Block phishing attacks & boost deliverability with Red Sift OnDMARC

What is DMARC?

DMARC, which stands for Domain-based Message Authentication, Reporting & Conformance, is an email authentication protocol which stops bad actors from using your domain to send fraudulent emails. It builds on the DKIM and SPF protocols, adding a reporting and enforcement function that allows senders to block fraudulent email impersonating a legitimate domain and increases deliverability.

DMARC uses the validation results of SPF & DKIM to understand if the email is authorized by the domain owner. Using this validation, it can tell receiving servers to reject or quarantine such email.

96%	On average, 96% of cyberattacks start with a phishing email
$4.6M	The average cost of a breach through phishing is $4.65 million
-5%	Organizations see a 5% drop in stock price in the first 6 months after a breach

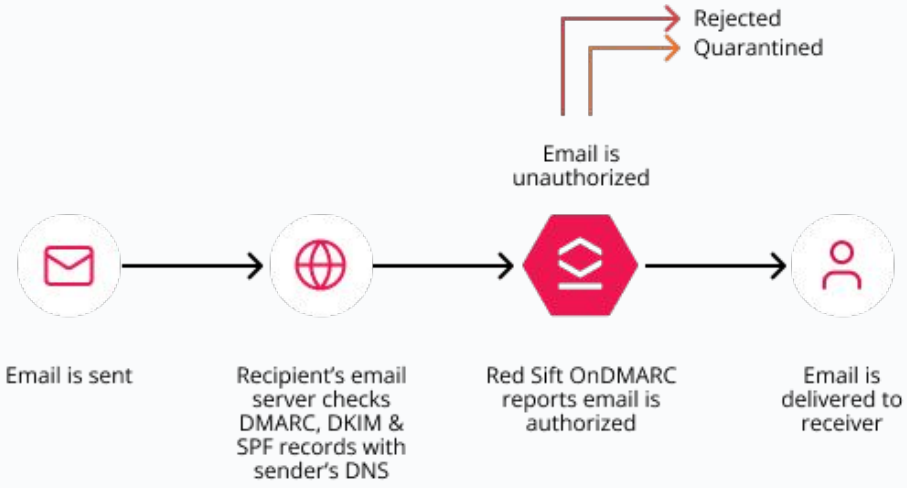
What is SPF?

Sender Policy Framework is a protocol that validates if a server is authorized to send emails on behalf of a domain.

What is DKIM?

DomainKeys Identified Mail is a digital signature that confirms that the email content has not been tampered with.

How does Red Sift OnDMARC work?



Take back control of your email reputation

With OnDMARC, you can stop exact domain impersonation in the inbox by getting to DMARC enforcement (p=reject) quickly and effectively. You will also boost deliverability and be eligible for Brand Indicators for Message Identification (BIMI).

18.5K

Unauthorized sending sources successfully blocked

99%

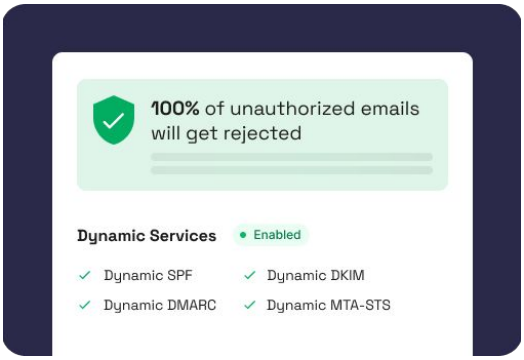
Average email deliverability rate

6 weeks

Time taken to reach full DMARC compliance

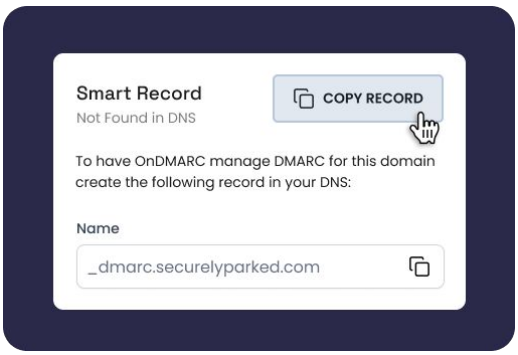
Simplify email security with a single DNS update

Configure SPF, DKIM, DMARC, BIMI, and MTA-STS in one place. No more manual change requests, no more DNS errors. And best of all, our customers do it in an average 6-8 weeks.



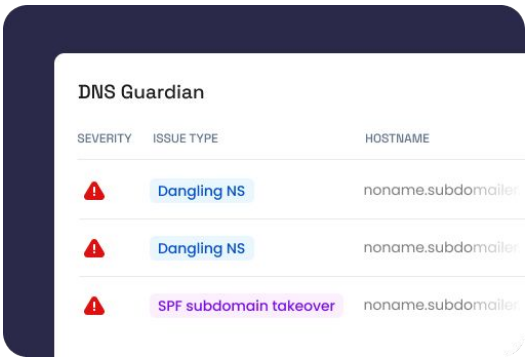
Overcome the 10 SPF lookup limit

Dynamic SPF provides a reliable SPF lookup limit fix by consolidating records and removing the need for macros. It simplifies management and ensures full deliverability across legacy systems and third-party gateways.



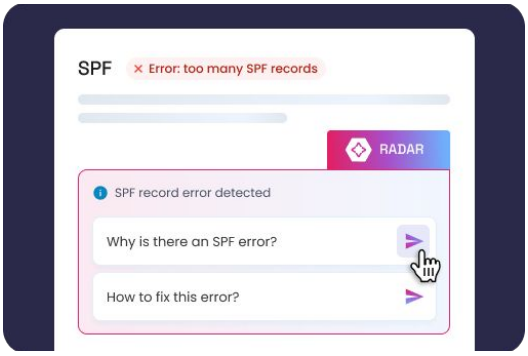
Identify subdomains with misconfigured or orphaned DNS records

DNS Guardian ensures better hygiene with continuous monitoring of your DNS configuration to prevent SubdoMailing, dangling DNS, and CNAME takeovers.



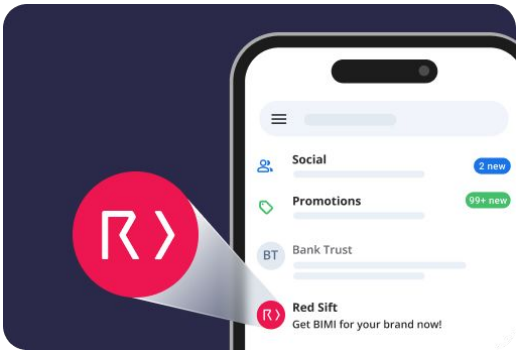
Find and fix email misconfigurations 10x faster

Red Sift Radar pinpoints issues like misaligned SPF records or unauthorized IPs and helps resolve them before they impact deliverability or security. Radar is fully integrated with Red Sift OnDMARC, making it the first LLM embedded in a DMARC application.



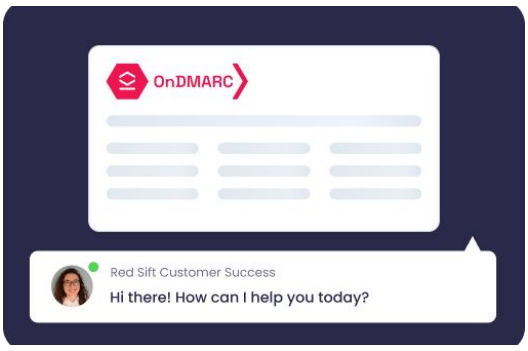
Stand out in the inbox with BIMI

Red Sift OnDMARC includes integrated VMC provisioning to simplify BIMI adoption. Improve open rates by 39% and boost brand recall by 44%.



Work with an industry-leading Customer Success team

Your dedicated account team — including customer success managers and engineers — supports you every step of the way. From kickoff to completion, you'll have expert guidance on hand whenever you need it.



Attackers don't stop at DMARC, and neither should you

Attackers exploit subdomains, gaps in DNS, and convincing lookalikes to bypass traditional controls. That's why comprehensive brand protection needs more than just DMARC.

Protect

Stop attackers from sending mail as you

Start by protecting your real domain with DMARC to block unauthorized senders and prevent exact-domain spoofing.

Monitor

Defend against attacks that bypass DMARC

DNS Guardian monitors for overlooked risks like dormant subdomains and DNS misconfigurations that attackers can exploit.

Enhance

Protect against lookalike domains

Red Sift Brand Trust uncovers lookalikes across the web, helping you identify threats and protect your brand from impersonation at scale.

Red Sift helps 1,200+ customers around the world

Capgemini ATHLETIC GREENS TUI Domino's zoominfo Rakuten

Ready to chat?

See how the world's most secure companies use Red Sift to power their cyber resilience at redsift.com.