



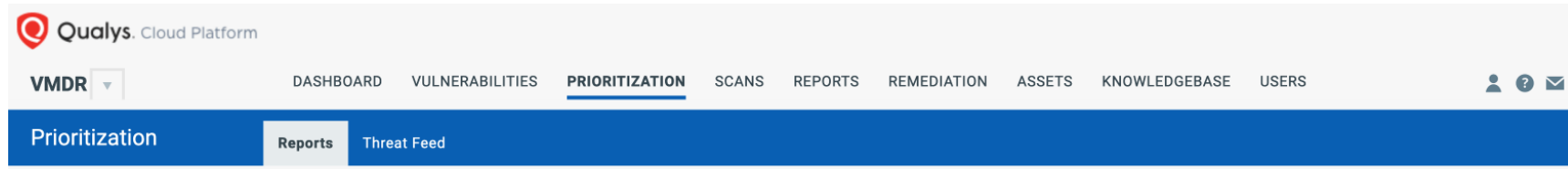
010 - Prioritization Report Use-Case: Databases



In this tutorial, we'll build a Prioritization Report that targets "High Data Loss" vulnerabilities on Database Servers. To get started we'll first need to create an Asset Tag that identifies hosts with database applications.



010 - Prioritization Report Use-Case: Databases



Welcome to VMDR Prioritization

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

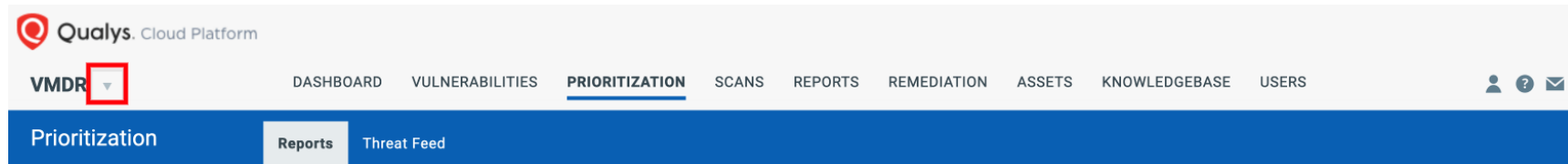




010 - Prioritization Report Use-Case: Databases



To create the "Databases" Asset Tag, click to open the application menu...



Welcome to VMDR Prioritization

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





010 - Prioritization Report Use-Case: Databases



...and select **CyberSecurity Asset Management**.

Qualys. Cloud Platform

VMDR ▾ DASHBOARD VULNERABILITIES **PRIORITIZATION** SCANS REPORTS REMEDIATION ASSETS KNOWLEDGEBASE USERS

CV Monitor changes on cloud platforms

ICS **Industrial Control System BETA**
Get real time visibility of critical industrial assets and manage their vulnerabilities.

ASSET MANAGEMENT (3)

CSAM **CyberSecurity Asset Management**
Identify security gaps and manage asset health across your hybrid IT environment

GAV **Global AssetView**
Maintain full, instant visibility of all your global IT assets (Formerly Global IT Asset Inventory)

AV **AssetView (Legacy)**
Discover assets and use dynamic tags to keep your assets automatically organized.

IT OPERATIONS (2)

PM **Patch Management**
Deploy patches to your systems

SAC **Secure Access Control BETA**
Network containment for your vulnerable, affected and non-compliant assets

SECURITY OPERATIONS (2)

EDR **Endpoint Detection and Response**
Malware Detection, Threat Hunting, Incident Investigation and Response

XDR **XDR**
Next-Gen Incident Response Beyond EDR with Security Analytics, User Behavioral Analytics (UBA) and Threat Hunting

Welcome to VMDR Prioritization

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

+



010 - Prioritization Report Use-Case: Databases



From the CyberSecurity Asset Management application, click **TAGS** (at the top of the page).

Qualys. Cloud Platform

CyberSecurity Asset Management ▾

HOME DASHBOARD INVENTORY **TAGS** RULES RESPONSES REPORTS

Hello Qualys

Welcome to CyberSecurity Asset Management

Identify all systems comprehensively, detect at-risk assets, and respond with appropriate actions to mitigate risk.

Discover and Inventory
Use multiple Qualys sensors, including cloud agent to gain comprehensive asset inventory. Enrich it with business context from CMDB sync.

Detect and Monitor
Detect software and hardware end of life, monitor unauthorized and missing required software.

Report and Respond
Define alerts, uninstall unauthorized software and produce compliance reports.

Your Asset Inventory At-A-Glance
Dive into asset inventory to get detailed insights



010 - Prioritization Report Use-Case: Databases



Just below the "Search" field, click the "Create Tag" button.

Qualys. Cloud Platform

CyberSecurity Asset Management

HOME DASHBOARD INVENTORY **TAGS** RULES RESPONSES REPORTS

Tags

Search for tags...

Actions (0) Create Tag Filters

	NAME	CRITICALITY	CREATED ON	MODIFIED ON
★	Static		Aug 27, 2021	Aug 27, 2021
★	Unmanaged		Jul 19, 2021	Jul 19, 2021
★	Passive Sensor		Jun 28, 2021	Jun 28, 2021
★	3QID90044&QID90080		Jun 07, 2021	Jun 07, 2021
★	2QID&QID&QID&QID		Jun 07, 2021	Jun 07, 2021
★	1QID&QID		Jun 07, 2021	Jun 07, 2021
★ ▶	BCC_SME		Apr 26, 2021	Apr 26, 2021
★ ▶	Test1_238	5	Apr 22, 2021	Sep 02, 2021
★ ▶	Test Set		Apr 12, 2021	Apr 12, 2021



010 - Prioritization Report Use-Case: Databases



We'll provide a Name and Description for this tag.

Qualys. Cloud Platform

← Create New

Basic Details

Start with providing the following information to create your tag

Name *

☐ Mark as Favourite

Description

Add a brief description for this rule

Asset Criticality Score

This score represents the criticality of the asset to your business infrastructure.

Tag Properties

Configure properties for your tag

Set Tag Color

Select Parent Tag

For this new tag, you can select an existing tag to set as a parent tag or you can create a new parent tag. If this is a root tag, then



010 - Prioritization Report Use-Case: Databases



We'll now scroll-down to the bottom of the tag editor.

Qualys. Cloud Platform

[← Create New](#)

Basic Details

Start with providing the following information to create your tag

Name *

☐ Mark as Favourite

Description

Asset Criticality Score

This score represents the criticality of the asset to your business infrastructure.

Tag Properties

Configure properties for your tag

Set Tag Color

Select Parent Tag

For this new tag, you can select an existing tag to set as a parent tag or you can create a new parent tag. If this is a root tag, then



010 - Prioritization Report Use-Case: Databases



Click to select the "Dynamic" radio button (under Tag Type).

Qualys. Cloud Platform

[← Create New](#)

Asset Criticality Score

This score represents the criticality of the asset to your business infrastructure.

☐

Tag Properties

Configure properties for your tag

Set Tag Color ☐

Select Parent Tag
For this new tag, you can select an existing tag to set as a parent tag or you can create a new parent tag. If this is a root tag, then ignore this selection.
[Create Tag](#)

Tag Type

☒ Static ☐ Dynamic

Cancel

Create



010 - Prioritization Report Use-Case: Databases



Under Tag Rules, click to open the "Rule" drop-down menu...

Qualys. Cloud Platform

[← Create New](#)

Tag Properties

Configure properties for your tag

Set Tag Color ☐ ▼

Select Parent Tag

For this new tag, you can select an existing tag to set as a parent tag or you can create a new parent tag. If this is a root tag, then ignore this selection.

[Create Tag](#)

Tag Type

☐ Static ☒ Dynamic

Tag Rules

Rule *

No Dynamic Rule

Cancel

Create



010 - Prioritization Report Use-Case: Databases



...and select the "Asset Inventory" rule engine.

Qualys. Cloud Platform

← Create New

Tag Properties

Configure properties for your tag

Set Tag Color ☐ ▼

Select Parent Tag

For this new tag, you can select an existing tag to set as a parent tag or you can create a new parent tag. If this is a root tag, then ignore this selection.

No Dynamic Rule

Asset Name Contains

Asset Inventory

IP Address In Range(s)

IP Address In Range(s) + Network(s)

Open Ports

Cloud Asset Search

Vuln(OID) Exist

No Dynamic Rule

Tag

Cancel Create



010 - Prioritization Report Use-Case: Databases



With the "Asset Inventory" rule selected, we'll provide an appropriate query.

Qualys. Cloud Platform

[← Create New](#)

Tag Type

☐ Static ☒ Dynamic

Tag Rules

Rule *

Asset Inventory

Query *

Type your query...

Test Rule Applicability on selected assets
Select assets to test if the defined dynamic rule is applied accurately

+

Test Applicability

☐ **Evaluate Rule on Creation**
You have already scanned a number of assets and they need to be re-evaluated for tag assignment.



010 - Prioritization Report Use-Case: Databases



The first condition in this query uses the software category1 token to identify hosts with database applications.

Qualys. Cloud Platform

← Create New

Tag Type

☐ Static ☒ Dynamic

Tag Rules

Rule *

Asset Inventory

Query *

software:(category1:Databases) and not software:(category2:'Client Tools')

Test Rule Applicability on selected assets
Select assets to test if the defined dynamic rule is applied accurately

Test Applicability

☐ **Evaluate Rule on Creation**
You have already scanned a number of assets and they need to be re-evaluated for tag assignment.



010 - Prioritization Report Use-Case: Databases



The second condition in this query, uses the software category2 token, to exclude "client-side" tools.

Qualys. Cloud Platform

[← Create New](#)

Tag Type

☐ Static ☒ Dynamic

Tag Rules

Rule *

Asset Inventory

Query *

software:(category1:Databases) and not software:(category2:'Client Tools')

Test Rule Applicability on selected assets
Select assets to test if the defined dynamic rule is applied accurately


Test Applicability

☐ **Evaluate Rule on Creation**
You have already scanned a number of assets and they need to be re-evaluated for tag assignment.



010 - Prioritization Report Use-Case: Databases

 Just below, click to select the "Evaluate Rule on Creation" checkbox...

 Qualys. Cloud Platform

[← Create New](#)

Tag Type

☐ Static ☒ Dynamic


Tag Rules

Rule *

Asset Inventory

Query *

software:(category1:Databases) and not software:(category2:'Client Tools')

**Test Rule Applicability on selected assets**
Select assets to test if the defined dynamic rule is applied accurately

+

Test Applicability

☐ **Evaluate Rule on Creation**
You have already scanned a number of assets and they need to be re-evaluated for tag assignment.



010 - Prioritization Report Use-Case: Databases



...and click the "Create" button.

Qualys. Cloud Platform

← Create New

☐ Static ☒ Dynamic


Tag Rules

Rule *

Asset Inventory

Query *

software:(category1:Databases) and not software:(category2:'Client Tools')

 Test Rule Applicability on selected assets
Select assets to test if the defined dynamic rule is applied accurately

+

Test Applicability

☒ Evaluate Rule on Creation
You have already scanned a number of assets and they need to be re-evaluated for tag assignment.

Cancel

Create



010 - Prioritization Report Use-Case: Databases



The "Databases" tag has been successfully created and will be applied to all assets (both new and existing) that meet the query conditions. We'll now use this tag to add context to our Prioritization Report.



010 - Prioritization Report Use-Case: Databases

Qualys. Cloud Platform

CyberSecurity Asset Management ▾

HOME DASHBOARD INVENTORY TAGS RULES RESPONSES REPORTS

Tags

☐ Actions (0) ▾ Create Tag ▾

NAME	CRITICALITY	CREATED ON ▾	MODIFIED ON
★ ▶ Databases		May 14, 2019	Sep 08, 2021




010 - Prioritization Report Use-Case: Databases




Click to open the application drop-down menu...






Qualys. Cloud Platform




CyberSecurity Asset Management 

HOME DASHBOARD INVENTORY **TAGS** RULES RESPONSES REPORTS

Tags

 Databases

☐ Actions (0)  **Create Tag**  Filters   

NAME	CRITICALITY	CREATED ON 	MODIFIED ON
  Databases		May 14, 2019	Sep 08, 2021



010 - Prioritization Report Use-Case: Databases



...and select **VMDR**.

The screenshot displays the Qualys Cloud Platform interface. The top navigation bar includes links for HOME, DASHBOARD, INVENTORY, TAGS (which is the active tab), RULES, RESPONSES, and REPORTS. On the right side of the navigation bar, there are icons for user profile, help, and notifications.

The left sidebar is titled "CyberSecurity Asset Management" and contains two main sections:

- INFRASTRUCTURE SECURITY (8)**: This section lists several security modules, each with a colored icon and a brief description:
 - VMDR** (blue icon): Detect, prioritize and remediate vulnerabilities, and monitor using dashboards. This option is highlighted with a light blue background.
 - CM** (blue icon): Continuous Monitoring. Set up monitoring and alerting of new security risks.
 - CERT** (blue icon): Certificate View. Analyse and manage SSL/TLS certificates and vulnerabilities.
 - CS** (blue icon): Container Security. Discover, track, and continuously protect containers and images.
 - SEM** (blue icon): Secure Enterprise Mobility. Visibility, security, continuous monitoring for Mobile Devices and Data for enterprises.
 - TP** (red icon): Threat Protection. Add threat intelligence feed to your existing AssetView.
 - CV** (green icon): CloudView. Monitor changes on cloud platforms.
 - ICS** (blue icon): Industrial Control System BETA. Get real time visibility of critical industrial assets and manage their vulnerabilities.
- ASSET MANAGEMENT (3)**: This section lists asset management modules:
 - CSAM** (blue icon): CyberSecurity Asset Management. Identify security gaps and manage asset health across your hybrid IT environment.
 - GAV** (blue icon): Global AssetView. Maintain full, instant visibility of all your global IT assets. (Formerly Global IT Asset Inventory).

The main content area on the right shows a table with the following columns: CRITICALITY, CREATED ON, and MODIFIED ON. The table contains one row of data:

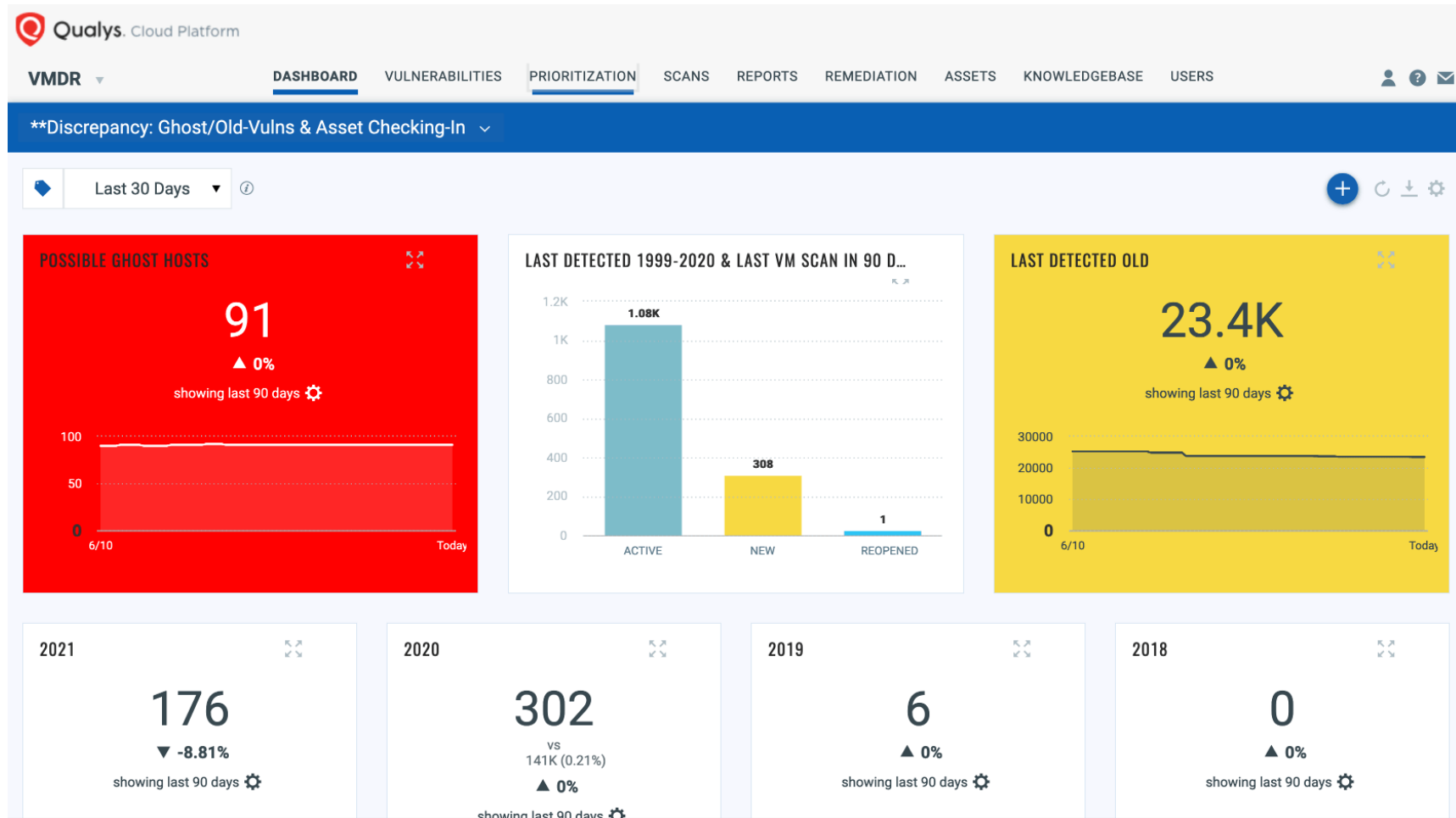
CRITICALITY	CREATED ON	MODIFIED ON
	May 14, 2019	Sep 08, 2021



010 - Prioritization Report Use-Case: Databases



Click **PRIORITIZATION** at the top of the page.





010 - Prioritization Report Use-Case: Databases



Click the button with the "+" symbol to create a new report.

Qualys. Cloud Platform

VMDR ▾ DASHBOARD VULNERABILITIES **PRIORITIZATION** SCANS REPORTS REMEDIATION ASSETS KNOWLEDGEBASE USERS

Prioritization Reports Threat Feed

Welcome to VMDR Prioritization

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





010 - Prioritization Report Use-Case: Databases



Adding Asset Tags to this report provides context for the host vulnerabilities you intend to prioritize. In this use-case we'll be targeting Database Servers with "High Data Loss" vulnerabilities. Click inside the **"Select Asset Tags"** field.



 Qualys. Cloud Platform




VMDR Prioritization

Prioritize your riskiest vulnerabilities on the most critical assets, reducing thousands of vulnerabilities to the few hundred that matter


Select Asset Tags

Start prioritization by selecting asset tags

Start Adding Asset Tags...



What's next in the prioritization process?





010 - Prioritization Report Use-Case: Databases



Select the checkbox for the "Databases" tag...

Qualys. Cloud Platform

←

VMDR Prioritization

Prioritize your riskiest vulnerabilities on the most critical assets, reducing thousands of vulnerabilities to the few hundred that matter

Select Asset Tags

Start prioritization by selecting asset tags

☐ Data Classification ☒ Databases ☐ VMDR ☐ San Diego Datacenter

→

What's next in the prioritization process?

↓



010 - Prioritization Report Use-Case: Databases



...and click the **Arrow** icon.

Qualys. Cloud Platform

←

VMDR Prioritization

Prioritize your riskiest vulnerabilities on the most critical assets, reducing thousands of vulnerabilities to the few hundred that matter

Select Asset Tags

Start prioritization by selecting asset tags

Databases x

x →

What's next in the prioritization process?

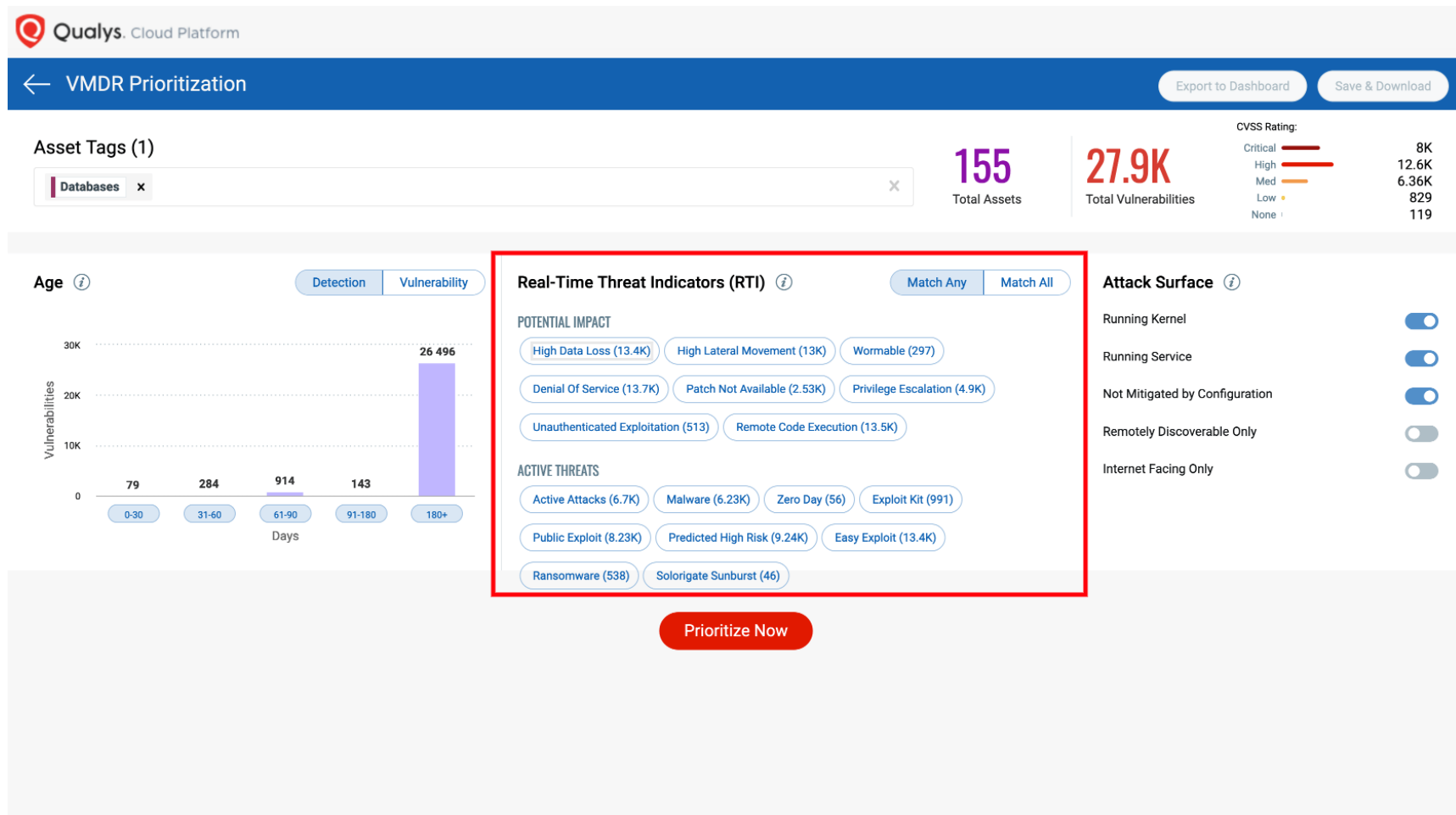
↓



010 - Prioritization Report Use-Case: Databases



With the "Databases" tag now providing the context for this report, we'll select the targeted Real-Time Threat Indicators.





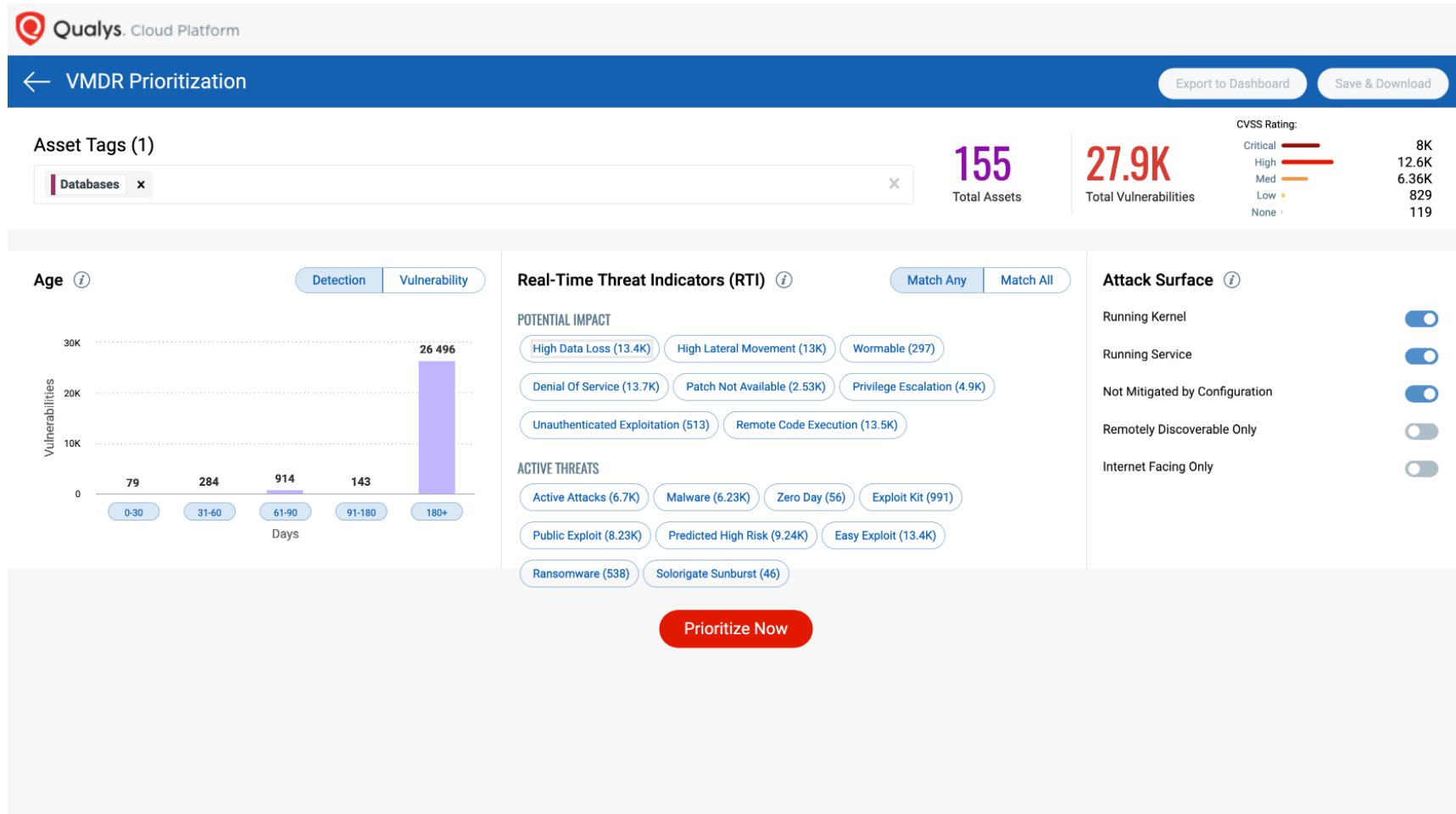
010 - Prioritization Report Use-Case: Databases



Although any of the threat groups listed here can impact a Database Server, we are especially interested in the "High Data Loss" category. This type of threat indicator will impact host assets with large data stores.



010 - Prioritization Report Use-Case: Databases

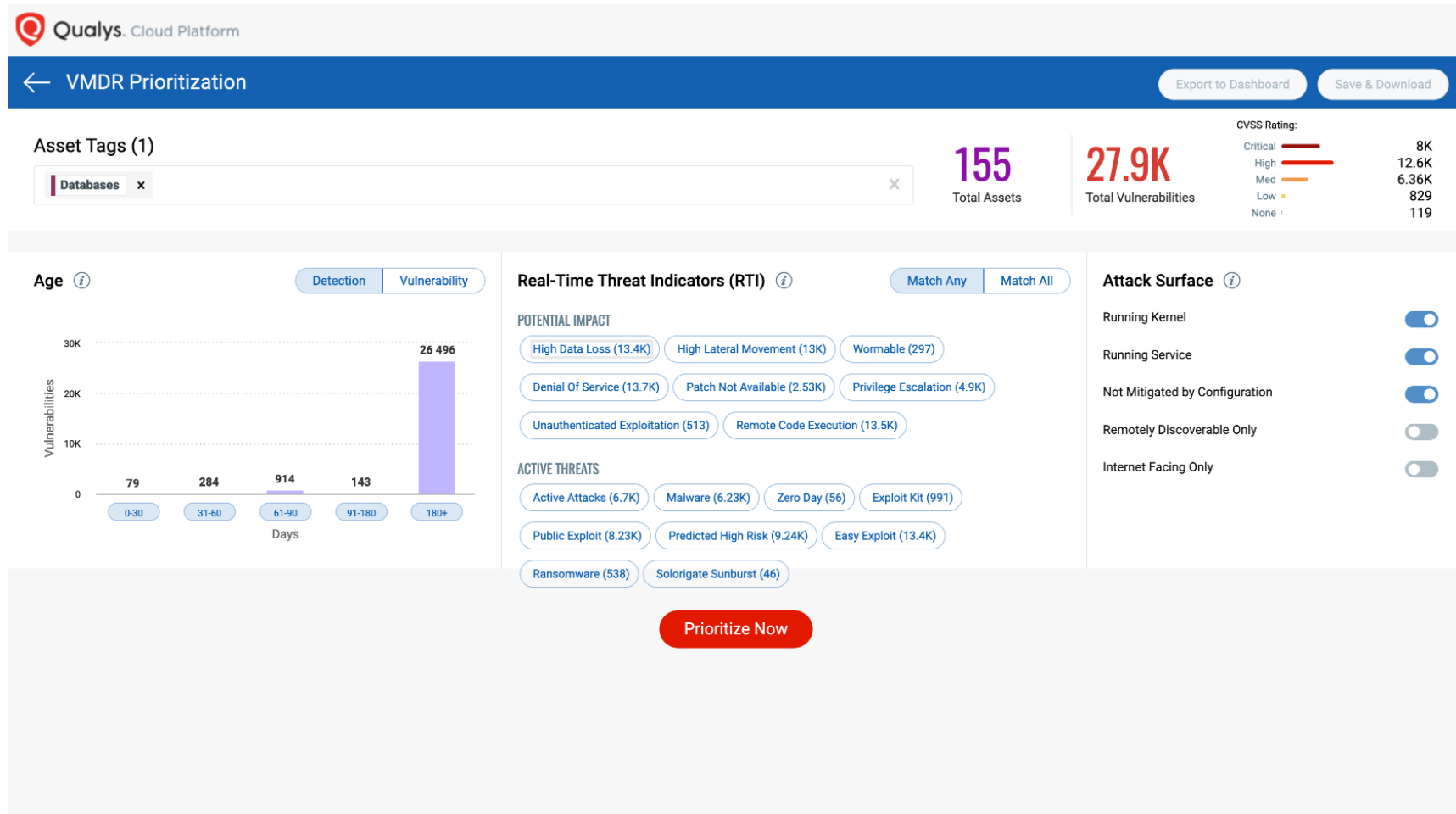




010 - Prioritization Report Use-Case: Databases



Under the POTENTIAL IMPACT section of Real-Time Threat Indicators, select **High Data Loss**.

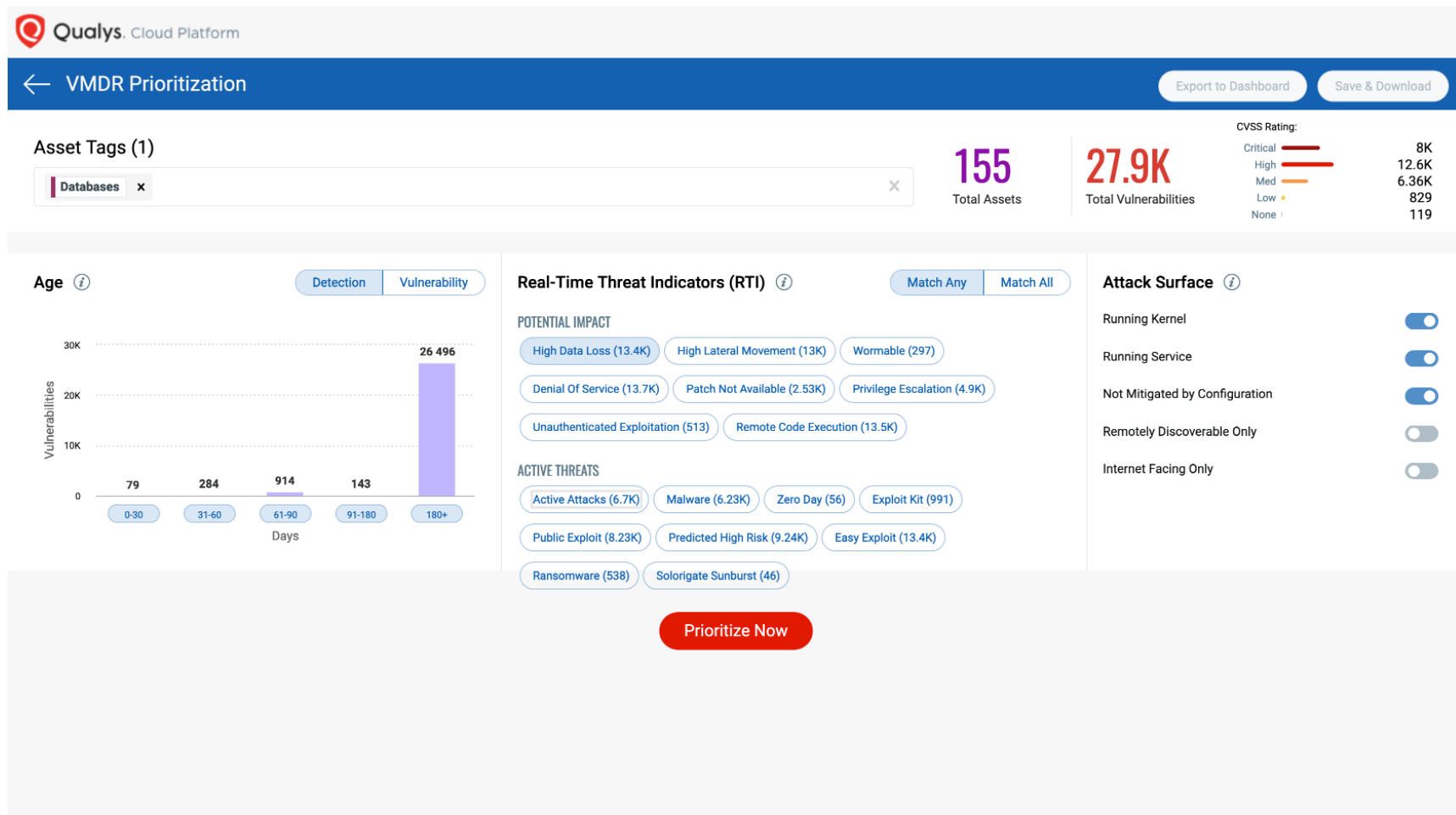




010 - Prioritization Report Use-Case: Databases



To add even greater risk potential and priority to this report, select **Active Attacks** (under the ACTIVE THREATS section).

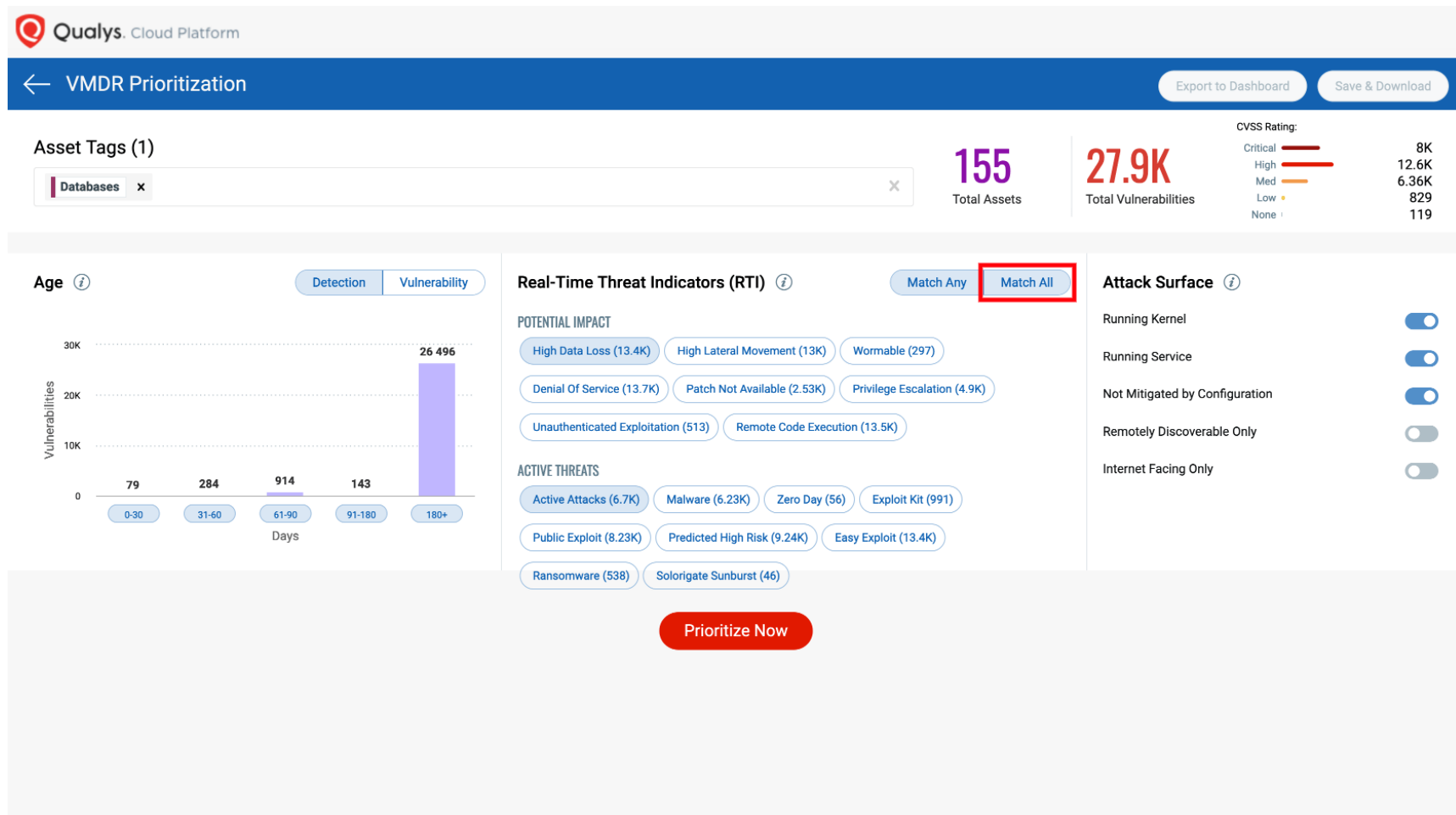




010 - Prioritization Report Use-Case: Databases



To target vulnerabilities that are high risks for massive data loss and actively being attacked, select the **"Match All"** operator. This will ensure prioritized vulnerabilities meet both conditions.

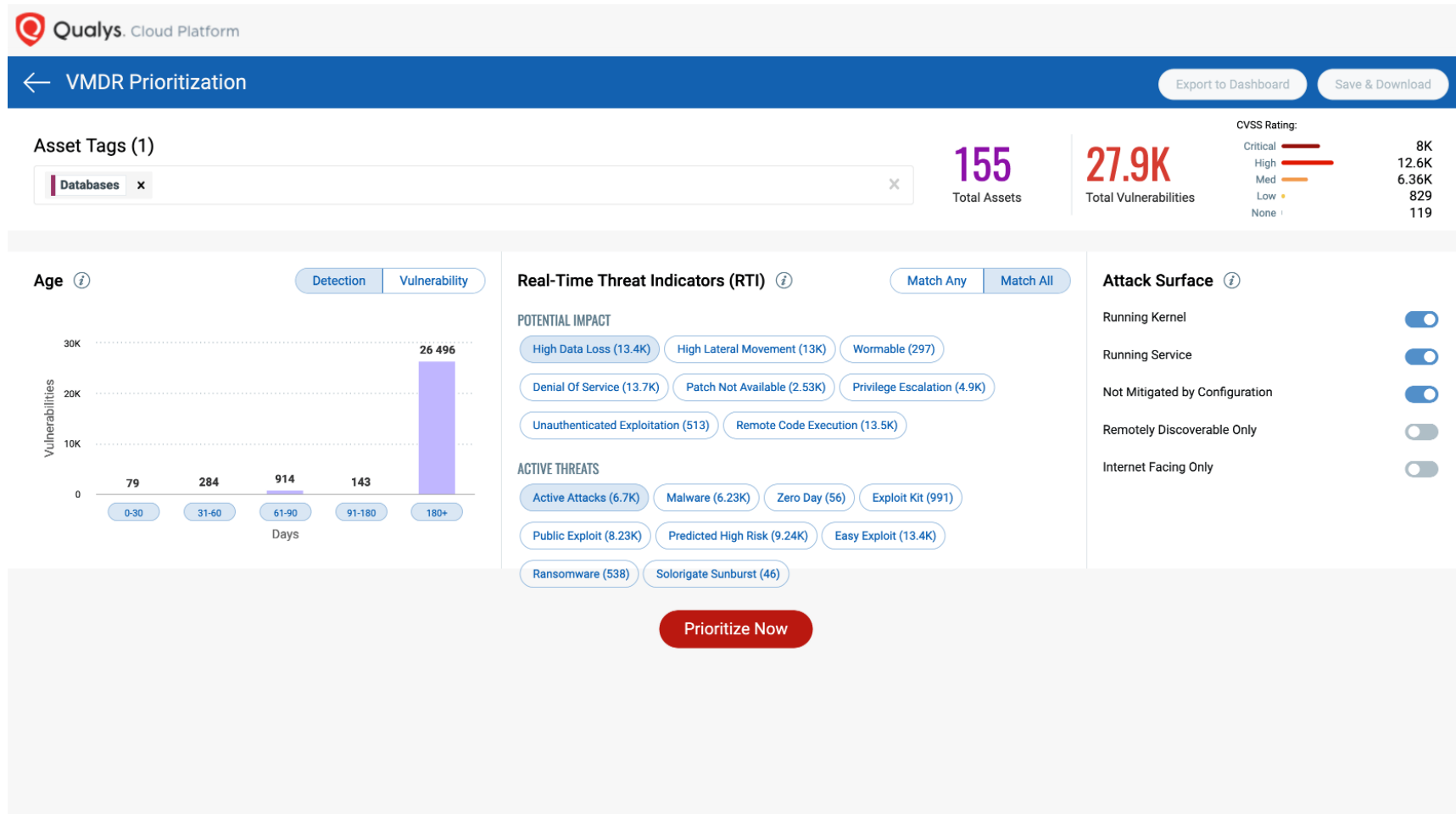




010 - Prioritization Report Use-Case: Databases



Click the "Prioritize Now" button.

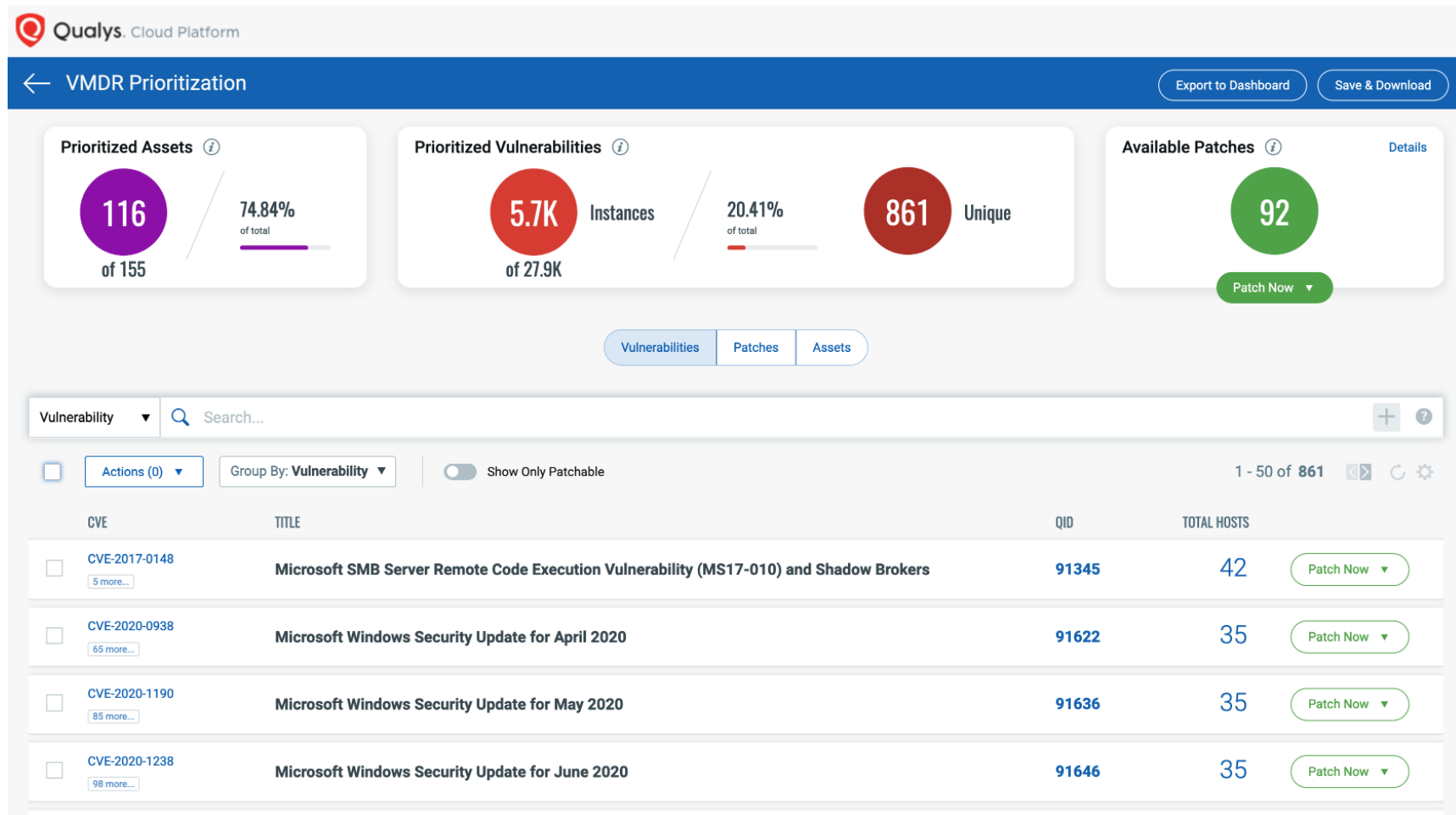




010 - Prioritization Report Use-Case: Databases



The vulnerabilities, patches, and assets that meet your prioritized options are now displayed.





010 - Prioritization Report Use-Case: Databases



You can apply patches individually...

Qualys Cloud Platform

← VMDR Prioritization Export to Dashboard Save & Download

Prioritized Assets ⓘ

116 of 155 74.84% of total

Prioritized Vulnerabilities ⓘ

5.7K Instances of 27.9K 20.41% of total **861 Unique**

Available Patches ⓘ Details

92 Patch Now ▾

Vulnerabilities Patches Assets

Vulnerability Search... + ?

☐ Actions (0) ▾ Group By: Vulnerability ▾ ☐ Show Only Patchable 1 - 50 of 861 ⌂ 🔄 ⚙️

CVE	TITLE	QID	TOTAL HOSTS	
<input type="checkbox"/> CVE-2017-0148 5 more...	Microsoft SMB Server Remote Code Execution Vulnerability (MS17-010) and Shadow Brokers	91345	42	Patch Now ▾
<input type="checkbox"/> CVE-2020-0938 65 more...	Microsoft Windows Security Update for April 2020	91622	35	Patch Now ▾
<input type="checkbox"/> CVE-2020-1190 85 more...	Microsoft Windows Security Update for May 2020	91636	35	Patch Now ▾
<input type="checkbox"/> CVE-2020-1238 98 more...	Microsoft Windows Security Update for June 2020	91646	35	Patch Now ▾



010 - Prioritization Report Use-Case: Databases



...or you can deploy all available patches at once. This concludes the Prioritization Report Use-Case for Database Servers. You may close this window and return to your lab tutorial supplement.

Qualys Cloud Platform

VMDR Prioritization [Export to Dashboard](#) [Save & Download](#)

Prioritized Assets ⓘ

116 of 155 **74.84%** of total

Prioritized Vulnerabilities ⓘ

5.7K Instances / 20.41% of total / 861 Unique

Available Patches ⓘ [Details](#)

92

[Patch Now](#) ▼

[Vulnerabilities](#) [Patches](#) [Assets](#)

Vulnerability ▼

☐ [Actions \(0\)](#) ▼ [Group By: Vulnerability](#) ▼ ☐ Show Only Patchable 1 - 50 of 861

CVE	TITLE	QID	TOTAL HOSTS
<input type="checkbox"/> CVE-2017-0148 5 more...	Microsoft SMB Server Remote Code Execution Vulnerability (MS17-010) and Shadow Brokers	91345	42 Patch Now ▼
<input type="checkbox"/> CVE-2020-0938 65 more...	Microsoft Windows Security Update for April 2020	91622	35 Patch Now ▼
<input type="checkbox"/> CVE-2020-1190 85 more...	Microsoft Windows Security Update for May 2020	91636	35 Patch Now ▼
<input type="checkbox"/> CVE-2020-1238 98 more...	Microsoft Windows Security Update for June 2020	91646	35 Patch Now ▼



Scan to go to the interactive player