



Vulnerability Management Detection and Response

Getting Started Guide

August 26, 2023

Copyright 2023 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100



Table of Contents

About this Guide	4
About Qualys	4
Qualys Support	4
About VMDR	5
How does it work?	6
Identify your Assets	7
Get Started with Cloud Agents	7
What are the other ways to find assets	10
Discover Vulnerabilities.....	11
Prioritize Threats with TruRisk	13
Prioritization Modes	13
Reading the VMDR Prioritization Report	17
Patch Management.....	21
Patch Vulnerabilities from VMDR Report	21

About this Guide

Welcome to Qualys Vulnerability Management, Detection, and Response (VMDR). The VMDR Getting Started Guide help you get acquainted to discover, assess, prioritize, and patch critical vulnerabilities in real time and across your global hybrid-IT landscape — all from a single solution.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the [Cloud Security Alliance \(CSA\)](#). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/

About VMDR

Vulnerability Management, Detection and Response (VMDR) enables you to discover, assess, prioritize, and patch critical vulnerabilities and misconfigurations in real time and across your global hybrid-IT landscape all in one solution.

It helps you get continuous vulnerability assessments with cloud agents, network level visibility using network scanners and multiple types of sensors' and leverages artificial intelligence to instantly assess and prioritize threats based on relevant context.

VMDR starts with asset discovery and inventory to make sure you have an accurate account of all devices in your environment.

With VMDR you get

- **Asset Inventory:** available for environments like, Certificate, Cloud, Container, Mobile Devices.
- **Unlimited Sensors:** identify assets like, Virtual Passive Sensors, Cloud Agents, Mobile Agents, Container Sensors.
- **Quick Search:** search any asset in seconds using over 200+ searchable attributes.
- **Customizable Dashboards and widgets:** customize dashboards and widgets along with trending information.

Know your Subscription Type

If you are an existing VM customer then you are upgraded to VMDR experience by default and you can buy VMDR to get additional features.

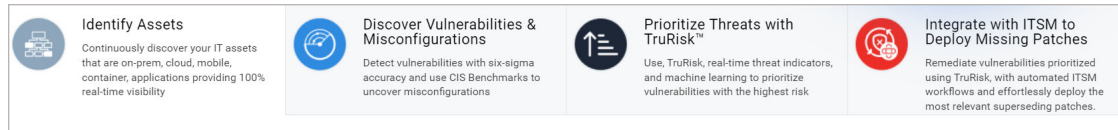
Once you upgrade to VMDR you'll also get

- **TruRisk:** mitigates risk in the business environment by optionally including VMDR TruRisk FixIT or VMDR TruRisk ProtectIT.
- **Security Configuration Assessment:** assess and identify security configuration and misconfigurations on your assets based on CIS benchmarks.
- **Threat-based Prioritization:** evaluates based on continuously updated Real-time threat indicators.
- **Real-time Alerting:** emails critical vulnerabilities and changes to your external perimeter, etc.
- **Deployment of missing patches:** Initiate deployment of missing patches from the Prioritization report directly.

Note: Deployment of patches is available only for customers with the Patch Management add-on.

How does it work?

With VMDR, you will be able to accomplish real time asset discovery and vulnerability information, prioritizing or short listing the vulnerabilities according to the threat intelligence and detecting and deploying right remedial patches at the click of a button.



Identify Assets

Start identifying assets by installing Cloud Agents or upgrading existing agents for VMDR. Assign tags to categorize and organize your assets. You can also use other methods such as Scanners, Passive Sensor, Cloud Inventory, Container Inventory, Mobile Device Inventory to build your inventory. To know more refer, to [Identify your Assets](#)

Discover Vulnerabilities & Misconfigurations

Our always up-to-date signature database continuously discovers software vulnerabilities and identifies security misconfigurations. Get a complete view of your vulnerability posture from an asset and vulnerability point of view in the Vulnerabilities tab. To know more, refer to [Discover Vulnerabilities](#)

Prioritize Threats with TruRisk™

Run the Prioritization report to prioritize most critical threats on your assets based on real-time threat indicators and identify what to remediate first. With TruRisk you can assess the risk scores of your assets and prevent attacks. TruRisk Score feature quantifies asset risks using Qualys Detection Score (QDS).

To know more about TruRisk Score, refer to [Discover Vulnerabilities](#).

To know more, refer to [Prioritize Threats with TruRisk](#)

Detect & Deploy Missing Patches

VMDR for IT Service Management (ITSM) manages tracking of open vulnerabilities and remediation mapping by using the ServiceNow ITSM platform. ServiceNow tasks are automatically assigned to the group to deploy the most relevant patches.

To know more, refer to [Patch Management](#)

Identify your Assets

Set up your Cloud Agents, scanners and sensors so as to continuously discover and build inventory of your IT assets that are on-prem, cloud, mobile, container, applications providing 100% real-time visibility.

Get Started with Cloud Agents

Start building your inventory by installing new cloud agents or by upgrading your existing cloud agents for VMDR.

VMDR requires the activation of a purpose-built engine for detecting missing patches for Cloud Agents. While this engine is extremely lightweight and efficient, activating Cloud Agents for VMDR will require a 20MB download and 100MB of free space on each host for these components.

[Install new agents](#)

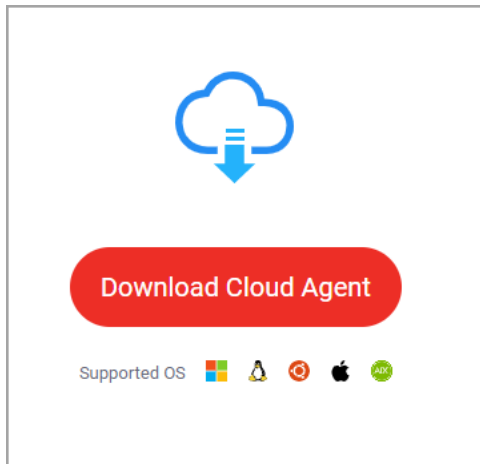
[Upgrade existing agents](#)

Know the requirements

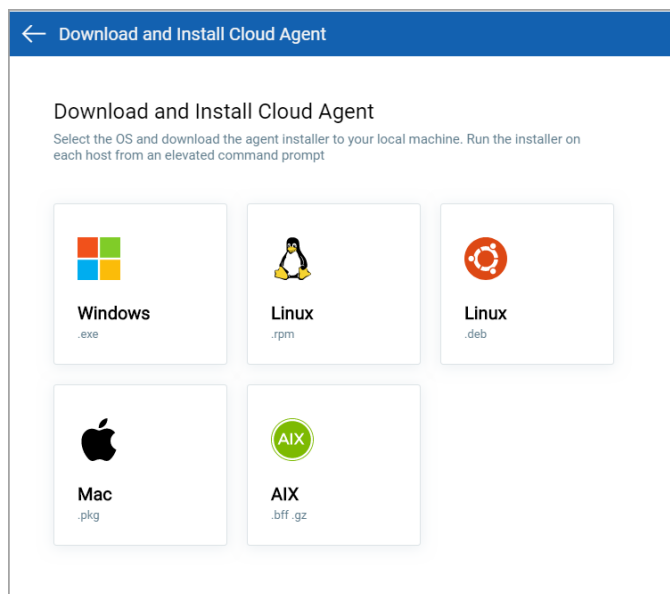
Here are the system requirements for installing and running Cloud Agents:

- Host must reach Qualys Cloud Platform (or Qualys Private Cloud Platform) over HTTPS port 443
- (Windows) Local administrator privileges on the host. Proxy configuration is supported.
- (Linux, Mac, AIX) Root privileges, non-root with sudo root delegation, or non-root with sufficient privileges. Proxy configuration is supported.

Install new agents



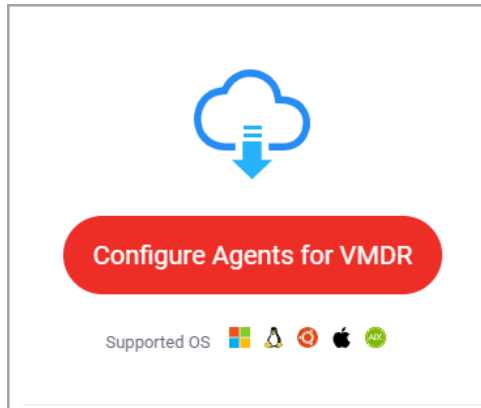
Navigate to the Welcome option in the Help menu to view the Welcome page. In the Identify Assets section click the Download Cloud Agent button.



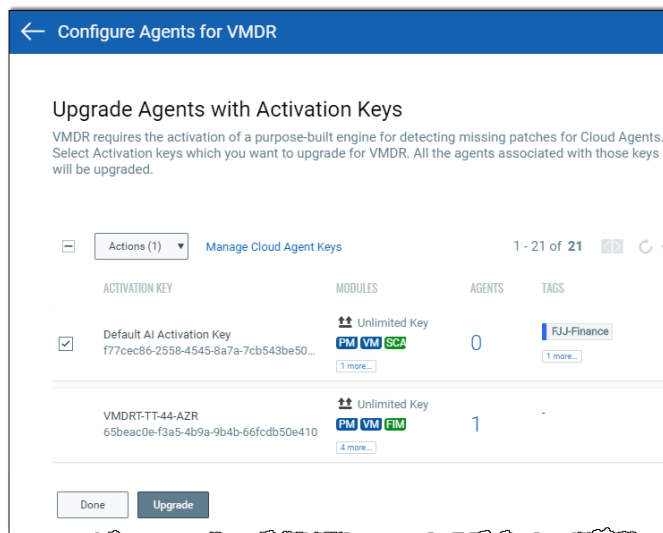
Select an OS and download the agent installer to your local machine. Run the installer on each host from an elevated command prompt.

For example, click Windows and follow the agent installation instructions displayed on the page. We provide you with a default AI activation key for the agent installation. To add or manage your keys, go to Cloud Agent > Agent Management.

Upgrade existing agents



Navigate to the Welcome option in the Help menu to view the Welcome page. In the Identify Assets section click the Configure Agents for VMDR button.



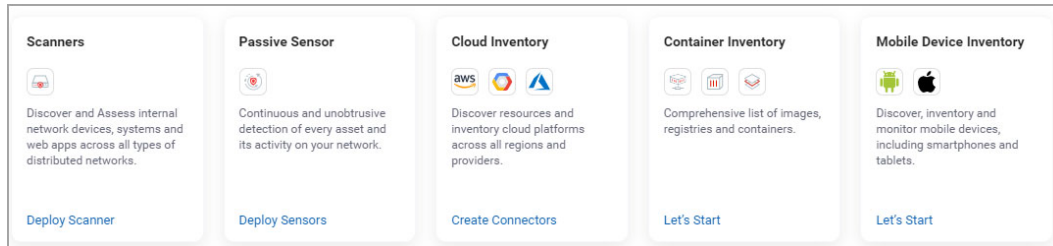
Select the desired activation keys and click Upgrade. The selected activation keys will be upgraded for VMDR.

To know more download the [Cloud Agent Getting Started Guide](#).

What are the other ways to find assets

You can also build your inventory for on-prem (devices and applications), mobile, endpoints, clouds, containers, OT and IoT assets using scanners, sensors, or connectors.

Navigate to the Welcome option in the Help menu to view the Welcome page. In the Identify Assets section select how you want to start configuring your inventory.



What's next?

You will start viewing all your assets and vulnerability details in the Vulnerability tab in VMDR.

Discover Vulnerabilities

Once your inventory is built, you can view the vulnerability posture of your assets in the **Vulnerabilities** tab. You can search for vulnerabilities by **Vulnerability** and by **Asset**. All the assets and their associated vulnerability details that are identified by cloud agents, scanners and sensors are listed in the **Vulnerabilities** tab. Using the [Qualys Query Language](#) you can use the **Asset** and/or **Vulnerability** view to search for a specific asset or vulnerability.

The following screenshot is a search example of the Windows assets that have severity as 4. You can download the search results in the CSV format to your local systems.

The screenshot shows the Qualys VMDR interface with the 'Vulnerabilities' tab selected. The search filters are set to 'vulnerabilities.severity:4' and 'operatingSystem:Windows'. The results table shows three entries for Microsoft Windows 10 assets, all with a criticality of 4 and a TraRisk Score of 706, 918, and 1000 respectively. The 'Quick Actions' menu is open, showing 'View Asset Details' and 'View Vulnerability Details' options.

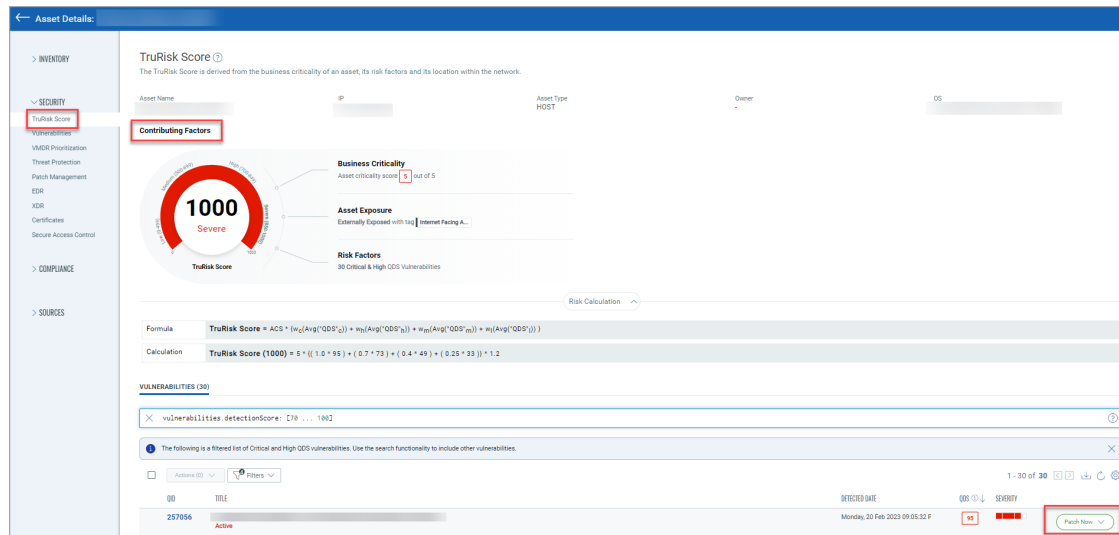
NAME	CRITICALITY	TraRisk™ Score	OPERATING SYSTEM	LAST LOGGED IN	LAST SCANNED	SOURCES	TAGS
[Redacted]	4	706	Microsoft Windows 10	Administrator	VM: 5 hours ago	Quays Service Tag	25 more...
[Redacted]	5	918	Microsoft Windows 10	Unknown	VM: Friday, 24 Ju...	saa	20 more...
[Redacted]	5	1000	Microsoft Windows	Unknown	VM: 4 days ago	saa	38 more...

Note: The download for detections is limited to 50,000 records across all assets. For a single asset, if more than 500 detections are reported, the download is limited to its first 500 detections.

From the **Quick Actions** menu, click **View Asset Details** or **View Vulnerability Details** to get more information about the selected **Asset** or the **Vulnerability**.

This screenshot is identical to the one above, but with the 'Quick Actions' menu open for the first row. The menu shows 'View Asset Details' and 'View Vulnerability Details' options.

The **TruRisk Score** column lists the assets score that is derived from the business criticality of an asset, its risk factors and its location within the network. The TruRisk Score page displays the TruRisk Contributing Factors - Business Criticality, Asset Exposure, and Risk Factors.



In case the vulnerability is Qualys patchable and you have the Patch Management add on in your subscription then you can click the **Patch Now** option which helps you initiate the deployment workflow in Patch Management.

If you have the Security Configuration Assessment add-on then you can do configuration assessment and identify security misconfigurations on your assets based on CIS benchmarks.

To know more about TruRisk Score, refer [Asset Details](#) in VMDR online help.

Prioritize Threats with TruRisk

VMDR Prioritization allows you to automatically prioritize the riskiest vulnerabilities on your most critical assets – reducing potentially thousands of discovered vulnerabilities, to the few that matter. Using real-time threat intelligence, we help you detect and prioritize the vulnerabilities to remediate first, based on your environment.

The VMDR Prioritization report indicates the most critical threats and prioritizes patching.

It also:

- Guides you to focus resources in the right area to first patch the highest risk vulnerabilities.
- Increases the security posture of your organization by identifying and remediating the vulnerabilities that are likely to get exploited in the wild by threat actors.
- Empowers security analysts to pick and choose the relevant threat indicators. For example, if an organization has financial data of users, they can prioritize vulnerabilities based on 'High Data Loss' indicator to first identify and remediate vulnerabilities that may result in data exfiltration, if exploited.
- Helps you identify the specific patch that fixes a particular vulnerability.
- Reduces remediation time by detecting the patch to be deployed from the same platform in an integrated workflow, at the click of a button (if Patch Management app is enabled in your subscription).
- Includes only the confirmed vulnerabilities.

Prioritization Modes

We provide you with the following two options to prioritize the remediation of vulnerabilities based on:


- Age, RTI, and Attack Surface
- Qualys TruRisk™ Mode

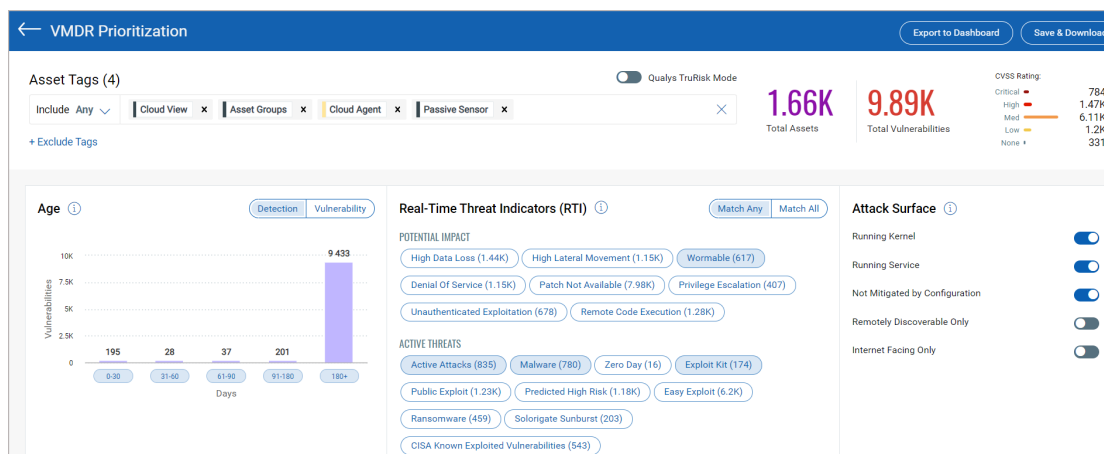
Age, RTI, and Attack Surface

Qualys offers you an option to prioritize and remediate vulnerabilities based on filters like Age, RTI, and Attack Surface.

Prerequisites: Before you start generating the prioritization report, ensure that:

- You have gathered the vulnerability posture for the assets. You could build your asset inventory using Cloud Agents or other methods such as Scanners, Passive Sensor, Cloud Inventory, Container Inventory, Mobile Device Inventory. All the assets and their associated vulnerability details that are identified by cloud agents and sensors are listed in the Vulnerabilities tab. Refer to [Identify your Assets](#).
- You have the Create Report permission (part of Global Reporting permissions). Contact your manager if you do not have the adequate permissions.

1. In the **Prioritization** tab click **Reports**.
2. Click **Start Prioritizing**
3. Select at least one Asset tag to display the prioritized list of vulnerabilities associated with the assets.
4. Click  to proceed with Prioritization.
5. In the Asset Tags section, from **Include** and **Exclude** menu, select one of the following options:
 - Any: to include or exclude all assets that might have any of the selected tags.
 - All: to include or exclude only those assets which have all the selected tags.
6. Select the various filters for VMDR Prioritization report.



Detection Age: Select detection age ranges (0-30, 31-60, etc.) to include in the report. The Detection age is based on when the vulnerability was first detected (by a scanner or cloud agent).

Real-Time Threat Indicators: Select the Real-Time Threat Indicators (RTIs) that you're interested in. Your report will include vulnerabilities that match *any* of the selected RTIs.

Attack Surface: Select these filters to remove vulnerabilities from the report that aren't the highest priority so you can focus on what's most critical to your organization.

7. Click **Prioritize Now** to enable the threat intelligence to prioritize the riskiest vulnerabilities on your network for the assets you selected.


Once you generate the report, you could proceed with patching the vulnerabilities (if Patch Management app is enabled in your subscription), export the report in the form of a widget to your dashboard or download the report in CSV format. To know more refer to [Reading the VMDR Prioritization Report](#)

Qualys TruRisk

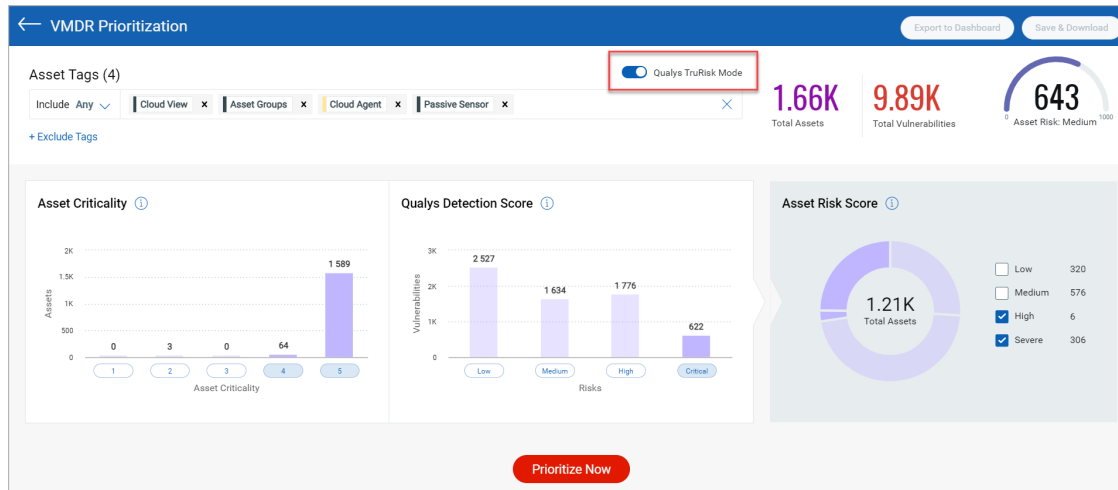
Attackers can exploit the vulnerabilities while you are in the process of reviewing, prioritizing, and patching all the reported vulnerabilities. Qualys VMDR with TruRisk™ offers risk-based vulnerability management with unique insights into an organization's outlook to prioritize its most critical threats.

Qualys TruRisk is an intelligence-driven vulnerability severity scoring. It detects the location of assets vulnerabilities, including their business and operational criticality, association with business-critical applications, context about the asset's exposure to attack and many more.

Qualys TruRisk Mode in the **Prioritization** tab prioritizes Assets or Vulnerabilities based on risks generated in the result. Perform the following steps to enable Qualys TruRisk™ Mode to provide data for Asset Criticality, Qualys Detection Score (QDS), and Asset Risk Score (ARS):

1. In the **Prioritization** tab click **Reports**.
2. Click **Start Prioritizing**
3. Select at least one Asset tag to display the prioritized list of vulnerabilities associated with the assets.
4. Click  to proceed with Prioritization.
5. In the Asset Tags section, from Include and Exclude menu, select one of the following options:
 - Any: to include or exclude all assets that might have any of the selected tags.
 - All: to include or exclude only those assets which have all the selected tags.
6. Toggle the **Qualys TruRisk™ Mode** to enable it.

By default, the result displays the highest value of Asset Criticality and the Qualys Detection Score.



7. You can select the range of **Asset Criticality** (1-5) using the Asset Criticality bar graph. The highest score is considered if multiple tags are assigned to the asset.

8. You can select the range of Risks (Low-Critical) in the **Qualys Detection Score** (QDS) bar graph. The risk scores generated prioritizes the assets and vulnerabilities.

9. You can select the **Asset Risk Score** (ARS) from the pie chart. ARS helps you prioritize your vulnerabilities based on the risk to your assets and not just the technical severity.

To know the calculation for Asset Criticality, QDS, and ARS, refer [Calculating TruRisk Score](#).

10. Click **Prioritize Now** to enable the threat intelligence to prioritize the riskiest vulnerabilities on your network for the assets you selected.

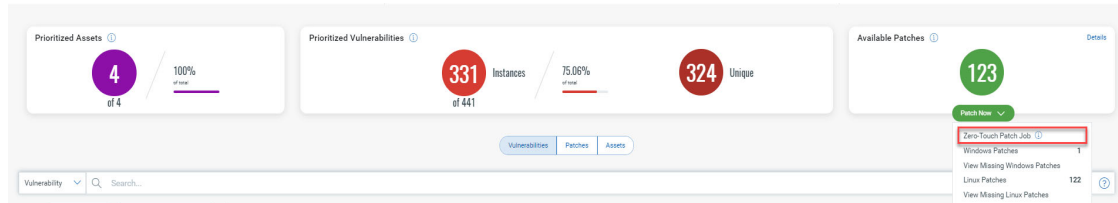
Once you generate the report, you could proceed with patching the vulnerabilities (if Patch Management app is enabled in your subscription), export the report in the form of a widget to your dashboard or download the report in CSV format. To know more refer to [Reading the VMDR Prioritization Report](#)

Reading the VMDR Prioritization Report

Using the VMDR Prioritization Report, you can detect which vulnerabilities to remediate first. The report contains of two sections: Summary and Details.

Summary

The Summary section of the VMDR Prioritization report displays the findings with the following three sections:



Prioritized Assets

Depending on the asset tags that you choose, the assets are identified for this report. Prioritized Assets is the count of assets out of the total assets with vulnerabilities that meet the combination of the detection age, RTIs, and attack vectors you selected.

In the above example, 8 assets matched the selected asset tags. Out of the 8 assets, 2 assets had vulnerabilities that met the combination of the selected detection age, RTIs, and attack surface.

Prioritized Vulnerabilities

The Prioritized Vulnerabilities section displays a summary of prioritized vulnerabilities that are detected on the assets.

Instances: The count indicates the total number of vulnerabilities that meet the combination of the detection age, RTIs, and attack surface you selected.

The count may include multiple occurrences of a single vulnerability (that is a single QID) detected on multiple assets.

In the above example, 154 vulnerabilities were detected on the 8 assets. Out of the 154 vulnerabilities, 8 vulnerabilities met the combination of the selected detection age, RTIs, and attack surface across the 2 assets.

Unique: The count of unique vulnerabilities (excluding duplicate QID instances) out of the vulnerability instances identified/detected.

In the above example, out of the 8 instances, 6 are unique vulnerabilities.

Available Patches

Count of the patches that are available with Qualys. Click Patch Now to initiate the process of patching the vulnerabilities. For more details refer to [Patch Management](#).

Note: The Patch Now button is enabled only when Qualys can automatically patch the vulnerability and the Patch Management app is enabled in your subscription.

Details

The details section includes detailed information about prioritized vulnerabilities, patches and prioritized assets. Use the tabs to toggle between the three views. The Vulnerabilities and Assets tabs offer search capabilities using limited tokens.

Vulnerabilities Patches Assets					
Vulnerability Search...					
Actions (0) Group By: Vulnerability Show Only Patchable 1 - 50 of 83					
CVE	TITLE	QID	QDS	TOTAL HOSTS	AVAILABLE REMEDIATION
CVE-2020-0646 2 more	Microsoft .NET Framework Security Updates for January 20...	91598	100	1	Patch Now
CVE-2021-31969 24 more	Microsoft Windows Security Update for June 2021	91772	100	1	Patch Now
CVE-2019-14287	CentOS Security Update for sudo (CESA-2019:3197)	256727	100	1	Patch Now

Export To Dashboard

You can export the VMDR Prioritization report to dashboard in the form of a widget and continuously monitor the widget to check the vulnerabilities on the prioritized assets.

Here are the steps to export the report to your dashboard.

Note: The Export to Dashboard button is enabled only after you have generated the report.

- 1) On the VMDR Prioritization report, click **Export to Dashboard**.
- 2) Provide a name for the widget.
- 3) Select the Dashboard you want to add the widget to and then click Export.

The widget is added to the dashboard.

Download Reports (CSV format)

You can download the VMDR Prioritization report to your local system in CSV format. The Download button is enabled after you have generated the VMDR Prioritization report.

Note: Missing patches can be downloaded in your report only if you have the Patch Management add-on enabled in your subscription.

- 1) On the VMDR Prioritization report, click **Download**.

- 2) Provide a name and description (optional) for the report.
- 3) Currently only CSV option is supported so it is preselected for you.
- 4) If required, you can change timezones for dates included in report using the Change timezones for dates included in report option. By default, the browser's time zone is used to report dates in the report.
- 5) Click **Download**.

The VMDR Prioritization report is downloaded to your local system in CSV format for future reference.

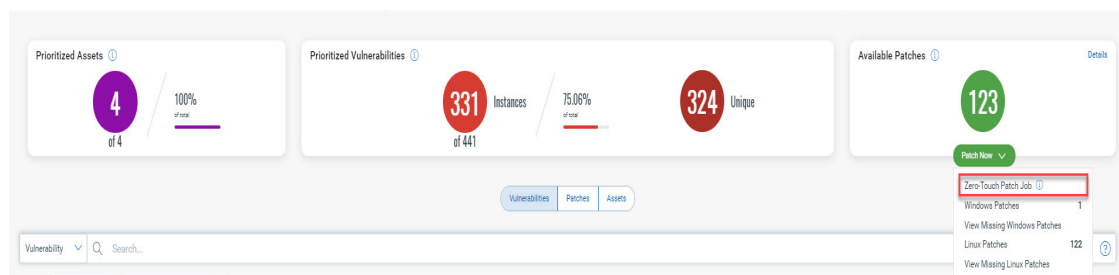
Patch Management

In the VMDR Prioritization report you can view the assets and vulnerabilities that can be patched by Qualys. You can initiate the patching process and patch the vulnerabilities directly from the report.

Note: Deployment of patches is available directly from the VMDR Prioritization report only for customers with the Patch Management add-on.

Patch Vulnerabilities from VMDR Report

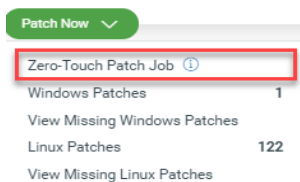
The Summary section of the VMDR Prioritization report displays findings with the following three sections:



The Available Patches widget shows the count of the patches that are available with Qualys. Click Patch Now to initiate the process of patching the vulnerabilities.

Note: The Patch Now button is enabled only when Qualys can automatically patch the vulnerability and the Patch Management app is enabled in your subscription.

To initiate the patching process click the Patch Now button and choose to perform one of the following actions:



Zero Touch Patch Job- Opens the wizard to create an automated job to proactively patch current and future Windows vulnerabilities based on the criteria selected while generating the Prioritization report in the Patch Management app. Follow the instructions in the wizard and initiate the patching process by creating a new job.

Windows Patches- Displays the list of Windows Patches in the Patch Management app.

View Missing Windows Patches - Displays the list of missing Windows patches for the prioritized assets and vulnerabilities. You can view the list of missing patches even with the free version of Patch Management app that is activated for the assets.

CVE-2019-1060 36 more...	Microsoft Windows Security Update for October 2019	91582	1	Patch Now ▾
No CVEs Assigned	Microsoft Windows IcmpSendEcho2Ex Denial of Service Vulnerability - Zero Day	118425	1	Add to New Job Upgrade
CVE-2020-0819 79 more...	Microsoft Windows Security Update for March 2020	91609	1	Add to Existing Job Upgrade
				View Missing Patches

Linux Patches -Displays the list of Windows Patches in the Patch Management app.

View Missing Linux Patches - Displays the list of missing Linux patches for the prioritized assets and vulnerabilities. You can view the list of missing patches even with the free version of Patch Management app that is activated for the assets.

For more information, refer to the [Patch Management online help](#).