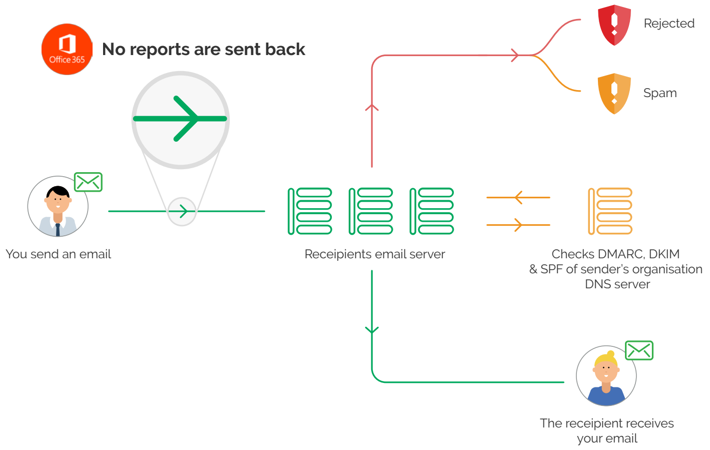
Uncover your blind spots - The only O365 reporting module for DMARC

Uncover your blind spots for accurate DMARC compliance using the only DMARC reporting module available for Office 365.

What's the problem?

DMARC (Domain-based Message Authentication, Reporting and Conformance) is considered the industry standard for email authentication to prevent phishing attacks. However, several email solutions today including Microsoft O365 do not have the capability to send crucial DMARC reports to your reporting service. This means that legitimate emails could be blocked when you move to a p=reject policy for full protection.


Office 365
No reports are sent back
Rejected
Spam
You send an email
Receipients email server
Checks DMARC, DKIM & SPF of sender's organisation DNS server
The receipient receives your email

How does this happen?

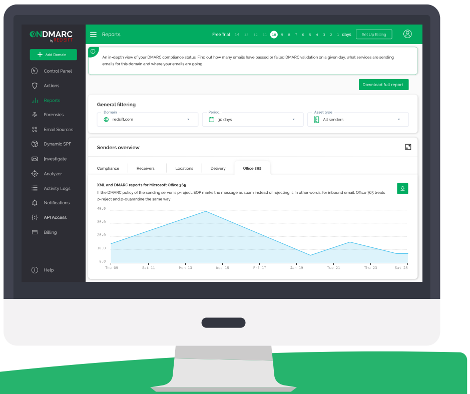
When you invest in a solution like OnDMARC you put a DMARC record in your DNS to be able to view reports sent back from all receiving inboxes. Although Microsoft did once report on DMARC, they turned this feature off some time ago which means you could miss crucial insight (and legitimate senders) that could then be blocked from sending emails once you flick the switch to p=reject.

Even if you are already at p=reject, any new services added in the future that report DMARC via O365 may also be missed and blocked without this module.

How will the O365 reporting module resolve this issue?

At Red Sift we pride ourselves on OnDMARC's full visibility and clear and easy guidance to configure DMARC for your email. This is why we developed a specific solution for the visibility of O365 reports. **To sum up, this module adds value if:**

- You are working on, or have achieved full DMARC compliance
- You use Microsoft Office 365
- You do not have a third party Secure Email Gateway in front of O365



An in-depth view of your DMARC compliance status. Find out how many emails have passed or failed DMARC validation on a given day, what services are sending emails for this domain and where your emails are going.

General filtering

Domain: redsift.com

Period: 30 days

Asset type: All senders

Senders overview

XML and DMARC reports for Microsoft Office 365

If the DMARC policy of the sending server is p=reject, EOP marks the message as spam instead of rejecting it. In other words, for inbound email, Office 365 treats p=reject and p=quarantine the same way.

Key Benefits

No service disruptions

- Remove the O365 reporting blind spot and mitigate the risk of service disruptions for a seamless transition when moving to a policy of p=reject

Attack Intelligence

- Surface attacks targeted specifically at your employees that wouldn't otherwise be visible

Full visibility

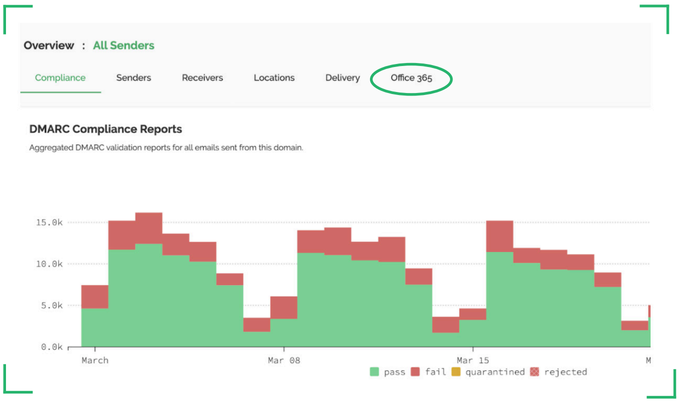
- Get daily aggregate DMARC reports for Office 365 which will allow you to flag sources seen via O365 that have not surfaced in your standard DMARC reports

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

How does it work?

Office 356 can be configured with our fully supported scripts to send daily aggregate DMARC reports (in CSV form) to OnDMARC. This data is then surfaced in the **Reports** section of OnDMARC via a special O365 tab.

One of the things your O365 reporting module will allow you to do is flag sources seen via O365 that have not already been seen in your standard DMARC reports. This fixes the blind spot that would have otherwise been there. Without this module you can move to reject and create service disruptions because legitimate O365 senders may be missed.



DMARC Compliance Reports

Aggregated DMARC validation reports for all emails sent from this domain.

Attack intelligence along the road to reject

If someone were to launch a highly targeted attack specifically at your employees before you are at policy of p=reject then this too will not appear in a regular DMARC report and is, therefore, left undetected. Once in reject, these malicious attacks are blocked by OnDMARC, but you would be missing useful intelligence on who attacked your domain without the O365 reporting module. It's good practice to have full visibility of such targeted attacks as it can be a useful indicator of the threat level the business is experiencing.

How easy is it to set up the o365 module?

We simply provide access to our unique O365 module inside your OnDMARC dashboard which instantly gives you the ability to access the extra reporting functionality for O365. As a fully supported add-on, we will ensure that a member of our support team guides you through the implementation which requires running a few simple PowerShell scripts on your O365 instance.

It is important to note that although Microsoft says they plan to re-enable DMARC reporting in the future they have not yet given a date for this. We fully support our O365 user base and as proud MISA members (Microsoft's Intelligent Security Association) we have put this crucial module in place to ensure that those invested in DMARC compliance have a straightforward path to reject. NB If you have a third party secure email gateway in addition to O365 please speak to us as this requires an alternative solution.

Get in touch today to find out how you can use OnDMARC's O365 Reporting Module to uncover your blind spots for accurate DMARC compliance.

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