



Qualys Cloud Platform v3.x

Release Notes

Version 3.1

July 1, 2020

Here's what's new in Qualys Cloud Suite 3.1!

AV

AssetView

[External ID Read-Only for EC2 Connectors](#)

VMDR

Vulnerability Management Detection and Response

[What's new in VMDR?](#)

- [Enhanced Asset Tag Selection](#)
- [New Age Criteria: Detection Age and Vulnerability Age](#)
- [Enriched RTI Filters](#)
- [Internet Facing Assets Attack Surface](#)
- [Advanced Search](#)
- [Grouping Report Data](#)
- [Save and Download Reports](#)

[Vulnerability Status in CSV File](#)

UD

Unified Dashboard

[Introducing Unified Dashboard](#)

CM

Continuous Monitoring

[New Threat Protection RTIs – Wormable and Predicted High Risk](#)

SAQ

Security Assessment Questionnaire

[Vendor On-boarding](#)

WAS**Web Application Scanning**

[Delete Catalog Entries](#)

[Web application XML Report to Show More Information for BURP Findings](#)

[Malware Detection module name changed to Web Malware Detection](#)

**Administration**

[Tagging Permissions](#)

**Qualys Cloud Platform 3.1 brings you many more
Improvements and updates! [Learn more](#)**



External ID Read-Only for EC2 Connectors

AWS recommends the External ID should be read-only field as one of its best practices. We have now standardized the EC2 connector creation process adhering to the best practices.

Qualys generates a unique External ID, and auto-populates it during EC2 connector creation. It is now a read-only field and you cannot edit the External ID field, thereby enhancing the security of your AWS account.



What's new in VMDR?

We have enriched our all-in-one Vulnerability Management, Detection, and Response (VMDR) Solution with the following enhancements:


- [Enhanced Asset Tag Selection](#)
- [New Age Criteria: Detection Age and Vulnerability Age](#)
- [Enriched RTIs Filters](#)
- [Internet Facing Assets Attack Surface](#)
- [Advanced Search](#)
- [Grouping Report Data](#)
- [Save and Download Reports](#)

Let us see each enhancement in detail.

Asset Tag Selection

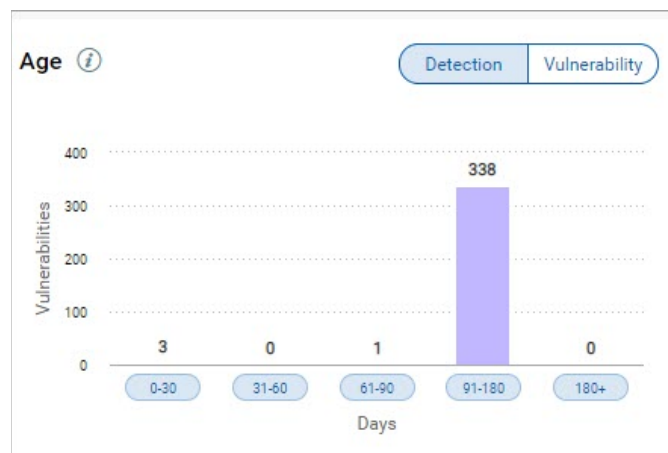
The first step towards VMDR prioritization report is choosing the asset tags. You can confine the list of vulnerabilities associated with the assets you select.

The screenshot displays the 'VMDR Prioritization' interface. At the top, a blue banner reads 'VMDR Prioritization' and 'Prioritize your riskiest vulnerabilities on the most critical assets, reducing thousands of vulnerabilities to the few hundred that matter'. Below this, the 'Select Asset Tags' section is shown, with the instruction 'Start prioritization by selecting asset tags'. A horizontal bar contains four selected tags: 'Business Units', 'Cloud Agent', 'AWS', and 'Asset Groups', each with a close button (x). A blue button with a right arrow is at the end of the bar. Below the bar, the text 'What's next in the prioritization process?' is followed by a circular arrow icon.

You need to select at least one asset tag before you proceed towards the report creation. Select the Asset Tags to narrow down the assets and then click  to proceed ahead.

New Age Criteria: Detection Age and Vulnerability Age

We have now added a new filter for age of vulnerabilities. You could switch between the two filters: Detection Age and Vulnerability Age.



Detection Age indicates age from the day when the vulnerability was first detected.

By default, the Detection Age filter is applied. To opt for Vulnerability Age filter, click Vulnerability tab and make the required selections of age categories.

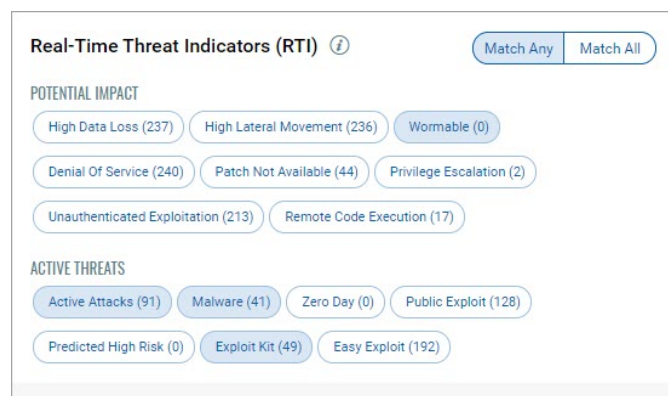
Vulnerability Age indicates age from the day when the vulnerability was first disclosed.

By default, all the age range are applicable. If you want to focus on vulnerabilities of specific age range, de-select the other

categories and ensure that you select only the required age range.

RTI Enhancements

We have enhanced the Real-Time Threat Indicators (RTIs) filter with following developments:



Toggle

We introduced a toggle button for **Match Any** (logical OR) and **Match All** (logical AND). Choose if you want any one of the selected vulnerabilities or ALL of the selected vulnerabilities to exist on the assets to be prioritized.

Categorization:

We have also categorized RTIs into two broad level types: **Potential Impact** and **Active Threats**.

New RTIs

We have introduced the following 3 new RTIs:

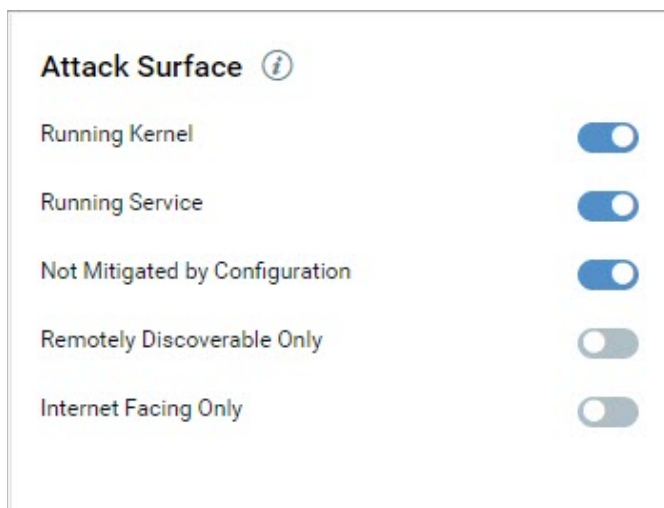
Privilege Escalation - Successful exploitation allows an attacker to gain elevated privileges.

Unauthenticated Exploitation - Exploitation of this vulnerability does not require authentication.

Remote Code Execution - Successful exploitation allows an attacker to execute arbitrary commands or code on a targeted system or in a target process.

Internet Facing Only Attack Surface

We have introduced a new attack surface named **Internet Facing Only**.



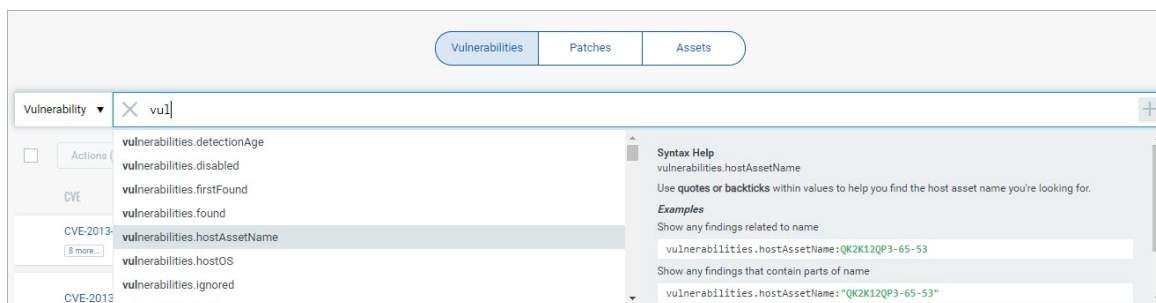
Toggle this filter On to include assets with IP addresses that could be exploitable. By default, this filter is disabled.

The attack surface primarily uses system-defined tag, named Internet Facing Assets (IFA). The tag includes pre-defined ranges of publicly routable IP addresses. This tag automatically tags assets with IPs that fall within the specified ranges.

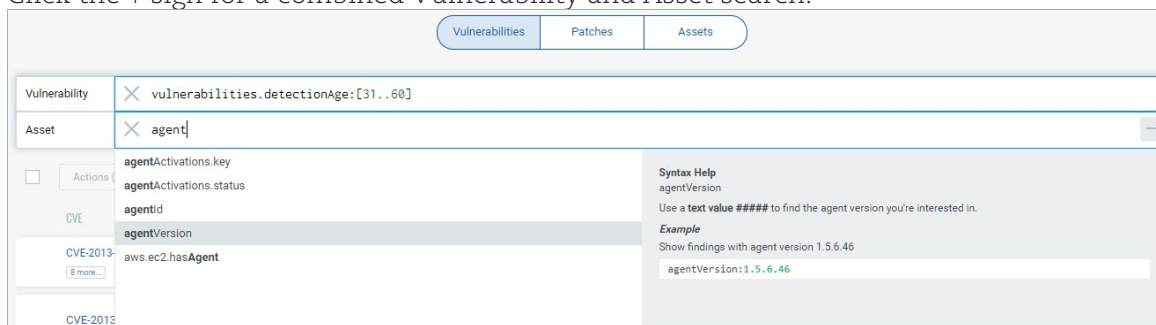
Advanced Search

We have now empowered our search with multiple criteria in a single go.

Start typing in the Search field and we'll show you the properties you can search such as vulnerability severity, detection age, etc. Select the one you're interested in.



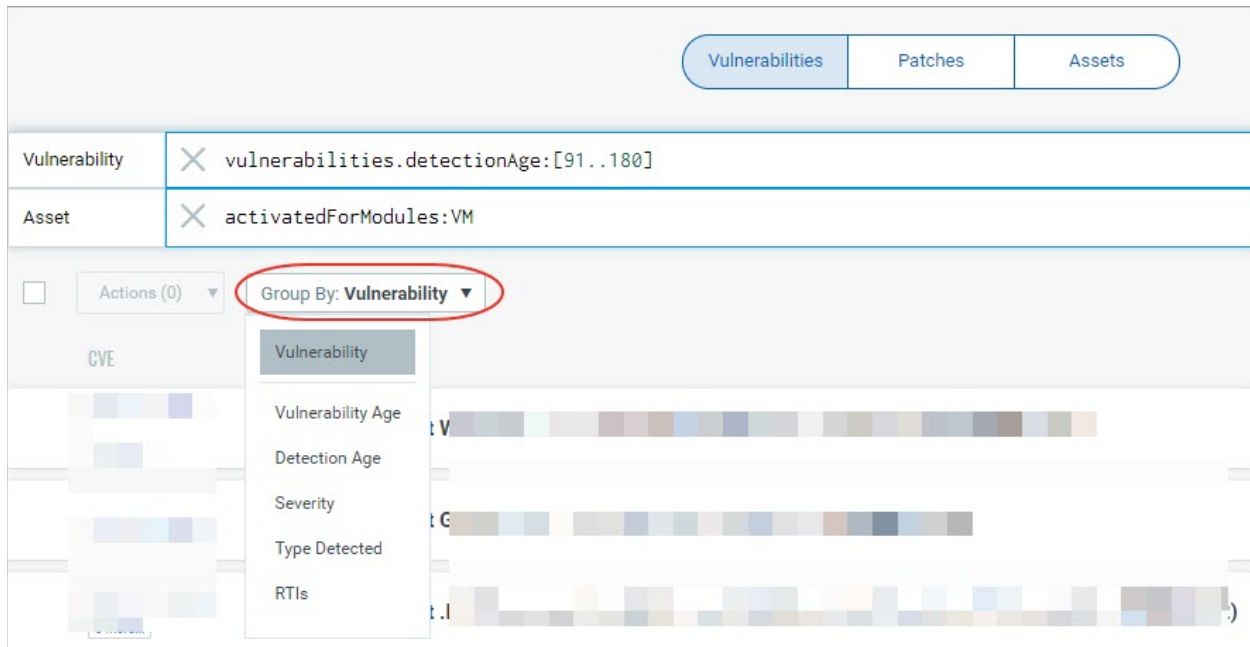
Click the + sign for a combined Vulnerability and Asset search.



Start typing and we'll show you the asset properties you can search like agentId, agent version, etc. Select the one you're interested in. Now, enter the value you want to match, and press Enter. That's it! Your matches will appear in respective tab.

Grouping Report Data

Once you have generated your online VMDR prioritization report, you may want to organize the data further into logical groupings. We offer several group by options such as detection age, vulnerability age, severity and more.



You'll see the number of unique groupings based on your selection and the number of vulnerabilities per group. Click on any grouping to update the search query and view the matching vulnerabilities.

Save and Download Reports

You can save or save and download the VMDR prioritization report to your local system in a single click.

Save and Download Report

You can save this report to the Reports tab or download the report to analyze or share it offline.

Name *

Description

225/250 characters remaining

Include

☒ Vulnerabilities - ☒ Grouped (Unique) ☐ All Instances

☒ Patches

☒ Assets

Report Format *

Comma-Separated Value (CSV)

▼

Select Timezone *

(GMT 05:30) India Standard Time (IST Asia/Colombo)

▼

Cancel

Save

Save & Download

On the VMDR Prioritization report, click **Save & Download**.

Note: Only after you generate the VMDR prioritization report, the **Save & Download** button is enabled.

On clicking **Save**, the VMDR prioritization report is saved to the reports list on **Reports** tab. On clicking **Save & Download**, the VMDR Prioritization report is saved to the report list and downloaded to your local system.

Vulnerability Status in CSV File

We have now introduced the status of vulnerabilities in the file you download from Vulnerabilities tab. When you download vulnerabilities in CSV format, we now include the status column, which indicates if the vulnerability is New or Active.

Go to Vulnerabilities tab and the vulnerabilities are displayed. You could type a search query to narrow down the list of vulnerabilities.

The screenshot shows the VMDR Vulnerabilities interface. On the left, there's a sidebar with '353 Total Detections' and a severity distribution chart. The main area displays a table of vulnerabilities. A download icon (a square with a downward arrow) is circled in red in the top right corner of the table area. The table has columns for QID, TITLE, SEVERITY, LAST DETECTED, FIRST DETECTED, and ASSET. The first few rows show vulnerabilities like 'Microsoft Windows Explorer AutoPlay Not Disabled' and 'Microsoft Windows Adobe Flash Player Security Update f...'. The status 'Active' is visible under the TITLE column for some entries.

Click  to download the data list in CSV format. The CSV file now includes Status column.

Asset Vuln	01 Jul 2020	353										
Qualys	Pune		Maharash	411021	India							
David Fro	user_davif											
QID	TITLE	SEVERITY	TYPE DETE	LAST DETECTE	FIRST DETECTED	PROTOCO	PORT	ASSET ID	ASSET NA	STATUS		
105170	Microsoft	2	Confirmed	1-Jul-20	30-Mar-20	'-	'-	4341336	VMDR1	ACTIVE		
372481	Mozilla Fi	4	Confirmed	1-Jul-20	10-Apr-20	'-	'-	4341336	VMDR1	ACTIVE		
372825	Mozilla Fi	4	Confirmed	1-Jul-20	17-Jun-20	'-	'-	4341336	VMDR1	ACTIVE		
372445	Mozilla Fi	4	Confirmed	1-Jul-20	30-Mar-20	'-	'-	4341336	VMDR1	ACTIVE		
372392	Mozilla Fi	5	Confirmed	1-Jul-20	30-Mar-20	'-	'-	4341336	VMDR1	ACTIVE		
100406	Microsoft	4	Potential	1-Jul-20	27-Jun-20	'-	'-	4341336	VMDR1	ACTIVE		
91634	Microsoft	4	Confirmed	1-Jul-20	27-Jun-20	'-	'-	4341336	VMDR1	ACTIVE		
372490	Mozilla Fi	4	Confirmed	1-Jul-20	10-Jun-20	'-	'-	4341336	VMDR1	ACTIVE		
91598	Microsoft	5	Confirmed	1-Jul-20	30-Mar-20	'-	'-	4341336	VMDR1	ACTIVE		
90213	Windows	1	Potential	1-Jul-20	30-Mar-20	'-	'-	4341336	VMDR1	ACTIVE		
90044	Allowed M	2	Confirmed	1-Jul-20	30-Mar-20	'-	'-	4341336	VMDR1	ACTIVE		
90007	Enabled C	2	Confirmed	1-Jul-20	30-Mar-20	'-	'-	4341336	VMDR1	ACTIVE		
105228	Built-in G	3	Confirmed	1-Jul-20	30-Mar-20	'-	'-	4341336	VMDR1	ACTIVE		
105171	Windows	2	Confirmed	1-Jul-20	30-Mar-20	'-	'-	4341336	VMDR1	ACTIVE		
105228	Built-in G	3	Confirmed	24-Mar-20	2-Mar-20	'-	'-	3894259	WIN10-11	ACTIVE		
100369	Microsoft	3	Confirmed	24-Mar-20	2-Mar-20	'-	'-	3894259	WIN10-11	ACTIVE		
90213	Windows	1	Potential	24-Mar-20	2-Mar-20	'-	'-	3894259	WIN10-11	ACTIVE		
90044	Allowed M	2	Confirmed	24-Mar-20	2-Mar-20	'-	'-	3894259	WIN10-11	ACTIVE		
90007	Enabled C	2	Confirmed	24-Mar-20	2-Mar-20	'-	'-	3894259	WIN10-11	ACTIVE		

Introducing Unified Dashboard

We have introduced a new app named Unified Dashboard (UD) to enrich your dashboarding experience.

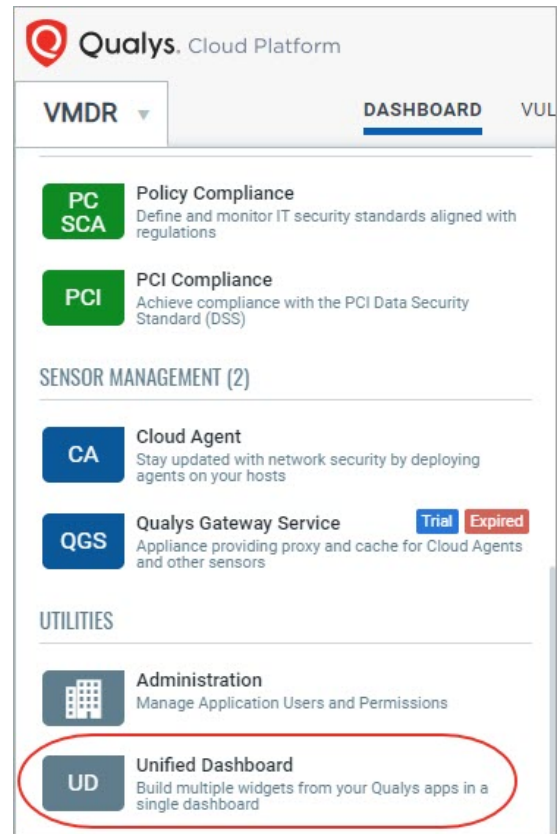
Unified Dashboard (UD) brings information from all Qualys applications into a single place for visualization. UD provides a powerful new dashboarding framework along with platform service that will be consumed and used by all other products to enhance the existing dashboard capabilities.

You can use dashboards to convey relevant information to any audience at any time and in any place. The dashboards can be customized and shared with their intended end-users.

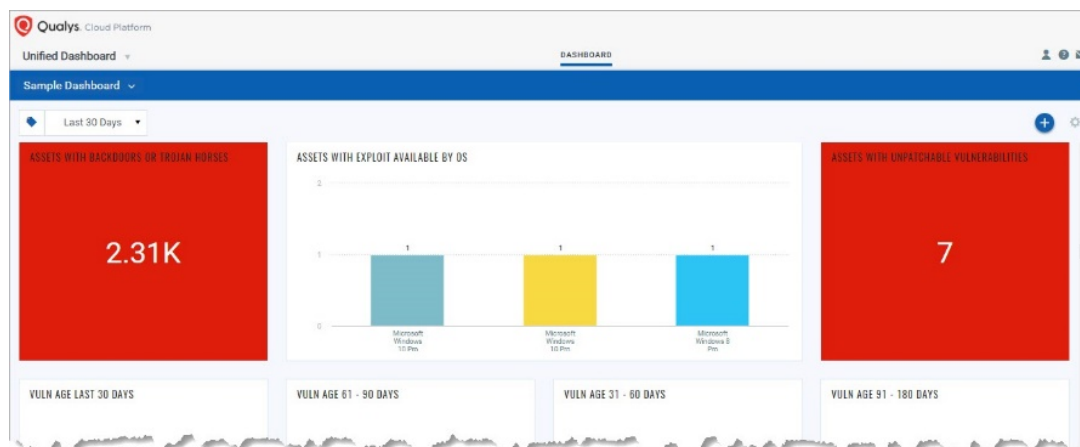
UD provides greater agility and enriches capabilities of dashboards. You can visualize data from other applications at a central place and get a better understanding of your data. You can use widget builder and improvise dashboards to make it uniform across all products.

Benefits

- Powerful platform to enhance your dashboards
- Capability to pull information from all Qualys applications
- Central place to visualize your data from different Qualys applications
- Enhanced widget builder capabilities for uniform widgets across all products.

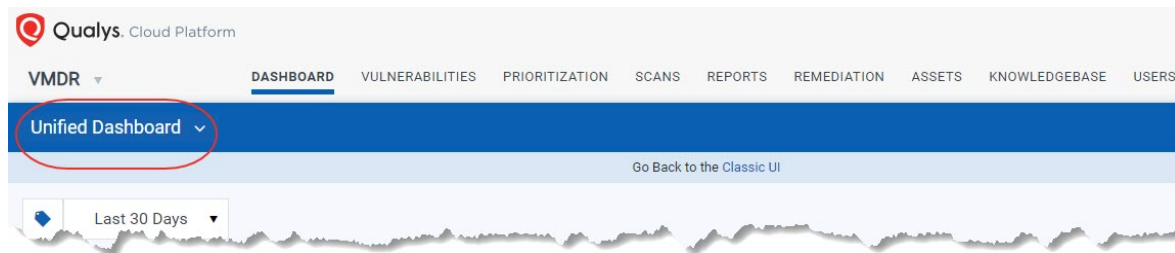


Sample Dashboard



Integration with VMDR

Unified Dashboard is integrated with VMDR for quick accessibility.



You can use the default VMDR 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.

New Threat Protection RTIs – Wormable and Predicted High Risk

With this release, you can configure a ruleset to get alerts on active security threats using these Threat Protection Real-Time Threat Indicators:

Wormable - Wormable has been associated with this vulnerability. The vulnerability can be used in “worms” - malware that spreads itself without user interaction.

Predicted High Risk - Predicted High Risk has been associated with this vulnerability. Qualys Machine Learning Model predicted this vulnerability as a High Risk based on various data sources including NVD, Social network, Dark web, Security Blogs, Code repository, Exploits etc.

How to configure a ruleset using threat indicators

Go to Configuration > Rulesets. Create a new ruleset or edit an existing one. In the Ruleset Builder, drag the Vulnerability rule type to the right side to start setting rule criteria.

First pick from vulnerability status levels (New, Active, etc) and then choose Add Criteria > Vulnerability. Scroll down and you'll see Threat Protection real-time indicators, including Wormable and Predicted High Risk.

The screenshot shows the 'Ruleset Builder' window. On the left, under 'Rule Types', 'Vulnerability' is selected. The main area shows 'Rule 1: New Vulnerability' with the following settings:

- When a vulnerability is:** ☒ New, ☐ Fixed, ☐ Active, ☐ Reopened
- ONLY IF:**
 - Type: ☐ Confirmed, ☐ Potential
 - Severity: ☐ 1, ☐ 2, ☐ 3, ☐ 4, ☐ 5
 - Title: Select one
 - QID: Select one
 - CVE: Select one
 - CVSS Score: Select one
 - Impact: ☐ Is Malware, ☐ Has Exploit, ☐ Has Patch, ☐ PCI
 - Exploit Kit Name: Select one
 - Malware Name: Select one
 - Exploit Public Name: Select one
- Threat Protection (RTI):** Select real-time threat indicators you would like to alert on.
 - ☐ Zero Day, ☐ Public Exploit
 - ☐ Active Attacks, ☐ High Lateral Movement
 - ☐ Easy Exploit, ☐ High Data Loss
 - ☐ Denial Of Service, ☐ No Patch
 - ☐ Malware, ☐ Exploit Kit
 - ☒ Wormable, ☒ Predicted High Risk

At the bottom, there is an 'Add Criteria' button and 'Cancel' and 'Finish' buttons.

You may also notice that we renamed Actively Attacked to Active Attacks and Exploit Public to Public Exploit to be consistent across Qualys apps.

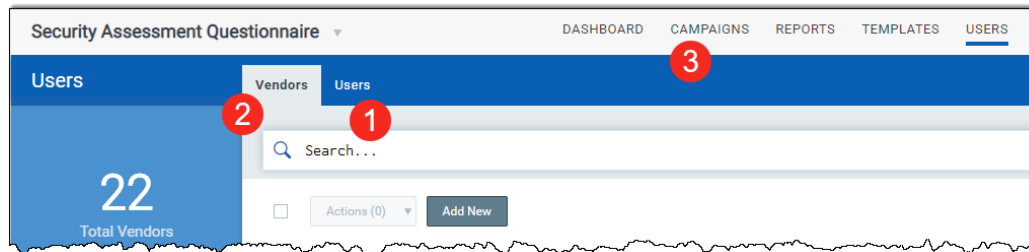
Not seeing Threat Protection (RTI) in the Ruleset Builder?

Threat Protection RTI options are only available to Threat Protection users with Trial or Full subscriptions.

Vendor On-boarding

We have now added the ability to onboard new vendors, keep track of the existing ones, and keeping record of their areas of business as well as gain accurate visibility into your vendors' records and related areas.

To onboard a new vendor and send out vendor assessments you need to do the following:



- 1) Create or identify existing users in SAQ for your vendor. Simply navigate to the USERS > Users tab to create new users.
- 2) Create a Vendor, by navigating to USERS > Vendors tab.
- 3) Create a campaign and add the user associated with that vendor to the campaign to initiate vendor assessment.

You can create Vendor profiles with required information such as contact details (SPOC), address, service provided and so on, including the ability to upload contractual files.

To onboard a vendor following onscreen wizard and do the following:

- Provide basic vendor information like company details, category of service provided, etc. Specify if the vendor is contractual or still in proposed state (RFP) and upload relevant contract documents
- In Assessment Configuration, identify the assessment areas that are relevant to services provided by your vendor. You can also add tags to better organize vendors in your organization.
- Identify Point of Contact for your vendor, along with identifying associated users and internal contact.
- Define vendor criticality manually or by using our internal campaign template to help you auto-calculate the criticality.

Once created this vendor is added to the vendors list in the Vendors tab. You can View, Edit, or Delete users using the Quick Actions menu.

To view vendor details, simply navigate to USERS > Vendors tab and choose the vendor you wish to view and from the Quick Actions menu select View.

← Vendor: Tetra Tech

VIEW MODE

Summary

Questionnaires

Criticality Evaluation Survey

Associated Users

Documents

Summary

Tetra Tech

Risk Rating: -

Next Assessment Date: -

Status: Active

Details

Criticality: HIGH

WebSite: -

Service Category: Administrative Support, Software

Parent Company: -

Vendor Type: Contractual

Address: 200 E Main St,Phoenix,85123,Arizona,USA

Assessment Areas: Compliance Server Security
2 more assessments

Vendor Contact: John Doe

Service Description

This is a software service company managing licenses

Activity

Onboarded On: Jun 22, 2020

Last Modified On: Jun 29, 2020

Tags

operatingSystem-U... software

Delete Catalog Entries

You can now delete catalog entries in the Web Applications > Catalog. Catalog entries are web applications discovered by maps and/or vulnerability and WAS scans in your account.

To delete one or more catalog entries, go to Web Applications > Catalog and select an entry and from the Quick Actions menu, click Delete.

Dashboard **Web Applications** Scans Detections Reports Configuration KnowledgeBase

Web Application Management Web Applications Authentication Catalog Maps

Search Results Actions (1) Update

Search

Filter Results

Status

- ☐ New
- ☐ Rogue
- ☐ Approved
- ☐ Ignored
- ☐ In Subscription

Operating System

IP Address	FQDN	Port	NetBIOS
<input checked="" type="checkbox"/> 10.11.68.60		8082	
<input type="checkbox"/> 10.115.95.146		80	
<input type="checkbox"/> 64.41.200.236	ys.com	80	
<input type="checkbox"/> 10.10.32.164		80	
<input type="checkbox"/> 10.11.68.58		85	
<input type="checkbox"/> mywebapp.com		80	
<input type="checkbox"/> 10.115.77.114		3001	

Quick Actions

- View
- Open In Browser
- Edit
- Mark As...
- Add Comment
- Add To Subscription
- Delete**

OR select multiple entries and from the Actions menu, click Delete.

Dashboard **Web Applications** Scans Detections Reports Configuration KnowledgeBase

Web Application Management Web Applications Authentication Catalog Maps

Search Results Actions (7) Update

Search

Filter Results

Status

- ☐ New
- ☐ Rogue
- ☐ Approved
- ☐ Ignored
- ☐ In Subscription

Operating System

Creation Date

Select a date

Last Update Date

IP Address	FQDN	Port	NetBIOS
<input checked="" type="checkbox"/> 10.11.68.60		8082	
<input type="checkbox"/> 10.115.95.146		80	
<input type="checkbox"/> 64.41.200.236	demo06.s02.sjc01.qualys.com	80	
<input type="checkbox"/> 10.10.32.164		80	
<input type="checkbox"/> 10.11.68.58		85	
<input checked="" type="checkbox"/> mywebapp.com		80	
<input checked="" type="checkbox"/> 10.115.77.114		3001	
<input checked="" type="checkbox"/> youtube.com		80	
<input checked="" type="checkbox"/> fonts.dzone.com		80	
<input checked="" type="checkbox"/> dz2cdn4.dzone.com		80	
<input type="checkbox"/> careers.dzone.com		80	

Actions

- View
- Open In Browser
- Edit
- Mark As...
- Add Comment
- Add To Subscription
- Delete**

Web Application XML Report to Show More Information for BURP Findings

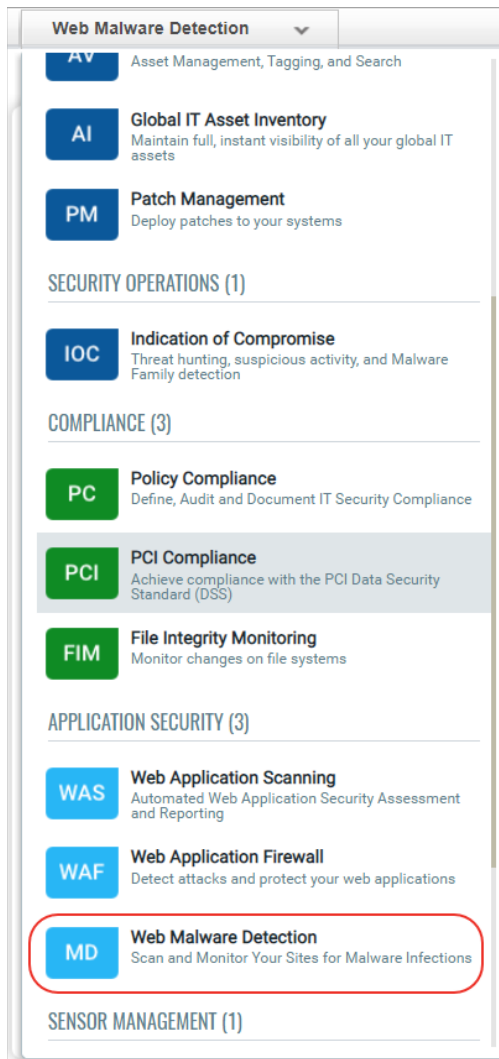
Web application reports in XML format will now show more information for BURP findings under GLOSSARY > BURP_TYPE_CODE_LIST > TYPE_CODE element.

Depending on the number of findings, the report may have one or more <TYPE CODE> elements under <BURP_TYPE_CODE_LIST>. A TYPE_CODE element will contain information about severity, category, title, description, and solution for BURP findings.

```
<GLOSSARY>
  <BURP_TYPE_CODE_LIST>
    <TYPE_CODE>
      <TYPE_CODE>5243392</TYPE_CODE>
      <SEVERITY>1</SEVERITY>
      <CATEGORY>Confirmed Vulnerability</CATEGORY>
      <TITLE>SSL cookie without secure flag set</TITLE>
      <DESCRIPTION><![CDATA[<p>If the secure flag is set on a cookie, the cookie is not
trivially intercepted by an attacker monitoring network traffic. However, if the secure
attacker may be able to induce this event by feeding a user a link that forces the
HTTP, an attacker may be able to use links of the form http://www.example.com/
>To exploit this vulnerability, an attacker must be suitably positioned on the
public Wi-Fi, or a corporate or home network that is shared with a computer. The
application's hosting infrastructure could also perform this attack. Note that this
<SOLUTION><![CDATA[<p>The secure flag should be set on all cookies that are used by
the application that are accessed over HTTPS should employ the secure flag.</p>]]>
    </TYPE_CODE>
    <TYPE_CODE>
      <TYPE_CODE>5243648</TYPE_CODE>
      <SEVERITY>5</SEVERITY>
      <CATEGORY>Potential Vulnerability</CATEGORY>
      <TITLE>Cookie scoped to parent domain</TITLE>
      <DESCRIPTION><![CDATA[<p>A cookie's domain attribute determines the scope of
able to access the cookie via JavaScript. If a cookie is scoped to a parent domain,
contains sensitive data (such as a session token) then this data is accessible to
<SOLUTION><![CDATA[<p>By default, cookies are scoped to the domain that created them.
scope, which is safe and appropriate in most situations. If you are concerned about
that domain and its subdomains, and confirm that you are working on the correct
    </TYPE_CODE>
    <TYPE_CODE>
      <TYPE_CODE>7340288</TYPE_CODE>
      <SEVERITY>2</SEVERITY>
      <CATEGORY>Potential Vulnerability</CATEGORY>
      <TITLE>Cacheable HTTPS response</TITLE>
      <DESCRIPTION><![CDATA[<p>Unless directed otherwise, browsers cache responses
sensitive information in application responses is stored in the cache. This can
<SOLUTION><![CDATA[<p>Applications should return caching headers that indicate that
caching for relevant paths within the web root. Alternatively, applications should
return the following HTTP headers in all responses containing sensitive information:
1>
```


Malware Detection module name changed to Web Malware Detection

We have changed the name of the Malware Detection module in the module picker from Malware Detection to Web Malware Detection. The icon of the module in the module picker will remain same.





Administration

Tagging Permissions

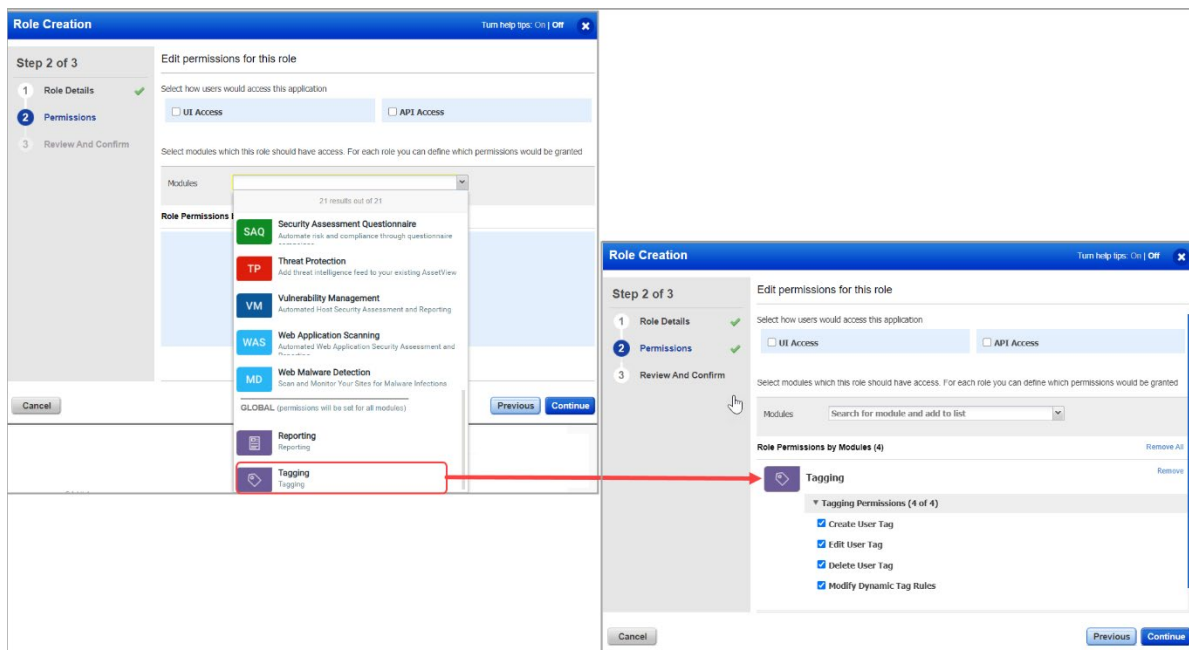
We have now moved the Tagging permissions under the GLOBAL section in the Administration (Admin) module. You can now enable Tagging permissions for more than one module simultaneously.

Using the Tagging permissions, you can:

- Create User Tags
- Edit User Tags
- Delete User Tags
- Modify Dynamic Tag Rules

The tagging permissions differ as per the user role.

Note: This change does not affect the existing Tagging permissions.



Issues addressed in this release

Qualys Cloud Platform 3.1 brings you many more improvements and updates.

AV AssetView

- Fixed an issue where the "operatingSystem.architecture" search query was not working.
- Fixed an issue where the "lastComplianceScanDate" search query was not populating correct results.
- Fixed an issue where dynamic tags were not being re-evaluated automatically even when the ""Re-evaluate rule on save"" option was selected.
- Depending on the type of scan executed for the asset, the Activity column indicates either the VM scan date or the compliance scan date. If both the scans are executed, we list two dates: VM scan date and Compliance scan date.

VMDR Vulnerability Management

- Fixed an issue where the last activity date was incorrectly displayed under the Vulnerabilities tab of VMDR.
- Fixed an issue where the Port number was not included in the CSV file downloaded from the Vulnerabilities tab of VMDR.
- Fixed an issue where you were incorrectly navigated to the KnowledgeBase page when you tried to navigate to Policy Compliance from the new VM Dashboard using the module picker.

CA Cloud Agent

- Fixed an issue to reduce a significant time for downloading agent list report.
- Fixed an issue where, when creating an activation key via version 1 was showing OTHER_ERROR in the response.
- Fixed an issue where API calls to endpoint `qps/rest/1.0/search/ca/agentactkey` was showing OTHER_ERROR in the response.
- Fixed an issue where Host List API response was showing inappropriate data for EC2_INSTANCE_ID.
- Fixed an issue where agents count sorting under the Activation Key tab was not working.
- Fixed an issue where partial activation of agent provisioned just before auto-activation job.
- Fixed an issue where status chirp was failing with response code 500.

- We have fixed an issue where comments in the comments section for the Catalog Entry was not shown. After the fix, you will be able to see the comments in the comments section properly for the Catalog Entry.
- We updated the help tip for scan name in the WAS online help to inform users to avoid using special characters in the scan name.
- We fixed an issue where an error was shown when the user was trying to launch a scheduled web application report using the Launch Now option. To fix the issue, we have added Schedule Report related permissions to the Manager role. Existing users need to add these permissions manually to the Manager role and set the "Create report" permission in the category "Reporting" for the user.
- We have fixed an issue where the scan reports were not showing correct data for some fields in the report. After the fix, the scan reports are showing correct data in all the fields.
- We fixed an issue where scheduled scans for web applications were skipped. After the fix, the scheduled scans are launched successfully.
- We fixed an issue where the WAS Engine version was not getting updated after the scan was completed. Hence, the user was shown an older version of the scan engine in the Help > About section. After the fix, the WAS Engine version will be updated in every scan processing if the WAS Engine is the later version than the version in the WAS settings.
- We removed the External Reference section from the scan report.
- We fixed an issue where on the bookmark panel, some bookmarks were not showing the names of the bookmarked sections in the WAS scan PDF reports. After the fix, WAS scan PDF reports show the names of all the bookmarked sections in the bookmark panel.
- We fixed an issue where an External Reference for one or more findings, added using Detections > Detection List > Actions > External References, was replaced when a second External Reference for the findings was added and saved. You can now add multiple external references. And we now show an error message if the user tries to add more than 10 external references for one or multiple findings.
- We fixed an issue where the users were not able to set IPs as DNS override using the Configuration > DNS Override > New DNS Override option. After the fix, you can now add any IP from 0.0.0.0 to 255.255.255.255 as DNS Override from both WAS UI and API.
- We fixed an issue where when the severity level was updated either for a finding from the Detections tab or for a QID from the KnowledgeBase, the changes were not reflecting on the Scan and the Web application reports in the HTML/PDF format. The reports were not showing the new severity levels set for the finding or the QID. After the fix, any changes made to the severity level of the findings or QIDs are reflecting in the reports.
- We fixed an issue where the user was getting an error message when saving the edited proxy settings for the web applications. You can now edit the proxy settings for web applications and save them successfully.

- We fixed an issue where the user was unable to update the Web application from the Web Malware Detection module when Malware monitoring is enabled in WAS. You can now update the Web application from the Web Malware Detection module when malware monitoring is enabled

Qualys Cloud Platform

- Fixed an issue where the VM icon was displayed when providing role permissions to the Threat Protection module.
- We have now fixed an issue where non-Gov Cloud regions were incorrectly displayed. The Gov cloud connectors now correctly display only Gov cloud regions that are enabled.
- Fixed an issue to improve the performance of the Purge Rule UI.