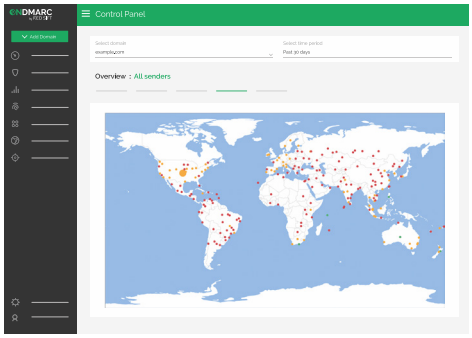
DMARC is for life, not just a project...

At Red Sift we often get asked "what next?" after someone has thrown the p=reject switch. Yes, a lot of the really hard work has been done, but like with all things security focused, constant care and attention are needed to stay one step ahead of phishers, spoofers and hackers.



Maintain existing email sending services

For your DMARC record to carry on protecting your organization it needs regular care and attention, take your eye off the ball and SPF or DKIM might break at some point and you'll have your emails rejected without knowing it has even happened. There are a few reasons why this might happen:

1. Email Forwarding

When someone forwards an email SPF is broken.

2. Misalignment

If you're using a third-party sending service then DKIM keys can get out of sync.

3. Server Overload

Sometimes an ISP, during high email peaks, may turn off DKIM checking as it requires high processing resources.

Without OnDMARC you'll struggle to pinpoint when this happens or be able to fix the underlying root cause.

Knowing what's going on across your email landscape is particularly valuable when you're using third-party sending services and may not otherwise have direct control over the exact configuration. Indeed, it's not uncommon for third-parties sending emails on behalf of their customers to suddenly stop DKIM signing emails, all because a small change has been made. Without the reporting functionality of OnDMARC you won't know if and when this happens so you won't be able to reach out to them for answers or have this corrected.

Key Benefits

- **Ongoing visibility** across your email sending domains - never lose sight of emerging threats or unexpected changes.

- **Troubleshoot** when things become misaligned.

- **Easy Configuration** add new and remove old email sending services.

- **Quick Modifications** add new domains (and subdomains) as your business grows and move these to p=reject as well.

www.ondmarc.redsift.com

contact@redsift.com

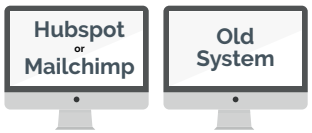
@redsift

Add new email services

The ongoing reporting capability of DMARC has the added benefit of highlighting new legitimate (and illegitimate) sources of email. Once you've seen them pop up on the OnDMARC radar you can go ahead and either properly configure them with SPF and DKIM, or block them altogether.

1. 

A common scenario is a department, such as Marketing, deciding to use a new application like Hubspot or Mailchimp, to manage email campaigns to customers.

2. 

Unfortunately, IT and email teams aren't always involved in these decisions, and so the new email sending application becomes part of an organizations' "shadow IT".

3. 

The problem with sending emails "from the shadows" is that with your DMARC record in p=reject none of these emails will reach their intended recipients.

Of course, the moment you know about the new application you can help correctly configure it to maximize deliverability rates.

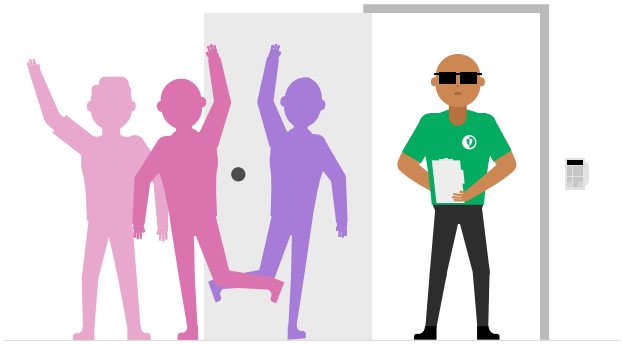
Building a futureproof email architecture

It's inevitable that over time new domains and subdomains will be added, this is commonly known as domain creep, and eventually, most organizations end up with far more domains under DMARC control than they first imagined when they started their journey.

Our experience of thousands of DMARC deployments has taught us that most organizations will want to make use of dedicated domains or subdomains for individual business groups, perhaps even with different policies for these domains. There will also be parked domains, purchased to protect domains you own but do not send email from.

> Being able to simply, and correctly, manage an ever-growing number of domains necessitates a tool like OnDMARC, because what your email landscape looks like today, isn't an indication of what it will look like tomorrow.

Furthermore, the proliferation of cloud-based services continues apace adding a new twist to the DMARC challenge: not busting the 10 SPF lookup limit. Some cloud-based email sending services can use up to 7 of the 10 available lookups, leaving you with very little space for additional services, let alone essential ones like G Suite or Office 365.



The OnDMARC Dynamic SPF works like a "bouncer"

OnDMARC's Dynamic SPF feature is the only way to overcome the 10 SPF look-up problem and guarantee you have a solution that's fit not just for today, but also tomorrow. With an unlimited number of SPF look-ups Dynamic SPF removes the need for you to have the technical knowledge required to write complex SPF records and manually edit your DNS.

Summary

Yes being at p=reject is a major milestone that should be celebrated, but sadly it doesn't mean you can take your foot off the gas. As we've explored in this document the email sending habits of domains change over time and things can go wrong at any point. This will negatively affect your deliverability, security and domain reputation. Continuing to use OnDMARC gives you the visibility over what is happening at all times as well as the tool kit to put things right again.

Get in touch today to find out more about how you can use OnDMARC to combat phishing and boost email deliverability.

Member CyberExchange

Member of Microsoft Intelligent Security Association

UK CLOUD AWARDS 2019 WINNER

2017 Computing Security Awards WINNER Anti Phishing Solution of the Year

bsi. ISO/IEC 27001 Information Security Management IS 672913

GLOBAL CYBER ALLIANCE

ONDMARC

The Red Sift Open Cloud is a data analysis platform that is purpose-built for the challenges of cybersecurity. By harnessing the power of AI we can securely collate, compute & visualize data from thousands of individual signals to help organizations to optimize their cybersecurity.

Our first product on the Red Sift platform is OnDMARC, a SaaS product that helps to implement and maintain DMARC. This email authentication protocol effectively blocks phishing attacks and increases the deliverability of genuine emails.

www.ondmarc.redsift.com
contact@redsift.com
@redsift