CloudWizard
Security Posture Report

Prepared for: **Valued Customer** | Date: **March 3, 2026**

CloudWizard Security Posture Report

Prepared for: **Valued Customer** | Date: **March 3, 2026**

Executive Summary

This complimentary security assessment was conducted by CloudWizard on your AWS infrastructure. Our automated scanning platform evaluated **2663** security controls across your cloud environment.

While your overall security posture shows an **47%** pass rate, we identified **1416** failing checks that require attention, including **14** critical-severity and **37** high-severity findings.

> ⚠ **Action Required**
>
> We recommend addressing the critical and high-severity findings within the next 7 days to minimize security exposure. CloudWizard can help you remediate these issues quickly with our managed security service.

CRITICAL RISKS	HIGH RISKS	CHECKS PASSED
14	37	47%

What's Included

- **Security posture overview:** High-level metrics and pass/fail breakdown

- **Top critical risks:** Prioritized list of the most urgent findings

- **Service-level analysis:** Issues grouped by AWS service (S3, IAM, EC2, etc.)

- **Compliance mapping:** How findings relate to CIS, PCI-DSS, and GDPR frameworks

- **Remediation guidance:** Basic steps to address common vulnerabilities

Top Security Risks

Priority findings requiring immediate attention

Critical & High Severity Findings

Below are the top security risks identified in your AWS environment. These represent the highest-priority items that could expose your organization to data breaches, unauthorized access, or compliance violations.

SEVERITY	CHECK / ISSUE	SERVICE	RESOURCE	STATUS
CRITICAL	**[DEPRECATED] Find secrets in EC2 Auto Scaling Launch Configuration** autoscaling_find_secrets_ec2_launch_configuration	autoscaling	`arn:aws:autoscaling:us-west-2:871349070445:launchConfiguration:845e824a-78d2-455c-b965-990932071e6a:launchConfigurationName/awseb-e-zaqtkmx4qe-stack-AWSEBAutoScalingLaunchConfiguration-6WDRB5GVZIG3`	FAIL
CRITICAL	**Find secrets in Lambda functions variables.** awslambda_function_no_secrets_in_variables	awslambda	`arn:aws:lambda:ap-southeast-2:871349070445:function:ebay-saas-listings-create`	FAIL
CRITICAL	**Ensure only hardware MFA is enabled for the root account** iam_root_hardware_mfa_enabled	iam	`arn:aws:iam:us-east-1:871349070445:mfa`	FAIL
CRITICAL	**Check if S3 buckets have policies which allow WRITE access.** s3_bucket_policy_public_write_access	s3	`arn:aws:s3:::ebay-saas-user-images-australia`	FAIL
CRITICAL	**Ensure there are no S3 buckets open to Everyone or Any AWS user.** s3_bucket_public_access	s3	`arn:aws:s3:::000-acloudwizard`	FAIL
CRITICAL	**Ensure there are no S3 buckets open to Everyone or Any AWS user.** s3_bucket_public_access	s3	`arn:aws:s3:::222-for-chatgpt-vids`	FAIL
CRITICAL	**Ensure there are no S3 buckets open to Everyone or Any AWS user.** s3_bucket_public_access	s3	`arn:aws:s3:::222-grist-4-da-mill`	FAIL
CRITICAL	**Ensure there are no S3 buckets open to Everyone or Any AWS user.** s3_bucket_public_access	s3	`arn:aws:s3:::222-gto-charts-clones`	FAIL
CRITICAL	**Ensure there are no S3 buckets open to Everyone or Any AWS user.** s3_bucket_public_access	s3	`arn:aws:s3:::cv-sheehy`	FAIL
CRITICAL	**Ensure there are no S3 buckets open to Everyone or Any AWS user.** s3_bucket_public_access	s3	`arn:aws:s3:::ebay-saas-user-images-australia`	FAIL
CRITICAL	**Ensure there are no S3 buckets open to Everyone or Any AWS user.** s3_bucket_public_access	s3	`arn:aws:s3:::0000-gto-charts`	FAIL
CRITICAL	**Ensure there are no S3 buckets open to Everyone or Any AWS user.**	s3	`arn:aws:s3:::aa-gtocharts-media-bucket`	FAIL

SEVERITY	CHECK / ISSUE	SERVICE	RESOURCE	STATUS
	s3_bucket_public_access			
CRITICAL	**Ensure there are no S3 buckets open to Everyoneor Any AWS user.** s3_bucket_public_access	s3	`arn:aws:s3:::elasticbeanst` `alk-us-east-1-871349070445`	FAIL
CRITICAL	**Ensure there are no S3 buckets open to Everyoneor Any AWS user.** s3_bucket_public_access	s3	`arn:aws:s3:::husng-protect` `ed-content`	FAIL

HIGH	**Check if EC2 Instance Metadata Service Version 2 (IMDSv2) is Enabled and Required.**
	ec2_instance_imdsv2_enabled
		ec2	`arn:aws:ec2:us-east-1:8713`
			`49070445:instance/i-dcdd5a`
			`74`
				FAIL

What do you want to do next?

Fix it yourself

Use this report to guide your team's remediation.

Use our dashboard + help

Dashboard access with support for top issues.

Work with a fractional CISO

Continuous review and SOC 2 compliance guidance.

Talk to us about your options

This is a sample CloudWizard Security Posture Report, provided for illustration only. To receive your own free, tailored AWS security audit and report, visit https://acloudwizard.com and request a Free AWS Security Audit.