

What is DNS Guardian and how does this feature work?

Enhance OnDMARC by adding DNS Guardian – a cutting-edge feature designed to identify and mitigate risks associated with subdomains that are susceptible to takeover (dangling DNS) and subdomains already controlled by bad actors. By leveraging our existing subdomain discovery capabilities, DNS Guardian will provide comprehensive insights into potential vulnerabilities and security threats within an organization's domain infrastructure. Best of all, we are the only DMARC provider able to offer this unique capability, thanks to Red Sift ASM and our deep expertise in DNS.

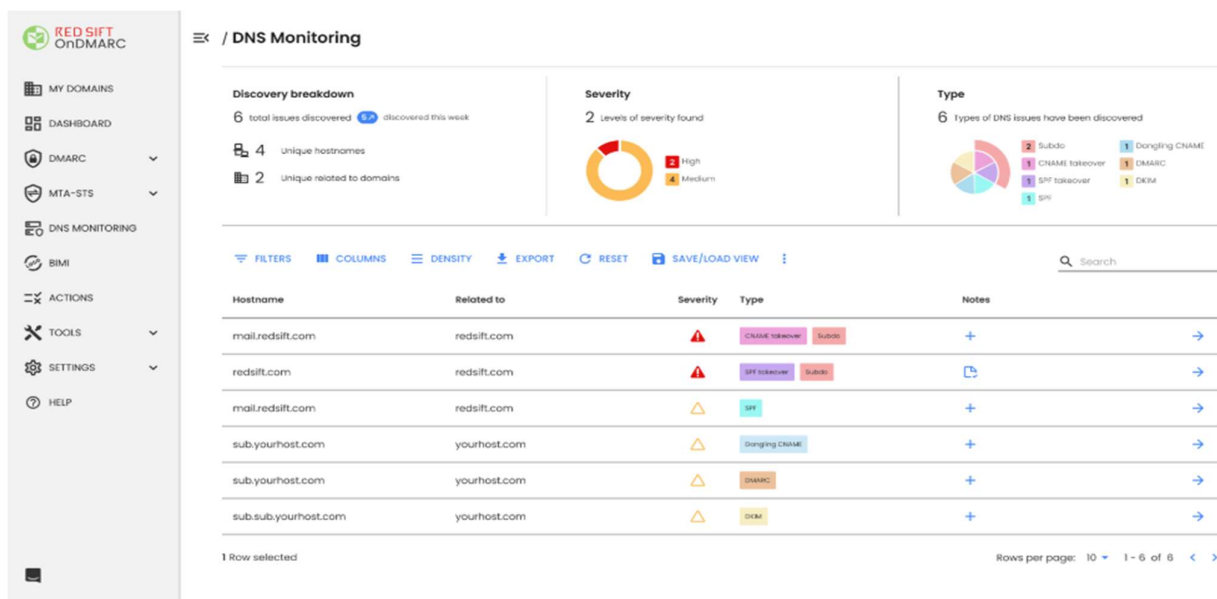
DNS Guardian is a feature available only in our [OnDMARC Premier](#) plan. It utilises our proprietary scanning technology to map out and scan all subdomains of the domains pointing to the *rua address* to OnDMARC to detect any issues that could allow attackers to send authenticated email as you or serve potentially malicious pages using your domain.

It is divided into two sections.

Header Section

The DNS Guardian section of OnDMARC contains the following information in the top section:

1. **Discovery Breakdown:** Shows how many individual issues have been identified. Also broken down by unique hostname and unique related to domains
2. **Severity:** Donut chart showing the breakdown of issues by severity (Either Medium or High)
3. **Type:** Pie chart showing the volume of each issue type.



The screenshot shows the OnDMARC DNS Monitoring dashboard. The left sidebar contains navigation links: MY DOMAINS, DASHBOARD, DMARC, MTA-STX, DNS MONITORING, BIM, ACTIONS, TOOLS, SETTINGS, and HELP. The main content area is titled "/ DNS Monitoring" and displays three summary charts: Discovery breakdown (6 total issues, 5 discovered this week), Severity (2 levels of severity: 2 High, 4 Medium), and Type (6 types of DNS issues: Subdo, CNAME takeover, DMARC, SPF takeover, DKIM, and Dangling CNAME). Below the charts is a table with columns: Hostname, Related to, Severity, Type, and Notes. The table lists several subdomains and their associated issues, including mail.redsift.com, redsift.com, and sub.yourhost.com. The bottom of the dashboard shows "1 Row selected" and "Rows per page: 10 - 1 - 6 of 8".

Hostname	Related to	Severity	Type	Notes
mail.redsift.com	redsift.com	High	CNAME takeover Subdo	+
redsift.com	redsift.com	High	SPF takeover Subdo	+
mail.redsift.com	redsift.com	Medium	SPF	+
sub.yourhost.com	yourhost.com	Medium	Dangling CNAME	+
sub.yourhost.com	yourhost.com	Medium	DMARC	+
sub.sub.yourhost.com	yourhost.com	Medium	DKIM	+

Table Section

Below the header section is a table. This section contains information about each individual issue that has been identified, as well as the ability to click into that issue to see more detail. The following information is available on this table:

1. **Hostname:** This is the hostname that has an issue detected
2. **Parent Domain:** This is the parent domain for the hostname with the issue
3. **Issue Type:** This is the issue type, such as Subdo, Dangling CNAME, CNAME Takeover, SPF Takeover, SPF, DMARC, DKIM, Dangling NS
4. **Severity:** This is the severity of the issue, either Medium or High
5. **Affected Record:** This is the DNS record that has been affected
6. **Notes:** You can leave notes next to each issue by pressing the +
7. **Arrow:** This will take you to a different screen that gives you more detail on the issue itself and how to fix it

Issue Type: Subdo Attack

If an issue has been detected related to the SubdoMailer campaign, the following information will be displayed:

8. **Hostname:** This is the hostname that has an issue detected
9. **Parent Domain:** This is the parent domain for the hostname with the issue
10. **Issue Type:** This is the issue type, such as Subdo, Dangling CNAME, CNAME Takeover, SPF Takeover, SPF, DMARC, DKIM, Dangling NS
11. **Severity:** This is the severity of the issue, either Medium or High
12. Explanation of the detected issue and how to fix it
13. **Record information:** Includes the chain that is dangling and the relevant records
14. **IP Addresses**
15. **Page Screenshot** (if an A record has been detected)
16. **SPF Checker:** Clicking this link will take you to our public SPF checker and will show the affected SPF records and tree

17. **Detected Emails:** A summary of the volume of any emails that have been sent as well as a link to the Forensic data for those emails where available

/ DNS Monitoring / Details
1 of 6 < >

mail.redsift.com Sub - CNAME takeover

▲ 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.

For intentional CNAME delegation

If this is an intentional CNAME delegation you should work with the team controlling **subdo.hijacker.com** to remove **include_splhijacker.com** from that SPF record. Below is an example of what the include could look like in the hijacked record within your DNS provider.

Type	Name	Content
TXT	mail	v=spf1 include_splhijacker.com ~all

For unintentional CNAME delegation

If this is not an intentional CNAME delegation go to your **DNS provider** and remove the CNAME from **mail.redsift.com**. Below is an example of the record that needs to be removed.

Type	Name	Content
CNAME	mail	subdo.hijacker.com

[Show less](#)

Screenshot discovered

Details

Related to
[redsift.com](#)

Date observed
2023-05-23 17:35:18 (16 hours ago)

Affected subdomain
mail.redsift.com

Notes
[+ ADD NOTE](#)

CNAME information

Hijacked CNAME

mail.redsift.com => subdo.hijacker.com

IP addresses (A records)

123.123.123.10

SPF records

SPF Record
 v=spf1 include_splhijacker.com ~all

[VIEW FULL CHAIN IN SPF CHECKER →](#)

MX records

mailhijacker.com

mail2hijacker.com

Detected emails

This domain is configured to send/receive emails

102 mails have been detected from this domain. View a list of emails by clicking on the button below.

Issues found

- ▲ 3 emails detected from Senders with bad reputations
- △ 2 emails detected from Senders with average reputations

[MORE DETAILS →](#)

Issue Type: Dangling DNS

If a Dangling DNS issue has been detected, the following information will be displayed:

- 18. **Hostname:** This is the hostname that has an issue detected
- 19. **Parent Domain:** This is the parent domain for the hostname with the issue
- 20. **Issue Type:** This is the issue type, such as Subdo, Dangling CNAME etc
- 21. **Severity:** This is the severity of the issue, either Medium or High
- 22. Explanation of the detected issue and how to fix it
- 23. **Record information:** Includes the chain that is dangling and the relevant record
- 24. **Domain Protection Tips:** These are tips on how to maintain good DNS hygiene