Qualys Cloud Platform v3.x

Release Notes

Version 3.13.1
December 1, 2022 (Updated on December 7, 2022)

What's New

CA **Cloud Agent**

Launch On Demand Scan using Cloud Agent

Manifest Field Renamed to Manifest Last Processed in Agent Summary

VMDR **Vulnerability Management, Detection, and Response**

New Widget for Vulnerability Management

Enhanced TruRisk Score Algorithm

Enhanced User Experience for TruRisk Score and Qualys Detection Score

Qualys Insights

New Tokens for VMDR

Updated Token for VMDR

WAS **Web Application Scanning**

New WAS User Interface

Qualys Cloud Platform 3.13.1 brings you many more improvements and updates! Learn more

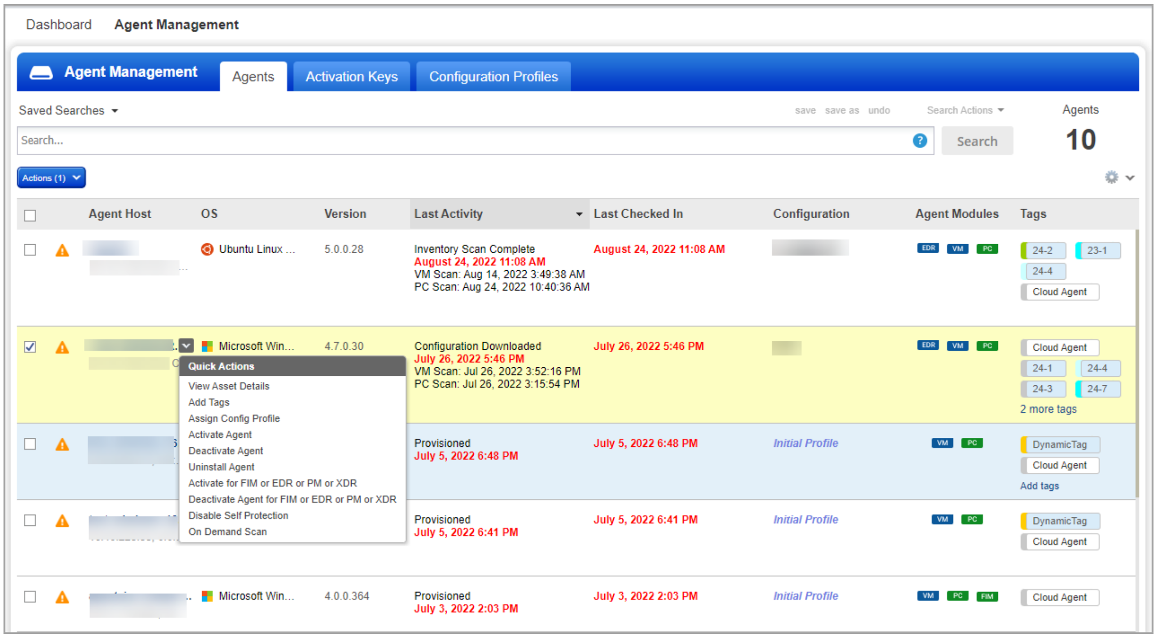
Launch On Demand Scan using Cloud Agent

With this release, you can launch the on-demand scan from the Cloud Agent UI.

The on-demand scan feature helps you with the flexibility to initiate a scan without waiting for the next scheduled scan. For example, running an on-demand scan can help you understand whether a vulnerability is remediated after the patch application. Currently, you can send 15000 on-demand scan requests per day.

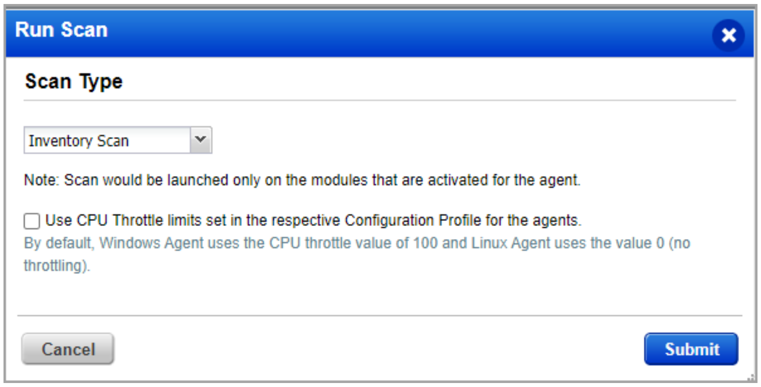
To launch a scan using the Cloud Agent module:

1. In the Cloud Agent, navigate to the **Agents** tab.
2. In the **Agents** tab, click the agent row > **On Demand Scan** from the **Quick Actions** menu.



□	Agent Host	OS	Version	Last Activity	Last Checked In	Configuration	Agent Modules	Tags
□	[redacted]	Ubuntu Linux ...	5.0.0.28	Inventory Scan Complete August 24, 2022 11:08 AM VM Scan: Aug 14, 2022 3:49:38 AM PC Scan: Aug 24, 2022 10:40:36 AM	August 24, 2022 11:08 AM	[redacted]	EDR VM PC	24-2 23-1 24-4 Cloud Agent
☑	[redacted]	Microsoft Win...	4.7.0.30	Configuration Downloaded July 26, 2022 5:46 PM VM Scan: Jul 26, 2022 3:52:16 PM PC Scan: Jul 26, 2022 3:15:54 PM	July 26, 2022 5:46 PM	[redacted]	EDR VM PC	Cloud Agent 24-1 24-4 24-3 24-7 2 more tags
□	[redacted]			Provisioned July 5, 2022 6:48 PM	July 5, 2022 6:48 PM	Initial Profile	VM PC	DynamicTag Cloud Agent Add tags
□	[redacted]			Provisioned July 5, 2022 6:41 PM	July 5, 2022 6:41 PM	Initial Profile	VM PC	DynamicTag Cloud Agent
□	[redacted]	Microsoft Win...	4.0.0.364	Provisioned July 3, 2022 2:03 PM	July 3, 2022 2:03 PM	Initial Profile	VM PC FIM	Cloud Agent

3. In the **Run Scan** screen, select **Scan Type**.



Scan Type

Inventory Scan

Note: Scan would be launched only on the modules that are activated for the agent.

□ Use CPU Throttle limits set in the respective Configuration Profile for the agents.
By default, Windows Agent uses the CPU throttle value of 100 and Linux Agent uses the value 0 (no throttling).

Currently, the following scans can be launched through the Cloud Agent module:

- Inventory scan
- Vulnerability scan
- Policy Compliance scan
- UDC scan
- SCA scan

4. Click **Submit**.

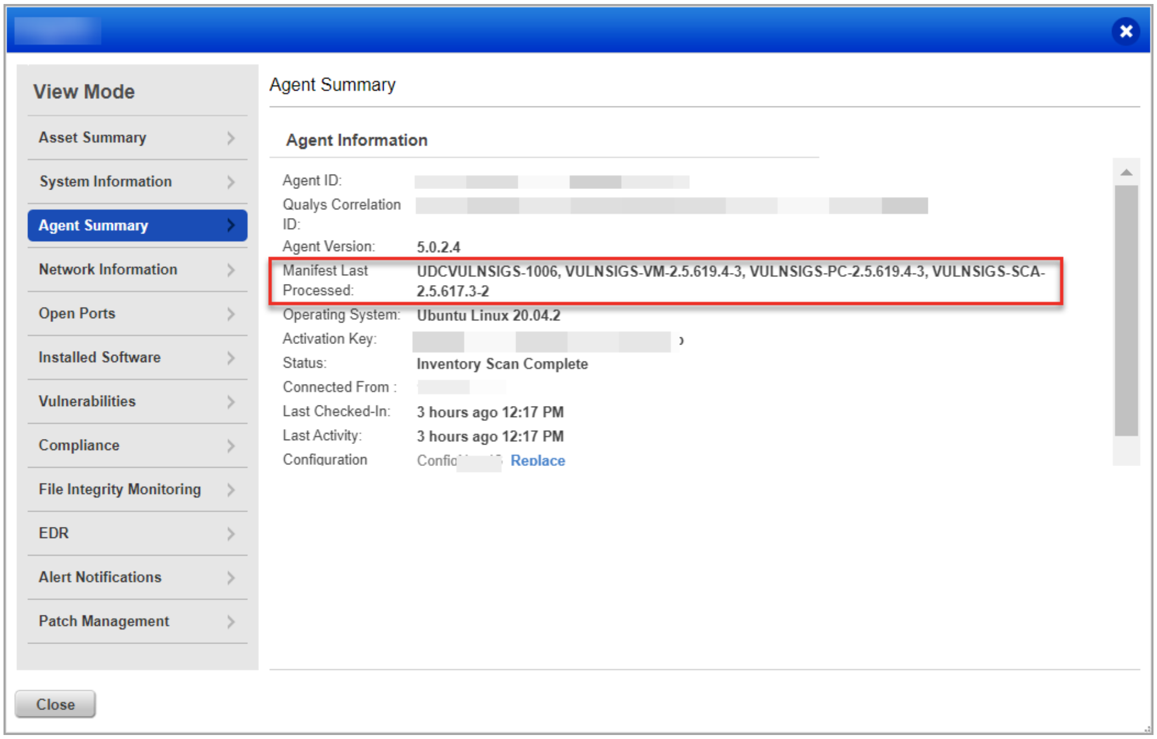
By default, Cloud Agent for Windows uses a throttle value of 100, and Cloud Agent for Linux uses a value of 0 (no throttling). If you want to use the values in the configuration profile, select the **Use CPU Throttle limits set in the respective Configuration Profile for agents** check box.

Note: This feature is supported only on Windows, Linux, and Linux_Ubuntu platforms and will be available only when the Windows and Linux agent binaries with on-demand scan support are available.

For the supported platform and Windows agent versions, refer to the *Features by Agent Version* section in the Cloud Agent Platform Availability Matrix.

Manifest Field Renamed to Manifest Last Processed in Agent Summary

With this release, the **Manifest** field in the **Agent Summary** tab in asset details is renamed to **Manifest Last Processed** to represent the data displayed correctly.



Agent Summary

Agent Information

Agent ID: [redacted]
Qualys Correlation ID: [redacted]
Agent Version: 5.0.2.4
Manifest Last Processed: UDCVULNSIGS-1006, VULNSIGS-VM-2.5.619.4-3, VULNSIGS-PC-2.5.619.4-3, VULNSIGS-SCA-2.5.617.3-2
Operating System: Ubuntu Linux 20.04.2
Activation Key: [redacted]
Status: Inventory Scan Complete
Connected From : [redacted]
Last Checked-In: 3 hours ago 12:17 PM
Last Activity: 3 hours ago 12:17 PM
Configuration Config[redacted] Replace

The **Manifest Last Processed** field displays the VM, PC, or UDC signature version of the manifest last processed by the Qualys Cloud Platform for the selected agent.

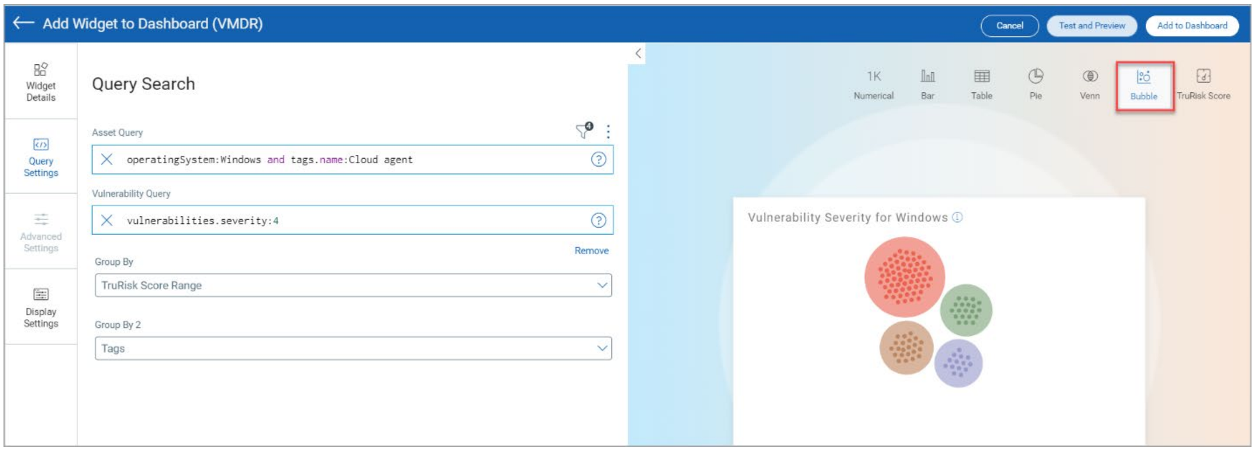
VMDR **Vulnerability Management, Detection, and Response**

New Widget for Vulnerability Management

With this release, we have introduced **Bubble** widget for the **Vulnerability Management** application. The Bubble widget is a logical grouping of assets comprising TruRisk Score in the outer circle and Asset tags in the inner circle of the widget. The outer and inner circles are clickable and direct you to the Vulnerabilities page.

Perform the following steps on the dashboard for the Vulnerability Management application to use the Bubble widget:

1. Click **Add Widget** + and select **Build your widget**.
2. In the **Widget Details**, select **Bubble** widget and provide the widget's name.
3. Click **Query Settings**.
4. Provide the **Asset** or **Vulnerability** query. By default, the Group By is for **TruRisk Score Range** and **Tags**.



Query Search

Asset Query

```
operatingSystem:Windows and tags.name:Cloud agent
```

Vulnerability Query

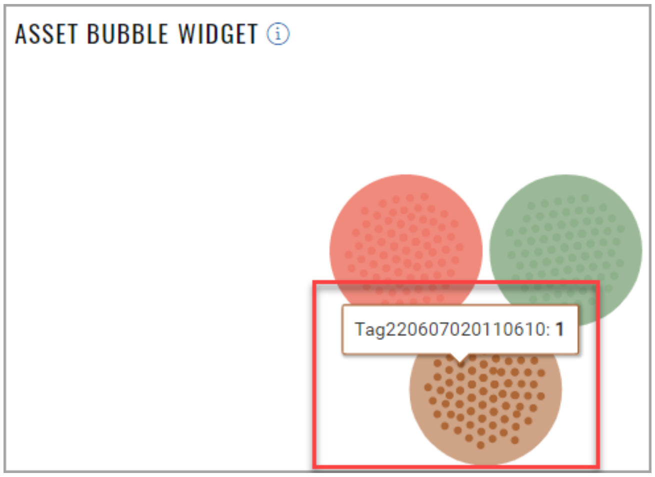
```
vulnerabilities.severity:4
```

Remove

Group By: TruRisk Score Range

Group By 2: Tags

5. Click **Add to dashboard** to view the widget on the dashboard.
6. To view the report of the query created, hover the mouse on the inner or outer circle of the Bubble widget.



7. You are redirected to the Vulnerabilities page that lists the assets based on your provided query.

Enhanced TruRisk Score Algorithm

With this release, the Asset Risk Score (ARS) is now renamed to TruRisk Score. We have enhanced the algorithm. Now, the new TruRisk algorithm includes the number of vulnerabilities and internal and external tags. In the new algorithm, the asset with greater vulnerabilities gets the higher score. The weight is based on the severity of the vulnerability. For example, the assigned weight value for vulnerability with severity five will be 1. The new algorithm score ensures the TruRisk Score value stays within 1000.

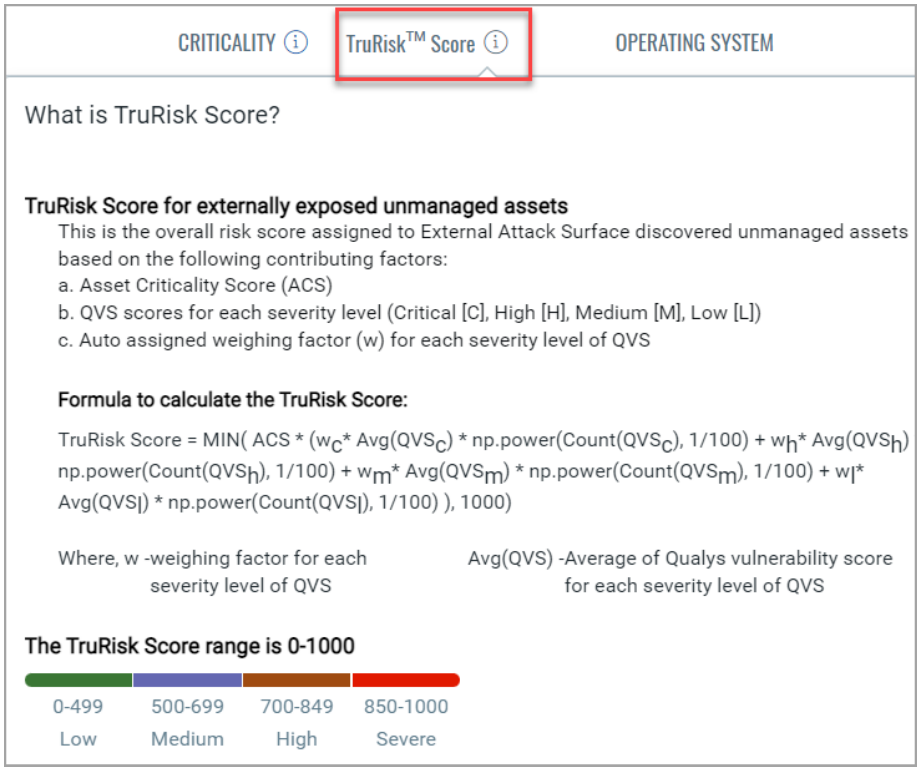
Following is the new TruRisk algorithm:

TruRisk Score = MIN(ACS * (w_c*Avg(QDS_c)*np.power(Count(QDS_c), 1/100) +
w_h*Avg(QDS_h)*np.power(Count(QDS_h), 1/100)+
w_m*Avg(QDS_m)*np.power(Count(QDS_m), 1/100)+
w_l*Avg(QDS_l)*np.power(Count(QDS_l), 1/100)),1000)

where,

- ACS - Asset Criticality Score.
- w - weighing factor for each severity level of QIDs [critical(c), high(h), medium(m), low(l)]
- Avg(QDS) - Average of Qualys risk score for each severity level of QIDs on that asset
- np.power – the value of np.power is constant to 0.01

The following screenshot is an example of the new TruRisk Score algorithm:



What is TruRisk Score?

TruRisk Score for externally exposed unmanaged assets

This is the overall risk score assigned to External Attack Surface discovered unmanaged assets based on the following contributing factors:

a. Asset Criticality Score (ACS)
b. QVS scores for each severity level (Critical [C], High [H], Medium [M], Low [L])
c. Auto assigned weighing factor (w) for each severity level of QVS

Formula to calculate the TruRisk Score:

TruRisk Score = MIN(ACS * (w_C* Avg(QVS_C) * np.power(Count(QVS_C), 1/100) + w_h* Avg(QVS_h) np.power(Count(QVS_h), 1/100) + w_m* Avg(QVS_m) * np.power(Count(QVS_m), 1/100) + w_l* Avg(QVS_l) * np.power(Count(QVS_l), 1/100)), 1000)

Where, w -weighing factor for each severity level of QVS

Avg(QVS) -Average of Qualys vulnerability score for each severity level of QVS

The TruRisk Score range is 0-1000

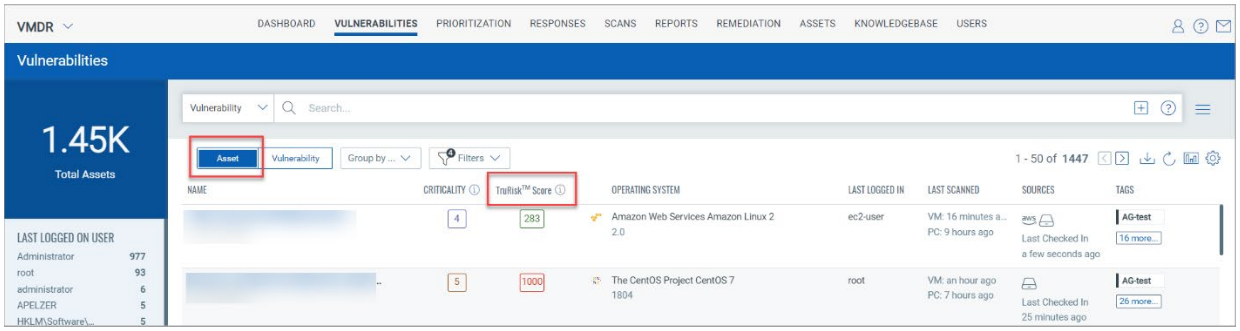
🟩	🟪	🟧	🟥
0-499	500-699	700-849	850-1000
Low	Medium	High	Severe

Enhanced User Experience for TruRisk Score and Qualys Detection Score

The new and enhanced TruRisk Score feature user interface gives you a visual of the contributing factors, recently trended vulnerabilities, Qualys Detection Score, and much more. Under the **Vulnerabilities** tab, **Asset** field, we have renamed the Risk Score column to **TruRisk Score**.

Perform the following steps to view the **TruRisk Score Details** for an asset:

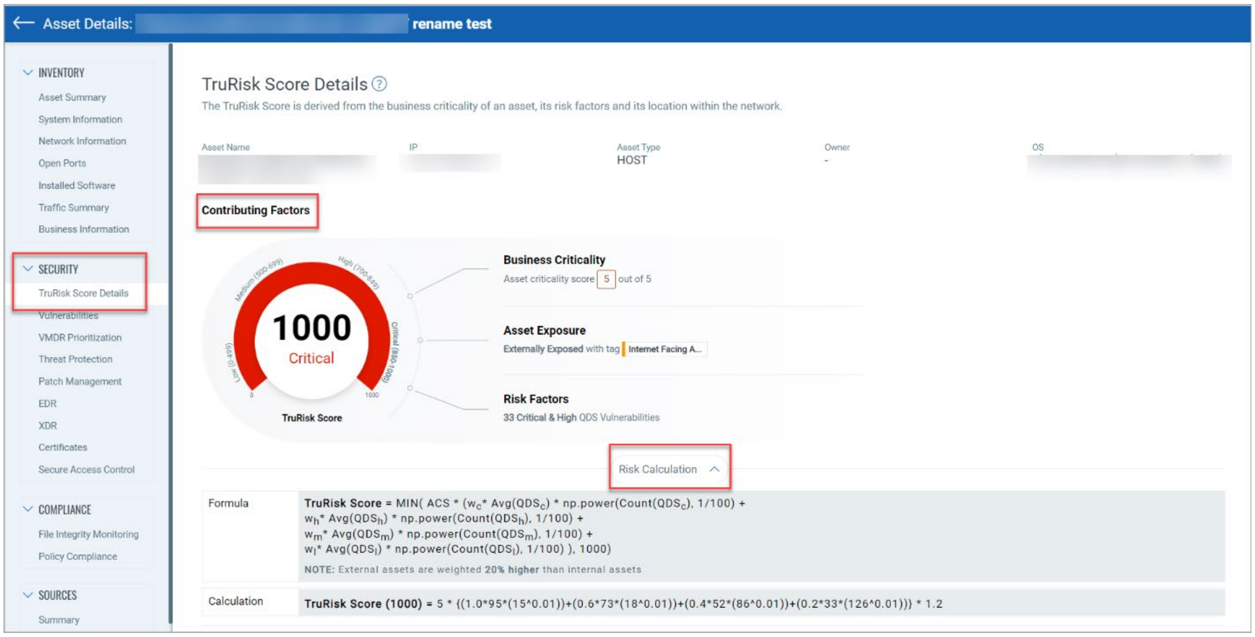
1. Under the **Vulnerabilities** tab, select the **Asset** field.
2. Click the value in the **TruRisk Score** column.



NAME	CRITICALITY	TruRisk™ Score	OPERATING SYSTEM	LAST LOGGED IN	LAST SCANNED	SOURCES	TAGS
[redacted]	4	283	Amazon Web Services Amazon Linux 2 2.0	ec2-user	VM: 16 minutes a... PC: 9 hours ago	aws Last Checked In a few seconds ago	AG-test 16 more...
[redacted] ..	5	1000	The CentOS Project CentOS 7 1804	root	VM: an hour ago PC: 7 hours ago	Last Checked In 25 minutes ago	AG-test 26 more...

LAST LOGGED ON USER	
Administrator	977
root	93
administrator	6
APELZER	5
HKLM\Software\...	5

You are redirected to the **TruRisk Score Details** page, which lists **Contributing Factors**, **Risk Calculation**, and **Vulnerabilities**. For more information, see VMDR online help.



TruRisk Score Details

The TruRisk Score is derived from the business criticality of an asset, its risk factors and its location within the network.

Asset Name	IP	Asset Type	Owner	OS
[redacted]	[redacted]	HOST	-	[redacted]

Business Criticality
Asset criticality score 5 out of 5

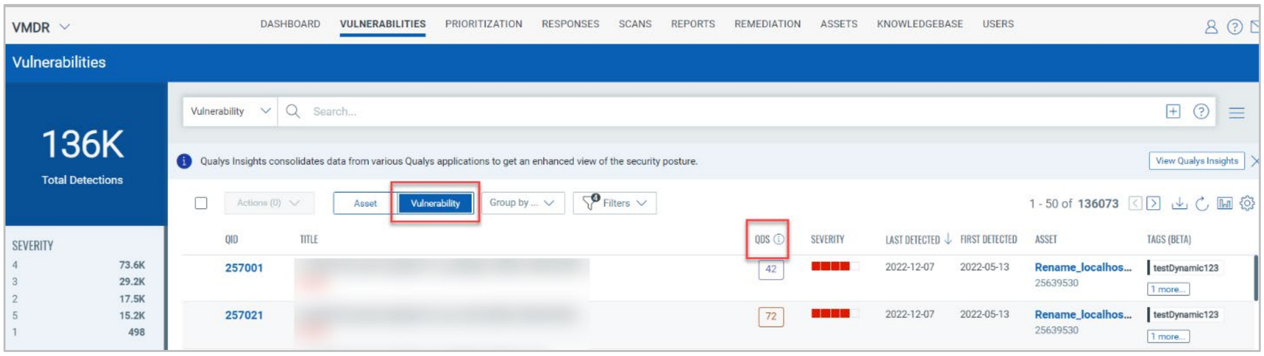
Asset Exposure
Externally Exposed with tag Internet Facing A...

Risk Factors
33 Critical & High QDS Vulnerabilities

Formula	**TruRisk Score** = MIN(ACS * (w_c* Avg(QDS_c) * np.power(Count(QDS_c), 1/100) + w_h* Avg(QDS_h) * np.power(Count(QDS_h), 1/100) + w_m* Avg(QDS_m) * np.power(Count(QDS_m), 1/100) + w_l* Avg(QDS_l) * np.power(Count(QDS_l), 1/100)), 1000) **NOTE:** External assets are weighted **20% higher** than internal assets
Calculation	**TruRisk Score (1000)** = 5 * {(1.0*95*(15^0.01))+(0.6*73*(18^0.01))+(0.4*52*(86^0.01))+(0.2*33*(126^0.01))} * 1.2

Perform the following steps to view the **Qualys Detection Score (QDS)** of a vulnerability detected on an asset:

1. Under the **Vulnerabilities** tab, select the **Vulnerability** field.
2. Click the value in the **QDS** column.

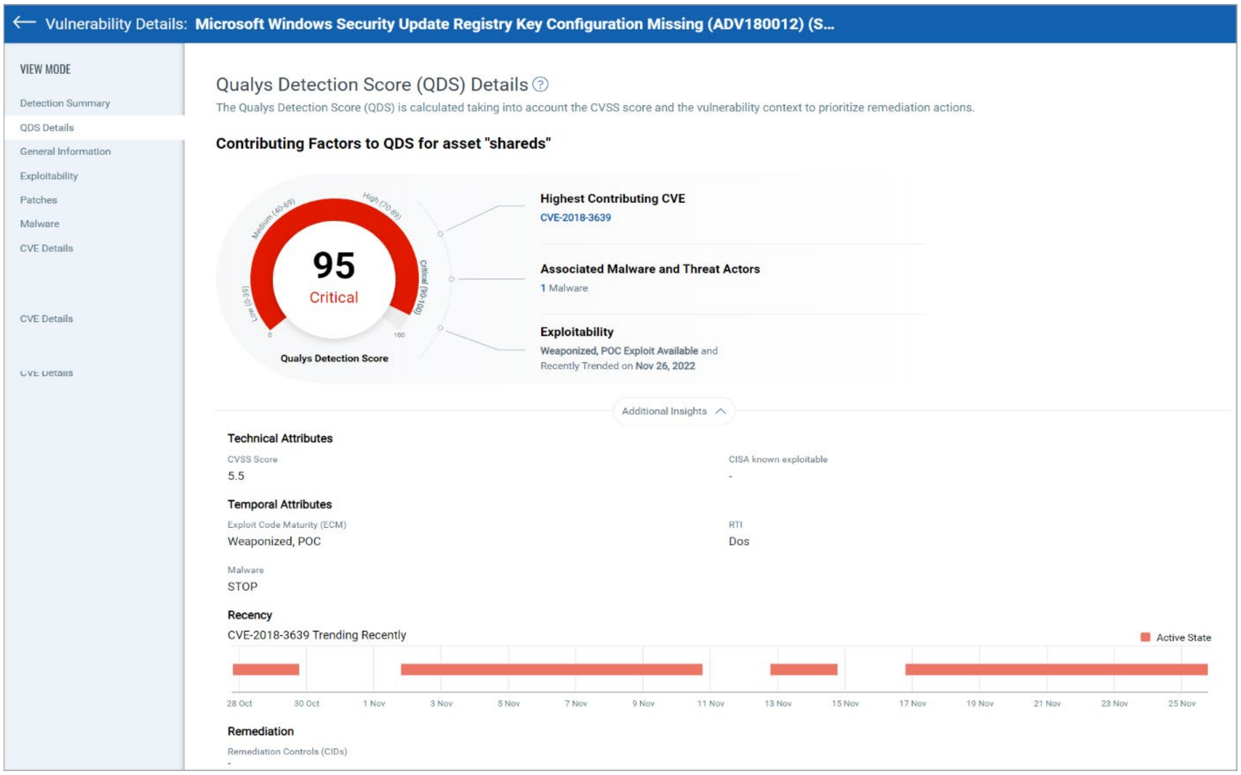


Qualys Insights consolidates data from various Qualys applications to get an enhanced view of the security posture.

SEVERITY	
4	73.6K
3	29.2K
2	17.5K
5	15.2K
1	498

QID	TITLE	QDS	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET	TAGS (BETA)
257001	[redacted]	42	■■■■	2022-12-07	2022-05-13	Rename_localhos... 25639530	testDynamic123 1 more...
257021	[redacted]	72	■■■■	2022-12-07	2022-05-13	Rename_localhos... 25639530	testDynamic123 1 more...

You are redirected to the **QDS Details** page, which lists **Contributing Factors**, **Technical Attributes**, **Temporal Attributes**, and **Recency**. For more information, see VMDR online help.



Qualys Detection Score (QDS) Details

The Qualys Detection Score (QDS) is calculated taking into account the CVSS score and the vulnerability context to prioritize remediation actions.

Contributing Factors to QDS for asset "shareds"

Highest Contributing CVE
CVE-2018-3639

Associated Malware and Threat Actors
1 Malware

Exploitability
Weaponized, POC Exploit Available and Recently Trended on Nov 26, 2022

Technical Attributes
CVSS Score: 5.5
CISA known exploitable: -

Temporal Attributes
Exploit Code Maturity (ECM): Weaponized, POC
RTI: Dos
Malware: STOP

Recency
CVE-2018-3639 Trending Recently

Remediation
Remediation Controls (CIDs): -

Qualys Insights

With this release, we have introduced Qualys Insights, which consolidates data from various Qualys applications and gives an enhanced view of the security posture. Currently, Qualys Insights displays data for Confirmed Malware Hashes along with TruRisk Score (for assets) and Qualys Detection Score (for vulnerabilities).

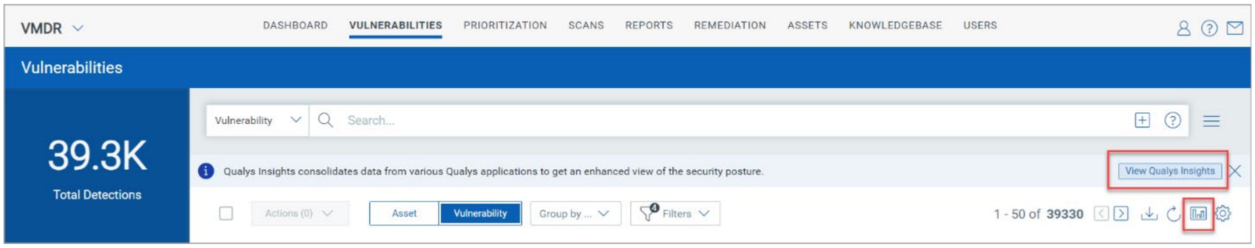
To view Qualys Insights, you should have the following:

- Full subscription to VMDR application, and
- Endpoint Detection and Response (EDR) module should be enabled.

Contact Qualys Support to enable the EDR module for your VMDR full subscription.

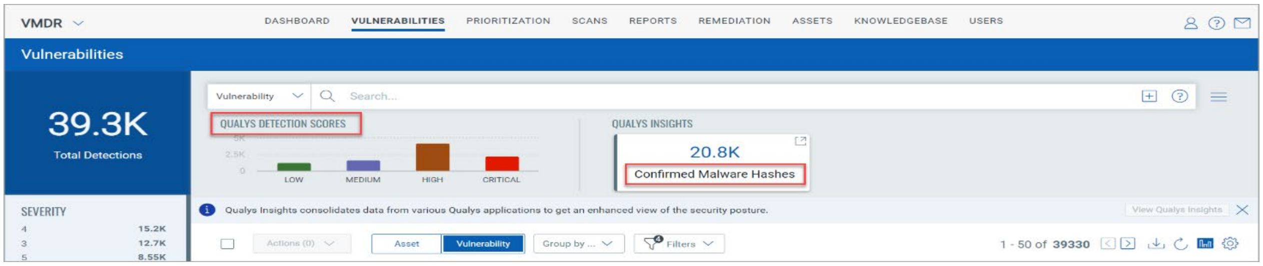
Perform the following steps to view Qualys Insights in VMDR:

1. Go to **VMDR** > **Vulnerabilities** tab
2. Click **View Qualys Insights** or **Toggle Graph**.



Qualys Insights consolidates data from various Qualys applications to get an enhanced view of the security posture.

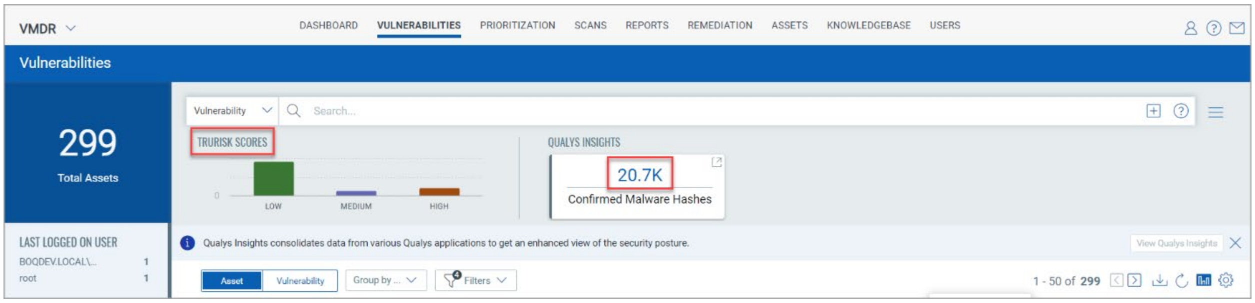
If the search is for **Vulnerability,** Qualys Insights displays **Qualys Detection Score** (QDS) along with **Confirmed Malware Hashes**. Following is an example of QDS with Confirmed Malware Hashes:



Qualys Insights consolidates data from various Qualys applications to get an enhanced view of the security posture.

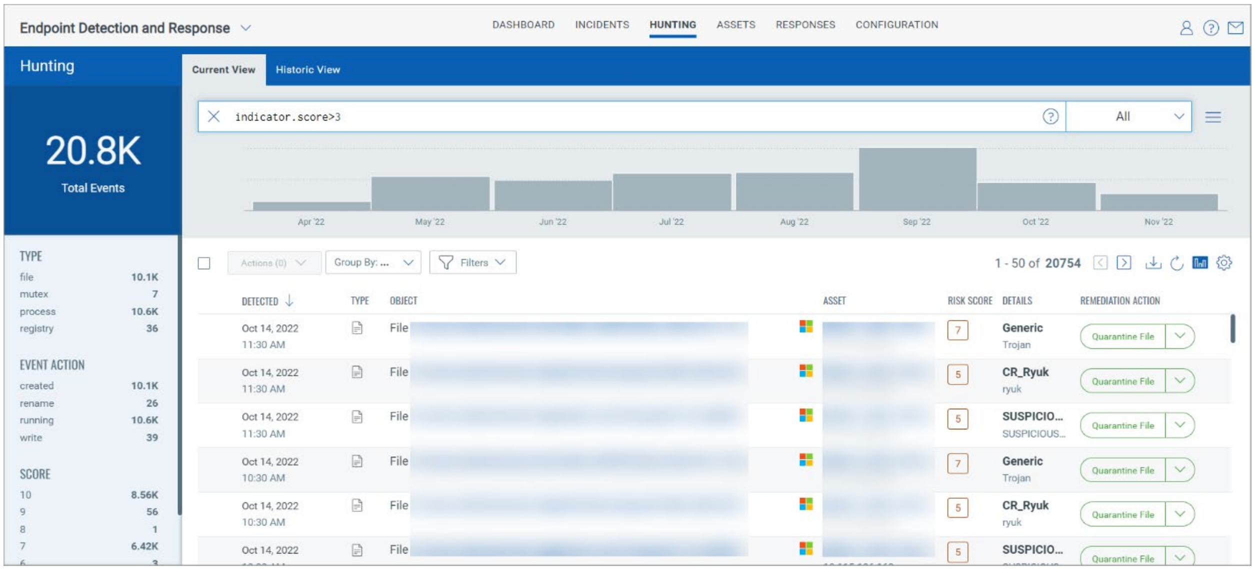
If you select the search for **Assets**, Qualys Insights displays **TruRisk Score** and **Confirmed Malware Hashes**.

3. Click the value of **Confirmed Malware Hashes,** and you will be redirected to Endpoint Detection and Response (EDR) page.



Qualys Insights consolidates data from various Qualys applications to get an enhanced view of the security posture.

The **Hunting** tab in the EDR application lists the files affected by malware along with the asset name. You can select the file to view the detailed information.



`indicator.score>3`

20.8K
Total Events

TYPE	
file	10.1K
mutex	7
process	10.6K
registry	36

EVENT ACTION	
created	10.1K
rename	26
running	10.6K
write	39

SCORE	
10	8.56K
9	56
8	1
7	6.42K

1 - 50 of **20754**

DETECTED	TYPE	OBJECT	ASSET	RISK SCORE	DETAILS	REMEDIATION ACTION
Oct 14, 2022 11:30 AM	File	[redacted]	[redacted]	7	**Generic** Trojan	Quarantine File
Oct 14, 2022 11:30 AM	File	[redacted]	[redacted]	5	**CR_Ryuk** ryuk	Quarantine File
Oct 14, 2022 11:30 AM	File	[redacted]	[redacted]	5	**SUSPICIO...** SUSPICIOUS...	Quarantine File
Oct 14, 2022 10:30 AM	File	[redacted]	[redacted]	7	**Generic** Trojan	Quarantine File
Oct 14, 2022 10:30 AM	File	[redacted]	[redacted]	5	**CR_Ryuk** ryuk	Quarantine File
Oct 14, 2022	File	[redacted]	[redacted]	5	**SUSPICIO...**	Quarantine File

New Tokens for VMDR

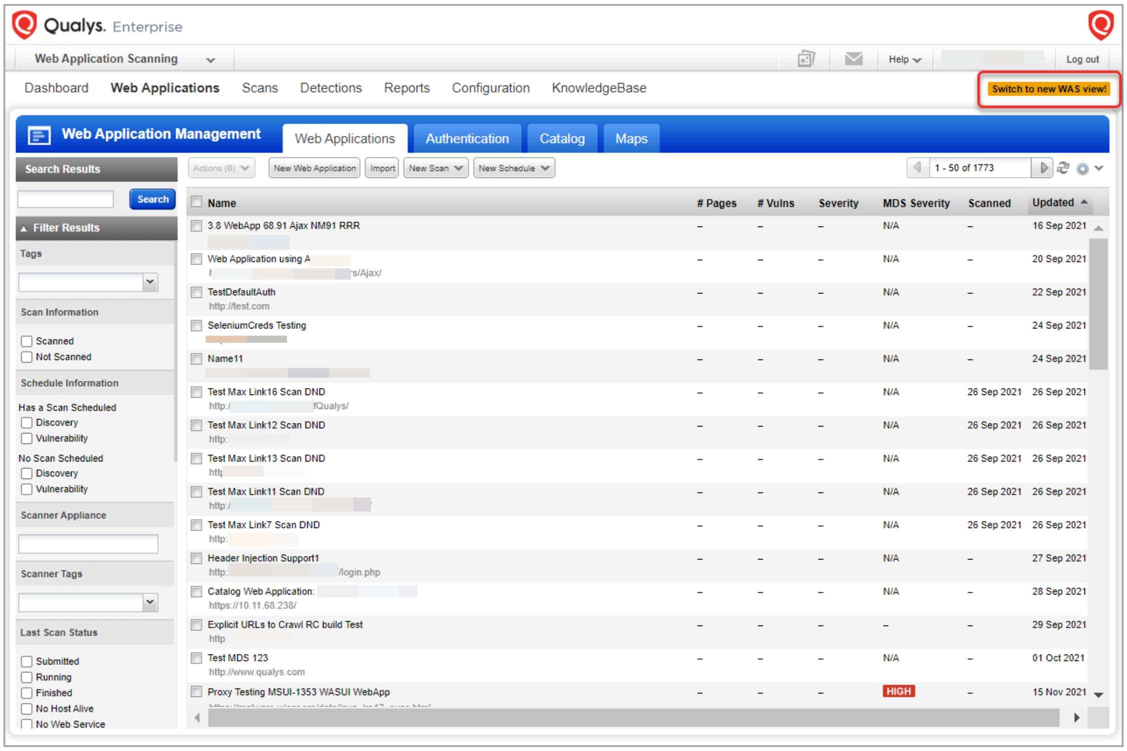
- **processors.threadsPerCore:** Select this token using the integer value to view the number of threads per core.
- **processors.coresPerSocket:** Select this token using the integer value to view the number of cores per socket.
- **processors.numberOfSockets:** Select this token using the integer value to view the number of sockets.
- **processors.numberOfCpu:** Select this token using the integer value to view the number of CPUs.
- **processors.isMultithreadingEnabled:** Select this token using the string value to define whether the processor has multi-thread enabled or disabled.
- **vulnerabilities.ttr.firstFound:** Select this token to determine the findings based on the Total and First Found time to remediate the vulnerability.
- **sensors.firstEasmScanDate:** Select this token to view the list of External Attack Surface assets based on their first scan date.
- **sensors.lastEasmScanDate:** Select this token to view the list of External Attack Surface assets based on their last scan date.

Updated Token for VMDR

- **trackingMethod: EASM**: We have updated the trackingMethod token and added External Attack Surface Management (EASM) to the list of the trackingMethod token.

New WAS User Interface

With this release, you can view the new and enhanced WAS user interface. To view the new WAS user interface, click the **Switch to new WAS view!** button.



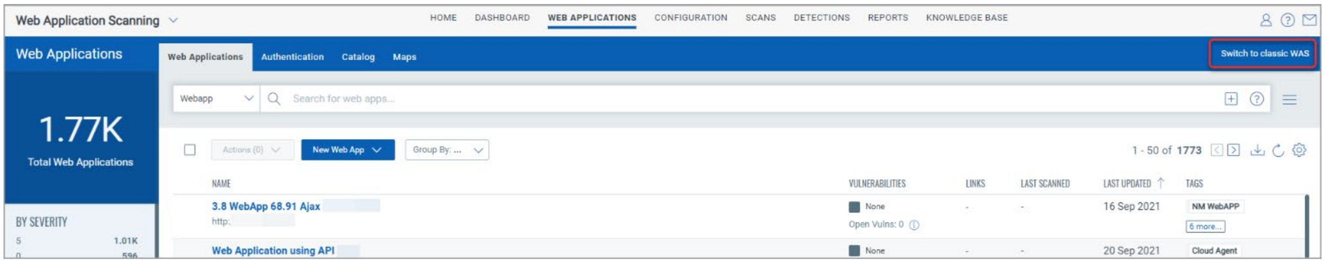
Name	# Pages	# Vulns	Severity	MDS Severity	Scanned	Updated
3.8 WebApp 68.91 Ajax NM91 RRR [redacted]	–	–	–	N/A	–	16 Sep 2021
Web Application using A[redacted] [redacted]s/Ajax/	–	–	–	N/A	–	20 Sep 2021
TestDefaultAuth http://test.com	–	–	–	N/A	–	22 Sep 2021
SeleniumCreds Testing [redacted]	–	–	–	N/A	–	24 Sep 2021
Name11 [redacted]	–	–	–	N/A	–	24 Sep 2021
Test Max Link16 Scan DND http:/[redacted]fQualys/	–	–	–	N/A	26 Sep 2021	26 Sep 2021
Test Max Link12 Scan DND http:[redacted]	–	–	–	N/A	26 Sep 2021	26 Sep 2021
Test Max Link13 Scan DND http[redacted]	–	–	–	N/A	26 Sep 2021	26 Sep 2021
Test Max Link11 Scan DND http:/[redacted]	–	–	–	N/A	26 Sep 2021	26 Sep 2021
Test Max Link7 Scan DND http:[redacted]	–	–	–	N/A	26 Sep 2021	26 Sep 2021
Header Injection Support1 http:[redacted]/login.php	–	–	–	N/A	–	27 Sep 2021
Catalog Web Application: [redacted] https://10.11.68.238/	–	–	–	N/A	–	28 Sep 2021
Explicit URLs to Crawl RC build Test http[redacted]	–	–	–	–	–	29 Sep 2021
Test MDS 123 http://www.qualys.com	–	–	–	N/A	–	01 Oct 2021
Proxy Testing MSUI-1353 WASUI WebApp	–	–	–	HIGH	–	15 Nov 2021

Currently, you can access **Web Applications**, **Authentication**, **Detections**, **Option Profiles**, and **Search Lists** tabs using the new interface.

The following enhancements are provided in the new WAS user interface:

- The **Home** tab provides an overview of all web applications under your subscription, their vulnerabilities, and an easy way to start integrated scanning.
- The **Dashboard** tab is integrated with the Qualys Unified Dashboard.
- The Qualys Query Language (QQL) is integrated for enhanced search.

If you switch to the new user interface in the current session, in the next login, WAS opens in the new user interface. To switch to the old user interface, click the **Switch to classic WAS** button.



NAME	VULNERABILITIES	LINKS	LAST SCANNED	LAST UPDATED	TAGS
3.8 WebApp 68.91 Ajax [redacted] http:[redacted]	None Open Vulns: 0	-	-	16 Sep 2021	NM WebAPP 6 more...
Web Application using API [redacted]	None	-	-	20 Sep 2021	Cloud Agent

Issues Addressed

CA Cloud Agent

- We have fixed an issue where an error occurred in assigning the UDC manifest while adding UDC to an asset.
- We have fixed an issue where the user could not download the Cloud Agent binary file using the **Download.exe** button when the browser used Japanese as the default language.

SAQ Security Assessment Questionnaire

- We fixed an issue where the user was unable to view the delegated questionnaire. The user was getting a blank page when clicking Questionnaire to view the questions.

VM Vulnerability Management

- We have fixed an issue where the Vulnerability/Host Ratio widget displayed the same vulnerability count for different queries.
- We have fixed an issue where VMDR UI did not display the port numbers. With this release, the VMDR UI displays the port number for Vulnerabilities having a port number. If a port number is unavailable for a Vulnerability, the value shown is 0.
- We have fixed an issue where users with a Reader role, having permission to view assets, could update the assets. With this release, the edit option is available for Super User or if the user role is converted to a Manager.
- We have fixed an issue where the user was unable to view the Asset details when clicked on the Count option.
- We have fixed an issue where the Vulnerability and Prioritization tabs are not displayed for the Shodan assets if the asset is not activated for the VM application.
- With this release, we have changed the character limit for asset and vulnerability queries from 1800 to 4096 characters. The following error message will be displayed if the vulnerability or asset query exceeds the 4096 character count:- "An error occurred while loading the GroupBy data."
- To maintain the count consistency across all widgets that has Display results as Assets and Groupby, we have renamed the following labels:
  - Operating System to Operating System Name
  - Operating System Name to Operating System Product Name

  The renaming of labels fixes the Operating Systems EOL count inconsistency issue.
- We have fixed an issue where non-EOL assets were listed in the EOL Asset query.

- We have fixed an issue where the list of Operating Systems was not displayed in the Vulnerabilities CSV report of the Operating System field.

WAS Web Application Scanning

- We have fixed an issue where the user was redirected to the login page when downloading scan results in legacy XML using the Download option in the **Quick Actions** menu in the **Scans** > **Scan List**.