SECURITY ASSESSMENT REPORT

Authorized Security Report

Prepared for the authorized owner of

example-customer.com

OVERALL RISK SCORE

35 /100

GRADE
C

Safe, authorized simulation results

RISK LEVEL	FINDINGS
Medium	2
PACKAGE	SCAN DATE
Cloud Posture	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 **C** with a risk score of **35/100** and **Medium** risk.

RISK SCORE	GRADE	RISK LEVEL	TOTAL FINDINGS
35/100	**C**	**Medium**	**2**

SEVERITY	FINDINGS	RECOMMENDED ACTION
HIGH	1	Remediate within days
MEDIUM	1	Remediate within current sprint

Executive Actions

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

Checks Performed

The **Cloud Posture** package ran **10** checks. **8** completed without producing findings.
Effectively tested 10 of 10 checks.

CHECK OUTCOME	COUNT	CHECKS
Passed	8	- AWS Open Security Group Ingress - AWS IAM Stale Access Keys - AWS CloudTrail Logging Disabled - AWS Default Encryption Gaps - Azure Public Blob Storage Exposure - Azure Open NSG Ingress Rules - GCP Public Cloud Storage Exposure - GCP Open VPC Firewall Ingress
Needs review	2	- AWS Public S3 Storage Exposure - AWS Overly-Permissive IAM Policies

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	10	2
Availability	3	
Confidentiality	6	2
Privacy	3	1
Processing Integrity	1	

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	
1.3.1	10	2
11.3.1	20	
4.2.1	7	
6.2.4	48	
6.3.1	4	
6.4.1	7	
7.2.1	28	2
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	2
A.5.24	3	
A.5.34	3	
A.8.14	7	
A.8.20	8	
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	2

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	
164.308(a)(7)	7	
164.312(a)(1)	36	2
164.312(c)(1)	36	
164.312(d)	18	
164.312(e)(1)	22	
164.502	3	

Detailed Findings

Public S3 Bucket

HIGH

An S3 bucket is configured with public read access and contains files that appear to be internal build artifacts.

AFFECTED URL	s3://example-customer-assets
CONFIDENCE	High
COMPLIANCE IMPACT	**SOC 2**: Confidentiality, Privacy, Security **PCI-DSS v4.0**: 1.3.1, 7.2.1 **ISO/IEC 27001:2022**: A.5.18, A.8.9 **HIPAA Security Rule**: 164.312(a)(1)
REMEDIATION	Remove public access from the bucket, enable Block Public Access at the account level, and audit what was exposed.
EVIDENCE	`observed: An S3 bucket is configured with public read access and contains files that appear to be internal build artifacts.`
REFERENCES	- CIS AWS Foundations Benchmark 2.1.5

Overly-Permissive IAM Policy

MEDIUM

An IAM policy attached to a CI/CD role grants s3:* on all resources rather than the specific buckets it needs.

AFFECTED URL	arn:aws:iam::example:policy/legacy-deploy-policy
CONFIDENCE	High
COMPLIANCE IMPACT	**SOC 2**: Confidentiality, Security **PCI-DSS v4.0**: 1.3.1, 7.2.1 **ISO/IEC 27001:2022**: A.5.18, A.8.9 **HIPAA Security Rule**: 164.312(a)(1)
REMEDIATION	Scope the policy down to the specific bucket ARNs and required actions (least privilege).
EVIDENCE	`observed: An IAM policy attached to a CI/CD role grants s3:* on all resources rather than the specific buckets it needs.`