

Neue Anforderungen von Google & Yahoo!

So kommen Mailings auch nach dem 1.2.2024 noch an

Background Story

- On October 3, 2023 Google and Yahoo both announced new requirements including mandatory email authentication (SPF and DKIM) for sending email to Gmail and Yahoo users. The new requirements go into effect in February 2024 and could have a significant impact on businesses that have not implemented email authentication.
- The requirements were presented at 2 levels; non-bulk senders and bulk senders, with additional DMARC requirements for bulk senders (defined as anyone that sends 5,000 or more messages to their users in a single day).
- Although not confirmed , we are making the assumption that this will be quantified per sending domain and not specific to Sending IP addresses on all emails , both Machine generated application email and emails sent from individual senders will be counted.

Umfrage 1 – Mailingaufkommen?!



Google & Yahoo Requirements for Senders

<5,000 per day

- SPF or DKIM email authentication required
- Ensure valid forward and reverse DNS records
- Spam rates reported in [Postmaster Tools](#) below 0.3%
- Message format adheres to [RFC 5322](#) standard
- No Gmail Impersonation in FROM headers (Gmail setting DMARC Quarantine policy)
- Email Forwarding requirements

>5,000 per day

- SPF **and** DKIM email authentication required
- Ensure valid forward and reverse DNS records
- Spam rates reported in [Postmaster Tools](#) below 0.3%
- Message format adheres to [RFC 5322](#) standard
- No Gmail Impersonation in FROM headers (Gmail setting DMARC Quarantine policy)
- Email Forwarding requirements
- **DMARC** email authentication for your sending domains
- From: header must be aligned with either the SPF domain or the DKIM domain
- One-click unsubscribe for subscribed messages

DKIM ,SPF ,DMARC – What are these?

What?	How?	Why?
DKIM <small>(since 2007)</small>	email authentication standard that works by assigning a digital signature to messages sent from (outbound) an email account.	helps protect email senders and recipients from spam, spoofing, and phishing
SPF <small>(since 2003)</small>	Each domain lists in one DNS record the list of servers that are allowed to send emails for that domain. As owner of a given domain, you will tell the world which servers you will send emails from. That is typically your SMTP server.	when an email provider like Gmail sees an email sent from an address @example.com but coming from a server not listed in the SPF record, it knows it is likely spam , non legitimate and Spoofed
DMARC <small>(since 2015)</small>	DMARC's alignment feature prevents spoofing of the "header from" address by: Matching the "header from" domain name with the "envelope from" domain name used during an SPF check, and Matching the "header from" domain name with the "d= domain name" in the DKIM signature.	DMARC ensures that legitimate email is properly authenticating against established DKIM and SPF standards, and that fraudulent activity appearing to come from domains under the organization's control (active sending domains, non-sending domains, and defensively registered domains) is blocked. Two key values of DMARC are domain alignment and reporting.

Panic Panic Do I need to Panic

(What is required to address this new rule?)



Can you answer the following questions?

- Are we ok or do we need to do something?
- Do we understand the scope of the work?
- Are we adequately resourced ?
- Do we have the time ?

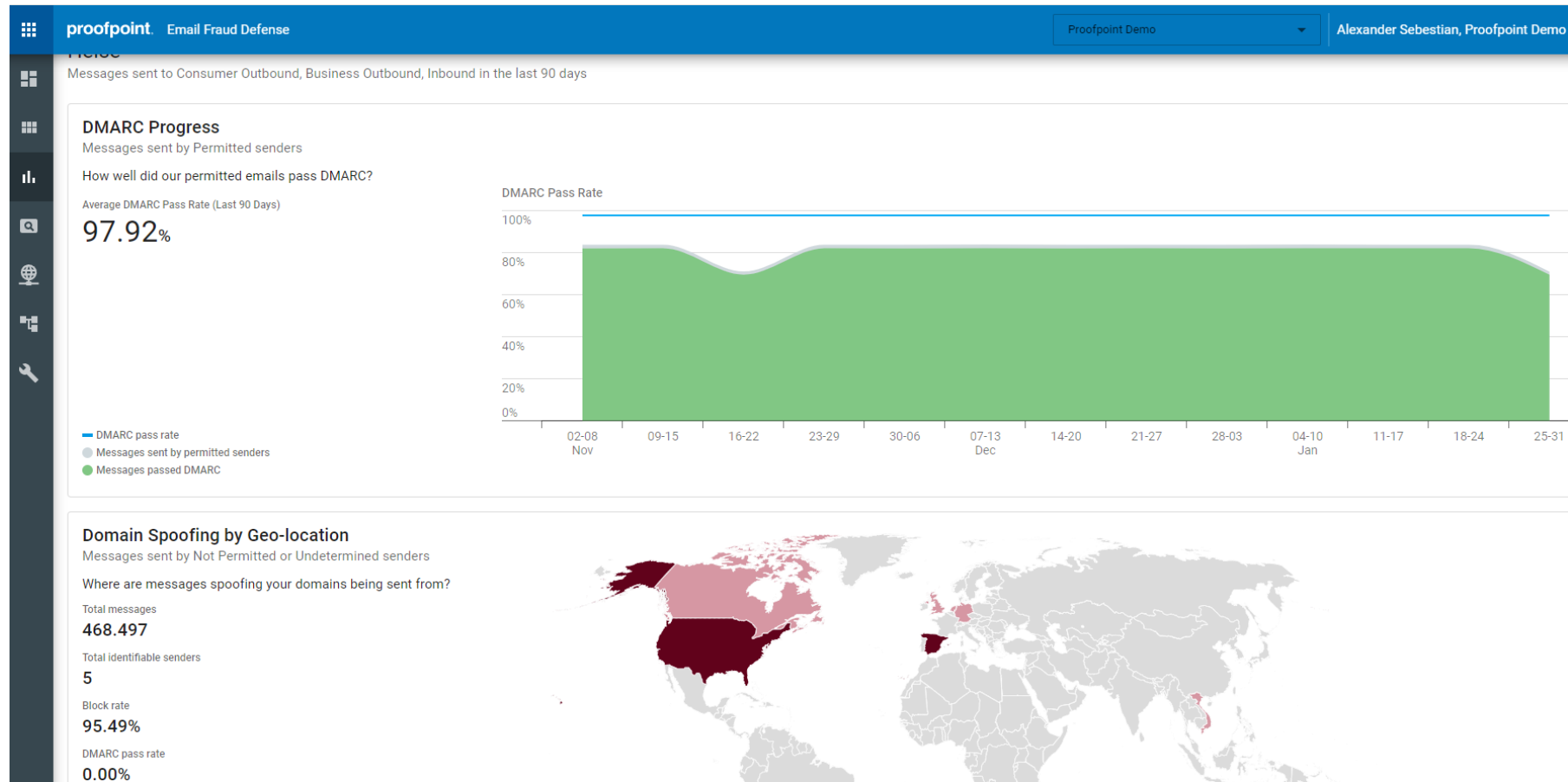
Umfrage 2 – Are you ready?!



How Proofpoint can help customers prepare:

- Proofpoint has 2 solutions that can help customers protect the deliverability of email to Gmail and Yahoo accounts.
- **Email Fraud Defense (EFD):**
 - Non-Bulk Senders – EFD provides hosted SPF and DKIM capabilities that could help simplify the management of a company's email authentication.
 - Bulk Senders – In addition to our Hosted SPF and Hosted DKIM capabilities, EFD helps companies enable DMARC and get the critical alignment that is being required by Google and Yahoo starting Feb 2024. With such a short window, our highly experienced EFD consultants will be of high value for companies that are racing to meet the mandates.
- **Secure Email Relay (SER):**
 - Bulk Senders – Applications often create the high volume that puts customers into the “bulk sender” category. If these applications do not support DKIM, they will not be able to meet the requirements and all these critical messages will be blocked or sent to SPAM folders. SER provides a simple, and fast solution to ensure DIM signing and DMARC alignment.

Live Demo – EFD Portal



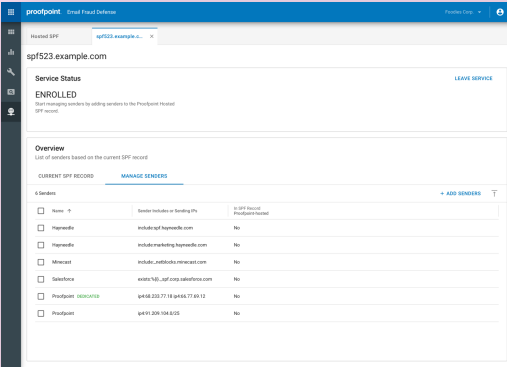
How can Proofpoint help ?

Requirements	<5,000 per day		>5,000 per day	
	EFD	SER	EFD	SER
SPF or DKIM email authentication required	✓	✓		
SPF and DKIM email authentication required			✓	✓
DMARC email authentication for your sending domains (we provide full visibility and Managed Service to assist)	✓	✓	✓	✓
From: header must be aligned with either the SPF domain or the DKIM domain (we provide visibility and Managed Service to assist)	✓	✓	✓	✓

Note - alignment is where the authentication check is performed against a record which is stored within DNS for the same domain that the email appears to come from

SPF Services

Hosted SPF



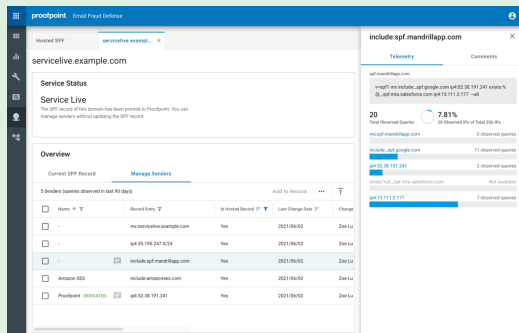
Improved efficiency

- Overcomes the DNS lookup limit of 10
- Reduces overhead of making SPF updates
- Real-time propagation

Better security

- Obfuscates senders published in your SPF record
- Simplifies SPF record by identifying authorized but unused IP addresses

SPF Telemetry



Activity Insights

- Provides total visibility of authorized sending IPs
- Enables customers to see which IPs are actively sending and which are not

Educated Actions

- Builds confidence in determining which SPF entries can be removed (no longer active)
- Removing inactive sending IPs can help lower a company's overall security risk

Hosted DKIM Service

- **Improved efficiency**

- Simplifies configuration and management of DKIM selectors and keys
- Provides flexible DKIM selector hosting options (delegated or non-delegated)
- Allows simple import of DKIM selects and public keys
- Geographically distributed and fault tolerant services

- **Better security**

- Accelerates DMARC enforcement
- Facilitates key rotation
- Supports DNSSEC

The screenshot shows the 'Hosted DKIM' management page in the Proofpoint Email Fraud Defense console. The page has a blue header with the Proofpoint logo, 'Email Fraud Defense', a 'Switch to Legacy' button, and a dropdown menu for 'Foodies Corporation'. A sidebar on the left contains navigation icons. The main content area is titled 'Hosted DKIM' and includes an 'Enroll Domain' button. Below the title, it says '3 domains' and displays a table with columns for Domain, Type, Enrollment Date, Status, Last Service Change, Selectors, DNSSEC, and Hosting Type. The table contains three rows of data for the foodies.com domain.

Domain	Type	Enrollment Date	Status	Last Service Change	Selectors	DNSSEC	Hosting Type
foodies.com	Sending	YYYY/MM/DD	Enrolled	YYYY/MM/DD	n/a	On	Delegated
reply.foodies.com	Sending	YYYY/MM/DD	Service live	YYYY/MM/DD	1	Off	Non-delegated
em.foodies.com	Non-sending	YYYY/MM/DD	Not enrolled	YYYY/MM/DD	3	On	Delegated

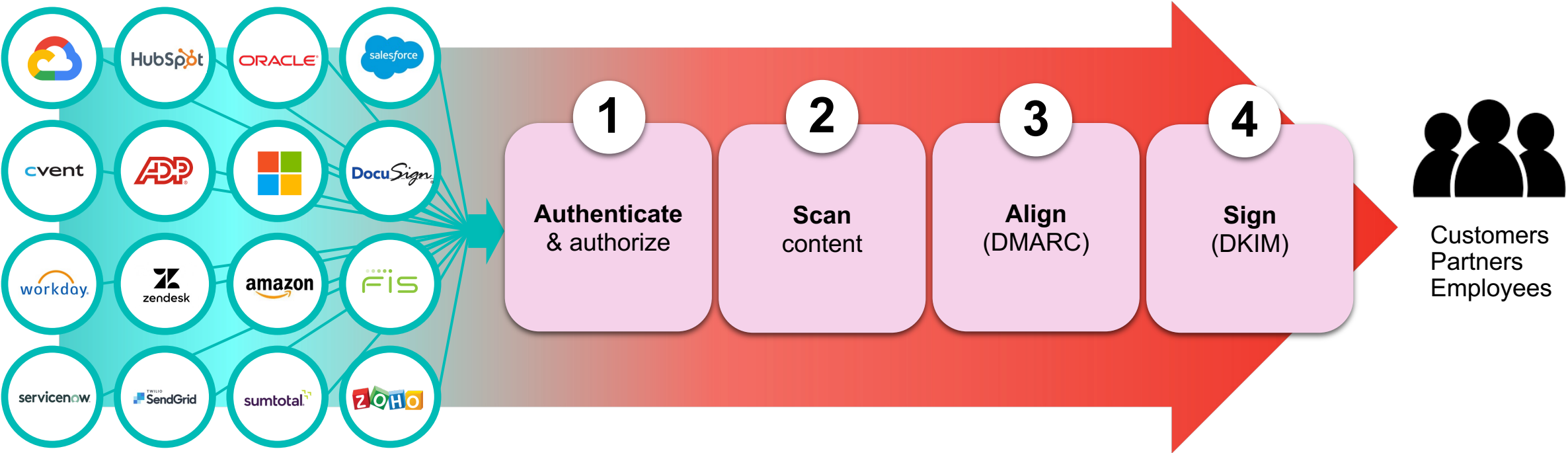
Secure Email Relay Service (for application email)



Non-DMARC compliant application email



Secure, compliant application email

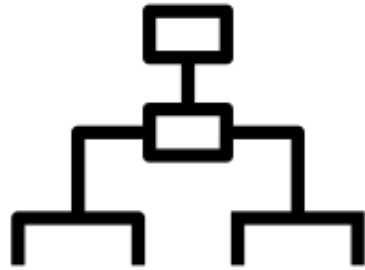


Dynamically Identify Lookalike Domains



SCAN

Continually scan over 400 million domains for threats



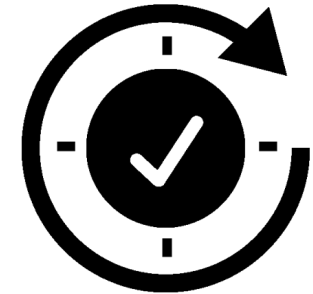
CLASSIFY

Automatically classify domains and identify potential BEC domains



INVESTIGATE

Provide detailed intel around registrant info, email traffic, web content; achieve workflow flexibility



RESPOND

- Add to block list
- Limit access
- Permanently remove via Virtual Takedown add-on

Key Messaging Points:

- Your business could be greatly impacted by the new requirements from Google and Yahoo
- There is a short window to get ready for these changes
- Proofpoint is the industry leader for email authentication
- We can help provide an Assessment to identify your gaps
- Proofpoint has the knowledge and solutions to close the gap

proofpoint®