RED SIFT

RED SIFT OnDMARC

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

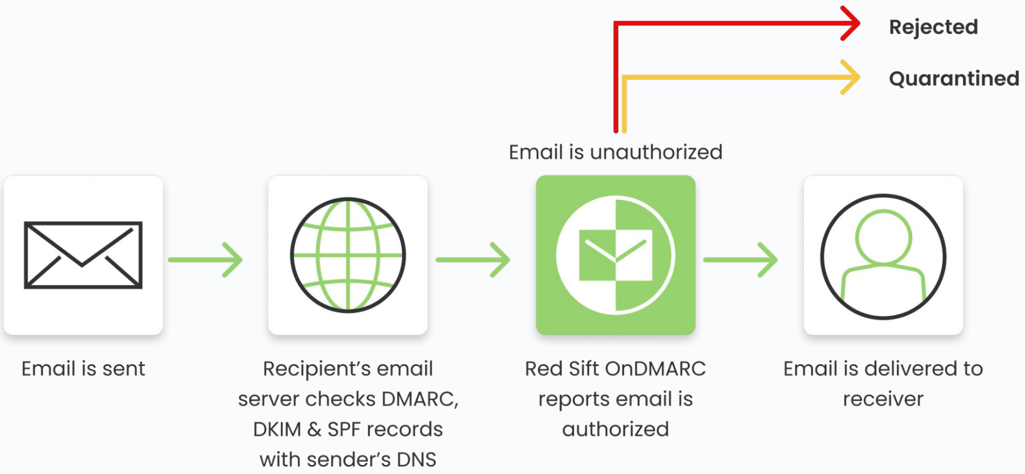
What is SPF?

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?



Rejected

Quarantined

Email is unauthorized

Email is sent

Recipient's email server checks DMARC, DKIM & SPF records with sender's DNS

Red Sift OnDMARC reports email is authorized

Email is delivered to receiver

Take back control of your email reputation with Red Sift OnDMARC

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

itv

99%

Average email deliverability rate

WISE

6 weeks

Time taken to reach full DMARC compliance

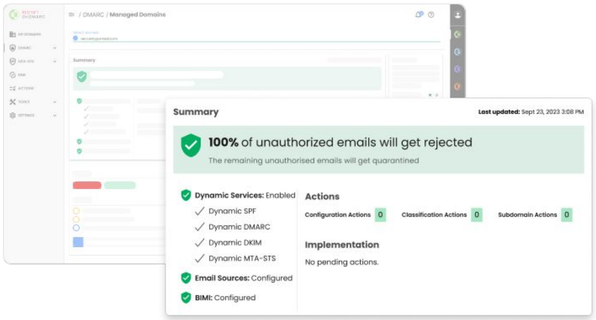
pipedrive

The fastest path to DMARC enforcement

Our customers see a 6-8 week average time to full DMARC enforcement (p=reject or p=quarantine) including large enterprises with broad networks of sending domains.

Simplify management of SPF, DKIM, DMARC & MTA-STS

Make a one-time DNS change and manage all of your email authentication from OnDMARC's UI. Save time, avoid manual configuration errors and quickly add, authenticate or remove services.



Summary

Last updated: Sept 23, 2023 3:08 PM

100% of unauthorized emails will get rejected

The remaining unauthorised emails will get quantined

Dynamic Services: Enabled

- ✓ Dynamic SPF
- ✓ Dynamic DMARC
- ✓ Dynamic DKIM
- ✓ Dynamic MTA-STS

Email Sources: Configured

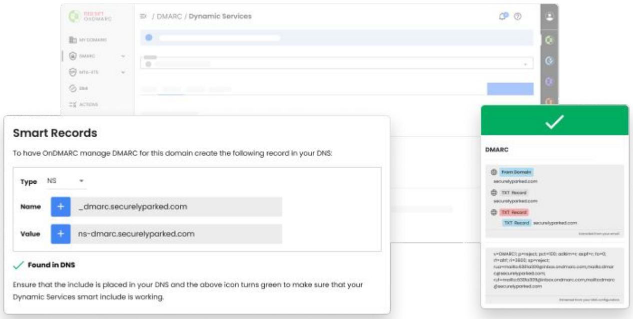
BIMI: Configured

Actions

Configuration Actions 0 Classification Actions 0 Subdomain Actions 0

Implementation

No pending actions.



Smart Records

To have OnDMARC manage DMARC for this domain create the following record in your DNS:

Type NS

Name _dmarc.securelyparked.com

Value ns-dmarc.securelyparked.com

✓ **Found in DNS**

Ensure that the include is placed in your DNS and the above icon turns green to make sure that your Dynamic Services smart include is working.

DMARC

From Domain securelyparked.com

TXT Record securelyparked.com

TXT Record

TXT Record securelyparked.com

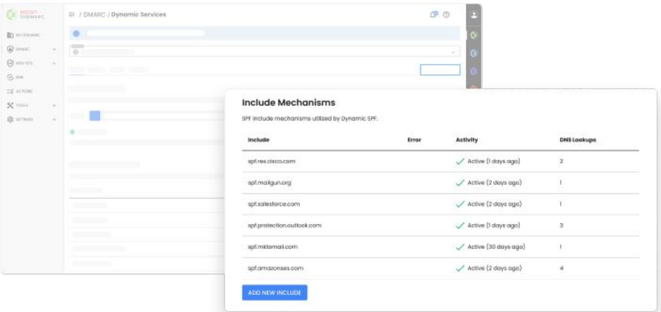
v=DMARC1; p=reject; pct=100; adkim=r; aspf=r; fo=0; rf=afrf; ri=3600; sp=reject; rua=mailto:[illegible]@inbox.ondmarc.com,mailto:dmarc@securelyparked.com; ruf=mailto:[illegible]@inbox.ondmarc.com,mailto:dmarc@securelyparked.com

RED SIFT

RED SIFT OnDMARC

Overcome the 10 SPF lookup limit

Streamline SPF management and avoid manual DNS changes. No macros means better deliverability with legacy receiving infrastructure.



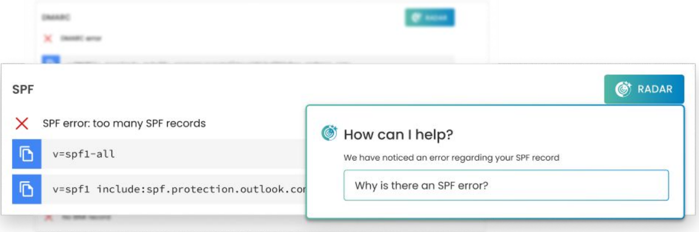
Include Mechanisms

SPF include mechanisms utilized by Dynamic SPF.

Include	Error	Activity	DNS Lookups
spf.res.cisco.com		✓ Active (1 days ago)	2
spf.mailgun.org		✓ Active (2 days ago)	1
spf.salesforce.com		✓ Active (2 days ago)	1
spf.protection.outlook.com		✓ Active (1 days ago)	3
spf.mktomail.com		✓ Active (30 days ago)	1
spf.amazonses.com		✓ Active (2 days ago)	4

Find and fix misconfigurations 10x faster

Through its familiar chat interface and intuitive in-app interactions, Radar identifies and diagnoses email security issues and embeds these insights directly into where you're already working.



SPF error: too many SPF records

```
v=spf1-all
v=spf1 include:spf.protection.outlook.co
```

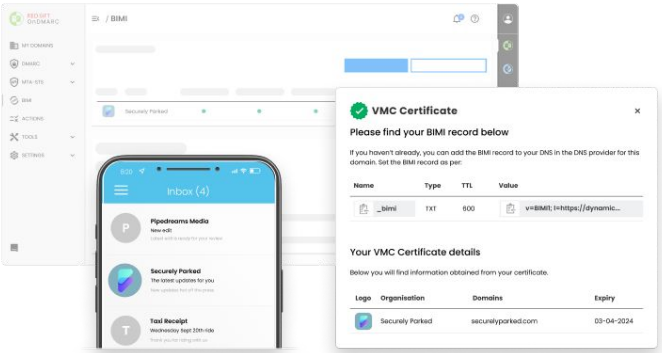
How can I help?

We have noticed an error regarding your SPF record

Why is there an SPF error?

Boost brand recognition and deliverability with BIMI

Red Sift OnDMARC is the only BIMI solution on the market with integrated VMC provisioning. Improve open rates by 39% and increase brand recall by 44%.



VMC Certificate

Please find your BIMI record below

If you haven't already, you can add the BIMI record to your DNS in the DNS provider for this domain. Set the BIMI record as per:

Name	Type	TTL	Value
_bimi	TXT	600	v=BIMI1; l=https://dynamic...

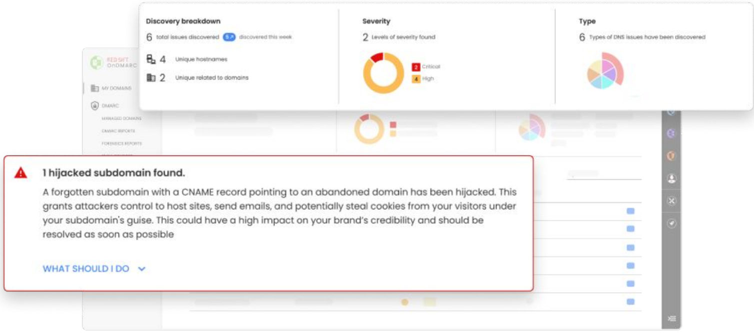
Your VMC Certificate details

Below you will find information obtained from your certificate.

Logo	Organisation	Domains	Expiry
	Securely Parked	securelyparked.com	03-04-2024

Protect against spam that bypasses DMARC

With DNS Guardian, you can swiftly identify and stop malicious mail that bypasses DMARC, including spam from domain takeovers and SubdoMailing.



Discovery breakdown

6 total issues discovered 5 ↗ discovered this week

4 Unique hostnames

2 Unique related to domains

Severity

2 Levels of severity found

2 Critical

4 High

Type

6 Types of DNS issues have been discovered

1 hijacked subdomain found.

A forgotten subdomain with a CNAME record pointing to an abandoned domain has been hijacked. This grants attackers control to host sites, send emails, and potentially steal cookies from your visitors under your subdomain's guise. This could have a high impact on your brand's credibility and should be resolved as soon as possible

WHAT SHOULD I DO ⌄

RED SIFT

RED SIFT OnDMARC

Award-winning OnDMARC features

Dynamic Services
Manage SPF, DKIM, DMARC, and MTA-STS records from inside the OnDMARC interface without needing to access your DNS.

Sender Intelligence
Turn complex forensics into clear, actionable information about your sending sources in order to pinpoint and solve issues quickly.

Dynamic SPF
Authenticate SPF across all approved sending services and ensure your email deliverability is uninterrupted.

Investigate
Verify if your approved sending services are set up correctly and check them against compliance profiles, including Google & Yahoo bulk sending requirements.

Integrated BIMI
Streamline and automate the VMC provisioning process to make the journey to BIMI as smooth as possible.

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

NEW!

Red Sift Radar
By integrating internet-scale intelligence, security analyst skills, and LLM power directly into workflows, Radar helps prevent email-based incidents before they happen.

Red Sift helps 1,000+ customers around the world

Capgemini ATHLETIC GREENS Domino's TalkTalk zoominfo

Ready to chat?

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

Users Love Us
Leader WINTER 2025
Leader Europe WINTER 2025
Best Meets Requirements WINTER 2025
Easiest To Do Business With WINTER 2025
High Performer WINTER 2025