Strengthening brand trust & recognition

By protecting your employees, customers, suppliers, and the whole world from email phishing and spoofing attacks originating from your own domain.

Benefits of implementing DMARC on your domain

Visibility
Gain full visibility of all servers, both legitimate and illegitimate, that are sending email from your domain.

Security
Ensure no attackers can send email impersonation /spoofing attacks from your domain.

Compliance
Ensuring employees can only send their emails via group approved email servers. This ensures correct record management of all email communication.

Delivery
Improve your email delivery, making sure it arrives in the intended inbox and not the spam bucket.

Our Purpose? Making The Internet a Safer Place

Defending your domain against phishing and spoofing attacks is made easy as DMARC automates the process.

Using global standards, along with our tools that enable you to easily understand who is sending email from your domain, where the threats lie, and the steps needed to authorise senders.

Sendmarc follows a well-defined process to take a client's domain to full protection while mitigating the risk of false-positives and allowing legitimate email services to operate without interruption

The Solution to Total Email Protection

DMARC's solution is built on the globally recognised email authentication standard, DMARC, that is supported by the vast majority of leading email providers across the world.

There are five core phases to achieving and maintaining full protection on your domain. Each phase has a set of implementation steps with clearly defined outcomes.

Each phase is designed to safely configure your sending infrastructure to send fully authenticated email while minimising the risk of legitimate email becoming blocked.

With your domain authenticated, deliverability of your transactional and marketing emails will see a significant increase.

Become DMARC Compliant

ARMD digital
advance risk mitigation digital

Phase 1: Monitoring & Analysis

The first phase of the project entails setting up reporting that Sendmarc can monitor and analyse which servers are sending emails from your domain.

This phase aims to build a map of your sending infrastructure and determine the scope of configuration required for phase 2. This analysis will allow us to create a plan of action to configure authorised senders.

Phase 2: Authorise Senders

Based on the report produced in phase 1, Sendmarc will guide the configuration of sending infrastructure to authenticate all legitimate email senders.

Legitimate senders could be employees, email service providers, or other third-party senders, which all need to be configured correctly.

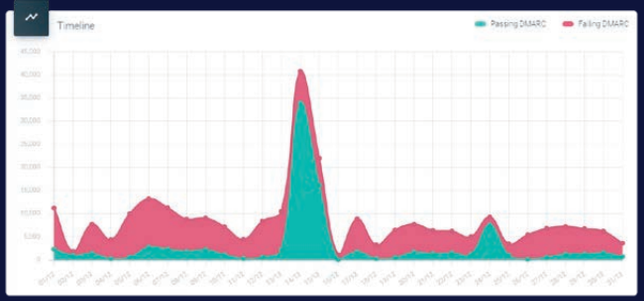
This phase aims to have these senders identified and authenticated so that we can proceed to Phase 3 and begin the quarantining of unauthorized email.

Phase 3: Quarantine

Once the reporting shows that all legitimate senders have been correctly configured, Sendmarc will begin to quarantine a certain percentage of unauthenticated emails.

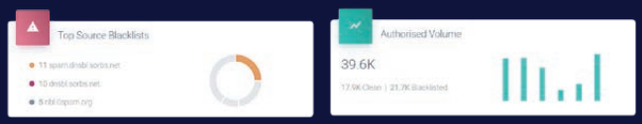
In this phase, we aim to reach 100% quarantine **without adversely affecting legitimate sources.** We will closely monitor all quarantine actions and react accordingly to ensure there are no false positives.

Aggregate Flow Report
Authorised vs. Unauthenticated Email



Top ISP Report

Top Volume & Blacklists Reports



Integrates With (to name a few)

mimecast · Office 365 · Google Workspace · solarwinds · aws · proofpoint. · Symantec · SYNAQ

Phase 4: Reject

After reaching the point where we can quarantine 100% of illegitimate emails, we can start to reject unauthenticated mail.

As in the previous phase, the goal is to get the policy to 100%, which will ensure there is no disruption to legitimate **traffic.**

Phase 5: Active Protection

At this point, your domain is 100% protected. However, it requires active monitoring and reporting to help you deal **with threats and attacks, as well as ensure that infrastructure changes do not affect email delivery.**

The following activities can be managed with our comprehensive set of tools:

Reporting and analysis of email traffic feedback

- Threat detection and real-time alerts
- Automatic onboarding of new email users and employees
- Identification of configuration issues and new infrastructure setup

DMARC ARMD

Making the internet a **safer** place

powered by SENDMARC

ARMD digital
advance risk mitigation digital