DMARC Troubleshooting

March 8th, 2024

DMARC Troubleshooting

- DNS and TXT Records
- DMARC
- SPF, DKIM and Alignment
- DMARC Reports
- Troubleshooting DMARC with Everest
- Q&A

validity

DNS and TXT Records

DNS - Domain Name System

https://youtu.be/UVR9IhUGAyU?si=_V5A-JQVQagSXnVB

Domains and Name Servers

- Domains are managed at the Registrar
  - validity.com uses Network Solutions
- Domain owner is required to provide 2 Name Servers
  - Name Servers are hostnames that point to IPs
- Name Servers are computers running a DNS server
  - Server is a term to describe a hardware or software that provides data for clients (those that make the requests)
- BIND, PowerDNS, Unbound are DNS server softwares
- Google Cloud DNS, Azure DNS, AWS Route 53, CloudDNS, GoDaddy Premium DNS are DNS as a service (web interface)

whois:validity.com Find Problems

Name	Value
Registrar	Network Solutions, LLC
Registrant Name	PERFECT PRIVACY, LLC
Registrant Phone	+1.5707088622
Registrant Email	zq9hh67e7cc@networksolutionsprivateregistration.com
Name Server	NS-181.AWSDNS-22.COM
Name Server	NS-582.AWSDNS-08.NET
Name Server	NS-1611.AWSDNS-09.CO.UK
Name Server	NS-1403.AWSDNS-47.ORG

Name Servers and DNS Records

- DNS Records are basically a text file that follow a specified format.
- Each Name Server will have a copy of the domain's DNS Record.
- DNS Records have a Record Type (A) and a value (B).
  - Each type has rules for valid values
- A Records will contain IP addresses
- MX Record will contain a number to specify the priority and a hostname (which will point to an IP).
- TXT Records values may contain various information in text format.
  - Values will be inside quotes "[value here]"
  - SPF, DKIM and DMARC are TXT type records


```
; <<>> DiG diggui.com <<>> @ns-181.awsdns-22.com validity.com ANY
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35471
;; flags: qr aa rd; QUERY: 1, ANSWER: 25, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;validity.com.                  IN      ANY

;; ANSWER SECTION:
validity.com.           300     IN      A       141.193.213.20
validity.com.           300     IN      A       141.193.213.21
validity.com.           172800  IN      NS      ns-1403.awsdns-47.org.
validity.com.           172800  IN      NS      ns-1611.awsdns-09.co.uk.
validity.com.           172800  IN      NS      ns-181.awsdns-22.com.
validity.com.           172800  IN      NS      ns-582.awsdns-08.net.
validity.com.           900     IN      SOA     ns-1403.awsdns-47.org. awsdns-hostmaster.amazon.com. 1 7200 900 1209600
86400
validity.com.           3600    IN      MX      10 us-smtp-inbound-1.mimecast.com.
validity.com.           3600    IN      MX      10 us-smtp-inbound-2.mimecast.com.
validity.com.           300     IN      TXT
"7cuNb512gYsbpbsUgRjTxPoVJDd3wV4+EHdWQ3fDW5uNCR4pLdAebOWYYGBn5wA0Ye8QR5ljoaoTIbFtJa8zhg=="
validity.com.           300     IN      TXT     "MS=ms95485999"
validity.com.           300     IN      TXT     "adobe-idp-site-
verification=64ce7203a2c160ec0e8a75295169fd758784eac50bcb159d87c93ce9cc7e8bad"
validity.com.           300     IN      TXT     "amazonses:S+q6LgxoMIiBvzdVotFN+iLpTDmrjSYrQ2gFWgMDKbQ="
validity.com.           300     IN      TXT     "apple-domain-verification=90LIX8uov9CDdGyl"
validity.com.           300     IN      TXT     "apple-domain-verification=nw7XJ7RYT1o2eINe"
validity.com.           300     IN      TXT     "atlassian-domain-
verification=FUPQ2FFgw0Krljtok3UHaPnW4DRqzyrWQQ3EdiSdapLmkUbqwuV6vxAs0RbTNNNM"
validity.com.           300     IN      TXT     "bcn=8B072106-2302-11ED-B1DE-8C9EFCEB5D6C"
validity.com.           300     IN      TXT     "docusign=dd15ad3a-4ee6-4a1d-9da9-e5812ef8c927"
validity.com.           300     IN      TXT     "google-site-verification=GLulH94hsn2AhWgJrTGRuzddp-UJSz4iT1XGhwv7TjA"
validity.com.           300     IN      TXT     "mmt85cgj0e1823d2kf5aeelk6r"
validity.com.           300     IN      TXT     "onetrust-domain-verification=d346c9b94f914b3192dd5fb503199b92"
validity.com.           300     IN      TXT     "postman-domain-
verification=8b0c2bf1f295f933862f4e377d90d4069fd031a8f585fa85fd6d9f2fb3e1c4cae3c4c961c97a8c1f24c21c4a96c52ff90c352ee315ae706
91b6f240e5b434245"
validity.com.           300     IN      TXT     "r0qpu9ihdgmnem09vbdi15jq5g"
validity.com.           300     IN      TXT     "smartsheet-site-validation=HaKKo7nEIlKYYIpM6rvSxQsu4tojiDLm"
validity.com.           300     IN      TXT     "v=spf1 include:us._netblocks.mimecast.com include:_spf.salesforce.com
include:mail.zendesk.com include:mktomail.com include:spf.protection.outlook.com " "ip4:54.204.201.126 ip4:52.204.80.252
ip4:149.72.164.184 ip4:167.89.82.131 ip4:149.72.232.65 -all"

;; Query time: 20 msec
;; SERVER: 2600:9000:5300:b500::1#53(2600:9000:5300:b500::1)
;; WHEN: Thu Mar 07 13:05:54 UTC 2024
;; MSG SIZE  rcvd: 1710
```

https://www.diggui.com/

validity

Subdomains and DNS Records

- Subdomains are managed at the Domain DNS record.
- A subdomain may a separate DNS Record (in the same server), or even delegated to another server.
- When delegating to another server, the subdomain points to the Name Server that will have the DNS record of the subdomain.

```
$ORIGIN example.com
@       IN SOA       ns1.example.com           hostmaster.example.com
(
                    2013010100                    ;Serial
                          2H                      ;Refresh
                          1H                      ;Retry
                          2W                      ;Expire
                          1H)                     ;TTL
         IN NS         ns1.example.com
         IN NS         ns2.example.com
localhost             IN A         127.0.0.1
                         IN MX 10       mailserver.example.com
;
;Delegate email.example.com to Salesforce Marketing Cloud
email                            IN NS              ns1.exacttarget.com
email                            IN NS              ns2.exacttarget.com
email                            IN NS              ns3.exacttarget.com
email                            IN NS              ns4.exacttarget.com
```

[Custom Domain or Subdomain Delegation in Marketing Cloud (salesforce.com)]

validity

validity

DMARC

What is DMARC?

Domain-based Message Authentication, Reporting, and Conformance

DMARC

DMARC lets you tell receiving servers what to do with messages from your domain that don't pass SPF or DKIM. Set up DMARC by publishing a DMARC record for your domain. To pass DMARC authentication, messages must be authenticated by SPF and/or DKIM. The authenticating domain must be the same domain that's in the message From: header. Learn how to add a DMARC record at your domain.

We recommend you set up DMARC reports so you can monitor email sent from your domain, or appears to have been sent from your domain. DMARC reports help you identify senders that may be impersonating your domain. Learn more about DMARC reports.

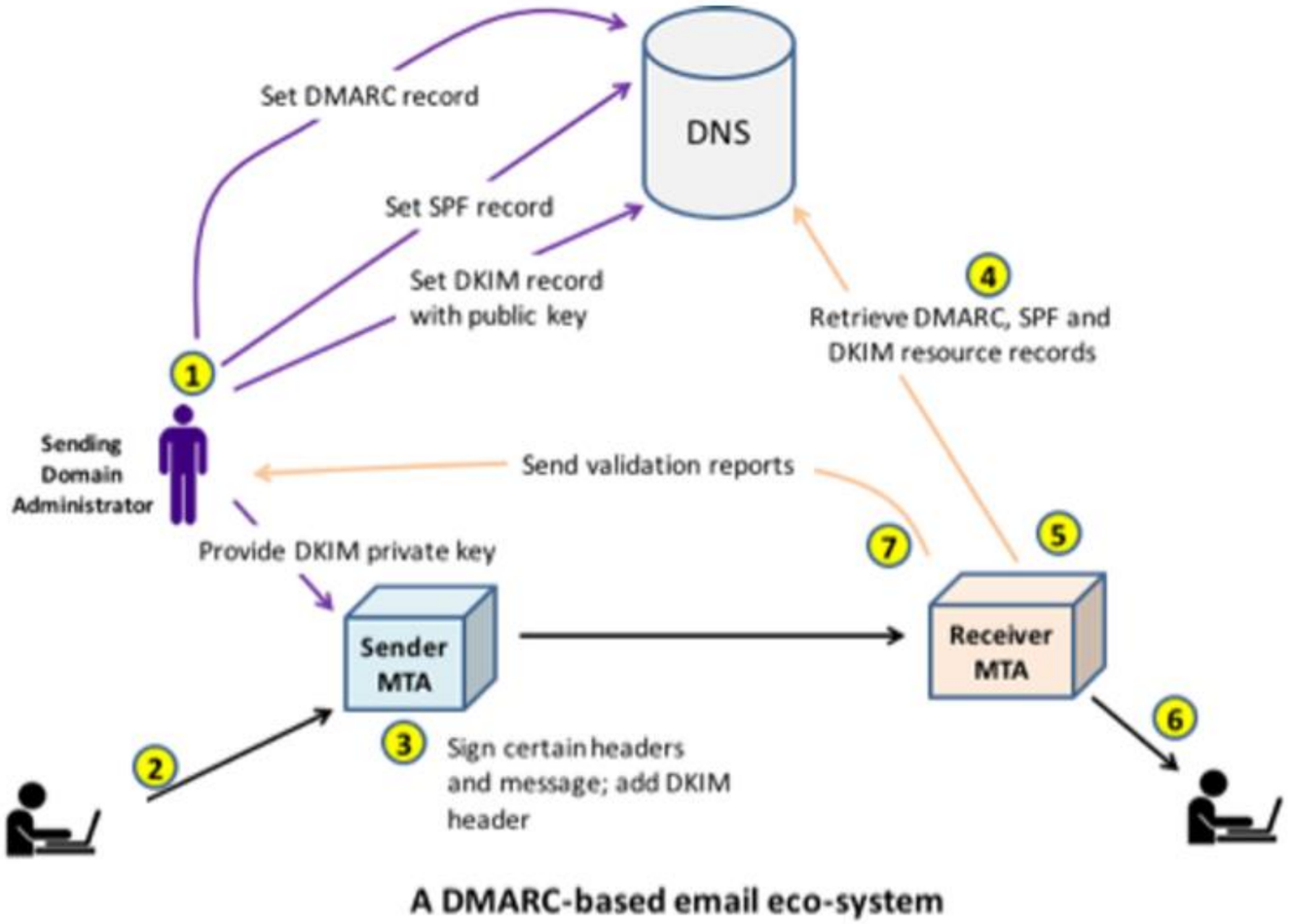
When you set up DMARC, you can then optionally set up BIMI to add your brand logo to messages sent from your domain. Learn how to add your brand logo with BIMI.

Email sender guidelines - Google Workspace Admin Help

Gmail and Yahoo now require all bulk senders to publish a DMARC record ensure alignment with their SFP/DKIM domains. It's recommended to implement a DMARC reporting solution.

DNS – Home of SPF, DKIM and DMARC

1. Sending domain owner populates its DNS with TXT for SPF, DKIM and DMARC.
2. Sender sends email or schedules a campaign to be sent.
3. An email sent from that domain has a DKIM header appended by the sending MTA (Mail Transfer Agent). MTAs have the appropriate private key for creating DKIM signatures.
4. Receiving MTA queries the sending domain's DNS to obtain its SPF, DKIM and DMARC policies .
5. Policies are evaluated and a decision will be made upon results.
6. Successful validation gets message delivered. Failures are subject to policy defined in p=.
7. DMARC Reports are sent by Receiver MTA to RUA and RUF (not all send reports; not in real-time).

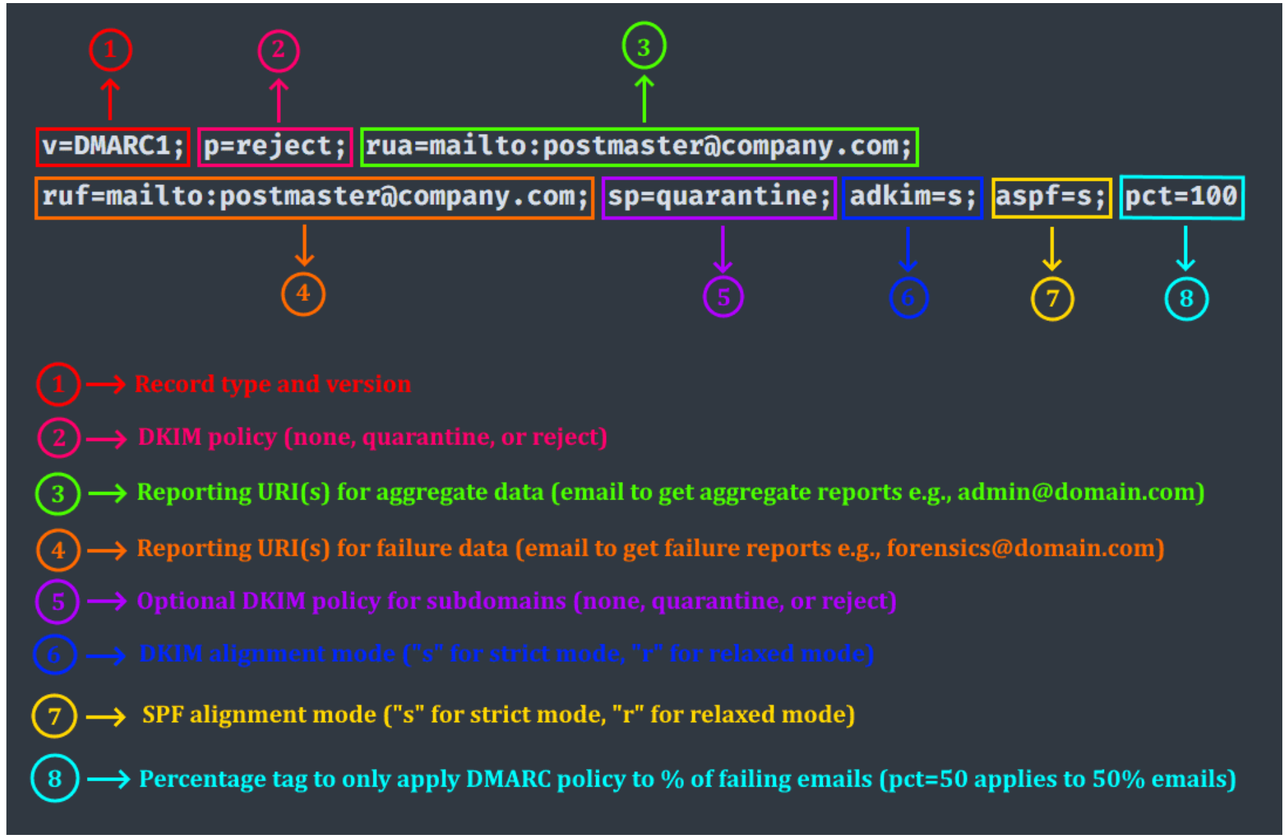


A DMARC-based email eco-system

Understanding a DMARC Record

- DMARC is a TXT record that lives in _dmarc.domain.com.
  - This subdomain should only have one TXT record, no other record types.
- Subdomains will inherit DMARC records from Domain if not overwritten with its own _dmarc.subdomain.domain.com record
  - DMARC at the subdomain level: When and why? (spamresource.com)
- Tags v= and p= are required, others are optional.
- RUA and RUF may contain multiple email address, just separate with a comma.
  - Can I have multiple reporting addresses in my DMARC record? – Validity Help Center

Type	Name	Content	TTL
TXT	_dmarc	v=DMARC1; p=none; rua=mailto: pattie@example.com	Auto



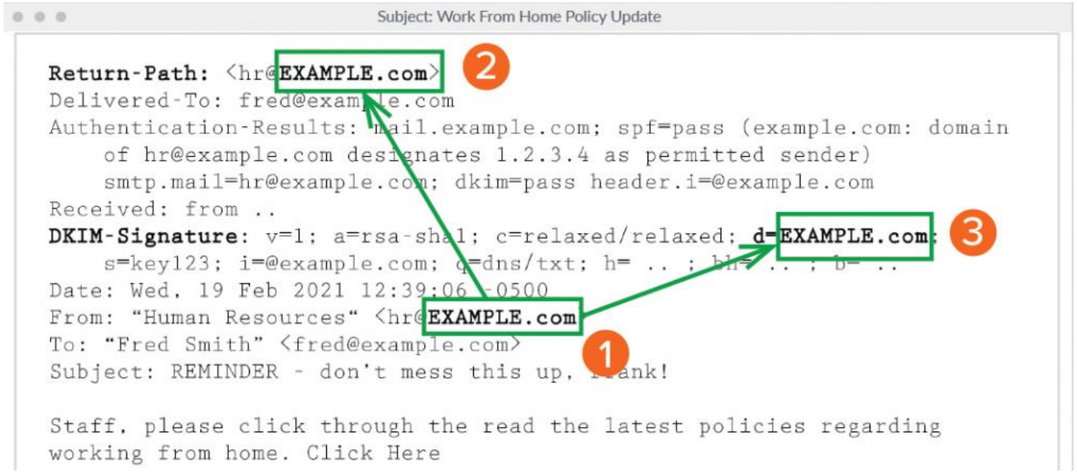
validity

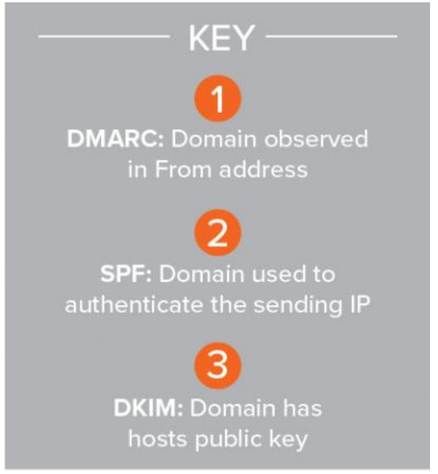
SPF, DKIM and Alignment

DMARC and Alignment

- DMARC ensures consistency between the domain in the "From" address and the domains authorized by SPF and/or DKIM.
- DMARC requires at least 1 alignment to pass.
- Relaxed alignment, the default setting, allows the domain used in the "Return-Path" (from SPF) or the domain in the DKIM signature ("d=") to be a subdomain of the "From" address in the email.

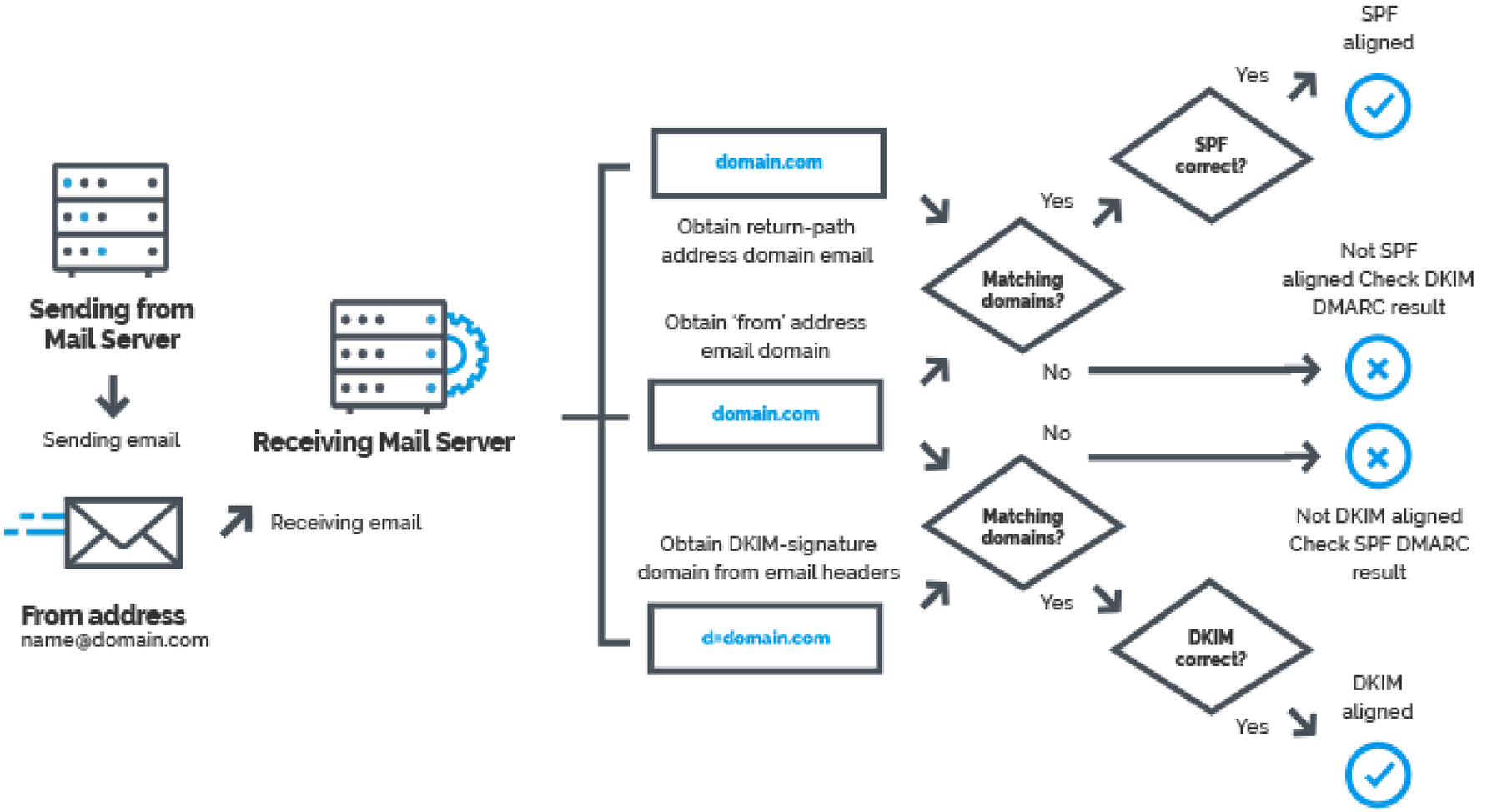
	DMARC RESULT	FROM:DOMAIN (DMARC)	DKIM DOMAIN (DKIM)	ENVELOPE_FROM / RETURN-PATH (SPF)
Full Alignment	✓	@client.net	@client.net	@client.net
DKIM Only	✓	@client.net	@client.net	@sample.net
SPF Only	✓	@client.net	@sample.net	@client.net
Fail	✗	@client.net	@sample.net	@sample.net





DMARC Alignment - dmarcian

How Email Servers Use DMARC



validity

DMARC Reports

DMARC Aggregate and Forensic Reports

- Aggregate reports (RUA) offer a comprehensive view of a domain's email traffic.
- They detail the authentication status (DKIM/SPF and DMARC) for all emails, including their source and authentication results.
- Reports are sent in XML file format to the email addresses listed in RUA tag.
- Everest consumes these files and displays it as graphs with filters.
- Although we recommend adding email address for RUF, **Everest doesn't consume or display that data.**
  - This is because it may contain PII.

Aggregate

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <report_metadata>
    <org_name>reporter_abc </org_name>                    ← reporter name
    <email>dmarc_ag_feedback@reporterdomain.com </email>
    <extra_contact_info>https://receiver.example/dmarc</extra_contact_info>
    <report_id>0001229911231 </report_id>
    <date_range>
      <begin>1569888000 </begin>
      <end>1569974399 </end>                              ← date range of the report
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>example.com </domain>
    <adkim>r </adkim>
    <aspf>r </aspf>                                       ← DMARC policy of domain evaluated
    <p>reject </p>
    <sp>reject </sp>
    <pct>100 </pct>
  </policy_published>
  <record>
    <row>
      <source_ip>192.0.2.24</source_ip>                   ← sending IP address
      <count>17 </count>
      <policy_evaluated>
        <disposition>none </disposition>
        <dkim>pass </dkim>
        <spf>pass </spf>                                  ← SPF/DKIM pass or fail results
      </policy_evaluated>
    </row>
    <identifiers>
      <header_from>example.com </header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>example.com </domain>
        <result>pass </result>                            ← SPF/DKIM alignment results
        <selector>1234 </selector>
      </dkim>
      <spf>
        <domain>example.com </domain>
        <result>pass </result>
      </spf>
    </auth_results>
  </record>
```

The Difference in DMARC Reports: RUA and RUF - dmarcian

Forensic

```
Feedback-Type: auth-failure
User-Agent: szn-mime/2.0.41
Version: 1
Original-Rcpt-To: xxxx@seznam.cz
Source-Ip: 198.2.183.22
Authentication-Results: email.seznam.cz 1;
        spf_align=fail;
        dkim_align=fail
Delivery-Result: delivered\r\n\r\nReceived: from mail22.suw13.rsgsv.net (mail22.suw13.rsgsv.net [198.2.183.22
        by email-smtpd9.ng.seznam.cz (Seznam SMTPD 1.3.106) with ESMTP;
        Fri, 12 Jul 2019 10:01:20 +0200 (CEST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=fbl.mcsv.net; s=k1;
        t=1562918478; bh=z+cM1nqHlHrjpgwrd2iSbq3xmFeT/VO5Zoa5XOw5TY8=;
        h=Subject:From:Reply-To:To:Date:Message-ID:Feedback-ID:List-ID:
         List-Unsubscribe:Content-Type:MIME-Version;
        b=QhxQk+uH4sVDFSYWdTJrdFzJc3wTQ9TBBlq2FDnri+hfqMAMHaAfGVHytqUcnWL3x
         H6X0zZZkwp6KJc2vsm/cH1Xls10xaPWHG3ioK0aM5kv7BJfBX2PRAfzPR4eaBvakZi
         o2acfXIPaCZ+GeBNxaz5JKDTuteM/xavDjcbObXs=
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=mailchimpapp.net;
        s=k1; t=1562918478; i=rortega=3D3Dasmusa.org@mailchimpapp.net;
        bh=z+cM1nqHlHrjpgwrd2iSbq3xmFeT/VO5Zoa5XOw5TY8=;
        h=Subject:From:Reply-To:To:Date:Message-ID:List-ID:List-Unsubscribe:
         Content-Type:MIME-Version;
        b=iJriMQtloII7ciJrNISIOixgf2oWoCfaq/xO2XnLq9OzxEAXR8U0bgWa0lJU8wq3+
         0OlgUsrU/Vd43B+umAAnKaRLoT3JjoExWh5B84cGnr+9MkcJWf+RB4QilG8GWtEgVl
         O4W1o6pcuVupqSqOiCnrcuVI2L9hEwlXfnIqSMMQ=
Received: from localhost (localhost [127.0.0.1])
        by mail22.suw13.rsgsv.net (Mailchimp) with ESMTP id 45lQNZ5cXVzt6G
        for <xxxx@seznam.cz>; Fri, 12 Jul 2019 08:01:18 +0000 (GMT)
x-mcpf-jobid: mc.us7_22465175.1121249.5d283e46c424e.full_000002
Subject: =?utf-8?Q?New=20from=20microTalk=20for=2007=2F11=2F2019?=
From: =?utf-8?Q?American=20Society=20for=20Microbiology?= <rortega@asmusa.org>
Reply-To: =?utf-8?Q?American=20Society=20for=20Microbiology?= <rortega@asmusa.org>
To: <xxxx@seznam.cz>
Date: Fri, 12 Jul 2019 08:01:17 +0000
Message-ID: <1772a0600a0b532d47343e0f9.0636065ea3.20190712080112.ac71646aa0.3ffee3b2@mail22.suw13.rsgsv.net>
X-Mailer: MailChimp Mailer - **CIDac71646aa00636065ea3**
X-Campaign: mailchimp1772a0600a0b532d47343e0f9.ac71646aa0
X-campaignid: mailchimp1772a0600a0b532d47343e0f9.ac71646aa0
```

DMARC Failure Reports (Forensic Reports) Explained. - DMARCLY

Aggregate Report in Everest

A. **Policy Domain:** Informs the domain or subdomain of the DMARC record.

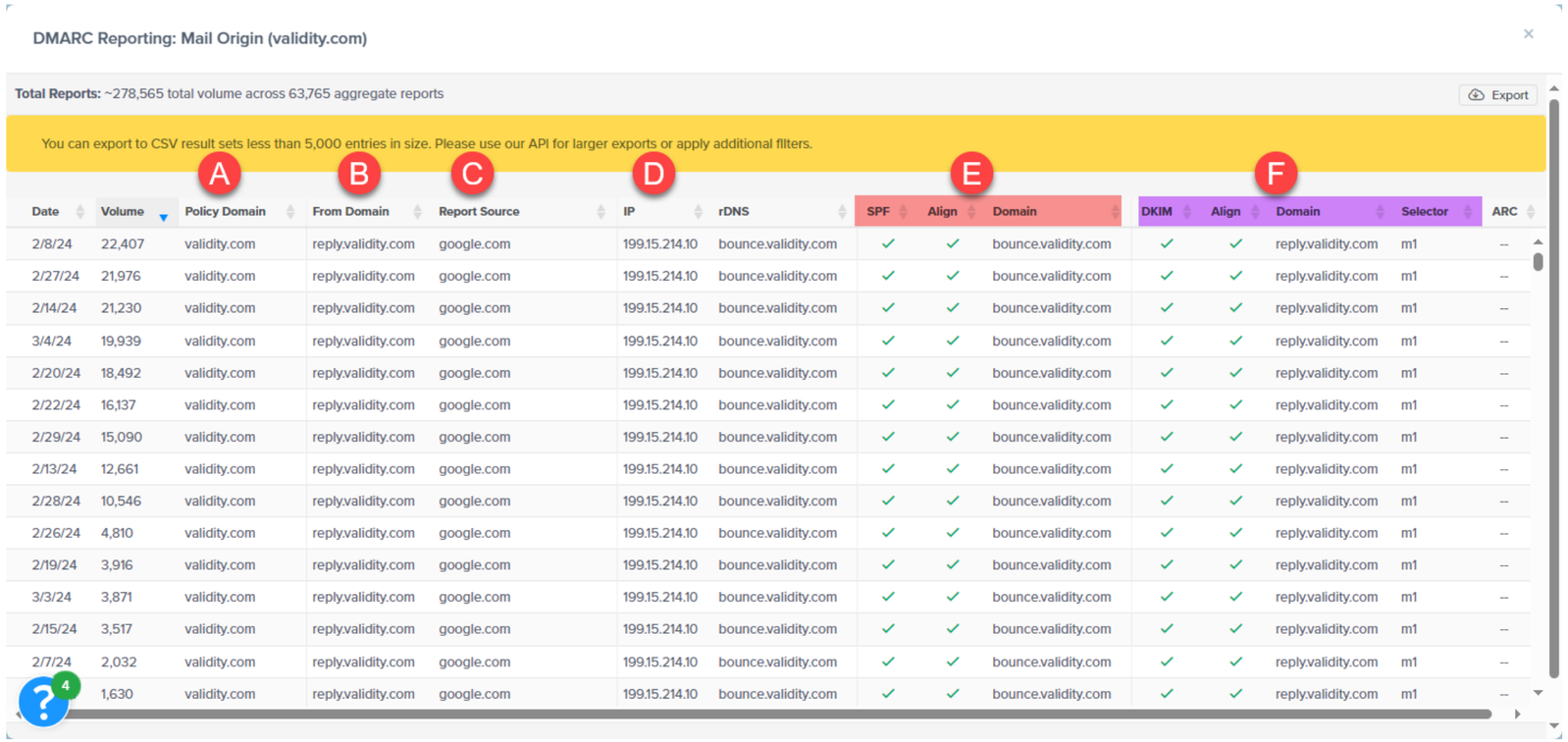
B. **From Domain:** Domain in the From header of the email message

C. **Report Source:** Entity that provided the report to Everest

D. **IP and rDNS:** Information about where the message originated from

E. **SPF:** The "Domain" column shows the domain associated with the "Return-Path," while the "SPF" and "Align" columns use icons to indicate whether SPF authentication passed, failed, or wasn't found.

F. **DKIM:** The "Domain" column displays the content found in the "d=" value of the DKIM signature. The "Selector" column shows the content of the "s=" value. Finally, the "DKIM" and "Align" columns use icons to indicate whether DKIM authentication and alignment passed, failed, or weren't found.



validity

Troubleshooting DMARC with Everest

Troubleshooting Steps

Using Everest to get visibility of email sources

1. Accounts may have multiple Policy Domains, do the following steps one by one.
   - Use the Domain & Policies page to view compliance for all at a glance.
   - This view will show the current policy being applied.
   - The goal of Everest's DMARC tool is to provide visibility of what are the authorized sources for the domain's email volume, and once everything has been mapped and vetted, move to a stricter policy.

2. Select the Policy Domain and view **Compliant sources**, this will allow to understand where authenticated emails are sent from.
   - Keep in mind that many companies have multiple departments, each may have a different sending platform.
   - Its common to share a subdomain of the Policy Domain.
   - Ask the client about what Everest is surfacing, it might be news to them too.

3. Analyze what the information in DMARC Trends
   - Every tab will give you more information about where email is sent from using the domains of the selected Policy Domain.
   - Senders usually don't distribute their email volume across multiple platforms or Ips, this means you should see volume concentrated on just a few sources, this can be observed in the "%" column.
   - Click on the arrow to get more details about the From domain, DKIM domain, SPF domain, authentication result and alignment.
   - Use tools like Senderscore, Whois, Cisco Talos, and Google to get information about the sources.

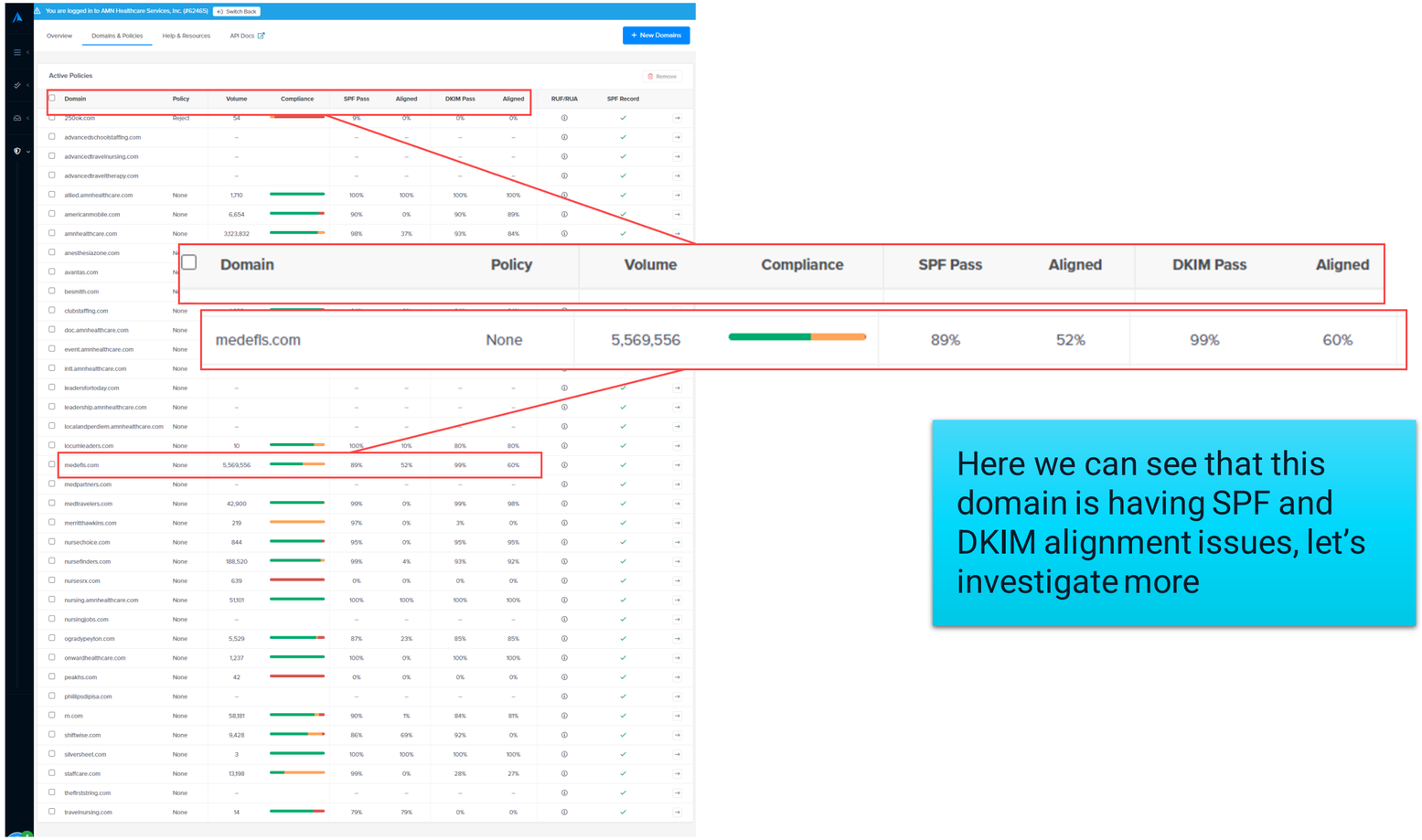
Troubleshooting Steps

Using Everest to get visibility of email sources

4. Filter to view **Non-Compliant** sources and analyze DMARC Trends
   - This will show sources that have passing SPF and/or DKIM but are **failing alignment**.
   - Surface what Everest is uncovering and any findings from analysis to client.
   - The idea here is to correct alignment issues, this often means the client will need to:
     - Ensure the domain of DKIM's signature's "d=" tag matches the domain in From header.
     - Ensure the domain in Return-Path matches the domain in From header.
   - Most of the changes required for proper alignment can be made via the ESP's interface or ticket.
     - Sometimes, alignment issues happen because the sender is using incorrect From header, this can happen more often with SFMC clients that don't know they need to pay extra for a Sender Authentication Package.
5. Filter to view **Unauthenticated** sources and analyze DMARC Trends
   - This will show sources that are failing both SPF and DKIM.
   - Alignment automatically fails because authentication fails.
   - Here you will often see google.com and outlook.com due to automatic forwarding setup by their users – nothing can be done about that, other then rely on ARC (not covered here).
   - Failed spoofing attempts will show up here, since they are failing SPF and DKIM it is very unlikely mailbox provider will send to inbox
   - Moving to a stricter policy is the best way to tell MBPs how to treat unauthenticated messages.

Example 1

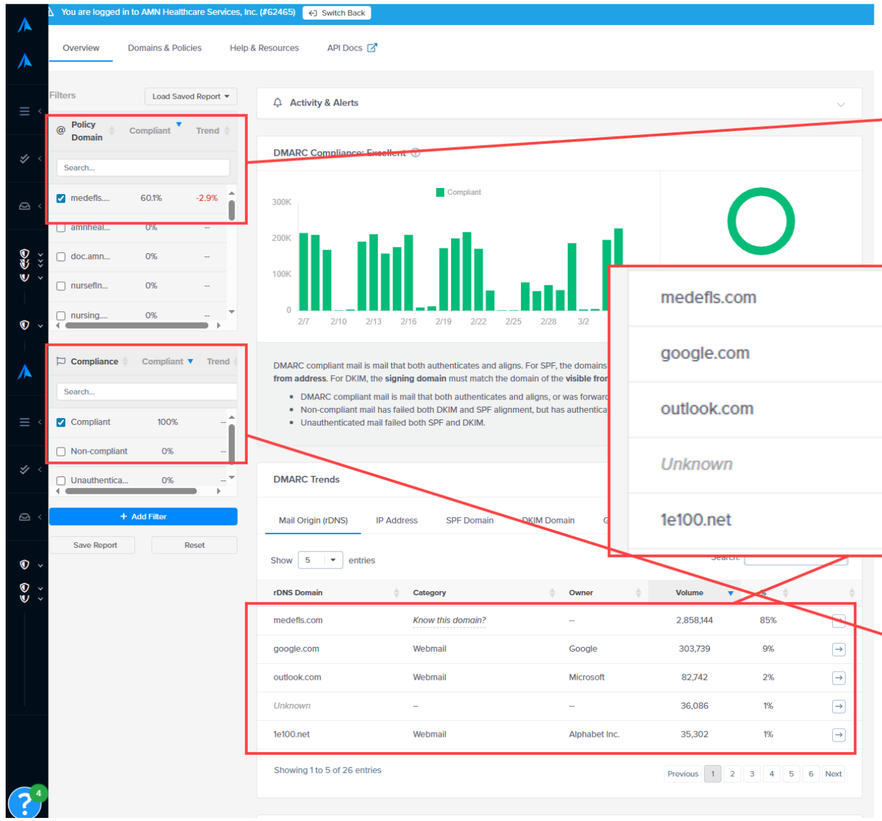
Use Domains & Policies

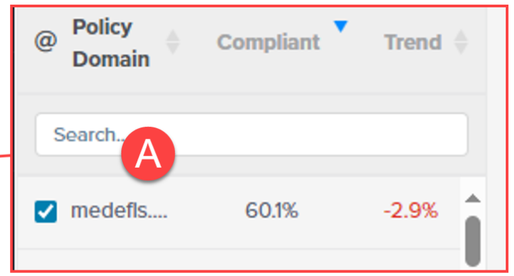


Here we can see that this domain is having SPF and DKIM alignment issues, let's investigate more

Example 2

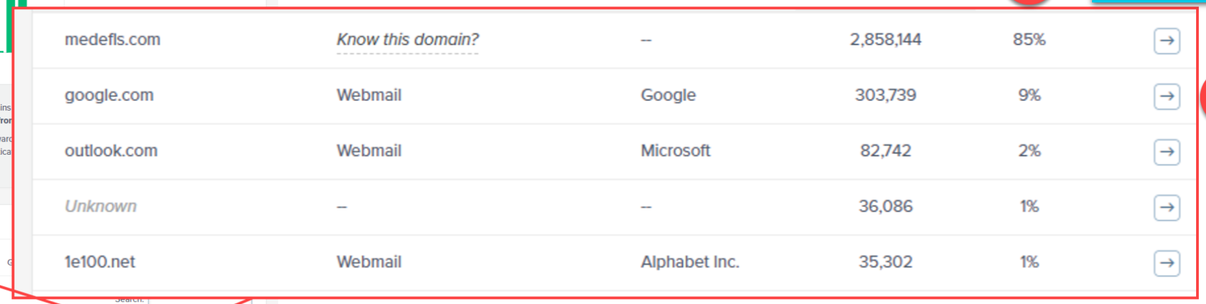
Filter to show Compliant sources to view where most emails are originating from



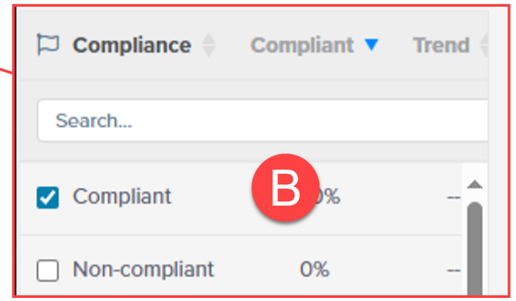


Select the Policy Domain to filter the report.

First source of the list is responsible for 89% of email messages. Google and Outlook, seams like domain is using Google Workspace and Office 365.



Click on the arrow to get more information about the source



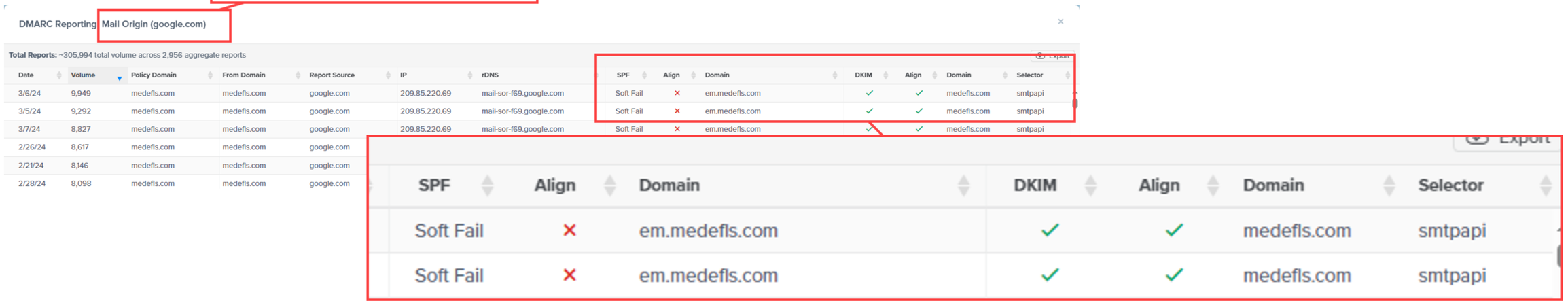
Review Compliant sources to have a better understanding of where emails are originating from.

Example 2

Filter to show Compliant sources to view where most emails are originating from

When we see this source, it usually means the domain is using Google Workspace.

Mail Origin (google.com)



DMARC Reporting | Mail Origin (google.com)

Total Reports: ~305,994 total volume across 2,956 aggregate reports

Date	Volume	Policy Domain	From Domain	Report Source	IP	rDNS	SPF	Align	Domain	DKIM	Align	Domain	Selector
3/6/24	9,949	medefls.com	medefls.com	google.com	209.85.220.69	mail-sor-f69.google.com	Soft Fail	✗	em.medefls.com	✓	✓	medefls.com	smtpapi
3/5/24	9,292	medefls.com	medefls.com	google.com	209.85.220.69	mail-sor-f69.google.com	Soft Fail	✗	em.medefls.com	✓	✓	medefls.com	smtpapi
3/7/24	8,827	medefls.com	medefls.com	google.com	209.85.220.69	mail-sor-f69.google.com	Soft Fail	✗	em.medefls.com	✓	✓	medefls.com	smtpapi
2/26/24	8,617	medefls.com	medefls.com	google.com									
2/21/24	8,146	medefls.com	medefls.com	google.com									
2/28/24	8,098	medefls.com	medefls.com	google.com									

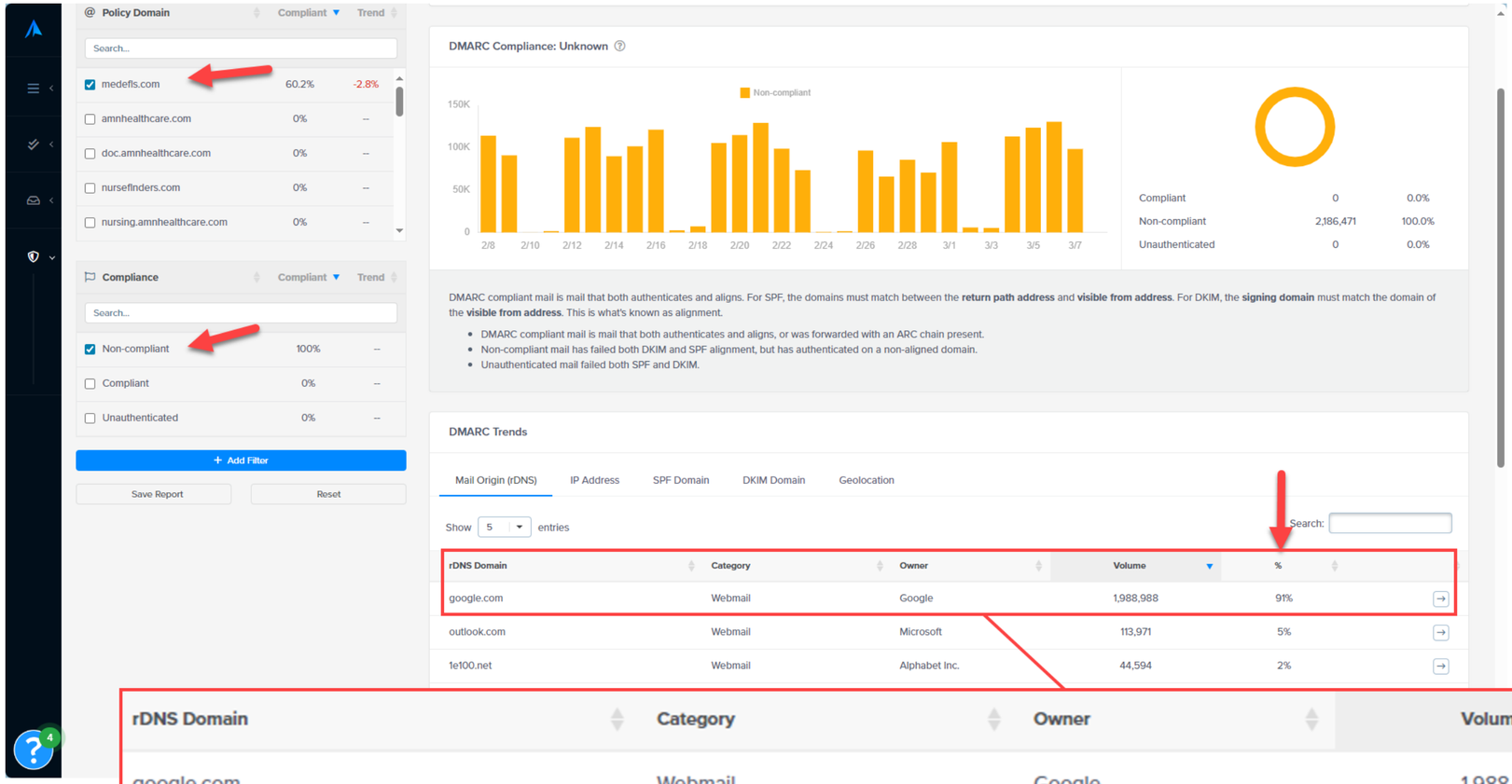
Export

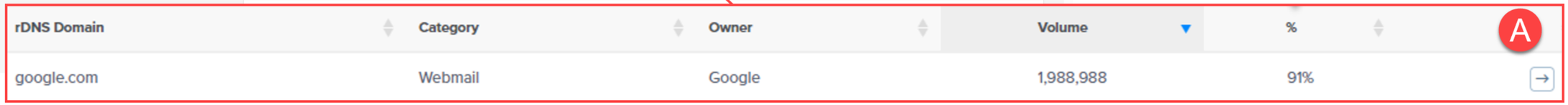
SPF	Align	Domain	DKIM	Align	Domain	Selector
Soft Fail	✗	em.medefls.com	✓	✓	medefls.com	smtpapi
Soft Fail	✗	em.medefls.com	✓	✓	medefls.com	smtpapi

It is accepted to have only one authentication passing and aligning.
Here we can see that is the case for DKIM.
If client can't do both, prioritize DKIM pass/align over SPF.

Example 3

Filter to show Non-Compliant sources and analyze DMARC Trends

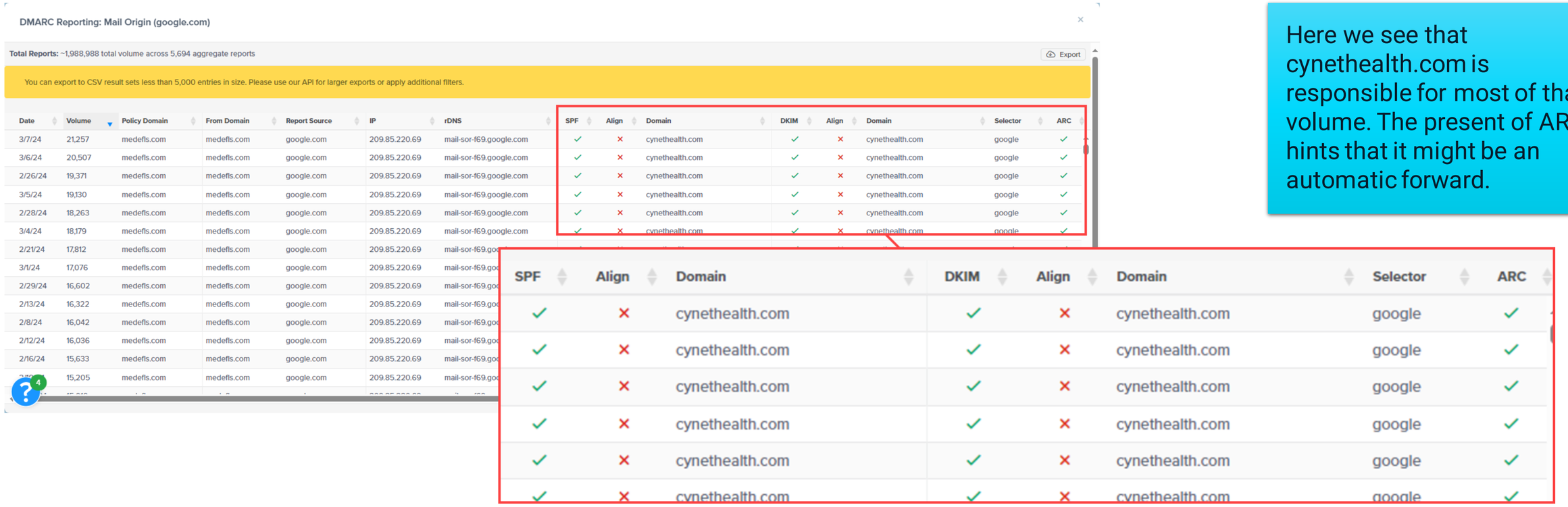




Here we see google.com again, but there is more non-compliant volume. Click on the arrow to investigate more.

Example 3

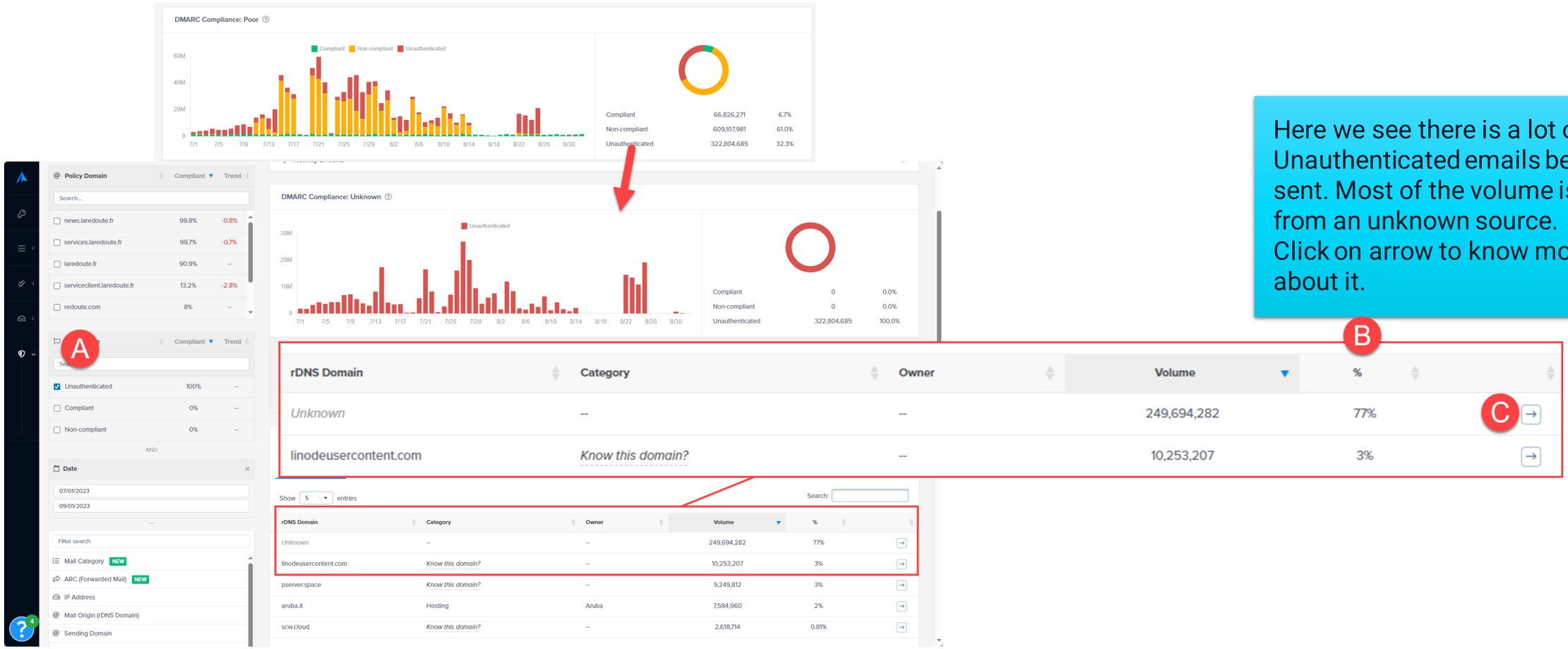
Filter to show Non-Compliant sources and analyze DMARC Trends



Here we see that cynethealth.com is responsible for most of that volume. The present of ARC hints that it might be an automatic forward.

Example 4

Filter to show Unauthenticated sources and analyze DMARC Trends



Here we see there is a lot of Unauthenticated emails being sent. Most of the volume is from an unknown source. Click on arrow to know more about it.

Example 4

Filter to show Unauthenticated sources and analyze DMARC Trends

These messages are sent using Ips that aren't known to the client and with different Return-Path domains. They lack SPF and DKIM signatures.
Some SPF domains will show fail because they have an SPF record that doesn't allow for that IP to send on their behalf.

DMARC Reporting: Mail Origin (Unknown)

Total Reports: ~249,694,282 total volume across 313,776 aggregate reports

You can export to CSV result sets less than 5,000 entries in size. Please use our API for larger exports or apply additional filters.

Date	Volume	Policy Domain	From Domain	Report Source	IP	rDNS	SPF	Align	Domain
7/3/23	473,514	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.170.11	--	--	--	kenigsm.shop
7/4/23	418,777	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.170.109	--	--	--	mimouzacity.shop
7/10/23	385,757	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.170.11	--	--	--	kenigsm.shop
7/11/23	351,725	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.170.11	--	--	--	kenigsm.shop
7/10/23	348,566	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.170.109	--	--	--	mimouzacity.shop
7/5/23	345,900	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.170.11	--	--	--	kenigsm.shop
7/4/23	333,488	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.170.11	--	--	--	kenigsm.shop
7/7/23	331,557	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.170.11	--	--	--	kenigsm.shop
7/2/23	328,312	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.170.11	--	--	--	kenigsm.shop
7/5/23	311,299	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.170.109	--	--	--	mimouzacity.shop
8/23/23	311,152	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.247.127	--	--	--	free-usasdsstuff.com
7/7/23	308,233	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.170.11	--	--	--	kenigsm.shop
7/1/23	306,961	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.170.11	--	--	--	kenigsm.shop
8/23/23	305,048	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.247.110	--	✕	✕	collegegrad.com
8/23/23	304,227	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.247.244	--	✕	✕	myrewarsdreddfcentre.uk.com
8/23/23	303,011	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.247.138	--	--	--	www.ukmdsdeodels.co.uk
8/23/23	302,626	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.247.164	--	--	--	premierosdsdfsodforsdirect.co.uk
7/6/23	301,194	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.170.11	--	--	--	kenigsm.shop
8/23/23	299,941	fr.redoute.com	fr.redoute.com	Outlook.com	85.121.247.106	--	--	--	prize-wave.com

kenigsm.shop
kenigsm.shop
mimouzacity.shop
free-usasdsstuff.com
kenigsm.shop
kenigsm.shop
collegegrad.com
myrewarsdreddfcentre.uk.com
www.ukmdsdeodels.co.uk
premierosdsdfsodforsdirect.co.uk

Questions to ask:

- What are you sending Ips?
- What are the domains that the brand uses to send emails?
- Are all the domains configured in Everest?
- Are there any registered domains associated with your organization that shouldn't be sending emails?
- Which team within your organization is responsible for managing domain names and DNS settings?
- What ESP(s) do you use?
- Do other departments within your organization send emails using our company's domain names?
- Does your brand use external services to send emails on its behalf?
- Where are corporate emails sent from? Ex.: Google Workplace, Office 365, Microsoft Exchange.
- Does the amount of email traffic shown in DMARC reports align with our usual sending volume?
- Have you heard about BIMI?

Reaching out to Professional Services

DMARC can turn into a PS opportunity:

- Our clients should lean on the Services Team and Support for:
  - Questions regarding DMARC record and how to update it using our help center articles and playbooks.
  - Help them navigate Everest's DMARC tool and understand what it provides, with our published contents and meetings.
- It could be a PS opportunity if:
  - Client manages multiple domains or brands.
  - Need hand holding to understand what Everest is surfacing, along with detailed next steps.
  - Complex DNS setups and dealing with more technical team.
  - Client wants to get BIMI but don't yet have DKIM, SPF or DMARC properly in place, so it needs to be a project with formalized next steps and roles.

Email:
- ProfessionalServices@validity.com

Slack:
- #proserve-help

validity

Q&A