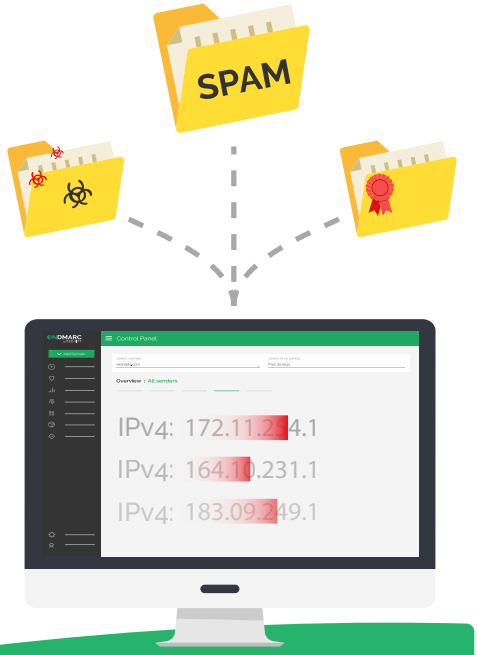
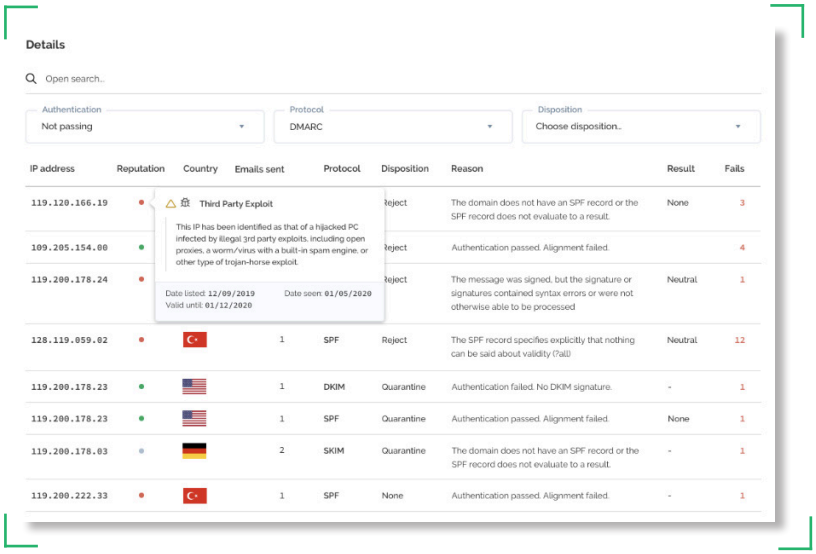
ONDMARC by RED SIFT



Quickly surface and block bad senders with OnDMARC's Threat Intelligence

Threat Intelligence from OnDMARC automatically identifies IPs sending on your domains that pose a threat. This means you can focus your time on identifying and configuring legitimate sources on your journey to DMARC compliance.



Which threats will OnDMARC identify?

For each IP address, OnDMARC's *Threat Intelligence* will give a breakdown of the specific type of threat and when it was last seen.

OnDMARC classifies these threats into three major categories:

1) Third Party Exploits The IP has been identified as belonging to a hijacked PC infected by illegal 3rd party exploits, including open proxies, a worm/virus with a built-in spam engine, or other type of trojan-horse exploit.

2) Advisory listing The IP is listed on a spam blacklist because it's been involved in the sending, hosting or origination of unsolicited bulk email (SPAM).

3) Low Reputation The IP has been identified as sending low reputation email. Low reputation is classified as; email that has signs of being unsolicited, being sent by a compromised account, webform or content management system, or comes from an email list that has poor hygiene (out of date email address etc), among other signs.

Key Benefits

Spot threats from sending IPs

- OnDMARC's Threat Intelligence feed provides a reputation score for every sending source and IP OnDMARC detects so you know if it needs your attention

Identify the root cause

- Quickly identify issues with valid senders such as email deliverability problems, or which senders are immediate threats

Understand threat types

- Reveal a specific breakdown of each threat type and when it was last seen for each IP address, such as third party exploits, advisory listings and low reputations

www.ondmarc.redsift.com
team@ondmarc.com
@redsift

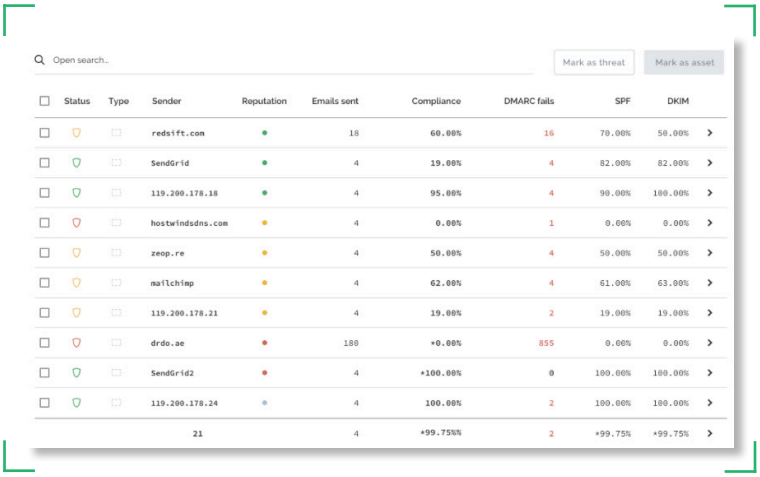
How does it work?

Every time OnDMARC sees a new IP, it is run through our 'IP Forensics' tool and checked against SPAM blacklists and exploits.

If the IP is clean it receives a green flag. If the IP is listed because a threat of some kind has been identified, it receives a red flag.

For sending sources with multiple IP's, OnDMARC gives an aggregate score based on the threat status of each IP. Irrespective of how many IP's are sending emails on behalf of a source, if just one IP receives a red flag, that source will be given an amber warning flag.

If more than 10% of a sources IP's are identified as threats the source will be flagged as red.



Threat Intelligence is a key tool on the journey to DMARC Compliance

The DMARC standard is the best method to secure your email domains against phishing attacks, secure your supply chain and employees, and protect your brand reputation. OnDMARC's *Threat Intelligence* will speed up the journey to compliance by quickly identifying senders with a low reputation and blocking these potential threats automatically..

Secure your company. Protect your clients.

signup.ondmarc.com

Member CyberExchange

CYBER ESSENTIALS

bsi. ISO/IEC 27001 Information Security Management IS 672913

Crown Commercial Service Supplier

GLOBAL CYBER ALLIANCE

Member of Microsoft Intelligent Security Association Microsoft

UK CLOUD AWARDS 2019 WINNER

2017 Computing Security Awards WINNER Anti Phishing Solution of the Year

CYBER SECURITY EXCELLENCE AWARDS WINNER 2020

RED SIFT

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.

Products on the platform include OnDMARC and OnINBOX, SaaS applications that work together to close the net on the phishing problem by blocking outbound phishing attacks and analyzing the security of inbound communications for company-wide email threat intelligence.

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