The 5 Minute Guide to DMARC Deployment

DMARC (Domain-based Message Authentication, Reporting and Conformance) helps legitimize email by doing two things:

- Gives feedback to the domain owner about the email itself, including if SPF and/or DKIM is properly aligned.
- Tells email receivers (like Gmail and Yahoo) how to handle messages that fail to align with those protocols.

DMARC is a domain-based email control. Email domains are a shared resource within most organizations, with use spanning from employees to entire departments, external parties that send email on behalf of the organization, and the organization's own internet-facing applications.

Deploying DMARC yields benefits across different facets of an organization. Many organizations look at DMARC for the first time from a specific perspective that might not take into consideration DMARC's total value.

- People in security see benefits in DMARC as anti-phishing technology.
- People in marketing see benefits in DMARC as a way to make email easier to deliver to their recipients.
- People in management see benefits in DMARC as a compliance tool to ensure an organization's standards are upheld.

Assess

The work required to deploy DMARC is directly related to the size and complexity of an organization's email infrastructure. An initial assessment should be performed to determine the context in which the deployment project will operate, the complexity of the existing email environment, and the implementation capabilities of the organization. Results of the assessment directly inform project scoping and planning.

When deploying DMARC, it's best to roll out DMARC across all of an organization's domains instead of focusing on individual domains. When DMARC is deployed at an organization across the entire domain portfolio, the process of deployment becomes much easier, and the benefits increase to the point where managers get new tools to ensure email is being sent in compliance with the organization's standards.

Built upon SPF & DKIM

DMARC, an open source standard, uses a concept called alignment to tie the result of SPF and DKIM to the content of an email.

> **SPF** — a way of publishing a list of servers that are authorized to send email on behalf of a domain — has been around since 2003.
> **DKIM** — a method of adding a tamper-evident domain seal to a piece of email — has roots going back to 2005.

If not already deployed, putting a DMARC record into place for your domain will give you feedback that will allow you to troubleshoot your SPF and DKIM configurations if needed.

DMARC Records

dmarcian's DMARC Record Wizard simplifies the process of creating the DMARC record itself.

Once you've published DMARC records, DMARC data will typically begin to generate within a day or two in the form of reports that give you insight into the way your domains are handling email. There are two forms of reports: those that provide a comprehensive view of all of a domain's traffic (as seen by the organization that generates the report), and those that are redacted copies of individual emails that are not 100% compliant with DMARC.

The comprehensive reports are XML-based and include information such as message counts, IP addresses, and the results of processing SPF and DKIM. It can be difficult for humans to read and make sense of XML reports, especially when they can number in the thousands. dmarcian specializes in processing these reports and identifying the steps needed so that DMARC can be more easily deployed throughout an organization.

DMARC policy

For an email message to be considered DMARC-compliant, the domain found in the "From:" header must match the domain validated by SPF or the source domain found in a valid DKIM signature. If the domains match and at least one of the two mechanisms succeeds verification, receivers can safely say that the email legitimately comes from the specified domain.

	DMARC CHECK	FROM: DOMAIN (DMARC)	DKIM DOMAIN (DKIM)	ENVELOPE-FROM / RETURN-PATH (SPF)
Full Alignment	✓	@client.net	client.net	@client.net
DKIM Only	✓	@client.net	client.net	@sample.net
SPF Only	✓	@client.net	sample.net	@client.net
FAIL	✗	@client.net	sample.net	@sample.net

** If SPF or DKIM is absent, this individual check will fail, leaving only the other to result in a pass. If SPF and DKIM are absent, automatic DMARC fail.*

A DMARC policy allows a domain owner to indicate that their messages are protected by SPF and/or DKIM and tells the recipient what to do if none of these are verified on a particular email, such as marking it as junk mail or rejecting delivery of the message.

Senders can set their DMARC policy (referred to as "*p*=") to determine what is done to non-compliant email:

> **Monitoring** (p=none) no impact on mail flows (only DMARC feedback should be collected)
> **Quarantine** (p=quarantine) messages that fail DMARC (e.g. move to the spam folder)
> **Reject** (p=reject) messages that fail DMARC (don't accept the mail at all)

The Road to p=reject

DMARC policies typically start at a state of *p=none,* which is a monitoring phase that gives insight into how your domain is being used and SPF and DKIM are functioning, and moves towards a policy of *p=reject*. Reject instructs email receivers to refuse to accept email that fails DMARC. By default, email that fails under a reject policy is not accepted. This behavior is a great control against the sending of unauthorized email making use of your domain.

It is estimated that only 30% of organizations who start the process of deploying DMARC ever complete the process. The challenge with deploying DMARC isn't the specification itself but with the email ecosystem and the interpretation of the feedback that is provided.

The process of adopting DMARC into an organization can be daunting, but with the proper partner, it can be easily managed.

dmarcian advantage

dmarcian is dedicated to upgrading the entire world's email by making DMARC accessible to all. **Dmarcian** brings together thousands of senders, vendors and operators in a common effort to build DMARC into the email ecosystem. Our customers range from banks, top Internet properties, governments, marketing agencies, telecoms and commercial enterprises of all sizes.

DMARC SaaS Platform - To turn thousands of XML records into something useful, **dmarcian** processes DMARC data using a complex set of identifiers. We categorize sources of email and present you with DMARC compliance status (based on email source, DKIM and SPF), and we alert you if there are any potential threats or abuse on your domains.

Deployment Services - The challenge with deploying DMARC isn't the specification itself, but with the email ecosystem and the interpretation of the feedback that is provided. **Dmarcian** offers a project-based approach for policy enforcement tailored to your organization's needs.

On Demand Support - Although deploying DMARC can be viewed as a one-time technology upgrade, managing and maintaining DMARC compliance needs long-term effort to remain effective. **Dmarcian** can help with managing DMARC-related incidents, regular data reviews, monitoring ongoing compliance, and embedding DMARC into daily operations. Fixed price support packages -- after deployment project or as stand-alone -- are available.

More information on getting started with DMARC can be found here.

dmarcian *CEO and founder, Tim Draegen, is a primary author of the DMARC technical specification and a previous chair of the IETF DMARC working group. Technical Advisor Scott Kitterman is one of the primary authors of the SPF technical specification*.