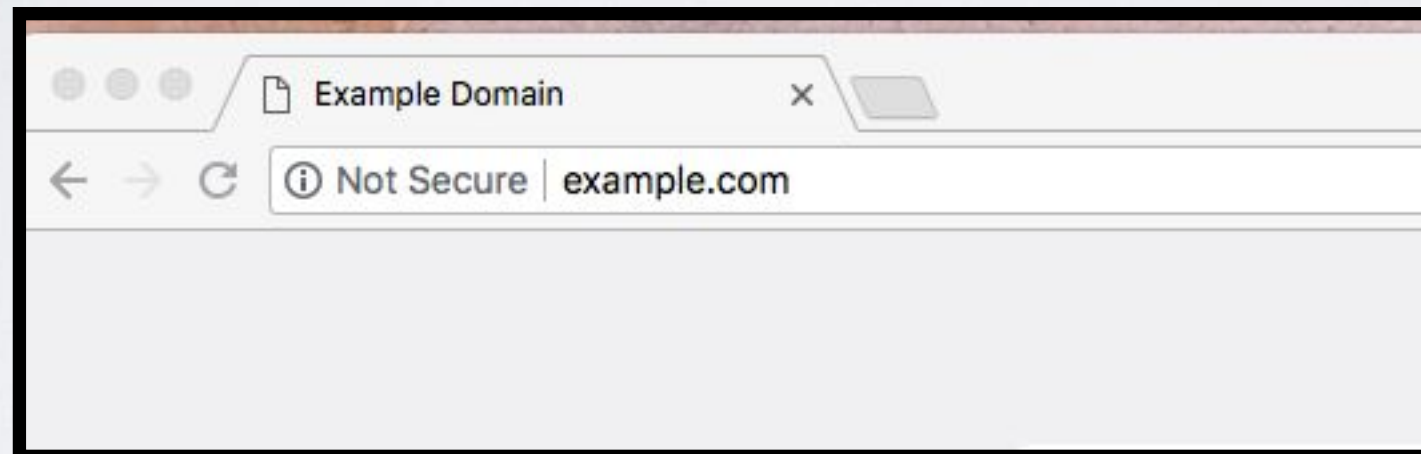


GREEN LOCKS FOR YOU & ME

Wendy Knox Everette
Senior Security Advisor, Leviathan Security Group
[@wendyck](#)

Crypto & Privacy Village, Def Con 26



WEBSITES WITHOUT
HTTPS
Chrome now labels these as “not secure”

A milestone for Chrome security: marking HTTP as “not secure”

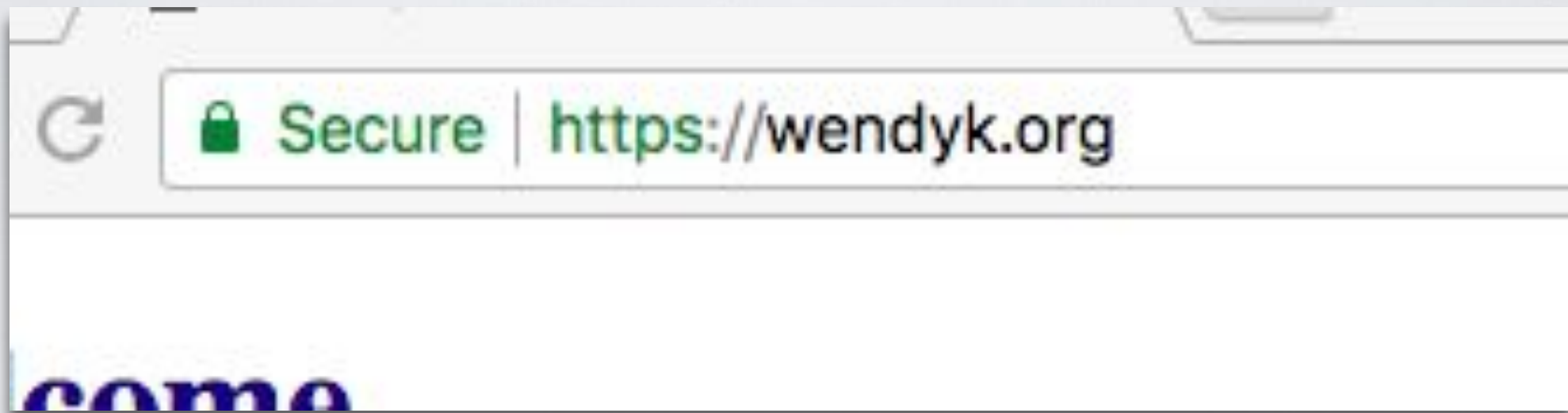


Emily Schechter
Chrome Security Product
Manager

Published Jul 24, 2018

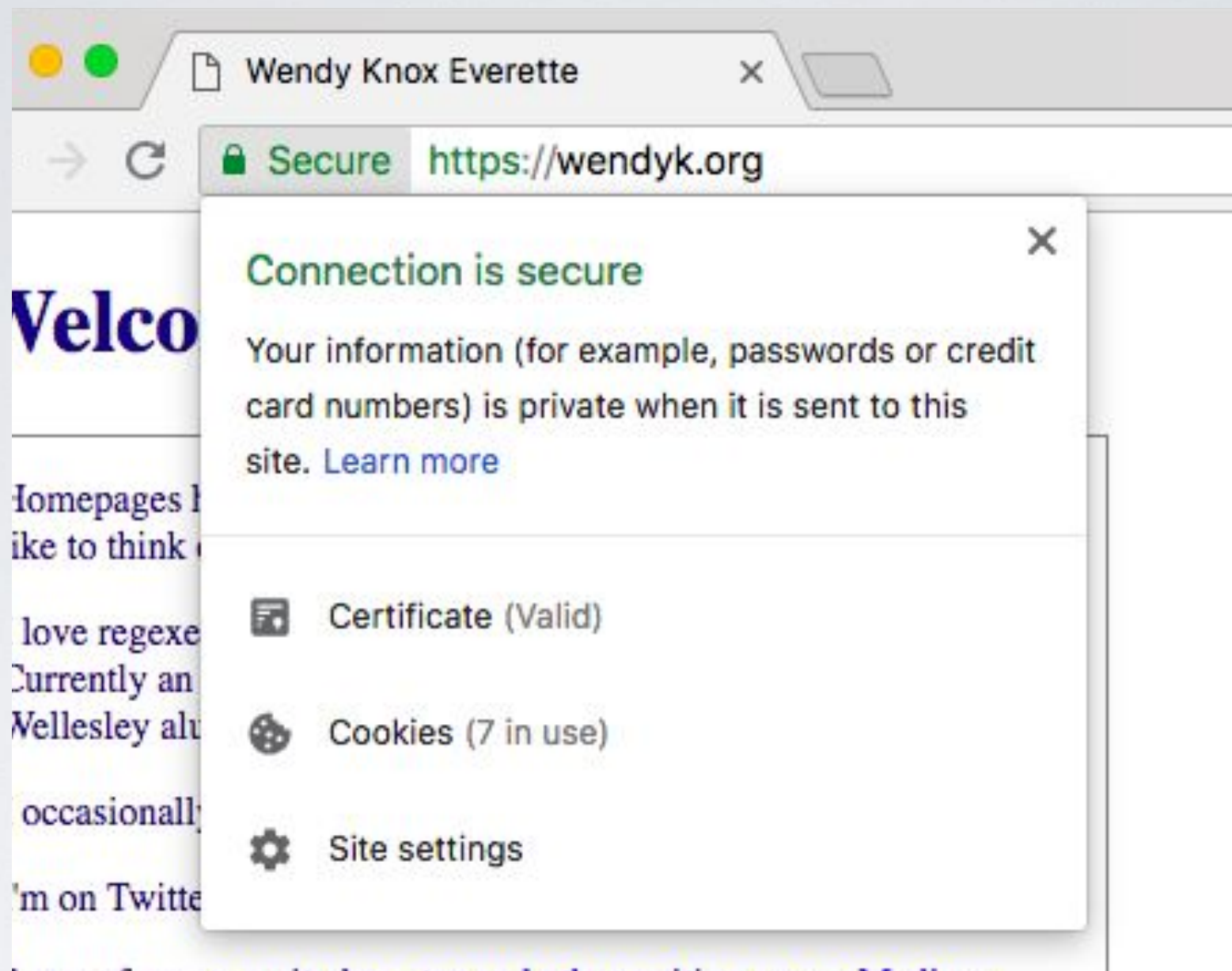
Security has been one of Chrome's core principles since the beginning—we're constantly working to [keep you safe](#) as you browse the web. Nearly two years ago, we [announced](#) that Chrome would eventually mark all sites that are not encrypted with HTTPS as "not secure". This makes it easier to know whether your personal information is safe as it travels across the web, whether you're checking your bank account or buying concert

<https://www.blog.google/products/chrome/milestone-chrome-security-marking-http-not-secure/>



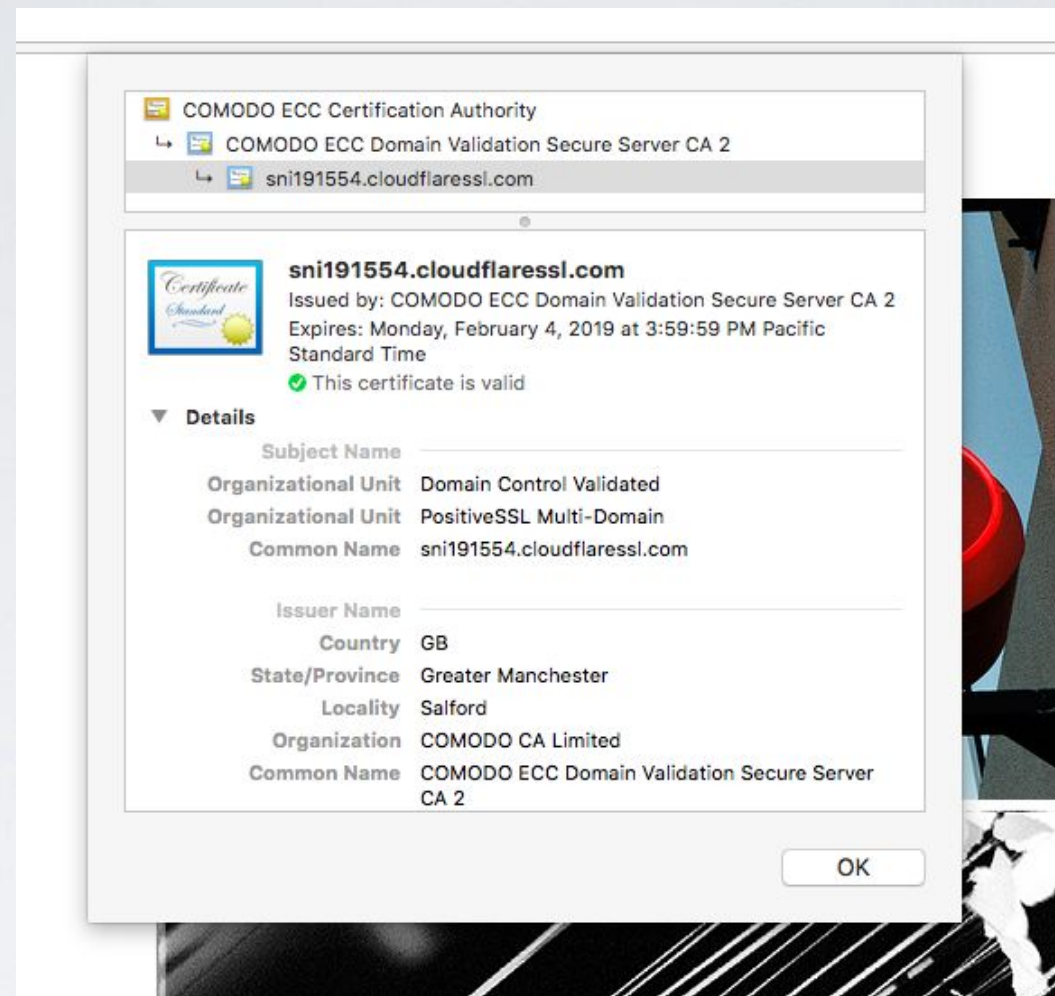
SITES WITH HTTPS

Green lock indicating SSL



HOW DO I SECURE MY WEBSITE?

- Lets Encrypt and Cloudflare are two of the services offering free certificates to websites
- Both work well with Github pages, which is what this talk will demonstrate
- There are lots of other hosting options like WordPress as well



CLOUDFLARE FREE ACCOUNT CERTIFICATE

SETTING UP THE CERTIFICATE AND DOMAIN

- Github Pages TLS with custom domains
announcement:

<https://blog.github.com/2018-05-01-github-pages-custom-domains-https/>

- Directions:

<https://help.github.com/articles/using-a-custom-domain-with-github-pages/>

Create your repo:
[USERNAME].github.io

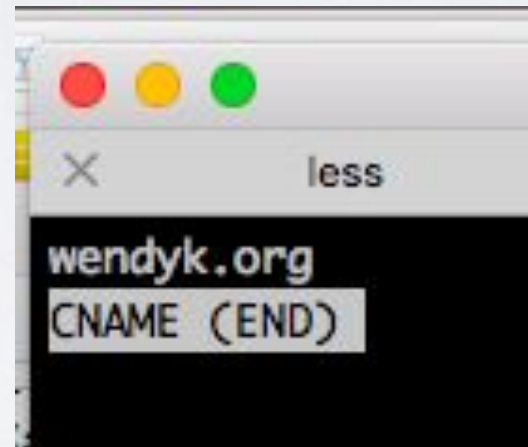
wendyck.github.io

● HTML

Check out the repo to your local machine (I like GitHub Desktop)
create a index.html (your homepage!) and any other webpage files

```
Revisionist:wendyck.github.io wck$ ls -ltr
total 40
-rw-r--r--  1 wck  staff  1076 Mar 10 14:27 LICENSE
-rw-r--r--  1 wck  staff    10 Mar 10 14:46 CNAME
drwxr-xr-x@  4 wck  staff   128 Mar 11 07:34 imgs
-rw-r--r--  1 wck  staff  2999 Mar 21 18:09 keybase.txt
-rw-r--r--  1 wck  staff  3018 Apr 28 07:16 index.html
-rw-r--r--  1 wck  staff  4031 May 30 17:54 talks.html
Revisionist:wendyck.github.io wck$
```

Create a new text file named CNAME at the root of the repo and put your domain name into it



Go to the Settings for your new repo
and scroll down to custom domain

✓ Your site is published at <http://wendyk.org/>

Source

Your GitHub Pages site is currently being built from the master branch. [Learn more.](#)

master branch ▾

Save

User pages must be built from the master branch.

Theme Chooser

Select a theme to publish your site with a Jekyll theme. [Learn more.](#)

Choose a theme

Custom domain

Custom domains allow you to serve your site from a domain other than wendyk.github.io. [Learn more.](#)

wendyk.org

Save

☐ **Enforce HTTPS** — Unavailable for your site because your domain is not properly configured to support HTTPS (wendyk.org) — [Troubleshooting custom domains](#)

HTTPS provides a layer of encryption that prevents others from snooping on or tampering with traffic to your site. When HTTPS is enforced, your site will only be served over HTTPS. [Learn more.](#)

Apex Domain DNS Configuration:

Create configure an ALIAS, ANAME, or A record at your DNS provider








Configuring A records with your DNS provider

- 1 Contact your DNS provider for detailed instructions on how to set up A records.
- 2 Follow your DNS provider's instructions to create A records that point your custom domain to the following IP addresses:
 - > 185.199.108.153
 - > 185.199.109.153
 - > 185.199.110.153
 - > 185.199.111.153

Tip: Your DNS changes can take over a full day to update and the wait varies among DNS providers.

Set the “A” record values to be the IP addresses that GitHub provides in their help pages

(<https://help.github.com/articles/setting-up-an-apex-domain/>)

Type	Name	Value	TTL	Status
A	wendyk.org	points to 185.199.111.153	Automatic	 
A	wendyk.org	points to 185.199.110.153	Automatic	 
A	wendyk.org	points to 185.199.109.153	Automatic	 
A	wendyk.org	points to 185.199.108.153	Automatic	 



NEXT... SO YOU HAVE EMAIL ON
YOUR PERSONAL DOMAIN: HOW
DO PREVENT IT FROM BEING
SPOOFED?

DO I NEED TO DO THIS?

I'd assumed at first that since I was using Google Apps Gmail for my email that it couldn't be used to spoof. Turns out I was wrong

SPF - SENDER PERMITTED FROM

- <https://blog.returnpath.com/how-to-explain-spf-in-plain-english/>
- Lets a domain owner specify the only IP addresses that can send email for that domain
- Up to recipients to check for matches

DKIM - DOMAINKEYS IDENTIFIED MAIL

- <https://blog.returnpath.com/how-to-explain-dkim-in-plain-english-2/>
- Allows us to cryptographically sign our emails! the elements of the email to be signed are encrypted with our private key.
- Public key to decrypt is available in DNS
- Unfortunately not really widely adopted yet - but GSuite supports it

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;

d=wendyk.org; s=google;

h=mime-version:from:date:message-id:subject:to;

bh=J4wOdPKBCGKDJu2gipRt6L/Ys5LW5rWG1r1oeQZ/Woo=;

b=dir909v+lNJ4mjzATO5fmgeXWdFzN6n+JNkPLtuxBcOeTF4JYYhMQR6s7JwN7k3/ou

67gPvacuG7ZZAn5v5aMv8TOI06XFCXv71CowSwfDz8rbF7B57RvoW5aog/vpy3s1/lPr

hMT9Kk3MULXbJQF48Qv/LbpMRsJDz1IizpgIxxrgDjZyKH4oWxZ1Lf0l2g4FGBjNv5I3

wHmQu/Ewgm040IsC4kGvXyFEKG2Yvw6U5BV1auM0UCZKKk/MuncvQcKAVmEnfUPUarsS

ioGBrncFJf4d2AEtGW18JXqnGNvfK2ZqB922hYLsxOcaMb6+tAWaXNUcBaym48xCgSpC

k+FQ==

X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;

d=1e100.net; s=20161025;

h=x-gm-message-state:mime-version:from:date:message-id:subject:to;

bh=J4wOdPKBCGKDJu2gipRt6L/Ys5LW5rWG1r1oeQZ/Woo=;

b=G7F+urifcvii9E+0NH7fn86HjxzcpLkDtU6VFW/grlFM7v17RsMdGjb7JfIHujJzy4

sCywy2zRTodm5/erlaYBpvPlHNDZzKIJzOS+Ti/giwuRDd7usuybQdEFE+9FU+zO3xiL

fwe2rSG0FsExe9LHR1arJaavE4oM12rKjC0BBuFgvcIyAnWEA3LIDK8BStXFD6F0OvvJ

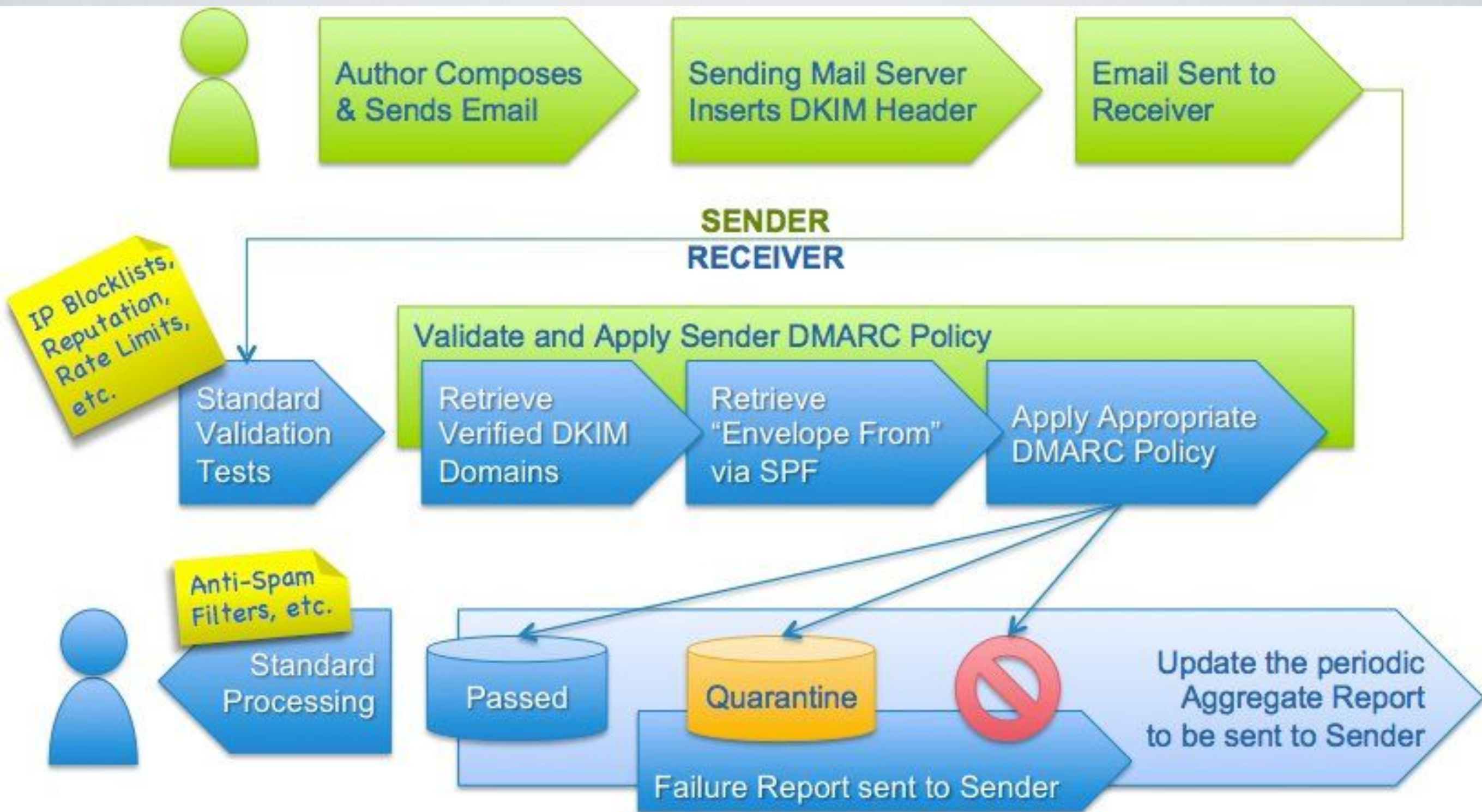
AftnZiR++4+zbBo0af9o1LMVBIcdQD/Y1Z4F56CZu3nsozlTraRbd7P7ihgES+4EUueh

gRjU02zfnIgXCR1XqG8UpLpDFNYN3KvNvxG96ppuNrxtVUM4Gfagc3s8LGfbSTNP/FQV

O8mQ==

DMARC - DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING & CONFORMANCE

- Builds on DKIM & SPF
- Ensures spoofed emails are blocked



<https://dmarc.org/overview>
w/

SETTING UP YOUR DOMAIN

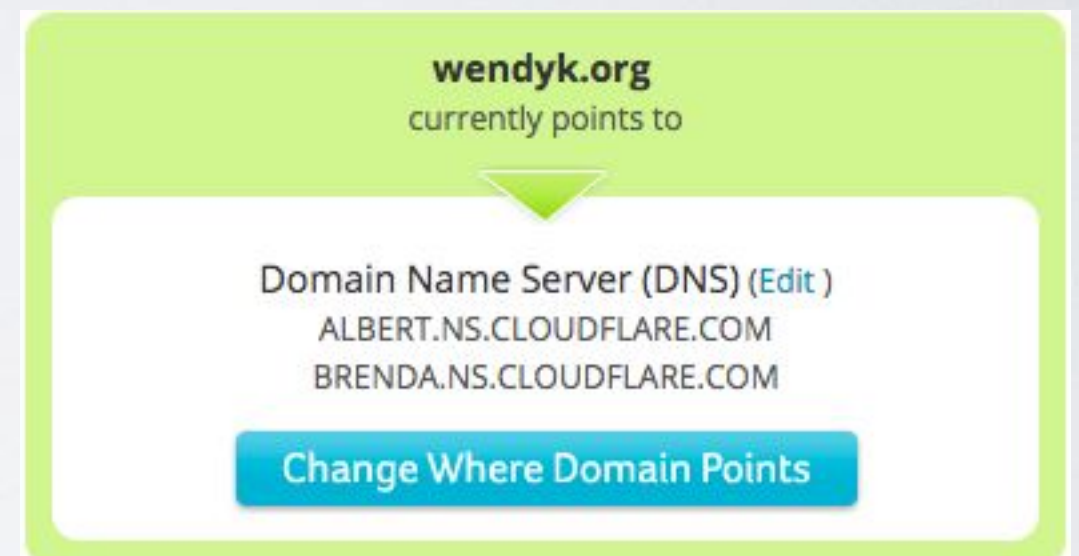
- If you're on GSuite:

<https://support.google.com/a/answer/174124?hl=en>

- <https://www.dmarcanalyzer.com/how-to-create-a-dmarc-record/>

SET UP NAME SERVERS

- If you're using Cloudflare, point to their DNS servers, and configure there



CLOUDFLARE FREE PLAN

- Once you're signed up on Cloudflare, we will add some DNS records
- We're going to make 3 TXT records to set up DMARC/DKIM/SPF

Subscription

[Manage your subscriptions](#)

Plan: Free Website

GENERATE DKIM PUBLIC KEYS

- This is will go into your DNS settings in a TXT record
- For GSuite, go to the admin dashboard, then Apps (in the left sidebar) > Gmail > Authenticate email

^ Authenticate email

The domains you select will use the DKIM (DomainKeys Identified Mail) protocol for authenticating outgoing emails. ?

wendyk.org



Status: **Authenticating email** ✓

You must update the DNS records for this domain.

To start authenticating email for the domain selected above, enter the following DNS TXT record into your domain provider's DNS settings page. Then click "Start authentication."

DNS Host name (TXT record name):

google._domainkey

TXT record value:

```
v=DKIM1; k=rsa;  
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAgWg2SDt7hAog9UKm8BQTs28Pq4BWK0jlL  
KXiP0nAnqfURMixf/IGMjJppOzbrCOCvW8gp0IN5udIGVZyFdpAbZa+Y+ubCS7n5cW+772pwgN15zFDDq  
FhDuEztKuibUwMC6Mdb0vBv9+sWqyqzOx5uf2OIrtljbcWiTX8I5bOfRRCU790Pjn8tYuadDSXBAu4Bp4N  
Diy2kSE1yh//sJde1IFwrQ2zTCLLxz+IZ2Ux49zrL5jRvkQwdb0NSu6iZwJNROQljpQXZ03yZFCNDOz2xJE  
OKMvpQiw9WJVxDO67Jbb3dy6f9R+1ksOe9gAJ7Za7eMjm2ROEv8CEs+cenRYBwIDAQAB
```

[Generate new record](#)

Note: It may take up to 48 hours for DNS changes to fully propagate.

[STOP AUTHENTICATION](#)

CREATE TXT RECORD

- Name of the TXT record will be “google._domainkey”
- Value will be the full contents of the string that starts with “v=DKIM1; k=rsa; p=.....”

Manage your Domain Name System (DNS) settings

DNS Records

A, AAAA, and CNAME records can have their traffic routed through the Cloudflare system. Add more records using this form, and click the cloud next to each record to toggle Cloudflare on or off.

TXT



Name

Click to configure

Automatic TTL



Add Record

CLOUDFLARE DNS ENTRY

Select TXT from the dropdown

DKIM DNS ENTRY ON CLOUDFLARE

TXT google._domainkey v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BA... Automatic



Legend

The DKIM legend lists all supported tags with their default values and short explanation. Refer to [RFC6376](#) for more in depth information. As the RFC states any unsupported tags MAY be present and MUST be ignored.

Tag	Name	Default	Translation
v	Version	DKIM1	Version of the DKIM key record (plain-text; RECOMMENDED). This tag MUST be the first tag in the record if present. Warning: some ISPs may mark the DKIM authentication check as neutral if the version tag is invalid.
h	Hash algorithms	* (allow all)	Acceptable hash algorithms (plain-text; OPTIONAL). A colon-separated list of hash algorithms that might be used. Unrecognized algorithms MUST be ignored. The currently recognized algorithms are "sha1" and "sha256".
k	Key type	rsa	Key type (plain-text; OPTIONAL). Unrecognized key types MUST be ignored. Currently only "rsa" is recognized.
n	Notes	(empty)	Notes that might be of interest to a human (OPTIONAL). Not interpreted in any way.
p	Public key	(none)	Public-key data (base64; REQUIRED). An empty value means that this public key has been revoked. This is the only required tag.
s	Service type	* (allow all)	Service Type (plain-text; OPTIONAL). A colon-separated list of service types to which this record applies. Unrecognized service types MUST be ignored. Currently only "email" is recognized.
t	Flags	(no flags set)	Flags (plain-text; OPTIONAL). A colon-separated list of names. Unrecognized flags MUST be ignored. The defined flags are as follows: "y" - this domain is testing DKIM (test mode) "s" - verifiers MUST check for domain alignment (strict mode)

DKIM TAGS

<https://us.dmarcian.com/dkim-inspector/>

ENTER SPF SETTINGS

TXT

wendyk.org

v=spf1 include:_spf.google.com ~all

Create an SPF record for your domain:

<https://support.google.com/a/answer/33786?hl=en>

**NOW WE'RE READY TO SET
UP DMARC DOMAIN KEYS**

SIGN UP FOR DMARCIAN



[Why DMARC?](#) [Solutions](#) [Pricing](#) [Tools](#) [News & Knowledge](#) [About](#)

Choose your region



Americas

Register on our American instance of dmarcian.

[SIGN UP FREE](#)



Europe/Africa/Russia

European data stays within Europe to fully comply with data protection regulations.

[SIGN UP FREE](#)



APAC

Register on our Asia-Pacific instance of dmarcian.

[SIGN UP FREE](#)

<https://dmarcian.com/register>

/



Add Domains

Add DMARC

Get Compliant

Publish Policy

Add DMARC data

To begin collecting DMARC data, publish the following DMARC record for your domain:

```
v=DMARC1; p=none; rua=mailto:d1tp3aec@ag.dmarcian.com;
```

Publish this as a TXT record located at `_dmarc`. You can use the same DMARC record for all of your domains.

Once you publish DMARC records, you should begin to see data within two or three days for active sending domains.

For more information about publishing DMARC records, visit [How to publish a DMARC record](#).

ADD DMARC SECTION

DMARC OPTIONS

Tag Name	Purpose	Sample
v	Protocol version	v=DMARC1
pct	Percentage of messages subjected to filtering	pct=20
ruf	Reporting URI for forensic reports	ruf=mailto:authfail@example.com
rua	Reporting URI of aggregate reports	rua=mailto:aggrep@example.com
p	Policy for organizational domain	p=quarantine
sp	Policy for subdomains of the OD	sp=reject
adkim	Alignment mode for DKIM	adkim=s
aspf	Alignment mode for SPF	aspf=r

Edit Record: TXT content



v=DMARC1; p=reject; sp=reject; aspf=r;
rua=mailto:ditp3aec@ag.dmarcian.com

Content

v=DMARC1; p=reject; sp=reject; aspf=r;
rua=mailto:ditp3aec@ag.dmarcian.com

Cancel

Save

POLICY SETTINGS

- Directions: <https://dmarcian.com/start-dmarc/>
- Start with p=none - this will give you reporting with no action taken on emails. Important so you don't block all **your** emails
- once that works, move to p=quarantine
- Can then move to p=reject

REPORTING DMARC DATA

- This is where reports of failures are sent. Can be any valid email address.
- If we send reporting to a DMarcian email, will show up in your DMarcian account
- rua=<mailto:ditp3aec@ag.dmarcian.com>

This is complicated! How do I build this string?

<https://dmarcian.com/dmarc-record-wizard/>

DMARC Record Wizard

Step 2/7

14%

What type of DMARC policy do you want?

DMARC allows you to apply different "policies" to email that appears unaligned with your domain. When first publishing your record, we suggest you start with "none". This allows you to collect data without affecting your email streams.

How do you want to treat mail that fails the DMARC check?

- ☒ Nothing yet, just collect data.
- ☐ Quarantine it for further analysis.
- ☐ Reject it outright.

Previous

Next

VIEWING YOUR DMARC REPORTS

REPORTS

- You could provide your own email in the “rua” tag to receive reports & crunch your own graphs....
- Or we can send reports to DMarcian and use their tools.
You can see reports on DMarcian’s Monitor tab
 - Sources shows where email sent with your domain is from
 - Threat/Unknown are emails from servers that don’t match your SPF/DKIM settings

Domain Overview

↔ 1
active domains

📁 0
inactive domains

7 Day Volume

10
DMARC Capable

0
Forwarded

36
Unknown

🔧 0
issues

📌 0
tasks


📊 Volume Details

👤 1
Identified sources

Source	DMARC Compliance
Google, Inc.	100.0%

View Source Details

⚠️ 36
Threat/Unknown Messages



0 Selected

Select Action

Go

export all as CSV

+ Add Domains

Domains

Issues (0)Tasks (0)

Show 10 entries

Search:

Column visibility

	Domain	DMARC	SPF state	DKIM state	Volume (7 days)
<input type="checkbox"/>	wendyk.org	☑ p=reject	☑ Good [-all]	☑ Good	<div></div>

Showing 1 to 1 of 1 entries

FirstPrevious1NextLast

[Add Domains](#)[Add DMARC](#)[Get Compliant](#)[Publish Policy](#)[Monitor](#)

Get Compliant

Once you have DMARC data for your domains, start getting DMARC capable sources of email into compliance with DMARC.

To view more about your sources of email and related DKIM & SPF compliance information, use the [Source Viewer](#).

Top sources & compliance by volume

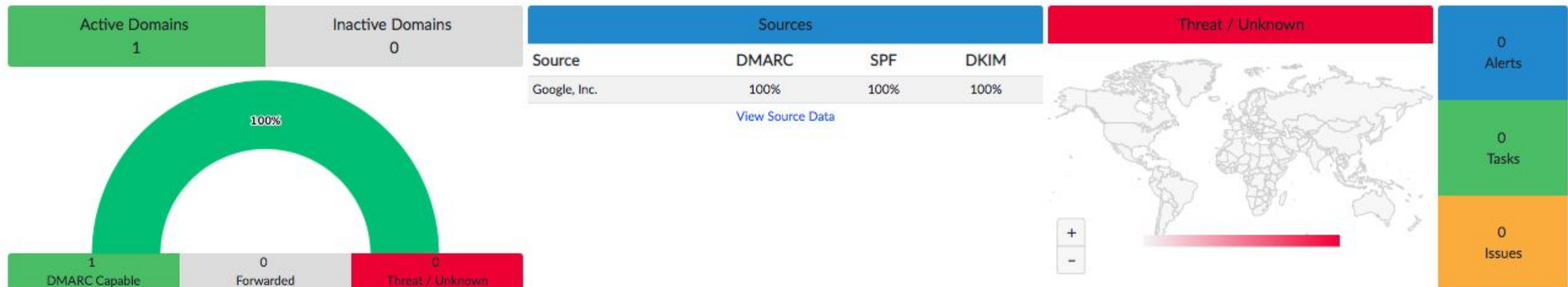
Source	DMARC	SPF	DKIM
Google, Inc.	100	100	100

dmarcian's mission – help people deploy DMARC

Domain Overview

Summary

7 Day Summary



Domain Groups

Click cells for details

Selected Domains...



Go

0 domains selected

Export as CSV

Add Domains

Domains:

▼ 1 selected

From:

2018-04-28

Compliance Filter: ?

None ▼

Recalculate

To:

2018-05-05

Providers:

google.com ▼

DMARC Capable

Non-compliant Sources

Forwarders

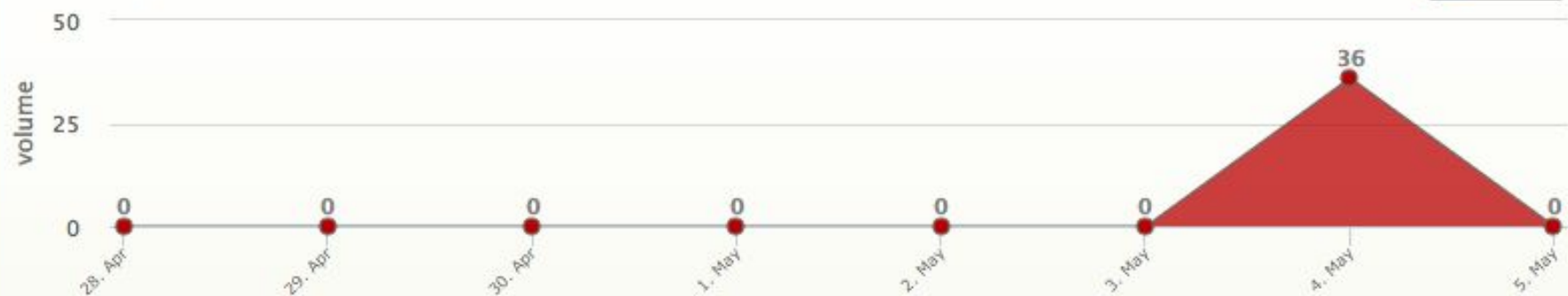
Threat/Unknown

Export All as CSV

Threat/Unknown sources are either fraudulent or need to be identified as legitimate. To help dmarcian identify unknown sources, click the ⓘ icon next to the source to provide more information.



Policy applied to Threat/Unknown emails:



source

volume

DMARC compliance



Other Servers

36

100% Reject

Other Servers

source

volume

DMARC compliance

36

100% Reject

Reject Policy Applying To 36 of 36 messages.

Show 10 entries

Search:

Server Name	From: domain count	Message count	IP count	DMARC Compliance
*.nxdomain	1	19	19	0% (SPF: 0%, DKIM: 0%)

Show 10 entries

Search:

Column visibility

From: Domain	IP	PTR	Country	Messages	Policy Applied	Override Reason	DKIM			SPF			As Received By
							DMARC	Raw	d=	DMARC	Raw	Domain	
wendyk.org	91.187.122.28	nxdomain		1	Reject	none	fail	none	none	fail	softfail	wendyk.org	google.com
wendyk.org	39.44.242.212	nxdomain		1	Reject	none	fail	none	none	fail	softfail	wendyk.org	google.com
wendyk.org	91.187.109.16	nxdomain		1	Reject	none	fail	none	none	fail	softfail	wendyk.org	google.com
wendyk.org	109.166.169.113	nxdomain		1	Reject	none	fail	none	none	fail	softfail	wendyk.org	google.com
wendyk.org	123.23.93.11	nxdomain		1	Reject	none	fail	none	none	fail	softfail	wendyk.org	google.com
wendyk.org	203.189.159.169	nxdomain		1	Reject	none	fail	none	none	fail	softfail	wendyk.org	google.com
wendyk.org	89.44.11.66	nxdomain		1	Reject	none	fail	none	none	fail	softfail	wendyk.org	google.com
wendyk.org	191.240.191.72	nxdomain		1	Reject	none	fail	none	none	fail	softfail	wendyk.org	google.com
wendyk.org	203.189.131.209	nxdomain		1	Reject	none	fail	none	none	fail	softfail	wendyk.org	google.com
wendyk.org	94.248.93.232	nxdomain		1	Reject	none	fail	none	none	fail	softfail	wendyk.org	google.com

Showing 1 to 10 of 19 entries

First

Previous

1

2

Next

Last

*.airtelbroadband.in

1

3

3

0% (SPF: 0%, DKIM: 0%)

*.servfail

1

3

3

0% (SPF: 0%, DKIM: 0%)

*.vnpt.vn

1

2

2

0% (SPF: 0%, DKIM: 0%)

*.airtel.in

1

1

1

0% (SPF: 0%, DKIM: 0%)

*.rafinsatellite.net

1

1

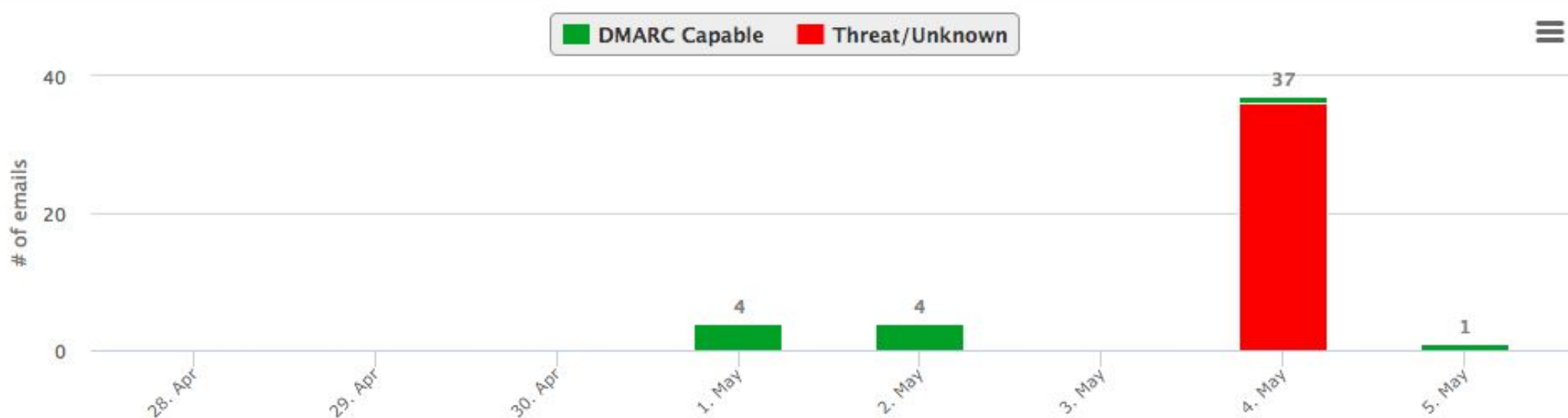
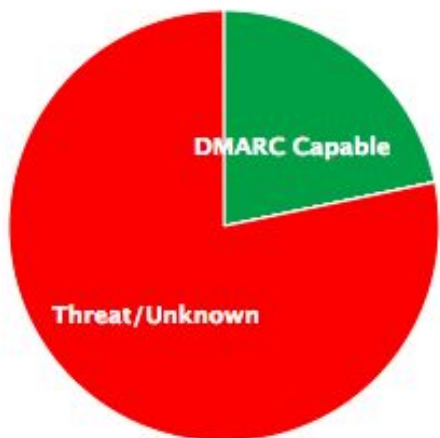
1

0% (SPF: 0%, DKIM: 0%)

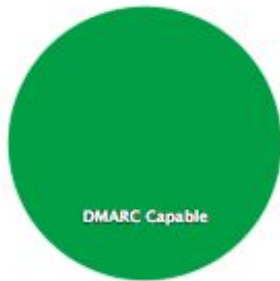
Detail Viewer

Domains	From	Filter:
wendyk.org	2018-04-28	None
Providers	To	Scale:
google.com	2018-05-05	Logarithmic

Email Volume by Category



Email Volume by Category



DMARC Capable Non-compliant sources Forwarders Threat/Unknown

Export All as CSV

DMARC Capable can send DMARC compliant email. Technical staff can attend to your organization's servers. External emailers listed here can send DMARC compliant email.

DMARC Capable by Email Volume



	Source	Volume	DMARC Compliance		
+	Google, Inc.	2	100%	SPF 100%	DKIM 100%

TROUBLESHOOTING

- DMarcian's Issues tab under "Monitor" is very helpful

Domains	Tasks (0)	Issues (0)
		Show: Active Ignored Hide Subdomains: No Yes
Domain	Issue	Action details Ignore
No Issues		

**IF YOU RUN
YOUR OWN MAIL SERVER**

MTA STRICT TRANSPORT SECURITY (MTA-STS)

- Allows domains to require authentication and TLS encryption for SMTP

START-TLS

- Allows your mail server to protect against downgrades
- <https://starttls-everywhere.org/>
 - Creating a list of email servers that use TLS

MORE RESOURCES

- <https://www.ftc.gov/news-events/blogs/business-blog/2017/03/want-stop-phishers-use-email-authentication>
- <https://blog.returnpath.com/how-to-explain-spf-in-plain-english/>
- <https://blog.returnpath.com/how-to-explain-dkim-in-plain-english-2/>
- <https://blog.returnpath.com/how-to-explain-dmarc-in-plain-english/>
- <https://zakird.com/papers/mail.pdf>