Qualys CloudView v2.x

Version 2.0.0
February 07, 2023

What's new!

Common Feature

Enhancements to Reports

Amazon Web Services

Migrated controls from AWS Best Practice to CIS Amazon Web Services Foundations Benchmark

Migrated controls from AWS Database Service Best Practices to CIS Amazon Web Services Foundations Benchmark

Qualys CloudView 2.0.0 brings you improvements and updates! Learn More

Common Feature

Enhancements to Reports

We have updated the outputs for PDF and CSV reports generated by CloudView. These enhancement will improve the accuracy of the compliance score and enable you to focus on the actual controls being evaluated.

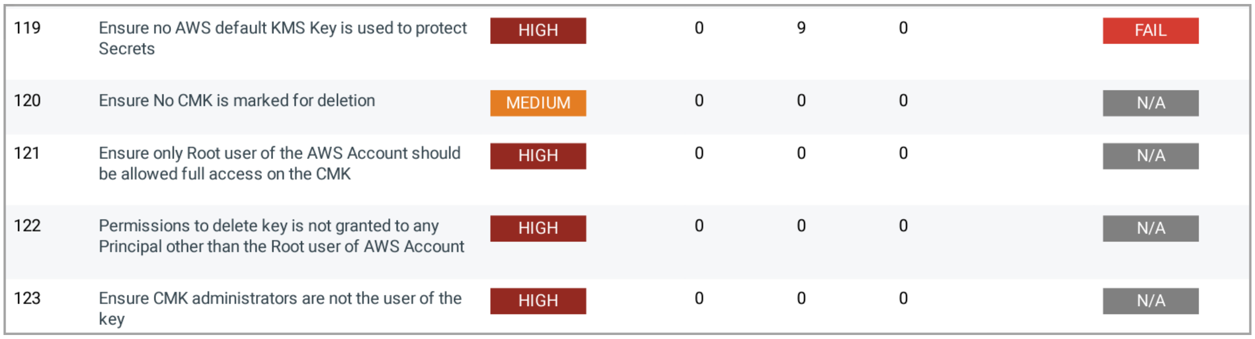
CSV Report

We are introducing additional fields to the downloadable CSV reports from CloudView. CSV reports for AWS, Azure and GCP also display Account Summary, Control Summary, and Resource Summary.

- Account Summary shows Evaluated Controls, Pass/Fail count of controls, and the compliance score.
- Control Summary shows Control Results, Passed/Failed Resources, and Exempted Resources.
- Resource Summary shows Resource ID, Connector, Control ID, Resource Type, and Resource Result.

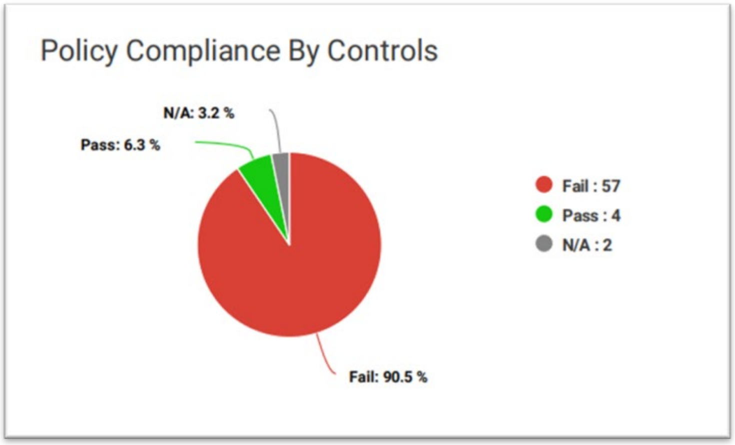
PDF Report

We are introducing changes to the PDF reports generated from CloudView. CloudView reports used to display controls with no evaluations with "Pass" results. Unevaluated controls are now marked as "N/A" to show that they are unmonitored.



119	Ensure no AWS default KMS Key is used to protect Secrets	HIGH	0	9	0	FAIL
120	Ensure No CMK is marked for deletion	MEDIUM	0	0	0	N/A
121	Ensure only Root user of the AWS Account should be allowed full access on the CMK	HIGH	0	0	0	N/A
122	Permissions to delete key is not granted to any Principal other than the Root user of AWS Account	HIGH	0	0	0	N/A
123	Ensure CMK administrators are not the user of the key	HIGH	0	0	0	N/A

Users can view the Not Evaluated Controls count under Policy Compliance by Controls Pie chart.



Amazon Web Services

Migrated controls from AWS Best Practice to CIS Amazon Web Services Foundations Benchmark

CID	Title
57	Ensure S3 Bucket Policy is set to deny HTTP requests
67	Ensure all S3 buckets employ encryption-at-rest
115	Ensure that EBS Volumes attached to EC2 instances are encrypted
116	Ensure that Unattached EBS Volumes are encrypted
144	Ensure EFS Encryption is enabled for data at rest
433	Ensure EC2 Instances are using IAM Roles

Migrated controls from AWS Database Service Best Practices to CIS Amazon Web Services Foundations Benchmark

CID	Title
55	Ensure auto minor version upgrade is enabled for a RDS Database Instance
78	Ensure that public access is not given to RDS Instance

Issues Fixed

- We have changed the detection logic of CID 313 to allow validation of an unlimited retention period.
- We have enhanced the detection logic of CID 186 to cover signature checks for HTTPS protocols as well.