



🔍 Search...

Proofpoint's Threat Research team has observed threat actors abusing M365 tenants to relay unauthorized messages. Please review these guidelines. [\(/community/s/article/Email-Protection-PPS-PoD-Prevent-Unauthorized-Microsoft-365-Allow-Relay\)](/community/s/article/Email-Protection-PPS-PoD-Prevent-Unauthorized-Microsoft-365-Allow-Relay)

Learn More

[\(/community/s/article/Email-Protection-PPS-PoD-Prevent-Unauthorized-Microsoft-365-Allow-Relay\)](/community/s/article/Email-Protection-PPS-PoD-Prevent-Unauthorized-Microsoft-365-Allow-Relay)

Email Protection (PPS/PoD)
[\(/community/s/topic/OTO39000000...\)](/community/s/topic/OTO39000000...)

EMAIL FIREWALL
[\(/community/s/topic/OTO39000000...\)](/community/s/topic/OTO39000000...)

Was this article helpful?



7



0

[Email Protection (PPS/PoD)] Prevent Unauthorized Microsoft 365 Allow-Relay

This article describes how to configure your PPS cluster and Microsoft 365 environment to prevent unauthorized Microsoft 365 allow-relay.

🕒 Jun 24, 2024 · Knowledge

TITLE

[Email Protection (PPS/PoD)] Prevent Unauthorized Microsoft 365 Allow-Relay

SUMMARY ⓘ

This article describes how to configure your PPS cluster and Microsoft 365 environment to prevent unauthorized Microsoft 365 allow-relay.

ARTICLE NUMBER

000022645

DESCRIPTION

Situation	You are configuring PPS to relay email for your Microsoft 365 environment, and you want to ensure that you prevent unauthorized allow-relay
Product / Version	Proofpoint Protection Server (PPS) version 8.x and newer

Summary	To prevent unauthorized allow-relay, you will create two Proofpoint policy routes that identify emails received from Office 365, then a Proofpoint firewall rule to block emails sent to external recipients that don't reference the M365 default tenant domains.
----------------	--

QUESTION

How do I configure my PPS environment to prevent unauthorized M365 allow-relay?

ANSWER

When a Proofpoint Protection Server is configured to relay email for Microsoft 365, another bad actor could configure their own M365 tenant to route email through the Proofpoint gateway. To prevent unauthorized allow-relay, you will create two Proofpoint policy routes that identify emails received from Office 365, then a Proofpoint firewall rule to block emails sent to external recipients that don't reference the M365 default tenant domains.

Adding rules to prevent allow-relay abuse needs to be carefully planned and executed. This configuration will first enable audit mode to identify messages that may be legitimate, such as forwarded messages or other status notification messages. Do not enable the final action of **Quarantine > Discard** in step 6 until reviewing the `m365_relaydeny` quarantine folder messages to identify legitimate emails.



Failing to complete this configuration correctly may cause emails received from the Microsoft 365 mail system to be quarantined and blocked. Ensure you complete step 5 before changing the final action to Quarantine > Discard in step 6.

Step 1 – Identify your Default M365 Tenant Domain

1. Log into your M365 Admin Center, then navigate to **Settings > Domains** or <https://portal.office.com/Adminportal/Home/#/Domains> (<https://portal.office.com/Adminportal/Home/#/Domains>)
2. Under your domain list, please notate the entry that indicates your "(Default)" tenant domain. The default domain could be your onmicrosoft.com (<http://onmicrosoft.com>) domain or one of your primary domains (e.g. tenant1.onmicrosoft.com (<http://tenant1.onmicrosoft.com>), primarydomain.com (<http://primarydomain.com>)).
3. Make a note of all your onmicrosoft fully qualified domain names (e.g. tenant1.onmicrosoft.com (<http://tenant1.onmicrosoft.com>), tenant2.onmicrosoft.com (<http://tenant2.onmicrosoft.com>), ...).
4. Identify other verified domains that are configured as a primary SMTP address for email-enabled objects. These domains may be needed when adding additional X-OriginatorOrg X-Header values to the firewall rule condition list.
5. Repeat these steps for all M365 tenants you plan on integrating with your Proofpoint Protection Server



Note: The default domain may not be used for the X-OriginatorOrg x-header value for all senders. During the audit phase, you will need to identify any other verified domains used by Microsoft 365 for your tenant.

Step 2 - Add your onmicrosoft.com (<http://onmicrosoft.com>) domain to your *Inbound Mail* domains list

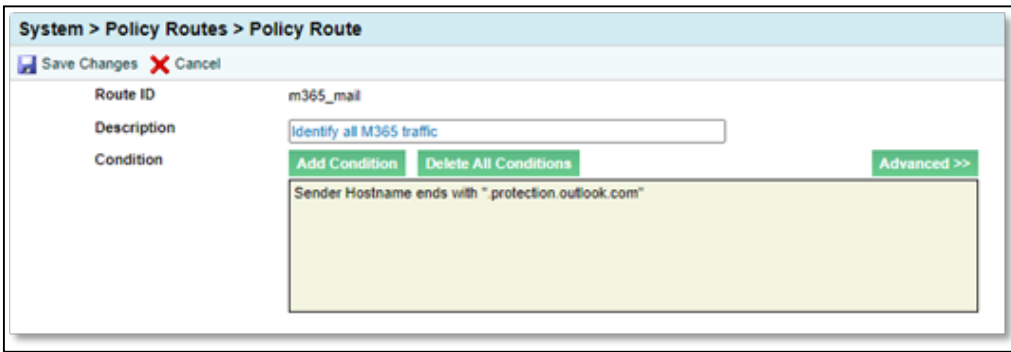
1. Log in to the Proofpoint Protection Server
2. Navigate to **System > System > Inbound Mail**
3. Click **Add**, then:
 - a. Under *Mail for Host / Domain*, enter your onmicrosoft.com (<http://onmicrosoft.com>) domain fully qualified domain name from Step 1.3 (above)
 - b. Under *Mailer*, select **ESMTP**
 - c. Under *Destination / Error Message*, enter the same value found in your list for your primary domain(s); this is typically tenant1-com.mail.protection.outlook.com (<http://tenant1-com.mail.protection.outlook.com>) or tenant1.mail.protection.outlook.com (<http://tenant1.mail.protection.outlook.com>) or tenant1.mail.eu.outlook.com (<http://tenant1.mail.eu.outlook.com>) (eg. this should ALWAYS match the destination for your primary domain)
 - d. Under *Lookup By*, select **A record only**
 - e. Under *Delivery Type*, select **Ordered**
 - f. Click **Save Changes** at the top
4. Repeat step 3 for each onmicrosoft.com (<http://onmicrosoft.com>) domain.



Note: If you have more than one M365 tenant sending email through your Proofpoint gateway, Step 2 above will need to be repeated for all tenants in your environment. There should be at least one onmicrosoft.com (<http://onmicrosoft.com>) domain per tenant; they will all need to be added to your *Inbound Mail* domains list.

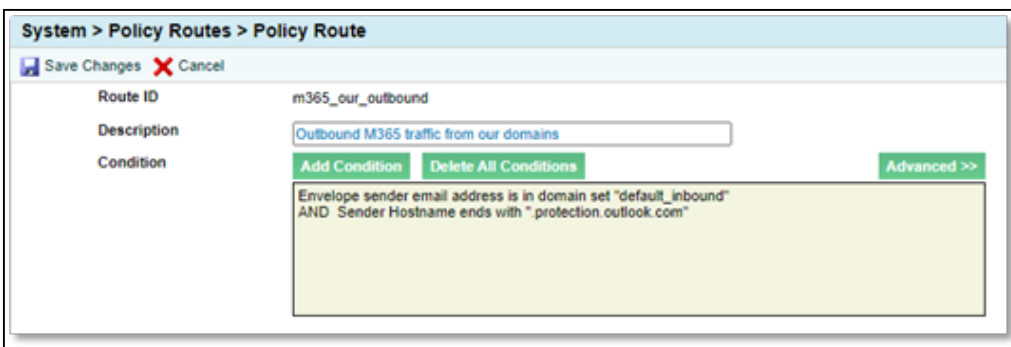
Step 3 – Create the `m365_mail` Policy Route

1. Log in to the Proofpoint Protection Server
2. Navigate to **System > System > Policy Routes**
3. Click **Add**, then:
 - a. For the *Route ID*, use `m365_mail`
 - b. For the *Description*, use **Identify all M365 traffic**
 - c. Click **Add Condition**, then select **Sender Hostname** as the condition, select the **Ends With** operator, then enter [.protection.outlook.com](http://protection.outlook.com) (<http://protection.outlook.com>) as the value
 - d. Click the **Add Condition** button, then click **Save Changes**



Step 4 – Create the m365_our_outbound Policy Route

1. Log in to the Proofpoint Protection Server
2. Navigate to **System > System > Policy Routes**
3. Click Add, then:
 - a. For the *Route ID*, use m365_our_outbound
 - b. For the *Description*, use **Outbound M365 traffic from our domains**
 - c. Click **Add Condition**, then select **Sender Hostname** as the condition, select the **Ends With** operator, then enter [.protection.outlook.com](http://protection.outlook.com) (<http://protection.outlook.com>) as the value
 - d. Click the **Add and New Condition** button
 - e. For the *Add condition as* value, select **And**
 - f. For the *Condition*, select **Envelope Sender**, then select **Is In Domain Set**, then select the default_inbound domain set
 - g. Click the **Add Condition** button, then click **Save Changes**



Step 5 – Create the m365_relaydeny Firewall Rule

1. Log in to the Proofpoint Protection Server
2. Navigate to **Email Protection > Email Firewall > Rules**
3. Click **Add Rule**, then:
 - a. For the *Rule ID*, use m365_relaydeny
 - b. For the *Description*, use **Only allow relay from my domain senders**
 - c. Under *Policy Routes*, select **Restrict processing to selected policy routes...**, then select m365_mail
 - d. Under *Policy Routes*, choose **Disable processing to selected policy routes...**, then select default_inbound and m365_our_outbound

- e. Click **Add Condition**, then select **Sender Hostname** as the condition, select the **Ends With** operator, then enter `.protection.outlook.com` (<http://protection.outlook.com>) as the value
- f. Click the **Add and New Condition** button
- g. For the **Add condition as** value, select **And**
- h. For the *Condition*, select **Message Headers**, then choose **User Defined**, then enter `x-ms-exchange-generated-message-source`
- i. For the *Operator*, choose **Does Not Equal**, then enter **mailbox rules agent** as the value, then click **Save**
- j. Click the **Add and New Condition** button.
- k. For the *Add condition as* value, select **And**
- l. For the *Condition*, select **Message Headers**, then choose **User Defined**, then enter `x-originatororg`
- m. For the *Operator*, choose **Does Not Equal**, enter your **default tenant domain** identified in Step 1, and click **Save**. If you identified other M365 tenant domains in step 1, repeat steps j through m.

Example conditions showing a single M365 tenant:

```
Sender Hostname ends with ".protection.outlook.com"
AND Message header "x-ms-exchange-generated-message-source" does not equal "mailbox rules agent"
AND Message header "x-originatororg" does not equal "tenant1.onmicrosoft.com"
```

Example conditions showing multiple M365 tenants:

```
Sender Hostname ends with ".protection.outlook.com"
AND Message header "x-ms-exchange-generated-message-source" does not equal "mailbox rules agent"
AND Message header "x-originatororg" does not equal "tenant1.onmicrosoft.com"
AND Message header "x-originatororg" does not equal "tenant2.onmicrosoft.com"
```

- n. Under **Dispositions > Quarantine Options**, select **Quarantine Message**, choose **New Folder...**, use `m365_relaydeny` as the folder name, and click **Add Entry** to add the quarantine folder
- o. Leave the *Delivery Method* set to **Continue** until you confirm the rule works as desired

p. Click **Add Rule** at the top to add the firewall rule

Rule Settings

Enable Off On

ID m365_relaydeny

Description

Conditions

Policy Routes

Restrict processing to selected policy routes...

Available:

Require Any Of:

Disable processing for selected policy routes...

Available:

Disable For Any Of:

Condition

Sender Hostname ends with ".protection.outlook.com"
AND Message header "x-ms-exchange-generated-message-source" does not contain "mailbox rules agent"
AND Message header "x-originatororg" does not equal "mytenant.onmicrosoft.com"

Dispositions


Quarantine Option Quarantine message...

Folder:

Delivery Method Continue Deliver Now Reject Retry Discard Re-route Secure

q. Upon completion of rule save, find the rule in your email firewall rules list. Click "Edit Rule" button to re-load the rule.

r. Verify all settings, Set the "Enable" radio selection to **On**, and click "Save Changes" at the top.

NOTE: In some cases, customers are still seeing some auto responses caught by this rule. Look in the quarantine folder at headers for example messages. In the quarantine folder, click on a message. In the message view (at the bottom of the page) mouse over the  "View:" button and change the view to "Headers". When the view loads, look for the "x-ms-exchange-generated-message-source" header. If anything follows that header field BESIDES a single instance of the string "mailbox rules agent", the rule condition operator will need to be changed from "Does Not Equal" to "Does Not Contain".

Step 6 - Review the Quarantine Folder for Valid Email

1. Log in to the Proofpoint Protection Server
2. Navigate to **System > Quarantine > Folders**
3. Locate the m365_relaydeny quarantine folder, then review each message to determine if it appears to be a valid email. If you see more than a few messages in this folder, check the configuration in steps 1 through 4.
4. Over the next several days, repeat the actions in this step to identify any valid email. Do not proceed to step 6 unless the quarantine folder is empty or all quarantined emails are unauthorized relay attempts.



Note: Please contact Proofpoint Support or your assigned Proofpoint Professional Services consultant for guidance if valid emails are quarantined in the `m365_relaydeny` folder to assist with exclusions.

Step 7 - Modify the `m365_relaydeny` to Quarantine and Discard

This step modifies the existing audit rule and changes the final action from *Quarantine and Continue* to *Quarantine and Discard*.

1. Log in to the Proofpoint Protection Server
2. Navigate to **Email Protection > Email Firewall > Rules**
3. Edit the `m365_relaydeny` firewall rule, then update the *Description* to **Block Unauthorized Outbound Email Received from outbound.protection.outlook.com**
(<http://outbound.protection.outlook.com>)
4. Confirm the firewall rule still has the **Quarantine message... > Folder: `m365_relaydeny`** selected
5. Change the *Delivery Method* action from **Continue** to **Discard**
6. Click the **Save Changes** button to save the firewall rule



Plan to monitor the messages in the `m365_relaydeny` folder for several days to confirm that no valid email was quarantined after setting this rule to Discard.

Step 8 - Add Envelope Spoofing Protection

Proofpoint has observed bad actors leveraging the above abuse methodology while also spoofing customers' envelope sending domains. The above ruleset alone will not protect against advance domain spoofing originating within M365. To further protect yourself from M365 envelope spoofing attacks, please follow these guidelines:

<https://proofpoint.my.site.com/community/s/article/Email-Protection-PPS-PoD-Prevent-Unauthorized-Microsoft-365-Allow-Relay-Envelope-Spoofing-Protection>
(<https://proofpoint.my.site.com/community/s/article/Email-Protection-PPS-PoD-Prevent-Unauthorized-Microsoft-365-Allow-Relay-Envelope-Spoofing-Protection>)

Additional Notes

- **Federal customers** leveraging Proofpoint and Microsoft secure services should reach out to Support (or your TAM) for additional guidance.
- Customer **hybrid environments w/centralized transport** should verify mail routing from M365-- if ANY mail is being routed directly from M365 to their Proofpoint instance, these steps need to be followed. If not, the "Allow Relay from Microsoft Office 365 IP Addresses" should be disabled.
-

INTERNAL NOTES

This information is directly pulled from the [\[Email Protection \(PPS/PoD\)\] Best Practices - Microsoft 365 Inbound and Outbound Mail Integration \(/community/s/article/Best-Practices-Office-365-Inbound-and-Outbound-Mail-Integration\)](#).

VISIBLE IN INTERNAL APP

VISIBLE TO CUSTOMER

VISIBLE TO PARTNER

VISIBLE IN PUBLIC KNOWLEDGE BASE

URL NAME


Email-Protection-PPS-PoD-Prevent-Unauthorized-Microsoft-365-Allow-Relay

CHAT ANSWER

<https://proofpoint.my.site.com/community/s/article/Email-Protection-PPS-PoD-Prevent-Unauthorized-Microsoft-365-Allow-Relay>
(<https://proofpoint.my.site.com/community/s/article/Email-Protection-PPS-PoD-Prevent-Unauthorized-Microsoft-365-Allow-Relay>).

INTERNAL URL

<https://proofpoint.lightning.force.com/lightning/articles/Knowledge/Email-Protection-PPS-PoD-Prevent-Unauthorized-Microsoft-365-Allow-Relay>
([/lightning/articles/Knowledge/Email-Protection-PPS-PoD-Prevent-Unauthorized-Microsoft-365-Allow-Relay](https://proofpoint.lightning.force.com/lightning/articles/Knowledge/Email-Protection-PPS-PoD-Prevent-Unauthorized-Microsoft-365-Allow-Relay)).

 [Files \(0\). \(/community/s/relatedlist/ka0Uy0000002353IAA/AttachedContentDocuments\)](#)

COMMENT ON THIS ARTICLE

Sort by:

Most Recent Activity ▼

🔍 Search this feed...

▼ ▼

↻



Peter Swisher (/community/s/profile/005390000067uYzAAI) published a new version of this Knowledge.



16h ago (/community/s/feed/0D5Uy00000L4I5SKAR)

3 comments 26 views



More comments

1 of 3



Ewen Fung (/community/s/profile/0055Y00000HEcMnQAL) (Customer)

10 hours ago

I have finished step 6 and there were few auto-reply messages being quarantined just like what was described in the note of step 5.

When I check the the value of the header "x-ms-exchange-generated-message-source" from the quarantined messages, the values were all "Mailbox Rules Agent" and that is. Is there anything I have missed? Does value has to be case-sensitive?

[Expand Post](#)

Like



Write a comment...



Peter Swisher (/community/s/profile/005390000067uYzAAI) published a new version of this Knowledge.

[May 4, 2024 at 12:49 AM \(/community/s/feed/0D5Uy00000Fd3cwKAB\)](#)

11 comments 90 views



Like



Comment

More comments

1 of 11



Edwin Sanchez (/community/s/profile/0055Y00000lgaliQAB) (Customer)

11 hours ago

Sorry to ask, but is this suppose to be a better or more secure method that following the approach to use Unique IDs for outbound messages from the Methods to Prevent Unauthorized Microsoft 365 Allow-Relay - Proofpoint Microsoft 365 Integration Guide?

Like



Write a comment...



Peter Swisher (/community/s/profile/005390000067uYzAAI) published a new version of this Knowledge.

[May 6, 2024 at 9:21 PM \(/community/s/feed/0D5Uy00000Fq5OCKAZ\)](#)

5 comments 86 views



Like



Comment

More comments

1 of 5



Peter Swisher (/community/s/profile/005390000067uYzAAI)

17 hours ago

@Stephanie-- hybrid environments depend... a KB update is forthcoming to address this in more detail.

@Erik-- correct, the KB update will include this as well.

Like



Write a comment...



Peter Swisher (/community/s/profile/005390000067uYzAAI) published a new version of this Knowledge. ▼

April 1, 2024 at 11:12 PM (/community/s/feed/0D5Uy00000C3MgPKAV)

8 comments 64 views



Like



Comment

David Prado (/community/s/profile/0055Y00000HEpGeQAL) and Chris Tackett (/community/s/profile/00539000006XIREAA4) like this.

More comments

1 of 8



Eddie Rowe (/community/s/profile/00539000005WUyoAAG) (Customer)

14 hours ago

I am curious why the Condition includes a check for Sender Hostname ends with [.protection.outlook.com \(https://protection.outlook.com\)](https://protection.outlook.com). Since the rule is written to ONLY apply to the m365_mail policy route, which uses this exact same condition, why is it necessary to have this logic as well in the Condition?

Like



Write a comment...



Kelly Muthler (/community/s/profile/00539000006EHqsAAG) published this new Knowledge. ▼

March 21, 2024 at 3:08 PM (/community/s/feed/0D5Uy00000AsJFUKA3)

11 comments 58 views



Like



Comment

David Prado (/community/s/profile/0055Y00000HEpGeQAL) likes this.

More comments

1 of 11



Eric Watkins (/community/s/profile/0051O000009OEqUQAW) (Customer)

14 hours ago

I echo Leo and Eddies opinion that the multi tenant issue looks like it would need nesting OR clauses instead of an an AND. Otherwise the rule would never trigger imho since that x-originatororg header would never have multiple domains in it to match the condition with the AND's.

Like



Write a comment...



Kelly Muthler (/community/s/profile/00539000006EHqsAAG) published a new version of this Knowledge.



April 1, 2024 at 6:08 PM (/community/s/feed/0D5Uy00000Bzx6dKAB).

6 comments 68 views



Like



Comment

David Prado (/community/s/profile/0055Y00000HEpGeQAL) likes this.

More comments

1 of 6



Peter Swisher (/community/s/profile/005390000067uYzAAI)

16 hours ago

@Erik-- thank you, this has been clarified in a forthcoming KB update.

Like



Write a comment...

RELATED ARTICLES

[Email Protection (PPS/PoD)] Changes to Email Feedback Plug-in Not Working (/community/s/article/Email-Protection-Changes-to-Email-Feedback-Plug-in-Not-Working)

211

[Archiving and Supervision] Wildcards within proximity search are unsupported (/community/s/article/Archiving-and-Supervision-Wildcards-within-proximity-search-are-unsupported)

153

[Archiving and Supervision] Using Wildcards for Content Searches in the Archive (/community/s/article/Using-Wildcards-for-Content-Searches-in-the-Archive)

1.9K

[Email Protection (PPS/PoD)] Best Practices - Microsoft 365 Inbound and Outbound Mail Integration (/community/s/article/Best-Practices-Office-365-Inbound-and-Outbound-Mail-Integration)

120.18K

[Email Protection (PPS/PoD)] Administrator's Guide For PoD (Cloud) Deployments (/community/s/article/Proofpoint-for-Outlook-Administrator-s-Guide-For-POD-Cloud-Deployments)

9.17K

About

[Overview](https://www.proofpoint.com/us/company/about) (<https://www.proofpoint.com/us/company/about>)
[Why Proofpoint](https://www.proofpoint.com/us/why-proofpoint) (<https://www.proofpoint.com/us/why-proofpoint>)
[Careers](https://www.proofpoint.com/us/company/careers) (<https://www.proofpoint.com/us/company/careers>)
[Leadership Team](https://www.proofpoint.com/us/our-leadership-team) (<https://www.proofpoint.com/us/our-leadership-team>)
[News Center](https://www.proofpoint.com/us/news) (<https://www.proofpoint.com/us/news>)
[Nexus Platform](https://www.proofpoint.com/us/why-proofpoint/nexus-threat-graph) (<https://www.proofpoint.com/us/why-proofpoint/nexus-threat-graph>)
[Privacy and Trust](#)

Threat Center

[Threat Hub](https://www.proofpoint.com/us/cyber-threat-hub) (<https://www.proofpoint.com/us/cyber-threat-hub>)
[Cybersecurity Awareness Hub](https://www.proofpoint.com/us/cybersecurity-awareness-hub) (<https://www.proofpoint.com/us/cybersecurity-awareness-hub>)
[Ransomware Hub](https://www.proofpoint.com/us/ransomware-hub) (<https://www.proofpoint.com/us/ransomware-hub>)
[Threat Glossary](https://www.proofpoint.com/us/threat-reference) (<https://www.proofpoint.com/us/threat-reference>)
[Threat Blog](https://www.proofpoint.com/us/threat-insight) (<https://www.proofpoint.com/us/threat-insight>)
[Daily Ruleset](https://www.proofpoint.com/us/daily-ruleset-update-summary) (<https://www.proofpoint.com/us/daily-ruleset-update-summary>)

Products

[Email Security & Protection](https://www.proofpoint.com/us/product-family/email-protection) (<https://www.proofpoint.com/us/product-family/email-protection>)
[Advanced Threat Protection](https://www.proofpoint.com/us/product-family/advanced-threat-protection) (<https://www.proofpoint.com/us/product-family/advanced-threat-protection>)
[Security Awareness](https://www.proofpoint.com/us/product-family/security-awareness-training) (<https://www.proofpoint.com/us/product-family/security-awareness-training>)
[Cloud App Protection](https://www.proofpoint.com/us/solutions/protect-cloud-apps) (<https://www.proofpoint.com/us/solutions/protect-cloud-apps>)
[Compliance & Data Archiving](https://www.proofpoint.com/us/products/compliance-and-archiving) (<https://www.proofpoint.com/us/products/compliance-and-archiving>)
[Defend Data](https://www.proofpoint.com/us/products/defend-data) (<https://www.proofpoint.com/us/products/defend-data>)
[Digital Risk Protection](https://www.proofpoint.com/us/product-family/digital-risk-protection) (<https://www.proofpoint.com/us/product-family/digital-risk-protection>)
[Product Packages](https://www.proofpoint.com/us/products/packages) (<https://www.proofpoint.com/us/products/packages>)

Resources

[Whitepapers](https://www.proofpoint.com/us/resources/white-paper) (<https://www.proofpoint.com/us/resources/white-paper>)
[Webinars](https://www.proofpoint.com/us/resources/webinar) (<https://www.proofpoint.com/us/resources/webinar>)
[Datasheets](https://www.proofpoint.com/us/resources/data-sheet) (<https://www.proofpoint.com/us/resources/data-sheet>)
[Events](https://www.proofpoint.com/us/company/events) (<https://www.proofpoint.com/us/company/events>)
[Customer Stories](https://www.proofpoint.com/us/customer-stories) (<https://www.proofpoint.com/us/customer-stories>)
[Blog](https://www.proofpoint.com/us/blog) (<https://www.proofpoint.com/us/blog>)
[Free Trial](https://www.proofpoint.com/us/free-trial-request) (<https://www.proofpoint.com/us/free-trial-request>)

Connect

+1-408-517-4710 (tel:+1-408-517-4710)
[Contact Us](https://www.proofpoint.com/us/contact) (<https://www.proofpoint.com/us/contact>)
[Office Locations](https://www.proofpoint.com/us/contact/office-locations) (<https://www.proofpoint.com/us/contact/office-locations>)
[Request A Demo](https://www.proofpoint.com/us/free-demo-request) (<https://www.proofpoint.com/us/free-demo-request>)

Support

[Support Login](https://proofpointcommunities.force.com/community/s/) (<https://proofpointcommunities.force.com/community/s/>)
[Support Services](https://www.proofpoint.com/us/support-services) (<https://www.proofpoint.com/us/support-services>)
[IP Address Blocked?](https://ipcheck.proofpoint.com) (<https://ipcheck.proofpoint.com>)



<https://www.proofpoint.com/us>



<http://www.facebook.com/proofpoint>



<http://www.twitter.com/proofpoint>



<https://www.linkedin.com/company/proofpoint>



<https://www.youtube.com/channel/UCIvtJgsrUzFo90NKeiVozhQ> [Sitemap](#)

[\(/community/s/topiccatalog\)](#) © 2023. All rights reserved. [Terms and](#)

[conditions \(https://www.proofpoint.com/us/license\)](https://www.proofpoint.com/us/license) [Privacy Policy](#)

<https://www.proofpoint.com/us/privacy-policy>