VMDR Onboarding Card

A guide for implementing Qualys VMDR

Contents

Purpose *4*

Important Links *5*

Operational and Support Links 5

Training Links 6

1. Start with Scoping *7*

2. Deploy Sensors to Collect Data *7*

3. Organize Assets for Increased Efficiency *7*

4. Communicate Effectively *8*

5. Reduce Risks by Eliminating Vulnerabilities *8*

1. Start with Scoping *9*

2. Deploy Sensors to Collect Data *13*

Scanner Appliances 13

Qualys Scanner Appliance Links 14

External Scanners 16

Adding Scannable Host Assets to Your Subscription *17*

Map Scan 17

Discovery Scan using a Scanner Appliance 17

Adding Cloud Agent Assets to Your Subscription *19*

Cloud Agent Deployment 19

Configuring a Scheduled Vulnerability Scan 21

Top Tips for Scanning Success 22

Merging Agent Records *24*

3. Organize Assets for Increased Efficiency *25*

Things to consider when using Asset Groups **25**

When to use Asset Tags **25**

4. Communicate Effectively *27*

Dashboards **27**

Qualys VMDR TruRisk **27**

Subscription Health **28**

VMDR Reports **30**

Tips for Reporting Success **31**

Account Maintenance **31**

5. Eliminate Risks *33*

Purpose

This document aims to provide a short and sweet battle plan for *Qualys Vulnerability Management Detection and Response (VMDR)*.

This is designed to get you started, provide best practices, point out gotchas, and show easy wins to make you more successful with Qualys.

This document is designed to provide a tool box of reference material and walk you through the essential steps in deploying Qualys Vulnerability Management Detection and Response.

Important Links

Before you go any further, we recommend visiting these pages and bookmarking them—you will use them again!

Operational and Support Links

Find My Platform

This shows you the Qualys platform that your organization uses and its related URLs. You will need these to verify that your scanner appliances and your cloud agent hosts can reach the Qualys platform.

Platform Status

This shows each platform's operational status, maintenance, upgrades, and outages. You can also subscribe to updates about platform status.

Support Portal

This is a useful landing page for docs, training, forums, and managing cases.

How to Collaborate with Support

This article explains all the different ways you can interact with Support, such as calling, chatting, or opening a case.

Opening Cases

This document tells you what you need to provide support to drive faster resolution for your cases.

Documentation

Here is where you can find ALL Qualys documentation.

Vulnerability Detection Pipeline

Browse, filter by detection status, or search by CVE to get visibility into upcoming and new detections (QIDs) for all severities.

Training Links

Qualys Training

This page describes the instructor-led and self-paced training that are available to you (all are provided free of charge).

Public Training Schedule

This shows the public schedule for online, instructor-led classes:

Enroll for Qualys Training

Here you can create a learning account in the Qualys Learning Management System to enroll in any instructor-led or self-paced course.

Qualys Training Video Libraries

Here you will find the video libraries which cover the same topics as the courses.

High-level steps for success

Below are high-level steps for using Qualys in a risk-based approach. They do not cover everything, but they provide an essential checklist for a successful implementation.

In the rest of this document, you will learn how to accomplish each step in more detail.

1. Start with Scoping

You may already have a security policy that states things like:

- Which assets are our most important, and how do we rank their criticality?
- What happens to the organization if they are compromised?
- Which metrics are we using to measure risk and remediation SLAs for each type of asset?

These points will directly impact how you implement VMDR in the remaining steps.

2. Deploy Sensors to Collect Data

Qualys sensors collect data about your environment. This document will walk you through deploying the most common ones: Scanner Appliances, Cloud Agents, and Connectors.

You get more visibility into your organization’s risks by correctly deploying sensors.

3. Organize Assets for Increased Efficiency

This step describes organizing your assets for more effective scanning, prioritization, remediation, reporting, and dashboards. Assets should be organized using *Asset Groups* and *Asset Tags*.

With tags, you will also set a criticality that reflects your organization’s security policy. This criticality score can be set manually or can be synchronized from your CMDB. By setting criticality in the initial implementation, you will effectively set up TruRisk to help you prioritize remediation using a risk-based approach.

4. Communicate Effectively

Learn how to create effective reports and dashboards to communicate risk to stakeholders, including C-level, line-of-business managers, security, and infrastructure operations. You can get started quickly by using report and dashboard templates.

5. Reduce Risks by Eliminating Vulnerabilities

It would be next to impossible to eliminate all cyber security risk to your organization. With *Qualys VMDR*, you can easily prioritize remediation actions to support your organizational objectives.

You will use *Qualys VMDR* to gather vulnerability information, measure, prioritize, and communicate those risks. You can use *Qualys TruRisk Eliminate* and other products to perform remediation actions.

1. Start with Scoping

Scoping is an essential step. It involves understanding the most significant risk factors, where they are and how quickly you must act.

1. Make a list of the organizational assets you'd like to manage in the short and long term.

   Examples: Cloud assets, workstations, internal servers, laptops, External Assets, and air-gapped networks.

2. Note the location of the assets. This will help you deploy scanner appliances more effectively. If you have a network diagram, use it to map out scanner locations. Understanding asset locations will also help with dashboarding, prioritization, and remediation efforts.

3. Rank your assets from most important to least important. What are the most critical assets in your organization? This may already be defined in your organization's security policy. If you are just getting started, consider the following:

   a) The asset value and impact of a successful exploit, such as a potential service outage or data breach.

   b) Is it easy or difficult to restore the system or recover data?

   c) Is the software or system critical to business operations?

   d) Is the software or system complex and integrated with other systems? Would business-critical processes be affected if this asset were to be compromised?

   e) Data: Consider the sensitivity or classification of its data and the potential impact of a data breach or loss.

   f) Data availability: When data is critical to business operations or decision-making processes, the availability of that data becomes a key factor in determining its criticality.

   g) Data redundancy: Data redundancy refers to storing multiple copies of data in different locations or formats to ensure its availability in the event of a loss or outage.

h) Data recovery: When considering the criticality of data assets, evaluating the ability to recover data promptly and the cost associated with doing so is important.

The table below summarizes five levels of asset criticality. You might find it useful to re-word the descriptions to emulate your organization’s SLAs. These criticalities can be configured on your asset tags.

Asset Criticality	**Description**
5	Customer-identified: Critically important based on customer input and system integration data. Compromise could lead to multiple severe consequences for the organization. DMZ Assets, that are exposed to Internet PCI Assets - Credit Card stored assets. Crown Jewel assets. Data Classification - Highly Confidential/Confidential
4	Greater Significance: Integral to core business processes and services. Severe harm to the organization if compromised. Data Classification – Restricted Client Internal - Highly Confidential Unrestricted - External (Non-Sensitive)
3	Typical Infrastructure: Generally important for organizational operations. Significant impact on organizational operations.
2	Default: Moderate level of importance. Low level of impact on organizational operations. Non-Production Test/QA/Sandbox assets

1	Low / Unimportant: Assets with negligible impact on organizational operations. Non-Production Test/QA/Sandbox assets

Notes

You can apply the definitions above to your assets using the Asset Criticality Score within your Asset Tags.

You may find it useful to change the descriptions given above to more closely align with your organizational service level agreements.

4. Define goals and SLAs for your Vulnerability Management program.
   a) Does your organization have a security policy that already defines your vulnerability ranking / prioritization and SLAs for remediation?
   b) What assets will be prioritized? Crown Jewels? External Assets? Internal Servers? Workstations?
   c) What types of vulnerabilities will be prioritized? If you are unsure, Qualys can help with that.
   d) What is your company's SLA for remediation for a given type of asset and vulnerability? For example, an exploitable vulnerability on an external asset should be treated more urgently than on an internal asset.
   e) Don't focus only on critical vulnerabilities.
      a. According to the 2023 Qualys TruRisk Threat Research Report, Initial Access Brokers attack what most organizations ignore.
      b. Have a protocol and follow it.

5. Boost efficiency through automation. This includes:
   - Scanning / Agent Data Collection
   - Reporting
   - Patching

   There will be tips for automating each of these in the coming sections.

2. Deploy Sensors to Collect Data

Determine what sensors you'll use to collect your vulnerability data. This step is vital and a big piece of your deployment.

The sensors that you should initially focus on are these:

- External Scanners
- Cloud Agents
- Scanner Appliances
- Connectors

Scanner Appliances

Scanners are active, point-and-shoot devices deployed across your environment to detect vulnerabilities on assets. These devices interact externally with your assets to identify vulnerabilities during a scan and can even detect them remotely. Scanner appliances are available as both physical and virtual units.

For thorough, defense-in-depth coverage, deploying a full range of scanners, including Qualys Scanner Appliances and Cloud Agents, across all internal (private IP) assets is recommended. This ensures consistent, comprehensive visibility into vulnerabilities across the environment. Scanners collect data only during a scan job, transmitting it to the platform afterward. This means that the accuracy of the data in the platform is dependent on the most recent scan results.

To maintain the most robust and up-to-date vulnerability detection, combining Scanner Appliances and Cloud Agents is advised. The number of Scanner Appliances required will depend on your network's size, configuration, and the frequency of desired scan results.

Once installed, each Scanner Appliance keeps itself updated with the latest vulnerability signatures via its connection to the Qualys Enterprise TruRisk Platform. For this to happen, ensure the scanner appliance can reach your Qualys platform on port 443. For more details, see this web page: https://www.qualys.com/platform-identification/.

Scanner Appliance location

To optimize scanning performance, deploy Scanner Appliances as close to target assets as possible to reduce latency and maximize bandwidth for scanning traffic.

Avoid placing them behind cascading firewalls, load balancers, or across multiple network hops. In high-bandwidth environments, central deployment can also be an effective option.

Firewall Pre-requisites

Ensure your firewalls allow scanners to scan without restrictions for complete vulnerability detection. Scans can be performed from both internal and external networks, so proper inbound and outbound firewall rules must be set (including on Windows firewalls). The scanner must access assets over all relevant TCP and UDP ports.

However, External scans should mirror an attacker's perspective, so no whitelisting or "safelisting" is necessary, and firewalls should block these scans to simulate real-world attack conditions.

We generally do not recommend scanning from the trusted to the untrusted side of a firewall, as this can overload the state table. Instead, segment scans to avoid routing through the firewall.

Ensure inbound ports 10001-10005 (or at least one) are open on assets. These ports are used to merge unauthenticated scan data with authenticated scan data.

Qualys Scanner Appliance Links

1. This video shows you how to install a scanner.
   Deploy Qualys Scanner

2. This video shows you where appliances are best deployed.
   Scanner Appliance Deployment Locations

3. Here are the official user guides for setting up scanners in all different environments.
   Scanner Appliance User Guides

4. These videos provide additional guidance for specific environments.
   Set up a virtual scanner

   Scanner Appliance Deployment in Microsoft Azure

   Scanner Appliance Deployment using the Microsoft Azure CLI

   Scanner Appliance Deployment in GCE

   Scanner Appliance Deployment in AWS (document)

   Scanner FAQ

5. The following articles discuss sizing and capacity in further detail (some in a lot of detail).

Virtual Scanner Appliance Sizing
Scanner appliance capacity required for various scan jobs
Virtual scanner capacity based on hardware
Estimated scan resource usage by scanner during Qualys scans

6. The following guides show you how to configure a scanner appliance when deployed in a segmented network environment, such as when scanner traffic is directed at multiple VLANs or subnets, or where a scanner needs to scan through layer 3 to access assets at layer 2.

Static Route Configuration
VLAN Scanning Guide

7. If you face issues with your scanner appliance, this troubleshooting guide is a good place to start.

Scanner Appliance Troubleshooting

External Scanners

Scanning your assets from the outside using the Qualys External Scanners already associated with your account will give you an “external attacker view” of your vulnerabilities from the outside. In other words, you can automatically launch scans against your external (public IP) assets.

To find the IP ranges used by the Qualys External Scanners:

1. Log into your instance of Qualys VMDR.
2. Go to Help (upper right corner) > About.

However, external scans should mirror an attacker’s perspective, so no whitelisting or “safelisting” is necessary, and firewalls should block these scans to simulate real-world attack conditions.

Adding Scannable Host Assets to Your Subscription

Before you can scan anything, the assets you intend to scan using a scanner must be added to your subscription. These assets are known as *Scannable Host Assets*.

This **video** explains how to add scannable host assets to your subscription.

The process includes the term *host tracking method*. This **article** explains what that means.

This process works well if you already know which IP addresses to add to the subscription. If you are not sure you have full visibility of the infrastructure, then you can choose to run a *Map Scan* or a *Discovery Scan*.

Map Scan

Launch map scans to discover your network devices and report comprehensive information about them. After discovering live devices on your network you can add them to your account and start scanning them for vulnerabilities.

Running a map scan is an option for a smaller organization with fewer, and often a fixed number, of IP addresses. If you are a larger enterprise, it is a better practice to skip Maps and use the Discovery Scan discussed in the next section.

Map scans are further described in these two articles:

Mapping – the Basics

Start a Map

Discovery Scan using a Scanner Appliance

A discovery scan is the same thing as a vulnerability scan except that you are searching for limited information about assets in order to add them to your subscription – as opposed to scanning them for vulnerabilities.

- Further information about scanning is found later in this document.
- This training **video** describes a discovery ("inventory") scan (start watching at 02m 45s).

Adding Cloud Agent Assets to Your Subscription

Deploying the Cloud Agent is the fastest way to gather data on your assets. By default, vulnerability assessments occur automatically every four hours, ensuring up-to-date information on all assets where agents are deployed.

Cloud Agents can be installed on workstations and servers, regardless of location, and are especially useful for assessing assets that a scanner appliance cannot easily reach—such as remote worker laptops not connected to the corporate network or ephemeral assets in the public cloud.

With Cloud Agents, you'll have the most current vulnerability data available in the Qualys Platform, ensuring your assessments reflect the latest status of existing assets.

Note

The same Cloud Agent also supports configuration management via Qualys Policy Compliance, Patching, Script Deployment (CAR), File Integrity Monitoring, and Endpoint Protection. One agent can do all of those things.

Cloud Agent Deployment

1. Confirm the asset's host operating system supports the Qualys Cloud Agent **here.**
2. Watch this **video** for the generic deployment process, and this **video** for MacOS-specific instructions.
3. This **How-To video series** walks you through how to deploy and configure Cloud Agents.
4. Documentation for Cloud Agent includes the Getting Started Guide, and installation guides for different operating systems, and can be found **here**.

   These installation guides also include the steps required to Cloud Agents in bulk to many assets. (Note that the specific steps vary slightly from one operating system to another.)

5. For certain use cases, scan Cloud Agent hosts with a scanner appliance to detect vulnerabilities which are only detectable remotely. Further explanation can be found in this **video.**

6. Troubleshoot Cloud Agent using this **article** and additional troubleshooting videos found in the **video library.**

7. Learn about recommended Cloud Agent configuration settings for different groups of assets, such as production and development. An overview and explanation of recommended settings can be found in this **blog article.**

8. Optimizing Cloud Agent network traffic can be achieved in part by configuration settings (see the blog mentioned in the step above). An additional option is to use the *Qualys Gateway Server* (QGS) which acts as a proxy for multiple Cloud Agent hosts, and can be configured to cache files downloaded by the agents from the Qualys platform.

   The Qualys Gateway Server user guide can be found **here,** and a video series for Qualys Gateway Server can be found **here.**

Note

The QGS can also be used to cache patches downloaded from OS and application vendors. The user guide referenced above describes the configuration process. Ensure that you read the whole guide before you being to configure the QGS.

Configuring a Scheduled Vulnerability Scan

1. Navigate to VMDR -> Scans -> Authentication.

2. Create Authentication Records.
   There should be one authentication record for each Windows domain, separate authentication records for Windows local authentication (if used), and authentication records for Linux / Unix / Mac devices. These How-Tos help you understand the process of creating Authentication Records.
   Creating a Windows Authentication Record
   Creating a Unix Authentication Record

3. Navigate to VMDR -> Scans -> Option Profiles.

4. Create an Option Profile. The Option Profile should include the TCP and UDP ports which are necessary to discover the hosts (the **Additional** tab). Other recommended settings in the **Scan** tab are given below:

   - Load Balancer Detection – ENABLED
   - Vulnerability Detection – COMPLETE
   - Authentication:

   o Windows - ENABLED

   o Unix/Cisco/Network SSH – ENABLED

   - Attempt least privilege for Unix – ENABLED
   - Enable the Dissolvable Agent – ENABLED
   - Enable Windows Share Enumeration – ENABLED

5. Navigate to VMDR -> Scans -> Schedules

6. Create a new scheduled scan which specifies the Option Profile that you would like to use. Also specify an appropriate schedule. An appropriate schedule would be once per week (or more often) for internal assets, and once per day for external assets.

The **Running Effective Vulnerability Scans** video explains the process.

Top Tips for Scanning Success

1. Ensure scan merging and agentless tracking are enabled. You'll get more on this later.

   Running authenticated scans gives you the most accurate results with fewer false positives. Spending the time to set up successful authenticated scans will save you time in the long run and provide more reliable vulnerability data. As outlined in CIS Control 4-3, ensuring authentication during vulnerability scans helps reduce the risk of overlooking critical vulnerabilities.

   Video explaining the advantages of authenticated scanning.

   Video explaining how to configure authenticated scans.

   Video explaining how to monitor authentication.

It is important to monitor that authentication continues to work successfully. If authentication to a host fails, the scanner will fall back to using unauthenticated scans for that host.

For further details, refer to the **documentation on host authentication.**

Remember that the username that you add to the Authentication Record should have local administrative privileges.

2. Deploy scanners to meet the organization's demand. It is a good practice to put scanners as close to the targets as possible.

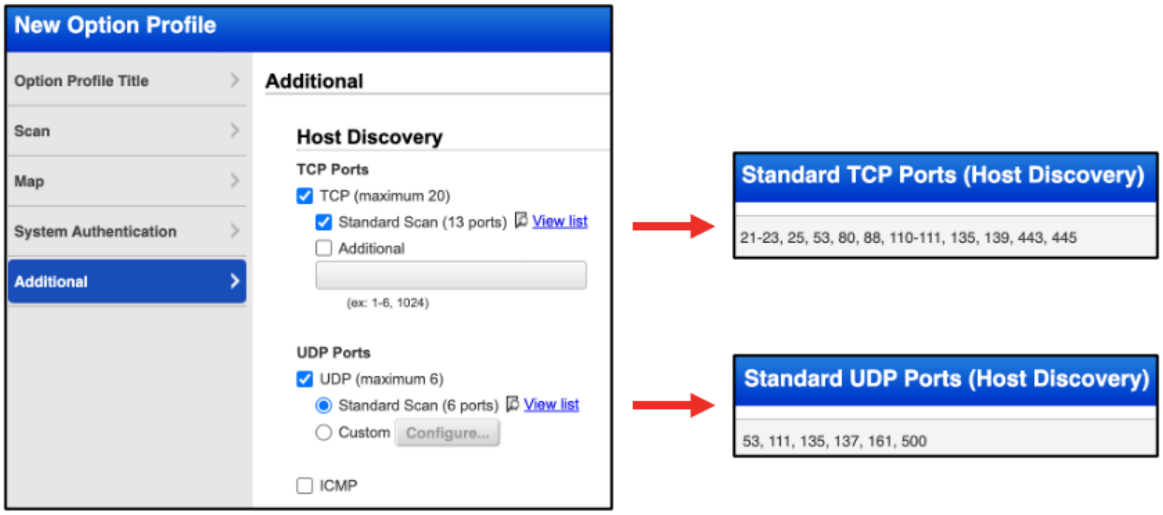
3. Scheduling: "Scan for as much as possible as often as possible." You should scan external assets daily, or set up continual scans. You should scan internal assets weekly and combine scanning with Cloud Agent scans (more on this topic later).

4. Scheduled scan jobs that you should include are:
   - **Perimeter Scan** – This is a vulnerability scan for your public DNS or public-facing IP addresses.
   - **On-Premise Scan** – This is a vulnerability scan for your company's internal infrastructure.

- **Cloud Perimeter Scan** – This is a vulnerability scan on publicly-exposed EC2 instances.
- **EC2 Scan** – This is a vulnerability scan on EC2 instances within a private network inside a cloud environment.

5. A summary of scanning best practices is provided by this article. **Scanning Best Practices**

6. Remember that only hosts that are deemed to be “alive” will be scanned for vulnerabilities. This check is made by the scanner before it does anything else. You can fine-tune which ports the scanner probes as part of the host-alive check in the Scan Options Profile. The defaults are given here:



Additional

Host Discovery

TCP Ports

☑ TCP (maximum 20)

☑ Standard Scan (13 ports) View list

□ Additional

(ex: 1-6, 1024)

UDP Ports

☑ UDP (maximum 6)

● Standard Scan (6 ports) View list

○ Custom Configure...

□ ICMP

Standard TCP Ports (Host Discovery)

21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445

Standard UDP Ports (Host Discovery)

53, 111, 135, 137, 161, 500

The scanner requires that a host responds to at least one of these probes before it continues to scan that host for vulnerabilities.

7. Understand the scan results by navigating to VMDR -> Vulnerabilities

Here you can see all of the discovered vulnerabilities in the subscription. The list can be filtered by clicking on the links in the left-hand panel, or by manually typing queries in the Search field.

To help you understand some of the findings, consult this video: **The Qualys Vulnerability Knowledgebase**

And also this How-To: **Understanding TruRisk Scoring.**

Merging Agent Records

Do not skip this section!

If you are using both Cloud Agent and Scanner Appliances, it's vital that you understand asset merging. This will ensure your asset records are populated correctly with the data collected by both the Cloud Agents and Scanner Appliances.

If you do not follow the advice provided by these resources, you might have duplicate asset records in your subscription.

These two videos are useful in explaining both what to do and why:
Asset Tracking and Data Merging

Asset Merging

This useful **article** also explains merging in further detail.

Note

You may find that some of the Merge settings are already enabled. This is because some of the Merge default settings have been recently changed. This **blog article** provides the details.

3. Organize Assets for Increased Efficiency

Your sensors will collect valuable data about your assets. Organizing the assets effectively will set you up for ongoing success with the Qualys platform. There are two ways to organize assets in Qualys:

There are two ways to organize assets in Qualys.

1. **Asset Groups** – The traditional method but still has valuable functionality.

2. **Asset Tags** – The newer approach, which should be your primary focus for streamlined asset management.

Things to consider when using Asset Groups

1. Use Asset Groups to define IP ranges for scannable host assets, typically when scanning full network ranges for vulnerabilities using a scanner appliance.
2. Do not use Asset Groups for scattered individual IP addresses or Cloud Agent-hosted assets.
3. For reporting and more granular management, Asset Tags are recommended.
4. Use these articles to help you set up Asset Groups:
   All About Asset Groups
   Configure Asset Groups

When to use Asset Tags

Asset Tags are highly versatile and are primarily used to categorize assets by attributes like OS, device type, software, and more. They are invaluable for running detailed reports and play a key role in Qualys Patch Management and other Qualys applications.

Although creating tags may seem overwhelming at first, even a few simple tags can provide significant value. Tags are essential for implementing Qualys TruRisk, which helps prioritize remediation actions based on the actual risk to your organization. This approach enables more informed decision-making and allows you to effectively communicate with business stakeholders about risks and remediation priorities.

Tags are especially beneficial for organizing and managing assets across different environments and applications. By consistently applying them, you gain better visibility into your assets, streamline workflows for vulnerability management and patching, and improve overall efficiency.

Here are some key resources to get you started:

Configure Tags in CSAM [and Global Asset View]

Organize Assets using Tags [video]

This blog **article** explains the importance of the Asset Criticality Score, and how to configure it.

Further, more detailed information about Asset Tags can be found in these articles:

Asset Tags: Are You Getting The Best Value?

Complete Tag List

4. Communicate Effectively

Technical teams are often responsible for explaining why simply reducing vulnerabilities is not enough to efficiently manage risk. Business leaders require clear, digestible information that translates into direct financial implications.

Qualys VMDR provides two principal methods of communicating risk information to both business leaders and to security operations: Dashboards and Reports.

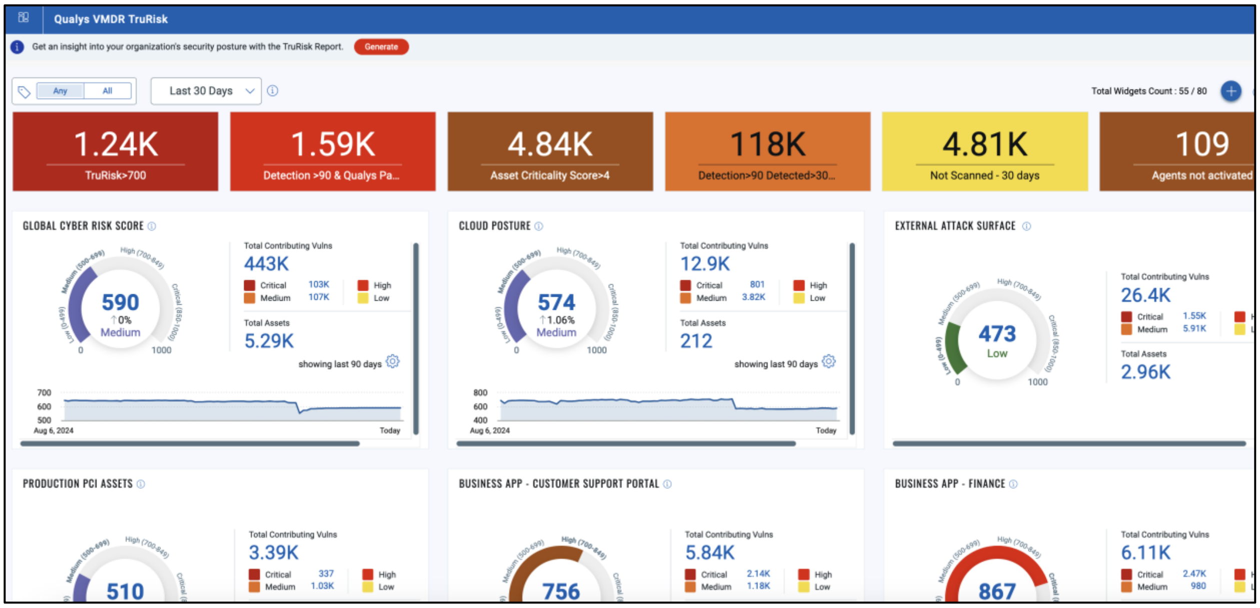
Dashboards

Dashboards are visual representations of your vulnerability, asset, and / or compliance data. Dashboard templates are provided out of the box. This makes it easier for you to become effective with VMDR more quickly. As time passes, you may wish to customize your dashboards and widgets.

For communicating to business leaders, consider this dashboard:

Qualys VMDR TruRisk

Using this dashboard, visualize and quantify cyber risk to accurately measure it and take steps to reduce exposure. Track risk reduction trends over time and better measure the effectiveness of your cyber security program.



For communicating information to security operations, consider using this template:

Subscription Health

The data that populates into the platform from your sensors must be curated and verified on an ongoing basis.

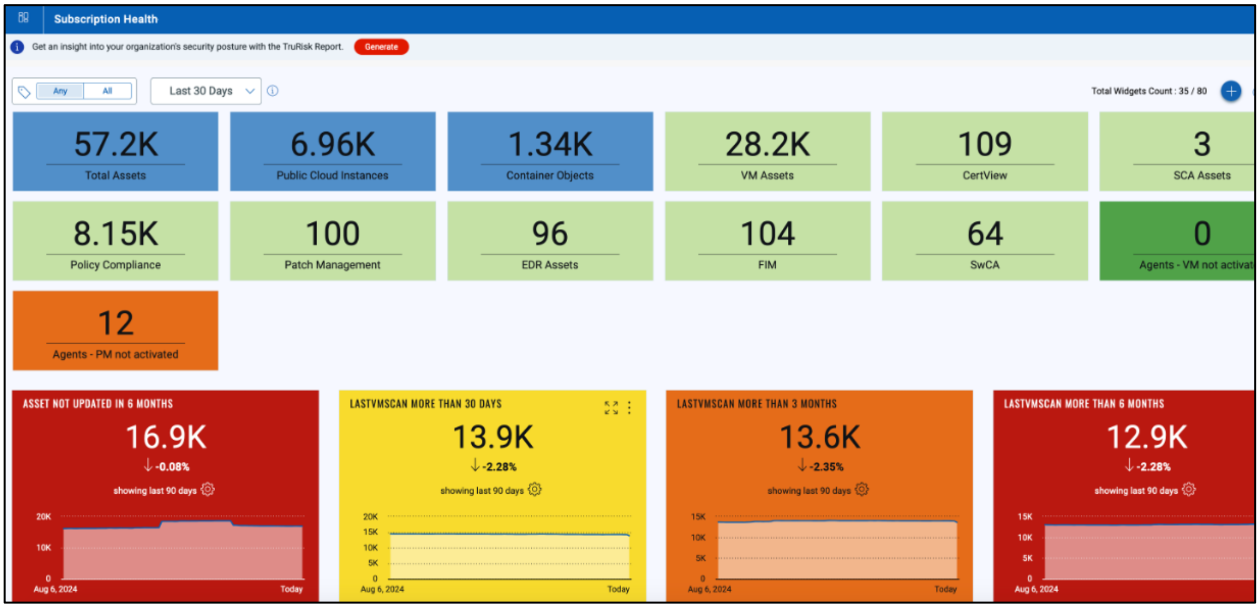
Some items that go into a “healthy” subscription are

1. Asset merging is configured correctly
2. Authenticated Scanning is configured correctly
3. Agents are deployed to your servers and endpoints
4. Top dashboards are configured
5. Stale Data is removed (purging) to ensure accurate reports

Asset Merging - Earlier in the document, asset merging and tracking was discussed. This is important because you want to avoid duplicate records in your subscription.

Authenticated Scanning – Setting up your authenticated scans correctly will ensure vulnerability data is collected by your scanner correctly. It will provide the most accurate representation of risk that each host carries.

Purging - Purging data is also important for platform performance and ensuring you accurately report and communicate risk to your organization. Purging is removing stale data from your subscription to ensure reports are accurate and remediation efforts are efficient.


Subscription Health
Get an insight into your organization's security posture with the TruRisk Report.
Generate
Any
All
Last 30 Days
Total Widgets Count : 35 / 80

57.2K Total Assets

6.96K Public Cloud Instances

1.34K Container Objects

28.2K VM Assets

109 CertView

3 SCA Assets

8.15K Policy Compliance

100 Patch Management

96 EDR Assets

104 FIM

64 SwCA

0 Agents - VM not activat

12 Agents - PM not activated

ASSET NOT UPDATED IN 6 MONTHS 16.9K ↓ -0.08% showing last 90 days

LASTVMSCAN MORE THAN 30 DAYS 13.9K ↓ -2.28% showing last 90 days

LASTVMSCAN MORE THAN 3 MONTHS 13.6K ↓ -2.35% showing last 90 days

LASTVMSCAN MORE THAN 6 MONTHS 12.9K ↓ -2.28% showing last 90 days

The Subscription Health dashboard is explained more fully in this blog **article.**

Some useful recommendations about implementing dashboards can be found in this **video.**

Subscription health issues, in general, are covered in this **video series.**

VMDR Reports

VMDR reports can be configured using *Report Templates* and can then be run on-demand or as a scheduled report job. This **article** explains how to configure a Report Template.

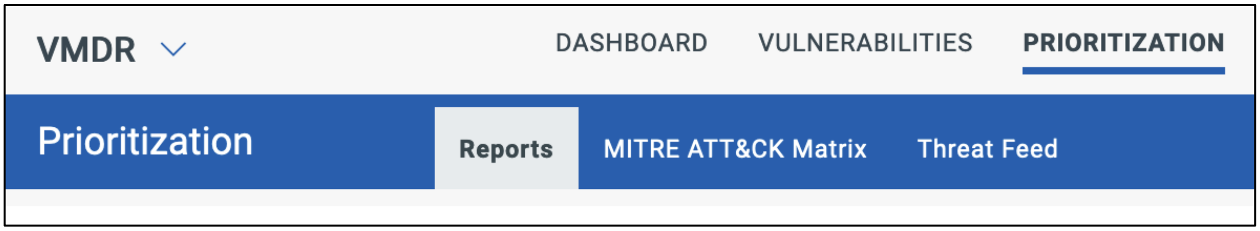
Report Templates are also explained in these videos:

Scan Report Template: Findings

Scan Report Template: Display

Scan Report Template: Filter

A special type of report is the *Prioritization Report*. You can find it in the PRIORITIZATION section of VMDR.



This report helps you report on which assets to prioritize for remediation according to the risk they pose to your organization. Further information about the Prioritization Report can be found in these articles and video.

Prioritize your Vulnerabilities [Note: TruRisk mode is recommended!]

Reading the VMDR Prioritization Report

Video: Prioritization with TruRisk

Tips for Reporting Success

1. To ensure data consistency, maintain regular and reliable scanning and reporting schedules and attempt to synchronize them.
2. Distribute reports that are aligned with your organization's security policies, goals and objectives.
3. Design report templates for your target audience. Solicit feedback from recipients (stay engaged) and tune reports to meet their unique requirements.
4. Use Host-Based Findings for vulnerability reports and take advantage of status and history information.
5. Use Scan-Based Findings to investigate anomalies or tune scan performance.

Account Maintenance

Account maintenance is extremely important to ensure that your communications and remediation actions are as efficient and accurate as possible.

Many of your assets may be in the cloud but may well be ephemeral in nature. They exist for a few minutes, hours, or days and then are terminated. These transitory assets pose unique asset and vulnerability management challenges. Stale assets records are an issue that we encounter all the time when working with our customers during health checks. The most significant problem caused by stale assets is the decline in data accuracy that affects your reports and dashboards.

Stale Assets Records:

- Decrease accuracy
- Impact your security posture
- Affect your compliance position
- Reduce Performance
- Increase your license costs

Reporting on assets that no longer exist in your environment causes IT teams to chase vulnerabilities that aren't there anymore (which impacts mean time to remediation (MTTR)), obscures an enterprise's overall security posture and compliance position, and results in management losing confidence in and starting to question the data. This is easily avoided using the *purge* features available in the Qualys platform.

This **video** explains about purging stale asset records in further detail.

This **article** explains why purging is important and how you can automate purging using purge rules in *Qualys CyberSecurity Asset Management*. The article includes a video.

5. Eliminate Risks

Your objective should be to eliminate risk. But not all risks – you should focus on the risks that threaten your organizational objectives.

The steps below help you to prioritize remediation actions.

1. Understand what TruRisk is – start with this **video.**

2. This **blog** article takes the discussion further by looking at TruRisk 2.0 (October 2024 update).

3. For a more in-depth look at TruRisk, read these three blog articles: https://blog.qualys.com/product-tech/2022/12/12/operationalizing-qualys-vmdr-with-qualys-trurisk-part-1

   https://blog.qualys.com/vulnerabilities-threat-research/2022/12/16/implement-risk-based-vulnerability-management-with-qualys-trurisk-part-2

   https://blog.qualys.com/product-tech/2023/01/03/implement-risk-based-vulnerability-management-with-qualys-trurisk-part-3

4. Use the VMDR Prioritization Report to help you easily and simply prioritize remediation actions. This report also provides a workflow from the report straight into a patch deployment job wizard using *Qualys TruRisk Eliminate*.

   This **video** explains how to use the Prioritization Report effectively. You should focus on the *TruRisk mode* of the Prioritization Report.

5. This blog **article** explains how inventory risks detected by CSAM are also included in TruRisk.