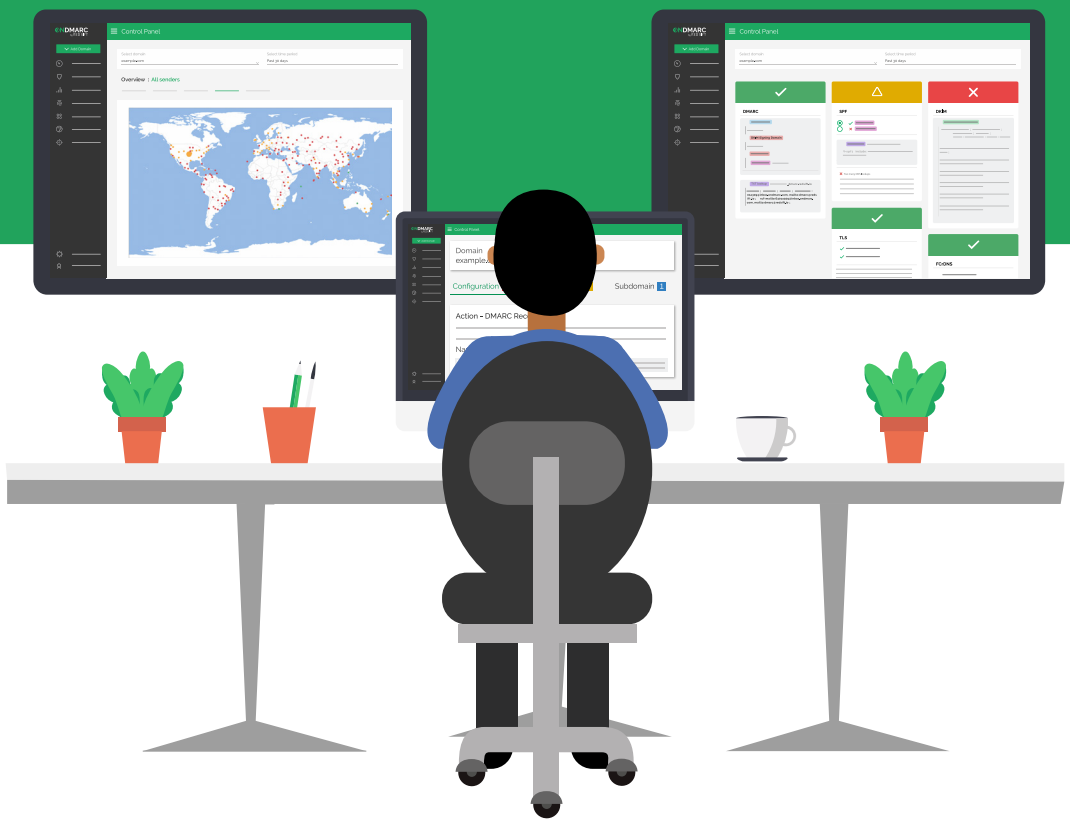
ONDMARC by RED SIFT

The essential guide to OnDMARC

A complete overview of the award-winning, cloud-based DMARC app that enables you to configure SPF, DKIM and DMARC for all your email sources.



Trusted by

ALVAREZ & MARSAL TransferWise pipedrive Telefónica Cambium Networks™

Everything within OnDMARC is designed to save you time and simplify your DMARC journey as you fully secure your domain.

Full visibility

Within 24 hours of adding your unique DMARC record to your DNS, OnDMARC begins to analyze and display your DMARC reports in clear and comprehensive dashboards. Who is sending on your behalf? Where in the world is your domain being used? Are your emails passing or failing DMARC validation? This gives a complete picture of your email landscape and not just the stuff which crosses your network boundary.

Brand protection

OnDMARC will give you the controls to stop malicious emails from being sent under your domain name. We'll guide you through every email security protocol that sets up these defenses. The result is peace of mind that you're protecting your brand's reputation, customers, suppliers and other stakeholders from email-based phishing attacks.

Save time

Relying on consultants is a time-consuming process to configure DMARC, leaving you with no ongoing visibility or knowledge of how it works, which may mean calling them again! The most commonly reported benefit of OnDMARC is the time it saves by making an issue known and putting you directly in control of fixing it quickly with clear instructions.

Reduce costs

DMARC alone is complex to navigate - once left to consultants with expensive expertise. OnDMARC gives you the tools to take back control of your domain (and budget) with easy instructions alongside every alert. Additionally, we're on standby via live chat inside your app and offer over 500 best practice articles in our Help Center.

Ongoing monitoring

Once you've hit the switch to p=reject, shared reports internally and celebrated all those blocked impersonation attempts, we'll help you keep it that way. As your trusted sidekick, if any of your defenses break then we'll alert you of the root cause and provide instructions on how to fix it.

Easy configuration

Our powerful automation does all the heavy lifting by continuously analyzing what's going on across your domain, surfacing alerts for where and how to make necessary changes to your email security. Then simply follow our extensive database with setup instructions for hundreds of well-known email sources. You've totally got this!

Simplicity is key

Innovation lets you fast-track your journey to DMARC and simplify ongoing management. Here are some of our most powerful features.

Dynamic SPF

Break free from the 10 SPF lookup limit and have unlimited services that are easy to manage.

What's the problem?

Modern cloud services often require multiple lookups so you can very easily go over the 10 SPF lookup limit. Once you're over the limit you're likely to experience SPF failures which are sporadic and hard to investigate. Worst of all, they can significantly affect the deliverability of your email. This won't do, because you want people to read your emails and you certainly don't want to be labelled as spam!

How we solve it

- Once you've added your domain you can add as many SPF include mechanisms as you need! We put them together as a string of includes, without limits, and call this the 'smart include'. You simply copy and paste this string into your SPF record.
- Your smart include statement simply points your SPF to OnDMARC, allowing you to manage everything directly from within your account such as MX records, A records and IPV4/6 addresses.
- You can then rest assured we're automatically ensuring every record for all third party services you use is up to date, so there's no fear of static "flattened" code becoming outdated or obsolete.
- In the unlikely event of anything happening to OnDMARC your SPF solution wouldn't break because Dynamic SPF runs on a highly available, geo-distributed and redundant infrastructure independent of OnDMARC.
- As an added bonus, it works with any existing mail service or ISP!

Dynamic DMARC

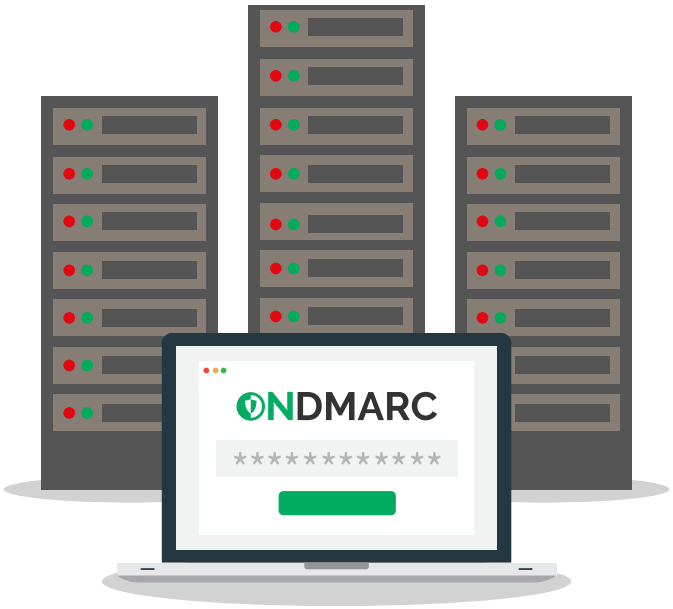
Ditch the DNS and Manage SPF, DKIM and DMARC records directly within OnDMARC with Dynamic DMARC.

What's the problem?

One of the challenges when implementing DMARC is having to add and update txt records in your domains DNS every time you want to change your DMARC policy or add a new service. It is a time consuming and error-prone process. This is particularly true if you have lots of domains, outsourced management, or strict change control policies in place for DNS alterations. *Dynamic DMARC* simplifies all this by enabling SPF, DKIM, and DMARC records to be managed directly in the OnDMARC application.

How we solve it

- *Dynamic DMARC* enables the management of DMARC, DKIM, SPF (and soon BIMI and MTA/STS) TXT records from within OnDMARC.
- This means that once the OnDMARC Smart Includes have been added to a domain's DNS, there's no need to go back to the DNS to update your records via OnDMARC's simple interface, saving you time.



Investigate

OnDMARC lets you fast-track configuration of your email security to see the results in seconds, not days.

What's the problem?

Making changes to your email security configuration typically means waiting quite some time for the first DMARC report to arrive - sometimes up to 24 hours - in order to see if the changes you made have had the desired effect. Without a tool such as *Investigate*, you'll be left to rely on cryptic email headers to understand the problems with your latest email configuration. This adds another layer of complexity to your investigation and ultimately slows you down.

How we solve it

- You can swiftly find out the results of every change you make to your email security via a unique inbox in your OnDMARC account. Simply send a 'test' email to Investigate's inbox and it will immediately decode those email headers for you.
- You'll immediately receive a checklist that tells you the status of five key signals: DMARC, SPF, DKIM, FCrDNS, and TLS, alongside the current status of your BIMI record. This highlights anything that didn't work and how to resolve it.
- Our *Threat Intelligence* feature within *Investigate* checks against databases of known spammers, malware disseminators, non mail transfer agents, botnet resources, phishers, or low-reputation senders, identifying suspicious emails that should be blocked. This feature also highlights deliverability issues on your domain from legitimate sending sources, giving you steps of how to improve your configuration.
- You can also compare the results of your email security against different security profiles: UK Minimum Security Standards, US Binding Operational Directive 18:01, OnDMARC Default, or simply to maximize deliverability. This gives you a clear target to aim for.

Supercharging security

With your smart initiative and our simplified tools, we can quickly help you confidently secure your domain from email impersonation and keep it that way.

Going beyond reporting

After we translate complex DMARC data into easy to understand visual reports and alert you of missing security protocols, we won't leave you hanging, we finish the job! Simply click an alert, learn what we've identified as needing fixing and then follow our guides to remediate. Not forgetting to run a quick check with our Investigate feature to be confident everything worked before moving on to the next task.

Fast turnaround

With OnDMARC, long complex DMARC configurations no longer require time consuming detective work and expensive experts. Instead, organizations can take back control of their domain's security and have immediate visibility of the results. An average OnDMARC customer can get to grips with their entire email landscape and make an impressively fast turnaround to full protection (p=reject) in just eight weeks!

Crystal clear dashboard

OnDMARC's intuitive dashboard is often a winner because it's easy to follow whether you're at the very beginning of your DMARC journey, or you're already fully protected and need clear, concise monitoring to stay there. We've got you covered with beautifully clear visual reports, alerts and step-by-step guides integrated into the platform throughout your journey.

Unparalled support

To ensure everyone can take control of their cybersecurity we have different levels of support to assist varied needs. In addition to our hands-free customer success packages, we have an in-app live chat feature for your ad-hoc questions, whilst "Daily Alert" emails can be set up to ensure domain issues are flagged automatically. The ever-growing help center is a further source of information where you can find step-by-step implementation guides for a variety of frequently asked questions.

Member of Microsoft Intelligent Security Association

2017 Computing Security Awards WINNER Anti Phishing Solution of the Year

UK CLOUD AWARDS 2019 WINNER

British Legal Technology Awards 2020 WINNER FOR 'IT SECURITY PROVIDER OF THE YEAR'

bsi. ISO/IEC 27001 Information Security Management IS 672913

GLOBAL CYBER ALLIANCE

The A to Z of OnDMARC

OnDMARC has everything you need to simplify your DMARC journey, check out the full feature list and the perks they bring to you.

Actions

Clear instructions for where and how to confidently configure your sources for full protection.

Activity Logs

This useful feature allows you to see who has made an “Addition”, “Modification” or “Deletion” as well as the time and date of that event. This is really important for complying with security standards like ISO 27001 by ensuring you have a clear way to manage systems access.

Analyzer

Look up any domain name to see if it has DMARC, SPF, and DKIM in place. A handy feature for finding out how secure your supply chain is and if they're vulnerable to email impersonation, which effectively puts you at risk!

API Access

A great feature that makes for a smooth new addition to the current workflow of larger organizations by allowing OnDMARC to easily integrate into existing security dashboards.

Control panel

Simply add the domains you want to secure and we'll give you a record for your DNS. Thanks to our Subdomain detection, if you have any that you haven't added to OnDMARC, we'll bring them to your attention to make sure they're covered in the process.

Domain Tagging

This feature allows you to tag and organize your domains any way you like. If you have a large number of domains this allows you to filter them down and easily search quickly.

Dynamic DMARC

Simplify your DNS management by configuring SPF, DKIM and DMARC txt records directly from inside the OnDMARC interface. For SPF specifically our smart automation tool *Dynamic SPF* lets you overcome the 10 SPF lookup limit and simplify ongoing SPF management.

Email Sources

This offers you a quick overview of your legitimate email sources, identified as assets, plus further insight into the status of each one to learn how complete each configuration is, or if there's still work to be done.

2 Factor Authentication

We recommend you enable this feature as it acts as a second line of defense when logging into your OnDMARC account.

Forensics

It's easy to search through the emails that failed DMARC for individual forensics. Don't worry though, the DMARC protocol redacts all sensitive information, such as the body of the email, and OnDMARC further redacts it to ensure compliance with GDPR.

Help

Gain access to our knowledge base anytime which is updated regularly by our DMARC experts. You can also reach out via the live chat tab in your dashboard with any questions!

Investigate

Investigate your emails with instant checklist reports for the status of each security protocol. Simply send an email to your exclusive OnDMARC inbox and highlight any issues with your SPF, DKIM and DMARC configuration. We'll also provide the steps on how to fix any you're missing.

Notifications

Set up your notifications to go directly to Slack or your email when you're not logged in and stay in the loop at all times.

Reports

Comprehensive reporting provides clear visual graphs on DMARC validation for all emails sent from your domain. This includes compliance, senders, receivers and locations. Additionally, we include ARC (Authenticated Received Chain) to help resolve issues that may arise with indirect mail flow.

Settings

Quick access to a list of all the domains you're managing as well as any tags you've created to organize them. You can modify or delete domains here any time.

SSO (SAML standard available)

OnDMARC has a secure single sign-on (SSO). If you would like to have SAML (Security Assertion Markup Language) as your SSO standard then we can get this set up for you.

Threat Intelligence

This feature checks new IP addresses against SPAM blacklists and exploits, allowing you to quickly identify senders with a low reputation and blocking these potential threats automatically.

Users and permissions

With OnDMARC you're able to add and remove users, customize their permissions such as "read-only", or assign them particular domains to manage if you're managing a bigger team.

Ready to shut down those spoofs?

Simply sign up to OnDMARC's free trial and plug us into your DNS for **14 days of free unlimited access**

British Legal Technology Awards 2020 WINNER FOR 'IT SECURITY PROVIDER OF THE YEAR'

finalist Cyber Security Awards

UK Cloud Awards 2019 WINNER

SendGrid Partner

2017 Computing Security Awards WINNER Anti Phishing Solution of the Year

RED SIFT

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.

Products on the platform include OnDMARC and OnINBOX, SaaS applications that work together to close the net on the phishing problem by blocking outbound phishing attacks and analyzing the security of inbound communications for company-wide email threat intelligence.

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