SENDMARC

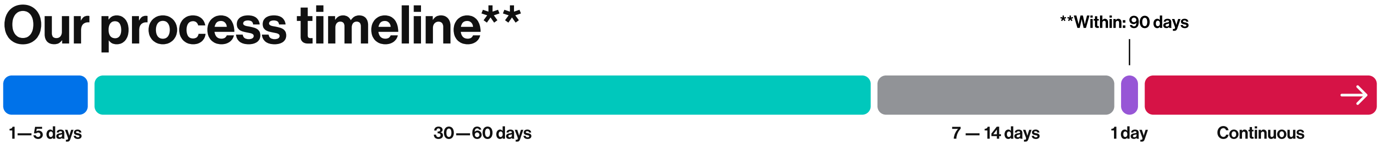
DMARC implementation: Navigating Sendmarc's step-by-step process

We've mapped out our implementation process to show how we ensure your customers' DMARC, SPF, and DKIM records are correctly configured, effectively protecting against email-based threats.

Our timeline highlights how we deliver on our promise of getting your clients to a policy of p=reject within 90 days*.

Below, we've provided a detailed breakdown of what to expect at each phase of our managed implementation process, including key milestones your customers will reach along the way.

Our process timeline**



*For customers on Sendmarc's Premium Plan.

1 Finalize DNS settings

This phase involves finalizing the DNS authentication settings for a business's domain(s) by uploading the existing SPF and DKIM records to the Sendmarc platform.

During this phase, we:

- Identify and add domains to the platform
- Import existing SPF and DKIM records
- Publish Sendmarc DMARC, SPF, and DKIM records
- Review the DNS for missing sources
- Verify and review the effectiveness of changes

2 Authorize senders

In this stage, we analyze data to ensure the SPF and DKIM records are correctly configured.

To do this, Sendmarc will (in partnership with the customer):

- Identify legitimate sending systems, services, and platforms, their business owners, and missing authentication protocols
- Research the capabilities and limitations of DNS authentication for each system
- Log internal change approvals for updates
- Update missing and/or new SPF record entries on our platform
- Create DKIM keys in the systems, services, and platforms and the Sendmarc Portal
- Verify the efficacy of the changes using DMARC data

3 p=quarantine

By this point, domain compliance and email deliverability should be nearing or at 100%, and the company should be ready to enforce DMARC protection.

We'll move the organization's domain to p=quarantine and:

- Review domain data for two weeks to check compliance and deliverability
- Validate and update configurations if needed
- Communicate the planned changes to stakeholders and log approvals

4 p=reject

The final step in the implementation process is setting the DMARC policy to p=reject.

After this, we recommend businesses:

- Review data for missed authorized sending sources
- Ensure their organization is set up to receive the appropriate proactive alerting

5 Continuous monitoring

Once the DMARC policy is set to p=reject, it's essential to maintain ongoing monitoring to ensure your customers' email environments remain secure and effective.

This phase focuses on proactive and responsive measures to address changes in their environments, helping us:

- Ensure new applications or services are properly authenticated and configured
- Monitor platform alerts for changes in DNS configurations, such as SPF or DKIM records

i **Sendmarc** provides support to organizations of all sizes and ensures fast, seamless, and scalable DMARC implementation.

Contact us to get started.

www.sendmarc.com