ONDMARC by RED SIFT

# A U.S. Government organization uses OnDMARC to get 150 domains to reject in 8 weeks

This Government organization runs a US state's official website providing public information and updates about services. Sending over 2,000,000 emails a month to the public about government services makes it essential that communications are secured to protect both sides.

## Upholding government mandated DMARC compliance

For this US state organization, DMARC protection is obligatory as the US government mandated DMARC in the Binding Operational Directive 18-01.[1] Luckily for this particular government organization, they were able to implement DMARC quickly with accessible control over their own DNS and the DNS zones of hundreds of other government entities, protecting them all.

## Reforming email security with modern security protocols

For the organization's Systems Administrator, it was essential that modern security protocols DMARC, SPF, and DKIM were implemented correctly. OnDMARC appealed as an ISO:27001 approved vendor giving them the confidence that transactional services are secure. Here are their highlights having taken hundreds of domains to reject with OnDMARC:

**1) Actionable Insight** The Systems Administrator independently worked through all configurations with OnDMARC's guidance and wasn't slowed down by 24-hour delays to check if each configuration had taken the desired effect thanks to Investigate, the immediate verification tool in OnDMARC. The result; 150 domains in reject in less than 8 weeks.

**2) Simplified SPF** As the organization managing the DNS zones for hundreds of organizations, SPF management once meant time-consuming efforts to manually make DNS updates. With OnDMARC's Dynamic SPF the organization can now add and facilitate unlimited lookups, simply and efficiently managing everything from directly inside OnDMARC.

**3) Securing suppliers** The Analyzer tool allowed the Systems Administrator to check the domain security status of all potential partners, to quickly verify whether or not they can do business with that company. Analyzer also helped to explore when remote senders were reportedly having issues sending emails to their organization as a first checkpoint to spot why.

*"We felt confident in getting to reject quickly and accurately for multiple domains with OnDMARC. A high-value feature for us was Dynamic SPF as we have so many agencies and vendors sending on our behalf. This was unique to other vendors and really helped in terms of simple and efficient SPF management."*

*- Systems Administrator at this U.S State Government organization*

## Highlights

- In 30 days 9,641 emails were sent from 104 email services, of which 23% were fake. All of the fakes were blocked by OnDMARC.
- Over 150 domains were taken from reporting only mode to full protection (p=reject) in less than 8 weeks after implementing DMARC.
- OnDMARC eliminated time-consuming efforts to make manual DNS updates to hundreds of DNS zones managed by the organization.
- In 90 days 77,000+ emails were sent with a 100% delivery rate as a result of DKIM and SPF passing perfectly thanks to OnDMARC.


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

## OnDMARC working in harmony with SEGs

The U.S Government organization, like most organizations, first invested in an expensive Secure Email Gateway to defend against inbound email fraud. With this in place, they then recognized the importance of protecting against the fraudulent activity that wasn't crossing their network boundary.

DMARC is the perfect solution, providing insight into all phishing emails that were being sent from their domains. However, with over 150 domains they needed to find a way to make the influx of DMARC data both comprehensible and manageable that they could accurately and effectively configure security protocols for every domain.

The Systems Administrator said, "It was essential that the tool would provide clear visibility. We found that after comparing other providers, the general layout and simplicity of OnDMARC's reports proved to be leaps and bounds better than most of what was out there". In the end, it was an easy investment to justify under the cost of operations and the final piece of the email security puzzle to protect against email fraud.

## Ongoing protection after reject continues to yield results

As an organization with email campaigns regularly deployed by a number of vendors, the Systems Administrator needed to be confident in ongoing protection and deliverability. To facilitate this for over 150 domains, the correct configuration of DKIM and SPF were essential to ensure they were continuously passing DMARC verification. This would not only protect each domain once in p=reject but also improve email deliverability.

Once the organization had all 150 domains in reject, they found the ongoing reports to be very reassuring. For example, a 90-day report showed 77,000+ emails sent with a 100% delivery rate as a result of DKIM and SPF still passing perfectly. This report was enough reassurance for the Systems Administrator who said: "we felt on the ball with constant reassurance from reports that nothing is failing thanks to OnDMARC".

As well as improved deliverability from legitimate emails sent by the organzation, the fraudulent emails being sent from their domain were successfully blocked time and time again. Take a 30-day report, for example, which revealed 9,641 emails sent from 104 email services, of which 23% were fake and successfully blocked by OnDMARC.

*"We tried DMARC Analyzer which lacked some information we felt should have been provided for effective insight and Fraudmarc were ridiculously expensive. Overall OnDMARC was leaps and bounds better than most of what's out there."*

*- Systems Administrator at this U.S State Government organization*

**Get in touch** today to find out more about how you can use OnDMARC to secure your email domain and block phishing attacks.

Member CyberExchange

Member of Microsoft Intelligent Security Association

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

[1] https://cyber.dhs.gov/bod/18-01/

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