Security posture report

Domain: cloudfare.com Started: 5/2/2026, 8:12:19 PM Completed: 5/2/2026, 8:12:22 PM

RISK SCORE

82 / 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.

0	1	0	1	7
CRITICAL	HIGH	MEDIUM	LOW	PASS

Issues to address (2)

HTTPS reachability

HIGH

WEB

Could not fetch the site over HTTPS to inspect security headers.

FIX

Ensure the site is served over HTTPS and reachable from the public internet.

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 (8)

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

PASS

EMAIL

DMARC is published with a strict reject policy.

DKIM detection

PASS

EMAIL

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

MX records

PASS

EMAIL

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

Nameserver redundancy

PASS

DNS

2 nameservers configured.

TLS certificate

PASS

TLS

Valid certificate issued by WE1, expires in 33 days. Protocol: TLSv1.3.

HTTP -> HTTPS redirect

PASS

WEB

HTTP requests redirect to HTTPS.