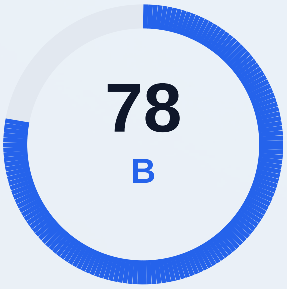
COMPLIANCE LAYER

Security Assessment Report

TARGET DOMAIN	google.com
ASSESSMENT DATE	2026-03-15
OVERALL GRADE	B (78/100)
RISK LEVEL	Medium
SCAN DURATION	4171ms
TOTAL ISSUES	23



OVERALL SCORE

Prepared for: robertcapel3@gmail.com

Scan to verify report

google.com | 2026-03-15

Executive Summary

Assessment Overview for google.com

The infrastructure scan evaluated 15 security modules and identified 23 total issues.
2 critical and 3 high-severity findings require immediate remediation.
The weakest area is Security Headers, scoring 50/100 (Grade D).
Strongest module: Breach Monitor at 100/100 (Grade A).

CRITICAL	HIGH	MEDIUM	LOW	INFO
2	3	5	4	9

Issue Distribution

Priority Recommendations

1. Add 'Secure' flag to all sensitive cookies to prevent transmission over HTTP.
2. Cannot scan private IP ranges, localhost, or cloud metadata endpoints
3. Contact your hosting provider to investigate and request delisting. Consider using a CDN or ...
4. Investigate potential malware or spam issues. Request delisting after resolving the underlyi...
5. Internal services (VPN, Jenkins, GitLab, etc.) should not be publicly reachable. Use private...

Module Scores

MODULE	DESCRIPTION	SCORE	GRADE	WEIGHT	STATUS
Blacklists	IP & domain reputation lists	65	C	3%	Action Needed
Breach Monitor	Known data breaches	100	A	0%	Pass
Cookie Security	Cookie flags & attributes	65	C	8%	Action Needed
DNS & Email Auth	SPF, DKIM, DMARC	85	B	15%	Review
DNSSEC	DNS integrity & signing	80	B	8%	Review
Security Headers	HTTP response headers	50	D	20%	Action Needed
JavaScript	Client-side libraries	100	A	0%	Pass
Port Security	Open port exposure	100	A	10%	Pass
Reputation	Threat intelligence feeds	100	A	2%	Pass
SSL/TLS	Certificate & encryption	90	A	20%	Review
Subdomains	Subdomain discovery	65	C	4%	Action Needed
Technology	Tech stack detection	100	A	0%	Pass
Privacy & Trackers	Third-party tracking	100	A	0%	Pass
WAF Detection	Web application firewall	85	B	7%	Review
WHOIS	Domain registration	100	A	0%	Pass

Module Analysis

Security Headers
HTTP response headers

50 /100 D

- Domain resolves to private/internal IP address

Blacklists
IP & domain reputation lists

65 /100 C

- IP address 192.178.50.78 is listed on 1 blacklist(s): CBL
- Domain is listed on 1 blacklist(s): Spamhaus DBL

Cookie Security
Cookie flags & attributes

65 /100 C

- Sensitive cookies without Secure flag: NID
- Cookies without SameSite attribute: NID, __Secure-BUCKET

Subdomains
Subdomain discovery

65 /100 C

- Development/staging environments publicly accessible: ads-nightly.qa.adz.google.co...
- Internal services publicly accessible: m.guts.corp.google.com, corp.google.com
- Large attack surface: 273 subdomains discovered

DNSSEC
DNS integrity & signing

80 /100 B

- DNSSEC is not enabled
- DNS server does not support EDNS

DNS & Email Auth
SPF, DKIM, DMARC

85 /100 B

- SPF uses ~all (softfail) - consider -all for stricter policy
- No DKIM records found using common selectors - manual verification recommended

WAF Detection
Web application firewall

85 /100 **B**

- ● No WAF detected

SSL/TLS
Certificate & encryption

90 /100 **A**

- ● Certificate expires in 42 days

Breach Monitor
Known data breaches

100 /100 **A**

- ● No known breaches found (limited data - API key not configured)

JavaScript
Client-side libraries

100 /100 **A**

- ● No detectable JavaScript libraries with known patterns

Port Security
Open port exposure

100 /100 **A**

Reputation
Threat intelligence feeds

100 /100 **A**

- ● Reputation check skipped - no API keys configured

Technology
Tech stack detection

100 /100 **A**

- ● No CDN detected

Privacy & Trackers
Third-party tracking

100 /100 **A**

- ● Good privacy score: 100/100 based on 0 known trackers

WHOIS Domain registration

- WHOIS privacy protection is not enabled

100
/100

A

Security Findings

CRITICAL (2)

Domain resolves to private/internal IP address

Recommendation: Cannot scan private IP ranges, localhost, or cloud metadata endpoints

Sensitive cookies without Secure flag: NID

Recommendation: Add 'Secure' flag to all sensitive cookies to prevent transmission over HTTP.

HIGH (3)

Domain is listed on 1 blacklist(s): Spamhaus DBL

Recommendation: Investigate potential malware or spam issues. Request delisting after resolving the underlying pr...

IP address 192.178.50.78 is listed on 1 blacklist(s): CBL

Recommendation: Contact your hosting provider to investigate and request delisting. Consider using a CDN or chang...

Internal services publicly accessible: m.guts.corp.google.com, corp.google.com

Recommendation: Internal services (VPN, Jenkins, GitLab, etc.) should not be publicly reachable. Use private DNS ...

MEDIUM (5)

Certificate expires in 42 days

Recommendation: Plan certificate renewal

Cookies without SameSite attribute: NID, __Secure-BUCKET

Recommendation: Add 'SameSite=Lax' or 'SameSite=Strict' to prevent CSRF attacks.

DNSSEC is not enabled

Recommendation: Enable DNSSEC to protect against DNS spoofing attacks. Contact your DNS provider for setup instru...

Development/staging environments publicly accessible: ads-nightly.qa.adz.google.com, fr...

Recommendation: Dev/staging environments should not be accessible publicly. Use authentication or VPN.

No WAF detected

Recommendation: Consider implementing a Web Application Firewall (WAF) like Cloudflare, AWS WAF, or ModSecurity t...

LOW (4)

DNS server does not support EDNS

Recommendation: Enable EDNS (Extension Mechanisms for DNS) for better performance and DNSSEC support.

Large attack surface: 273 subdomains discovered

Recommendation: Review all subdomains for necessity. Remove or secure unused services.

No DKIM records found using common selectors - manual verification recommended

Recommendation: This scanner checks common DKIM selectors (Google, Microsoft 365, etc.). Many organizations use c...

SPF uses ~all (softfail) - consider -all for stricter policy

Recommendation: Consider changing ~all to -all if all legitimate senders are listed

Compliance-Relevant Technical Controls

SOC 2 Type II

20%
applicable controls

● Pass: 1/5 ● Partial: 4/5 ● Fail: 0/5

PCI DSS 4.0

22%
applicable controls

● Pass: 2/9 ● Partial: 7/9 ● Fail: 0/9

HIPAA Security Rule

20%
applicable controls

● Pass: 1/5 ● Partial: 4/5 ● Fail: 0/5

NIST CSF 1.1

25%
applicable controls

● Pass: 2/8 ● Partial: 6/8 ● Fail: 0/8

ISO 27001:2022

0%
applicable controls

● Pass: 0/6 ● Partial: 6/6 ● Fail: 0/6

CIS Controls v8

0%
applicable controls

● Pass: 0/5 ● Partial: 5/5 ● Fail: 0/5

ComplianceLayer assesses externally observable technical controls. This report does not constitute a compliance certification. Full compliance requires organizational controls, policies, and formal audits.

About This Report

Assessment Methodology

This report was generated by the ComplianceLayer Infrastructure Risk Intelligence platform. The assessment performs non-intrusive external scanning across 15 security modules, each weighted according to its relative importance to overall infrastructure security posture.

Modules include: network port exposure, SSL/TLS configuration, security header analysis, DNS and email authentication (SPF/DKIM/DMARC), DNSSEC validation, cookie security, JavaScript library vulnerability detection, subdomain enumeration, WAF detection, blacklist monitoring, breach monitoring, reputation analysis, and technology fingerprinting.

Compliance mapping covers SOC 2 Type II, PCI DSS 4.0, HIPAA Security Rule, NIST CSF 1.1, ISO 27001:2022, and CIS Controls v8.

Grading Scale

A	90-100	Excellent
B	75-89	Good
C	50-74	Needs Improvement
F	0-49	Critical

Severity Levels

CRITICAL	Immediate action
HIGH	Urgent fix needed
MEDIUM	Should address soon
LOW	Minor improvement
INFO	Informational only

This report is generated from external, non-intrusive scanning and may not reflect all internal security controls.
Results should be validated by qualified security personnel. ComplianceLayer is not a substitute for professional security assessment.