



End-User Experience Changes



YOU DESERVE THE
BEST SECURITY

Welcome To Check Point Harmony Email & Collaboration Security!

To help you roll-out Check Point Harmony Email & Collaboration Security to your end users, we have a series of templates to help you message and prepare your end-users.

Many of these changes will depend on the settings you as an administrator set in the Check Point Harmony Email & Collaboration Security console; therefore, make sure to only send out the relevant content to your end-users.

Welcome Template (1 of 3)

[COMPANY NAME] Employees,

Our security team is advancing in the global cyber security battle. Some of the major challenges include malware and phishing attacks entering our systems via the cloud applications we use along with sensitive information leaked out.

I'd like to announce our integration with the Check Point Harmony Email & Collaboration Security Cloud Security platform. Check Point Harmony Email & Collaboration Security protects our cloud from the latest security threats by combining the power of best security tools in the market. Whether it's fake login form that attempt to steal your credentials, ransomware that locks attempts to lock down our devices, or impersonated emails pretending to be from someone we are familiar with – Check Point Harmony Email & Collaboration Security protects you.

More info about Check Point Harmony Email & Collaboration Security can be found at: <https://www.checkpoint.com/harmony/email-security/email-office/>

In preparation to protecting our entire organization, Check Point Harmony Email & Collaboration Security has provided us with a few safety tips to keep in mind:

- Rather than sending files to non-employees as email attachments, it's always preferred to share files over [FILE-SHARING-SAAS], where access permissions are clearly defined, and can be revoked as needed.
- Warning messages might come up in your emails in the form of a subject change or even within the email body. For example, when someone new sends you an email, you will be asked to confirm whether you trust this email or not.
- Some emails detected as phishing or malicious before arriving in your inbox – and therefore quarantined, you may receive a notification with the option to retrieve the original email. Please use caution when attempting to retrieve quarantined data.

Let me know if you have any questions or concerns about the new security change.

You can reach me at: Email: [ADMIN EMAIL] Phone: [ADMIN PHONE] Thanks, [ADMIN NAME] System Administrator [COMPANY NAME]

Welcome Template (2 of 3)

[COMPANY NAME] Employees,

We are deploying a new security application for our [Office 365, Google] email.

You may notice a few changes to your inbox.

- The subject of the email might indicate if it is suspicious with an [Alert/Phishing] message. Treat these messages carefully.
- You may see a message at the top of the email which asks if you trust this user. Take a moment to confirm the source and the content and select "yes" or "no" as appropriate.
- If you receive an email with a suspicious attachment, it may be quarantined. In some cases, you will have an option to retrieve the document. If so, proceed with caution.
- [insert other security policies here]

Examples:

- When sharing a file, it is always better to use [file-sharing app: Box/OneDrive/etc.] than to send via email.]
- When any email requests money, personal data, or other confidential information, contact the sender via phone or other method to confirm the message.
- Never use the same password on more than one site.

As always, we take your email security concerns seriously. Refer any questions or doubts to us at:

Email: [ADMIN EMAIL] Phone: [ADMIN PHONE] Thanks, [ADMIN NAME] System Administrator [COMPANY NAME]

Welcome Template (3 of 3)

Our security team is advancing in the global cyber security battle. Some of the major challenges include phishing and malware attacks entering our systems via Office 365. Therefore, I'd like to announce our integration with the Check Point Harmony Email & Collaboration Security Cloud Security platform. More info about Check Point Harmony Email & Collaboration Security can be found at:

<https://www.checkpoint.com/harmony/email-security/email-office/>

In preparation to protecting our entire organization, please note the following changes of behavior for email:

- Emails detected as phishing or malicious before arriving in your inbox will be quarantined. If you did not receive an email that you are expecting, please reach out to [OUR IT TEAM] with the sender's information to see if the email was quarantined.
- Emails detected as phishing or malicious before arriving in your inbox will be quarantined. You will be notified of this, and given the option to request the email be restored to you by [OUR IT TEAM].
- You may receive warnings at the top of the email bodies that indicate that an email contains qualities of phishing

These 3 templates can be used in conjunction with the screenshots and further messaging below.

Warning Banners

With Check Point Harmony Email & Collaboration Security, we should be seeing very few legitimate emails blocked because one of the new things you will see are detailed Warning Banners above the body of an email that Check Point Harmony Email & Collaboration Security suspects to be phishing.

The banners also allow you to give feedback to Check Point Harmony Email & Collaboration Security on whether you think the email is legitimate.

The following screenshots will show examples of these informative warning banners.

Warning Banners

Phishing Alert! [phishing_2020-11-08_1639]



avtestlab2@hush.com

Sun 11/8/2020 4:41 PM

To: user2_av_test



Warning: This email contains elements that may indicate "Phishing" intent - aimed at tricking you to disclose private/financial information or even your credentials. Do you trust this sender?

[Yes](#) [No](#)

<http://this-is-confident.com/login.php>

Yours, Hush.

[Reply](#) | [Forward](#)

ail1@hush.com>

on behalf of hush.com

Sun 11/8/2020 3:44 PM

To: user2_av_test



Warning: This email contains elements that may indicate "Phishing" intent - aimed at tricking you to disclose private/financial information or even your credentials. Do you think this email is legitimate?

[Yes](#) [No](#)

Hi this is Hen

how are you?

i am great

please see this link

<https://hush.com/v1/url?o=http%3A//this-is->

Warning Banners

A

ail11@avanan.com>

on behalf of [redacted]

Sun 11/8/2020 3:44 PM

To: [redacted]

Warning: The email is sent from the organization's domain (www.avanan.com), but suspected as non-authentic.

Hi this is Hen

how are you?

i am great

please see this link

[https://\[redacted\]/v1/url?o=http%3A//this-is-](https://[redacted]/v1/url?o=http%3A//this-is-)

A

ail11@avanan.com>

on behalf of [redacted]

Sun 11/8/2020 3:44 PM

To: [redacted]

Warning: The sender iral@gmail.com seems to be using a different email address than in the previous correspondence (iral@avanan.com), this often indicates an impersonation attempt.

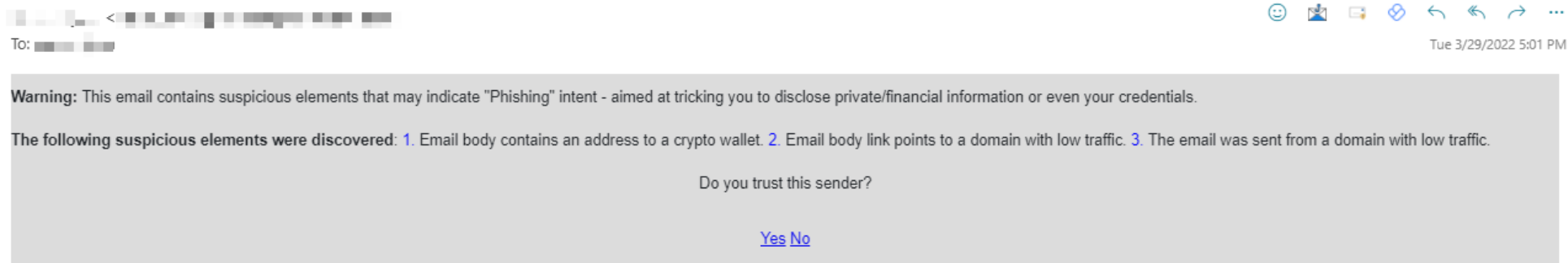
how are you?

i am great

please see this link

[https://\[redacted\]/v1/url?o=http%3A//this-is-](https://[redacted]/v1/url?o=http%3A//this-is-)

Warning Banners



Warning banner for potential impersonation.

Warning: The sender <sender> seems to be using a different email address than in the previous correspondence (<previous email>), this often indicates an impersonation attempt.

[Yes](#) [No](#)

Daily Email Security Summary

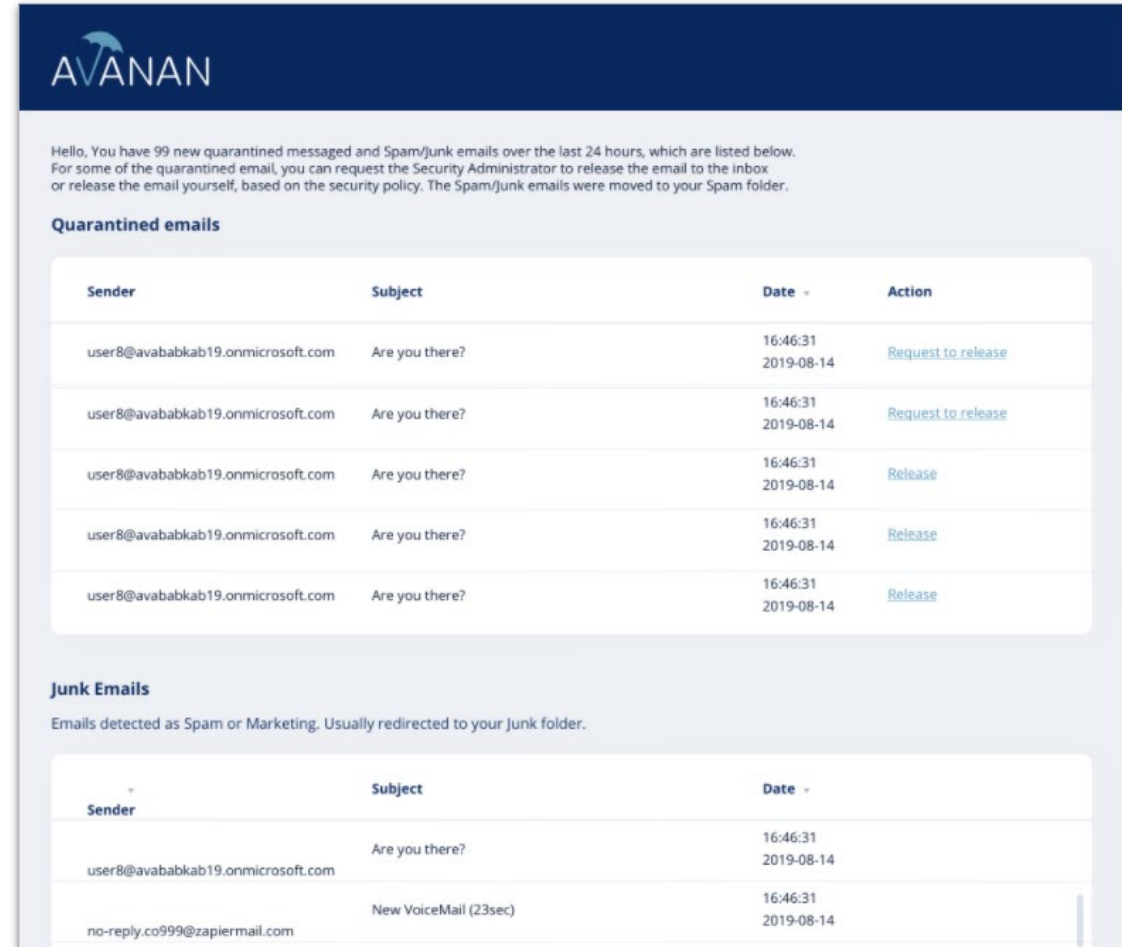
You will now receive a summary of all the emails that Check Point Harmony Email & Collaboration Security blocks

From this summary email, you will get a glimpse of all the security threats that bombard your mailbox every day.

If you disagree with Check Point Harmony Email & Collaboration Security, with a simple click of a button found in the summary email, you will be able to Release any emails that Check Point Harmony Email & Collaboration Security found Suspicious.

As well as Request To Release any emails that Check Point Harmony Email & Collaboration Security is confident is Phishing

- The email will then be submitted to the admins for review



The screenshot shows the AVANAN interface for a Daily Email Security Summary. It includes a header with the AVANAN logo, a greeting message, and two main sections: 'Quarantined emails' and 'Junk Emails'. The 'Quarantined emails' section contains a table with columns for Sender, Subject, Date, and Action. The 'Junk Emails' section also contains a table with columns for Sender, Subject, and Date.

AVANAN

Hello, You have 99 new quarantined messages and Spam/Junk emails over the last 24 hours, which are listed below. For some of the quarantined email, you can request the Security Administrator to release the email to the inbox or release the email yourself, based on the security policy. The Spam/Junk emails were moved to your Spam folder.

Quarantined emails

Sender	Subject	Date	Action
user8@avababkab19.onmicrosoft.com	Are you there?	16:46:31 2019-08-14	Request to release
user8@avababkab19.onmicrosoft.com	Are you there?	16:46:31 2019-08-14	Request to release
user8@avababkab19.onmicrosoft.com	Are you there?	16:46:31 2019-08-14	Release
user8@avababkab19.onmicrosoft.com	Are you there?	16:46:31 2019-08-14	Release
user8@avababkab19.onmicrosoft.com	Are you there?	16:46:31 2019-08-14	Release

Junk Emails

Emails detected as Spam or Marketing. Usually redirected to your Junk folder.

Sender	Subject	Date
user8@avababkab19.onmicrosoft.com	Are you there?	16:46:31 2019-08-14
no-reply.co999@zapiermail.com	New VoiceMail (23sec)	16:46:31 2019-08-14

Individual Quarantine Alerts

In addition to a summary of alerts, your administrator can configure individual alerts to go out whenever an email is blocked by Check Point Harmony Email & Collaboration Security. The individual alert email will also contain a link to request to release the quarantined email.

The frequency of these alerts can be adjusted by your administrator and you can also request to restore these emails from the alert email.

The next few screenshots will show examples of these individual quarantine alerts.

What a Quarantine Notification Looks like

The screenshot displays an email client interface. On the left is the 'Inbox' sidebar with a 'Filter' dropdown and an 'Agenda' icon. The main pane is titled 'Quarantined [Test Malware Workflow 1]'. It shows an email from 'User3 Avanandemo1' received 'Today, 4:46 PM'. The email body contains a warning about a suspicious email from Chris Isbrecht, a link to release the email, and a warning to 'Use with caution!'. It also lists an attached file 'Malware 2.2.2017.pdf'. At the bottom, there is a section titled 'Test Malware Workflow 1' with the example text 'Example 1 - User is alerted and allowed to restore the email'. On the right side of the email pane, there are icons for 'Reply all' and a dropdown arrow. A dark blue modal window titled 'AVANAN Mail recover' is open, showing the message 'Mail restored successfully!'. Three red arrows are overlaid on the image: one points to the 'Quarantined' header, another points to the 'Use with caution!' text, and a third points to the 'Malware 2.2.2017.pdf' attachment.

Inbox Filter ▾
Next: No events for the next two Agenda

☐ User3 Avanandemo1
Quarantined [Test Malware Workflow 4:46 PM
The following email from Chris Isbrecht was f...

Quarantined [Test Malware Workflow 1]

User3 Avanandemo1
Today, 4:46 PM
User3 Avanandemo1 ▾

The following email from Chris Isbrecht was found suspicious,
and the attachments have been quarantined.
To release from quarantine, [click here](#) or contact your system administrator.
Use with caution !

Attached files:
Malware 2.2.2017.pdf

Test Malware Workflow 1
Example 1 - User is alerted and allowed to restore the email

AVANAN
Mail recover
Mail restored successfully!

What Restoring a Quarantined Notification Looks like

The diagram illustrates the 'Mail recover' process in the AVANAN interface. It consists of two panels connected by a red arrow pointing from left to right.

Left Panel (Input Form):

- Header: AVANAN (with umbrella logo)
- Title: Mail recover
- Instruction: Enter a message to be sent with email recover request
- Text Area: This email is from a trusted sender please release |
- Button: SUBMIT

Right Panel (Confirmation Message):

- Header: AVANAN (with umbrella logo)
- Title: Mail recover
- Message: The admin has received your request, your e-mail will return to inbox once approved.

If the request is approved by the administrator the original message will be delivered unaltered to the user.

Click-Time Protection

From time to time, you will see links in your emails that are not in a format you expect. Check Point Harmony Email & Collaboration Security will change all suspicious links in your emails to a safe version. The Check Point Harmony Email & Collaboration Security secured links will have the format:

https://url.Check Point Harmony Email & Collaboration Security.click/v2/____<original malicious link>____<encrypted gibberish>

Here's an example of such a link:



Click-Time Protection

If you cannot determine that an email with a custom Check Point Harmony Email & Collaboration Security secure link is malicious, you can click the link to have Check Point Harmony Email & Collaboration Security perform a real-time scan of the target website.

If the link is benign, you will be taken to the website like normal; however, if the link is found to be malicious, you will see the page below open up instead.



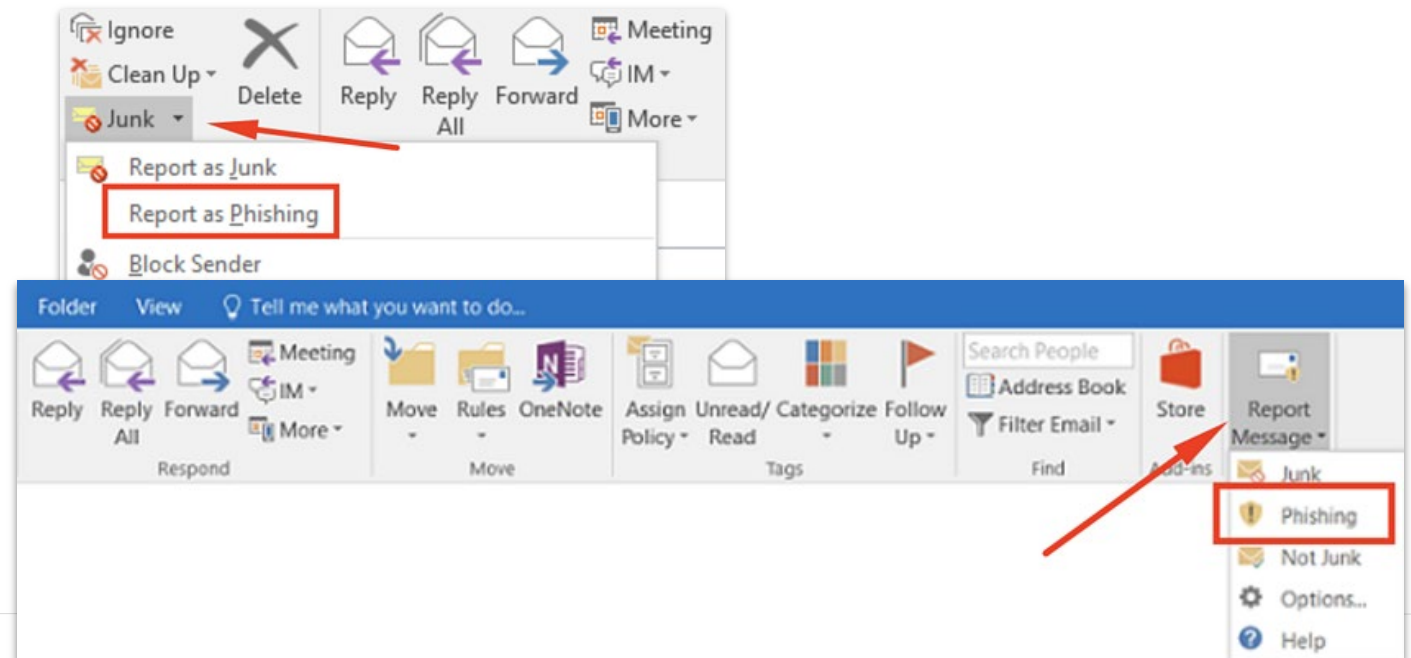
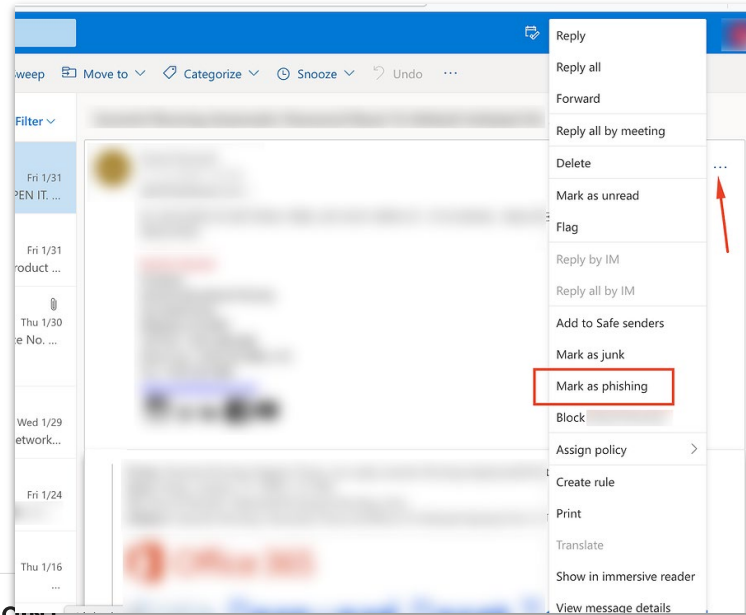
The web site you are trying to access was found to contain **malicious/deceptive** content.

Your organization has deployed a security service which protects users from visiting harmful content such as malicious web pages (containing viruses for example), phishing pages (trying to steal your credentials) and more.

If you still wish to visit the blocked page: [<< CLICK HERE >>](#)

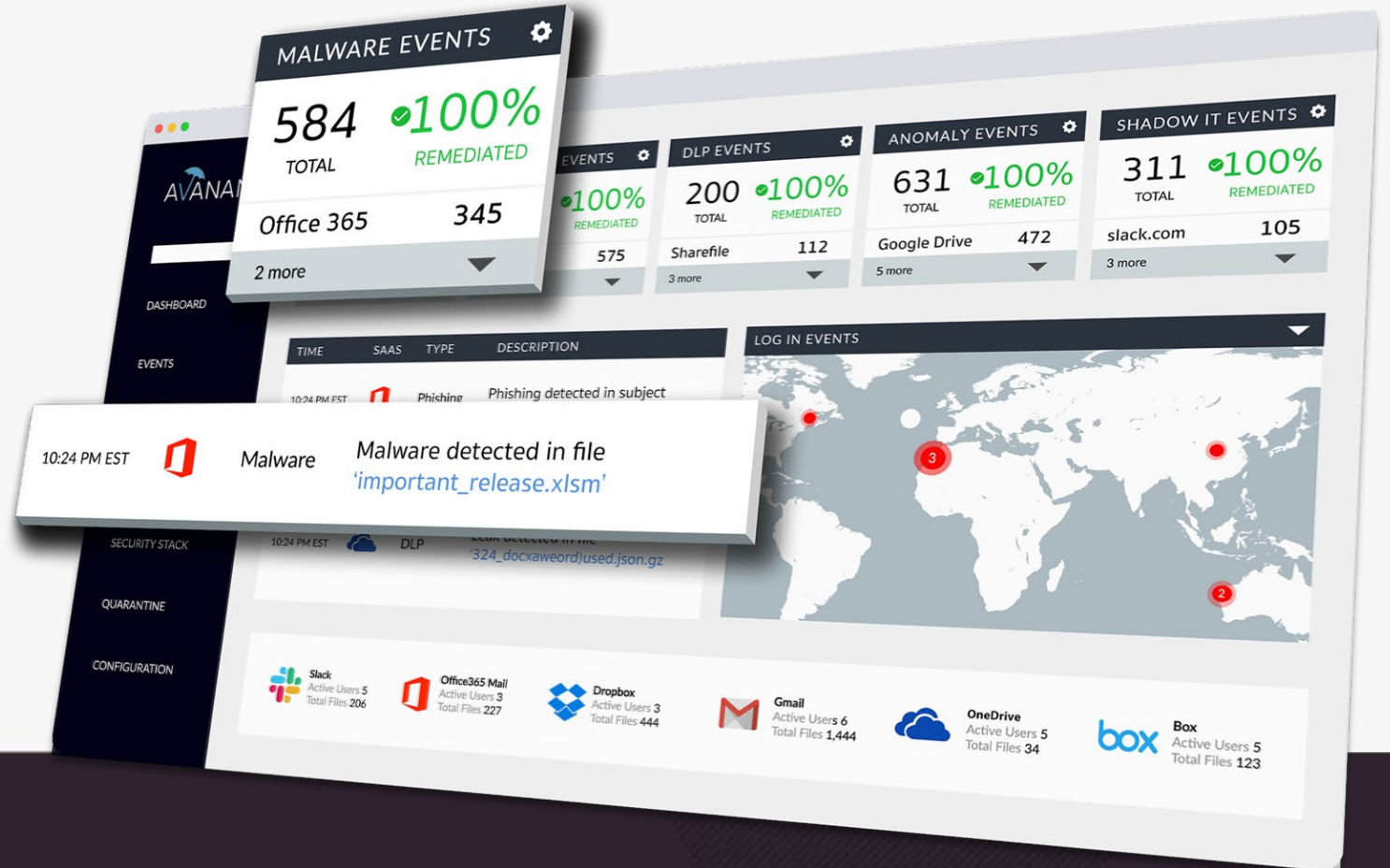
User Reported Phishing

One of the ways you can improve Check Point Harmony Email & Collaboration Security and your company's security posture is by diligently reporting potentially missed attack emails as Phishing. Check Point Harmony Email & Collaboration Security and your administrators will then investigate the issue and if the missed email is proven to be malicious, we will promptly adjust our configurations to make sure those attacks are dealt with automatically next time.





Thank you!



YOU DESERVE THE BEST SECURITY