ONDMARC
by RED SIFT

Investigate - unlock email headers to perfect DMARC

An innovative inspection tool that helps you demystify DMARC for faster implementation and full protection.

ONDMARC
Select compliance profile
OnDMARC Default
OnDMARC Deliverability
UK Minimum Cyber standard
US Binding Operational 18-01

What's the problem?

Waiting a day to verify DNS changes slows you down

Making changes to your DNS typically means waiting quite some time for the first report to arrive - sometimes up to 24 hours - in order to see if the changes you made have had the desired effect. When you do eventually get these reports, you're faced with cryptic email headers to spot the problems with your latest email configuration. This adds another layer of complexity to your investigation and will ultimately slow you down.

Why is Investigate the solution?

You can immediately see the results of your changes

With a feature like *Investigate*, you hold the key to quickly unlocking the information hidden in email headers and turning it into something you can easily work with for perfect DMARC configuration.

You can instantly see the results of every change you made to your email security with a fast automated checklist via *Investigate's* inbox in your OnDMARC account. Simply send a 'test' email to this inbox and it will immediately decode those tricky email headers and produce the status of five key signals you'll want to know about:

✓ DMARC ✓ DKIM ✓ FCrDNS ✓ TLS ✗ SPF*

Investigate will also highlight anything that didn't work and tell you how to resolve it.

Investigate swiftly unlocks cryptic email headers to show you what's working and what's missing from your email security for perfect DMARC configuration.

4 easy steps to verify your changes

1. Send an email to *Investigate's* inbox address from the domain you want to check.
2. The email will appear in *Investigate's* inbox labeled as 'Compliant' or 'Non-compliant'.
3. Open the email for a more detailed breakdown of each protocol and its current status.
4. Adjust your domain setup where necessary by following the instructions provided to you.

Key Benefits

Save time

- With *Investigate* you get to reject faster as you no longer need to wait up to a day to see the impact your changes make.

Save money

- Making informed changes to your email set up is now in your hands - no need for expensive consultants.

Gain knowledge

- By using *Investigate* you'll continually learn more about how email authentication works.

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

Why do these results matter?

Investigate gives you an easy-to-digest overview of your evolving setup, including actionable next steps if something is not configured as it should be. Whilst each security protocol has a specific mission, the more boxes you tick for your email, the lower the risk to both you and those that you communicate with. Think of it as a security scorecard for your domain and with *Investigate's* speedy checks you can confidently achieve full marks and get to full protection (p=reject) faster.

DMARC *(Domain-based Message Authentication, Reporting and Conformance)*

This signals the authentication of your email. It's designed to give you the ability to protect your domain from impersonation, commonly known as email spoofing.

SPF *(Sender Policy Framework)*

This signal validates that your server is authorized to send emails on behalf of the domain it claims to be sent from so the recipient knows you are who you say you are.

DKIM *(Domain Keys Identified Mail)*

A signal for the receiving inbox that your email is digitally signed by the domain it came from, confirming that the email content has not been tampered with along the way.

FCrDNS *(Forward-confirmed reverse DNS)*

This is a strong indicator of your deliverability. If not set up properly, emails are more likely to end up in spam.

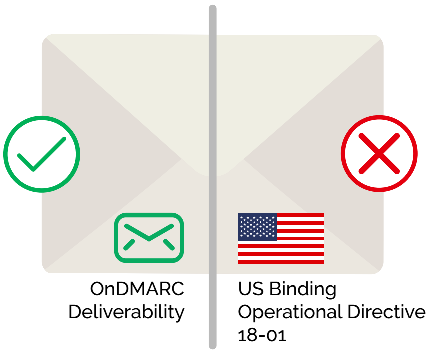
TLS *(Transport Layer Security)*

This signal verifies that the contents of your email can't easily be snooped on by people who are not your intended recipients.

Compare your level of compliance

You can compare the results of your email security against different security profiles: UK Minimum Security Standards, US Binding Operational Directive 18:01, OnDMARC Default (Checks for DMARC, DKIM, SPF and TLS), or simply to maximize email deliverability. This gives you a clear target to aim for.

As a result, you're able to have a clear and concise overview of how your email service is configured, compared directly against your desired level of compliance. This enables you to identify any errors and implement the necessary fixes for compliance.



Get in touch today and find out more about our speedy inspection tool, *Investigate* with OnDMARC.

Member CyberExchange

Member of Microsoft Intelligent Security Association Microsoft

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