Sendmarc

Powered by SYNAQ

The Sendmarc service, powered by SYNAQ, aims to help companies protect themselves, their clients and their brand from email phishing and spoofing attacks using successful DMARC implementation. Sendmarc is an add-on to the SYNAQ Securemail Service, which allows for a full comprehensive line of defence in securing business email.

What is DMARC?

DMARC is a policy that a domain owner creates and publishes on the internet. The policy will instruct email receivers what to do when they receive an email that fails either SPF, DKIM or both for their domain.

DMARC adds the additional benefit of reporting, so when a receiver detects DMARC (SPF and/or DKIM) failures, the policy will also inform them where to send details of these failures.

With this level of visibility, DMARC can identify legitimate sources of email that need to be included as part of existing SPF or DKIM authentication policies. This provides insight into illegitimate email senders who are spoofing your domain, so that these threats can be effectively removed.

Why Sendmarc?

To protect clients who are open to impersonation attacks from:

- ✓ **Unauthorised sending:** Where anyone can send from a client's domain.
- ✓ **Interception:** An email can be intercepted and changed without anyone knowing.
- ✓ **Lack of visibility:** When it's almost impossible to identify who is sending mail on a client's domain – legitimate and illegitimate sources.
- ✓ **Lack of trust:** Without protection, it's hard for a receiver to tell if an email is arriving from a legitimate sender.
- ✓ **Reactive action:** Attacks are dealt with reactively after the damage has been done to a company's brand.
- ✓ **Closed protection:** Most systems only protect users inside the company which leaves their clients and suppliers at risk.

What is Sendmarc?

Sendmarc, available as an add-on to the SYNAQ Securemail Service, was built on globally recognised email authentication standards (supported by the vast number of ISPs across the world) and developed with decades of combined email industry knowledge, experience and know-how to help clients achieve full email protection by understanding the threats, identifying the sources and actively protecting their domain.

The Sendmarc service automates the process of clients defending themselves against phishing and spoofing using tools that allow them to easily understand who is sending email on their domain, where the threats lie, and the steps needed to authorise senders.

More specifically, by offering this service, we aim to stop phishing and spoofing on a client's domain through full DMARC compliance and help guide you through the process of authenticated email while limiting the risk of legitimate emails being undelivered.

How does it work?

The journey to full email protection on a client's domain consists of five core phases. Each phase is designed to safely configure their sending infrastructure to send fully authenticated email while minimising the risk of legitimate email becoming blocked.

Phase 1: Monitoring and analysis

Without protection, it's hard for a receiver to tell if an email is arriving from a legitimate sender.

Phase 2: Authorise senders

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

Phase 3: Quarantine

Once the reporting shows that all legitimate senders have been configured properly, the service will begin to quarantine unauthenticated emails.

Phase 4: Reject

Once 100% of illegitimate mails can be quarantined, we can start to reject unauthenticated mail.

Phase 5: Active protection

At this point, your domain is 100% protected.

Benefits

This service enhances a client's existing email ecosystem to achieve:

- ✓ **Visibility:** Full visibility of legitimate and unauthorised servers sending email from their domain.
- ✓ **Security:** Unauthorised, intercepted or changed emails from their domain will be rejected by receiving servers.
- ✓ **Compliance:** Ensure that employee communications are sent from authorised channels that are archived and recorded.
- ✓ **Delivery:** Increase deliverability, as the receiving server can trust their legitimacy and no longer divert mails to spam.

About SYNAQ

✓ **Proven track record:** Established in 2004, SYNAQ is trusted to process and deliver mail for thousands of clients across South Africa, Africa and the globe.

✓ **Backed by Internet Solutions:** South Africa's leading ISP acquired a majority stake in SYNAQ in 2011.

✓ **Flexible contracts:** Fixed-term and monthly contracts are available to meet individual company needs.

✓ **Leading punitive SLA:** 100% anti-virus and 100% phishing protection against leading South African banks, backed by our money-back guarantee.

SENDMARC Powered By SYNAQ

To become a SYNAQ Client, contact us on **(011) 262 3632** or email: **sales@synaq.com**