Certification Troubleshooting

January 26th, 2024

Certification Troubleshooting

- Suspension vs. Chronic Suspension
- Troubleshooting Certification Suspensions
  - Performance Issue Suspensions
    - Troubleshooting Spam Complaints
    - Troubleshooting Microsoft Sender Reputation Data (SRD)
    - Troubleshooting Blocklistings
  - Security Suspensions
  - Infrastructure & Policy Suspensions
- Q&A

validity

Certification Suspension Troubleshooting Challenges

There is no one-size-fits-all solution when troubleshooting a Certification IP suspension…

…because no two email programs are the same.

validity

Suspension vs. Chronic Issues

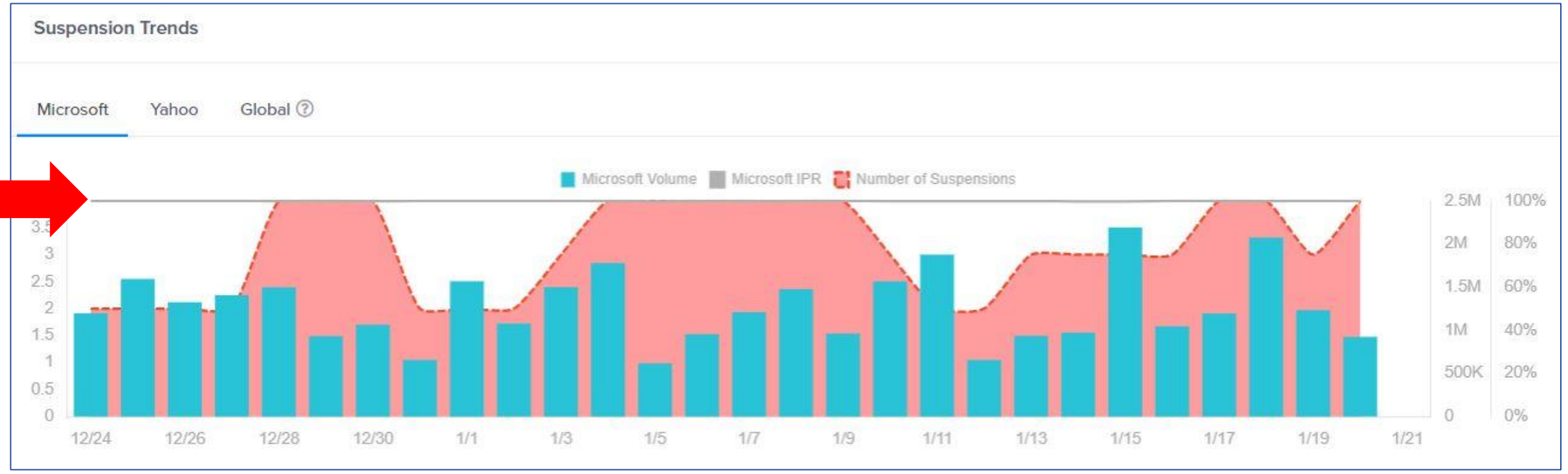
Suspension vs. Chronic Suspension

Suspension

- ✓ Occasional or one-off IP suspension(s).
- ✓ Occurring rarely.
- ✓ Does not necessarily represent a broader issue with the email program.
- ✓ Addressed w/ client via AM, COE, CSM

Chronic Suspension

- ✓ Repeated or frequent IP suspension(s)
- ✓ Ongoing.
- ✓ Represents a consistent issue with the email program
- ✓ For AMs and COE: should be escalated for PS engagement
  - When in doubt – reach out to PS!



validity

Reaching out to Professional Services

Email:
ProfessionalServices@validity.com

Slack:
#proserve-help

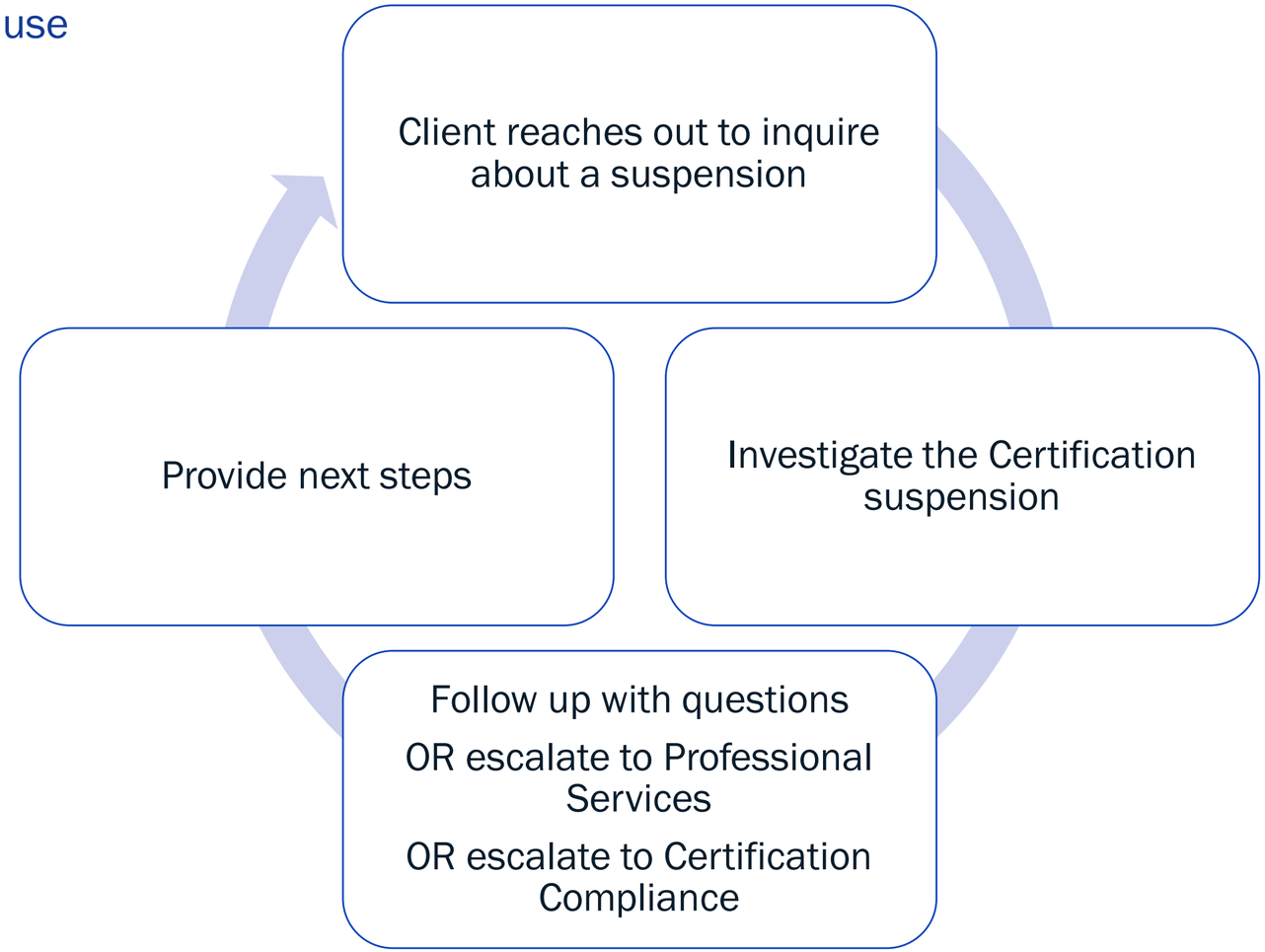
validity

Troubleshooting Certification Suspensions

Troubleshooting Certification Suspensions

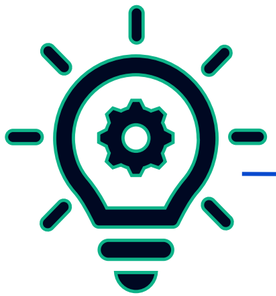
When an IP address has been suspended in Certification, use the **W4H thought process:**

- **Why**: *Why has the IP been suspended?*
- **When**: *When was the IP suspended?*
- **What**: *What sending practice triggered the issue?*
- **How to Get Re-Enabled**: *How to correct the issue?*



When in doubt, follow the path to the inbox when thinking about how to investigate performance issues.

The Path to the Inbox



Content
Text
Images
Text-Image Ratio
Spam Words
Responsive Design
Spam Laws

List
Signup Permission
Welcome
Data Sources
Unknown Users
Spam Traps
Segmenting
Hygiene

Infrastructure
MTA
IP Address
DNS

Delivery Plan
Cadence
Frequency
Volume

SENT

Reputation
IP History
Allow list
Blocklist
Shared IP

Security
Spoofing
Phishing

Authentication
SPF
DKIM
DMARC

Spammers

Gmail Microsoft yahoo!

Blocking & Missing
ISP Firewalls
Unknown User Rate
Spam

Bouncing
Unknown Address
Undeliverable
Mailbox Full
Auto-Reply

DELIVERED

Filtering
Classification
Automatic
Personal
Graymail

INBOX

Competition
Similar Offers
Social Updates
Changing Interests

SPAM

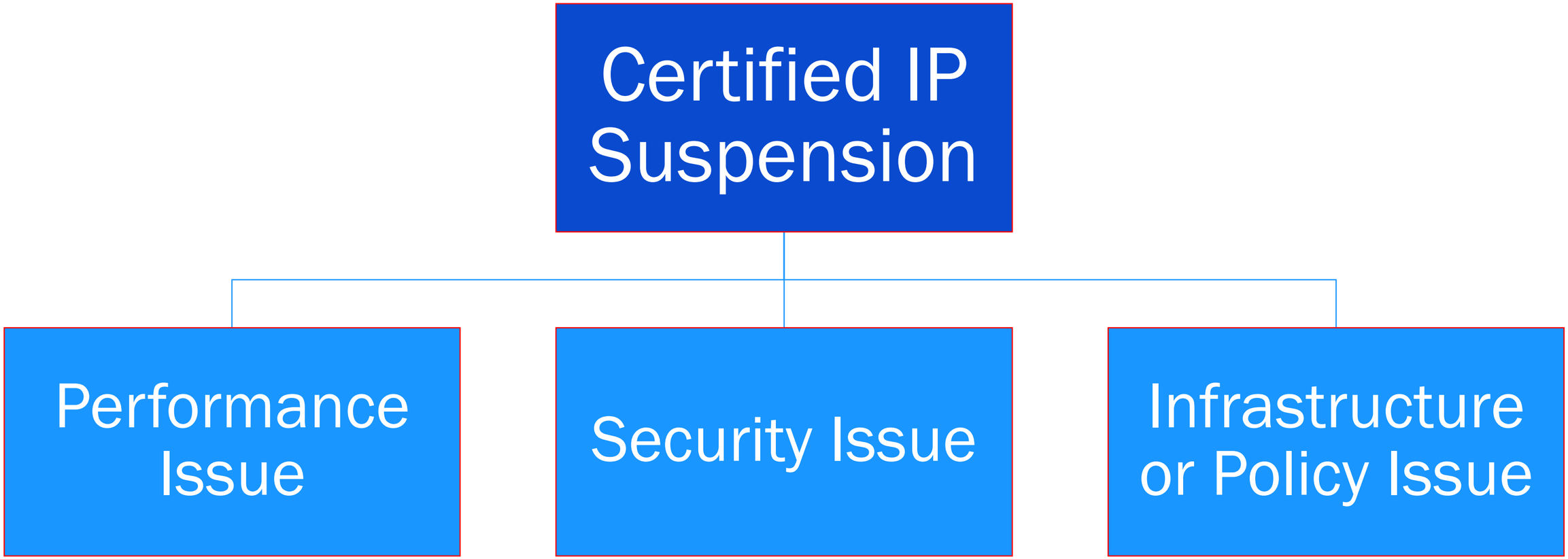
Subscribers

(+) Engagement
Reads
Opens
Clicks
Shares
Gmail Tabs

Rendering
Images On
HTML Errors
Email Clients
Mobile Devices

(-) Engagement
Ignore/Delete
Unsubscribes
Complaints
SRD Rate
Feedback Loops

Reasons for Certification Suspension



validity

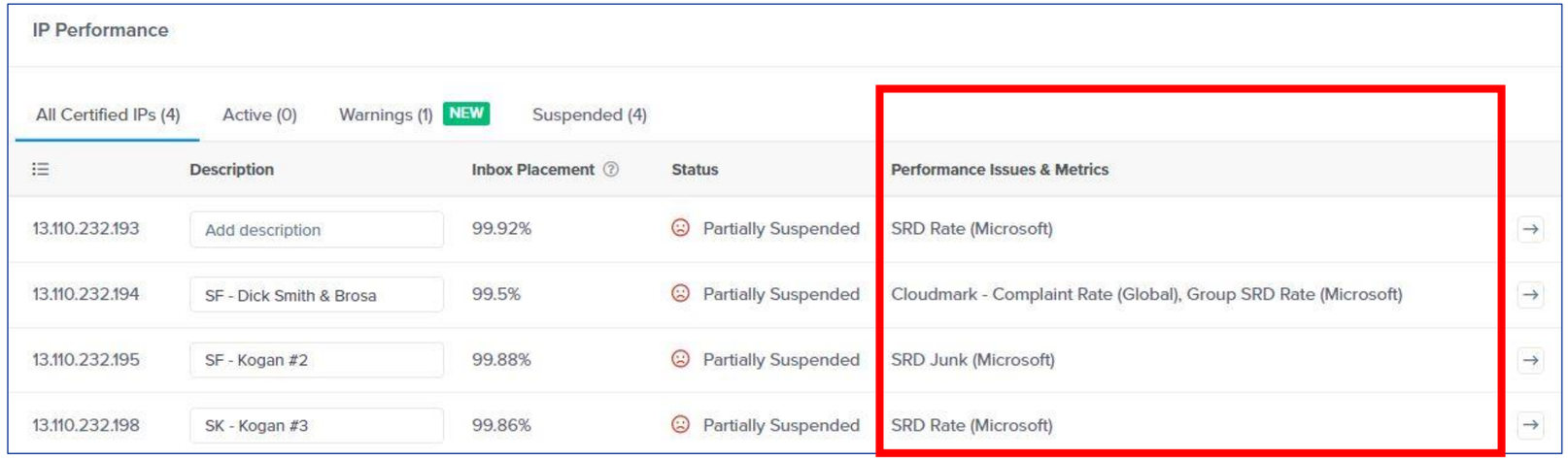
IP Suspension: Performance Issues

Performance Issue Suspensions

IPs can be suspended from Certification for a number of performance-related issues, including:

- Exceeding spam complaint rate thresholds
- Exceeding Microsoft Sender Reputation Data (SRD) Junk Thresholds
- Hitting spam traps
- Blocklistings
- Failing to meet minimum volume thresholds

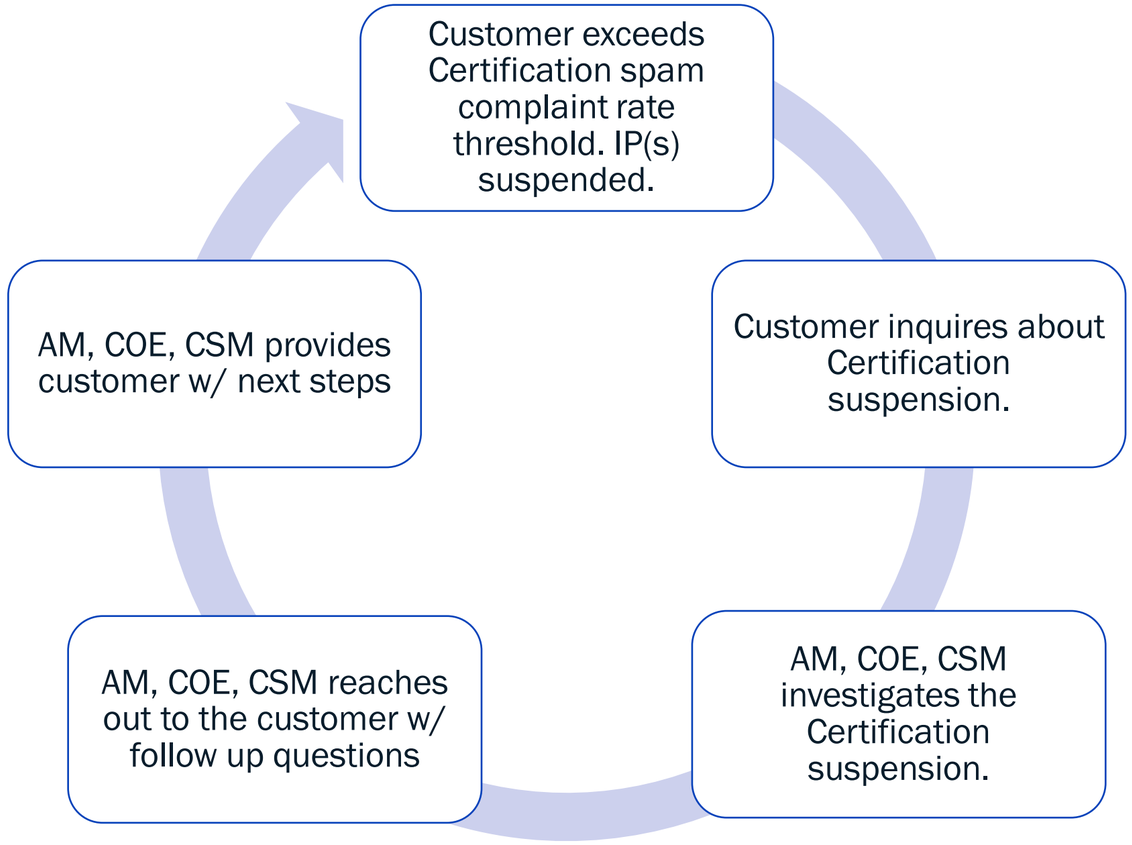
Performance issues can be identified in Everest > Certification:



Suspension Scenario #1: Spam Complaint Threshold Exceeded

Spam complaint spikes or increases can occur for a variety of reasons. The main goals in responding to client spam complaint suspensions should be:

1. Clearly communicating the date of the spam complaint spike and impacted mailbox provider.
2. Providing details on when the current spam complaint rate and spam complaint threshold for the impact mailbox provider.
3. Indicating which campaigns may have generated spam complaints
4. Asks questions that encourage the customer to investigate the root cause of the suspension.
5. Provide guidance on reducing spam complaint rates in the future.



Spam Complaint Spike Troubleshooting

Ask the right questions!

- Did you stop using opt-in permission methods with subscribers?
- Did you recently use a high-risk list acquisition method such as list purchase, list harvesting or co-registration?
- Did you change your list hygiene strategy?
- Did you accidentally send email to a suppression list?
- Did you send a new email stream to subscribers without their consent?
- Did you suddenly increase the sending frequency of email to your subscribers during a major holiday?
- Did you update your branding (which changed the look and feel of your content) without notifying subscribers?
- Was there a breakdown in the complaint-handling process?
- Was an ad-hoc email sent to the entire list file?
- Did your sending volume drop significantly in a short period of time relative to your average sending volume (aka complaint hangover)?

Performance Issue Troubleshooting

Performance Issue	Thought Process	Client Investigation
Spam Complaint Threshold Exceeded	Was there a recent change to the email program?	An unexpected increase in sending frequency, new list acquisition sources, and sending to a suppression file are the most common reasons for sharp increases in complaint rates and increases over time.
	Are spam complaints coming from a specific subscriber segment?	Examine the segment to determine what sets it apart from the others. For example, if you recently added a new group of subscribers to your list and that group has a higher complaint rate than the rest of the list, examine how that list was acquired and whether the mailing you sent met the expectations that were presented at the point of collection.
	Has sending volume been consistent?	For example, senders typically send a significantly higher volume of mail in December to encourage customers to purchase gifts, then taper off after December 25th. It is common to see a spike in complaints the first business day in January when subscribers check their work email and complain about the emails they received. Complaint rates are calculated by dividing the number of complaints received by the number of emails delivered within a given time frame. The date the campaign was sent is not factored into the rate.
	Are complaints associated with a specific brand, mail stream, etc.?	Organizations can sometimes associate a sharp increase in complaints to a specific brand, IP address, sending domain or email stream. Work with them to ensure email best practices are being followed. Complaints occur when the email sent to subscribers does not meet their expectations. A preference center is a good way to help reduce complaints since it allows subscribers to choose the content and frequency of email they want to receive.

validity

Everest

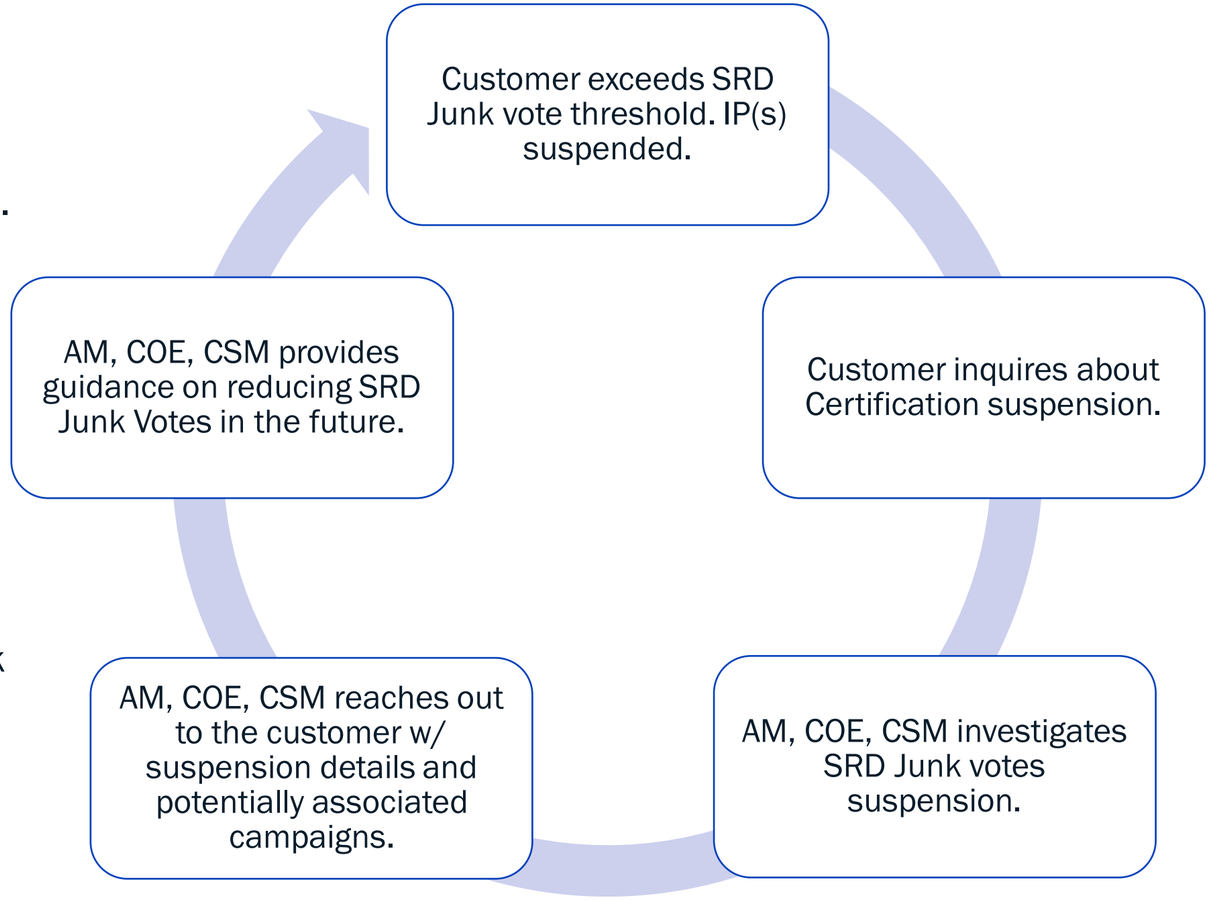
Suspension Scenario #2: Microsoft SRD Junk Rate Exceeded

SRD Junk Vote suspensions may be a one-off occurrence. SRD Junk Votes indicate subscriber dissatisfaction with the emails they received.

The main goals in responding to client SRD suspensions should be:

1. Clearly communicating what SRD Junk Votes are.
2. Providing details on when the SRD Junk Votes were cast.
3. Providing Certification SRD Junk rate thresholds.
4. Shedding light on which campaigns may have resulted in SRD Junk votes.
5. Explaining what root causes for SRD Junk votes and providing recommendations.

Senders who encounter frequent or recurring SRD Junk vote suspensions should be escalated to the Professional Services team.



SRD Junk Vote Thresholds

Validity Certification **Individual IP Microsoft SRD compliance thresholds**			
SRD Volume	0-4	5-10	11 or more
SRD Rate Threshold	Not enforced	5 Junk Votes	45%

Validity Certification **Microsoft Group SRD compliance thresholds**				
SRD Volume	0-9	10-30	31-50	51 or more
SRD Rate Threshold	Not enforced	75%	65%	55%

SRD Junk Vote Troubleshooting

Ask the right questions!

- Did you experiment with or change your Friendly-From name? A leading reason why SRD voters mark an email as junk is when they don’t recognize you as the sender.
- Did your sending frequency increase or change? How frequently are you contacting subscribers?
- Do you offer a subscriber email preference center?
- Do you process unsubscribe requests quickly? Requests should be honored immediately.
- Are you sending duplicate emails?
- Did you increase your sending volume recently?
- Has your branding changed recently? Is your branding consistent?
- Do you set expectations for email frequency and content type at point of signup?
- Are you acquiring subscribers organically and requiring express consent?
- Was an ad-hoc email sent to the entire list file?

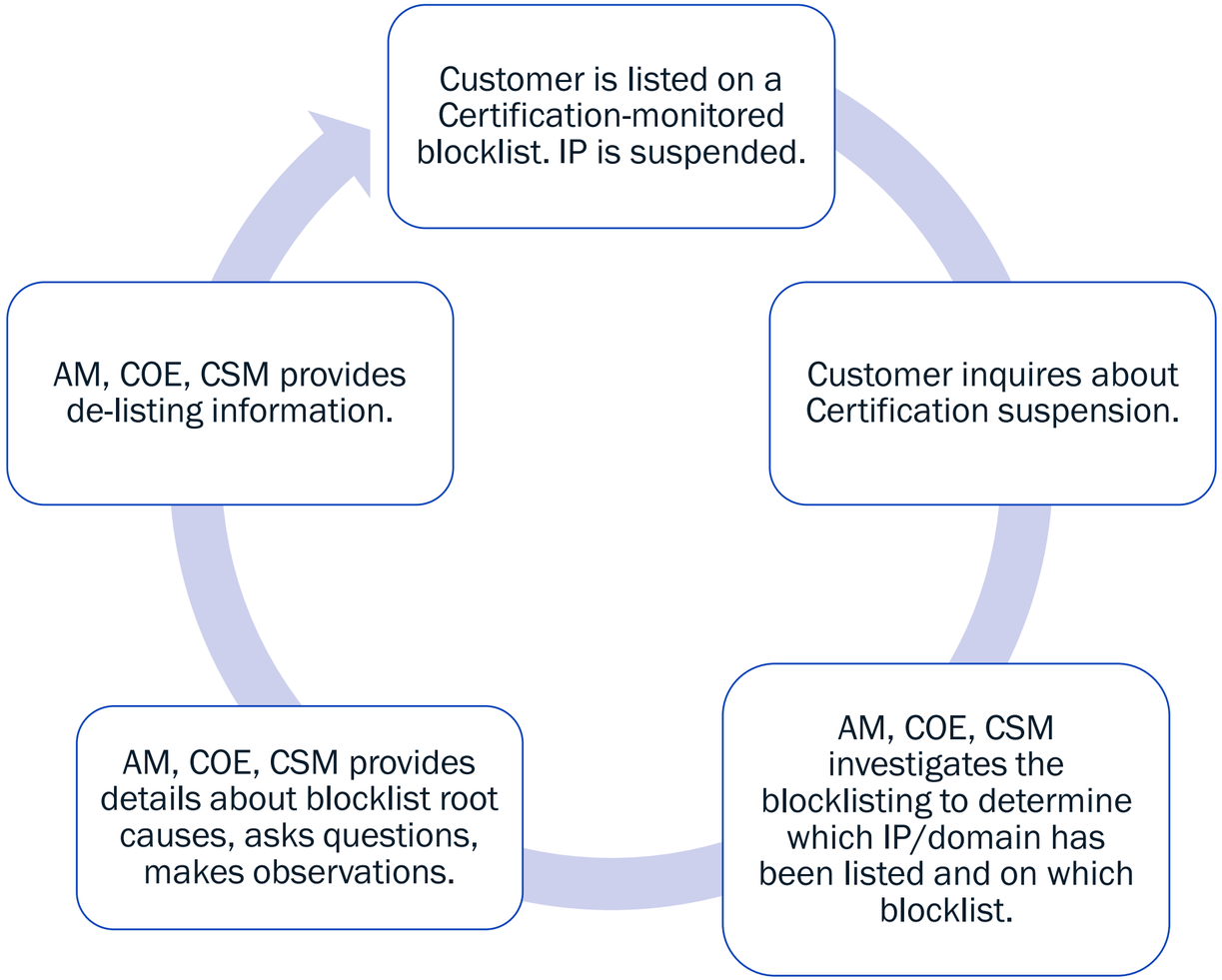
validity

Everest

Suspension Scenario #3: Blocklisting

Blocklistings may be a one-off occurrence. IPs may achieve Certified status once the blocklisting has been addressed and the IP/domain has been de-listed. The main goals in responding to client SRD suspensions should be:

1. Clearly communicating which IP/domain has been blocklisted, and the date of listing.
2. Providing information about the blocklist and root causes for listing.
3. Asking questions to prompt customer investigation. Reviewing Reputation data for recent changes.
4. Share de-listing information.



Note: Blocklistings may overlap with Security suspensions.

When in doubt, reach out to the Certification team!

Blocklist Troubleshooting

Ask the right questions!

- Have you purchased or rented email lists?
- Are you working with new partners or affiliates to acquire subscribers?
- Do you use a Confirmed Opt-in (COI) acquisition strategy?
- Have you started sending to riskier subscriber segments?
- Has your sending infrastructure recently changed? Have you worked with your IT team to ensure there are no open relays?
- Have you observed an increase in spam trap hits?
- Have you observed an increase in spam complaints?
- Are you validating subscribers at point-of-signup or before receiving campaigns? If so, are you suppressing risky and/or unknown addresses?
- Did you accidentally send to a suppression file?

validity

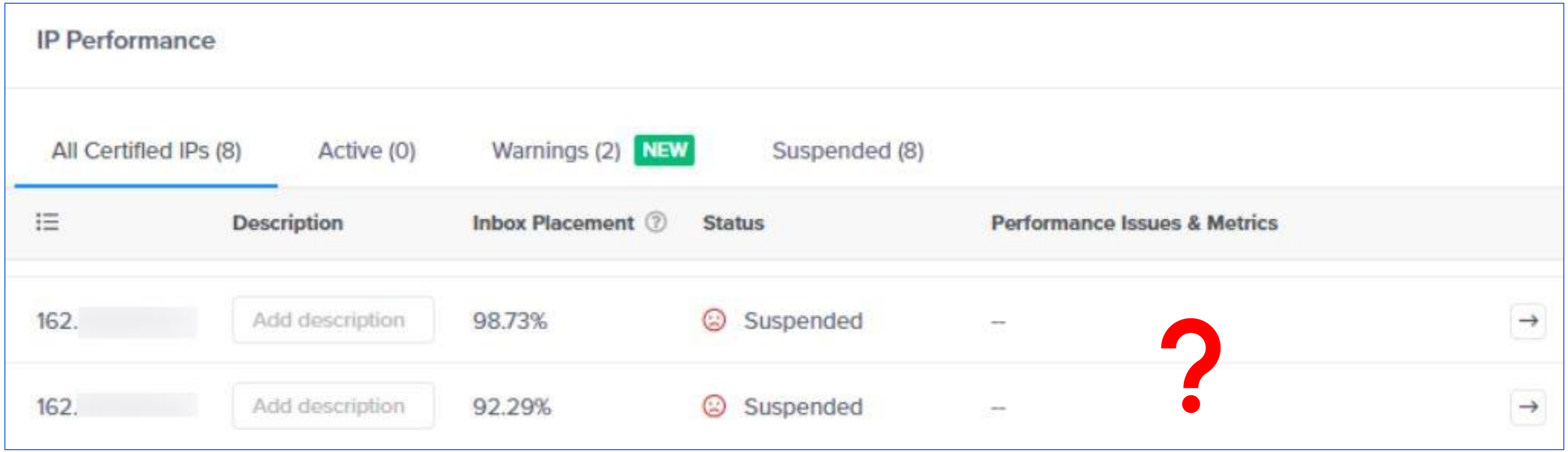
IP Suspension: Security

Security Suspensions

IPs can be suspended from Certification due to security issues. A security suspension results when email activity across a Certified IP address appears suspicious.

To detect potential security compromises, we:

- Look for email traffic from sending domains not owned or related to your business during an investigation by the Certification Compliance Team
- Monitor performance metrics such as sending volume, complaints, and spam trap hits to spot abnormal patterns of behavior
- Examine real-time alerts from third-party spam and security sources, such as Spamhaus, the Spam Uniform Resource Identifier Real-time Block List (SURBL), and SpamAssassin



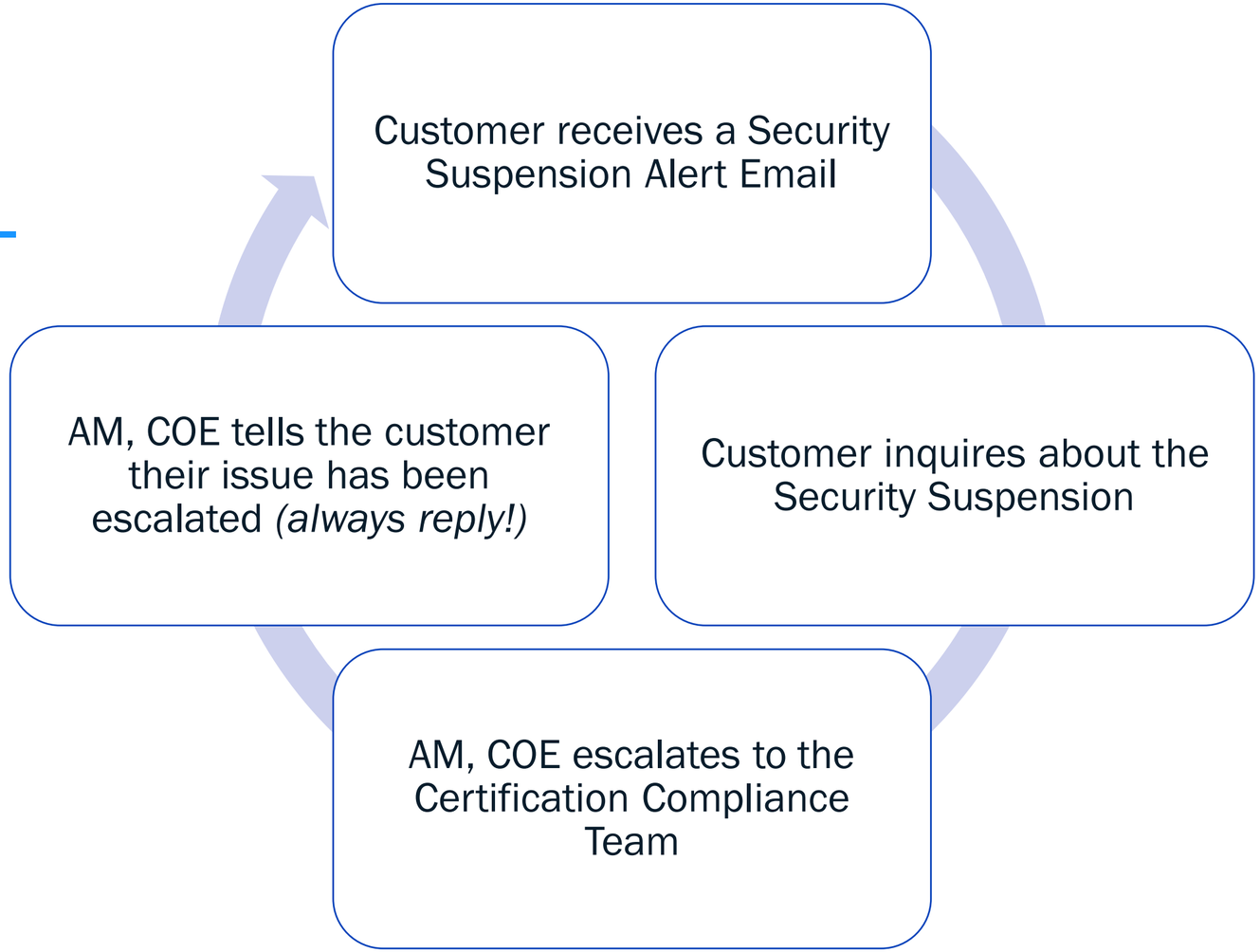
- When a Certified IP address receives a security suspension, it temporarily loses Certification benefits until the security event is cleared and compliance thresholds are met.
- As a precaution, Certified IP addresses showing abnormal activity are immediately suspended and then reviewed and verified by a Certification analyst within one hour of detection.

Clients are **notified** of security suspensions **via email alerts** and are not clearly marked in Everest > Certification

Suspension Scenario: Security Suspension

Security Suspensions should be always addressed by the Certification Compliance Team!

certification@validity.com



validity

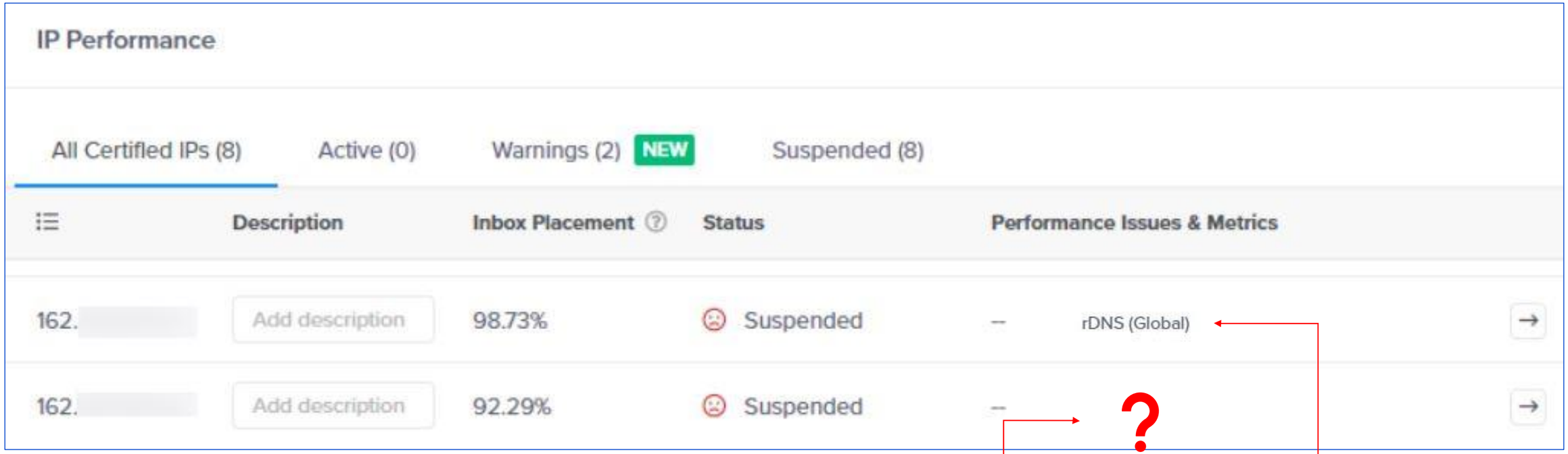
IP Suspension: Infrastructure & Policy

Infrastructure and Policy Suspensions

IPs can be suspended from Certification due to infrastructure and/or policy issues. A policy suspension results when email activity across a Certified IP fails to comply with one or more Sender Certification requirements.

To detect potential infrastructure and/or policy compromises, we:

- Regularly audit email traffic sent on Certified IPs to ensure it complies with Certification requirements
- Launch investigations (Certification Compliance Team)
- Monitor sending infrastructure of Certified IPs for changes



- When a Certified IP address receives a policy or infrastructure suspension, it temporarily loses Certification benefits until the security event is cleared and compliance thresholds are met.
- The process for resolving a Certified IP security or policy suspension varies based on the type of suspension. Resolving these suspensions almost always requires the assistance of the Certification Compliance Team.

Clients are **notified** of policy suspensions **via email alerts** and are not clearly marked in Everest > Certification

Clients are **notified** of infrastructure suspensions **via email alerts.** These are clearly marked in Everest > Certification

Suspension Scenario: Infrastructure & Policy Suspensions

Infrastructure and Policy Suspensions should be always addressed by the Certification Compliance Team!

certification@validity.com

Customer receives an Infrastructure or Policy Suspension Alert Email

Customer inquires about the Infrastructure or Policy Suspension

AM, COE, CSM escalates to the Certification Compliance Team

AM, COE tells the customer their issue has been escalated *(always reply!)*

Certification Requirements PDF

Being updated by Tyler re: Google & Yahoo Requirements 2024. Training to come!

validity

Q&A