



- ⓘ The VMDR Prioritization Report can be used to quickly create patch jobs for high risk vulnerabilities. To begin building a Prioritization Report, from Qualys VMDR, click "**PRIORITIZATION**" at the top of the page.



# 009 - VMDR Prioritization Report

Qualys Cloud Platform

VMDR ▾ DASHBOARD VULNERABILITIES PRIORITIZATION SCANS REPORTS REMEDIATION ASSETS KNOWLEDGEBASE USERS

Hello Qualys!

## Welcome to Qualys VMDR®

Discover, assess, prioritize, and patch critical vulnerabilities in real time and across your global hybrid-IT landscape all from a single solution.

[Learn more](#)



**Identify Assets**  
Continuously discover your IT assets that are on-prem, cloud, mobile, container, applications providing 100% real-time visibility

**Discover Vulnerabilities & Misconfigurations**  
Detect vulnerabilities with six-sigma accuracy and use CIS Benchmarks to uncover misconfigurations

**Prioritize Threats**  
Use real-time threat intelligence and machine learning to prioritize vulnerabilities with the highest risk

**Detect & Deploy Missing Patches**  
Promptly and effortlessly deploy the most relevant superseding patches to remediate prioritized vulnerabilities



[Configure Agents for VMDR](#)

**Find all your IT assets**

Discover, track and normalize asset information, including installed software and packages. Create dynamic tags, leveraging normalized data for grouping assets as and when they show up, based on intuitive rules.

[Manage Tags](#) [Visit Dashboard](#)



## 009 - VMDR Prioritization Report

- ⓘ At the bottom of the page, click the **button labeled with the "plus-sign" symbol**, to begin creating a report.

ⓘ At the bottom of the page, click the **button labeled with the "plus-sign" symbol**, to begin creating a report.



- ⓘ Asset Tags help to add context to the assets, vulnerabilities and patches to be prioritized. For this example, we'll target remote endpoints running the Remote Desktop Protocol (RDP).

The screenshot shows the Qualys Cloud Platform interface for VMDR Prioritization. The main title is "VMDR Prioritization" with the subtitle "Prioritize your riskiest vulnerabilities on the most critical assets, reducing thousands of vulnerabilities to the few hundred that matter". Below this, there's a section titled "Select Asset Tags" with the sub-instruction "Start prioritization by selecting asset tags". A search bar says "Start Adding Asset Tags...". To the right is a large blue "→" button. Below the search bar are several asset tag categories with checkboxes:

- Activation Key (selected)
- Asset Groups
- Business Units
- Cloud Agent
- RDP
- Web App
- Misc.
- OS: Linux
- Network
- Internet Facing...
- OS: Windows



- ⓘ Select the check box for the "RDP" Asset Tag...

The screenshot shows the Qualys Cloud Platform interface for VMDR Prioritization. At the top, it says "VMDR Prioritization" and "Prioritize your riskiest vulnerabilities on the most critical assets, reducing thousands of vulnerabilities to the few hundred that matter". Below this, there's a section titled "Select Asset Tags" with the sub-instruction "Start prioritization by selecting asset tags". A large button labeled "Start Adding Asset Tags..." is present. Below the button is a grid of asset tags, each with a checkbox. The "RDP" tag is highlighted with a blue background and a yellow border, indicating it is selected.

Asset Tag	Status
Activation Key	unchecked
Asset Groups	unchecked
Business Units	unchecked
Cloud Agent	unchecked
RDP	checked
Web App	unchecked
Misc.	unchecked
OS: Linux	unchecked
Network	unchecked
Internet Facing...	unchecked
OS: Windows	unchecked



...and click the "Arrow" to proceed.

The screenshot shows the Qualys Cloud Platform interface for VMDR Prioritization. At the top, it says "VMDR Prioritization" and "Prioritize your riskiest vulnerabilities on the most critical assets, reducing thousands of vulnerabilities to the few hundred that matter". Below this, there's a section titled "Select Asset Tags" with the sub-instruction "Start prioritization by selecting asset tags". A modal window is open, titled "RDP" with an "x" button. It contains a grid of asset tags with checkboxes:

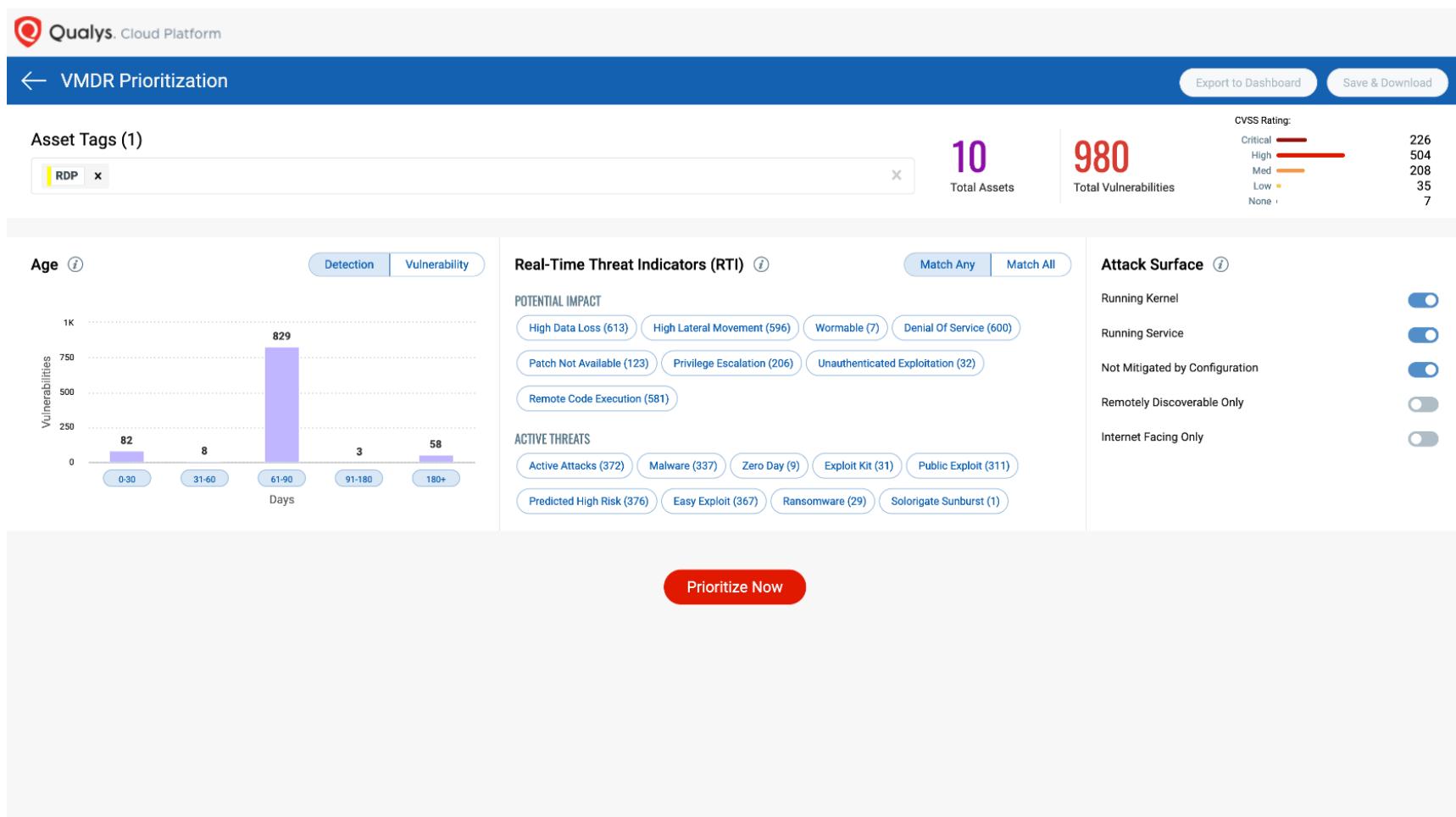
Activation Key	Asset Groups	Business Units	Cloud Agent
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> RDP	<input type="checkbox"/> Web App	<input type="checkbox"/> Misc.	<input type="checkbox"/> OS: Linux
<input type="checkbox"/> Network	<input type="checkbox"/> Internet Facing...	<input type="checkbox"/> OS: Windows	

A red box highlights the "RDP" checkbox. To the right of the modal is a large red arrow pointing right, which is also highlighted with a red box.



## 009 - VMDR Prioritization Report

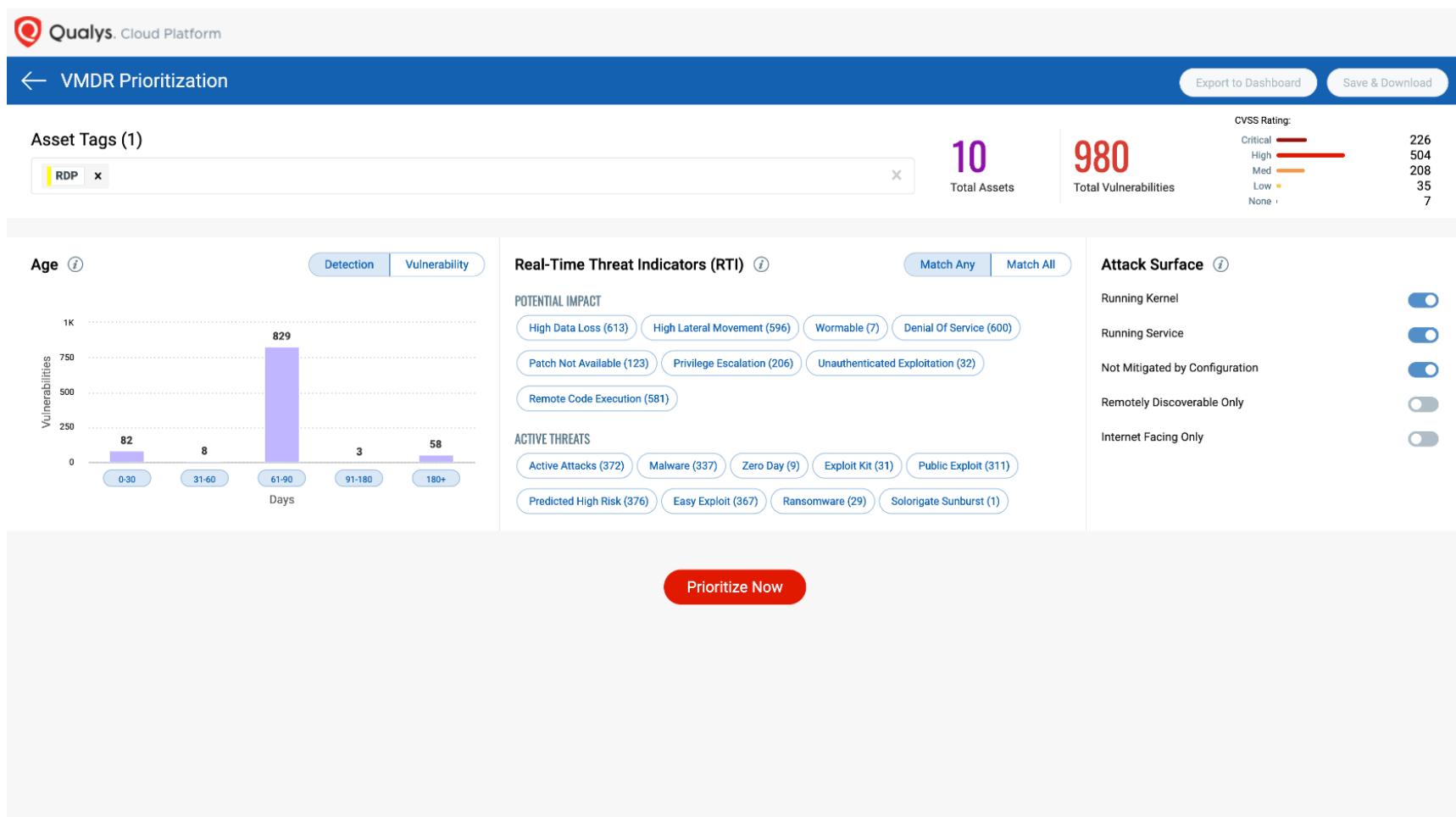
- Once you have selected one or more tags for asset context, the Prioritization Report provides priority options based on vulnerability Age, Real-Time Threat Indicators, and Attack Surface.





## 009 - VMDR Prioritization Report

- ⓘ Initially, the vulnerability "Age" graph, on the left, distributes vulnerabilities by their "Detection" age. This is calculated as the number of days since the vulnerability was discovered by your scans.

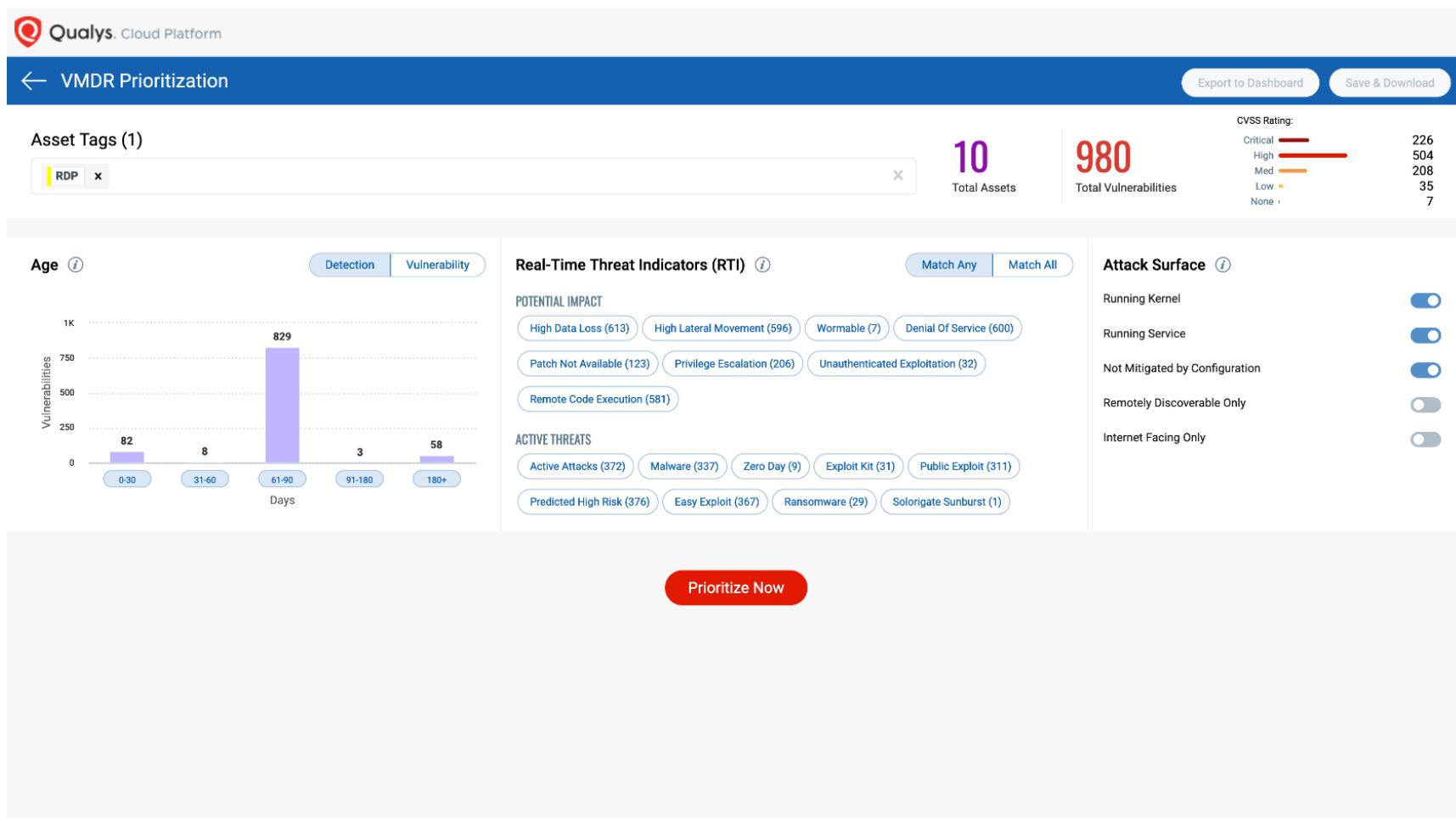




## 009 - VMDR Prioritization Report



The KnowledgeBase age of a vulnerability, identifies the number of days since it was added to the Qualys KnowledgeBase.





## 009 - VMDR Prioritization Report



To group vulnerabilities by their KnowledgeBase age, click the "Vulnerability" option.

Qualys Cloud Platform

← VMDR Prioritization

Asset Tags (1) RDP

10 Total Assets 980 Total Vulnerabilities

CVSS Rating: Critical (226), High (504), Med (208), Low (35), None (7)

Age (i) Detection Vulnerability

Real-Time Threat Indicators (RTI) Match Any Match All

POTENTIAL IMPACT: High Data Loss (613), High Lateral Movement (596), Wormable (7), Denial Of Service (600), Patch Not Available (123), Privilege Escalation (206), Unauthenticated Exploitation (32), Remote Code Execution (581)

ACTIVE THREATS: Active Attacks (372), Malware (337), Zero Day (9), Exploit Kit (31), Public Exploit (311), Predicted High Risk (376), Easy Exploit (367), Ransomware (29), Solorigate Sunburst (1)

Attack Surface (i)

Running Kernel (On), Running Service (On), Not Mitigated by Configuration (On), Remotely Discoverable Only (Off), Internet Facing Only (Off)

Vulnerabilities

Days

0-30: 82, 31-60: 8, 61-90: 829, 91-180: 3, 180+: 58

Prioritize Now



- ⓘ As you can see, displaying vulnerabilities by their KnowledgeBase age provides a much different perspective. Many vulnerabilities that were only recently detected, have been in the Qualys KnowledgeBase for 180 days or longer.



# 009 - VMDR Prioritization Report

Qualys Cloud Platform

← VMDR Prioritization

Asset Tags (1)

RDP x

10 Total Assets

980 Total Vulnerabilities

CVSS Rating:

Critical	High	Med	Low	None
226	504	208	35	7

Age (i)

Vulnerabilities

Days

Real-Time Threat Indicators (RTI) (i)

Match Any Match All

POTENTIAL IMPACT

- High Data Loss (613)
- High Lateral Movement (596)
- Wormable (7)
- Denial Of Service (600)
- Patch Not Available (123)
- Privilege Escalation (206)
- Unauthenticated Exploitation (32)
- Remote Code Execution (581)

ACTIVE THREATS

- Active Attacks (372)
- Malware (337)
- Zero Day (9)
- Exploit Kit (31)
- Public Exploit (311)
- Predicted High Risk (376)
- Easy Exploit (367)
- Ransomware (29)
- Solorigate Sunburst (1)

Attack Surface (i)

Running Kernel

Running Service

Not Mitigated by Configuration

Remotely Discoverable Only

Internet Facing Only

Prioritize Now

This screenshot shows the Qualys Cloud Platform VMDR Prioritization Report. At the top, it displays 'Total Assets' (10) and 'Total Vulnerabilities' (980). Below this, there's a 'CVSS Rating' legend with categories: Critical (226), High (504), Med (208), Low (35), and None (7). The 'Asset Tags' section shows one tag: 'RDP'. The 'Age' chart shows the distribution of vulnerabilities by age: 14 (0-30 days), 12 (31-60 days), 14 (61-90 days), 37 (91-180 days), and 903 (180+ days). The 'Real-Time Threat Indicators (RTI)' section lists potential impacts like High Data Loss, High Lateral Movement, Wormable, Denial Of Service, Patch Not Available, Privilege Escalation, Unauthenticated Exploitation, and Remote Code Execution. It also lists active threats such as Active Attacks, Malware, Zero Day, Exploit Kit, Public Exploit, Predicted High Risk, Easy Exploit, Ransomware, and Solorigate Sunburst. The 'Attack Surface' section includes filters for Running Kernel, Running Service, Not Mitigated by Configuration, Remotely Discoverable Only, and Internet Facing Only. A prominent red button at the bottom right says 'Prioritize Now'.



## 009 - VMDR Prioritization Report

- ⓘ In the middle of the page, Real-Time Threat Indicators, from the Qualys Threat Protection application, can help to single-out vulnerabilities with known or existing threats.

The screenshot shows the Qualys Cloud Platform VMDR Prioritization report. At the top, it displays "Total Assets: 10" and "Total Vulnerabilities: 980". A legend for CVSS Rating shows: Critical (red) 226, High (orange-red) 504, Med (orange) 208, Low (yellow) 35, and None (green) 7. Below this, there are sections for Asset Tags (RDP), Age (Days), and Real-Time Threat Indicators (RTI). The RTI section is highlighted with a red box and contains two main categories: POTENTIAL IMPACT and ACTIVE THREATS, each with a list of threat types and counts. At the bottom right is a "Prioritize Now" button.

**Real-Time Threat Indicators (RTI)**

**POTENTIAL IMPACT**

- High Data Loss (613)
- High Lateral Movement (596)
- Wormable (7)
- Denial Of Service (600)
- Patch Not Available (123)
- Privilege Escalation (206)
- Unauthenticated Exploitation (32)
- Remote Code Execution (581)

**ACTIVE THREATS**

- Active Attacks (372)
- Malware (337)
- Zero Day (9)
- Exploit Kit (31)
- Public Exploit (311)
- Predicted High Risk (376)
- Easy Exploit (367)
- Ransomware (29)
- Solorigate Sunburst (1)



- ⓘ Although any of the threats listed here, can impact a remote endpoint, we are especially interested in the "Malware" and Ransomware categories. Both types of threat indicators will significantly impact remote endpoint hosts.



# 009 - VMDR Prioritization Report

Qualys Cloud Platform

← VMDR Prioritization

Asset Tags (1)

RDP x

10 Total Assets

980 Total Vulnerabilities

CVSS Rating:

Critical	High	Med	Low	None
226	504	208	35	7

Age i

Vulnerabilities

Days

Real-Time Threat Indicators (RTI) i

Match Any Match All

POTENTIAL IMPACT

- High Data Loss (613)
- High Lateral Movement (596)
- Wormable (7)
- Denial Of Service (600)
- Patch Not Available (123)
- Privilege Escalation (206)
- Unauthenticated Exploitation (32)
- Remote Code Execution (581)

ACTIVE THREATS

- Active Attacks (372)
- Malware (337)
- Zero Day (9)
- Exploit Kit (31)
- Public Exploit (311)
- Predicted High Risk (376)
- Easy Exploit (367)
- Ransomware (29)
- Solorigate Sunburst (1)

Attack Surface i

Running Kernel on

Running Service on

Not Mitigated by Configuration on

Remotely Discoverable Only off

Internet Facing Only off

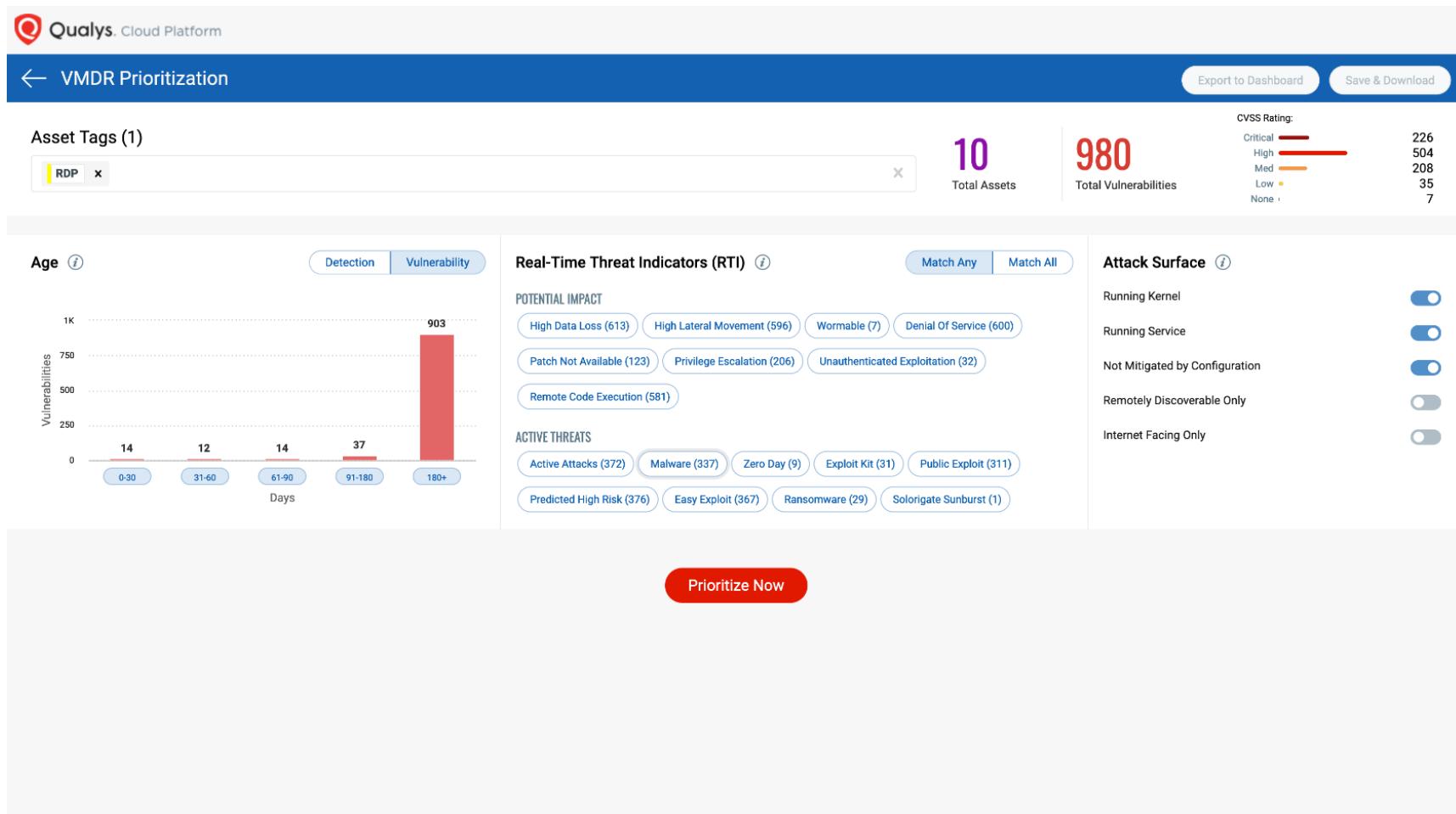
Prioritize Now

This screenshot shows the Qualys Cloud Platform VMDR Prioritization Report. At the top, it displays 'Total Assets' (10) and 'Total Vulnerabilities' (980). Below this, there's a 'CVSS Rating' legend with categories: Critical (226), High (504), Med (208), Low (35), and None (7). The 'Asset Tags' section shows one tag: 'RDP'. The 'Age' chart shows the distribution of vulnerabilities by age: 14 (0-30 days), 12 (31-60 days), 14 (61-90 days), 37 (91-180 days), and 903 (180+ days). The 'Real-Time Threat Indicators (RTI)' section lists potential impacts like High Data Loss (613) and Active Threats like Active Attacks (372). The 'Attack Surface' section includes filters for Running Kernel, Running Service, Not Mitigated by Configuration, Remotely Discoverable Only, and Internet Facing Only.



## 009 - VMDR Prioritization Report

- Under the ACTIVE THREATS section, of Real-Time Threat Indicators, select **Malware**.





## 009 - VMDR Prioritization Report

- Under the same section, select **Ransomware**.

Qualys Cloud Platform

← VMDR Prioritization

Asset Tags (1) RDP x

10 Total Assets 980 Total Vulnerabilities

CVSS Rating:  
Critical (226)  
High (504)  
Med (208)  
Low (35)  
None (7)

**Age** Detection Vulnerability

Vulnerabilities

1K  
750  
500  
250  
0

14 12 14 37 903

Days

0-30 31-60 61-90 91-180 180+

**Real-Time Threat Indicators (RTI)** Match Any Match All

POTENTIAL IMPACT

High Data Loss (613) High Lateral Movement (596) Wormable (7) Denial Of Service (600)  
Patch Not Available (123) Privilege Escalation (206) Unauthenticated Exploitation (32)  
Remote Code Execution (581)

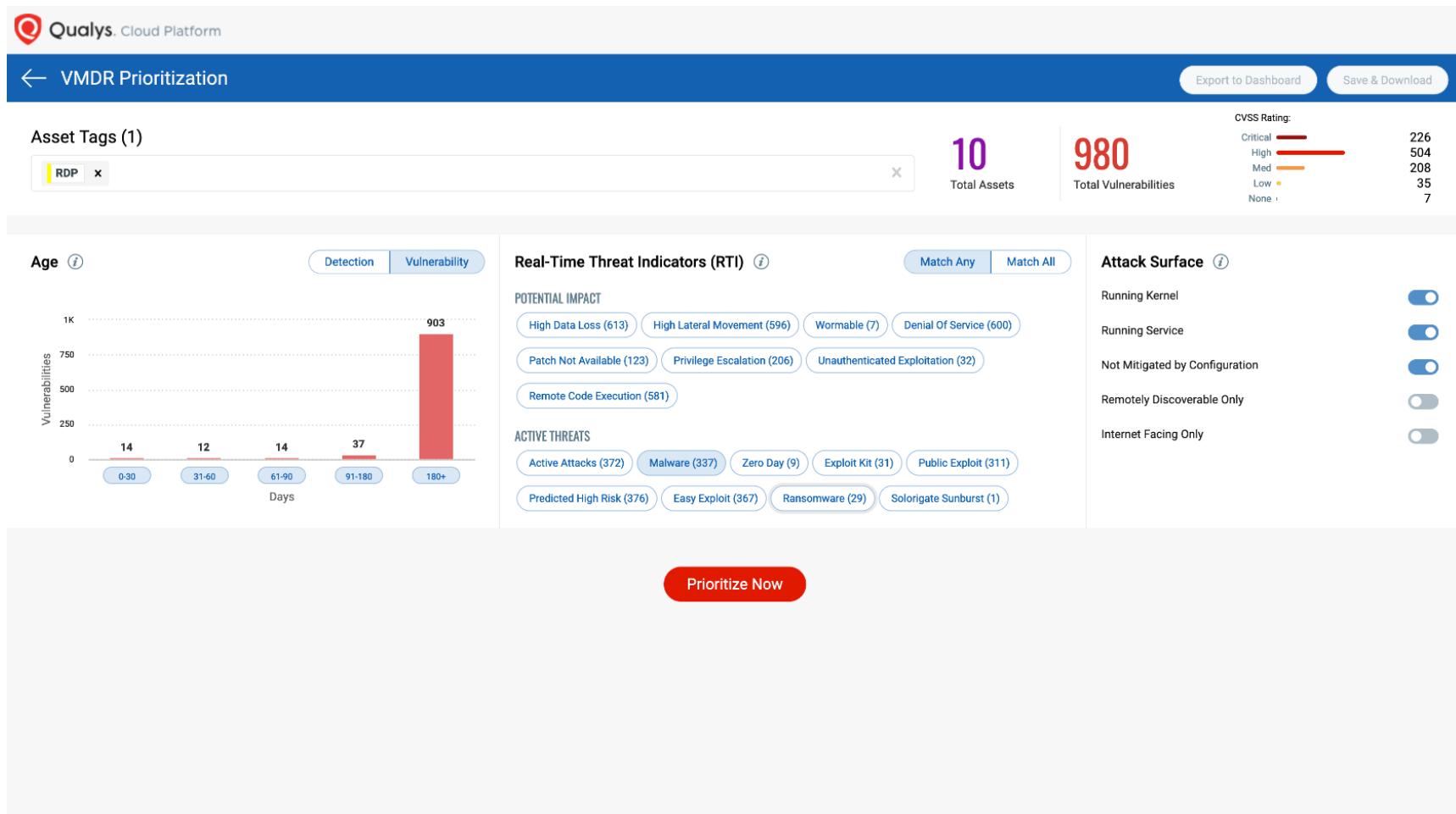
ACTIVE THREATS

Active Attacks (372) Malware (337) Zero Day (9) Exploit Kit (31) Public Exploit (311)  
Predicted High Risk (376) Easy Exploit (367) Ransomware (29) Solorigate Sunburst (1)

**Attack Surface** i

Running Kernel (On)  
Running Service (On)  
Not Mitigated by Configuration (On)  
Remotely Discoverable Only (Off)  
Internet Facing Only (Off)

Prioritize Now





## 009 - VMDR Prioritization Report



We'll leave the "Match Any" operator selected, to include hosts that have either type of vulnerability (those that are targeted by Malware or Ransomware).

The screenshot shows the Qualys Cloud Platform VMDR Prioritization Report. At the top, it displays "Total Assets: 10" and "Total Vulnerabilities: 980". A legend for CVSS Rating shows: Critical (red bar), High (orange bar), Med (yellow bar), Low (light blue bar), and None (green bar). Below this, there are sections for Asset Tags (RDP), Real-Time Threat Indicators (RTI), and Attack Surface.

**Real-Time Threat Indicators (RTI) section:**

- Match Operator:** Match Any (selected, highlighted with a red box)
- POTENTIAL IMPACT:** High Data Loss (613), High Lateral Movement (596), Wormable (7), Denial Of Service (600), Patch Not Available (123), Privilege Escalation (206), Unauthenticated Exploitation (32), Remote Code Execution (581).
- ACTIVE THREATS:** Active Attacks (372), Malware (337), Zero Day (9), Exploit Kit (31), Public Exploit (311), Predicted High Risk (376), Easy Exploit (367), Ransomware (29), Solorigate Sunburst (1).

**Attack Surface section:**

- Running Kernel (switch off)
- Running Service (switch off)
- Not Mitigated by Configuration (switch off)
- Remotely Discoverable Only (switch off)
- Internet Facing Only (switch off)

**Bottom right:** A large red button labeled "Prioritize Now".



## 009 - VMDR Prioritization Report

- ⓘ On the right, the "Attack Surface" options can help to add even more asset context to this report.

Qualys Cloud Platform

← VMDR Prioritization

Asset Tags (1)

RDP

10 Total Assets

980 Total Vulnerabilities

CVSS Rating:

Critical	High	Med	Low	None
226	504	208	35	7

Age (i)

Detection Vulnerability

Real-Time Threat Indicators (RTI) (i)

Match Any Match All

POTENTIAL IMPACT

- High Data Loss (613)
- High Lateral Movement (596)
- Wormable (7)
- Denial Of Service (600)
- Patch Not Available (123)
- Privilege Escalation (206)
- Unauthenticated Exploitation (32)
- Remote Code Execution (581)

ACTIVE THREATS

- Active Attacks (372)
- Malware (337)
- Zero Day (9)
- Exploit Kit (31)
- Public Exploit (311)
- Predicted High Risk (376)
- Easy Exploit (367)
- Ransomware (29)
- Solorigate Sunburst (1)

Attack Surface (i)

Running Kernel

Running Service

Not Mitigated by Configuration

Remotely Discoverable Only

Internet Facing Only

Prioritize Now

The 'Attack Surface' section is highlighted with a red border.



## 009 - VMDR Prioritization Report

- ⓘ Leave the "Attack Surface" options at their default settings and click **Prioritize Now**.

Qualys Cloud Platform

← VMDR Prioritization

Export to Dashboard | Save & Download

Asset Tags (1)  
RDP

10 Total Assets | 980 Total Vulnerabilities

CVSS Rating:  
Critical (226) | High (504) | Med (208) | Low (35) | None (7)

Age (i)  
Detection | Vulnerability

Vulnerabilities  
1K  
750  
500  
250  
0

Days  
0-30 (14) | 31-60 (12) | 61-90 (14) | 91-180 (37) | 180+ (903)

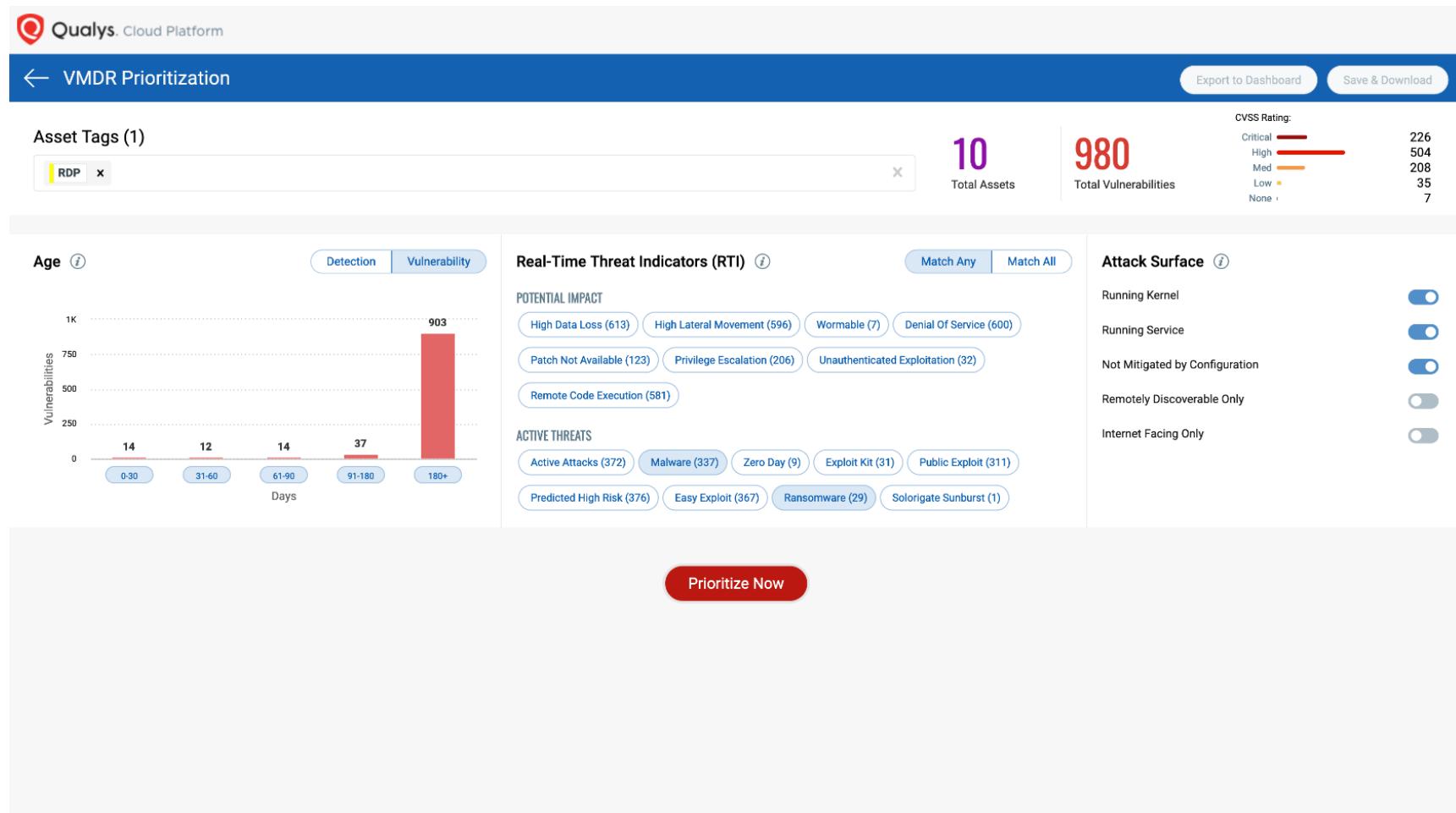
Real-Time Threat Indicators (RTI) (i)  
Match Any | Match All

POTENTIAL IMPACT  
High Data Loss (613) | High Lateral Movement (596) | Wormable (7) | Denial Of Service (600)  
Patch Not Available (123) | Privilege Escalation (206) | Unauthenticated Exploitation (32)  
Remote Code Execution (581)

ACTIVE THREATS  
Active Attacks (372) | Malware (337) | Zero Day (9) | Exploit Kit (31) | Public Exploit (311)  
Predicted High Risk (376) | Easy Exploit (367) | Ransomware (29) | Solorigate Sunburst (1)

Attack Surface (i)  
Running Kernel (On) | Running Service (On) | Not Mitigated by Configuration (On) | Remotely Discoverable Only (Off) | Internet Facing Only (Off)

Prioritize Now





## 009 - VMDR Prioritization Report

- ⓘ The priority options are applied and all affected vulnerabilities are listed. Changing any of the priority options, will immediately update the list of displayed vulnerabilities, patches, and assets.

The screenshot shows the Qualys Cloud Platform VMDR Prioritization report. At the top, there are three summary cards: 'Prioritized Assets' (8 of 10, 80% of total), 'Prioritized Vulnerabilities' (337 Instances of 980, 34.39% of total), and 'Available Patches' (202 Unique). Below these are tabs for 'Vulnerabilities' (selected), 'Patches', and 'Assets'. The main table lists vulnerabilities grouped by title, showing QID, total hosts, and a 'Patch Now' button for each. The table includes rows for Microsoft Windows Security Updates for August, October, and November 2020, as well as a Microsoft Windows Kernel Privilege Escalation Vulnerability and a Microsoft Splwow64 Windows Elevation of Privilege Vulnerability.

CVE	TITLE	QID	TOTAL HOSTS	Patch Now
CVE-2020-1509 [87 more]	Microsoft Windows Security Update for August 2020	91668	5	Patch Now ▾
CVE-2020-16939 [51 more]	Microsoft Windows Security Update for October 2020	91683	5	Patch Now ▾
CVE-2020-17087	Microsoft Windows Kernel Privilege Escalation Vulnerability	91690	5	Patch Now ▾
CVE-2020-17071 [53 more]	Microsoft Windows Security Update for November 2020	91691	5	Patch Now ▾
CVE-2020-17008 [1 more]	Microsoft Splwow64 Windows Elevation of Privilege Vulnerability	91709	5	Patch Now ▾



## 009 - VMDR Prioritization Report

ⓘ Presently, 202 unique vulnerabilities are listed.

The screenshot shows the Qualys Cloud Platform VMDR Prioritization interface. At the top, there are three summary boxes: 'Prioritized Assets' (8 of 10, 80% of total), 'Prioritized Vulnerabilities' (337 Instances of 980, 34.39% of total), and 'Available Patches' (7). Below these are tabs for 'Vulnerabilities' (selected), 'Patches', and 'Assets'. A search bar at the top says 'Search...'. The main table lists 202 vulnerabilities, with the first five rows shown:

CVE	TITLE	QID	TOTAL HOSTS
CVE-2020-1509 [87 more]	Microsoft Windows Security Update for August 2020	91668	5
CVE-2020-1693 [51 more]	Microsoft Windows Security Update for October 2020	91683	5
CVE-2020-17087	Microsoft Windows Kernel Privilege Escalation Vulnerability	91690	5
CVE-2020-17071 [53 more]	Microsoft Windows Security Update for November 2020	91691	5
CVE-2020-17008 [1 more]	Microsoft Splwow64 Windows Elevation of Privilege Vulnerability	91709	5



## 009 - VMDR Prioritization Report

- ① Click the toggle-switch to "Show Only Patchable" vulnerabilities.

The screenshot shows the Qualys Cloud Platform VMDR Prioritization interface. At the top, there are three summary cards: 'Prioritized Assets' (8 of 10, 80% of total), 'Prioritized Vulnerabilities' (337 Instances of 980, 34.39% of total), and 'Available Patches' (202 Unique). Below these are tabs for 'Vulnerabilities', 'Patches', and 'Assets'. The main table lists vulnerabilities, grouped by title, with columns for CVE, Title, QID, and Total Hosts. Each row includes a 'Patch Now' button. A red box highlights the 'Show Only Patchable' toggle switch in the search bar.

CVE	TITLE	QID	TOTAL HOSTS
CVE-2020-1509 [87 more]	Microsoft Windows Security Update for August 2020	91668	5
CVE-2020-1693 [51 more]	Microsoft Windows Security Update for October 2020	91683	5
CVE-2020-17087	Microsoft Windows Kernel Privilege Escalation Vulnerability	91690	5
CVE-2020-17071 [53 more]	Microsoft Windows Security Update for November 2020	91691	5
CVE-2020-17008 [1 more]	Microsoft Splwow64 Windows Elevation of Privilege Vulnerability	91709	5



- ⓘ The report is now updated to display only vulnerabilities that are "Qualys Patchable." These vulnerabilities were discovered on hosts running the Qualys Cloud Agent and the Patch Management module has been activated.



# 009 - VMDR Prioritization Report

Qualys Cloud Platform

## VMDR Prioritization

Export to Dashboard | Save & Download

Prioritized Assets: 8 of 10 (80% of total)

Prioritized Vulnerabilities: 337 Instances of 980 (34.39% of total)

Available Patches: 202 Unique

Available Patches: 7

Vulnerability ▾ Search... ▾

Actions (0) ▾ Group By: Vulnerability ▾ Show Only Patchable 1 - 16 of 16

CVE	TITLE	QID	TOTAL HOSTS
CVE-2017-5753 [2 more]	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown)	91426	3
CVE-2020-1509 [87 more]	Microsoft Windows Security Update for August 2020	91668	2
CVE-2020-16939 [51 more]	Microsoft Windows Security Update for October 2020	91683	2
CVE-2020-17087	Microsoft Windows Kernel Privilege Escalation Vulnerability	91690	2
CVE-2020-17071 [53 more]	Microsoft Windows Security Update for November 2020	91691	2



## 009 - VMDR Prioritization Report

ⓘ Patches can be individually added to a new or existing patch job...

The screenshot shows the Qualys VMDR Prioritization Report interface. At the top, there are three summary cards: 'Prioritized Assets' (8 of 10, 80% of total), 'Prioritized Vulnerabilities' (337 Instances of 980, 34.39% of total), and 'Available Patches' (202 Unique). Below these are tabs for 'Vulnerabilities' (selected), 'Patches', and 'Assets'. The main area displays a table of vulnerabilities with columns for CVE, Title, QID, Total Hosts, and a 'Patch Now' button. A red box highlights the 'Patch Now' buttons for the first five rows.

CVE	TITLE	QID	TOTAL HOSTS	Patch Now
CVE-2017-5753	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown)	91426	3	Patch Now
CVE-2020-1509	Microsoft Windows Security Update for August 2020	91668	2	Patch Now
CVE-2020-16939	Microsoft Windows Security Update for October 2020	91683	2	Patch Now
CVE-2020-17087	Microsoft Windows Kernel Privilege Escalation Vulnerability	91690	2	Patch Now
CVE-2020-17071	Microsoft Windows Security Update for November 2020	91691	2	Patch Now



## 009 - VMDR Prioritization Report

...or you can deploy all available patches together. Later in this course, you'll perform another lab tutorial that will walk you through the steps to build a Patch Deployment Job.

The screenshot shows the Qualys Cloud Platform VMDR Prioritization interface. At the top, there are three summary cards: 'Prioritized Assets' (8 of 10, 80% of total), 'Prioritized Vulnerabilities' (337 Instances of 980, 34.39% of total), and 'Available Patches' (7 Unique). The 'Available Patches' card is highlighted with a red border. Below these cards is a navigation bar with tabs for 'Vulnerabilities', 'Patches' (which is selected), and 'Assets'. The main content area displays a table of vulnerabilities with the following data:

CVE	TITLE	QID	TOTAL HOSTS	ACTION
CVE-2017-5753 [2 more]	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown)	91426	3	Patch Now ▾
CVE-2020-1509 [87 more]	Microsoft Windows Security Update for August 2020	91668	2	Patch Now ▾
CVE-2020-16939 [51 more]	Microsoft Windows Security Update for October 2020	91683	2	Patch Now ▾
CVE-2020-17087	Microsoft Windows Kernel Privilege Escalation Vulnerability	91690	2	Patch Now ▾
CVE-2020-17071 [53 more]	Microsoft Windows Security Update for November 2020	91691	2	Patch Now ▾



## 009 - VMDR Prioritization Report

- ⓘ Any Prioritization Report can be exported to an existing dashboard as a widget. In the upper-right corner of this report, click the "Export to Dashboard" button.

The screenshot shows the Qualys Cloud Platform VMDR Prioritization Report. At the top, there are three summary cards: 'Prioritized Assets' (8 of 10, 80% of total), 'Prioritized Vulnerabilities' (337 Instances of 980, 34.39% of total), and 'Available Patches' (202 Unique). Below these are tabs for 'Vulnerabilities' (selected), 'Patches', and 'Assets'. The main table lists 16 vulnerabilities, each with a 'Patch Now' button. The columns are: CVE, TITLE, QID, and TOTAL HOSTS.

CVE	TITLE	QID	TOTAL HOSTS
CVE-2017-5753 [2 more]	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown)	91426	3
CVE-2020-1509 [87 more]	Microsoft Windows Security Update for August 2020	91668	2
CVE-2020-16939 [51 more]	Microsoft Windows Security Update for October 2020	91683	2
CVE-2020-17087	Microsoft Windows Kernel Privilege Escalation Vulnerability	91690	2
CVE-2020-17071 [53 more]	Microsoft Windows Security Update for November 2020	91691	2



## 009 - VMDR Prioritization Report



We'll add the Prioritization Report widget, to the VMDR Lab Dashboard, created earlier.

The screenshot shows the Qualys Cloud Platform interface for the VMDR Prioritization report. In the background, there are three main summary cards: 'Prioritized Assets' (8 of 10, 80% of total), 'Prioritized Vulnerabilities' (337 Instances of 980, 34.39% of total), and 'Available Patches' (202 Unique). Below these are sections for 'Vulnerability' and 'CVE' lists. A modal dialog box is overlaid on the page, titled 'Export to Dashboard', with instructions: 'This will export the report as a widget in the selected dashboard.' It has two required input fields: 'Name \*' and 'Select Dashboard \*'. The 'Select Dashboard \*' field is currently set to 'Please Select Dashboard'. At the bottom of the dialog are 'Cancel' and 'Export' buttons.



## 009 - VMDR Prioritization Report

- ⓘ With a name provided and the target dashboard selected, click the "Export" button.

The screenshot shows the Qualys Cloud Platform interface for the VMDR Prioritization report. In the center, a modal dialog box titled "Export to Dashboard" is displayed. It contains fields for "Name" (set to "VMDR Prioritization Report") and "Select Dashboard" (set to "VMDR Lab Dashboard"). At the bottom of the dialog are "Cancel" and "Export" buttons. The background shows summary statistics: 8 prioritized assets (8 of 10), 337 prioritized vulnerabilities (34.39% of total instances), and 202 unique available patches. Below these are lists of vulnerabilities and their titles, such as Microsoft Windows Security Update for October 2020 and Microsoft Windows Kernel Privilege Escalation Vulnerability. A table on the right lists QID, TOTAL HOSTS, and patching options for various items.

QID	TOTAL HOSTS	
91426	3	Patch Now ▾
91668	2	Patch Now ▾
91683	2	Patch Now ▾
91690	2	Patch Now ▾
91691	2	Patch Now ▾



## 009 - VMDR Prioritization Report



To see the results, click the navigation arrow to leave this report...

Qualys Cloud Platform

VMDR Prioritization

Export to Dashboard | Save & Download

Prioritized Assets: 8 of 10 (80% of total)

Prioritized Vulnerabilities: 337 Instances of 980 (34.39% of total)

Available Patches: 202 Unique

Details | Patch Now

Vulnerability Search: Search...

Actions (0) | Group By: Vulnerability | Show Only Patchable | 1 - 16 of 16 | Filter | Settings

CVE	TITLE	QID	TOTAL HOSTS
CVE-2017-5753 [2 more]	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown)	91426	3
CVE-2020-1509 [87 more]	Microsoft Windows Security Update for August 2020	91668	2
CVE-2020-16939 [51 more]	Microsoft Windows Security Update for October 2020	91683	2
CVE-2020-17087	Microsoft Windows Kernel Privilege Escalation Vulnerability	91690	2
CVE-2020-17071 [53 more]	Microsoft Windows Security Update for November 2020	91691	2



## 009 - VMDR Prioritization Report

ⓘ ...and click DASHBOARD at the top of the page.

The screenshot shows the Qualys Cloud Platform VMDR interface. At the top, there's a navigation bar with the Qualys logo and the text "Qualys Cloud Platform". Below it, a secondary navigation bar has "VMDR" with a dropdown arrow, followed by tabs for "DASHBOARD", "VULNERABILITIES", "PRIORITY", "SCANS", "REPORTS", "REMEDIATION", "ASSETS", "KNOWLEDGEBASE", and "USERS". On the far right of this bar are icons for user profile, help, and email. Below these bars is a blue header bar with three tabs: "Prioritization" (which is selected), "Reports", and "Threat Feed". The main content area features a large blue icon of a pie chart inside a monitor. Below the icon, the text "Welcome to VMDR Prioritization" is centered, followed by a descriptive subtitle: "Prioritize your remediation activities by adding threat intelligence and asset context to your vulnerabilities".



### Welcome to VMDR Prioritization

Prioritize your remediation activities by adding threat intelligence and asset context to your vulnerabilities





## 009 - VMDR Prioritization Report

- Once added to a dashboard, a "Prioritization Report" widget will be dynamically updated as conditions change. Clicking on this widget will reproduce the report from which it was created, automatically.

The screenshot shows the Qualys Cloud Platform interface with the VMDR Lab Dashboard selected. A red box highlights the 'VMDR PRIORITIZATION REPORT' section. The dashboard includes a large red callout for 'VULNERABILITIES 180+ DAYS OLD' with the value '2.25K' and a comparison 'vs 2.41K (93.41%)'. The 'VMDR PRIORITIZATION REPORT' section contains the following data:

Prioritized Assets	Prioritized Vulnerabilities	Available Patches
8 of 10	Instances 337 of 980 (34.39%)	Unique 202
80%	34.39%	7



- ⓘ This concludes the "VMDR Prioritization Report" tutorial. Close this window and continue to read through your Lab Tutorial Supplement, for a review of the steps you just completed, and some additional details.



## 009 - VMDR Prioritization Report

Qualys Cloud Platform

VMDR ▾ DASHBOARD VULNERABILITIES PRIORITIZATION SCANS REPORTS REMEDIATION ASSETS KNOWLEDGEBASE USERS

VMDR Lab Dashboard ▾

Last 30 Days ▾ ⓘ

+ ⏪ ⏴ ⏵ ⚙️

VULNERABILITIES 180+ DAYS OLD

2.25K  
vs  
2.41K (93.41%)

VMDR PRIORITIZATION REPORT

Prioritized Assets	Prioritized Vulnerabilities	Available Patches
8 of 10   80%	Instances 337 of 980   34.39% Unique 202	7

The screenshot shows the Qualys VMDR Cloud Platform interface. At the top, there's a navigation bar with links for DASHBOARD, VULNERABILITIES, PRIORITIZATION, SCANS, REPORTS, REMEDIATION, ASSETS, KNOWLEDGEBASE, and USERS. Below the navigation is a blue header bar for 'VMDR Lab Dashboard'. On the left, a large red box displays the count of vulnerabilities 180+ days old: '2.25K' (vs 2.41K, 93.41%). To the right, a white box titled 'VMDR PRIORITIZATION REPORT' contains three columns: 'Prioritized Assets' (8 of 10, 80%), 'Prioritized Vulnerabilities' (Instances 337 of 980, 34.39%, Unique 202), and 'Available Patches' (7). The bottom half of the screen is mostly blank.



## 009 - VMDR Prioritization Report



Scan to go to the interactive player