



Harmony Email & Collaboration

Post-Sales Deployment Guide

Brit Robinson | Customer Success Manager

Paul Welford | MSP Security Engineer

10/07/2024



YOU DESERVE THE BEST SECURITY

Agenda

Review Deployment Phases

Review Recommend Configurations and Best Practices

Discuss Day to Day Operations

Review Configurations for Specific Needs

Deployment Phases

INITIAL

- Reviewing Coverage Needs
- Start Services in Monitor-Only Mode

ROLLOUT

- Review Monitor-Only Results
- Create Protect (Inline) Policy
- Configure Advanced Settings

CLOSING

- Review Results
- Discuss Experience

Initial Phase

During this initial phase:

- Connecting to the Mail Server (O365 or Gmail)
 - Connecting to any service will automatically create a Monitor-Only rule for All Users and Groups
 - This is considered the Learning Phase and MUST be completed before going Inline
- Learning Mode occurs once connected to the mail service
- This phase is used to identify any issues handling messages before actions take place
- Identify additional needs for coverage
 - Malware coverage for these integrations is included in the Protect and Advanced Protection License levels
 - Additional services include the following:



Rollout Phase

During the Rollout Phase:

- Beginning to create Inline policies that enforce actions
- Rollout policies to specific groups or individuals for initial action testing
- Configure Advanced Anti-Impersonation and Phishing Confidence Levels
- Configure Click-Time Protection
- Configure Malware/DLP policies for integrations
- Review ShadowIT/Anomalies
- Review the Security CheckUp Report
- Review User Integrations

Closing Phase

Follow Up on Results

- Any false positives?

Follow Up on Customer Interaction Experience

- Have end users struggled with the workflow?
- Any need for Phishing Allow-Lists or excessive restorations?

Discuss Any Improvements

- Anything that would help with your workflow or user understanding?

DEPLOYMENT SUMMARY

- Initial: Monitor and Review Results
- Rollout: Deploy Inline
- Closing: Review Experience

Configuration Recommendations

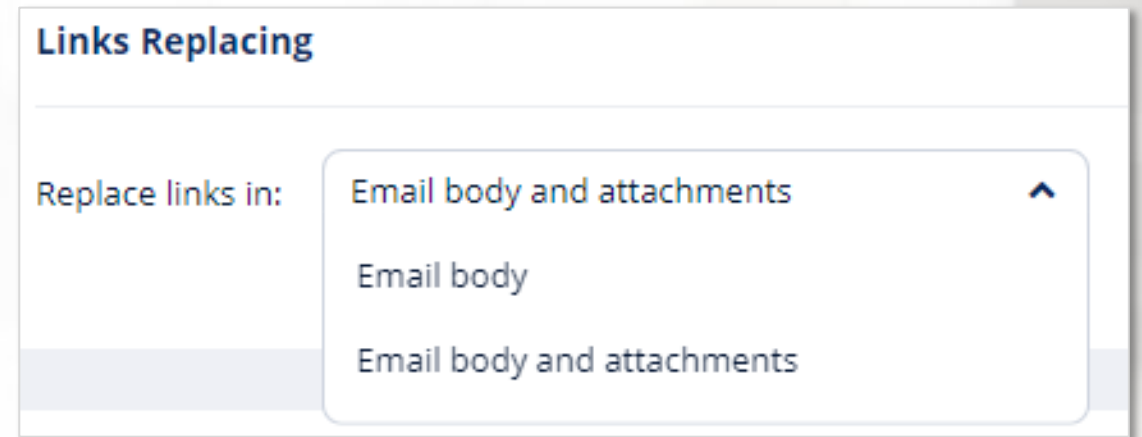
- Click-Time Protection
- Different Threat Detection Policy Suggestions
- Anti-Impersonation and Phishing Confidence Level
- User Configuration
- Quarantine Settings

Click-Time Protection Policy

Click-Time Protection is the URL rewriting aspect of Check Point

- As a message is received, the hyperlink of the URL is rewritten to go back to Check Point's URL scanning engine
- Enabled via a dedicated O365 Mail policy from the "Policy" section
- Offers URL Replacement for Email body and attachments

Recommendation: Enabled but only if not using another rewriting service



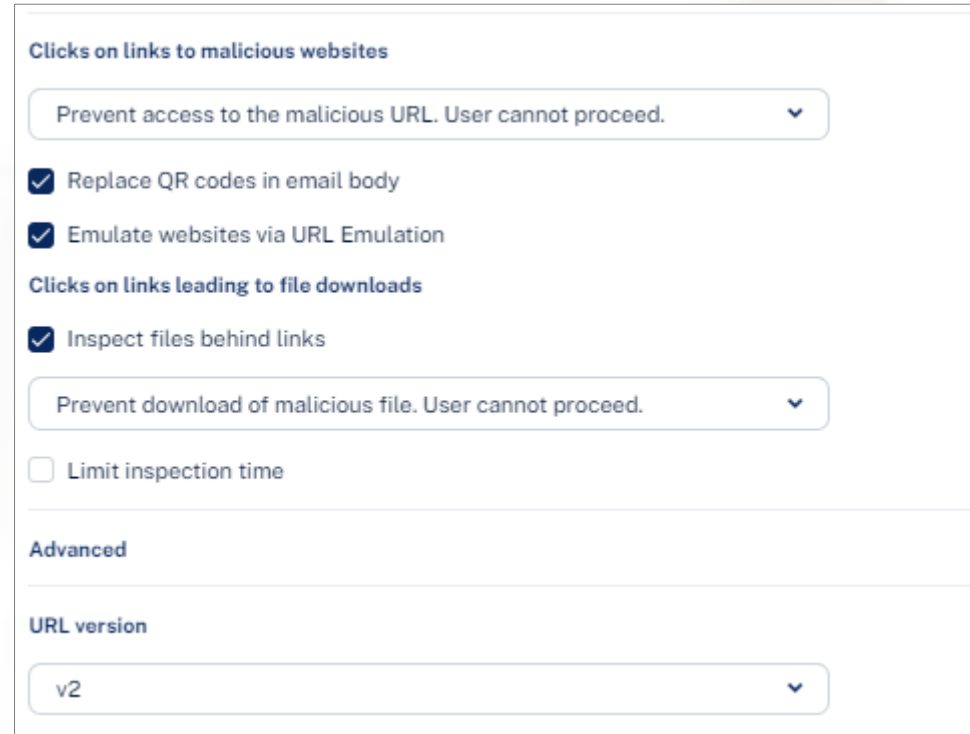
Click-Time Protection Re-Writing QR Codes

Replace QR codes in email body: Recommendation:

Allows for Check Point to replace QR codes found in emails so that way they can be rewritten to ensure the URL can be scanned

Recommendation:

Enable Relace QR codes in email body



The screenshot displays the 'Click-Time Protection' configuration interface. It is organized into several sections: 'Clicks on links to malicious websites' with a dropdown menu set to 'Prevent access to the malicious URL. User cannot proceed.'; a list of checkboxes where 'Replace QR codes in email body' and 'Emulate websites via URL Emulation' are checked; 'Clicks on links leading to file downloads' with 'Inspect files behind links' checked and a dropdown set to 'Prevent download of malicious file. User cannot proceed.'; an unchecked 'Limit inspection time' checkbox; an 'Advanced' section header; and a 'URL version' dropdown menu set to 'v2'.

Clicks on links to malicious websites

Prevent access to the malicious URL. User cannot proceed.

☒ Replace QR codes in email body

☒ Emulate websites via URL Emulation

Clicks on links leading to file downloads

☒ Inspect files behind links

Prevent download of malicious file. User cannot proceed.

☐ Limit inspection time

Advanced

URL version

v2

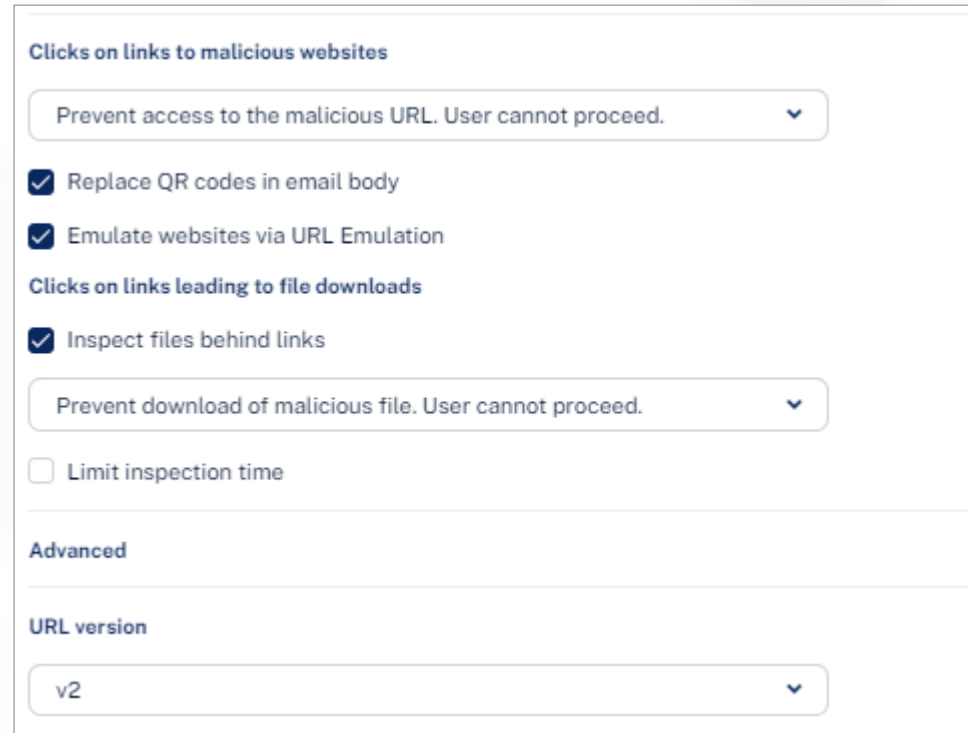
Click-Time Protection

Emulate websites via URL

Emulation: In addition to protecting users based on the reputation of the URL, we are now able to perform URL Emulation

- Once the link is clicked, Check Point's engine will scan the behavior of the landing URL
 - Looking for odd file download requests
 - Looking for odd sites prompting email login

Recommendation:
Enable URL Emulation



The screenshot displays the 'Click-Time Protection' configuration interface. It is organized into sections: 'Clicks on links to malicious websites', 'Clicks on links leading to file downloads', 'Advanced', and 'URL version'. Under the first section, a dropdown menu is set to 'Prevent access to the malicious URL. User cannot proceed.' Below this, two checkboxes are checked: 'Replace QR codes in email body' and 'Emulate websites via URL Emulation'. The second section has a dropdown set to 'Prevent download of malicious file. User cannot proceed.' and an unchecked checkbox for 'Limit inspection time'. The 'Advanced' section is currently collapsed. The 'URL version' section shows a dropdown menu set to 'v2'.

Section	Setting
Clicks on links to malicious websites	Prevent access to the malicious URL. User cannot proceed.
	<input checked="" type="checkbox"/> Replace QR codes in email body
Clicks on links leading to file downloads	<input checked="" type="checkbox"/> Emulate websites via URL Emulation
	<input checked="" type="checkbox"/> Inspect files behind links
Clicks on links leading to file downloads	Prevent download of malicious file. User cannot proceed.
	<input type="checkbox"/> Limit inspection time
Advanced	(Collapsed)
URL version	v2

Click-Time Protection

Inspect files behind links:

- This feature allows us to inspect files when a URL leads directly to them. This inspection includes sandboxing the file to determine any malicious characteristics

Recommendation:

Inspect files behind links enabled

Prevent the download of malicious files. User cannot proceed

URL Version: v2

Clicks on links to malicious websites

Prevent access to the malicious URL. User cannot proceed. ▾

☒ Replace QR codes in email body

☒ Emulate websites via URL Emulation

Clicks on links leading to file downloads

☒ Inspect files behind links

Prevent download of malicious file. User cannot proceed. ▾

☐ Limit inspection time

Advanced

URL version

v2 ▾

Threat Detection Policies

Policies and their workflow allow for the scanning and automation of message handling through Check Point.

These policies can have different workflows based on several factors

- The level of communication between admin and end-user
- The level of security vs. disruption to business operations

Threat Detection Policy Workflows

User receives the email with a warning

- Message is received by the end-user but with a warning banner in Outlook

Warning: This mail is suspected to be a phishing e-mail. Are you sure you trust the sender (<sender>)?
[Yes](#) [No](#)

- Low security since the message isn't quarantined
- High user interaction since they can view the message still

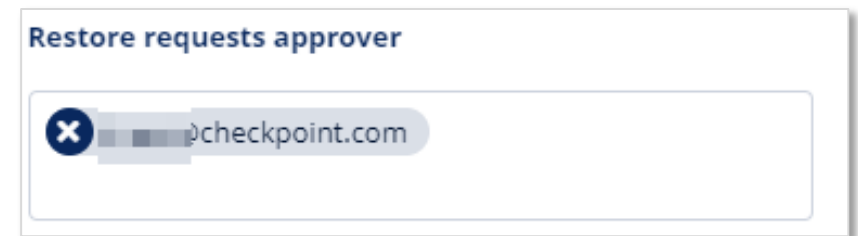
Quarantine. User is alerted and allowed to restore the email

- End user is notified that the message was quarantined but the user can restore the message themselves
- Low security since the user can restore the message themselves
- High user interaction since the user can restore the message themselves

Threat Detection Policy Workflows

Quarantine. User is alerted and allowed to request a request (admin must approve)

- Message is quarantined and the user is alerted and allowed to request a restore
- Users identified as Restore request approvers receive email notifications of a restore request
 - Those individuals are defined under “Configure” > “SaaS Application” > Office 365 Mail or Gmail then under “Restore requests approver”
- High security due to an admin having to approve
- Low user interaction since a user must request and wait for the restore



Threat Detection Policy Workflows

Quarantine. User is not alerted (admin can restore)

- User isn't alerted, and the message is just sent to quarantine if detection is found
- If a user is missing a message, they will need to reach out to the portal admin to locate it for restoration or confirmation it was quarantined.
- High security because the message was quarantined
- Low user engagement because the end-user never knows about the message

Threat Detection Policy Workflows

Email is allowed. Delivered to Junk.

- Message is allowed but delivered to the junk folder
- Low security because users are still able to access the message directly
- High user engagement because they have access to the message

Do nothing.

- Never recommended. Should always have an action

Email is allowed. Header is added to the email.

- Message is allowed and a Header is added
- Exchange rules can be created to perform certain actions based on the added header
- Low security because the message is still allowed
- High user interaction because the message is allowed

Password Protected Attachments Workflows

Require the end-user to enter a password.

- This option allows the end user to receive a prompt to enter in the attachment password.
- This allows Check Point to scan the attachment before releasing to the user.

Do nothing.

- Never recommended. Should always have an action

Trigger suspected malware workflow.

- This triggers the action defined under the “Suspected malware attachments workflow” section.

Attachment Cleaning (Threat Extraction) Workflows

Threat Extraction is the Check Point Content Disarm and Reconstruction (CDR) engine.

Attachment Cleaning (Threat Extraction) can create a safe version of an email attachment in these ways:

- **Clean** - removes macros, embedded objects, and any active content from the attachment while maintaining the file type.
 - For example, if a DOC file is cleaned, the end user will get a modified DOC file.
- **Convert** - the file is converted into PDF format, regardless of its original file type, ensuring no active content can ever be a part of it.
 - For example, if a DOC file is converted, the end user will get the file in PDF format.

Spam Threat Detection Policy Workflows

Email is allowed. Deliver to Junk folder.

- Message is sent directly to the user's Junk Folder
- Most common workflow for Spam

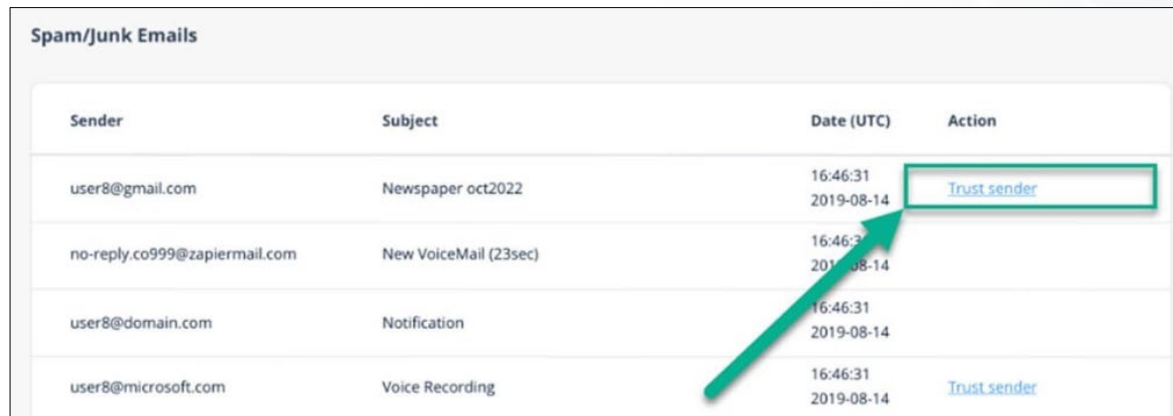
Add [Spam] to subject.

- Message is sent to the user's Inbox with [Spam] added to the subject
- Useful if users don't want to check their Junk folder

Spam Threat Detection Policy

Allow end-users to trust senders of Spam emails

- Enabling this allows end-users to trust senders from the Daily Digest
- This trust allows for messages marked as spam to be delivered to the Inbox instead.
- This Trust only extends to messages identified as Spam
 - Any malicious messages would still be handled according to the policy



Sender	Subject	Date (UTC)	Action
user8@gmail.com	Newspaper oct2022	16:46:31 2019-08-14	Trust sender
no-reply.co999@zapiermail.com	New VoiceMail (23sec)	16:46:31 2019-08-14	
user8@domain.com	Notification	16:46:31 2019-08-14	
user8@microsoft.com	Voice Recording	16:46:31 2019-08-14	Trust sender

Graymail workflow

Email is allowed. Deliver to Promotions folder

Graymail consists of legitimate but often unwanted emails, such as newsletters and promotional emails, which many users find unnecessary, making it harder to find important messages.

The Graymail workflow moves these unwanted emails to a dedicated folder in the user's mailbox, ensuring a well-maintained inbox and enhancing productivity.

When setting the policy, the mail folder can be named and created automatically in the users' mailbox.

Clean Emails Threat Detection Policy Workflows

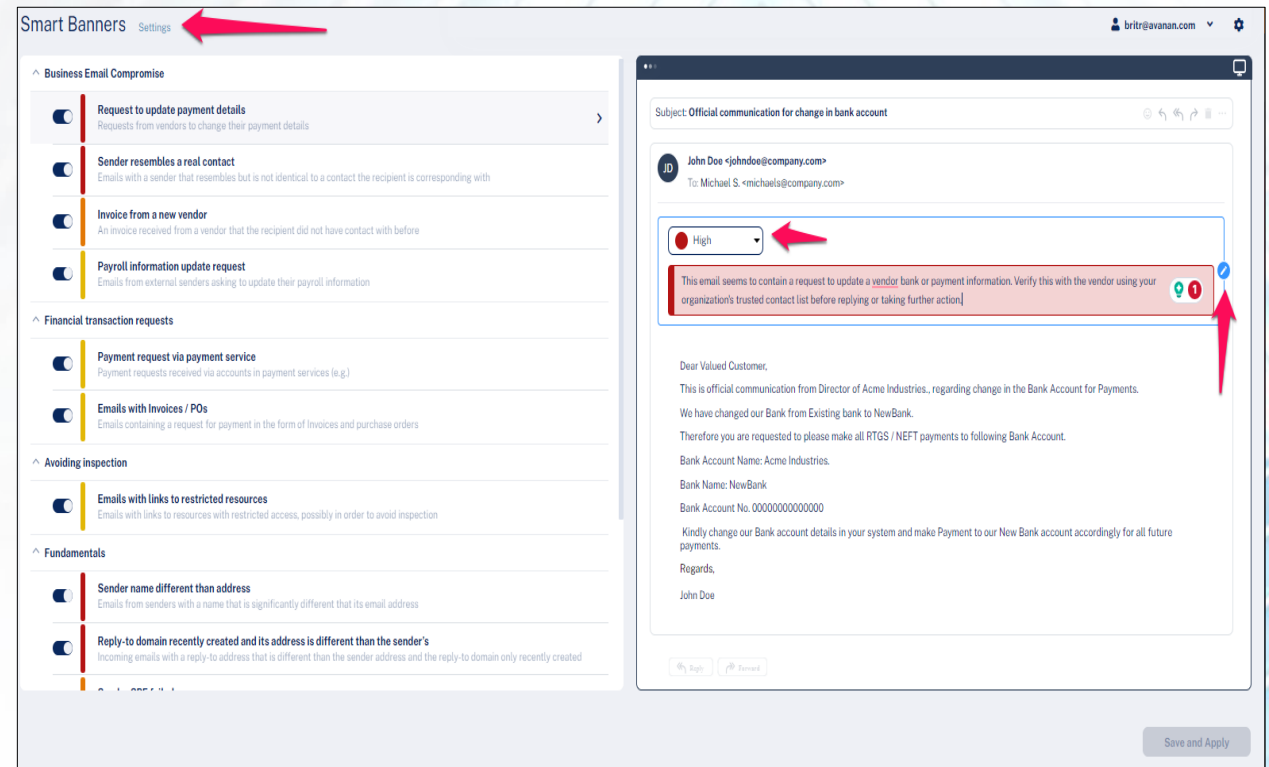
SmartBanner

Clean Email Workflow

- Check Point can apply an additional workflow on messages that have passed without malicious or spam detection.
- This scanning is looking for the following use cases:
 - All external Emails
 - Emails with Invoices
 - Requests to change bank accounts
 - Emails from new partners
 - Any many more

Smart Banner

- Smart Banners are located under the “User Interaction” section.
- From here, Smart Banners can be turned on or off as desired, and the wording in the banner can also be edited.
- The severity of the event can also be changed.
- The Settings section at the top lets you enable new banners automatically when they’re released.



Policy Suggestions

- Following are some policy suggestions depending on the level of security you want to apply across your users.
- Multiple Threat Detection policies can be created for different groups within the organization.
- Policies are enforced from Top Down.
- Smart Banners recommended for all policies

“Low Security” Threat Detection Policy

- This policy allows for the most user interaction.
- Users only get warned about phishing messages but still can receive them.
- Messages containing malware are quarantined, but users can release them
- Recommended for only the highly Security minded end-users (typically within the MSP)

The screenshot displays the configuration interface for a 'Low Security' Threat Detection Policy. It is organized into several sections, each with a title and a list of workflow settings. Each setting consists of a workflow name, a dropdown menu for the action, and a gear icon for further configuration.

- Phishing**
 - Phishing workflow: User receives the email with a warning
 - Suspected phishing workflow: ★ User receives the email with a warning
- Attachments**
 - Malware Attachments**
 - Malware attachments workflow: Quarantine. User is alerted and allowed to restore the email
 - Suspected malware attachments workflow: ★ Quarantine. User is alerted and allowed to restore the email
 - Password Protected Attachments**
 - Password-protected attachments workflow ⓘ: ★ Require the end-user to enter a password
- Spam**
 - Spam workflow: ★ Email is allowed, Deliver to Junk folder
- Attachment Cleaning (Threat Extraction)**
 - ☐ Clean attachments before delivering to end users

“Middle” Threat Detection Policy

- Workflows with the star icon are suggested
- Policy uses several workflows that allow Users to be self-sufficient
- Higher severity events require Administrator approval
- Spam messages go to the Junk
- Attachment Cleaning removes macros, embedded objects, any active content. User able to restore

Phishing

Phishing workflow	★ Quarantine. User is alerted and allowed to request a restore (admin...	⚙️
Suspected phishing workflow	★ User receives the email with a warning	⚙️

Attachments

Malware Attachments

Malware attachments workflow	★ Quarantine. User is alerted, allowed to request a restore (admin m...	⚙️
Suspected malware attachments workflow	★ Quarantine. User is alerted and allowed to restore the email	⚙️

Password Protected Attachments

Password-protected attachments workflow ⓘ	★ Require the end-user to enter a password	⚙️
---	--	----

Spam

Spam workflow	★ Email is allowed. Deliver to junk folder	⚙️
---------------	--	----

Attachment Cleaning (Threat Extraction)

☒ Clean attachments before delivering to end users

Clean	All supported file types ⓘ
Convert to PDF	None ⓘ
Attachment cleaning workflow	User is allowed to restore any attachment

“High” Threat Detection Policy

- Mostly Quarantine, but the user is not alerted
- Minimal User Interaction
- If users are missing anything, they can reach out to locate the message and restore it as needed by the administrators

Phishing

Phishing workflow	Quarantine. User is not alerted (admin can restore) ▼
Suspected phishing workflow	Quarantine. User is not alerted (admin can restore) ▼

Attachments

Malware Attachments

Malware attachments workflow	Quarantine. User is not alerted (admin can restore) ▼
Suspected malware attachments workflow	Quarantine. User is not alerted (admin can restore) ▼

Password Protected Attachments

Password-protected attachments workflow ⓘ	★ Require the end-user to enter a password ▼ ⚙️
---	---

Spam

Spam workflow	★ Email is allowed. Deliver to Junk folder ▼
---------------	--

Attachment Cleaning (Threat Extraction)

☒ Clean attachments before delivering to end users

Clean	None ▼ ⓘ
Convert to PDF	All supported file types ▼ ⓘ
Attachment cleaning workflow	User is allowed to request a restore for any attachment (admin must approve) ▼

Advanced Options

The Advanced Options allows us to extend Check Point's advanced scanning to outbound messages

Protect (Inline) Outgoing Traffic

- Checking this box allows Check Point to scan messages as they leave the organization.
- The use-case for this is so that in the event of a compromised account, Check Point can catch any attempts to send out spam or malicious messages to maintain your organization's reputation.
- SPF records updates are recommended to ensure delivery with this specific configuration.
- SPF Entry: include:spf.cpmail.com
- This covers both Inline, Outgoing scanning and DLP

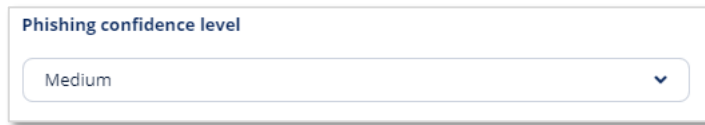
Advanced Impersonation and Phishing Confidence

- These are some Advanced configuration recommendations
- This section is available at the bottom of the Threat Detection Policy
- Also available under “Configuration” > “Security Engines” > “Configuration” to the right of Smart-Phish

Advanced Impersonation and Phishing Confidence

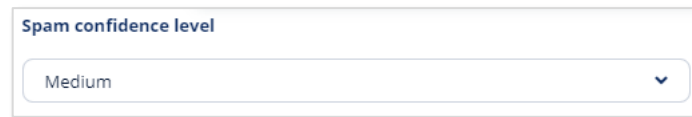
Confidence Level

- Confidence level is how sure Avanan is that a message is phishing or spam
- The higher the Confidence Level, the fewer messages identified but the messages we flag we're more confident
- Recommendation: Medium
- Changes needed: Only when dealing with large amounts of false positives but this reduces the number of messages caught.
- Spam Confidence level is configured at the bottom. Also, recommend Medium.



Phishing confidence level

Medium



Spam confidence level

Medium

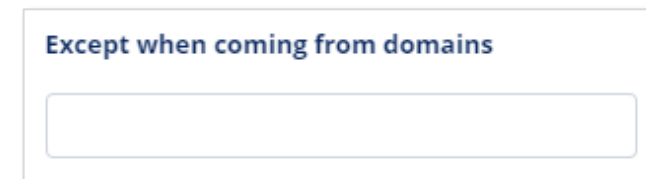
Advanced Impersonation and Phishing Confidence

Detect nickname impersonations attempts from:

- This setting is used to determine whom to provide nickname impersonation protection
- Recommendation: Any internal User
- For any legitimate impersonations, add just the domain to “Except when coming from domains”
 - These are separated by a comma then a space: Domain1.com, domain2.com, domain3.com



The screenshot shows a configuration panel titled "Detect nickname impersonation attempts from". It features a dropdown menu with "Any internal user" selected. Below the dropdown is a search bar with a magnifying glass icon and a vertical bar. Under the search bar, there are three options: "Important/key-people only", "Any internal user", and "Do not detect nickname impersonation attempts".



The screenshot shows a configuration panel titled "Except when coming from domains". It contains a single, empty text input field for entering domain names.

Advanced Impersonation and Phishing Confidence

Important/key-people group

- This section is used if you want to define a specific group/people
- This isn't needed if using "Any Internal Users"

Important/key-people group

When a nickname impersonation is detected

- Use the "Suspicious" workflow while tuning out legitimate Impersonations

When a nickname impersonation is detected

- ☐ Trigger "Phishing" workflow
- ☒ Trigger "Suspicious" workflow

Advanced Impersonation and Phishing Confidence

Detect impersonation attempts only for human names

- This address impersonation detections for generic accounts such as support@domain.com and admin@domain.com

☐ Detect impersonation attempts only for human names

Advanced Impersonation and Phishing Confidence

When a newly registered domain sends an email, apply the following workflow:

- Recommend using the “Trigger “Suspicious” workflow” while tuning the policy.

When a newly registered domain sends an email, apply the following workflow

- ☐ Do nothing
- ☒ Trigger "Suspicious" workflow
- ☐ Trigger "Phishing" workflow

- Once confident in the results, the “Trigger “Phishing” workflow” can be used

Minimum age of newly registered domain (in days)

- Default is 15
- Other suggestions are 30 or 45

Minimum age of newly registered domain (in days)

15

Advanced Impersonation and Phishing Confidence

When the sender domain resembles the domain of a partner

- This setting determines what happens when a sender's domain appears similar to a domain used by a trusted partner.
 - Trusted Partners are developed over time or as part of the Learning Mode during onboarding.
 - Recommendation/default: Consider as an indicator in the standard Anti-Phishing inspection
 - Additional security: Trigger Phishing workflow

Advanced Impersonation and Phishing Confidence

Allow-list emails that are allow-listed by Check Point also in Microsoft/Google

- This option allows items added to the Check Point Anti-Phishing Allow List to be added to the Allow Lists within Microsoft/Google.
- This ensures that the allowed traffic is allowed through the data flow.
- Suggested

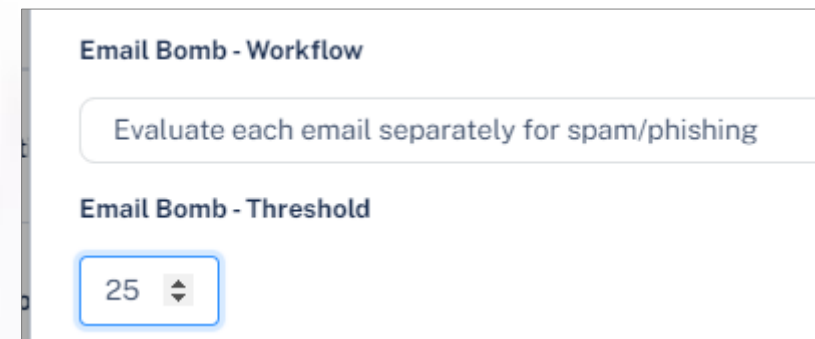
Allow-list emails that are allow-listed by Microsoft (SCL = -1) also in Check Point

- This option allows messages sent from Microsoft to Check Point with an SCL score of -1 to be added to the Check Point Anti-Phishing Allow List
- Not suggested

Advanced Impersonation and Phishing Confidence

Email Bomb

- This is when an email is used to sign up for a large number of unsolicited services or mainlining lists, which then begin to send you welcome emails, registration emails, or marketing information.
- This creates a flood of messages that crowd out legitimate emails in the mailbox.
- The challenge this poses is that these emails come from legitimate senders and from so many different senders that detection and blocking become difficult.
- Recommendation: Evaluate each email separately for spam/phishing
- Threshold: 25



The screenshot displays a configuration window titled "Email Bomb - Workflow". It contains a button labeled "Evaluate each email separately for spam/phishing". Below this, the "Email Bomb - Threshold" section shows a numeric input field with the value "25" and a small up/down arrow icon.

Advanced Impersonation and Phishing Confidence

Enforce the following workflow on DMARC failed emails, with action reject/quarantine

- DMARC failures are the failure of both SPF and DKIM to establish the identity of the sender
- A CSV of failed DMARC for a specific domain can be requested from Support
- Recommendation:
Utilize “Trigger “Suspicious” workflow” while addressing DMARC failures

Enforce the following workflow on DMARC failed emails, with action = reject/quarantine

☒ No extra action

☐ Trigger "Suspicious" workflow

☐ Trigger "Phishing" workflow

Advanced Impersonation and Phishing Confidence

Emails flagged as Spam by Microsoft/Google but Clean by Check Point

- This allows for an override of messages identified by Microsoft or Google as Spam, but the Avanan/Check Point finds them clean.
 - This allows Check Point to deliver the messages to the Inbox instead of the Junk folder.
 - Recommendation: Treat as Clean email

Emails flagged as Spam by Microsoft/Google but Clean by Check Point

Treat as Clean emails



Advanced Impersonation and Phishing Confidence

Mark emails from your domains(s) as phishing when

- This only applies to your domains / the tenant domains
- Hard Fail vs. Soft Fail
 - Depends on how the domains server is set up
 - Soft Fail usually means to send to spam while hard fail means the message should be discarded
 - Recommendation:
SPF = Fail, only after all SPF issues have been addressed

Mark emails from your domain(s) as phishing when

No extra action

Q |

No extra action

SPF=Softfail OR SPF=Fail

SPF=Fail

SPF<>Pass

Advanced Impersonation and Phishing Confidence

Match nicknames by email address

- Useful for identifying someone trying to add another email address to the nickname field
- Recommendation: Enable

☒ Match nicknames by email address

Best Practice Summary

- Utilize Click-Time Protection
- Determine your level of engagement with the customer
- Review Advanced Impersonation and Phishing Confidence Levels
- Identify and correct any SPF issues

User Management – RBAC

- **User access to portals can be controlled on a per-tenant basis.**
- **MSP Admin**
 - Access to everything
- **MSP Help Desk**
 - No access to “Settings” section
 - Can be configured to limit portal access
 - All tenants
 - All except named tenants
 - Only named tenants

▼ MSP Portal Settings ⓘ

Role

MSP Help Desk

Tenant Access

☐ All tenants ⓘ

☒ All tenants except ⓘ

Type to search

☐ Only specific tenants ⓘ

User Management – User Data

- An important consideration when creating users is whether they will be reviewing messages
- Any user that is expected to investigate malicious messages should have the option “Allow drill-down into user data” enabled
- This can be turned on at the MSP level to limit access to All User Data or when a Detection Exists
 - Flagged as phishing, malware, or spam

- ☒ Allow drill-down into customer data ⓘ
- ☐ All User Data ⓘ
- ☒ When Detection Exists ⓘ

User Management – User Data Message View

- With this option enabled, users get the ability to view the body of the raw email as well as download the message from the “Email Profile” section
- Having this enabled also shows the “AI textual analysis of the email body” section for the message which can be imperative in understanding the “Text analysis” aspect of the AI model

Show body from raw email

[Show](#)

Download this email

[Download](#)

AI textual analysis of the email body

This widget presents the AI analysis of the email body

☒ Raw body

From Address: [redacted] [No SPF record] [First Time Sender]

To: [redacted]

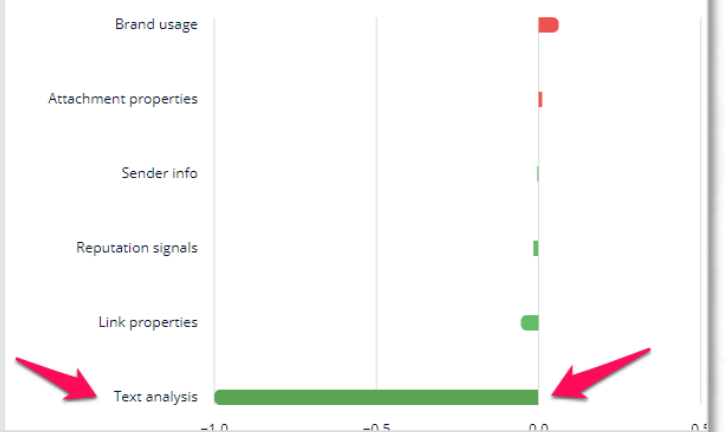
Reply-To: [redacted]

Subject: Urgent Google Workspace Notification

Google Account Login Notification Dear Google Customer, We have recently made some changes on your Google account. When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control. Login You Google Account can also be connected with other services. Login for Gmail Connect Gmail to Outlook

AI model impact

This chart shows how each group of features affect the overall decision of the AI model




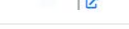







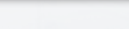


Daily Workflow

- Review any Pending Security Events
- Restore Request/
User Reported Phishing
- Investigate Messages

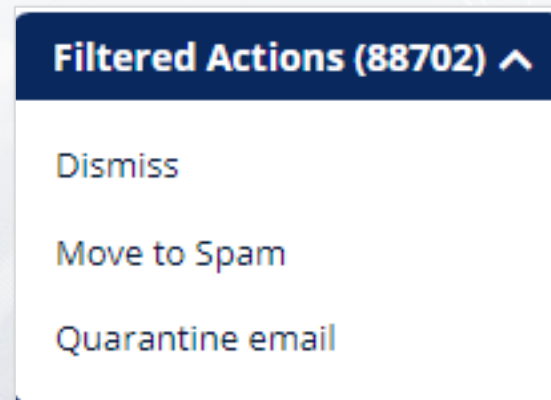
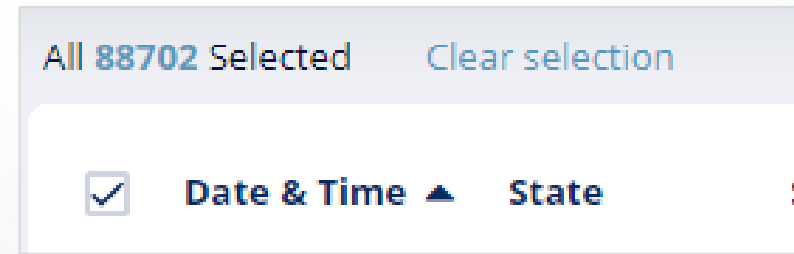
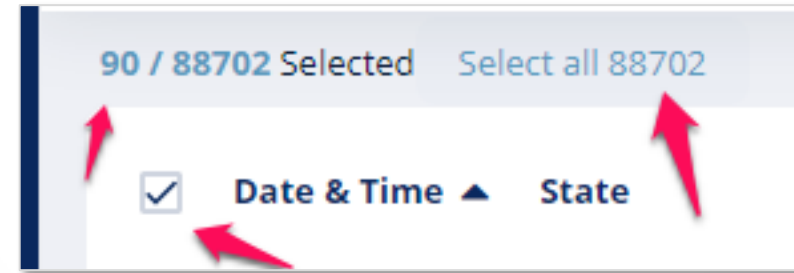
Daily Workflow – Reviewing Pending Security Events

- From the MSP portal, under “Security Events” you have a window into the pending events for each of your tenants
- Pending events should only occur for items that don’t have a workflow
 - Either the tenant doesn’t have Inline policies taking action (Events identified while in Monitor-Only mode will need to be dealt with manually)
 - Or with Anomalies/ShadowIT, this must be manually reviewed and create Exceptions as needed
- Clicking any of the numbers should drop you directly into the portal

Tenant	Overall Pending Events	Phishing	Malware	Suspicious Malware	DLP	Anomaly Events	Malicious URL Click	Shadow IT	Alert	Spam
	4	0	0	0	0	0	0	0	0	4
	218	12	1	0	0	1	0	0	3	201
	573	0	0	0	0	0	0	0	0	573
	313	14	1	0	0	0	0	0	0	298
	6	0	0	0	0	0	0	3	0	3
	2	0	0	0	0	0	0	0	1	1
	5	0	0	0	0	0	0	1	0	4
	3	0	0	0	0	0	0	3	0	0
	1	0	0	0	0	0	0	1	0	0
	7	0	0	0	0	1	0	0	0	6
	2	0	0	0	0	0	0	1	1	0
	1	0	0	0	0	0	0	1	0	0

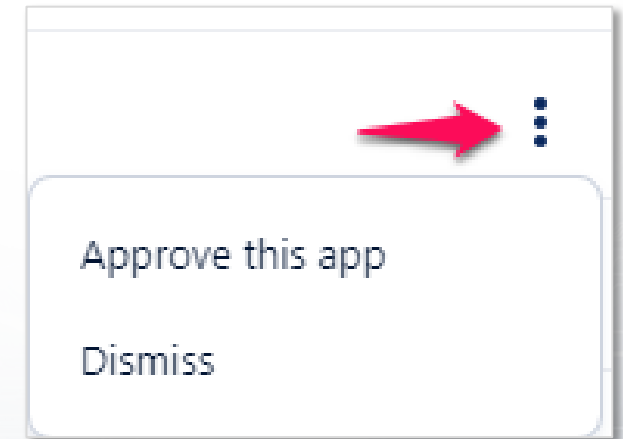
Pending Events

- Pending Phishing/Malware/Spam events can be handled in bulk from the “Events” section.
- Using the “Type” and “State” filters, you can identify all these messages and act on them.



Shadow IT

- Shadow IT can take messages related to applications and call out what specific application is being used.
- The purpose of this section is to filter out all of the business-approved applications so all the rest bubble up to the top.
- Approval for an application is only needed for one user and it approves it for everyone.
- This does not grant any users access they didn't already have.
- Don't hesitate to use the "Dismiss" option for applications you wish to monitor.



Anomalies

Anomalies are mail activity events that are pulled by the portal for any events that are outside the usual activity for this user.

- This can include first-time logins from new countries
- Performing activity in one location and then performing another activity from a distant location
 - Typical with VPNs
- Large number of password resets
- Varies Exceptions can be created depending on the event

Check Point's Engineering has put a great focus on identifying what we consider "Critical Event"

- New delete-all-emails Outlook rule
- Internal user is sending malicious/spam emails

Restore Requests

- End-users can request the restoration of messages and files that they believe are safe.
- When the workflow includes “admin must approve,” anyone listed as a “Restore request approver” will receive an email notifying them of a request for restoration.
- A link in the email will take you to the approval page, which can also be found under “User Interaction” > “Restore Requests”.
- Approvers can review the message and then decide to Restore or Decline the request.
- Providing end-user feedback is configured under “User Interaction” > “Configuration,” then check the box for “Send feedback email to end users.”

User Reported Phishing

- A message may come in that end-users feel is unsafe or suspicious so they can report this message according to their internal process.
- Due to recent changes in how Microsoft handles these messages, you must now specify the mailbox to which these reported messages are sent.
- You must specify this mailbox in Microsoft and the portal
 - This account can be a shared mailbox, so it doesn't require a Microsoft license
- The message can be investigated within Check Point under "User Interaction" > "User Reported Phishing".
- An admin can then quarantine that message or decline the notification.

User Reported Phishing

- **Workflow**

- “Phishing” event vs. “Alert” event
 - The “Alert” event will notify users with the “Send Alert” option turned on.
 - The “Phishing” event will be flagged in the events section as a pending “Phishing” event.

- **Phishing reporting mailboxes**

- This is the mailbox set to receive user-reported phishing events that Check Point will monitor.
- Users can report suspected malicious emails using a plugin for Outlook
- Configuring Microsoft to send these reports to a specific mailbox can be found [here](#).

User Reported Phishing

Reviewing phishing reports

- Allows for automated handling of user-reported phishing events that the system has Re-evaluated.
 - Based on this Re-evaluation, workflows can be set depending on how its Re-evaluated.

Reviewing phishing reports

The Check Point AI re-evaluates every reported email and provides a recommended action on the phishing report.

Select if you want to automate the actions.

★★★★ Automatic

★★★★ Manual
Every report will be manually reviewed by an admin.

★★★★ Semi-automatic
Automated actions for some updated verdicts and manual review for others.

★★★★ Automatic
The automatic recommendations will be performed. You will not have to do anything.

★★★★ Incident Response as a Service (IRaaS) ⚡
Check Point analysts handle your user's phishing reports and quarantine restore requests.

Re-evaluated as: Inconclusive

Approve report. Quarantine the email

☒ Notify Admin ⚙️

☒ Notify User ⚙️

Re-evaluated as: Phishing

Approve report. Quarantine the email

☒ Notify Admin ⚙️

☒ Notify User ⚙️

User Reported Phishing

- **Reviewing phishing reports**
 - Suggestion: Automation with some changes to “Clean” depending on your needs.

▼ **Reviewing phishing reports**

The Check Point AI re-evaluates every reported email and provides a recommended action on the phishing report.

Select if you want to automate the actions.

★★★★ Automatic ▼

▼ **Workflows and notifications**

Re-evaluated as: Clean	Re-evaluated as: Inconclusive	Re-evaluated as: Phishing
<div>Send for admin review ▼</div> <div><input checked="" type="checkbox"/> Notify Admin ⚙️</div> <div><input checked="" type="checkbox"/> Notify User</div> <div><input type="checkbox"/> When report is sent for review ⚙️</div> <div><input checked="" type="checkbox"/> When report is approved ⚙️</div> <div><input checked="" type="checkbox"/> When report is declined ⚙️</div>	<div>Approve report. Quarantine the email ▼</div> <div><input checked="" type="checkbox"/> Notify Admin ⚙️</div> <div><input checked="" type="checkbox"/> Notify User ⚙️</div>	<div>Approve report. Quarantine the email ▼</div> <div><input checked="" type="checkbox"/> Notify Admin ⚙️</div> <div><input checked="" type="checkbox"/> Notify User ⚙️</div>

User Reported Phishing

Phishing simulation emails

- Check Point can identify phishing simulation emails, which will automatically be declined from being reported to Check Point for being simulations.
 - Notify User
 - Depends on organization's discretion.

Email notification sender

- Allows administrators to make changes to the user-reported notifications, including;
 - Friendly From name
 - From address
 - Custom name can be used but requires SPF record be updated.
 - Reply-to address

Quarantine Settings

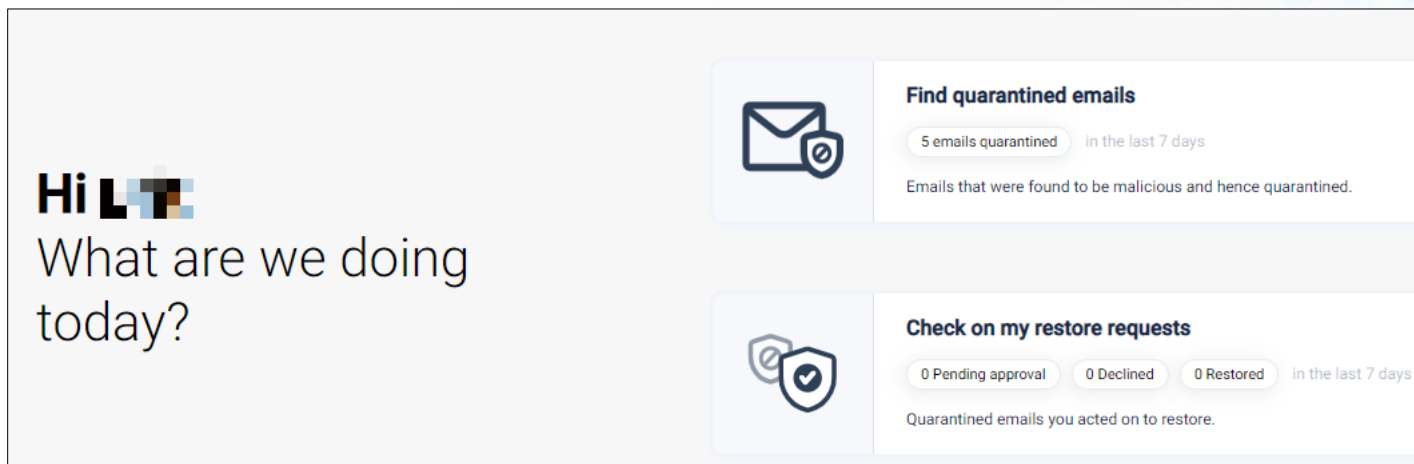
- This section controls how users can be notified of quarantined emails.
- This includes an End-User portal and routine End-User reports that can be scheduled.
- Section also includes settings for handling Emails quarantined by Microsoft.
- Found under “Security Settings” > “User Interaction” > “Quarantine”
- Also found under “User Interaction” > “Quarantined Items” then “Settings” at the top

Quarantine Settings

Email Security Portal for End Users

- Portal that can be used for end-users to access their quarantined emails, request/monitor restoration if the policy allows, and add senders to their Trusted Senders list.
 - <https://email-security-portal.avanan.net/#/auth>
 - <https://email-security-portal.checkpoint.com/#/auth>
 - Depends on if you're using an Avanan or Check Point-based tenant

Recommendation: Enable



Restore Request Feedback

Restore Request Feedback

- Allows Administrators to decide if Restore Requests are declined, should the end user be notified.
- Recommendation:

Email notification sender

- This sender is used for Restore Requests communications to the end users.
 - Friendly From name
 - From address
 - Custom name can be used but requires SPF record be updated.
- Reply-to address

End User Quarantine Report

End User Quarantine Report

- Enable to allow end users to receive daily digests regarding messages of theirs that were quarantined.
- For phishing messages to appear in this digest, there must be a Threat Detection policy that mentions “User is Alerted,” as this gets the messages added to the digest.

Include spam emails that are sent to the Junk folder

- This allows for spam messages to appear on the daily digest
- This is used with the Threat Detection policy option, “Allow end-users to trust senders of Spam Emails,” to allow end-users to trust senders of spam messages so they get delivered to Inbox.

Allow end users to generate a quarantine report on demand.

- Allows users to access previously received digests. At the bottom is a link that will generate a new digest for the user for the last 24 hours.
 - This will still be sent even if the user hasn’t had any messages quarantined in the last 24 hours.

End User Quarantine Report

Office 365/Google Users – Stop sending immediate quarantine notification emails

- This means that immediate notifications when a message is quarantined will be suppressed, allowing only the Quarantine Digest to be sent to the end user.
 - This is useful for customers looking to limit how many notifications are sent to users.

Scheduling

- This allows administrators control over when the daily digest is sent to end users, setting the time zone and allowing the report to be sent multiple times a day.
 - If no messages have been quarantined, no digest will be sent.

Recipients

- This controls who receives the digests.

Email Quarantined by Microsoft

Emails Quarantined by Microsoft as High Confidence Phishing

- This acts as an override for when Microsoft labeled a message “High Confidence Phishing,” but Check Point found it clean/spam/suspected phishing.
 - This was created to address several false positives with the High Confidence Phishing label, which can’t be turned off, or exclusions created on the Microsoft side.
 - Recommendation: Turn it on and set it to “Clean.”

Include emails quarantined by Microsoft.

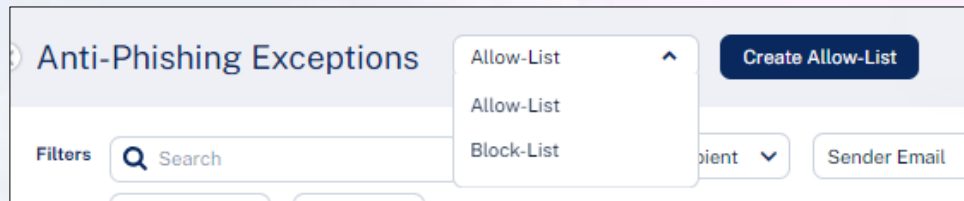
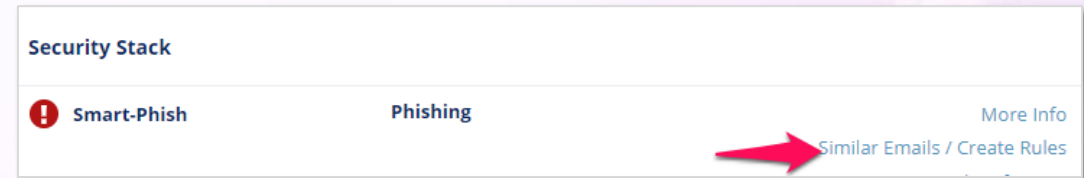
- This allows for messages quarantined by Microsoft to appear on the digest and enable the workflows to be set based on how Microsoft flagged them.
- Recommendation: Enabled

Exceptions

- There are many ways to create exceptions
- There are exceptions for any sort of need

Anti-Phishing Allow/Block List

- Avanan/Check Point's Anti-Phishing lists cover both phishing and spam events
- These can be created in several different locations
 - Directly from the message view
 - This will pull in data from the message
 - From “Mail Explorer”
 - Under “Configuration” > “Anti-Phishing Allow-List/Anti-Phishing Block-List”

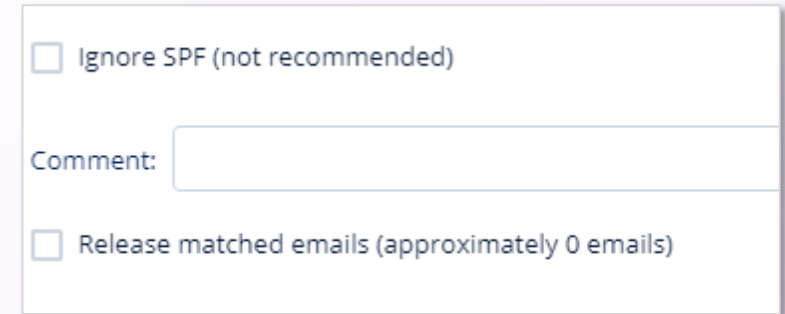


- Use data and adjust the “Date Received” to locate matches

Anti-Phishing Allow/Block List Continued

Create Allow-List Rule

- Only use “Ignore SPF” if necessary
 - SPF is how we prevent spoofing on Allow-List
- “Release matched email” we release messages previously quarantined



The screenshot shows a configuration panel for an Allow-List rule. It contains three main sections: a checkbox for 'Ignore SPF (not recommended)', a 'Comment:' label followed by a text input field, and another checkbox for 'Release matched emails (approximately 0 emails)'.

☐ Ignore SPF (not recommended)

Comment:

☐ Release matched emails (approximately 0 emails)

Create Block-List Rule

- “Detection type” is how the matched event will be identified
- “Quarantine matched email” will quarantine all messages identified.

Anti-Malware Allow/Block-List

Lists used to allow files identified by signature/sandboxing of the Malware Engine.

Can create Allow/Block-Lists based on File MD5 and MD5 of macros within the file.

- Useful for allowing spreadsheets with macros where the MD5 of the file changes.
- Acts as a sort of watermark for identifying the file when other aspects change.

Click-Time Protection Exceptions

Allow-List

- Click-Time Protection engine automatically flags this URL as clean without even scanning it.

Block-List

- Click-Time Protection engine automatically flags this URL as malicious without even scanning it.

Ignore-List

- Click-Time Protection engine will not replace this URL.



Anti-Spam

- The Anti-Spam exceptions tie back into our “Trusted Senders” feature on the Daily Digest.
- These exceptions ensure that messages marked as Spam are instead sent to the Inbox if they’re from a specific sender.
- This section in the UI allows the Admin to create their exceptions for specific sender/recipient and also view any that the end-user has created.

URL Reputation

- This section entirely depends on the site's reputation and how other services view this site.
- This section is used if a detected URL is flagged as malicious due to the reputation of the site but doesn't contain any malicious elements
 - This may be due to prior reputation
- This includes Exceptions for our “Password Protected Attachment” scanning feature
 - This Exception ensures that we no longer strip off the attachment before the user receiving the message.

DLP Allow-List

- Used to allow items to pass through when identified by the DLP engine
- Allow-List Type can be either a string or the MD5 of a file
 - String option only available with “View Private Data” enabled

Create DLP Allow-List

Allow-List Type

String ▲
File MD5
String

Type a String to add Allow-listed String with DLP violation.

Type a string

+ Add String

Comment

Type comment...



Thank You!



YOU DESERVE THE BEST SECURITY