SECURITY ASSESSMENT REPORT

Authorized Security Report

Prepared for the authorized owner of

example-customer.com

OVERALL RISK SCORE

13 /100

GRADE
B

Safe, authorized simulation results

RISK LEVEL	FINDINGS
Low	2
PACKAGE	SCAN DATE
Compliance Report	01 Aug 2026
STATUS	REPORT TYPE
Completed	Client Evidence

Executive Summary

This report summarises the findings from an automated security simulation performed by BreakMesh against **https://example-customer.com**. All checks are passive and safe-simulated — no destructive payloads are used. Overall result: grade **B** with a risk score of **13/100** and **Low** risk.

RISK SCORE	GRADE	RISK LEVEL	TOTAL FINDINGS
13/100	B	Low	2

SEVERITY	FINDINGS	RECOMMENDED ACTION
MEDIUM	1	Remediate within current sprint
LOW	1	Schedule remediation in backlog

Executive Actions

What passed: **8** checks completed without findings. What needs action: **2** checks produced findings for review.

Checks Performed

The **Compliance Report** package ran **10** checks. **8** completed without producing findings.
Effectively tested 10 of 10 checks.

CHECK OUTCOME	COUNT	CHECKS
Passed	8	- Security Contact Evidence - Privacy and Terms Evidence - Cookie Consent Mechanism - WHOIS and Domain Expiry - Mail/DNS Hardening (MTA-STS / TLS-RPT / CAA) - Availability Status Evidence - Blocklist and Reputation Checks - GDPR/CCPA Data Subject Rights
Needs review	2	- DNSSEC Review - Mail Security SPF/DKIM/DMARC

Scope & Confidence

Breakmesh is a continuous safeguard, not a guarantee of safety. This scan identifies and prioritises common, detectable weaknesses so they can be fixed before an attacker finds them — it reduces risk but cannot prove the absence of every vulnerability. No scanner can. Absence of findings means the checks that ran did not surface an issue, not that the target is immune to attack. Use these results as one layer of a defense-in-depth programme alongside secure development, timely patching, monitoring, and periodic human-led penetration testing.

SOC 2 Evidence Mapping

This mapping shows which SOC 2 trust service themes the completed checks can support as audit evidence.

SOC 2 THEME	MAPPED CHECKS	FINDINGS
Security	6	2
Availability	3	1
Confidentiality	1	
Privacy	3	

PCI-DSS v4.0 Control Mapping

This mapping shows which PCI-DSS v4.0 controls the completed checks can support as audit evidence.

CONTROL	MAPPED CHECKS	FINDINGS
1.2.1	8	1
1.3.1	10	
11.3.1	20	
4.2.1	7	
6.2.4	48	
6.3.1	4	
6.4.1	7	
7.2.1	28	
8.3.1	18	

ISO/IEC 27001:2022 Control Mapping

This mapping shows which ISO/IEC 27001:2022 controls the completed checks can support as audit evidence.

CONTROL	MAPPED CHECKS	FINDINGS
A.5.18	10	
A.5.24	3	1
A.5.34	3	
A.8.14	7	
A.8.20	8	1
A.8.24	7	
A.8.26	12	
A.8.28	30	
A.8.3	18	
A.8.5	18	
A.8.8	4	
A.8.9	26	

HIPAA Security Rule Control Mapping

This mapping shows which HIPAA Security Rule controls the completed checks can support as audit evidence.

CONTROL	MAPPED CHECKS	FINDINGS
164.308(a)(1)	4	
164.308(a)(6)	3	1
164.308(a)(7)	7	
164.312(a)(1)	36	1
164.312(c)(1)	36	
164.312(d)	18	
164.312(e)(1)	22	
164.502	3	

Compliance Appendix

Use this appendix to record human review and audit disposition after validating scanner evidence.

FIELD	VALUE
Policy notes	Pending organization-provided narrative
Reviewer	Pending
Review date	Pending
Disposition	Pending

Detailed Findings

DMARC Policy Set to p=none

MEDIUM

The domain publishes a DMARC record, but its policy is p=none, so spoofed mail using this domain is not rejected or quarantined.

AFFECTED URL: example-customer.com

CONFIDENCE: High

COMPLIANCE IMPACT: **SOC 2**: Security
ISO/IEC 27001:2022: A.5.24
HIPAA Security Rule: 164.308(a)(6)

REMEDIATION: Move the DMARC policy to p=quarantine, then p=reject, once SPF/DKIM alignment is confirmed for all legitimate senders.

EVIDENCE:

```
observed: The domain publishes a DMARC record, but its policy is p=none, so spoofed mail using this domain is not rejected or quarantined.
```

DNSSEC Not Enabled

LOW

The domain does not have DNSSEC enabled, leaving DNS responses unsigned.

AFFECTED URL: example-customer.com

CONFIDENCE: High

COMPLIANCE IMPACT: **SOC 2**: Availability, Security
PCI-DSS v4.0: 1.2.1
ISO/IEC 27001:2022: A.8.20
HIPAA Security Rule: 164.312(a)(1)

REMEDIATION: Enable DNSSEC at the domain registrar and DNS provider to protect against DNS spoofing/cache poisoning.

EVIDENCE:

```
observed: The domain does not have DNSSEC enabled, leaving DNS responses unsigned.
```

Scan ID: ac8481da-256b-5baa-b813-b93ccff478af · This report is confidential and intended solely for the authorised owner of example-customer.com. Breakmesh performs passive simulation only. All findings should be validated by a qualified security professional prior to remediation.