



Solairus Aviation simplifies email security protocols and jettisons email fraud with OnDMARC

Solairus Aviation is a private aviation services company whose core business is managing the private aircraft of both large organizations and high-net-worth individuals. The company is highly regarded for customizing its services for individual client requirements, such as assistance in recouping fixed costs for an aircraft by offering to charter it out to the public.

Shutting down the spoofs and making email trustworthy

The Solairus team sends approximately 1.5 million emails per month. With this in mind, it was imperative that not only do email operations remain resilient and deliverability rates high, but that all emails are secure and the chance of a client ever receiving a fraudulent email is eliminated.

Upholding high standards for email security and performance

Processing invoices and managing expenses daily, Solairus needed to ensure that crucial business email functions were protected against potential vulnerabilities including email impersonation leading to phishing attacks and ultimately, data breaches.

1) Securing the supply chain Despite having traditional secure email gateway protection in place, Solairus knew that it was imperative to secure their domain to block phishing attacks and assure partners, suppliers and customers that invoices and financial documents would only be exchanging hands between the two parties.

2) Simplified SPF OnDMARC made it easy to accept more SPF records, a feature not typically supported by other tools. The IT Director, Jeff Ritzinger, reported that the ability to get immediate verification on their SPF configurations with a tool like *Investigate* also meant fast reliable insight saving them time.

3) Email deliverability Before using Red Sift's automated solution, Solairus's IT team were dealing with manual SPF flattening, an unreliable option and resource-heavy to manage. With Red Sift's *Dynamic SPF* feature they have been able to automatically keep their SPF records up to date.

"We take in invoices and manage expenses all day long so we're aware it's open to being taken advantage of if malicious emails get through. Ensuring we're able to function securely with OnDMARC is absolutely imperative."

Jeff Ritzinger, IT Director, Solairus Aviation

Highlights

- Solairus went beyond the 10 SPF lookup limit and can now automate updates from inside their account without manual DNS updates.
- Email deliverability continues to increase after deploying OnDMARC thanks to easy configurations resulting in strong signals of authorization to receivers.
- Solairus instantly verified configurations inside OnDMARC without waiting 24 hours to see if they had the desired effect from DNS updates.

Migrating to OnDMARC

Solairus was able to deploy OnDMARC with ease, migrating from another DMARC product. Although the organization was already at full protection (p=reject), OnDMARC was the product of choice ultimately because it went beyond reporting with its own configuration instructions and the ability to easily review SPF limits. This additional feature made it a very "straight forward decision" for Jeff, Director of IT, to switch solutions. Jeff also said "the software does all the work for me" allowing the IT team to simply make routine check-ins and easily spot if there are any new sources that they weren't aware of, particularly useful for identifying and eliminating any shadow IT issues.

Simplicity is key with Dynamic SPF

Jeff uses OnDMARC to check the state of their email landscape on a regular basis. Having previously tried other DMARC solutions, they quickly found that being able to perform more than 10 SPF lookups isn't typically supported. However, with Red Sift's *Dynamic SPF*, he has been able to ensure that every record for all third party services is up to date at the point of query and hasn't become obsolete.

Quick insights when it matters

Thanks to OnDMARC, the IT team's ability to ascertain immediate feedback on the configuration status of their domains saves them time and untangles the complexity of decoding encrypted email headers. This means changes made to their DNS can be verified within seconds, not days. Jeff explains "as a priority initiative, we focus on understanding our cybersecurity and what we need to do with updating policies - especially since we have a clear idea of what we will and won't accept from the people we do business with". OnDMARC's speedy configuration checks are enabled by the *Investigate* feature, which gives Solairus Aviation's IT team the ability to validate the status of five key signals: DMARC, SPF, DKIM, FCRDNS, and TLS, ensuring that they're not missing anything.



"Deployment was really simple and the software does all the work for me. I routinely go in there to check and make sure we don't have any new sources that I'm not aware of."

Jeff Ritzinger, IT Director, Solairus Aviation



Get in touch today to find out more about how you can use OnDMARC to break free from the 10 SPF lookup limit and secure your domain from impersonation.



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.com

 contact@redsift.com

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