



OnDMARC's Slack Bot helps DST Controls make ongoing email protection easy

DST Controls has manufactured control system panels and OEM sub-systems for industrial customers since 1975. With their engineers often needing remote access to sensitive customer information, cybersecurity is paramount to protect this information and keep it confidential.

Maintaining existing email sending services

When the IT team discovered email deliverability issues one day they were puzzled as they had already configured their domain into a DMARC reject policy. Usually this boosts email deliverability as DMARC blocks email impersonation, repeatedly reinforcing to receiving inboxes that your message is genuine. This prompted Andrew Pong, Senior ICS Solutions Architect to find a solution that would give them visibility into the root cause of such unexpected changes, as well as guidance on how to resolve it.

High-level security without the high-level price

As a small, growing business with big customers, a key criteria for a suitable DMARC provider was high-level security without the high-level price tag. Additionally, as a small team, they must ensure email security processes run efficiently and attention is only given where necessary. Here's how OnDMARC met their needs:

1) Offline alerts Compliance reports via Slack meant Senior Solutions Architect Andrew Pong could be confident in ongoing protection. In his own words, "Instead of flooding me with noise, it tells me clearly if there's a problem and how to address it. This saves me having to remember to log in and check".

2) Authorizing services OnDMARC's reporting meant the IT team knew exactly what the 192 unauthorized sending services using the company domain were. All of these emails were blocked from being delivered, protecting the business' reputation, customers and partners.

3) Supporting SAML SAML (Security Assertion Markup Language) is a Single Sign On standard available with OnDMARC. Senior Solutions Architect, Andrew Pong, found onboarding "pretty quick" when getting set up.



"As a testament to your service, the Slack bot gives me accurate alerts instead of flooding me with noise. If there's a problem it tells me clearly as well as how to address it."

Andrew Pong, Senior ICS Solutions Architect

Highlights

- In just 90 days 192 unauthorized services were blocked from sending emails from their domain using OnDMARC.
- Cutting through the noise with clear, concise and regular compliance reports delivered via OnDMARC's Slack Bot. This tells the IT team when there's an issue for reliable ongoing protection.
- 60% of the emails sent in a 90 day period failed DMARC checks, all were reported and safely blocked from delivery using OnDMARC.
- The Analyzer tool in OnDMARC gave DST the ability to verify any supplier's email security in seconds, reducing the risk of email impersonation into their business.

Automatically highlighting changes within the email landscape and alerting users to necessary updates

Before OnDMARC, the team were having to manipulate SPF and DKIM manually with regular updates to keep everything aligned. This can be dangerous as a single misalignment in a p=reject policy can stop legitimate emails from being delivered. For DST, maintenance would often be in reaction to a reported fault with their emails, such as deliverability.

Unfortunately, without ongoing pass/fail reports, it wasn't totally clear how long emails had been failing for and to add to this, investigations often ending up being time-consuming with no clear root cause. Senior ICS Solutions Architect Andrew Pong described it as "doing a lot of random stuff", whereas "OnDMARC provided me with precise actions to take without me having to sit and figure out what I have to do next to get the service working correctly again. Previously I might have spent days on configuring and testing manually."

Speedy spot-checks instantly verify a supplier's security

As a general rule, the stronger your supplier's security, the lower the risk to you. When Andrew received suspicious email reports about DST's outsourced food delivery service, he needed to investigate quickly. OnDMARC's Analyzer tool meant not needing to have any initial involvement from the supplier to investigate. Instead Andrew used Analyzer "to check our supplier's security when spot-checking or as a fast investigation to potential compromise". With the results through in seconds for the company's DMARC, SPF, and DKIM status, further action can be confidently taken. For example, getting in touch with the supplier to request they configure DMARC to block email impersonation, alongside the report to back it up.

Since this incident, a spoof email was reported from their external accounting firm. Once again the business used Analyzer to spot-check this supplier, before going on to carry out an email security audit on their top 10 suppliers and customers to further secure the company.



"OnDMARC's the most user-friendly service which provided me with actions to take, without me having to sit and figure out what I have to do next in order to ensure the service is working correctly."

Andrew Pong, Senior ICS Solutions Architect

Get in touch today to find out more about how OnDMARC can secure your domain and provide regular reports directly to Slack, if anything needs your attention.



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](https://twitter.com/redsift)