



# Security posture report

Domain: cloudfare.com Started: 5/5/2026, 7:16:09 PM Completed: 5/5/2026, 7:16:12 PM

## RISK SCORE

**89** / 100  
**Good**



## Executive summary

Your domain shows a solid external security posture with 2 items worth addressing. None are catastrophic, but closing these gaps will make you noticeably harder to attack and easier to insure.



## Issues to address (2)

**Header: content-security-policy** MEDIUM

WEB

CSP restricts which sources of scripts, styles, and other content the browser will load - the strongest defense against XSS.

**FIX**

Define a CSP appropriate to your site. Start with: Content-Security-Policy: default-src 'self'; then refine.

**CAA records** LOW

DNS

No CAA records published. CAA records restrict which Certificate Authorities can issue certificates for your domain, reducing the risk of mis-issuance.

**FIX**

Publish CAA records naming the CAs you use, e.g. "0 issue \"letsencrypt.org\"" and "0 issue \"digicert.com\"".

## Passed checks (13)

**Port scan summary** INFO

PORTS

Checked 12 common ports on 104.21.77.216. Open: 80/HTTP, 443/HTTPS.

**SPF record** PASS

EMAIL

SPF record is present and uses an enforcing policy.



### DMARC policy

EMAIL

DMARC is published with a strict reject policy.

PASS

### DKIM detection

EMAIL

DKIM key detected at selector(s): default, google, selector1, mail, k1, selector2, s2, s1.

PASS

### MX records

EMAIL

MX records present (4). Mail will be routed to mailstream-east.mxrecord.io.

PASS

### Nameserver redundancy

DNS

2 nameservers configured.

PASS

### TLS certificate

TLS

Valid certificate issued by WE1, expires in 89 days. Protocol: TLSv1.3.

PASS

### Header: strict-transport-security

WEB

strict-transport-security is set.

PASS

### Header: x-frame-options

WEB

x-frame-options is set.

PASS

### Header: x-content-type-options

WEB

x-content-type-options is set.

PASS

### Header: referrer-policy

WEB

referrer-policy is set.

PASS

### Header: permissions-policy

WEB

permissions-policy is set.

PASS

### HTTP -> HTTPS redirect

WEB

HTTP requests redirect to HTTPS.

PASS