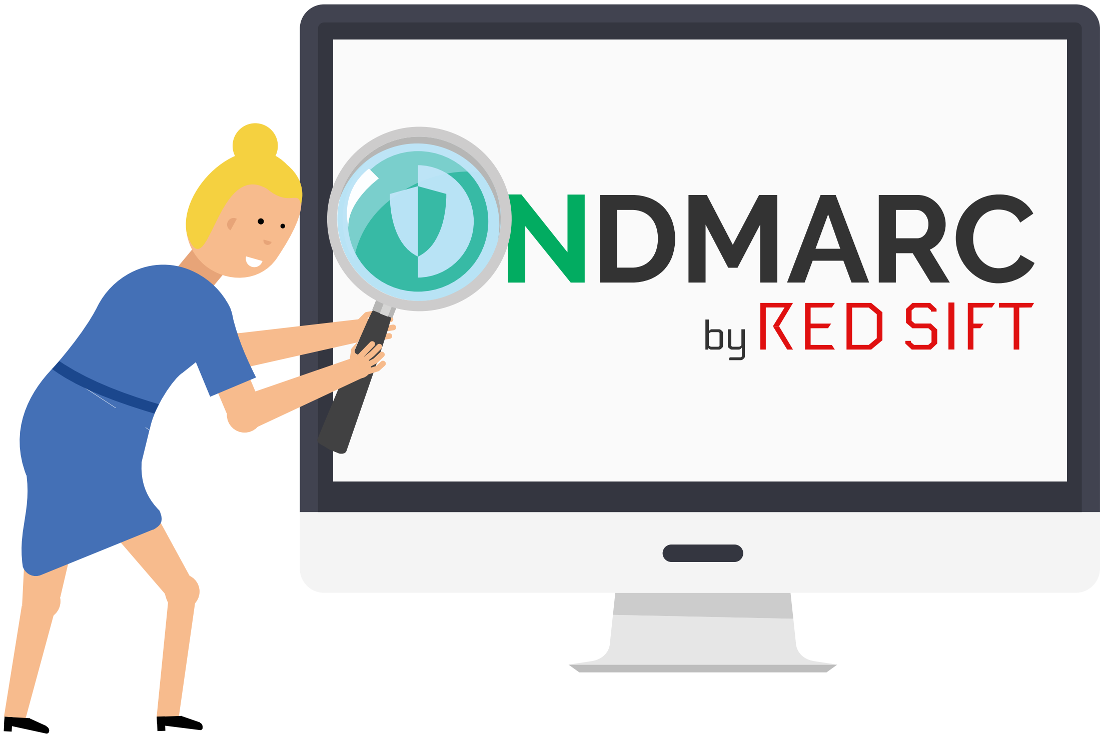
Finding your perfect DMARC provider

Here's everything you need to know about the key aspects of a trustworthy and easy-to-use DMARC provider.



Contents

Missed part one "**DMARC: What is it and why should it be your next priority?**" of this series? Don't worry you can find it *here* and get the background to DMARC.

It seems quick and easy to cover the basics for a very basic price, but it may slow you down later if your provider doesn't go beyond reporting and walk you through fixing the issues they identified. Here's the inside scoop on the type of unique innovation, thoughtful design and helpful extras out there which help you fast track your DMARC journey.

1. Supplier Checklist

- **What are their security accreditations?** It is important to check if the DMARC provider has the appropriate security accreditations. Check if they are ISO27001 certified or have Cyber Essentials.

- **Are they using the p=reject policy themselves?** In order to trust that a provider can implement DMARC effectively within your organization, you should check if they have been able to properly implement DMARC themselves. You can easily check using free online tools.

- **What do existing customers think?** If possible, try to speak to one of their current customers to get an insight on the provider's product and services.

- **What does their roadmap look like?** You might be buying the product for what it currently offers today, but also consider what other innovations are being developed that may be of interest in the future.

- **What are their support services?** Without in-house IT systems expertise, DMARC may appear to be complex to implement in smaller organizations or to deploy across larger organizations. A provider's' support services may, therefore, be integral to fast and effective implementation of DMARC. Support teams will also be invaluable to ongoing implementation and refinement of DMARC over time.

2. Product Checklist

What you should look for in your DMARC solution

The basics

- **Reporting and dashboards:** You need to be able to see all the email validations taking place within your domain. The best tools will simplify the complex DMARC XML reports so that you can quickly get an overview of the DMARC compliance of your emails. Simple dashboards will enable you to easily identify any misconfigurations, as well as to see the scale and frequency of spoofing attacks. For those looking for an in-depth understanding of their phishing attacks, forensic reports provide greater insight into how an organization's domain is being exploited.

- **Configuration:** Once you have used DMARC to understand the security of your domain, you can put in place a solution which will enable you to configure your SPF and DKIM policies to ensure that your organization's identity can only be used by legitimate users. A clearly structured solution is important for organizations which do not have specialist in-house DMARC expertise and/or limited resources. The solution should help you to confidently move you through the various stages of DMARC implementation until the organization reaches the p=reject policy.

- **Ongoing protection:** As your organization grows and changes you will undoubtedly have to update your DMARC configuration to ensure that your domain continues to be protected and that deliverability is unaffected. A good DMARC solution will allow you to easily update and maintain your SPF and DKIM configurations, as well as provide clear alerts when one of these 'breaks'. A solution like ***OnDMARC*** will highlight any changes that need your attention and provide clear instructions on how to resolve it quickly.

3. Helpful extras

Look out for these helpful extras available from some providers

- **Dynamic SPF:** The SPF protocol is limited to 10 DNS lookups. This is often an issue for organizations with a complex email infrastructure or those that use a number of cloud services since they will quickly reach this limit. Once this limit has been reached, legitimate emails may fail SPF authentication. The Dynamic SPF feature, which is available from ***OnDMARC***, overcomes this problem by allowing an organization to use only 1 SPF lookup to connect to OnDMARC's system, from where it will have unlimited lookups.

- **API Access:** The ability to seamlessly integrate the data from your DMARC solution into your existing security dashboards is a useful way to create a one-stop-shop for all email security analysis.

- **Single-Sign-On (SSO):** Some providers, including ***OnDMARC***, enable an organization to integrate DMARC with other key IT systems, such as Okta, so that it can be accessed with a single sign-on to an organization's security setup.

- **ChatBot:** A chatbot can deliver real value by allowing an organization to receive and action DMARC alerts directly in Slack. This means you do not need to check your DMARC application regularly.

- **DMARC Checkup:** Typically when you make a DNS change, you have to wait for the first aggregate reports to arrive in order to see the impact of the change, this can take up to 24 hours. With ***OnDMARC*** the inspection tool 'Investigate' enables you to immediately check the results of changes to the configuration of 5 essential signals: DMARC, SPF, DKIM, FCrDNS and TLS in human readable dashboards.

- **Forensics:** Forensic reports for emails that have failed DMARC validation give you comprehensive and useful insight into the individual emails themselves. Be sure to double check that a provider does this after they've redacted the body of the email.

- **Email security profiles:** Being able to quickly compare your email configuration with an industry standard is a great way to guarantee you can meet the needs of any regulation in place. Providers like ***OnDMARC*** enable you to compare your compliance against the requirements of different security profiles such as the UK Minimum Security Standards or US Binding Operational Directive 18:01.

4. Ensuring DMARC success

- **Implementation:** An implementation package can help an organization to put DMARC protection in place more quickly, minimizing its exposure to email impersonation. The services included should enable you to identify valid sources of email within your organization, configure them correctly and then put DMARC into quarantine or reject.

- **Managed Services:** The benefit of having a managed service is that you secure access to a team of experts who are available at all times. These experts can notify you of incident alerts and suggest resolutions, freeing your team up to focus on other tasks.

- **Support:** Customer support is a great way to tackle any ad hoc troubleshooting or get help using the DMARC tool. Some solutions, such as ***OnDMARC*** incorporate chat functions into their DMARC portal, so with a single click of a button you can be connected to an engineer ready to help solve your query.

- Also check to see if your provider's services include a knowledge base, including answers to frequently asked questions and handy hints and tips to enable you to optimize your implementation of DMARC and in-life management.

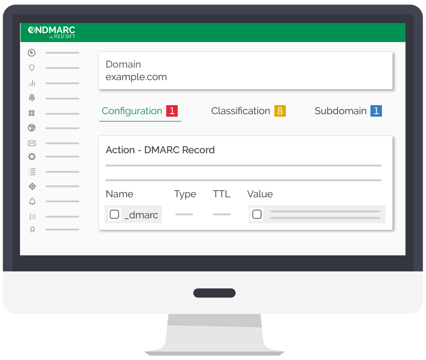
7. What's next?

We hope you're feeling confident now about what to expect from a trusted and proven DMARC provider. If you have any questions simply get in touch with one of the team at contact@redsift.com - we'll be happy to help!

Now that you've read Part 2, check out Part 3 of this handy DMARC Digest series Making DMARC work for your organization for a clear understanding of how DMARC can work for your organization.

Want to see DMARC in action?

An easy-to-use DMARC provider, such as ***OnDMARC*** will help you reach full protection mode far more quickly. Test the waters to see how simple it is to navigate your email landscape and take the first steps to secure your domain from impersonation by signing up to our free trial at: https://login.ondmarc.com/signup.



Domain
example.com

Action - DMARC Record

Name	Type	TTL	Value
□ _dmarc	—	—	□

Stay safe,

Team OnDMARC

References

1. http://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf
2. https://techcrunch.com/2018/11/01/half-fortune-500-dmarc-email-security/
3. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
4. http://www.newsweek.com/origins-nigerias-notorious-419-scams-456701
5. https://enterprise.verizon.com/resources/reports/dbir/
6. https://www.ncsc.gov.uk/guidance/board-toolkit-five-questions-your-boards-agenda
7. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf
8. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Start your DMARC conversation today!

www.ondmarc.redsift.com

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