MIS|TI™ PRESENTS
InfoSecWorld
Conference & Expo 2018

SHOULD YOU IMPLEMENT DMARC FOR SAFER EMAIL?

Greg Arnette
Data Protection CTO
@gregarnette

WHAT YOU’LL LEARN TODAY

Why email authentication matters

Evolution of email authentication

What is DMARC and why should you care?

DMARC deep dive

Deploying DMARC for your domain

LEGITIMATE OR NOT?

It says it's from BigBank

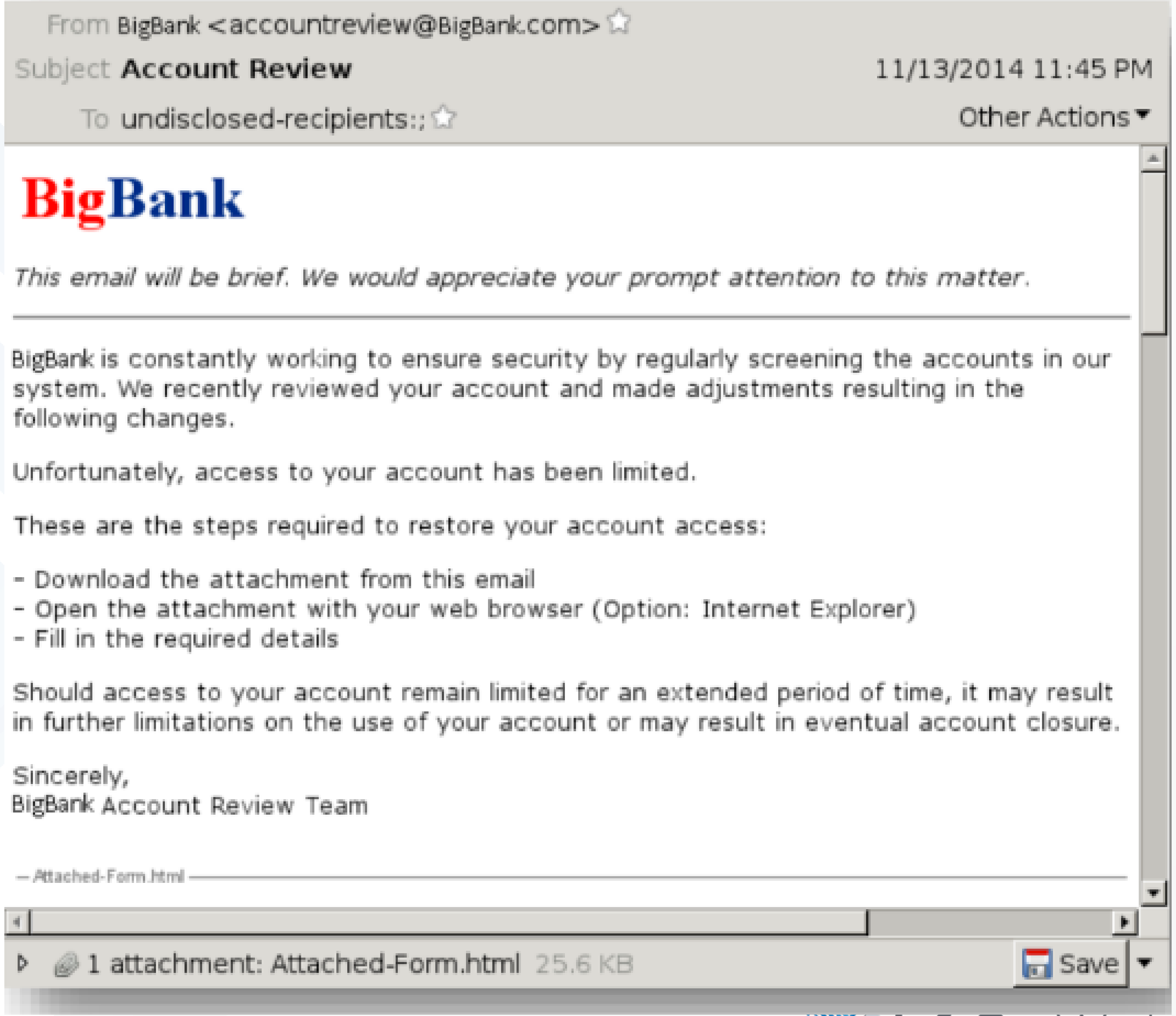
It shows the BigBank logo

It shows the BigBank address

It looks legitimate

I have a BigBank account

I don't want my BigBank account to close



From BigBank <accountreview@BigBank.com>

Subject **Account Review** 11/13/2014 11:45 PM

To undisclosed-recipients:;

This email will be brief. We would appreciate your prompt attention to this matter.

BigBank is constantly working to ensure security by regularly screening the accounts in our system. We recently reviewed your account and made adjustments resulting in the following changes.

Unfortunately, access to your account has been limited.

These are the steps required to restore your account access:

- Download the attachment from this email
- Open the attachment with your web browser (Option: Internet Explorer)
- Fill in the required details

Should access to your account remain limited for an extended period of time, it may result in further limitations on the use of your account or may result in eventual account closure.

Sincerely,
BigBank Account Review Team

— Attached-Form.html

1 attachment: Attached-Form.html 25.6 KB

EMAIL AUTHENTICATION

Email Au-then-ti-ca-tion: [ôˌTHen(t)iˈkāSH(ə)n/]

the process or action of verifying the identity or origin of an email

LACK OF EMAIL AUTHENTICATION EXPOSES YOUR DOMAIN TO SPOOFING

Attacks on company employees

- Hacker sends an email FROM “CEO@yourcompany.com” with a REPLY TO “notyourCEO@gmail.com”

Attacks on customers, vendors, partners

- Hacker sends an email with malicious content FROM aperson@yourcompany.com

SPEAR PHISHING IS A GROWING THREAT

$5B

Losses from spear phishing

FBI

2,370%

Increase from 2015-2016

FBI

DMARC IS THE ONLY WAY TO PROTECT YOUR ORGANIZATION AND YOUR BRAND

DMARC IS THE EVOLUTION OF EMAIL SECURITY

2003 – SPF
Sender Policy Framework
www.openspf.org

2007 – DKIM

Domain Keys Identified Message

www.opendkim.org

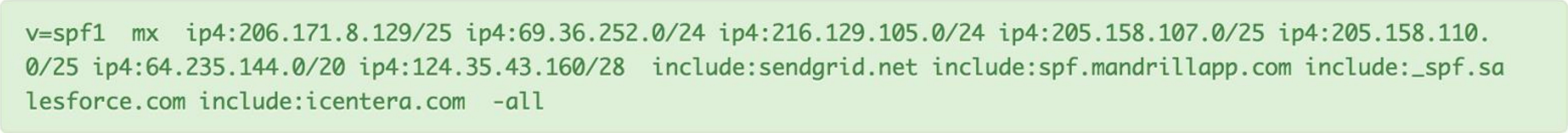
2012 – DMARC

Domain-based Message Authentication, Reporting, and Conformance

www.dmarc.org

SPF USES IP WHITELISTS FOR AUTHENTICATION

DNS entry defines which IPs are authorized to send emails on behalf of the domain



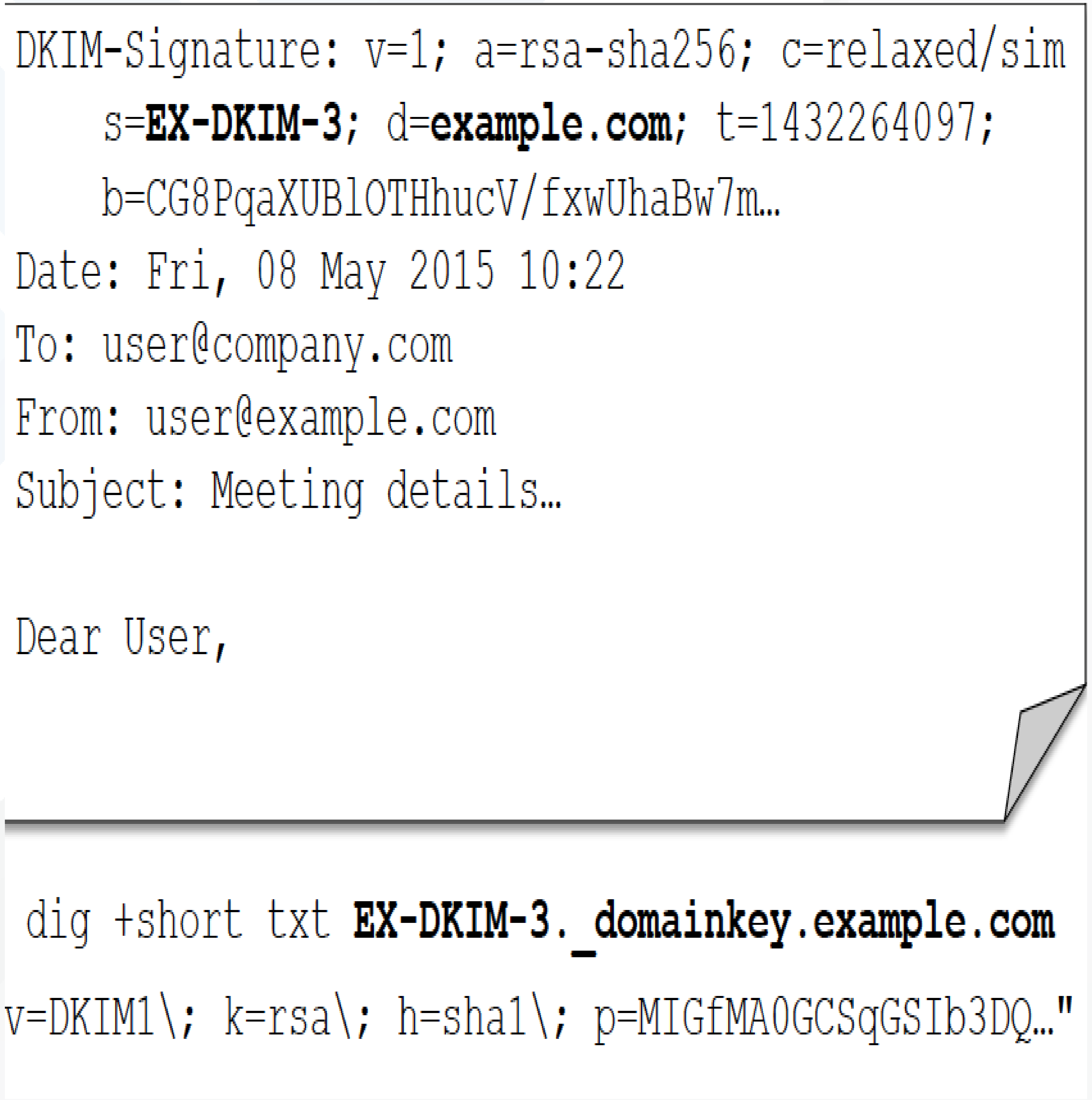
```
v=spf1  mx  ip4:206.171.8.129/25 ip4:69.36.252.0/24 ip4:216.129.105.0/24 ip4:205.158.107.0/25 ip4:205.158.110.
0/25 ip4:64.235.144.0/20 ip4:124.35.43.160/28  include:sendgrid.net include:spf.mandrillapp.com include:_spf.sa
lesforce.com include:icentera.com  -all
```

DKIM USES SIGNATURES FOR AUTHENTICATION

Sender signs message with a private cryptographic key

Public key is published as DNS record on the domain

Recipient uses public key to authenticate the message



```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/sim
    s=EX-DKIM-3; d=example.com; t=1432264097;
    b=CG8PqaXUBlOTHhucV/fxwUhaBw7m…
Date: Fri, 08 May 2015 10:22
To: user@company.com
From: user@example.com
Subject: Meeting details…

Dear User,
```

```
dig +short txt EX-DKIM-3._domainkey.example.com
v=DKIM1\; k=rsa\; h=sha1\; p=MIGfMA0GCSqGSIb3DQ…"
```

SPF/DKIM ARE INSUFFICIENT

SPF/DKIM do not cover all use cases, e.g.:

- SPF: forwarding and mailing lists
- DKIM: emails modified by mailing lists and gateways

Admins do not have visibility into misconfigurations

↓

Email recipients experience false positives

↓

Email recipients do not consistently respect SPF/DKIM

HOW DMARC WORKS

Sender publishes DNS entry on the domain

- Lets recipients know how to handle SPF/DKIM failures
- Makes recipients send feedback to sender about failures

Recipients use SPF/DKIM to authenticate and DMARC to determine how to handle unauthenticated emails

- Most email recipients enforce DMARC, e.g., Office 365, Gmail, G Suite, AOL, Exchange

DMARC IS A UNIFIED FRAMEWORK

Admin gets visibility into senders using her domain

- Put control back in admin’s hands

Helps fix misconfigurations

- Builds confidence in correctness of SPF/DKIM setup
- Enhance email deliverability

Communicates unauthenticated email policy to recipients

- Demonstrates the sender’s configuration is trustworthy

Leverages both DKIM and SPF

- Best of both worlds

CLOUD EMAIL POLL

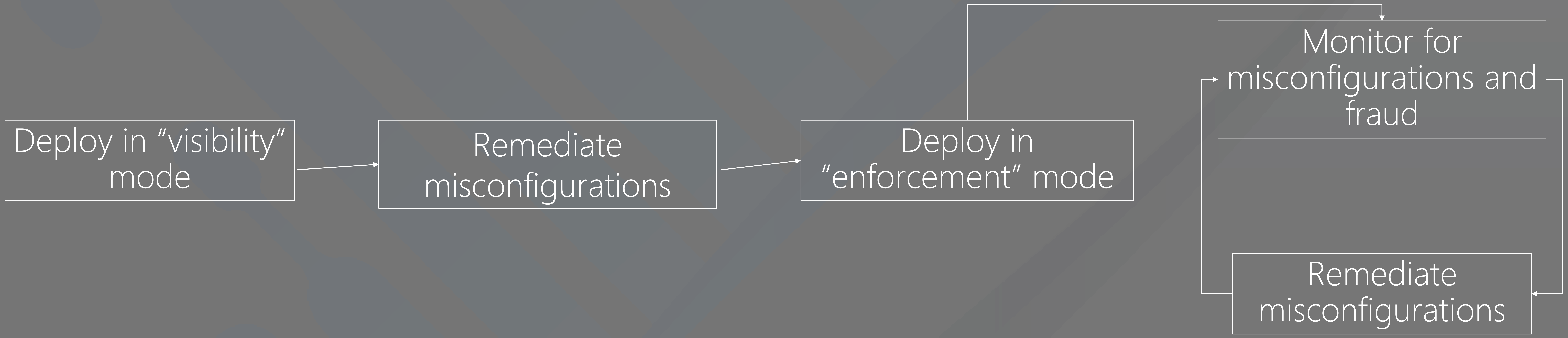
YOU MUST DEPLOY DMARC FOR OFFICE 365 TO PROTECT YOUR DOMAIN

Office 365 protects domains that have deployed DMARC, e.g., bankofamerica.com

- Evaluate SPF/DKIM/DMARC for inbound emails
- Send DMARC feedback

Office 365 does not deploy DMARC for your domain

HOW TO SAFELY DEPLOY DMARC FOR YOUR DOMAIN



Deploy in "visibility" mode

Remediate misconfigurations

Deploy in "enforcement" mode

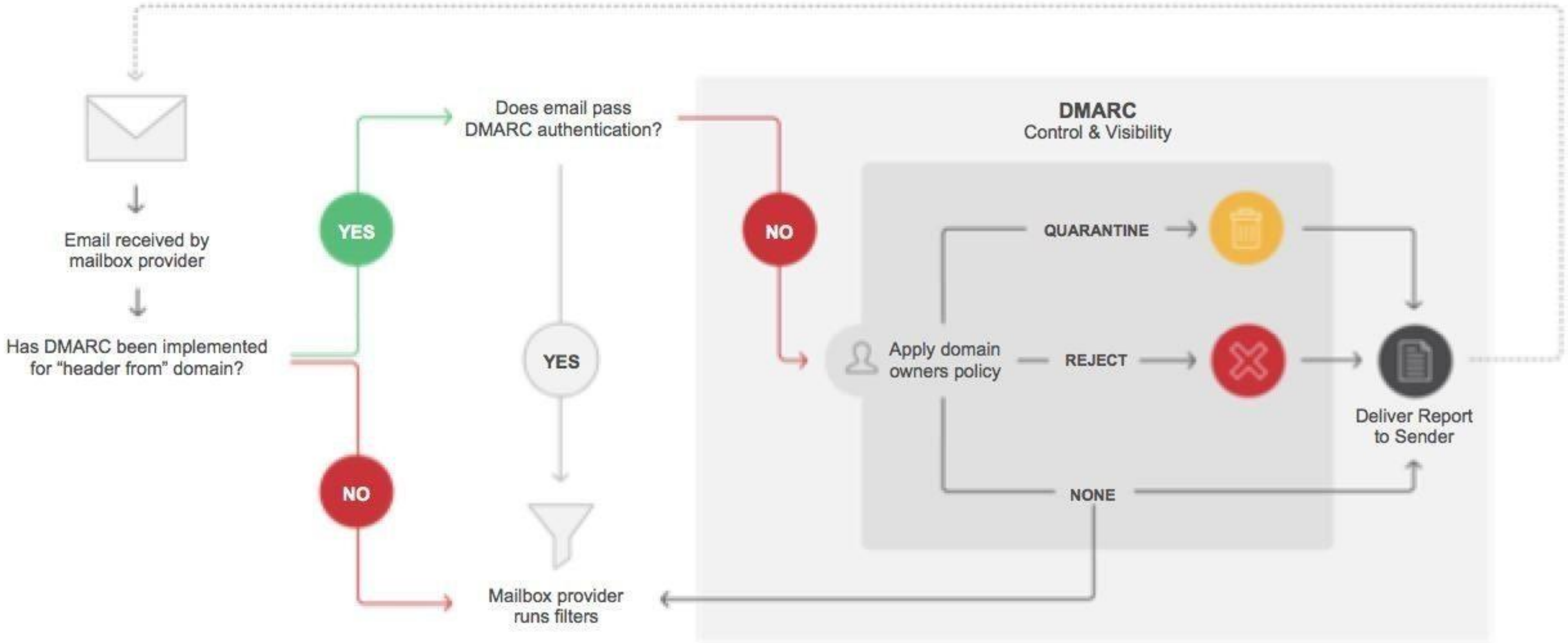
Monitor for misconfigurations and fraud

Remediate misconfigurations

5 EASY STEPS FOR SUCCESS

1. Correctly implement DKIM and SPF protocol.
2. Create a DMARC record in your DNS and start monitoring a domain to see where email traffic using that domain is coming from.
3. Set mail receiver policy to “none” to receive DMARC data reports while ensuring messages are still being delivered.
4. Analyze the breadth of data provided in the DMARC reports to make informed decisions about the organization’s communications system.
5. And finally, as you gain experience with DMARC, consider modifying your DMARC policy flags from “none” to “quarantine” or “reject”. This moves from monitoring mode to proactive protection.

How DMARC Works

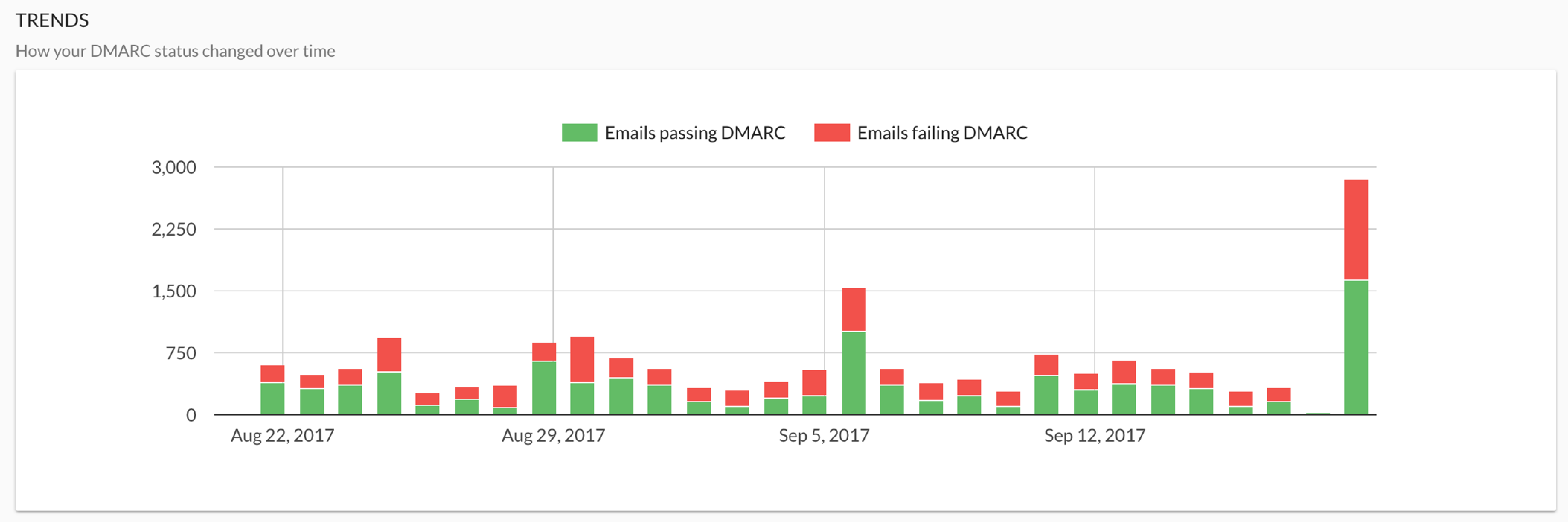

Email received by mailbox provider
Has DMARC been implemented for “header from” domain?
YES
NO
Does email pass DMARC authentication?
YES
NO
Mailbox provider runs filters
DMARC
Control & Visibility
Apply domain owners policy
QUARANTINE
REJECT
NONE
Deliver Report to Sender

LESSONS LEARNED FROM REAL-WORLD DMARC

- 75% of email traffic uses SPF / DKIM
- 25% uses nothing
- 25% is where phishing happens = the “Swiss cheese”
- DMARC = spf + dkim
- Small webmail hosts don’t want to incur the processing / expense to process the DMARC analysis

WHAT CAN YOU DO ABOUT IT?

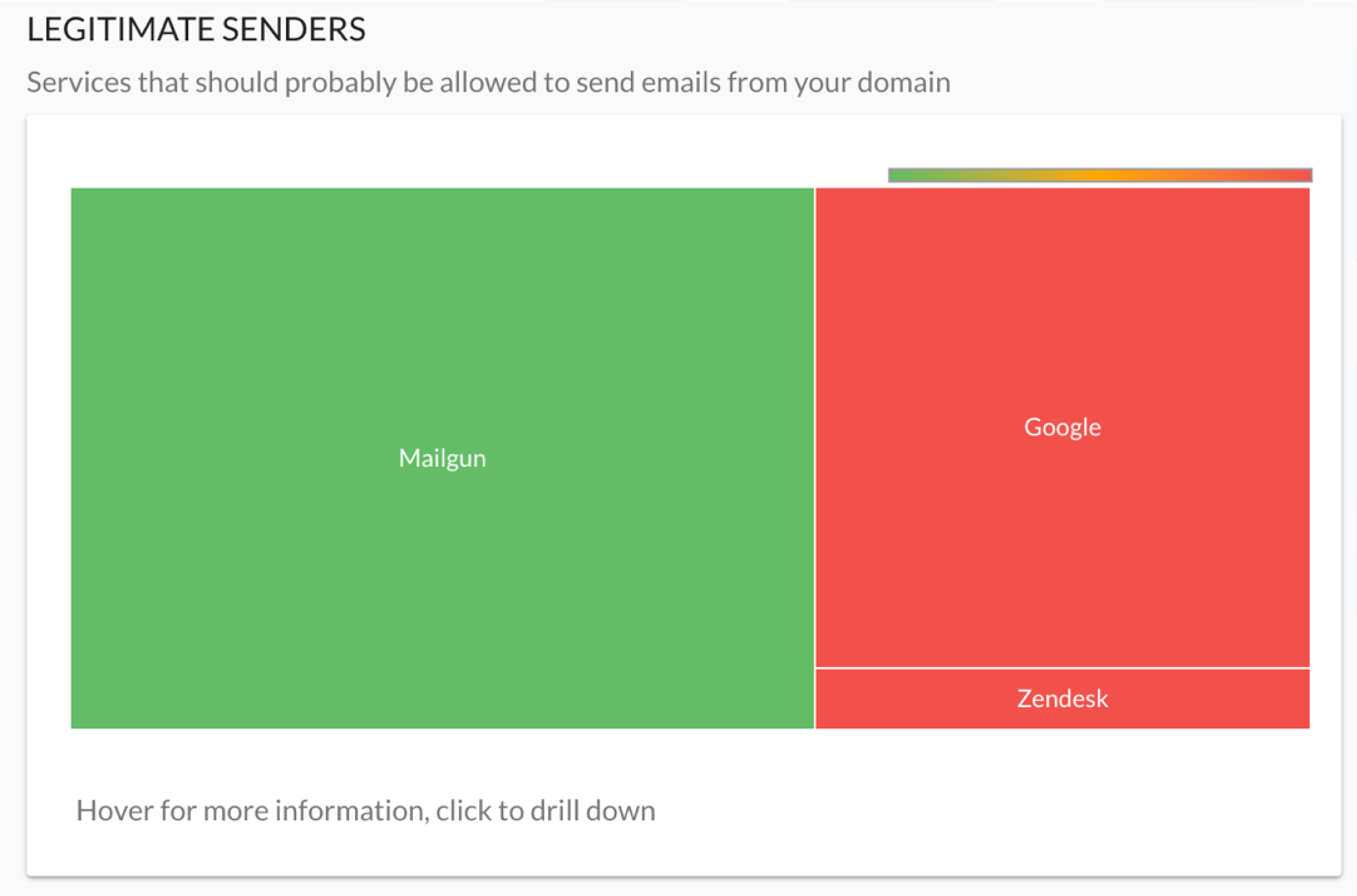
USE A SERVICE TO COLLECT & ANALYZES DMARC FEEDBACK DATA FOR OPTIMIZATION



TRENDS

How your DMARC status changed over time

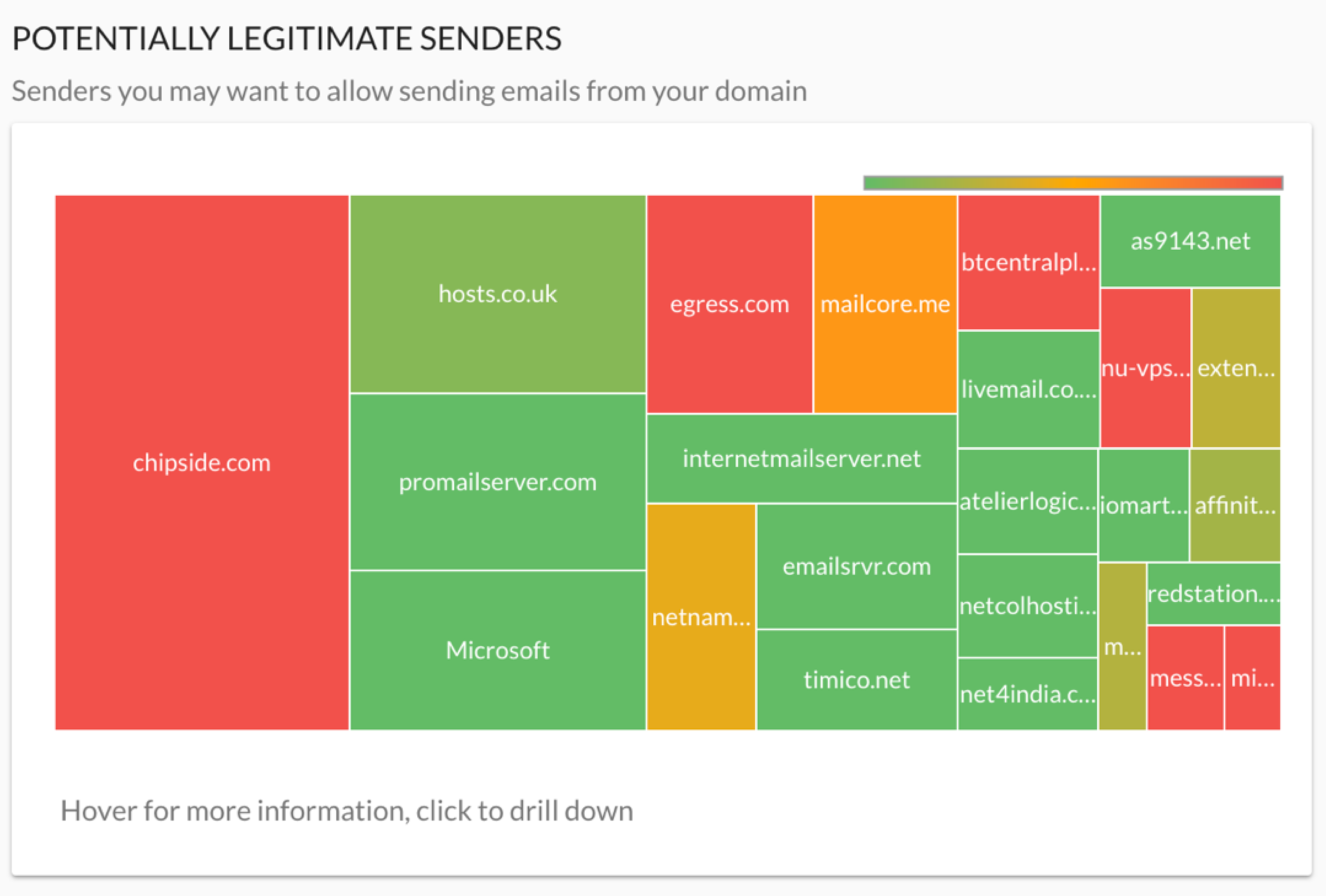
GAIN VISIBILITY INTO ALL SENDERS USING YOUR DOMAIN



LEGITIMATE SENDERS

Services that should probably be allowed to send emails from your domain

Hover for more information, click to drill down

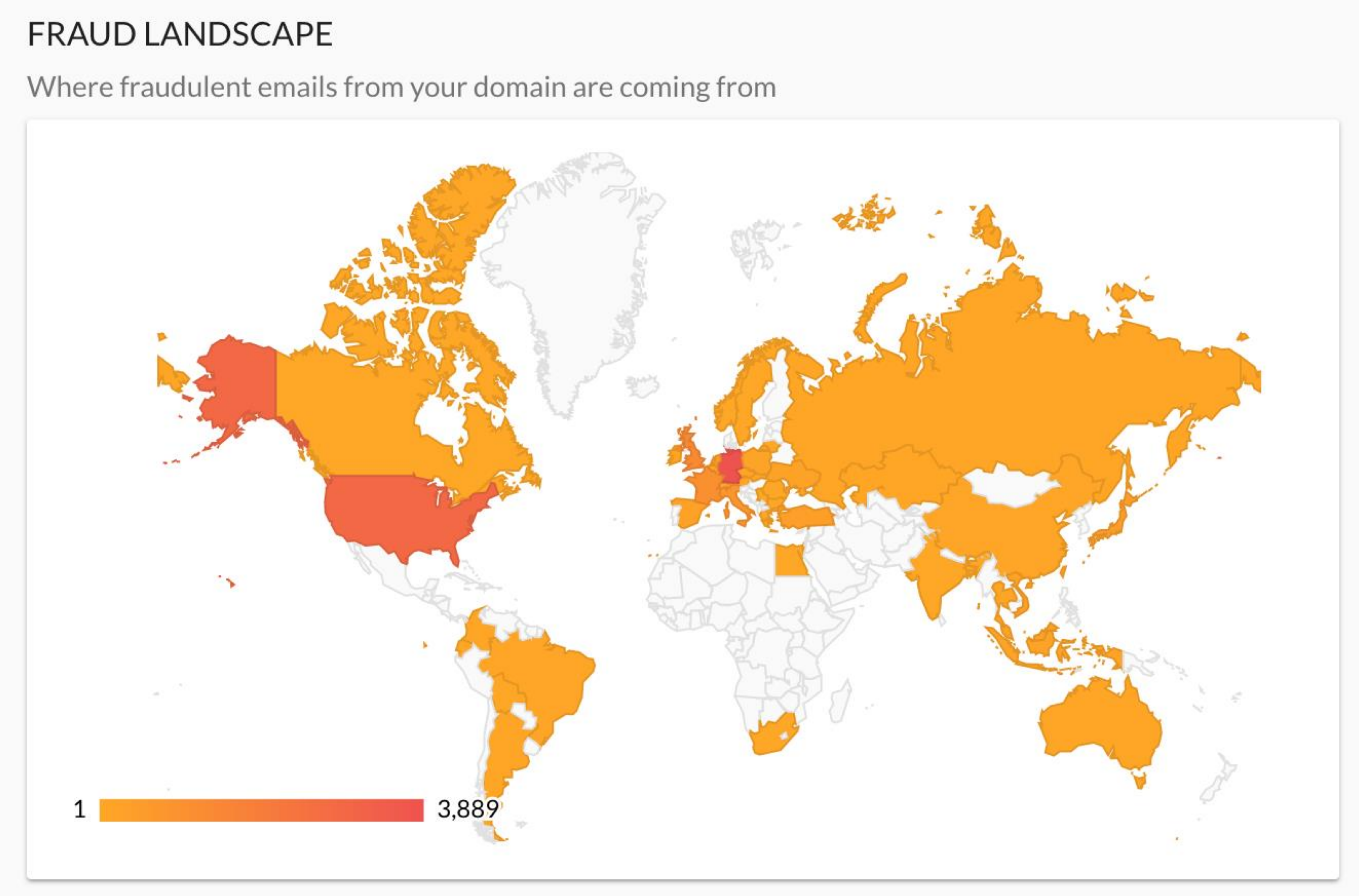


POTENTIALLY LEGITIMATE SENDERS

Senders you may want to allow sending emails from your domain

Hover for more information, click to drill down

AND ALSO FRAUD…



FRAUD LANDSCAPE

Where fraudulent emails from your domain are coming from

LOOK FOR SOLUTIONS THAT PROTECT PEOPLE, BUSINESSES, AND BRANDS FROM SPEAR PHISHING AND CYBER FRAUD

COMPREHENSIVE FRAUD PROTECTION

AI

AI for Real-Time Spear Phishing Prevention

Domain Fraud Visibility and Protection with DMARC

Fraud Simulation for High-Risk Individuals

MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Greg Arnette
Data Protection CTO
@gregarnette