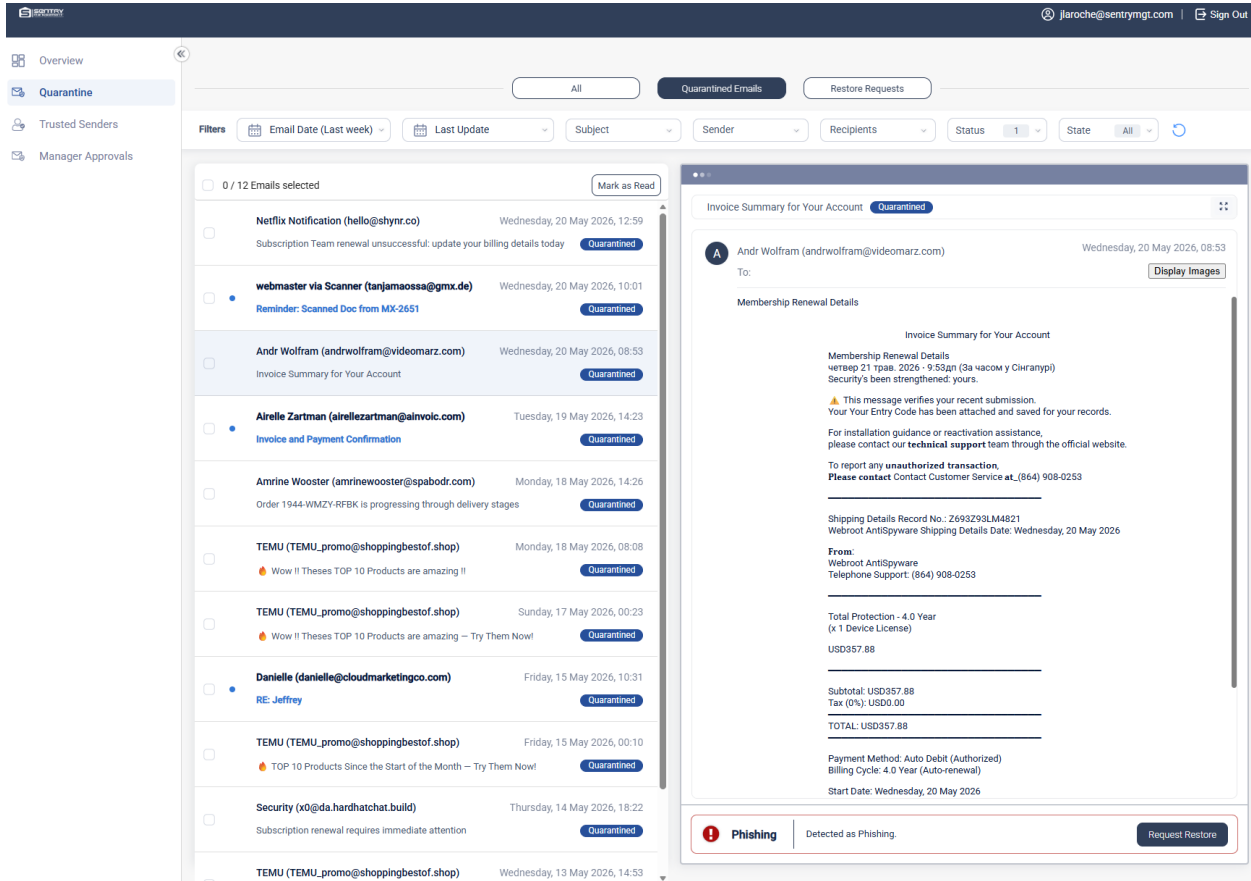
Access the Email Security Portal using <https://email-security-portal.checkpoint.com>.

NOTE: Sentry Technology Services will also push down a bookmark to your browser.

1. Click > **Sign in with Microsoft credentials:**
2. Follow the on-screen instructions and sign in with your **Sentry Management email address.**



NOTE: Below is the Quarantine Portal Interface



The screenshot displays the Sentry Quarantine Portal interface. On the left, a navigation sidebar includes 'Overview', 'Quarantine', 'Trusted Senders', and 'Manager Approvals'. The main area features a top navigation bar with 'All', 'Quarantined Emails', and 'Restore Requests' tabs. Below this is a filter section with dropdowns for 'Email Date (Last week)', 'Last Update', 'Subject', 'Sender', 'Recipients', 'Status' (set to '1'), and 'State' (set to 'All').

The email list shows 0/12 emails selected. The selected email is from 'Andr Wolfram (andrwolfram@videomarz.com)' with the subject 'Invoice Summary for Your Account', dated Wednesday, 20 May 2026, 08:53. The email content is displayed in a preview pane on the right, titled 'Invoice Summary for Your Account' and 'Membership Renewal Details'. The preview includes a warning icon and text: 'This message verifies your recent submission. Your Your Entry Code has been attached and saved for your records. For installation guidance or reactivation assistance, please contact our technical support team through the official website. To report any unauthorized transaction, Please contact Contact Customer Service at_(864) 908-0253'. The invoice details show 'Total Protection - 4.0 Year (x 1 Device License)' for USD357.88, with a subtotal of USD357.88 and tax of USD0.00. The payment method is 'Auto Debit (Authorized)' and the start date is 'Wednesday, 20 May 2026'.

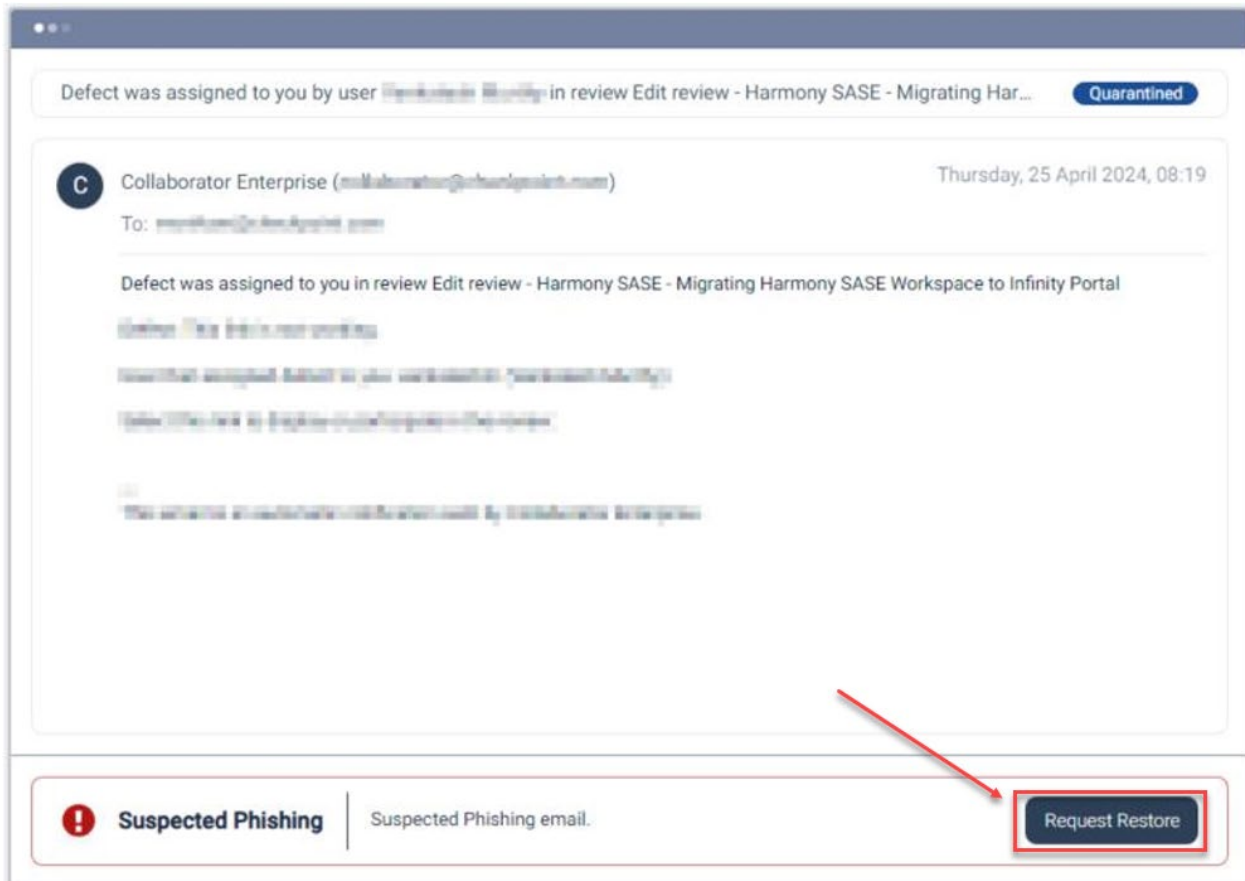
At the bottom of the preview pane, a red warning icon indicates 'Phishing' and 'Detected as Phishing', with a 'Request Restore' button.

How to restore emails that need an administrator's approval

NOTE: **Request Restore** option bottom right.

To restore these emails:

1. Select the email you want to restore.
2. Click > **Request Restore**



- a. The Request Restore window appears.
- b. Enter the restore reason and click **Submit** button.

Request Restore

Please enter the restore reason below:

 0/250

Cancel

Submit

3. The Request Submitted window appears > click **Close**

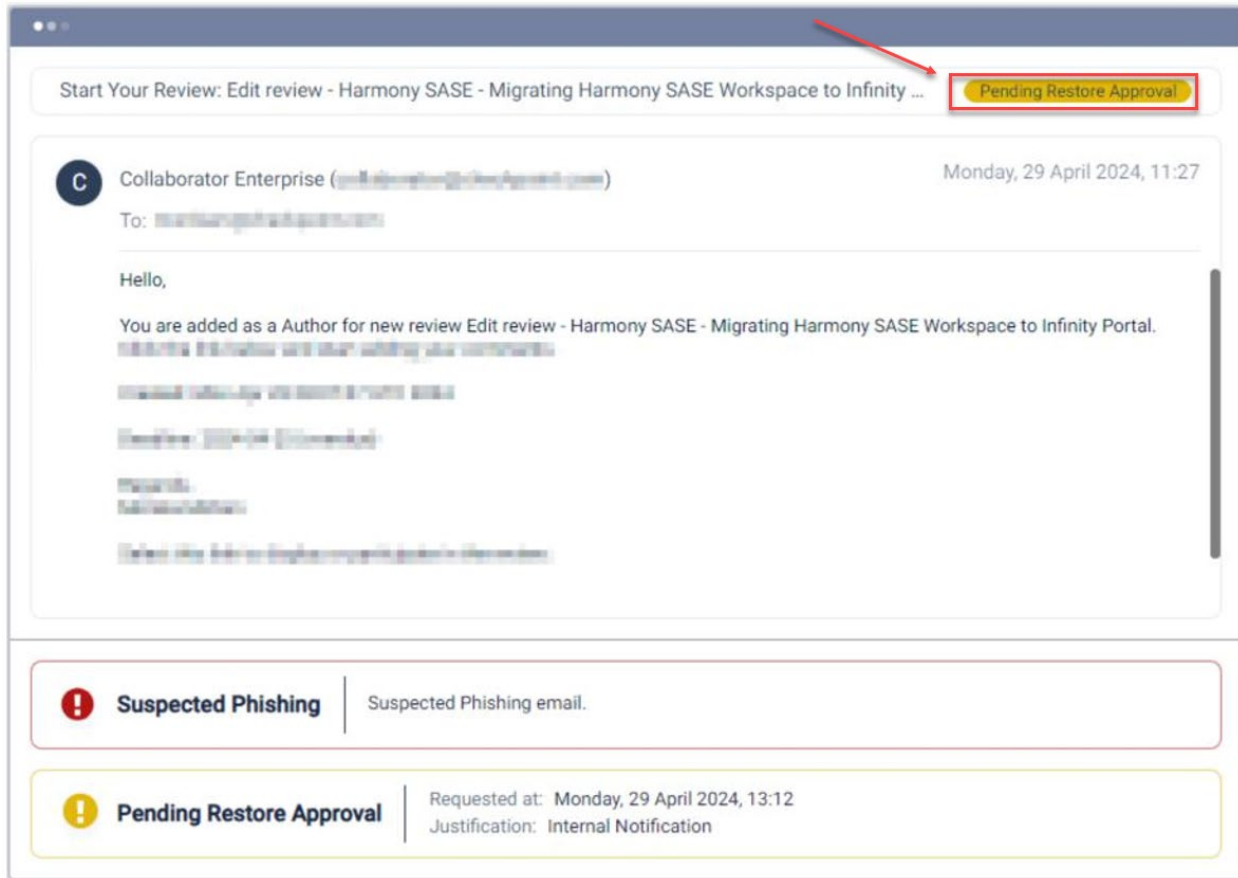


Request Submitted

Your request will now be reviewed by an administrator.

Close

4. The email status changes from **Quarantined** to **Pending Restore Approval**.



NOTE: If the administrator (Tech Support) approves the request, the email is restored to your mailbox and the email status changes to Restored.

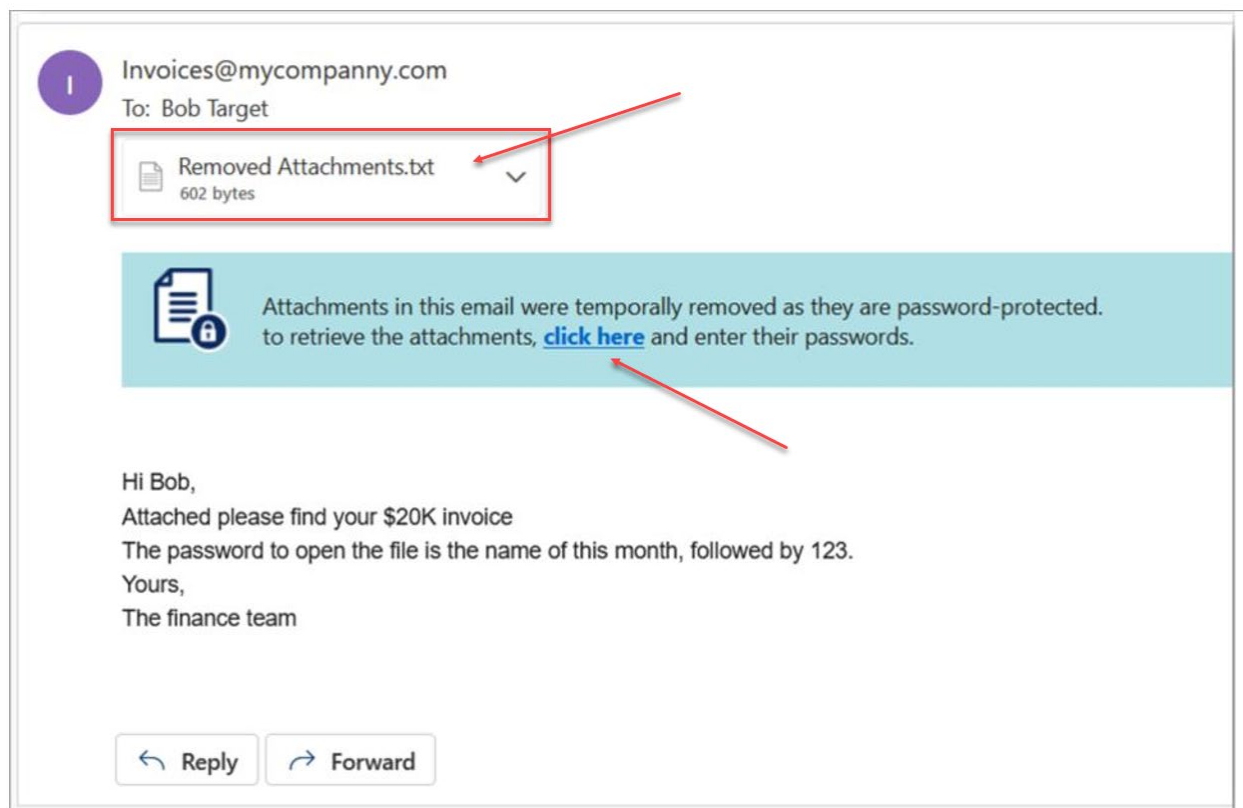
Password Protected Attachment(s)

e.g. Excel, PDF attachments, etc.

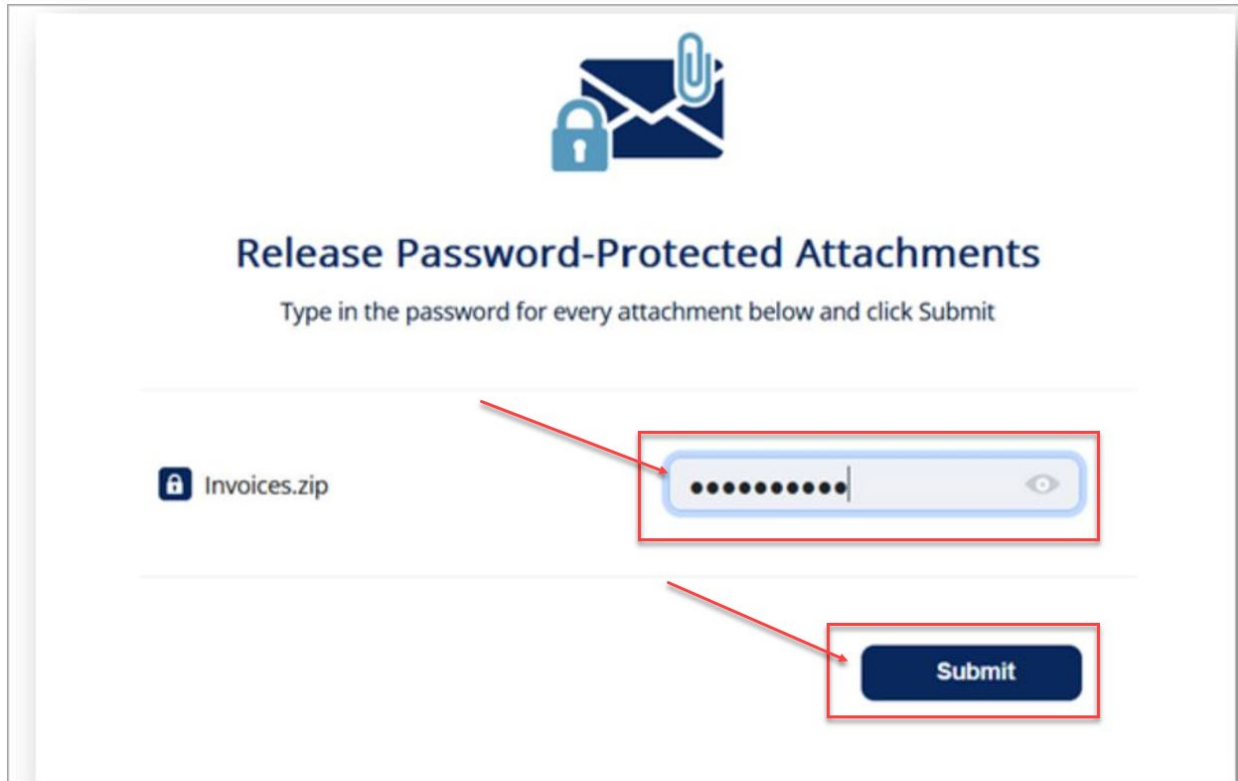
If you receive an email that includes an attachment that is password protected AND the password is NOT found in the message, to secure sensitive data Check Point adds an extra layer of protection against unauthorized access.


Check Point has configured the policy to require users to enter the **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**.





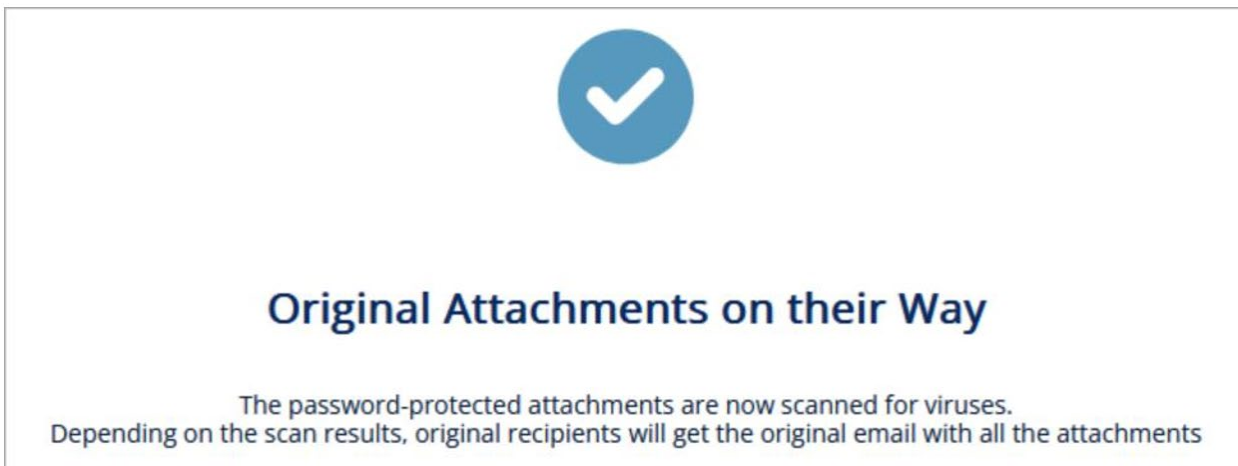
Release Password-Protected Attachments


Type in the password for every attachment below and click Submit

 Invoices.zip

Submit

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





Original Attachments on their Way

The password-protected attachments are now scanned for viruses.
Depending on the scan results, original recipients will get the original email with all the attachments

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.

If the email was already released, this message appears:

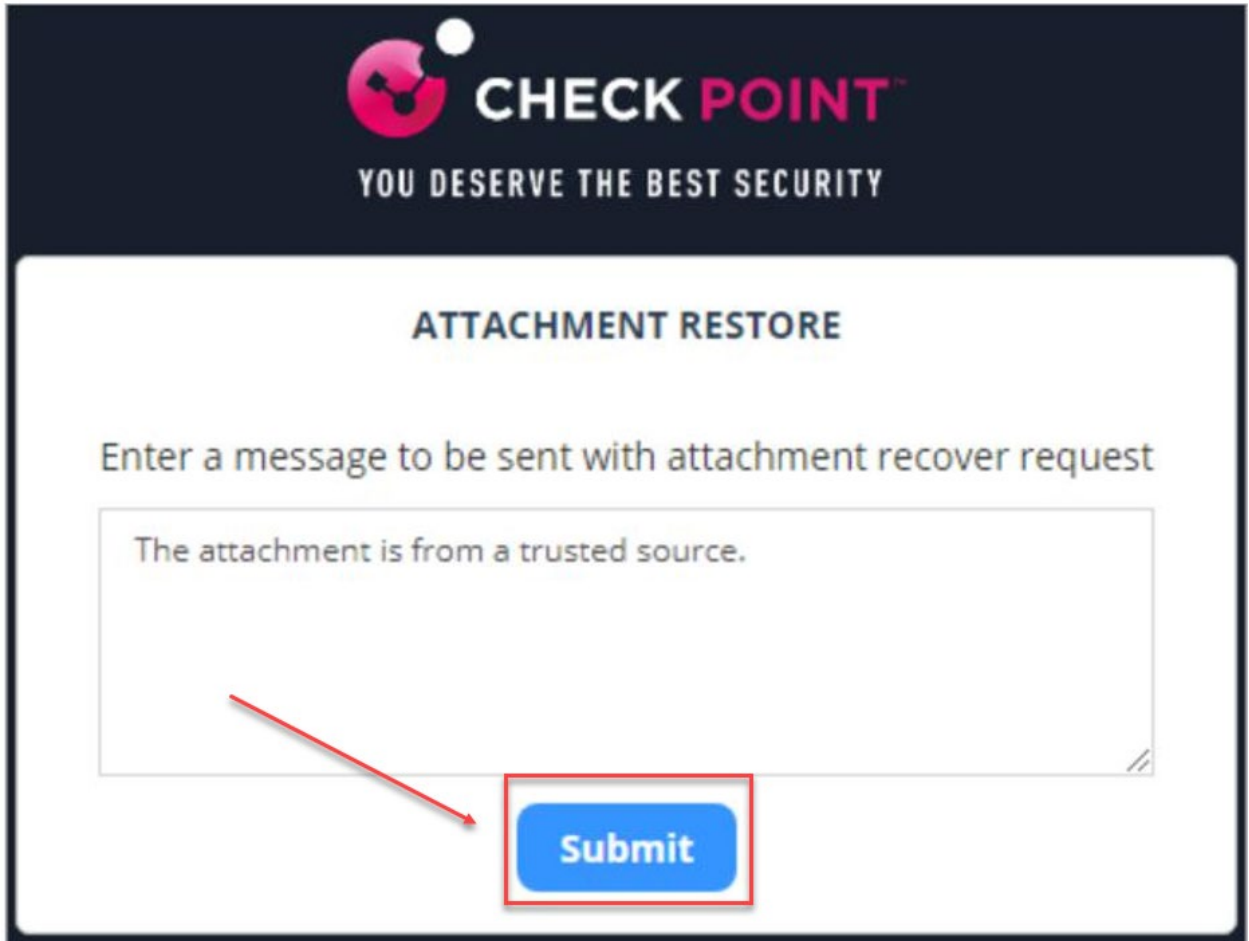


Original Attachments on their Way

The password-protected attachments are now scanned for viruses.
Depending on the scan results, original recipients will get the original email with all the attachments

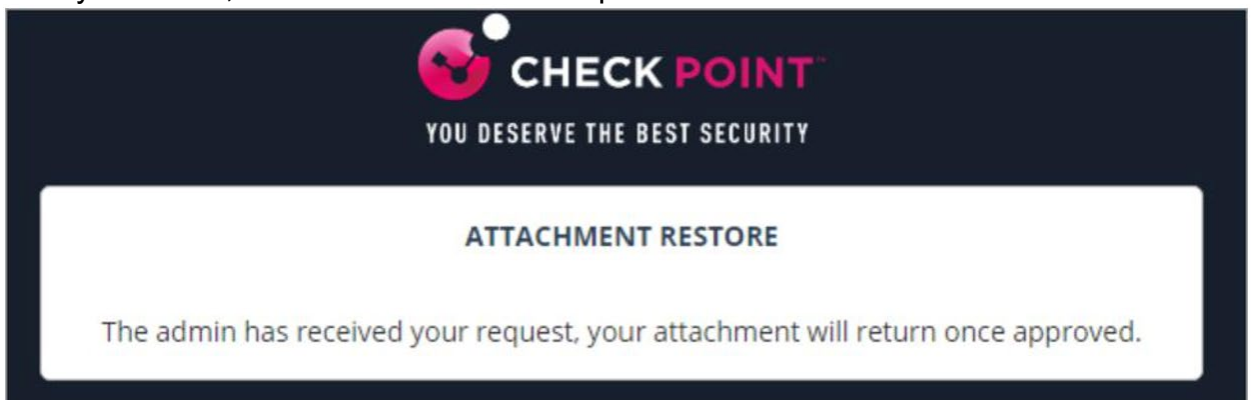
To restore an email and its attachments from quarantine:

1. Click the link provided in the email.
2. If prompted, enter the reason for restoring the attachment, click > **Submit**



The screenshot shows the Check Point logo and tagline at the top. Below it, the heading "ATTACHMENT RESTORE" is centered. A text prompt asks the user to "Enter a message to be sent with attachment recover request". A text input field contains the text "The attachment is from a trusted source." A red arrow points from this text to a blue "Submit" button, which is also highlighted with a red rectangular border.

After you submit, the admin receives the request.



The screenshot shows the Check Point logo and tagline at the top. Below it, the heading "ATTACHMENT RESTORE" is centered. A message states: "The admin has received your request, your attachment will return once approved."

After the admin approved, the user receives the original email.