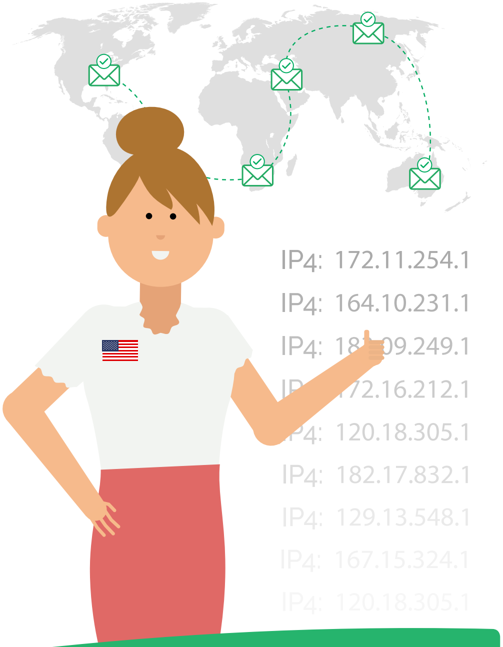
ONDMARC by RED SIFT



OnDMARC simplifies the complexities of SPF for an international exchange company

This case study looks at a non-profit organization specializing in the administration of exchange visitor programs on behalf of the U.S. Government. For more than 50 years they have been responsible for facilitating exchange programs between the U.S. and over 60 countries requiring them to send over 3 million emails each year.

Uncovering services and instantly verifying SPF alignment

With only a basic DMARC reporting tool at the time, the organization knew they were over the SPF lookup limit and that their SPF alignment needed work, but had no guidance from the tool on how to fix it. With different services using their email across the organization the challenge was to identify and secure all senders:

1) Discovery The Chief Technology Officer (CTO) compared how "Unlike other DMARC reporting tools, OnDMARC offered an intuitive interface with clear insight into what's aligned or not aligned for SPF for each service using our domain. This kept us on track and got the job done effectively".

2) Validation The team instantly verified configurations without having to wait 24 hours for changes to take effect in their DNS thanks to *Investigate*. The CTO commented "This tool was fundamental. We used *Investigate* as proof to heads of department that we could safely implement DMARC and SPF without blocking any legitimate business emails".

3) Ongoing protection After securing their domain with OnDMARC a 30-day report revealed that of the 566,395 emails sent from their domain, 68% were fake. The CTO acknowledged that "Due to the nature of what we do we're a high-risk industry for phishing scams" but reports comfortingly confirmed that all unauthorized emails were blocked from delivery.

> *"Nothing has compared to OnDMARC, seeing clear visual breakdowns, reports over time, diving into senders and receiving domains and being able to do a better analysis of where emails are being sent from."*
>
> *Chief Technology Officer, U.S. designated visa sponsor*

Highlights

- In one month unauthorized senders decreased by over 36% after getting to reject with OnDMARC and it continues to drop.
- Simplified SPF management with Dynamic SPF means no more limits or manual DNS changes for 20+ entries.
- OnDMARC's Investigate tool proves to business heads that turning to reject won't block anything legitimate.
- Over 300,000 potential phishing emails were blocked from delivery after implementing OnDMARC.

🌐 www.ondmarc.redsift.com
✉ contact@redsift.com
@redsift

Jumping the lookup hurdle to push the project over the finish line

SPF lookups are a common hurdle for IT teams as a DNS' lookup limit is designed as 10 or fewer. This is to reduce the potential for highly amplified Denial of Service (DoS) attacks against the Internet's DNS infrastructure. For every email service added there are one or more lookups added to the list, a popular service like Gmail, for example, has 3 lookups alone! After an email marketing platform was added to the organization's services, the CTO found "we couldn't handle the number of SPF entries on our stock integration for all of our email sources", confirming the need for a solution.

It quickly became apparent to the CTO that "we had no guidance on what to do from the weekly digests our previous DMARC reporting tool gave us. It was only when searching for a solution that we discovered Dynamic SPF. This tool and OnDMARC's ongoing guidance got us over our technical IP limitations and enabled us to move forward with the project by managing all lookups from inside our account". When using OnDMARC however the team were able to get to work quickly simplifying the management of their 20+ entries in the first 3 days of setting up their account.

Shining a light on Shadow IT to uncover new services

The IT team found that OnDMARC proved to be a great tool for bringing unknown services out from the shadows. This often happens when an email service is brought onto the corporate network without IT's knowledge. You might think nothing of setting up an automated email marketing platform to improve productivity and engagement insights, but not only will this increase the domain's number of lookups, but it's not guaranteed to be secured without going through configuration checks first.

The CTO complimented OnDMARC as a great solution whereby they're "using it to find people signing up for services company-wide. It's great being able to spot them popping up and making sure they're secured for use". This U.S. Designated J-1 Visa Sponsor has since been able to confidently sort through a list of email services using their domain, classifying those that are legitimate and in the process uncovering nearly 7000 unauthorized senders. As a result, the team were able to confidently work their way to p=reject and reduce unauthorized senders. In just one month, for example, a post reject report shows a 36% reduction in unauthorized services and it's set to drop further.

> *"Being able to tell the CEO we blocked over 300,000 illegitimate emails over the summer was a great win for our team and of course the company's reputation."*
>
> *Chief Technology Officer, U.S. designated visa sponsor*

Get in touch to find out more about how Dynamic SPF removes the need for complex SPF records and simplifies management by removing manual updates to your DNS.

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