Qualys CloudView v1.x

Version 1.17.0

July 19, 2021

Here's what's new in Qualys CloudView 1.17.0!

Amazon Web Services

New controls for AWS Best Practices Policy
New controls for AWS Database Service Best Practices

Google Cloud Platform

New controls for CIS Google Cloud Platform Foundation Benchmark
Migrated Controls

Common Feature

Support for Exceptions at Connector Level
Control Metadata Information
Unified Dashboard (UD) Support for CloudView

API Features and Enhancements

Qualys CloudView 1.17 brings you many more Improvements and updates! Learn more

Amazon Web Services

New controls for AWS Best Practices Policy

We have introduced the following 19 new controls for AWS Best Practices Policy.

CID	Service	Resource	Title
203	EC2	EBS	Ensure EBS volumes are encrypted with customer managed master keys
204	EC2	EBS	Ensure AWS EBS Volume snapshots are encrypted with customer managed master keys
205	Workspace	Directory	Ensure "RestartWorkspace" is Enabled in all the regions
208	Workspaces	Directory	Ensure WorkDocs is not enabled in Workspace Directories
209	Workspaces	Directory	Ensure Access to Internet Access is not enabled in Workspace Directories
210	Workspaces	Directory	Ensure Local Administrator setting is not enabled in Workspace Directories
211	Workspaces	Directory	Ensure Maintenance Mode is not enabled in Workspace Directories
212	Workspaces	Directory	Ensure Device Type Windows Access Control is not enabled in Workspace Directories
213	Workspaces	Directory	Ensure Device Type MacOS Access Control is not enabled in Workspace Directories
214	Workspaces	Directory	Ensure Device Type Web Access Control is not enabled in Workspace Directories
215	Workspaces	Directory	Ensure Device Type iOS Access Control is not enabled in Workspace Directories
216	Workspaces	Directory	Ensure Device Type Android Access Control is not enabled in Workspace Directories
217	Workspaces	Directory	Ensure Device Type ChromeOS Access Control is not enabled in Workspace Directories
218	Workspaces	Directory	Ensure Device Type ZeroClient Access Control is not enabled in Workspace Directories
184	LoadBalancer	LoadBalancer	Ensure there are no Internet facing Application load balancers

CID	Service	Resource	Title
185	LoadBalancer	LoadBalancer	Ensure ALB using listener type HTTPS must have SSL Security Policy
186	LoadBalancer	LoadBalancer	Ensure that ALB using listener type HTTP must be redirected to HTTPS
187	LoadBalancer	LoadBalancer	Ensure that ALB listeners have HTTPS enabled Target Groups
188	Workspace	Directory	Ensure IncreaseVolumeSize is Disabled for Workspace directories in all regions

New controls for AWS Database Service Best Practices

We have introduced the following 5 new controls for AWS Database Service Best Practices

CID	Service	Resource	Title
189	AmazonRedshift	Redshift	Ensure Automated backup retention is set for Redshift Cluster
206	Document DB	Document DB	Ensure Document DB Cluster snapshots are encrypted
207	Document DB	Document DB	Ensure Document database Cluster snapshots are not public
219	Neptune DB	Neptune DB	Ensure Neptune DB Cluster snapshots are encrypted
220	Neptune DB	Neptune DB	Ensure Neptune database Cluster snapshots are not public

Google Cloud Platform

New controls for CIS Google Cloud Platform Foundation Benchmark

We have introduced the following controls for CIS Google Cloud Platform Foundation Benchmark.

CID	Service	Resource	Title
52111	Compute Engine	VM Instances	Ensure that Compute instances have Confidential Computing enabled
52112	SQL	PostgreSQL	Ensure log_parser_stats database flag for Cloud SQL PostgreSQL instance is set to off
52113	SQL	PostgreSQL	Ensure log_planner_stats database flag for Cloud SQL PostgreSQL instance is set to off
52114	SQL	PostgreSQL	Ensure log_executor_stats database flag for Cloud SQL PostgreSQL instance is set to off
52115	SQL	PostgreSQL	Ensure 'log_statement_stats' database flag for Cloud SQL PostgreSQL instance is set to off

Migrated Controls

We have migrated the following controls from GCP Cloud SQL Best Practices Policy to CIS Google Cloud Platform Foundation Benchmark.

CID	Title	Service	Resource
52035	Ensure that MySQL Database Instance does not allows root login from any Host	SQL	SQL
52061	Ensure "log_duration" database flag for Cloud SQL - PostgreSQL instance is set to on	SQL	PostgreSQL
52062	Ensure "log_error_verbosity" database flag for Cloud SQL - PostgreSQL instance is set to "DEFAULT" or stricter	SQL	PostgreSQL
52063	Ensure "log_statement" database flag for Cloud SQL - PostgreSQL instance is set to "ddl" or stricter	SQL	PostgreSQL
52064	Ensure "log_hostname" database flag for Cloud SQL - PostgreSQL instance is set to "off"	SQL	PostgreSQL
52071	Ensure "log_min_error_statement" database flag for Cloud SQL - PostgreSQL instance is set to "Error" or stricter	SQL	PostgreSQL
52075	Ensure "skip_show_database" database flag for Cloud SQL - Mysql instance is set to "on"	SQL	MySQL
52077	Ensure "external scripts enabled" database flag for Cloud SQL - SQL Server instance is set to "off"	SQL	SQL Server
52080	Ensure "user options" database flag for Cloud SQL - SQL Server instance is not configured	SQL	SQL Server
52081	Ensure "remote access" database flag for Cloud SQL - SQL Server instance is set to "off"	SQL	SQL Server
52082	Ensure "3625 (trace flag)" database flag for Cloud SQL - SQL Server instance is set to "off"	SQL	SQL Server

We have migrated the following controls from GCP Best Practices Policy to CIS Google Cloud Platform Foundation Benchmark.

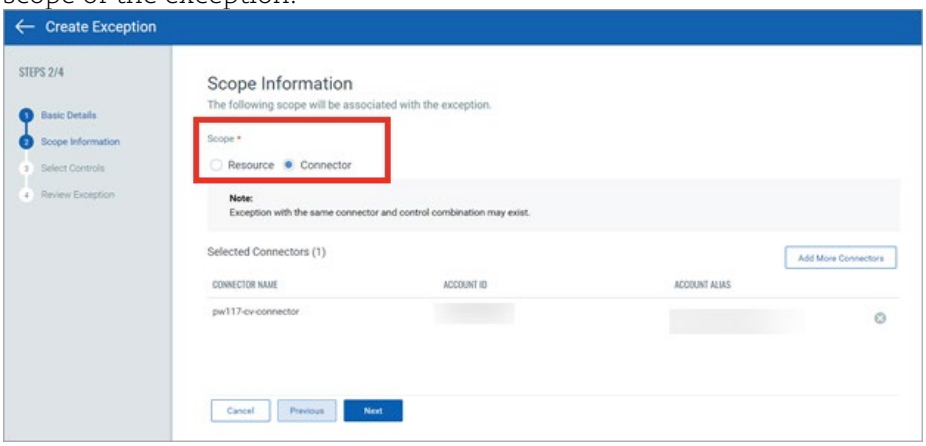
CID	Title	Service	Resource
52095	Ensure that BigQuery Dateset is encrypted with Customer-managed key	BigQuery	Dataset
52096	Ensure that BigQuery Table is encrypted with Customer-managed key	BigQuery	Table
52109	Ensure that GCP Cloud DNS zones is not using RSASHA1 algorithm for DNSSEC key-signing	Network Services	Cloud DNS
52110	Ensure that GCP Cloud DNS zones is not using RSASHA1 algorithm for DNSSEC zone-signing	Network Services	Cloud DNS

Common Feature

Support for Exceptions at Connector Level

We have now updated our exception creation flow to allow you to create exceptions at a connector level. It implies that if you create an exception at a connector level, all the resources discovered/associated with the connector are exempted from control evaluation. You have the choice to exclude resources from single or multiple controls. You can now define the scope of an exception: create exceptions for a particular resource or all resources in an account.

From the Monitor tab, when you trigger the Exception creation wizard, you can now define the scope of the exception.



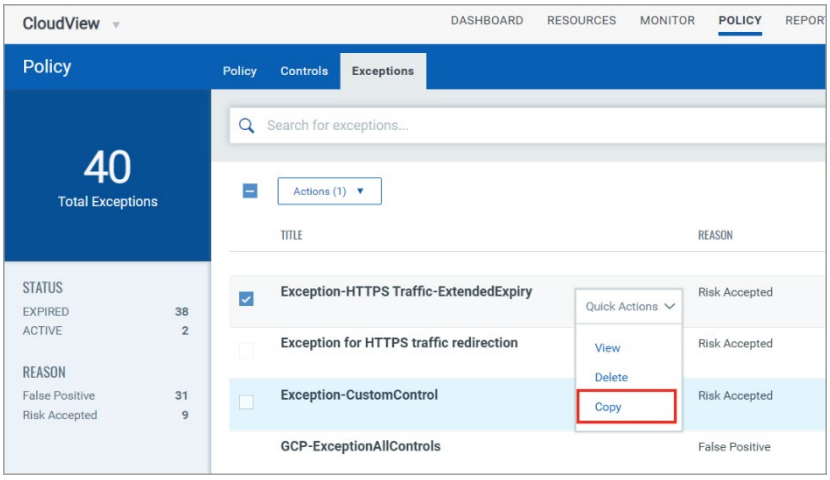
Scope Information: Decides the scope of the exception you are creating. You could expand the scope of the exception to all resources in a specific account.

- **Resource**: Choose to create exception at resource level and the exception is applicable only for the selected resource. By default, the Resource option is selected.
- **Connector**: Choose to create exception for all resources in the account associated with the connector. By default, the connector associated with the resource is selected. You could click **Add More Connectors** to add multiple connectors for the exception.

Note: The exception created at connector level is implemented on the resource evaluation result in the next connector run.

You can now also create an exception from an existing exception, using **Copy** quick action menu option that we newly added.

Go to **Policy** > **Exceptions** to see exceptions. Select an existing exception from the list and click Copy from the quick actions menu. The exception creation wizard is displayed with settings pre-configured from the existing exception. You can alter the required settings and create a new exception using the pre-populated configuration.



Control Metadata Information

You can now fetch the control metadata such as control type, cloud provider, control criticality, details about the control evaluation (including specification, evaluation description, and so on). You can use our newly introduced API to fetch this information. We also support filters such as cid, control.type, and few more that help you narrow down the controls for which you want to fetch the metadata. To know the complete details about this new API, refer to CloudView 1.17 API Release Notes.

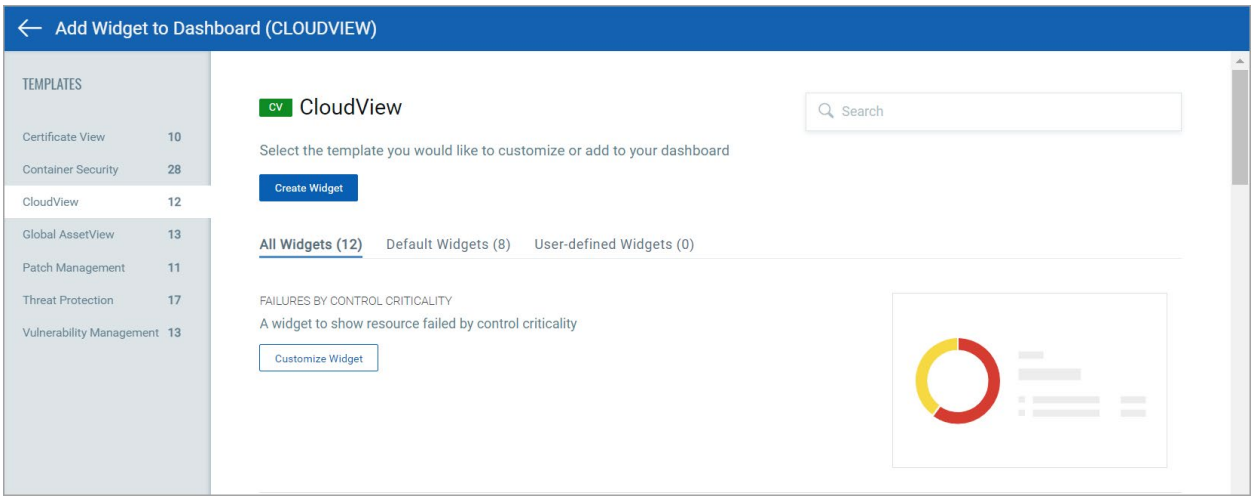
Unified Dashboard (UD) Support for CloudView

Dashboards help you visualize your cloud resources, evaluation of your cloud resources, see your threat exposure, leverage saved searches, and fix resource misconfigurations quickly.

We have integrated Unified Dashboard (UD) with CloudView. UD brings information from all Qualys applications into a single place for visualization. UD provides a powerful new dashboarding framework along with platform service that will be consumed and used by all other products to enhance the existing dashboard capabilities.

You can use the default dashboard provided by Qualys or easily configure widgets to pull information from other modules/applications and add them to your dashboard. You can also add as many dashboards as you like to customize your vulnerability posture view.

Click the **Add Widget** icon on the Dashboard page to go to **Add Widget to Dashboard (CloudView)** screen.



API Features and Enhancements

We have introduced a new API to fetch control metadata information. For detailed information, refer to CloudView 1.17 API Release Notes.

Issue addressed in this release

- Updated control logic for CID 19: CID 19 will now also evaluate for the account which does not have any CloudTrail configured within it.