



# **QSC 2021 VMDR**

## **Lab Tutorial Supplement**

## Table of Contents

<b>ASSET MANAGEMENT</b> .....	<b>3</b>
COMPREHENSIVE SENSORS.....	3
Scanner Appliance.....	3
Cloud Agent.....	4
Passive Sensor.....	7
Cloud Connector.....	11
Container Sensor.....	12
Container Runtime Security.....	13
CYBERSECURITY ASSET MANAGEMENT .....	15
Example Queries.....	17
Dynamic Rule-Based Tags.....	17
Unidentified vs. Unknown.....	18
Managed vs. Unmanaged Assets.....	18
CMDB Sync.....	19
Asset Criticality Score.....	21
Product Lifecycle Management.....	23
Software Authorization Rules.....	25
Reports.....	28
Interactive Report.....	31
Rule-Based Alerts.....	34
Asset Tokens.....	35
<b>VULNERABILITY MANAGEMENT</b> .....	<b>38</b>
CSAM .....	38
VMDR.....	39
DASHBOARDS & WIDGETS.....	41
<b>THREAT DETECTION &amp; PRIORITIZATION</b> .....	<b>45</b>
VMDR THREAT FEED.....	45
PRIORITIZATION REPORT .....	46
Age.....	46
Real-Time Threat Indicators (RTI).....	47
Attack Surface.....	49
Zero-Touch Patch Jobs.....	50
Export to Dashboard.....	51
<b>PATCH MANAGEMENT</b> .....	<b>52</b>
DEPLOYMENT JOB .....	52
PATCH CATALOG .....	58
PRIORITIZED PRODUCTS LIST .....	61
<b>VMDR CERTIFICATION EXAM</b> .....	<b>62</b>
<b>VMDR COURSE SURVEY AND TRIAL ACCOUNT</b> .....	<b>64</b>
<b>APPENDIX A: ADDITIONAL VMDR APPLICATIONS</b> .....	<b>65</b>
<b>APPENDIX B: PRIORITIZATION REPORT USE CASES</b> .....	<b>72</b>

# Asset Management

## Comprehensive Sensors

Qualys Sensors provide the most comprehensive approach to collecting all your asset and software inventory data. This lab provides an overview of the various Qualys Sensors, with some special attention given to the Qualys Cloud Agent.

## Scanner Appliance

Qualys scanner appliances are available in three different varieties: 1) Internet-based appliances located within the Qualys Cloud Platform, 2) Physical appliances, and 3) Virtual Appliances.

Any Qualys user with scanning privileges has access to Qualys' pool of Internet-based Scanner Appliances. These appliances are ideal for targeting and scanning other Internet-facing assets.

Qualys physical and virtual scanner appliances can be deployed throughout your business or enterprise architecture.

Virtual scanner appliances are available for multiple virtualization platforms:

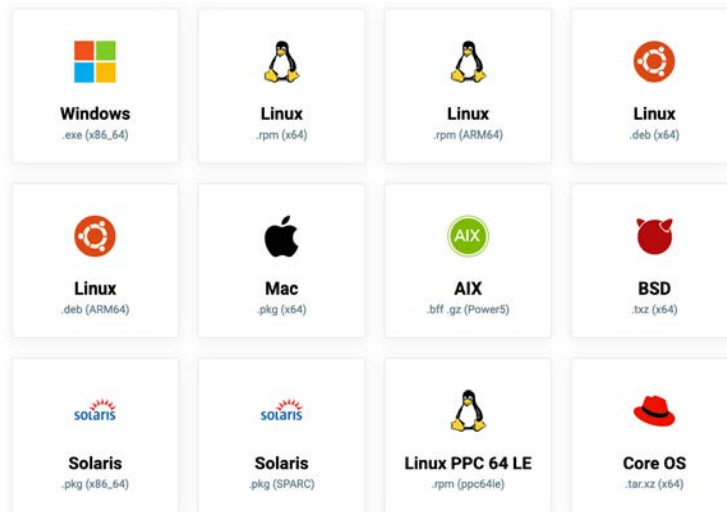
Amazon EC2
Citrix XenServer
Microsoft Hyper-V
VMware Workstation, Workstation Player, Fusion
VMware ESXi, vCenter Server (standard)
VMware vCenter Server (vApp)
OpenStack
Microsoft Azure
Google Cloud Platform

For a detailed discussion of Scanner Appliance deployment and usage, please see the "Scanning Strategies and Best Practices" training course ([qualys.com/learning](https://qualys.com/learning)).

## Cloud Agent

Qualys Cloud Agents install locally on the host assets they protect, sending all collected data to the Qualys Cloud Platform, for analysis.

Qualys agents presently support various Windows, Mac, Linux, and Unix-based operating systems.



For a complete list of supported operating systems, see the “Platform Availability Matrix” within the Cloud Agent Getting Started Guide:

<https://www.qualys.com/docs/qualys-cloud-agent-getting-started-guide.pdf>

## Configure Agents for VMDR

Multiple VMDR applications are supported by Qualys Cloud Agent:

- CyberSecurity Asset Management (CSAM)
- Vulnerability Management (VM)
- Security Configuration Assessment (SCA) / Policy Compliance (PC)
- Patch Management (PM)

These supported application modules must be activated for your VMDR host assets.

**Click the following URL to view the “Configure Agents for VMDR” tutorial:**



LAB 1 - <https://ior.ad/7SEb>

Activation Keys can be configured from the Cloud Agent application or the VMDR “Welcome” page.

**Upgrade Agents with Activation Keys**

VMDR requires the activation of a purpose-built engine for detecting missing patches for Cloud Agents. Select Activation keys which you want to upgrade for VMDR. All the agents associated with those keys will be upgraded.

Actions (1) Manage Cloud Agent Keys 1 - 2 of 2

	MODULES	AGENTS	TAGS
<b>Upgrade</b>	Unlimited Key SCA VM PM CSAM	0	
Default VMDR Activation Key 28f4b0cd-f622-42e0-a809-c12474161c3f			
<input checked="" type="checkbox"/> Minimum Module Activation Key 549c7a3f-fc20-44bf-8c54-e74f234b95d8	Unlimited Key CSAM	0	VMDR Lab

Upgrade Activation Keys to include the CSAM, VM, SCA, and PM application modules.

**Activation Key** Turn help tips: On | Off

Edit the activation key

An activation key is used to install agents. This provides a way to group agents and better manage your account. By default this key is unlimited - it allows you to add any number of agents at any time.

Title: VMDR Lab Activation Key

Provision Key for these applications

<input checked="" type="checkbox"/> CSAM CyberSecurity Asset Management Activations managed by CSAM	<input checked="" type="checkbox"/> PM Patch Management 115 Activations Remaining
<input checked="" type="checkbox"/> VM Vulnerability Management 15 Activations Remaining	<input type="checkbox"/> PC Policy Compliance 15 Activations Remaining
<input checked="" type="checkbox"/> SCA Secure Config Assessment 15 Activations Remaining	

Set limits

Close Unlimited Key Save

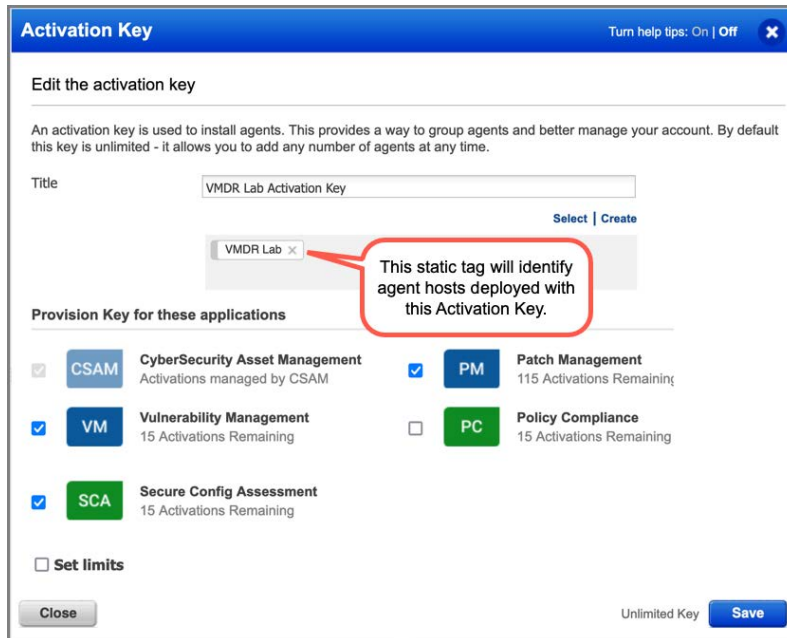
While VMDR includes the “Security Configuration Assessment” module (by default), agent Activation Keys can be updated to include Policy Compliance (PC) instead of SCA.

## Activation Key Tagging Strategy

Asset Tags provide an effective way to assign your agent host assets to their appropriate configuration settings, assessment profiles, and patch jobs.

Unlike dynamic tags, static tags “stick” to their host systems. Once a “static” tag is assigned to a target host, it will remain assigned to that host, until it is manually removed or replaced.

The non-dynamic or predictable nature of a static tag makes it especially useful for tracking host assets that are installed from the same Activation Key.



The same Asset Tags that are assigned to agent Activation Keys can then be used to assign patching licenses to specific hosts and ensure agent hosts are correctly assigned to their appropriate Configuration Profile, Patch Assessment Profile, and Patch Jobs.

For a detailed discussion of agent installation and configuration steps, see the “Cloud Agent” training course ([qualys.com/learning](http://qualys.com/learning)).

## Passive Sensor

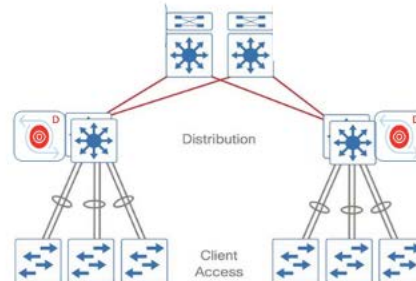
Qualys Passive Sensor operates in “promiscuous” mode, capturing network traffic and packets from either a network TAP, or the SPAN port of a network switch.

### Physical

- 1 Gbps sensor - up to 3K assets
- 4 Gbps sensor - up to 15K assets
- 10 Gbps sensor - up to 30K assets

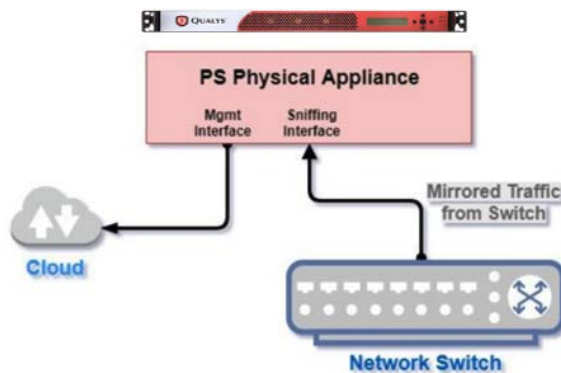
### Virtual

- 1 Gbps sensor - up to 3K assets



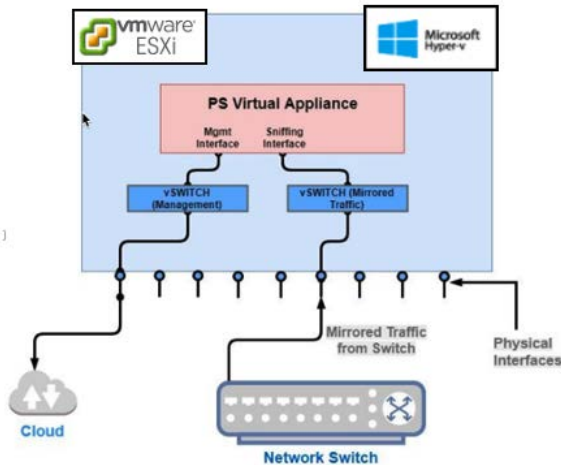
Sensors deployed at lower layers of your network architecture (i.e., at distribution switches closest to LAN traffic) may require greater bandwidth capacity.

Both physical (hardware-based) and virtual sensor appliances are available:

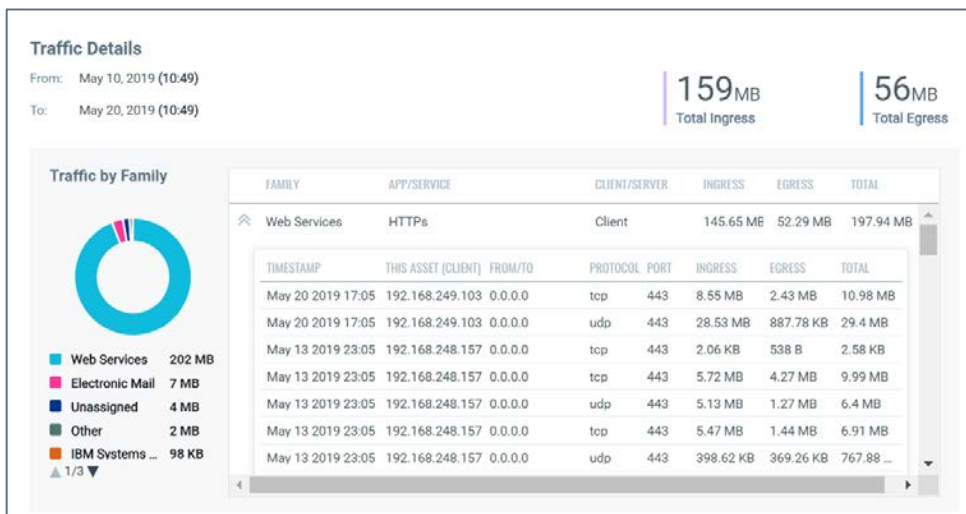


The Management Interface of the sensor appliance is assigned an IP address and must successfully connect to the Qualys Cloud Platform.

The Sniffing Interface is not assigned an IP address and receives traffic from a network TAP or the SPAN port of a network switch.



An important advantage to capturing network traffic, comes from the bonus information collected from network conversations (conversations between communicating hosts).



A passive sensor not only collects the traffic from “managed” company assets, but it also sees traffic from other host assets and services that are attempting to communicate with your “managed” host assets (including communications coming from unknown or “unmanaged” assets).

New assets typically appear in Qualys CSAM within 5-10 minutes. As more information is discovered it is aggregated across all assets and sent every 15 minutes.

When your subscription is enabled for traffic analysis, summarized traffic information is sent to the Qualys Cloud Platform every 30 minutes for traffic analysis.



## Passive Sensor Deployment Scenarios

There are different types of network environments and topologies where you may want to deploy passive sensor. When attempting to connect Passive Sensor to the SPAN port on a network switch, here are the different types of port mirroring options that can be used:

### 1. Local SPAN

**Switch Port Analyzer (SPAN)** mirrors traffic from one or more interfaces or VLAN to one or more interfaces on the same switch. This method is also called Local SPAN. In this scenario the sensor appliance is connected directly to one of the switch ports (i.e., passive sensor and switch are in the same location).

### 2. RSPAN

If your network has many Layer 2 switches then it may not be possible to do local mirroring on each Layer 2 switch and deploy multiple passive sensors connecting to SPAN port of each Layer 2 switch. To handle this situation, you need to use **Remote Switch Port Analyzer (RSPAN)** method to centralize the mirror traffic from various Layer 2 switches. RSPAN provides remote monitoring traffic from source ports distributed over multiple switches. It supports source ports, source VLANs, and destination ports on different switches.

### 3. ERSPAN

Some enterprises may have a requirement to passively monitor their networks, including those remotely located, and it may not be possible to install a sensor in each of the remote locations. To monitor traffic across a WAN or different networks, you can use **Encapsulated Remote Switch Port Analyzer (ERSPAN)**.

The ERSPAN feature supports source ports, source VLANs, and destination ports on different switches, which provides remote monitoring of multiple switches across your network.

ERSPAN allows mirrored traffic to be encapsulated and transported over L3 network to a remote destination. This requires that each location have switches having ERSPAN capability and the switches be configured to tunnel mirror traffic to a destination L3 switch/router interface.

*Please consult the PS Deployment Guide for more information on deployment scenarios and configuration steps.*

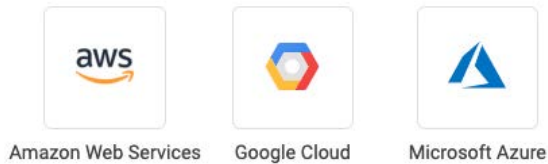
# Network Passive Sensor User Guides

The screenshot shows the Qualys Community website. At the top, there is a navigation bar with the Qualys logo and the text "Qualys Community". To the right of the logo are links for "Discussions", "Blog", "Training", "Docs", and "Support". Below the navigation bar is a search bar with the text "Search documentation" and a magnifying glass icon. To the right of the search bar is the URL "qualys.com/documentation". Below the search bar is a section titled "Sensors". Under "Sensors", there are two expandable categories: "Cloud Agents" and "Scanner Appliance". The "Scanner Appliance" category is expanded, showing a list of sub-items: "Network Passive Sensor", "Online Help", "Getting Started Guide", "Physical Appliance User Guide", "Virtual Appliance User Guide", "Deployment Guide", "Release Notes", and "Training". The "Network Passive Sensor" item is highlighted with a red rectangular box. To the right of the "Sensors" section, there is a checkmark icon followed by the text "Stay up-to-date with the latest sensor features and specifications."

Look for “Network Passive Sensor” User Guides (under Sensors) in the Qualys Documentation Community (qualys.com/documentation).

## Cloud Connector

Create connectors for your AWS, Google, and Azure accounts.



Enumerate cloud instances and collect useful metadata such as:

- Instance or virtual machine ID
- Location or region
- External and private IPs
- Installed software and active services
- and much more...

Search Tip: Within the CyberSecurity Asset Management application, use the “inventory.source” query token, to quickly find AWS, Azure, and Google instances:

- `AWS - inventory.source:INSTANCE_ID`
- `Azure - inventory.source:VIRTUAL_MACHINE_ID`
- `Google - inventory.source:GCP_INSTANCE_ID`

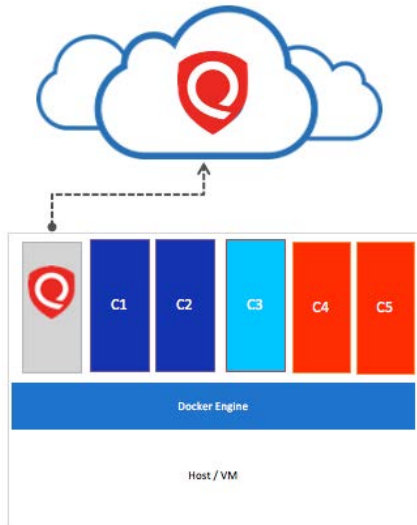
Leverage Qualys Cloud Security Assessment (CSA), to identify and correct misconfigurations.



Look for more information on Cloud Connectors, in the “CSA Getting Started Guide” on the Qualys Documentation Community ([qualys.com/documentation](https://qualys.com/documentation)).

## Container Sensor

Qualys Container Sensor is installed on a Docker host as a container application, right alongside other containers.



Once installed, CS will assess all new and existing Docker images and containers for vulnerabilities.



Types of Container Sensors:

- General – Scan Docker hosts.
- Registry – Scan images in public or private registries.
- CI/CD Pipeline – Scan images within CI/CD pipeline (e.g., Jenkins and Bamboo).

*For more information and details on deploying and using Qualys Container Sensors, see the “Container Security” training course ([qualys.com/learning](https://qualys.com/learning)).*

## Container Runtime Security

Qualys Container Runtime Security provides container runtime visibility and protection and allows you to create rules or policies to actively block or prevent unwanted actions or events within your container applications.



This is achieved by instrumenting images with Container Security components that gather functional-level, behavioural data about the processes running within a container.

*We use an application-native instrumentation process that provides complete visibility of the application inside the container. The instrumentation is very lightweight and provides configurable data collection options with low/no impact on application performance.*

Behavioural data is used by Container Security to monitor process activity, allowing you to apply security policies and custom security controls, to block specific events or attempted activities.

Container Runtime Security (CRS) can be deployed for both on-prem and cloud container environments and is particularly useful for securing containers in a CaaS environment where the underlying host infrastructure is managed by a cloud service provider.

Presently, the Container Runtime Security instrumenter supports the following registries for instrumentation:

- Public registries: Docker Hub
- Private registries: v2-private registry: JFrog Artifactory (secure: auth + https)

# Container Sensor User Guides



The screenshot shows the Qualys Community website. At the top, there is a navigation bar with the Qualys logo and the text "Qualys Community". To the right of the logo are links for "Discussions", "Blog", "Training", "Docs", and "Support". Below the navigation bar is a search bar with a magnifying glass icon and the text "Search documentation". To the right of the search bar is the URL "qualys.com/documentation". Below the search bar is a section titled "Cloud/Container Security". Under this section is a list of links, which is highlighted with a red box. The links in the list are: "Container Security", "Online Help", "User Guide", "API User Guide: HTML | PDF", "CRS User Guide", "CRS API User Guide: HTML | PDF", "Container Security Registry Scanning", "Sensor Deployment Guide", "Qualys Container Scanning Connector for Jenkins", "Qualys Container Scanning Connector for Bamboo", "Qualys Container Scanning Connector for Azure", "DevOps", "Release Notes", and "Training".

Look for Container Sensor User Guides on the Qualys Documentation Community (qualys.com/documentation).

# CyberSecurity Asset Management

The Qualys CyberSecurity Asset Management application collects raw data from Qualys Sensors and then adds its own categorization, normalization and enrichment information.

Qualys provides Level 1 and 2 categories for Hardware, Operating Systems, and Software Application assets.

## Hardware Classification

Attribute	Examples	Search Token
category (level1 / level2)	Computer / Notebook	hardware.category
category (level1)	Computer	hardware.category.1
category (level2)	Notebook	hardware.category.2
full hardware name	Dell Latitude e7470	hardware
manufacturer	Dell	hardware.manufacturer
product	Latitude	hardware.product
model	e7470	hardware.model

The table (above) provides some useful examples of “hardware” tokens.

To view all of the hardware categories in your account, group assets by hardware category (i.e., INVENTORY > Assets > Group Assets by... > Hardware > Category).

## Operating System Classification

Attribute	Examples	Search Token
category (level1 / level2)	Windows, Unix, Linux, Mac, ...	operatingSystem.category
category (level1)	Windows	operatingSystem.category.1
category (level2)	Client	operatingSystem.category.2
full operating system name	Windows 7 Enterprise (6.1 SP2) 64-Bit	operatingSystem
publisher	Microsoft	operatingSystem.publisher
name	Windows 7	operatingSystem.name
architecture	64Bit	operatingSystem.architecture
market version	7	operatingSystem.marketVersion
version	6.1	operatingSystem.version
update	SP2	operatingSystem.update
edition	Enterprise	operatingSystem.edition

The table (above) provides some useful examples of “OS” tokens.

To view all of the OS categories in your account, group assets by operating system category (i.e., INVENTORY > Assets > Group Assets by... > Operating System > Category).

## Software Classification

Attribute	Examples	Search Token
type	Application, Driver, OS Update, Unknown	software.type
category (level1 / level2)	Productivity > Productivity Suites	software.category
category (level1)	Productivity	software.category.1
category (level2)	Productivity Suites	software.category.2
full software name	Microsoft Office 2016 (16.0.1.2) Professional 64-Bit	software.name
publisher	Microsoft	software.publisher
product	Office	software.product
architecture	64-Bit	software.architecture
market version	2016	software.marketVersion
version	16.1	software.version
update	16.1.1.2	software.update
edition	Professional	software.edition

The table above provides some useful examples of “software” tokens.

To view all of the software categories in your account, group software by software category (i.e., INVENTORY > Software > Group Software by... > Category).

**Click the following URL to view the “Search Using Categories” tutorial:**



LAB 2 - <https://ior.ad/7SEF>



## Example Queries

To build a dynamic tag for Windows-based systems, use the “Asset Inventory” rule engine with the following query:

```
operatingSystem.category1:'Windows'
```

To build a dynamic tag for “Server” host assets, use the “Asset Inventory” rule engine with the following query:

```
operatingSystem.category2:'Server'
```

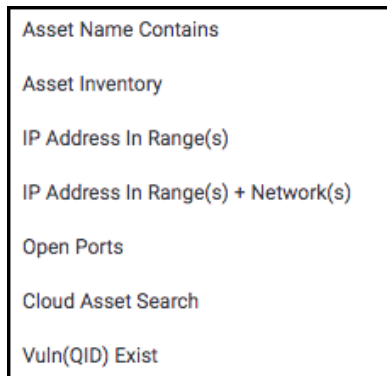
To build a dynamic tag for Windows Servers, use the “Asset Inventory” rule engine with the following query:

```
operatingSystem.category:Windows / Server
```

The first value (Windows) is separated from the second value (Server) by the slash (“/”) symbol.

## Dynamic Rule-Based Tags

Qualys CSAM provides multiple rule engines for creating dynamic Asset Tags.



The “Asset Inventory” rule engine allows you to build tags using the Qualys Query Language and various query tokens, including the hardware, OS, and software category tokens.

***Click the following URL to view the “Dynamic Rule-Based Tags” tutorial:***



Lab 3 - <https://ior.ad/7SEK>

## Unidentified vs. Unknown

The OS and Hardware values for some assets may be displayed as Unidentified or Unknown. This is especially common within the list of “**Unmanaged**” assets.

### Unidentified

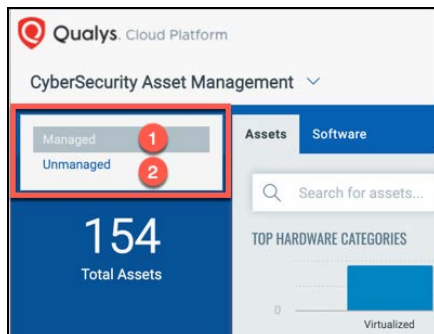
- Not enough data has been discovered/collected for Qualys to determine the hardware or operating system.
- To reduce the number of unidentified assets in your account, attempt to perform scans in “authenticated” mode and ensure network filtering devices allow your scan traffic to pass.

### Unknown

- Adequate data exists for Qualys to categorize the asset, but it has yet to be cataloged.
- Assets are processed by Qualys labs for analysis and categorization. Qualys researchers review data and update the catalog daily.

## Managed vs. Unmanaged Assets

With Qualys Passive Sensor, the CSAM application will help you to distinguish between 1) Managed and 2) Unmanaged host assets.



Managed assets in your account, will have known values for hostname, IP address, and MAC address. Newly discovered hostnames, IPs, and MAC Addresses will be initially labeled as new or “Unmanaged.”

New data collected can potentially be merged with existing data only when:

- Both IP address and MAC address have been successfully matched, or
- Both IP address and hostname have been successfully matched.

CSAM uses these combinations, plus operating system and time to uniquely identify assets. NOTE: A single asset can potentially have multiple interfaces.

## CMDB Sync

With the Qualys CMDB Sync App, your ServiceNow CMDB can serve as another source of data. Also, ServiceNow CMDB can benefit from Qualys categorization, normalization, and data enrichment.

To work successfully, the app needs to be installed in Qualys and ServiceNow. Once installed, metadata can move in both directions. Asset metadata synchronization is performed for assets already in Qualys and ServiceNow, concurrently (i.e., not for new asset discovery).

### Business Context Attributes

Automatically import business context attributes from ServiceNow CMDB.

```
businessApp:(businessCriticality
businessApp:(environment
businessApp:(id
businessApp:(managedBy
businessApp:(name
businessApp:(operationalStatus
businessApp:(ownedBy
businessApp:(supportGroup
businessApp:(supportedBy
```

***Click the following URL to view the “Business Context through CMDB Sync” tutorial:***



Lab 4 - <https://ior.ad/7SEX>

To implement ServiceNow CMDB Integration, a Qualys subscription with API access is required, along with the following application modules:

- CSAM
- Vulnerability Management

Qualys provides two apps for integrating Qualys with ServiceNow CMDB:

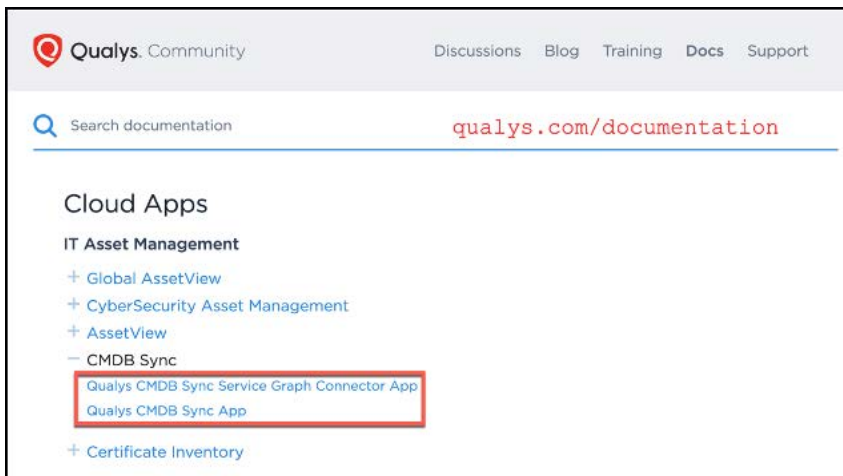
1. **Qualys CMDB Sync App**

- Install the Qualys CMDB Sync App (available in ServiceNow Online Store)

2. **Qualys CMDB Sync Service Graph Connector App**

- Install the Qualys Service Graph Connector App (available in ServiceNow Online Store)
- ITOM Visibility license in ServiceNow

The Qualys CMDB Sync Service Graph Connector App, requires ServiceNow “Orlando” version or later.



Look for both CMDB Sync User Guides within the Qualys Documentation Community (qualys.com/documentation).

## Asset Criticality Score

With GAV/CSAM, you can apply tags manually or dynamically to host assets and you can configure an Asset Criticality score for any tag, which is applied to its assigned assets.

You can set the asset criticality score between 1 to 5. Score 1 being the lowest criticality and 5 being the highest criticality assigned to an asset, when selected.

Asset Criticality Score

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

Here, score 1 being the lowest criticality and 5 being the highest criticality assigned to an asset, when selected.

1  2  3  4  5

CSAM automatically calculates the Asset Criticality Score of an asset based on its highest criticality score.

Qualys Cloud Platform

CyberSecurity Asset Management

HOME DASHBOARD INVENTORY TAGS NETWORK

Managed 12.1K Total Assets

MANUFACTURER

Unidentified	8.89K
VMware	1.42K
Google	857
Amazon Web Ser...	407
Microsoft	170
37 more	

ASSET TAGS

ASSET TAGS	ASSET CRITICALITY SCORE
Type: Servers	3
Unauthorized...	5
Webserver	4

WIN-JK9PJ04FTHL 192.168.0.115,fe80:0:0:18d3:7c58:5f... 5

Microsoft Windows Server ... Amazon Web Ser...  
Datacenter6.1 SP1 64-Bit Cloud Instance

In the example above the host is awarded an Asset Criticality Score of five (5).

*\*Note that tag criticality score for **system tags** (e.g., Cloud Agent, Business Unit, etc...) will always be Null.*

The default criticality score for an asset is two (2), if it has no tag (with an Asset Criticality Score) attached to it.

## Asset Group Tags

Assets Groups configured with a Business Impact Score are mapped to their respective Asset Criticality Scores as follows:

<b>Business Impact Score</b>	<b>Asset Criticality Score</b>
<b>Critical</b>	5
<b>High</b>	4
<b>Medium</b>	3
<b>Minor</b>	2
<b>Low</b>	1

By default, a new Asset Group has a Business Impact Score of High.

## Product Lifecycle Management

End-of-life and End-of-support software and obsolete hardware increase risk to organizations. Organizations unable to get support can incur extended downtimes and technical issues that lead to decreased performance and productivity. EOL and EOS assets can also impact compliance objectives.

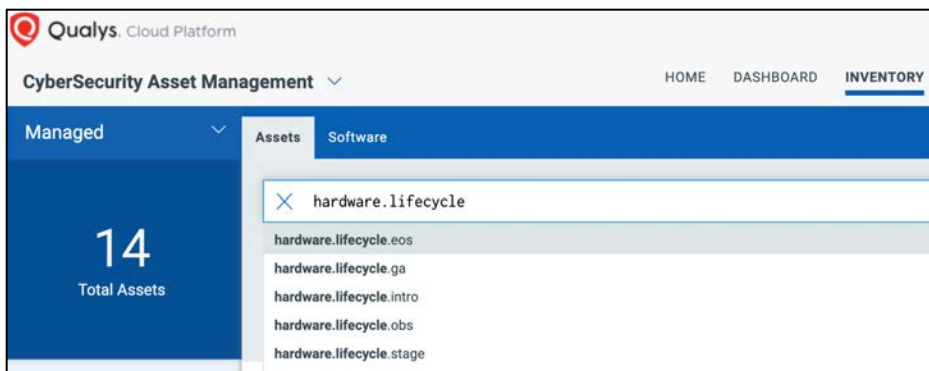
**Click the following URL to view the “Product Lifecycle Management” tutorial:**



Lab 5 - <https://ior.ad/7Sxg>

## Hardware Lifecycle

CSAM provides hardware vendor lifecycle dates and support details. CSAM has lifecycle information for hundreds of hardware manufacturers and thousands of models. Qualys continuously adds new hardware manufacturers, products and models to its catalog.

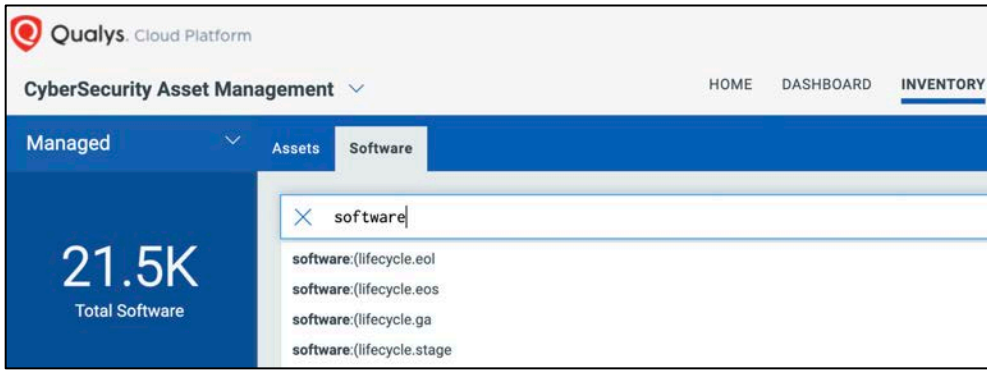


You can use multiple search tokens in CSAM to quickly filter assets based on their hardware lifecycle information to identify assets requiring replacement or upgrade.

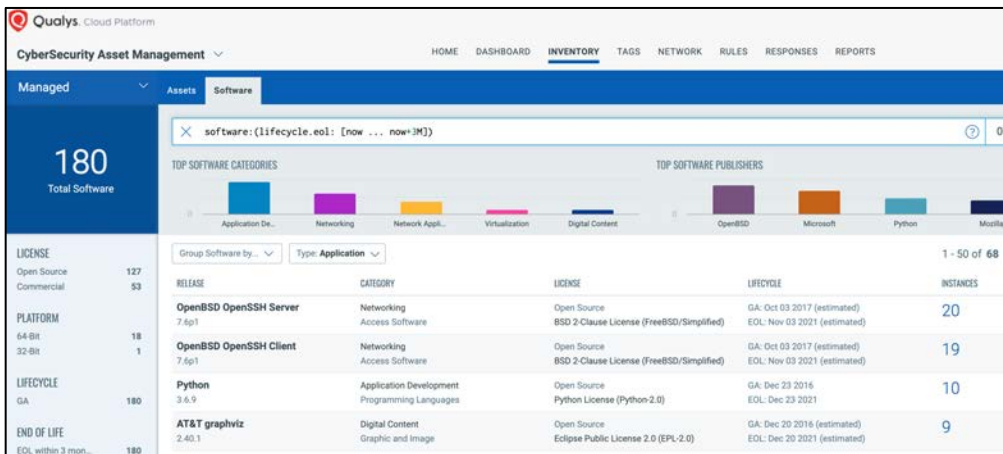
IT can leverage end-of-life and end-of support dates to plan ahead for future procurement activity (e.g. technology refreshes, extended warranty and support, etc.)

## OS & Software Lifecycle

CSAM also provides software vendor lifecycle dates and support details, so that organizations can analyze how end-of-life and end-of-support software on their environment may pose risk and potential productivity impact (e.g. lack of patches, incompatibility with future OS/applications, etc.)



You can use multiple search tokens in CSAM to quickly filter assets and software based on the software lifecycle information.



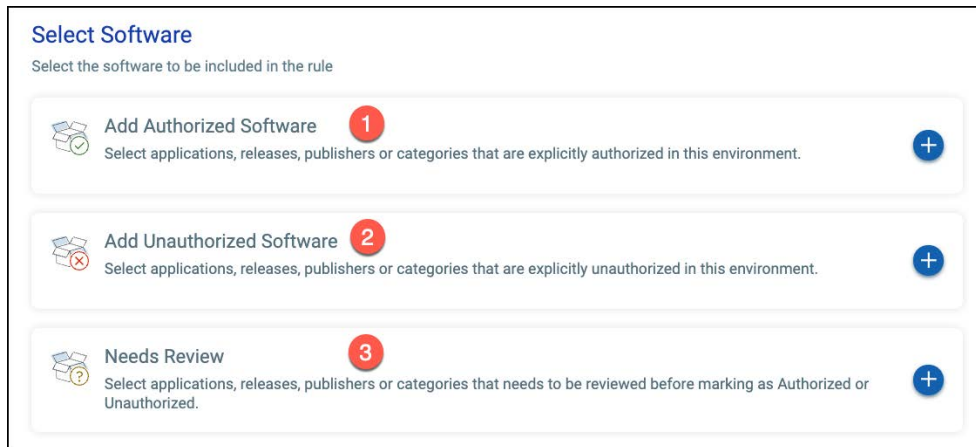
You can find out what software/OS is end-of-life or end-of-support now and within a future timeframe, so that you can assess impact and plan proper remediation (e.g. technology refresh, OS compatibility checks, budgeting, etc.)

This gives IT teams some notice on when software updates are needed. You can also search on end-of-support.



## Software Authorization Rules

In CSAM, you can create different types of rules to define software authorization:



1. Authorized – software is authorized for use.
2. Unauthorized – software is NOT authorized for use.
3. Needs review – review is required to determine software authorization.

***Click the following URL to view the “Software Authorization” tutorial:***



Lab 6 - <https://ior.ad/7SFq>

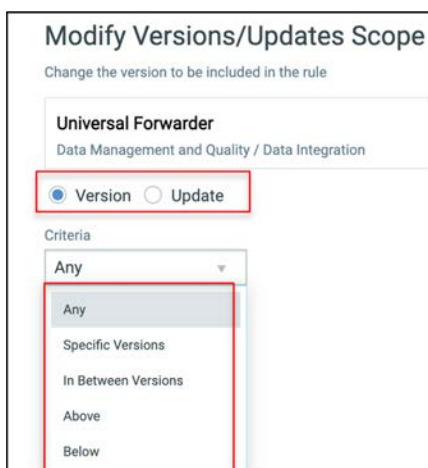
Rules are designed for specific groups of assets. For example, while browsers are commonly authorized for use on desktop and laptop systems, they add greater risk to a host and should NOT be authorized for production servers.

## Software Version\Update Criteria

Rules support criteria for software versions and updates.



Each product can be configured to match against a specific **Version** or **Version Updates**.



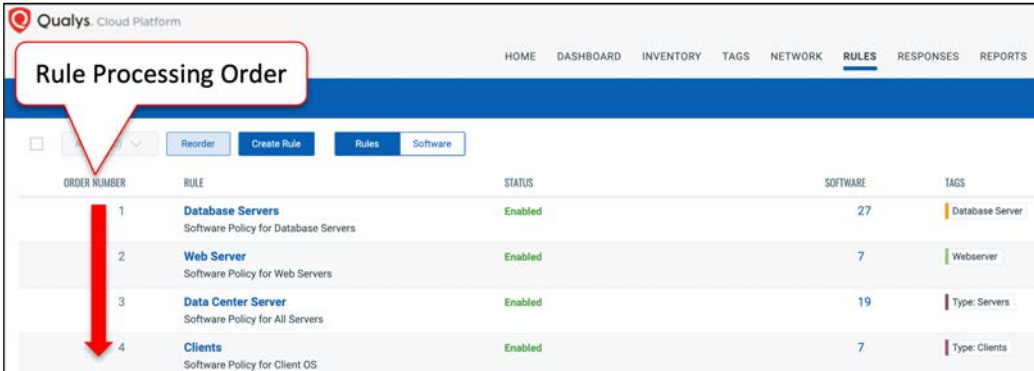
Further, a user can configure rule matching under following categories for a single product:

- **Any Version (default setting)** - Will apply the rule to all versions of the selected product.
- **Specific Versions** - Will apply rule to the selected subset of product's version.
- **In Between Versions** - Will apply rule to versions of the product which have order between than the two selected versions. Please note that the selected versions are excluded in the matching criteria.
- **Above** - Will apply rule to versions of the product which have version greater than the selected version. Please note that the selected version is excluded in the matching criteria.
- **Below** - Will apply rule to versions of the product which have version less than the selected version. Please note that the selected version is excluded in the matching criteria

## Rule Processing Requirements

1. Host must have one or more Asset Tags \*
2. Host must have one or more installed software applications
3. Software Rules match host assets based on specific applications/versions and Asset Tags included/excluded

\* For a new asset, software authorization rules won't be applied until tag evaluation and assignment is completed.



ORDER NUMBER	RULE	STATUS	SOFTWARE	TAGS
1	<b>Database Servers</b> Software Policy for Database Servers	Enabled	27	Database Server
2	<b>Web Server</b> Software Policy for Web Servers	Enabled	7	Webserver
3	<b>Data Center Server</b> Software Policy for All Servers	Enabled	19	Type: Servers
4	<b>Clients</b> Software Policy for Client OS	Enabled	7	Type: Clients

Rules are applied on the basis of rule order precedence. Any Rule has precedence over the rules below it. Rule processing begins at the top of the rule list and ends when the first match is found.

## Software Authorization Tokens

Once you have created one or more software authorization rules, search for authorized/unauthorized software using the “software authorization” tokens:

- Authorized

```
software:(authorization:'Authorized')
```

- Unauthorized

```
software:(authorization:'Unauthorized')
```

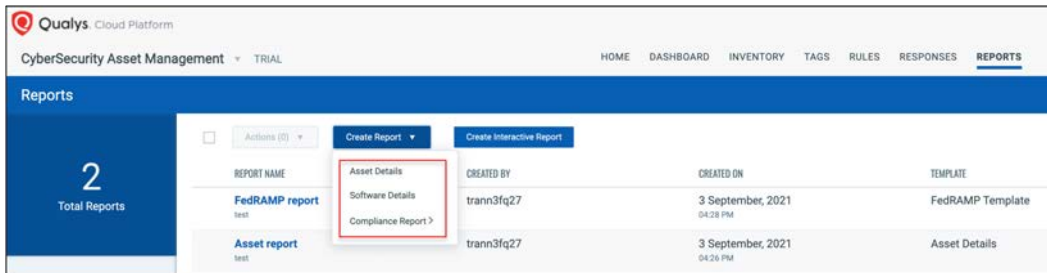
- Needs Review

```
software:(authorization:'Needs Review')
```

Query results can be viewed by software name or impacted assets. Alternatively, create a “software authorization” report (i.e., REPORTS section), using the “software authorization” tokens.

## Reports

Mandates like FedRAMP and PCI require you to track all assets and software, as well as continuously monitor their security gaps. With CSAM you can easily generate reports so you can demonstrate compliance. Reporting includes configurable out-of-the-box templates, for example to address FedRAMP requirements. You can also generate reports to provide information about your environment to internal or external stakeholders using our reporting function.



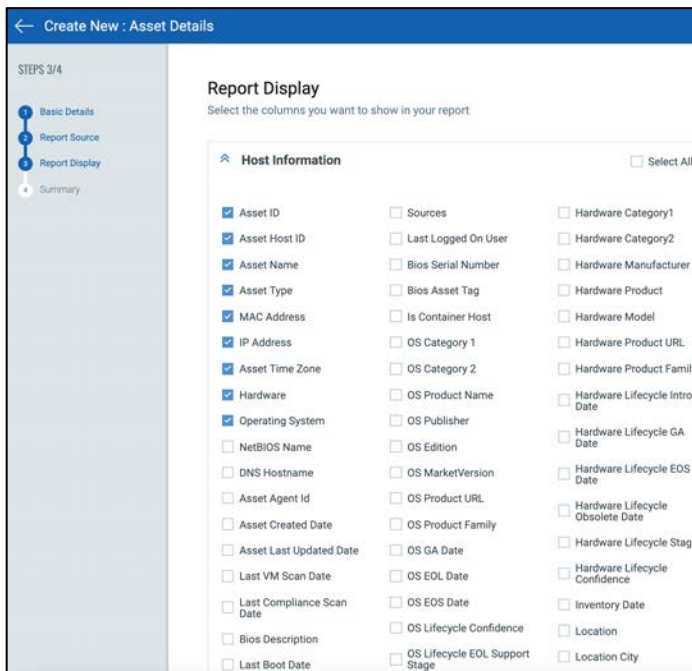
Click the following URL to view the “Asset, Software, & Compliance Reports” tutorial:



Lab 7 - <https://ior.ad/7Rfd>

## Asset Details Report

This report shows asset inventory data for selected assets based on host information (attributes).



You can select the asset scope for the report using asset name, asset tags or using queries. Once you create report, it shows 'Accepted' status.

REPORT NAME	CREATED BY	CREATED ON	TEMPLATE	STATUS
Asset Details Report	trann3fq27	6 October, 2021 10:04 AM	Asset Details	Completed

Once report execution is finished, it will show status as 'Completed' and you'll be able to download the report.

The attributes selected in the report will become column headers in the CSV report.

Asset ID	Asset Host ID	Asset Name	NetBIOS Name	DNS Hostname	Asset Type	MAC Address	IP Address	Asset Time Zone	Asset Agent ID	Asset Created	Asset Last Updated
153450468	146148757	trn-win2012-dc.t	TRN-WIN2012	trn-win2012	HOST	00:50:56:82:C5:76	64.41.200.249			07 Sep 2021 07:00	07 Sep 2021 07:00
153468805	146148750	trn-win10-pro.trn	TRN-WIN10	trn-win10-pr	HOST	00:50:56:82:C5:76	64.41.200.248			07 Sep 2021 07:00	07 Sep 2021 07:00
138428500	137932989	WIN2012R2-SVR	WIN2012R2	WIN2012R2	HOST	08:00:27:45:8F:44	64.41.200.247		4-4277	30 Jun 2021 04:23	30 Sep 2021 04:23
153071679	145888890	demo13.s02.sjc01.qualys.com	demo13.s02	demo13.s02	HOST					05 Sep 2021 03:03	03 Oct 2021 03:03
91981880	112873109	demo15.s02.sjc01.qualys.com	demo15.s02	demo15.s02	HOST					13 Nov 2020 03:03	03 Oct 2021 03:03
153429147	146148748	trn-win7.trn.qual	TRN-WIN7	trn-win7.trn	HOST	00:50:56:82:71:76	64.41.200.247			07 Sep 2021 07:00	07 Sep 2021 07:00

Selected attributes are listed in column headers

## Software Details Report

This report shows detailed report of the selected assets based on software and host information (attributes).

### Report Display

Select the columns you want to show in your report

**Software Information**  Select All

<input checked="" type="checkbox"/> Software Name	<input type="checkbox"/> Software Market Version	<input type="checkbox"/> Software Lifecycle EOS Support Stage
<input checked="" type="checkbox"/> Software Type	<input type="checkbox"/> Software Architecture	<input type="checkbox"/> Software Lifecycle Support Stage
<input checked="" type="checkbox"/> Software Product	<input type="checkbox"/> Software Package Name	<input type="checkbox"/> Software License Category
<input checked="" type="checkbox"/> Software Version	<input type="checkbox"/> Software Support Stage Description	<input type="checkbox"/> Software License Subcategory
<input checked="" type="checkbox"/> Software Update	<input type="checkbox"/> Software Lifecycle GA Date	<input type="checkbox"/> Software Instance Count
<input checked="" type="checkbox"/> Software Publisher	<input type="checkbox"/> Software Lifecycle EOL Date	<input type="checkbox"/> Software Product URL
<input checked="" type="checkbox"/> Software Authorization Status	<input type="checkbox"/> Software Lifecycle EOS Date	<input type="checkbox"/> Software Formerly Known As
<input type="checkbox"/> Software Product Family	<input type="checkbox"/> Software Lifecycle Stage	<input type="checkbox"/> Is Software Package
<input type="checkbox"/> Software Category 1	<input type="checkbox"/> Software Lifecycle Confidence	<input type="checkbox"/> Is Software Package Component
<input type="checkbox"/> Software Category 2	<input type="checkbox"/> Software Lifecycle EOL Support Stage	
<input type="checkbox"/> Software Component		
<input type="checkbox"/> Software Edition		

**Host Information**  Select All

<input type="checkbox"/> Asset ID	<input type="checkbox"/> Sources	<input type="checkbox"/> Hardware Category1
<input type="checkbox"/> Asset Host ID	<input type="checkbox"/> Last Logged On User	<input type="checkbox"/> Hardware Category2
<input type="checkbox"/> Asset Name	<input type="checkbox"/> Bios Serial Number	<input type="checkbox"/> Hardware Manufacturer
<input type="checkbox"/> Asset Type	<input type="checkbox"/> Bios Asset Tag	<input type="checkbox"/> Hardware Product

## Compliance Report

This report shows detailed report of the assets for FedRAMP compliance based on software and host information (attributes).

**Software Information**  Select All

<input checked="" type="checkbox"/> Software/ Database Vendor	<input checked="" type="checkbox"/> Comments	<input checked="" type="checkbox"/> Software Lifecycle Stage
<input checked="" type="checkbox"/> Software/ Database Name & Version	<input checked="" type="checkbox"/> Software Lifecycle GA Date	<input checked="" type="checkbox"/> Software Lifecycle Confidence
<input checked="" type="checkbox"/> Patch Level	<input checked="" type="checkbox"/> Software Lifecycle EOL Date	<input checked="" type="checkbox"/> Software Lifecycle EOL Support Stage
<input checked="" type="checkbox"/> Function	<input checked="" type="checkbox"/> Software Lifecycle EOS Date	<input checked="" type="checkbox"/> Software Lifecycle EOS Support Stage

---

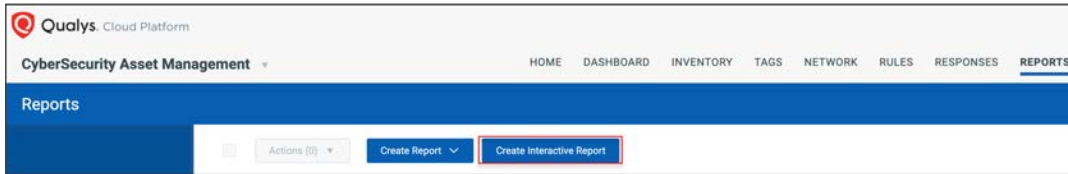
**Host Information**  Select All

<input checked="" type="checkbox"/> Qualys Unique identifier	<input checked="" type="checkbox"/> Location	<input checked="" type="checkbox"/> OS Lifecycle EOS Date
<input checked="" type="checkbox"/> UNIQUE ASSET IDENTIFIER	<input checked="" type="checkbox"/> Asset Type	<input checked="" type="checkbox"/> OS Lifecycle Stage
<input checked="" type="checkbox"/> IPv4 or IPv6 Address	<input checked="" type="checkbox"/> Hardware Make/Model	<input checked="" type="checkbox"/> OS Lifecycle Confidence
<input checked="" type="checkbox"/> Virtual	<input checked="" type="checkbox"/> In Latest Scan	<input checked="" type="checkbox"/> OS Lifecycle EOL Support Stage
<input checked="" type="checkbox"/> Public	<input checked="" type="checkbox"/> Bios Asset Tag	<input checked="" type="checkbox"/> OS Lifecycle EOS Support Stage
<input checked="" type="checkbox"/> DNS Name or URL	<input checked="" type="checkbox"/> Bios Serial Number	<input checked="" type="checkbox"/> OS Lifecycle GA Date
<input checked="" type="checkbox"/> NetBIOS Name	<input checked="" type="checkbox"/> VLAN/Network ID	<input checked="" type="checkbox"/> HW Lifecycle Intro Date
<input checked="" type="checkbox"/> MAC Address	<input checked="" type="checkbox"/> System Administrator/ Owner	<input checked="" type="checkbox"/> HW Lifecycle EOS Date
<input checked="" type="checkbox"/> Authenticated Scan	<input checked="" type="checkbox"/> Application Administrator/ Owner	<input checked="" type="checkbox"/> HW Lifecycle Obsolete Date
<input checked="" type="checkbox"/> Baseline Configuration Name	<input checked="" type="checkbox"/> OS Lifecycle GA Date	<input checked="" type="checkbox"/> HW Lifecycle Stage
<input checked="" type="checkbox"/> OS Name and Version	<input checked="" type="checkbox"/> OS Lifecycle EOL Date	<input checked="" type="checkbox"/> HW Lifecycle Confidence

This report that satisfies your auditors without you having to manually extract and aggregate the data or push the data to a 3rd party and do manual scripting. This makes your job much simpler and quicker.

## Interactive Report

This report provides an interactive workflow and focuses on asset health issues instead of just inventory data. By correlating security gaps with asset context and business context, the Interactive Report will help you to “zero in” on the most critical asset health issues so that you can address them quickly.

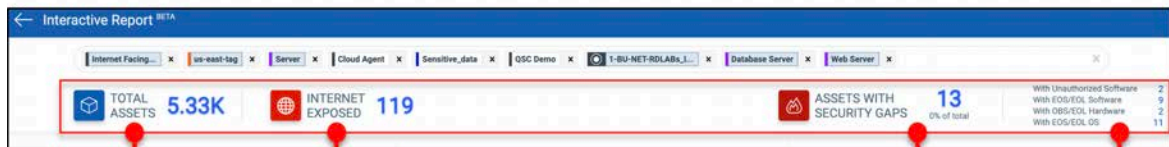


Click the following URL to view the “Interactive Report” tutorial:



Lab 8 - <https://ior.ad/7Rfc>

After selecting one or more asset tags as your targeted assets, you are provided a summary of all assets that are in scope and the area of concern.



Total Assets in Scope

Assets exposed to the Internet

Assets with one or more security gaps

Breakdown by security gap

## Internet Facing Assets

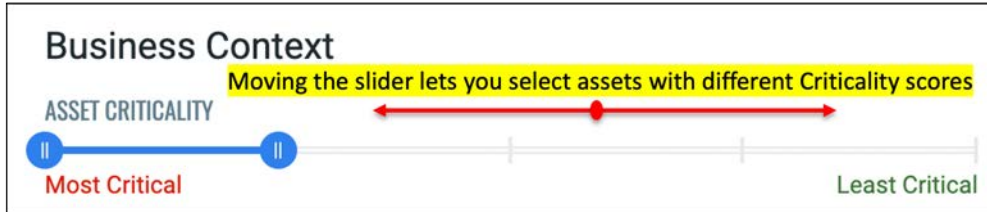
Hosts with public interfaces are at greater risk because of their exposure to the Internet, especially with vulnerabilities that can be exploited without authentication. The risk becomes even more significant if the same host has unauthorized and EOL/EOS software. So, you need to have visibility into assets with such an exposure.

From here, you can pivot further on assets of interest by applying various filters. The filter options are provided in three categories:



## Business Context

It's important to consider the business impact of an asset when prioritizing assets for security gap analysis. Here, you can select Asset Criticality, Department and Asset Support Groups as filters.



With the slider set to the position illustrated above, only assets with Criticality score of 4 and 5 will be considered for the report.

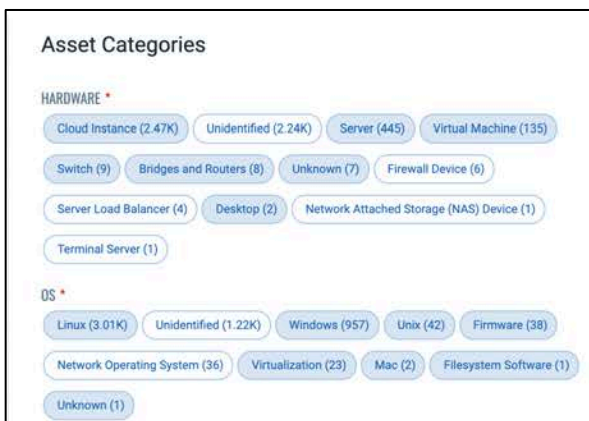


The interface shows two filter sections. The "DEPARTMENT" section has four selected items: IT Operations, DevOps, Corp IT, and Customer Support. The "ASSET SUPPORT GROUP" section has four selected items: DevOps Group, IT Operations, Corp IT, and Development Group.

Department and Asset Support Group filters are based on business information derived from CMDB sync and provide additional means to refine your asset scope.

## Asset Categories

You can also use Level 1, hardware (server, desktop, mobile device, network device, etc.) and OS (Windows, Linux, Mac, etc.) category filters which gives the user an idea about the primary function of the product, to pivot on specific asset categories. The categories listed in the report are based on the assets that are mapped to the selected asset tags.





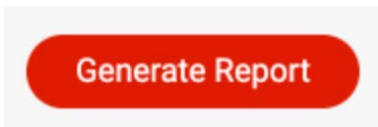
## Security Gap

And lastly, you can filter assets based on the security gap area such as EOL/OBS hardware, EOL/EOS software or OS and unauthorized software.

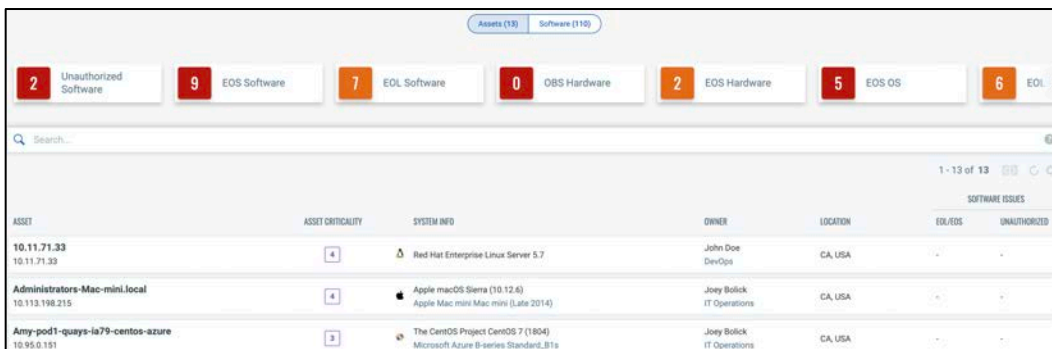
### Security Gap ⓘ

- Unauthorized Software
- EOL/EOL Software
- OBS/EOS Hardware
- EOL/EOL OS

Once your filter options have been selected, click the “Generate Report” button.



The displayed assets and software will reflect the priority options you specify.



The screenshot shows a dashboard with filter cards at the top: Unauthorized Software (2), EOS Software (9), EOL Software (7), OBS Hardware (0), EOS Hardware (2), EOS OS (5), and EOL (6). Below the filters is a search bar and a table of results. The table has columns for ASSET, ASSET CRITICALITY, SYSTEM INFO, OWNER, LOCATION, and SOFTWARE ISSUES (EOL/EOS, UNAUTHORIZED). The table contains three rows of data.

ASSET	ASSET CRITICALITY	SYSTEM INFO	OWNER	LOCATION	SOFTWARE ISSUES	
					EOL/EOS	UNAUTHORIZED
10.11.71.33 10.11.71.33	4	Red Hat Enterprise Linux Server 5.7	John Doe DevOps	CA, USA	-	-
Administrators-Mac-mini.local 10.113.198.215	4	Apple macOS Sierra (10.12.6) Apple Mac mini Mac mini (Late 2014)	Joey Bolick IT Operations	CA, USA	-	-
Amy-pod1-quays-ia79-centos-azure 10.95.0.191	3	The CentOS Project CentOS 7 (1804) Microsoft Azure B-series Standard_B1s	Joey Bolick IT Operations	CA, USA	-	-

At the top, you can see a summary of count of assets or software instances (depending on whether you are in the Assets or the Software section of the result) with a security gap. Clicking on these cards/numbers filters assets/software as per the identified security gap.

## Rule-Based Alerts

Rule-based alerts provide ongoing detection, automatically triggering alerts for critical events based on real-time activity. This eliminates the need to manually search the same event or security gaps over and over by leveraging time-saving automation.

In CSAM, you can configure rules to monitor critical events and define actions to send you alert messages if events/incidents matching the condition are detected.

**Click the following URL to view the “Rule-Based Alerts” tutorial:**

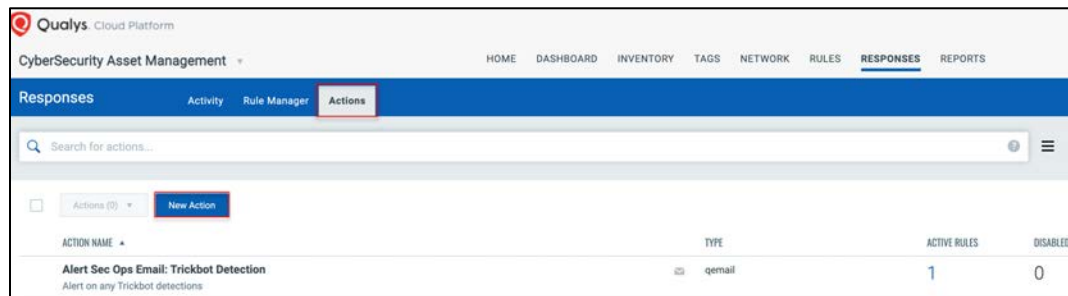


Lab 9 - <https://ior.ad/7Rfe>

You can set rules and create actions under the 'RESPONSES' tab.

On the **RESPONSES** tab:

- 1. Define Actions** → Configure rule actions to specify one or more actions to be performed when events matching a condition are detected. You can set alerts to be sent by Email, PagerDuty, or Post to Slack.



- 2. Set up your rules in the Rule Manager tab** → Here you create a rule with a specific criteria and then determine a course of action for any instance that meet that the criteria.

Let's say your goal here is to track all databases that are going to be EOS in 6 months. You want some time to react and address the issue before they actually go EOS.

The QQL query to configure for this rule is:

```
software:(category1:`Databases` and component:`Server` and lifecycle.eos:[now+179d ... now+180d])
```

Using this type of alert, your security teams can always stay on top of EOL/EOS software in your environment.

Rule Name \*

Rule to Alert for EOS Database

Description \*

Email alert for upcoming Database EOS event.

1956/2000 characters remaining

Rule Query

Provide a query to match particular source that will trigger the alert

Rule Query \*

software:(category1:`Databases` and component:`Server` and lifecycle.eos:[now+179d ... now+180d])

Sample Queries

Test Query

Action Settings

Choose an appropriate alert action

Actions \*

Email Alert for EOS Database

Email Alert for EOS Database

Recipient \*

dbowner@qualys.com

*Currently CSAM only supports the single match that is one alert for one match.*

## Asset Tokens

CSAM also supports use of tokens within the message body which work as placeholders or variables for data values that populate when the search completes. You can include a variety of search tokens pertaining to asset search, cloud metadata search and others. All 3 action types (Email, Slack, PagerDuty) support the use of tokens.

asset.created	openPorts.firstFound	software.lastUpdated	aws.ec2.privateIpAddress
asset.lastLoggedInUser	openPorts.lastUpdated	software.lastUseDate	aws.ec2.publicIpAddress
asset.lastUpdated	openPorts.port	software.license.category	aws.ec2.region.code
asset.name	operatingSystem	software.lifecycle.eol	aws.ec2.subnetId
asset.netbiosName	operatingSystem.architecture	software.lifecycle.eos	aws.ec2.vpcId
asset.trackingMethod	operatingSystem.category	software.lifecycle.stage	azure.vm.location
asset.lastLocation	operatingSystem.category1	software.marketVersion	azure.vm.name
asset.criticalityScore	operatingSystem.category2	software.name	azure.vm.privateIpAddress
asset.assetID	operatingSystem.edition	software.product	azure.vm.publicIpAddress
hardware	operatingSystem.installDate	software.authorization	azure.vm.resourceGroupName
hardware.category	operatingSystem.lifecycle.eol	software.publisher	azure.vm.size
hardware.category1	operatingSystem.lifecycle.eos	software.update	azure.vm.state
hardware.category2	operatingSystem.lifecycle.stage	software.version	azure.vm.subnet
hardware.lifecycle.eos	operatingSystem.marketVersion	software.component	azure.vm.subscriptionId
hardware.lifecycle.obs	operatingSystem.name	software.firstFound	azure.vm.vmlId
hardware.lifecycle.stage	operatingSystem.publisher	tags.name	gcp.compute.hostname
hardware.manufacturer	operatingSystem.update	volumes.free	gcp.compute.machineType
hardware.model	operatingSystem.version	aws.ec2.availabilityZone	gcp.compute.network
hardware.product	software.architecture	aws.ec2.imageId	gcp.compute.privateIpAddress
interfaces.address	software.category	aws.ec2.instanceState	gcp.compute.projectId
interfaces.gatewayAddress	software.category1	aws.ec2.instanceId	gcp.compute.projectNumber
inventory.created	software.category2	aws.ec2.accountId	gcp.compute.publicIpAddress
inventory.lastUpdated	software.edition	aws.ec2.instanceType	gcp.compute.state
inventory.source	software.installDate	aws.ec2.launchDate	gcp.compute.zone

When a condition matching the rule is detected, the alert that is generated will include the asset name, asset criticality score, hardware category, OS of the asset, etc. depending on the tokens inserted in the message body.

When a rule is triggered based on trigger criteria, CSAM will send to your configured account alerts that will have details of the events.

The screenshot shows an email client interface with a list of messages and a detailed view of one message. The list includes several alerts from 'noreply@qualys.com' with subjects like 'ITAM Alert MApper regression' and 'AWS Asset [Cloud Instance only]'. The detailed view shows the following content:

```

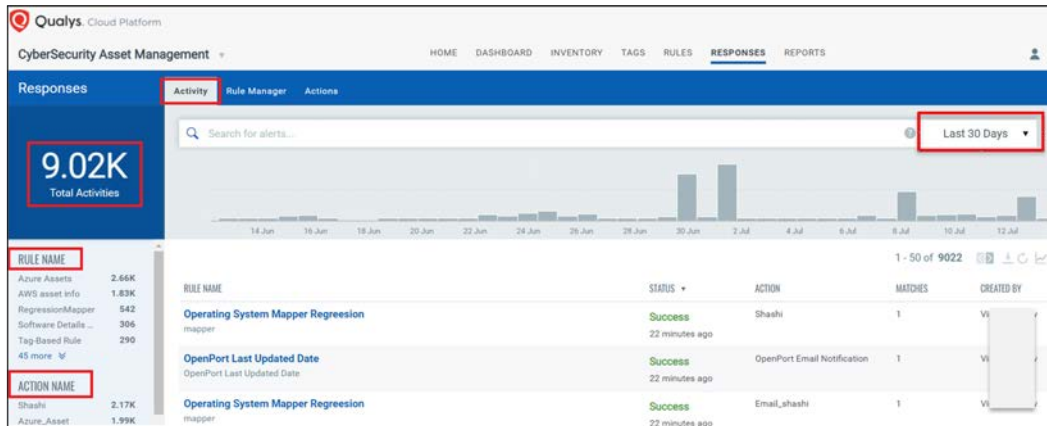
From: noreply@qualys.com <noreply@qualys.com>
Subject: ITAM Alert MApper regression
To: Me

Alert for Asset create and updated
asset.assetID : 8779050
asset.created : 1622122157000
asset.lastUpdated: 1626126913997

```

The illustration above is for an email type alert action.

3. Monitor all the alerts in Activity Tab → Monitor alerts that were sent after the rules were triggered. Users can monitor all the action events in this tab.



# Vulnerability Management

Qualys VMDR and CSAM provide numerous tools and features for working with vulnerabilities, including dynamic Widgets and Dashboards, search and query tools, and the “Prioritization Report.”

## CSAM

While vulnerability findings can be viewed from multiple Qualys applications, CyberSecurity Asset Management also provides some response capabilities.

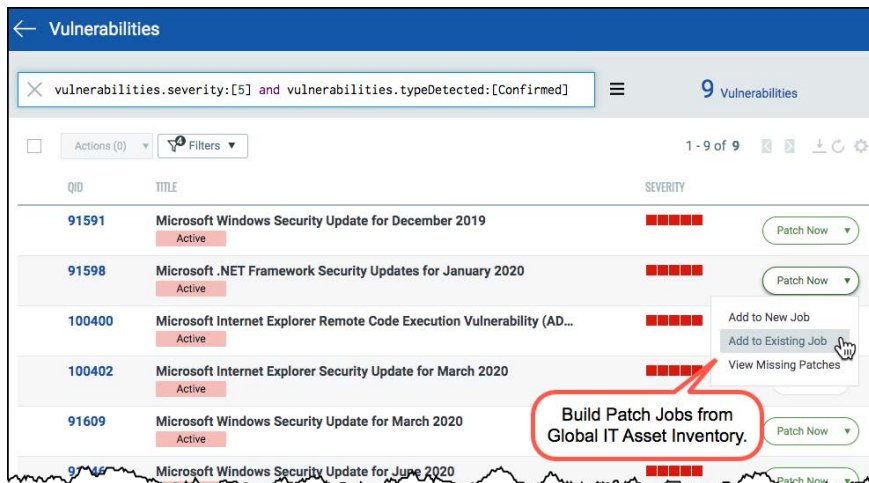
When viewing asset details from within the CSAM application, vulnerability findings are initially displayed graphically.



Qualys severity levels rank the potential impact or outcome of a successful vulnerability exploit. A “Severity 5” vulnerability is the most urgent, while a “Severity 1” vulnerability is the least urgent.

Specific vulnerability details can be quickly displayed with a click of your mouse.

Patches for selected vulnerabilities can then be added to a new or existing patch job.



In the CSAM application, patching and response tasks are performed “host-by-host.” To deploy patches pervasively (for a large number of assets), the tools in VMDR and PM provide a better solution.

## VMDR

Once required assessment data is collected from Qualys scanners and agents, the VULNERABILITIES section of Qualys VMDR, displays your complete list of discovered vulnerabilities along with powerful search and query capabilities.

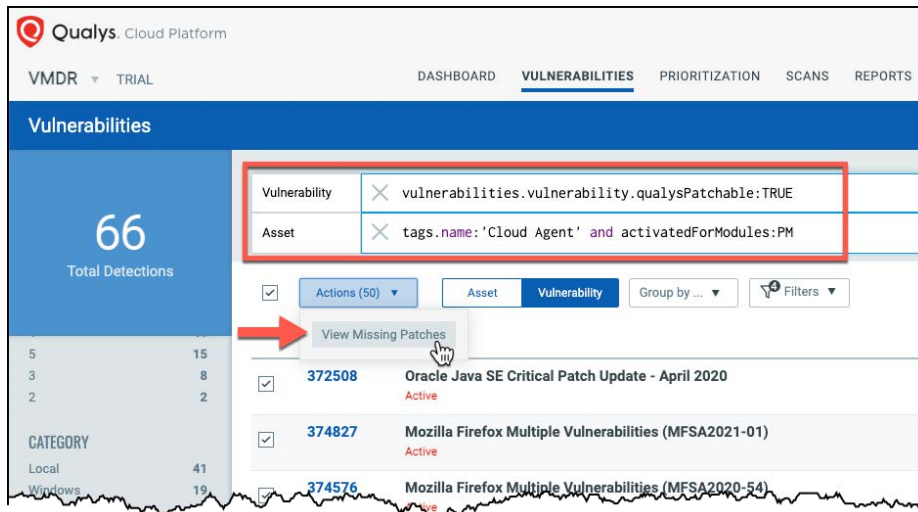
Patch Jobs can be quickly and conveniently created for a specific list of high-risk vulnerabilities and assets, allowing you to deploy patches, based upon the vulnerabilities they actually fix.

**Click the following URL to view the “Vulnerability Findings” tutorial:**



Lab 10 - <https://ior.ad/7SGa>

After selecting one or more patchable vulnerabilities, click the “View Missing Patches” option, to build the list of required patches that are missing.



Not all vulnerabilities are patchable. Patchable vulnerabilities must meet the following conditions:

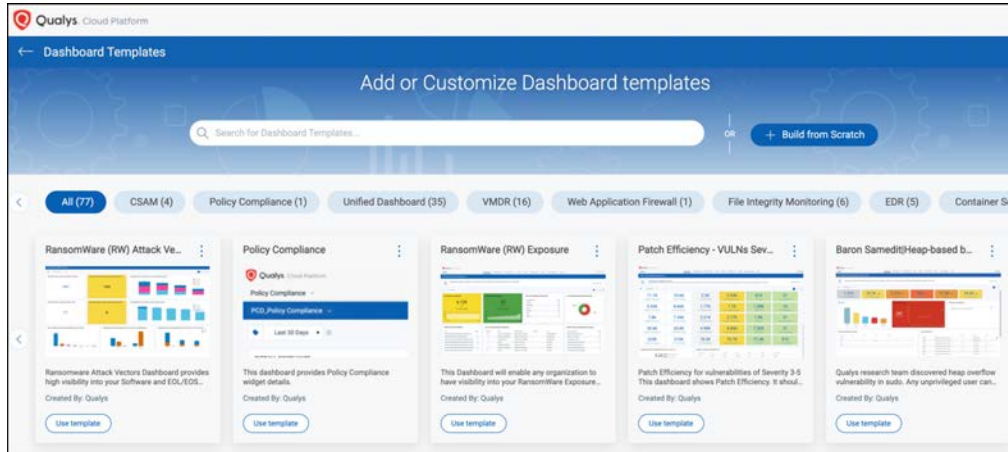
- Detected vulnerabilities must be associated with one or more patches found in the PM Patch Catalog (*vulnerabilities.vulnerability.qualysPatchable:TRUE*).
- Detection Host must be running the Qualys Cloud Agent (*tags.name:'Cloud Agent'*).
- Cloud Agent must have the PM module activated (*activatedForModules:PM*)

The Qualys Cloud Agent performs the “Patching” function for the Qualys Platform.

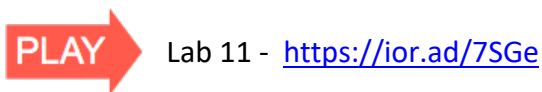


# Dashboards & Widgets

Continuously monitor assets and vulnerabilities with any number of “out-of-box” Dashboards or build your own custom Dashboards and Widgets.



Click the following URL to begin the “Dashboards & Widgets” tutorial:



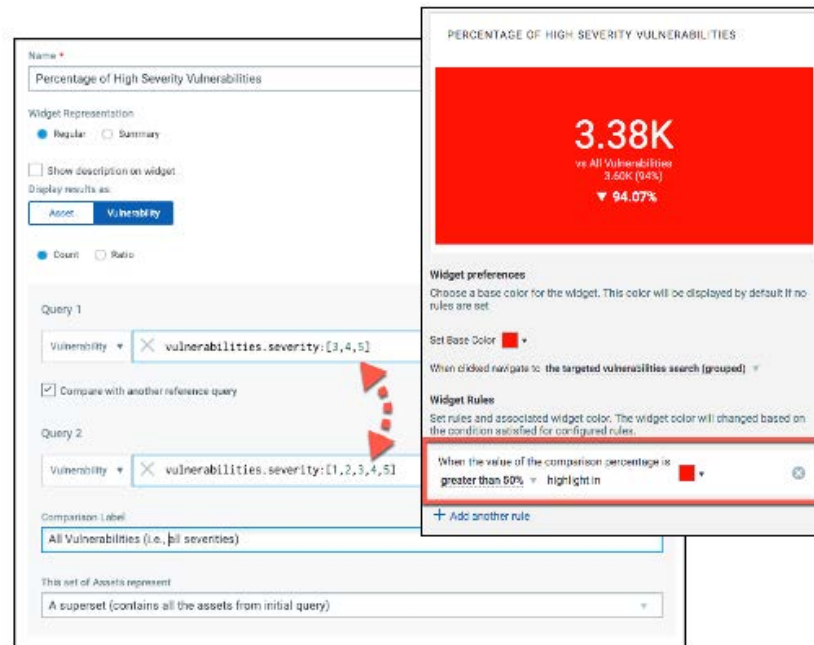
## Widget Types

Widgets are designed to display query results graphically. There are four different graphic options:



Widgets are automatically updated to reflect changes in your asset data and findings.

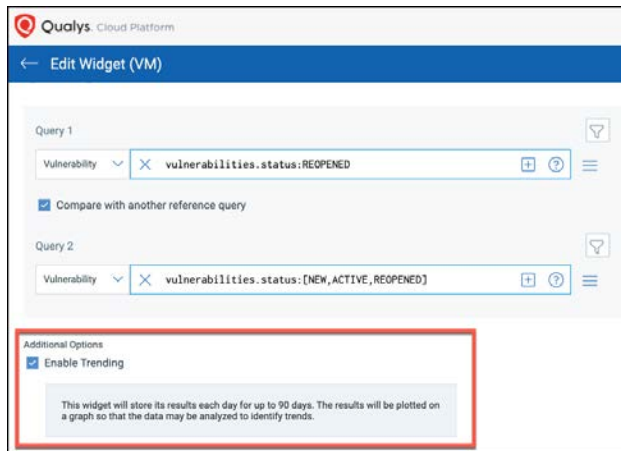
The “count” widget can be configured to change color, as changes to assets and vulnerability findings reach specific thresholds or special conditions.



A “reference” query in the count widget, is useful for comparing the “initial” query’s result set to some type of control or benchmark. The difference between the result sets of both queries is represented as a percentage.

In the example above, HIGH severity vulnerabilities (Sev. 3, 4, 5) are presently about 94% of ALL vulnerabilities (Sev. 1, 2, 3, 4, 5). The “count” widget is configured to change from its base color to red, when this percentage is greater than 50 percent.

Count widget types have the option to Enable Trending. When enabled, widgets can store trend data for up to 90 days.

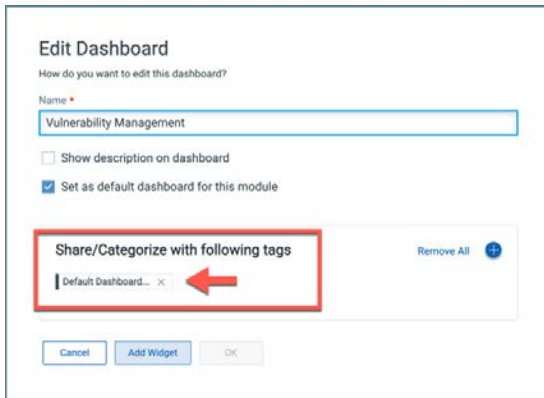


A trend line plotted on a graph will be added to the other information normally displayed in the widget.

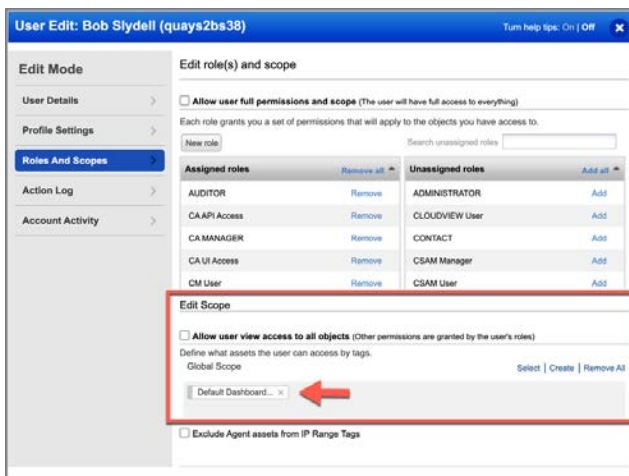


The graphic perspective provided by the trend line will make it easier to visualize swings in momentum and to anticipate critical thresholds and milestones.

You can add one or more Asset Tags to a Dashboard through the Dashboard Editor.



The “Default Dashboard Access Tag” is created by Qualys.



Share dashboards with other Qualys users by assigning “dashboard” tag(s) to their accounts.

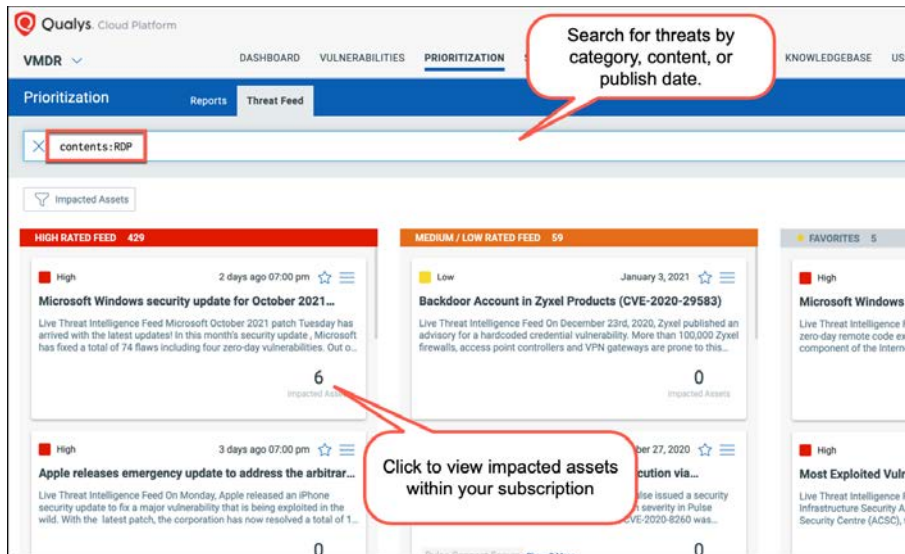
For more information and details on Dashboard and Widget capabilities, check-out the Qualys “Reporting Strategies & Best Practices” training course ([qualys.com/learning](https://qualys.com/learning)).

# Threat Detection & Prioritization

Use the VMDR Prioritization report to automatically prioritize the riskiest vulnerabilities for your most critical assets – reducing potentially thousands of discovered vulnerabilities, to the few that matter.

## VMDR Threat Feed

The Threat Intelligence Feed provides a key element to the Prioritization Report. Focus remediation efforts on high-severity vulnerabilities with known or existing threats.



This Threat Intelligence Feed is provided by Qualys Threat & Malware Labs, along with several other exploit and malware sources.

### Other Threat Feed Sources

#### Exploit Sources

Source Type	Data Type
Core Security	PoC Exploits mapped to CVEs
Exploit-DB	PoC Exploits mapped to CVEs
Metasploit	PoC Exploits mapped to CVEs
Contagio Dump	Exploit Kits mapped to CVEs
Immunity - Agora - Dsquare - Enable Security - White Phosphorus	PoC Exploits mapped to CVEs
Google Project Zero	Zero-Days mapped to CVEs

#### Malware Sources

Source Type	Data Type
Reversing Labs	CVEs associated with malware
Trend Micro	Malware names associated with CVEs
McAfee	Ransomware mapped to CVEs

- Qualys Threat Protection leverages exploit and malware data from multiple sources.

# Prioritization Report

By correlating vulnerability information with threat intelligence and asset context, The Prioritization Report will help you to “zero in” on your highest risk vulnerabilities and quickly patch them.

The VMDR Prioritization report :

- Guides you to target and quickly patch your highest risk vulnerabilities.
- Helps you find the specific patch to fix a particular vulnerability.
- Allows you to quickly identify and remediate the vulnerabilities that are most likely to get exploited.
- Empowers security analysts to pick and choose the relevant threat indicators for your specific and unique organization.
- Provides an integrated workflow that reduces the time between vulnerability detection and patch deployment.

**Click the following URL to begin the “VMDR Prioritization Report” tutorial:**



Lab 12 - <https://ior.ad/7SH3>

After selecting one or more Asset tags to specify report context, prioritization options are provided in three categories:

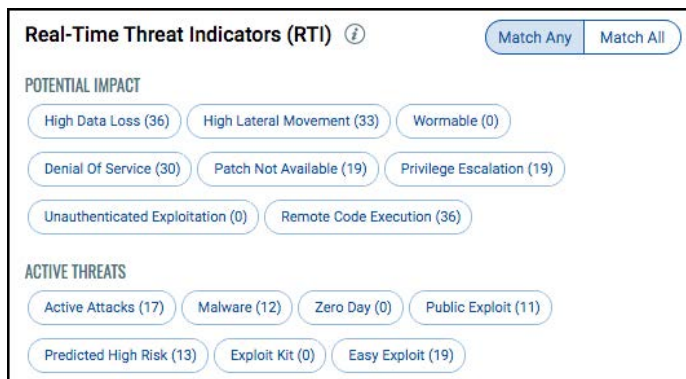
## Age

Prioritize vulnerabilities by their age. Detection age is the number of days since the vulnerability was first discovered (e.g., by a scanner or cloud agent). The “Vulnerability” option will distribute vulnerabilities by actual or KnowledgeBase age.



## Real-Time Threat Indicators (RTI)

Prioritize vulnerabilities by their known and existing threats.



Combine multiple threat indicators, using the “Match Any” or “Match All” operators. Current Real-time Threat Indicators are:

**High Data Loss** - Successful exploitation will result in massive data loss on the host.

**High Lateral Movement** - After a successful compromise, attacker has high potential to compromise other machines in the network.

**Denial of Service** - Successful exploitation will result in denial of service.

**Patch Not Available** - Vendor has not provided an official fix.

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

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

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

**Actively Attacked** - Active attacks have been observed in the wild. This information is derived from Malware, Exploit Kits, acknowledgment from vendors, US-CERT and similar trusted sources.

**Malware** - Malware has been associated with this vulnerability.

**Zero Day** - Active attacks have been observed in the wild and there is no patch from the vendor. If a vulnerability is not actively attacked this RTI will not be set (even if there is no patch from the vendor). If a patch becomes available Qualys will remove the Zero Day RTI attribute.

**Public Exploit** - Exploit knowledge is well known and working exploitation code is publicly available. This attribute is set for example when PoC exploit code is available from Exploit-DB, Metasploit, Core, Immunity or other exploit vendors. While potentially increasing the probability of attack, this RTI does not necessarily indicate that active attacks have been observed in the wild.

**Predicted High Risk** - Leverages machine learning to determine if a presently non-exploited vulnerability should be prioritized.

**Easy Exploit** - The attack can be carried out easily and requires little skills or does not require additional information.

**Exploit Kit** - Exploit Kit has been associated with this vulnerability. Exploit Kits are usually cloud based toolkits that help bad actors to identify vulnerable browsers/plugins and install malware. Search for Exploit Kits by name like Angler, Nuclear, Rig and others.

**Wormable** - The vulnerability can be used by “worms” – to spread without user interaction.

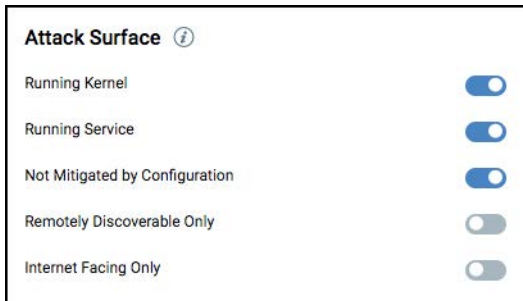
**Solorigate Sunburst** - Solorigate Sunburst has been associated with all the CVEs used by FireEye's Red Team tools to test the security of their client environments and compromised versions of SolarWinds Orion.

**Ransomware** - This vulnerability has been exploited in attack vectors where ransomware has been deployed. In other words, this vulnerability is associated with known ransomware.



## Attack Surface

Attack Surface options provide additional context for the assets in the Prioritization Report.



Use Attack Surface options to further refine the context already provided by the included Asset Tags.

**Running Kernel** - It's possible that multiple kernels may be detected on the same Linux host. Toggle this filter On to filter out kernel-related vulnerabilities that are not exploitable because they were found on a non-running kernel.

**Running Service** - Toggle this filter On to filter out service-related vulnerabilities that are not exploitable because they were found on a non-running port/service.

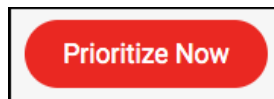
**Not Mitigated by Configuration** - We may detect software on a host that is considered vulnerable, however there's a specific configuration present on the host that makes it not exploitable. Toggle this filter On to filter out config-related vulnerabilities that are not exploitable due to host configuration.

**Remotely Discoverable** - Only Toggle this filter On to only include vulnerabilities that can be detected by a scanner using remote (unauthenticated) scanning.

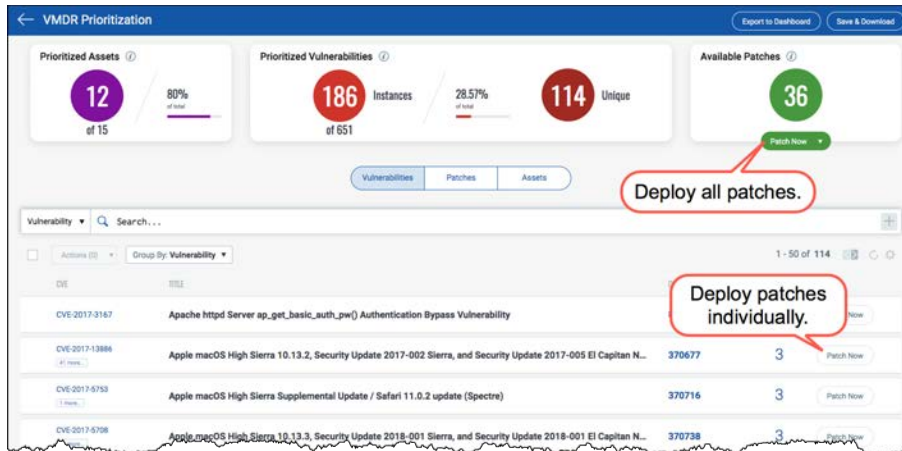
**Internet Facing Only** - Toggle this filter On to include assets with IP addresses that could be exploitable. Our system tag named Internet Facing Assets includes a range of pre-defined IP addresses. We automatically tag assets that matches this pre-defined IP address range in the tag.

To view the complete range of IP addresses that are included in the Internet Facing Assets system tag, go to AssetView app, navigate to Assets > Tags and then select Internet Facing Assets tag. From the quick-action menu, select View and then click Tag Rule in the View mode to view the complete list of IP addresses defined in the tag.

Once your priority options have been selected, click the "Prioritize Now" button.



The displayed assets, vulnerabilities and patches will reflect the priority options you specify.



As you continue to make adjustments to the priority options, the displayed vulnerabilities and patches are automatically adjusted. Patches can be deployed individually or all at once.

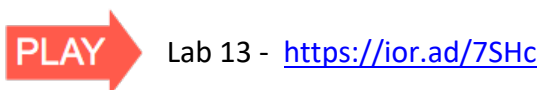
## Zero-Touch Patch Jobs

Select the “Zero-Touch Patch Job” option from the VMDR Prioritization Report.

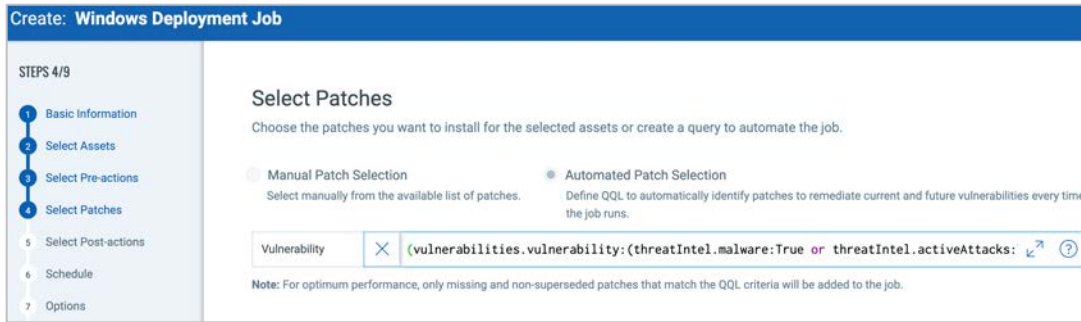


- Automates the selection of patches for recurring deployment jobs
- Patches are selected using QQL
- Patches meeting the query condition are included in scheduled deployment jobs (daily, weekly, monthly)

**Click the following URL to begin the “Zero-Touch Patch Job” tutorial:**



Patches will be expressed as query conditions.



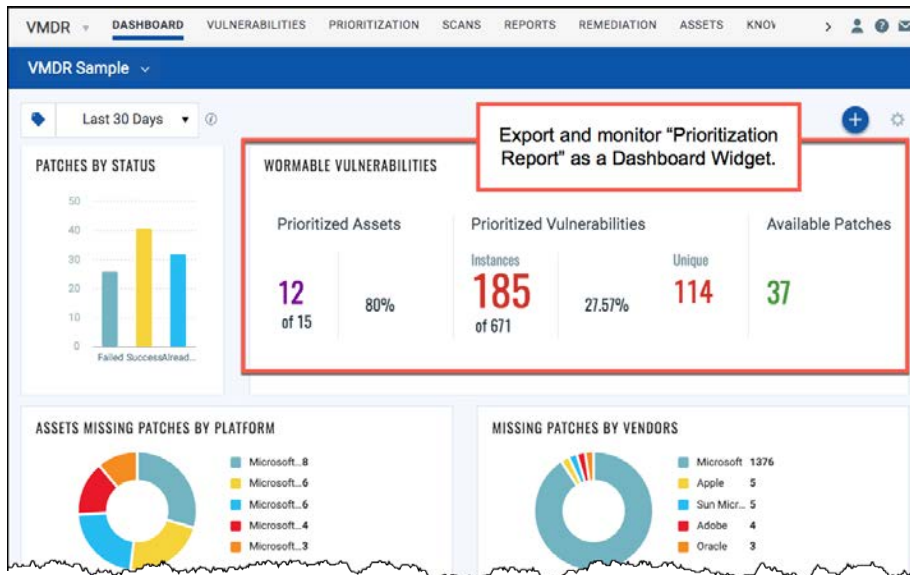
The query is generated from the options (Age, RTIs, and Attack Surface) selected in the Prioritization Report.

## Export to Dashboard

Export the results of any VMDR Prioritization Report as a Dashboard Widget.



Results will be continuously updated within the Widget.



# Patch Management

Along with the help of Qualys Cloud Agent, the Patch Management application provides the patch response functionality in VM DR.

## Deployment Job

While a patch assessment is useful for providing a list of “installed” and “missing” patches, “Deployment Jobs” perform the tasks of actually installing patches to host assets.

**Click the following URL to view the “Patch Deployment Job” tutorial:**



Lab 14 - <https://ior.ad/7SHt>

Before creating any job, you’ll need to add “patchable” agent hosts to the “Licenses” tab (within the CONFIGURATION section of the Patch Management application).

The screenshot shows the Patch Management application interface. The top navigation bar includes 'Patch Management', 'DASHBOARD', 'PATCHES', 'ASSETS', 'JOBS', and 'CONFIGURATION'. The 'CONFIGURATION' section is active, and the 'Licenses' tab is selected. The main content area is titled 'License Consumption' and features a 'Patch Management' card with a 'Total Consumption' indicator showing 2 of 10 licenses used (100%). Below this is a 'License Details' section showing 10 licenses purchased and 2 licenses used. The 'Select assets for patch management' section includes an 'Include Assets Tags' input field with 'PM Lab' selected, and a 'Select Tags' button. There are also 'Reset' and 'Save' buttons at the bottom.

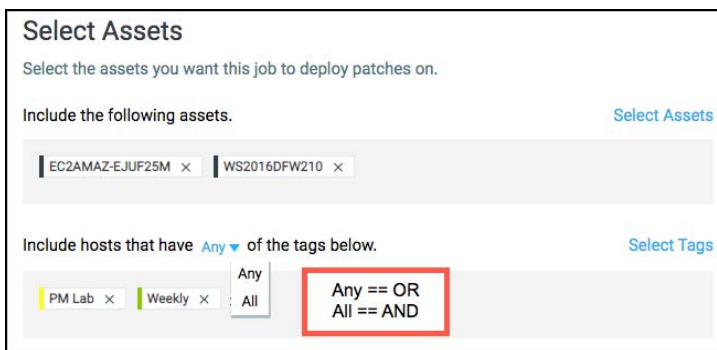
Use Asset Tags to include host assets for license consumption. The “Total Consumption” indicator is updated with the number of agent hosts labelled with the tag(s) included.

## Create Deployment Job

You can create a “Deployment Job” for agent host assets that are missing patches.

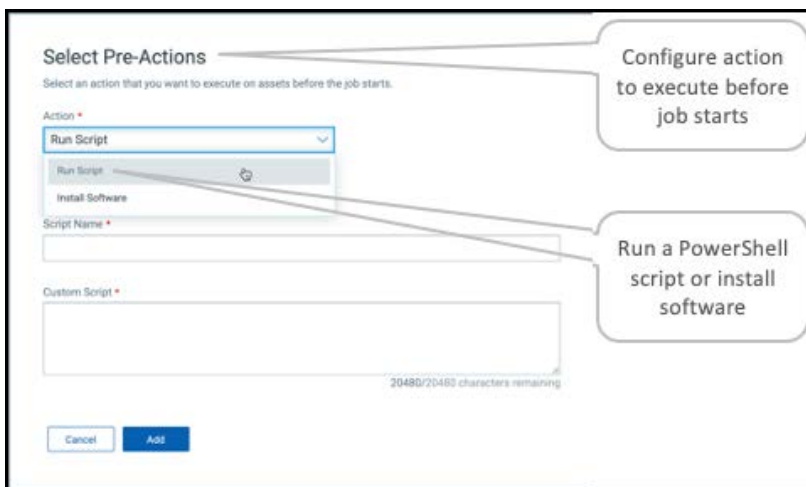


While it is common to build a job from the JOBS section (of the PM application) jobs can also be created within the PATCHES and ASSETS sections.

The screenshot shows the 'Select Assets' form. It has a title 'Select Assets' and a subtitle 'Select the assets you want this job to deploy patches on.' Below this, there are two sections: 'Include the following assets.' with a 'Select Assets' link, and 'Include hosts that have Any of the tags below.' with a 'Select Tags' link. The 'Any' radio button is selected. A red box highlights the 'Any == OR' and 'All == AND' options.

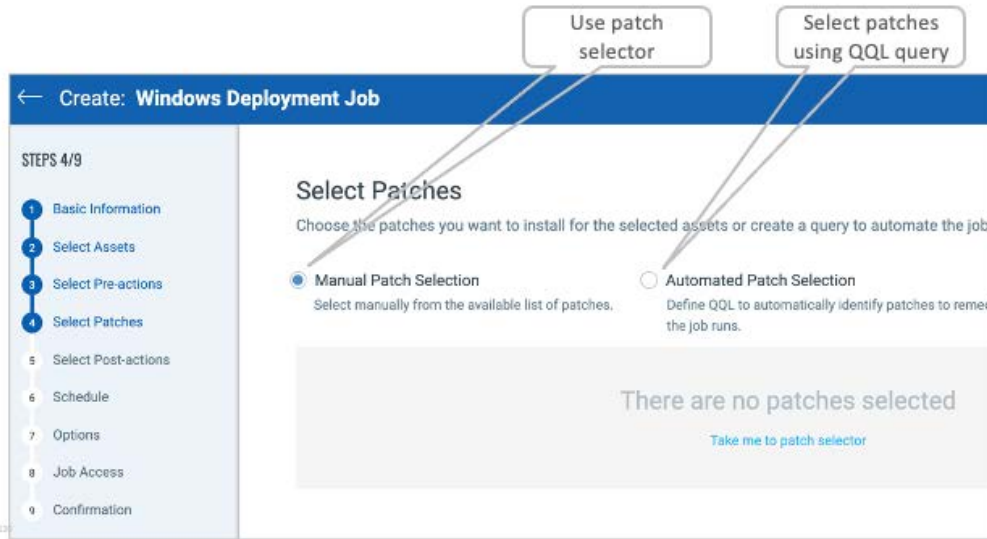
You can add assets to a job by Host Name or by Asset Tag. If you include more than one Asset Tag, be sure to select an appropriate Boolean operator (i.e., Any or All).

Run a PowerShell script or install software, before the patch job begins.

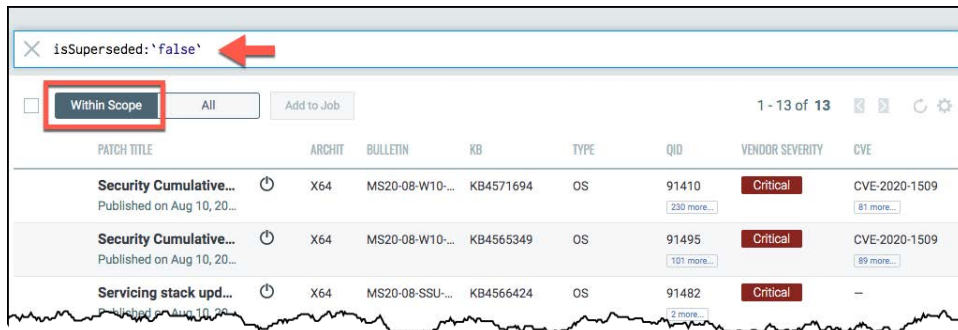
The screenshot shows the 'Select Pre-Actions' form. It has a title 'Select Pre-Actions' and a subtitle 'Select an action that you want to execute on assets before the job starts.' Below this, there are two sections: 'Action' with a dropdown menu showing 'Run Script' and 'Install Software', and 'Script Name' with a text input field. A red box highlights the 'Run Script' option. Two callout boxes are present: one pointing to the 'Run Script' dropdown with the text 'Configure action to execute before job starts', and another pointing to the 'Script Name' field with the text 'Run a PowerShell script or install software'. At the bottom, there are 'Cancel' and 'Add' buttons.


Additionally, Post-Actions can be configured to execute at the completion of the patch job.

Use the “Manual Patch Selection” option to select patches individually from the Patch Catalog.

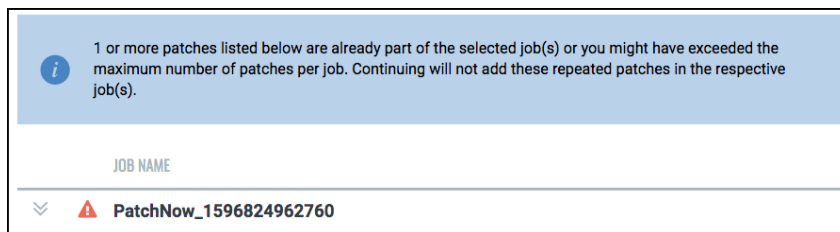


By default, the “Patch Selector” displays patches that are “Within Scope” of the host asset(s) your job is targeting.



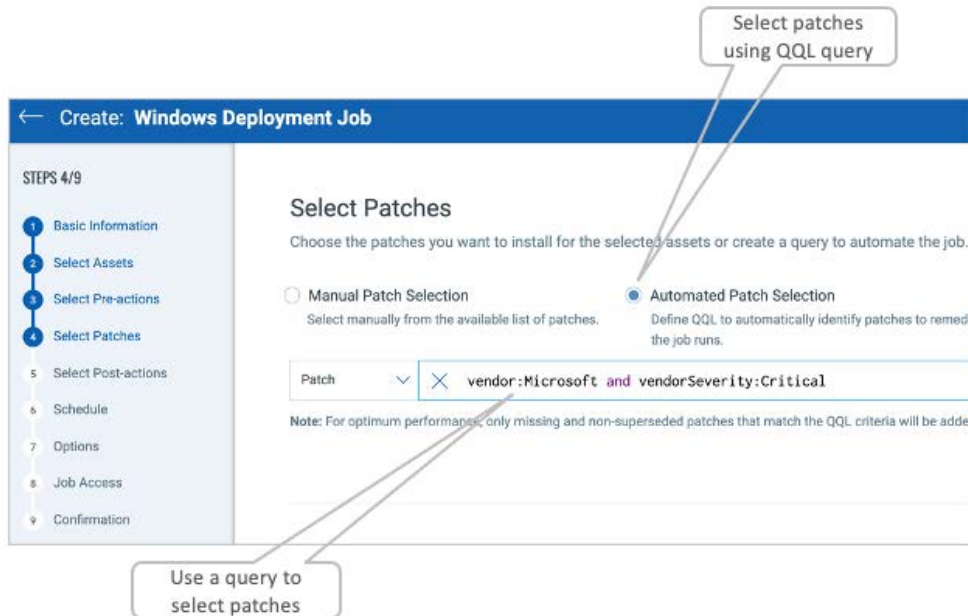
For greater patching efficiency, consider selecting patches that have NOT been superseded (“isSuperseded:false”) to eliminate older, redundant patches. Patches that display the  symbol will require a reboot.

If you attempt to add patches (to an existing job) that are already included, you will receive a warning message similar to the one below:



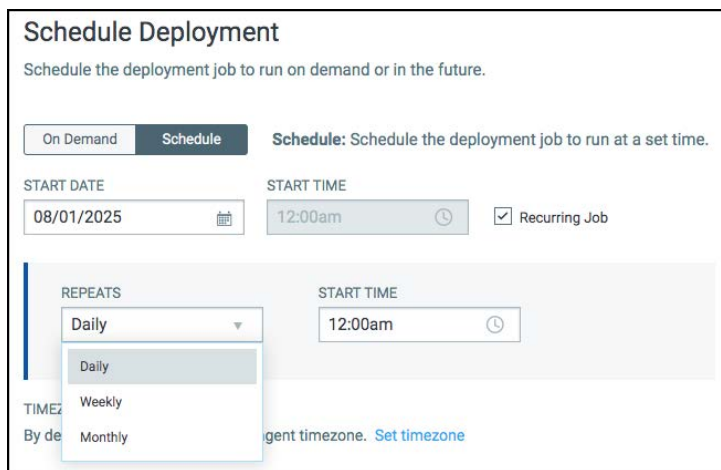
Duplicate patches will not be added to a job.

Alternatively, with the “Automated Patch Selection” option, patches can be selected using a query.



One or more conditions within the query will decide which patches get included in the job.

You can run jobs on demand, or you can schedule your jobs to run at a future date and time.




Schedule jobs to run once, or to recur on a daily, weekly or monthly basis.

You have the option to configure a “Patch Window” (i.e., “Set Duration” option), to restrict patching to a specific time frame.



**Patch Window**  
 You can configure a patch window to run the deployment job only within a particular time frame.

None
  Set Duration 


**Note:** Setting this will restrict the agent to complete the job within the specified patch window (e.g., start time + 6 hrs). The job gets timed out outside this window.

Patch Window

A host will display the “Timed out” status, if its installation does not start within the specified patch window. All other hosts that started within the specified window, will be allowed to finish.

Select the “None” option to give Cloud Agent as much time as it needs to start and complete the job.

The Deployment and Reboot Communication Options, allow you to specify the type of “pop-up” messages end-users will receive, before, during and after job deployment.

**Pre-Deployment**   ON

Display message to users before patch deployment starts.  
 (If no user is logged in, deployment process starts per job schedule)


TITLE

MESSAGE

DEFERMENT: NUMBER OF DEFERMENTS:

Remind again in    times

The “Deferment” settings provide active end-users the option to postpone the start of a job and to postpone a system reboot (if required).

**Reboot Request**   ON

Show a message to users indicating that a reboot is required.  
 (If no user is logged in, the reboot will start immediately after patch deployment)

TITLE

MESSAGE

DEFERMENT: NUMBER OF DEFERMENTS:

Remind again in    times



If no user is logged-in, patching will begin as scheduled and rebooting will start immediately following patch deployment.

### Additional Job Settings

**Enable opportunistic patch download**

The agent attempts to download patches before a scheduled job runs.

The option to “Enable opportunistic patch downloads” potentially allows scheduled jobs to save time by attempting to download patches, prior to job execution.

Use the “Quick Actions” menu to view the progress of any job.

STATUS	NAME	CREATED BY	SCHEDULE	PATCHES	ASSET COUNT			TAGS
					ASSETS	TAGGED ASSETS	TAGS	
Disabled	<b>On Demand</b> Install Job	2tw81 13, 2020	On-demand	15	0	3	PM Lab	
Disabled	<b>Scheduled - Run Once</b> Install Job	2tw81 13, 2020	Once, Nov 10 2020 12...	7	1	0	-	
Enabled	<b>Recurring - Monthly</b> Install Job	2tw81 13, 2020	Monthly on Second T...	5	3	0	-	

Verify the status of each host targeted.

## Job Status

Status	Description
Canceled – Blackout	Patch deployment job is canceled on the asset due to blackout window
Completed	Patch deployment job is completed on the asset
Downloaded	Patch file is successfully downloaded on the asset
Downloading – failed	Patch failed to download on the asset
Not licensed	Job manifest cannot be sent as the asset does not have PM license
Job started	Agent has started the job
Job resumed	Asset is restarted and agent has resumed the job
Job failed	Agent encountered an error while executing the job
Patching	Patch job is running on the asset
Pending	Patch job is pending for execution on the asset
Pending reboot	Reboot activity is pending for the asset
Rebooted	Asset is restarted after patch installation
Timed out	Job is timed out

Assets and patches can be added to a “Recurring” job, both before and after it is “Enabled.” Jobs that run only once, cannot be updated once they are enabled.

Once patch deployment is complete, another patch assessment scan will begin automatically and the number of missing and installed patches will be updated for the affected host(s).

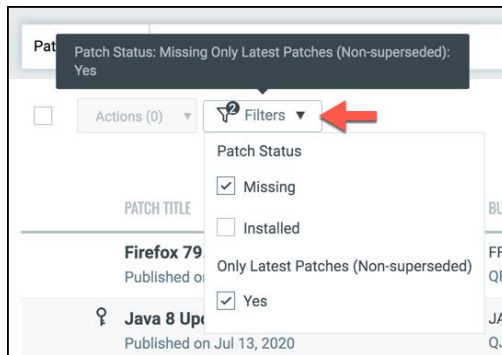
# Patch Catalog

The Patch Catalog contains tens of thousands of OS and application patches. Presently you can add up to 2000 patches to a single job.

**Click the following URL to view the “Patch Catalog” tutorial:**



By default, only the latest (non-superseded) and missing patches are displayed. This is done to help you focus on the essential patches required by your host assets.



To view ALL patches in the catalog, remove (uncheck) the “Missing” and “Non-superseded” filter options and then click somewhere outside of the “Filters” drop-down menu (to refresh the displayed patches).

APP FAMILY	
Windows	1.25K
Office	48
.Net	34
Office Viewer	25
Internet Explorer	16
⌵ 39 more	
VENDOR	
Microsoft	1.38K
Sun Microsystems	5
Apple	5
Adobe	4
Oracle	3
⌵ 21 more	
CATEGORY	
Security Patches	882
Non-Security Pat...	458
Security Tools	80
TYPE	
OS	1.25K
Application	170
VENDOR SEVERITY	
None	526
Important	493
Critical	377
Moderate	22
Low	2
REBOOT REQUIRED	
true	1.42K

Quickly search for specific groups of patches in the Patch Catalog, using the faceted search pane on the left.

Search for patches by:

- Application Family
- Vendor
- Category
- Type
- Vendor Severity
- Reboot Requirements

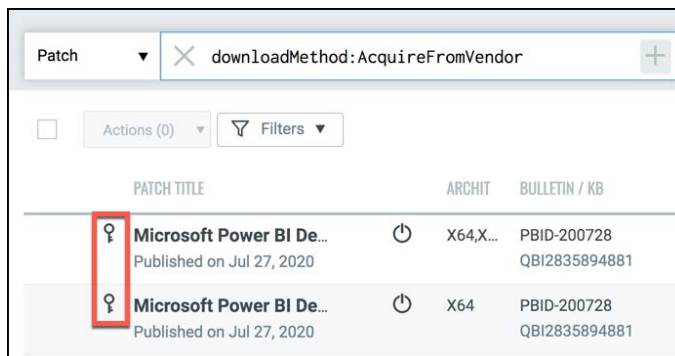
For more sophisticated queries, use Query Tokens and the Qualys Query Language (QQL) in the “Search” field, at the top of the Catalog.

Any query entered into the “Search” field will be affected by the current filtering options. Be sure to verify the filter options, prior to submitting queries.

Patches identified with the “key-shaped” icon, cannot be downloaded by Qualys’ Cloud Agent. This is often the case, when patches first require credentials prior to downloads.

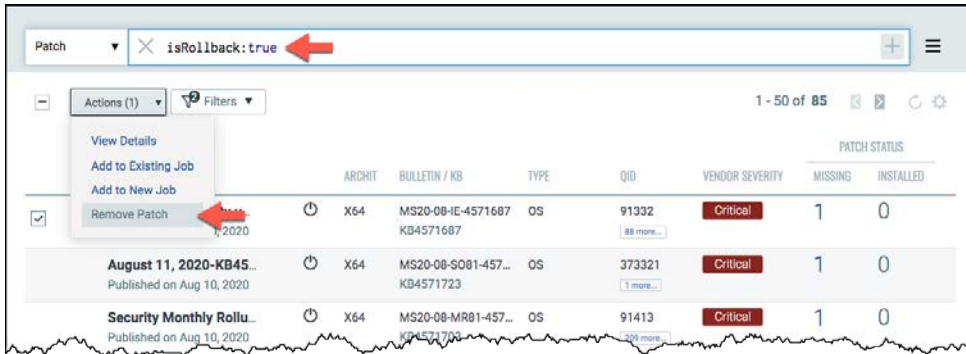
Type the following query into the “Search” field and press the “Enter” key:

```
downloadMethod:AcquireFromVendor
```



If attempting to add these patches to a job, they will not be included.

The “Rollback” patches in the catalog are candidates for an Uninstall Job. Not all patches can be uninstalled.



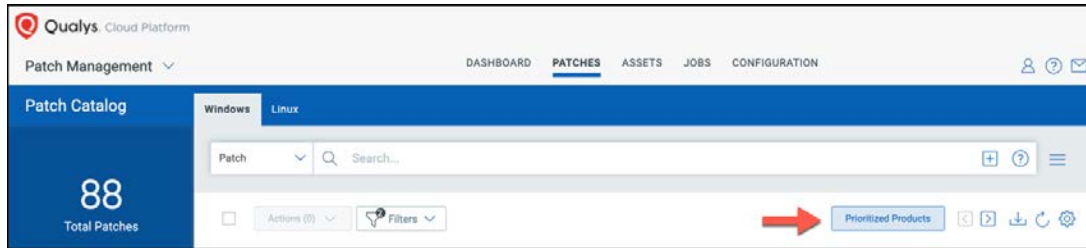
Use the 'isRollback' query token to list rollback patches:

```
isRollback:true
```

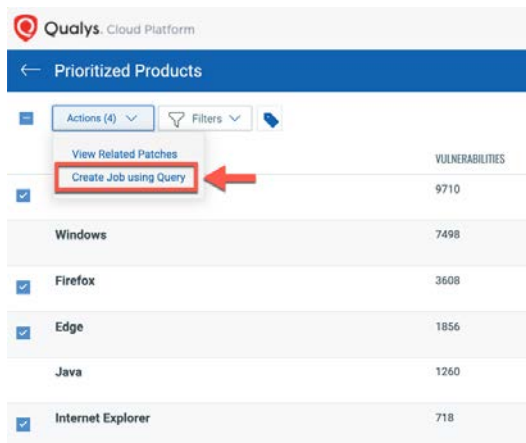
Patch jobs can also be created and updated from within the PATCHES section of the Patch Management application.

# Prioritized Products List

Click the “Prioritized Products” button (in the PATCHES section) to view a list of your software applications and products, ranked by the number of vulnerabilities each product added to your environment.



Products at the top of the list are associated with the greatest number of vulnerabilities. The Qualys Platform provides the unique capability to target and deploy patches based on the relationship between products, patches and their associated vulnerabilities. In some cases, applications that contribute a large number of vulnerabilities, are common client applications that are relatively resilient to the impact of frequent patching.



Select specific applications from the list and use the “Actions” button to “Create Job using Query.”

A query designed to patch the selected application(s) is constructed automatically (using QQL).

Patch jobs of this type will keep the selected products updated when new patches become available. Achieve “zero-touch” patching by scheduling this job to run daily, weekly, or monthly.

For more assessment and patching details, enroll in the “Patch Management Self-Paced Training” course ([qualys.com/learning](https://qualys.com/learning)).

# VMDR Certification Exam

Participants in this VMDR training course have the option to take the VMDR Certification Exam. This exam is provided through our Learning Management System ([qualys.com/learning](https://qualys.com/learning)). To take the exam, candidates will need a “learner” account.

Qualys. Training & Certification  
[qualys.com/learning](https://qualys.com/learning)

Login

Please log in to the Qualys training site. First time users need to create an account.

\*Required Field

\*Username:

\*Password:

Sign In


Forgot your password? Request a new account. 


If you would like to take the exam, but do not already have a “learner” account, click the “Request a new account” link (above), from the “Qualys Training & Certification” login page ([qualys.com/learning](https://qualys.com/learning)).


Once you have created a “learner” account (and for those who already have an account), click the following link to access the “QSC 2021 VMDR” course page:

<https://gml.geolearning.com/geonext/qualys/scheduledclassdetails4enroll.geo?&id=22511237827>

Qualys. Training & Certification

My Home ▾ Learner Information ▾ 

Course Catalog: Class Details 



Course: Qualys VMDR from Asset Management to Remediation - QSC 2021 

To see how a class below fits into your schedule, click View My Class Schedule.

**CLASS DETAILS: QSC 2021 VMDR LAS VEGAS**

**Course Name:** Qualys VMDR from Asset Management to Remediation - QSC 2021  
**Class Name:** QSC 2021 VMDR Las Vegas  
**Class Code:** 2250729076520210917130358  
**Class Description:** Participants at QSC 2021 in Las Vegas, can access the VMDR certification exam  
**Contact Name:** Phil Niegos  
**Private Class:** Yes  
**Maximum Class Capacity:** 150  
**Class Cost:** \$0.00

Session Name	Location	Classroom	Address 1	Address 2	Times	Instructor(s)
Session 1	Las Vegas - Bellagio	Las Vegas - Bellagio - Classroom A	3600 Las Vegas Blvd. South,	N/A	Monday, November 15, 2021 9:00 AM to 5:00 PM (America/Los_Angeles) (UTC -07:00)	Philip Niegos

From the “QSC 2021 VMDR” course page, click the “Enroll” button (lower-right corner).

After successfully completing the course enrollment, click the “Launch” button, for the Qualys VMDR Exam.

Qualys Training & Certification

My Home - Learner Information -

Qualys VMDR from Asset Management to Remediation - QSC 2021 Close Record

Class Name	Date	Location	Instructor(s)
QSC 2021 VMDR Las Vegas	Monday, November 15, 2021 9:00 AM to 5:00 PM (America/Los_Angeles) (UTC -08:00)	Las Vegas - Bellagio	Philip Niegos

To access a learning activity, select the activity name and click Launch or Open.

Activity Name	Type	Score	Progress	Last Accessed	Action
QSC 2021 VMDR Lab Tutorial Supplement	pdf	N/A	N/A	N/A	Open
QSC 2021 VMDR Slides	pdf	N/A	N/A	N/A	Open
VMDR Exam	Actual Test	N/A	Not Attempted	N/A	Launch

Each candidate is provided five attempts to pass the exam. You may use the course presentation slides and lab tutorial supplement to help you answer the exam questions. You may also use any of the resources within the Qualys UI (such as the “Help” menu) and resources found on the Qualys Community (community.qualys.com) to answer exam questions.

Qualys Training & Certification

My Home - Learner Information -

Qualys Vulnerability Management Detection & Response - QSC 2020 Close Record

Progress: Completed Status: Enrolled Required: No Duration: 6 hours

Class Name	Date	Instructor(s)
VMDR - QSC 2020	Tuesday, November 17, 2020 9:00 AM to 4:00 PM (America/Los_Angeles) (UTC -08:00)	Philip Niegos

To access a learning activity, select the activity name and click Launch or Open.

Activity Name	Type	Score	Progress	Last Accessed	Action
QSC20 VMDR Lab Tutorial Supplement	pdf	N/A	N/A	N/A	Open
QSC20 VMDR Presentation Slides	pdf	N/A	N/A	N/A	Open
Qualys Vulnerability Management Detection & Response (VMDR) Exam	Actual Test	100%	Passed	11/3/2020 7:38:14 PM	Launch

With a passing score of 75% (or greater), click the “Print Certificate” button to download and print your course exam certificate.

# VMDR Course Survey and Trial Account

Please lets us know what you think about the “QSC 2021 VMDR” training course.  
Survey - <https://forms.office.com/r/rsy0Aja6Xz>

Would you like a VMDR trial account to practice and experiment with the lessons and topics provided in this course?

Link to Trial - <https://www.qualys.com/forms/vmdr/>

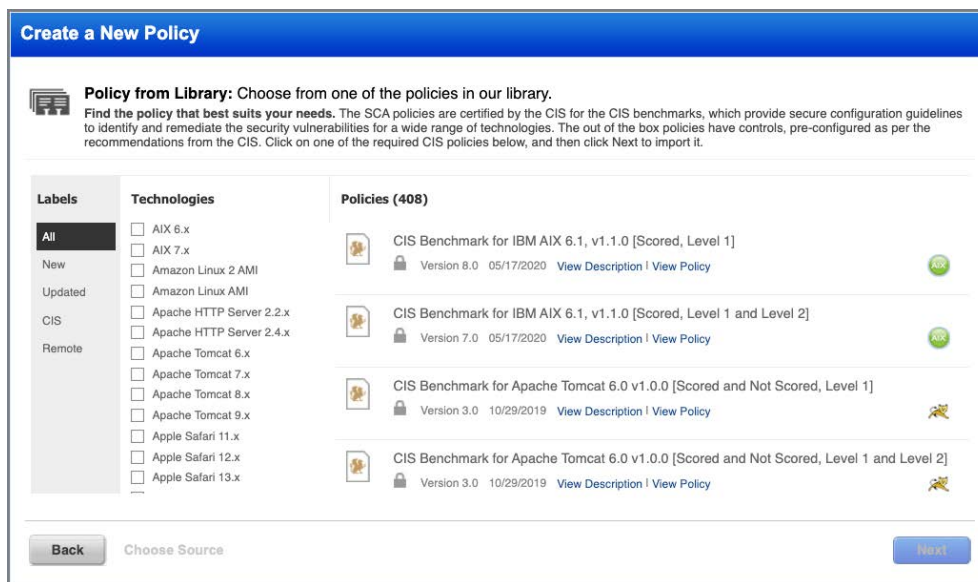


# Appendix A: Additional VMDR Applications

While this “VMDR Overview” training course focuses on four Qualys applications (i.e., CSAM, VM, TP, and PM), there are more VMDR applications that address and mitigate vulnerabilities as well as enforce security policies.

## Security Configuration Assessment (SCA)

Monitor and assess technical security controls and security-related misconfigurations. Qualys Scanners and Agents collect the data points needed to perform host compliance assessments.

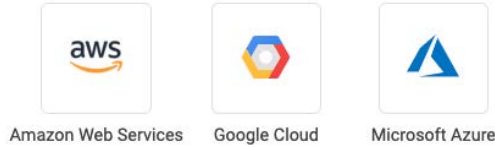


Qualys SCA provides over 400 CIS Benchmark Policies for hundreds of OS and application technologies. All compliance scans are performed using the "Scan by Policy" option.

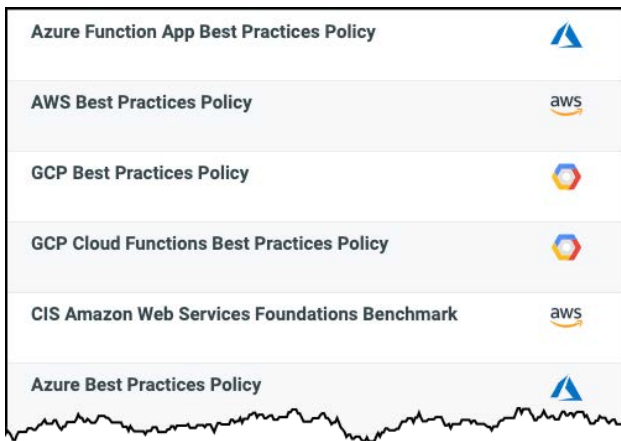
Qualys SCA contains a subset of the tools and features found in the Qualys Policy Compliance application. For more information and details, please see the Qualys Policy Compliance Self-Paced Training Course ([qualys.com/learning](https://qualys.com/learning)).

# CloudView & Cloud Security Assessment (CSA)

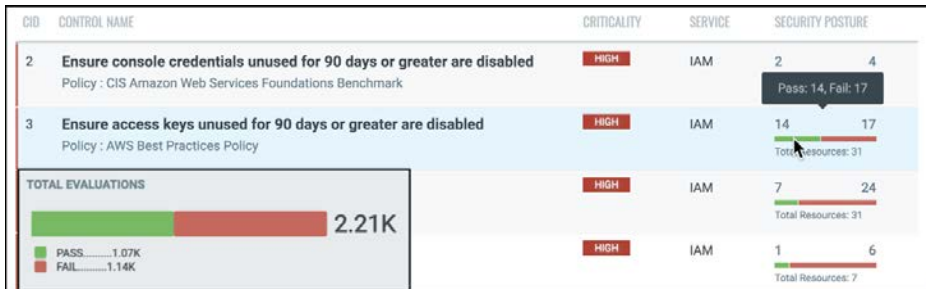
Continuously monitor and assess your PaaS/IaaS resources for misconfigurations and non-standard deployments.



With Qualys Cloud Connectors and the Qualys CloudView application, you can enumerate your cloud instances and collect metadata from your AWS, Google Cloud, and Microsoft Azure accounts:

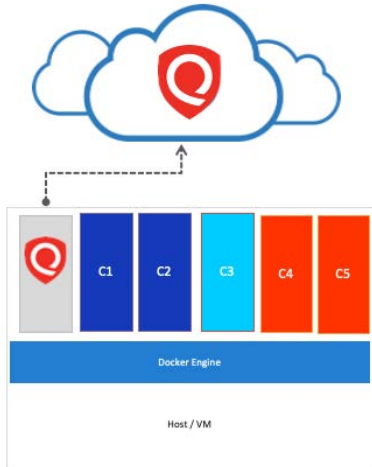


With Qualys Cloud Security Assessment (CSA) you can leverage “out-of-box” policies to assess technical controls and identify security-related misconfigurations, for your AWS, Azure, and Google accounts.



## Container Security (CS)

The Qualys Container Security application uses the same KnowledgeBase as Qualys VM and VMDR, to assess and detect vulnerabilities in Docker images and containers.



Qualys Container Sensor downloads as a Docker image and is installed on a Docker host as a container application, right alongside other container applications.

Presently, there are 3 different types of Container Sensors:

1. A General Sensor will scan images and containers on a single docker host.
2. A Registry Sensor will scan images in public and private Docker registries.
3. A CI/CD Pipeline Sensor (also referred to as a "Build" sensor), scans images within your DevOps CI/CD pipeline projects, allowing you to identify and correct vulnerable images, during the build process. Integrations with Jenkins and Bamboo are presently supported.

Another feature in the Qualys Container Security application is Container Runtime Security, which provides runtime visibility and protection into container applications.

This is achieved by instrumenting images with Qualys Container Security components, to gather functional and behavioural data about the container's running processes; thereby allowing you to create rules and policies that actively block or prevent unwanted actions or events.



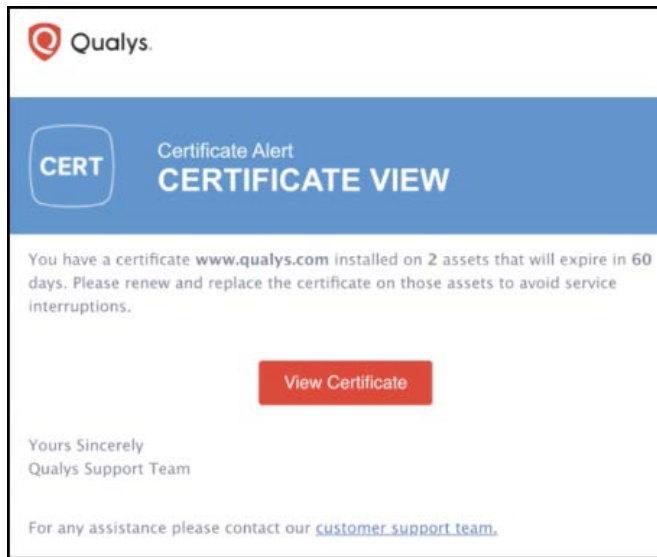
As one example, you could build a policy that prohibits access to sensitive system files, such as the shadow or passwd files on a Linux host.

The instrumentation process places a few binaries into the image at the security layer. This application-native instrumentation process provides complete visibility of the application inside the container. The instrumentation is very lightweight and provides configurable data collection options with low/no impact on application performance.

## CertView (CERT)

Qualys CertView provides visibility into certificates and their configurations, across your network and enterprise architecture (on-premise and cloud-based).

CertView leverages Qualys Scanner Appliances to collect all the certificate, vulnerability and configuration data required for inventory and analysis, helping you to identify and prevent expired and expiring certificates from interrupting business functions.



Qualys CertView also provides the ability to enroll or renew certificates to avoid potential service interruptions.

Certificate Assessment generates certificate instance grades that allow administrators to quickly assess server SSL/TLS configurations.



Certificate Assessment identifies out-of-policy certificates with weak signatures or key lengths and shows you how many certificates were issued by Certificate Authorities (CAs)

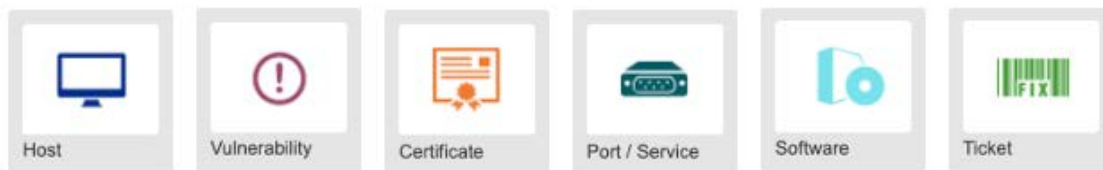
that have been vetted and approved (per your policy) and how many certificates are self-signed or were issued by CAs that have not been authorized to issue certificates in your environment.

For more information and details, please see the Qualys Certificate View video series (<https://www.qualys.com/training/library/certview/>).

## Continuous Monitoring (CM)

Get alerts when new threats and unexpected changes to your hosts are detected, including:

- New hosts detected within your Qualys subscription.
- High severity vulnerabilities and vulnerabilities with known exploits detected.
- New ports and services detected.
- New or unexpected software applications detected
- Expiring or vulnerable SSL certificates
- Remediation tickets that are opened or closed



CM works in tandem with VM/VMDR:

- Deploy Qualys Scanner Appliances and/or activate the VM module for deployed Qualys Agents.
- Schedule frequent or continuous vulnerability scans.

Qualys CM evaluates rules against your most recent vulnerability scans. Alerts are generated as soon as scan results are processed. Certificate rules are evaluated daily, and are not based on scans.

For more information and details, please see the Qualys Continuous Monitoring video series (<https://www.qualys.com/training/library/continuous-monitoring/>).

# VMDR for Mobile Devices

Qualys Secure Enterprise Mobility (SEM) provides visibility into your mobile devices by collecting their inventory and configuration data.

- Android OS Released
  - Android Things
  - Android TV
  - Chrome OS
  - Wear OS
  - iOS Released
  - Mac OS
  - Apple Watch
  - Apple TV
  - Windows 10
- 

Your company's mobile device inventory is added to the Qualys CSAM application, providing you with greater insight into mobile devices that are managed vs. unmanaged (especially when combined to Qualys Passive Sensor).

Qualys vulnerability and compliance assessments help to keep your mobile devices hardened and secure. Vulnerability assessment tests are provided for both OS and applications.

Compliance assessment examples include: passcode not present, encryption status, unauthorized root access (rooted), etc...

With Qualys SEM, you can perform active device operations, like locking a screen or locating a missing device.

# Appendix B: Prioritization Report Use Cases

The VMDR Prioritization Report provides countless ways to combine Asset Context, Vulnerability Age, Real-Time Threat Indicators, and Attack Surface options. Here are a couple use cases to demonstrate different approaches to building Prioritization Reports.

## Databases

Hosts with large data stores are especially impacted by “High Data Loss” vulnerabilities.

*Click the following URL to view the “Prioritization Report Use-Case: Databases” tutorial:*



<https://ior.ad/7SH7>

## Internet Facing Assets

Hosts with public interfaces are at greater risk because of their exposure to the Internet, especially with vulnerabilities that can be exploited without authentication. The risk becomes even more significant if the same host has vulnerabilities that can lead to privilege escalation.

*Click the following URL to view the “Prioritization Report Use-Case: Internet Facing Assets” tutorial:*



<https://ior.ad/7SH8>