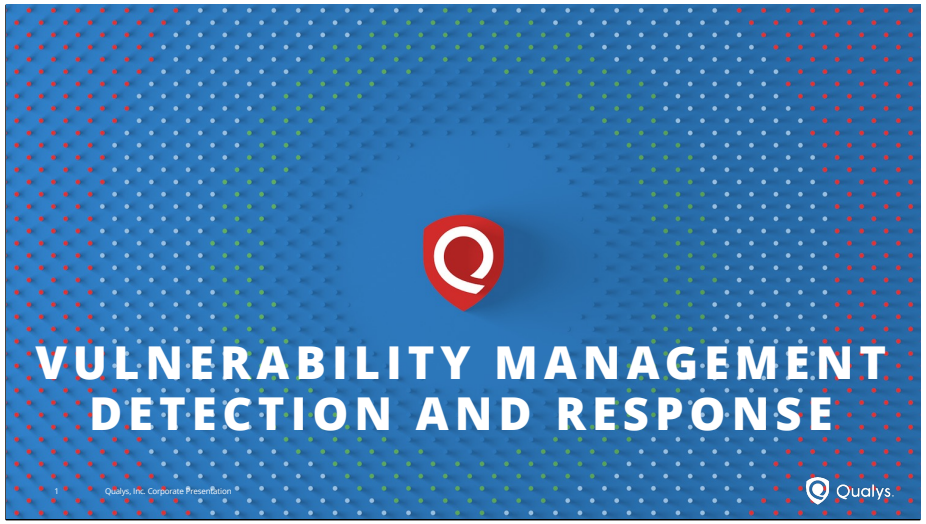
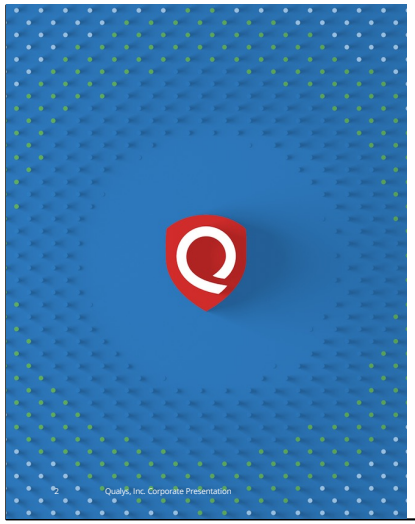


Welcome to Qualys Vulnerability Management Detection and Response (VMDR) training.



WELCOME

The objectives for this section are:

Understand the course objectives.
Understand where to get help.

LEARNING RESOURCES

Page	Link	Description
Training Page	https://www.qualys.com/training/	Shows all available training. After going through this onboarding, enhance your knowledge on this site.
Learning System	https://qualys.com/learning	Where you can enroll in all Qualys Training.
Cloud Platform	https://www.qualys.com/docs/qualys-cloud-platform-whitepaper.pdf	Basics of the Qualys Platform
Docs	https://www.qualys.com/documentation/	Here is where you can find ALL Qualys documentation
VMDR How-to videos	https://www.qualys.com/training/library/vmdr-onboarding/	This video series will walk you through the steps for setting up Qualys Vulnerability Management, Detection, and Response (VMDR).

These links are also found in the Lab Tutorial Supplement - Appendix C

Qualys.

Here are some additional learning resources which you may find helpful.

https://www.qualys.com/training/
https://qualys.com/learning
https://www.qualys.com/docs/qualys-cloud-platform-whitepaper.pdf
https://www.qualys.com/documentation/
https://www.qualys.com/training/library/vmdr-onboarding/

Recommendation - take a look at each site, and bookmark them for future use!

SUPPORT RESOURCES

Page	Link	Description
Systems Status	https://status.qualys.com/	Shows the operational status, maintenance, upgrades, and outages of each platform.
Find my platform	https://www.qualys.com/platform-identification/	Shows the Qualys platform your organization is using.
Support Portal	https://success.qualys.com/customersupport/s/	Useful landing page for docs, training, forums, and managing cases.
How to Collaborate with Support	https://success.qualys.com/support/s/article/000003610	This article tells you all the different ways you can interact with Support. Call, chat, open a case, etc.
Opening Cases	https://success.qualys.com/support/s/article/000006839	This document tells you what you need to provide support to drive faster resolution for your cases.

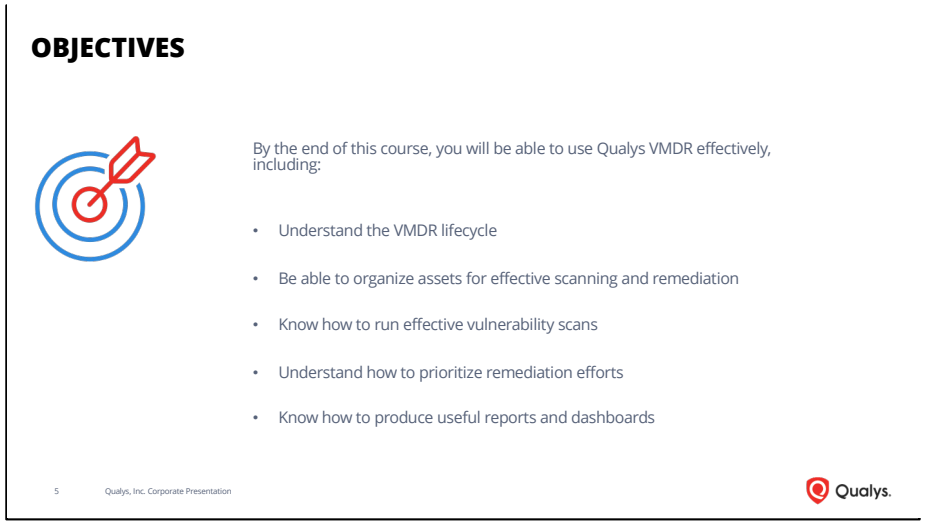
These links are also found in the Lab Tutorial Supplement - Appendix C

Qualys.

Here are some support resources which you may find helpful.

https://status.qualys.com/
https://www.qualys.com/platform-identification/
https://success.qualys.com/customersupport/s/
https://success.qualys.com/support/s/article/000003610
https://success.qualys.com/support/s/article/000006839

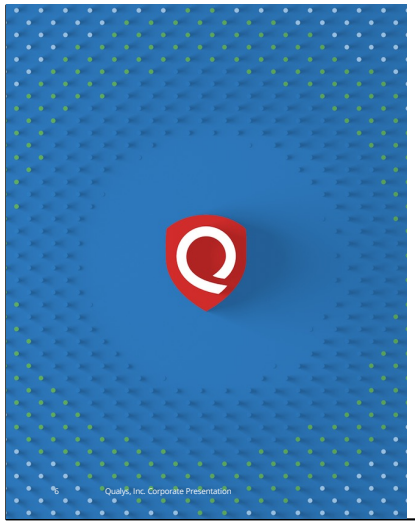
Recommendation - take a look at each site, and bookmark them for future use!



The objectives for this course are:

By the end of this course, you will be able to use Qualys VMDR effectively, including:

- Understand the VMDR lifecycle
- Know how to use the Qualys Knowledgebase
- Know how to organise assets
- Understand the vulnerability scanning process
- Know how to prioritize remediation using reports and dashboards



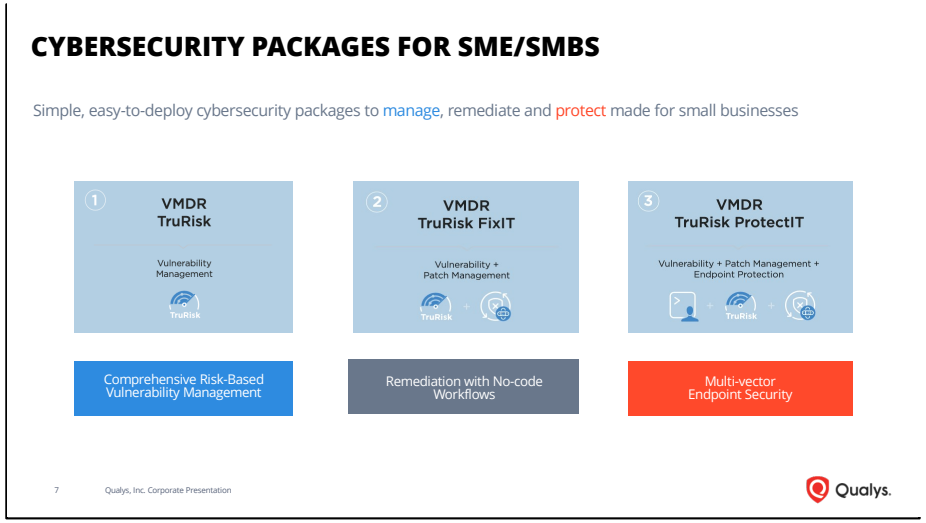
INTRODUCTION TO VMDR

Qualys.

The objectives for this section are:

Learn about the different Qualys sensors.

How to add assets to the Qualys platform.



Qualys VMDR TruRisk is available in three packages, allowing organizations to optionally add remediation (Patch Management) capabilities with *VMDR TruRisk FixIT* and endpoint detection and response (Multi-Vector EDR) capabilities with *VMDR TruRisk ProtectIT.*

VMDR TruRisk FixIT leverages the enterprise-grade Qualys Cloud Platform and VMDR with TruRisk to help IT and security teams quickly and efficiently remediate vulnerabilities and patch systems, tailored specifically for our SMB customers.

Patch management functionality is tightly integrated with VMDR TruRisk allowing customers to efficiently map VMDR findings to an actionable remediation job that automatically includes all the relevant patches and configuration changes required.

VMDR TruRisk ProtectIT brings together VMDR TruRisk, Patch Management and Endpoint Security capabilities into a natively integrated offering specifically tailored for SMBs. Qualys Endpoint Security adds-in proactive protection from known malware and zero-day threats.

Endpoint security functionality is tightly integrated with VMDR TruRisk.

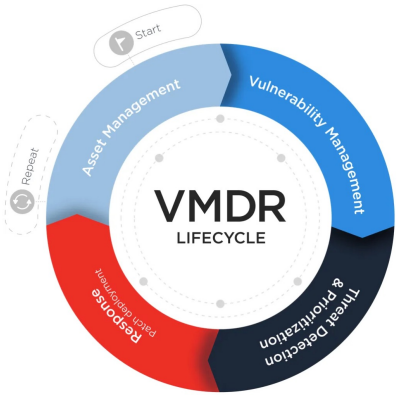
QUALYS VMDR LIFECYCLE

The Qualys VMDR lifecycle is a continuous, seamlessly orchestrated workflow of automated asset discovery, vulnerability management, threat prioritization, and remediation.

By adopting the VMDR lifecycle, organizations decrease their risk of compromise by effectively preventing breaches and quickly responding to threats.

Benefits of using Qualys VMDR include:

- Reduced time to remediate (TTR)
- Full visibility and control
- Reduced risk
- Lower TCO and higher productivity



8 Qualys, Inc. Corporate Presentation

Qualys.

The Qualys VMDR lifecycle is a continuous, seamlessly orchestrated workflow of automated asset discovery, vulnerability management, threat prioritization, and remediation.

Asset Management
You can't secure what you can't see. It's essential to have a complete, updated global inventory of all assets across your network: on prem, endpoints, clouds, containers, mobile, OT and IoT — everywhere. This continuous discovery process must detect all assets — approved and unapproved — and collect granular details about each, such as installed software, hardware details and running services.

Asset data should be normalized, and assets automatically categorized with dynamic rules-based tagging. This classification context helps assess risk. For example: Does this server contain a database with customer data?

Vulnerability Management
The traditional "scan-the-network" approach doesn't scale well for modern IT infrastructure. Therefore all assets — on premises, in public clouds, on

endpoints — must be checked for vulnerabilities and misconfigurations continuously, using active, authenticated scans, passive network analysis and, even better, lightweight agents that reside on the assets and detect and report any changes in real time. This Vulnerability Management, Detection and Response phase also includes assessment of digital certificates and TLS configurations.

Vulnerability Detection and Prioritization
Vulnerability Management, Detection and Response leverages the latest threat intelligence, advanced correlation and machine learning to pinpoint the riskiest vulnerabilities on the most critical assets. VMDR highlights indicators of compromise, and leverages ML to surface potentially severe vulnerabilities. That way you can prioritize which threats to mitigate first, before attackers exploit them.

Vulnerability Remediation
Vulnerability Management, Detection and Response identifies the most appropriate remediation for each threat, whether it's deploying a patch, adjusting a configuration, renewing a certificate or quarantining an asset. If patching is the course of action, an effective VMDR solution will automatically correlate vulnerabilities and patches, and select the most recent patch available for fixing a particular vulnerability in a specific asset.

With VMDR, remediation is fast, precise and smooth — all critical elements when a delay can give attackers a chance to breach your defenses.

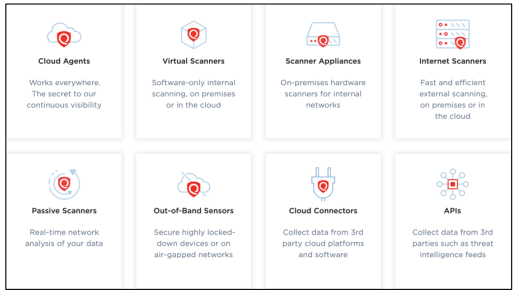
By combining these four core elements, a VMDR process allows security teams to make decisions and take actions that are based on data-driven risk assessments.

QUALYS SENSOR PLATFORM

Qualys sensors collect data from your IT environment and automatically beam it up to the Qualys Cloud Platform, which continuously analyzes and correlates the information to help you quickly and precisely identify and eliminate threats.

The Qualys Cloud Platform's sensors are:

- Always on
- Remotely deployed
- Centrally managed
- Self-updating.



9 Qualys, Inc. Corporate Presentation

Qualys.

With its always-on sensors, the Qualys Cloud Platform gives organizations continuous, real-time visibility of all their IT assets – on-premises, at endpoints or in clouds
– for comprehensive prevention, detection and response.

Centrally managed and self-updating, the Qualys sensors come as remote scanners located in the Qualys cloud, physical or virtual appliances, or lightweight agents.
These sensors help you inventory, track, and even correct enterprise assets.

The sensors which we focus on this course are Cloud Agents, Virtual Scanners, Scanner Appliances, and Internet (aka Remote) Scanners.

More about Internet (aka Remote) Scanners:
Scanning your assets from the outside, using the Qualys Internet Scanners already associated with your account, will give you an "external attacker view" of your vulnerabilities from the outside. In other words, if you have a

Scanner role or above in Qualys, you'll automatically be able to launch scans against your external (public IP) assets.

IP range for inbound scan traffic

1. Log into your instance of Qualys for VMDR.
2. Go to Help (upper right corner) > About
3. Find the IP ranges you need to allow for inbound scan traffic.

More about the other Sensors

- Local Scanners are deployed on local area networks and are commonly used to scan assets within reserved or private IP address ranges. These local scanners can be deployed as physical or virtual appliances. Once installed, each Scanner Appliance keeps itself updated with the latest vulnerability signatures via its connection to the Qualys Cloud Platform

- Qualys Cloud Agents run as a local process on the host they protect. Qualys agents support a wide variety of OS platforms. Agents play a special role in VMDR, by providing the patching and response functions.

- Qualys Passive Sensors can be deployed as physical or virtual appliances. Working with TAPs and Switches throughout your network, passive sensors operate by sniffing network traffic which is sent to the Qualys platform for processing. Passive Sensor will help you to identify the unmanaged assets throughout your network architecture.

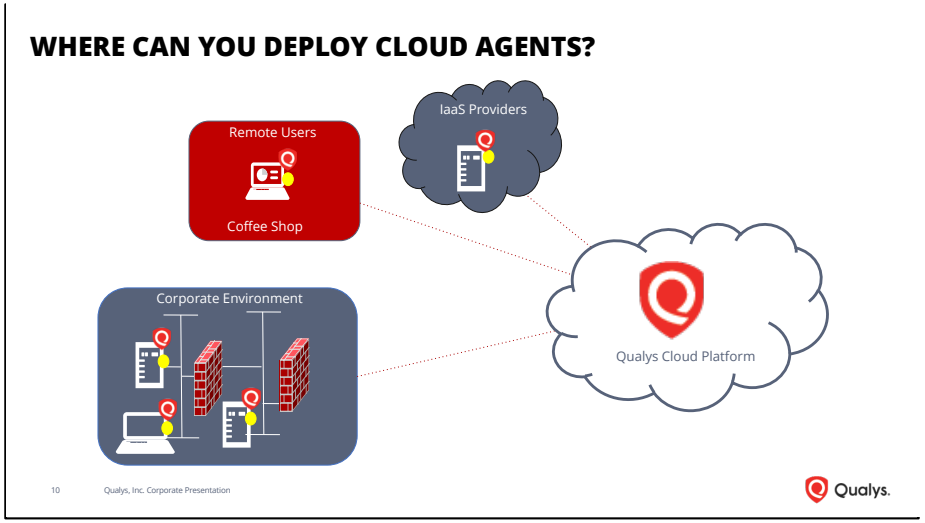
- Cloud and SaaS Connectors work with the native services of your cloud and SaaS providers to identify misconfigurations and security blind spots. Cloud Connectors can be created for your AWS, Google Cloud, and Microsoft Azure accounts. SaaS Connectors are available for O365, Google Workspace, Zoom, and Salesforce.

- Qualys Container Sensor downloads as a Docker image and is installed on a Docker host as a container application, right alongside other container applications. Once installed, Container Sensor will assess all new and existing Docker images and containers for vulnerabilities. Presently, there are 3 different types of Container Sensors. A General Sensor scans images and containers on a single docker host. A Registry Sensor scans images in public and private Docker registries. 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.

- Out-of-band sensors help to secure devices on air-gapped networks.
- And finally (during our discussion of CyberSecurity Asset Management) we'll examine the prospect of using the Qualys API to share data between the Qualys Platform and the ServiceNow CMDB.

All of these sensors come together, into one comprehensive framework to help you stay on top of today's challenging Hybrid IT Environments.



Cloud Agent delivers visibility and security solutions for assets that are not easily scanned from the network including remote or roaming users, distributed offices and cloud server instances.

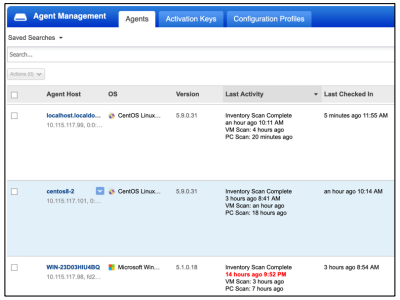
Cloud Agent communication is optimized to support large-scale agent deployments while providing flexible and granular performance configuration controls allowing organizations to tune agent performance and bandwidth usage for their specific environmental requirements.

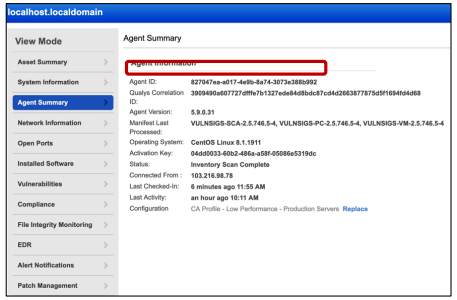
The agent initiates all connections on port 443 from the agent to the platform using REST over HTTPS/TLS.

AGENT HOSTS

Once the agents are successfully deployed, you will see respective agent hosts under the "Agents" tab in the Cloud Agent application. You do *not* see these agent hosts listed in the VMDR application under VMDR > Assets > Address Management tab.

Qualys Host ID is the default tracking method for agent hosts.





11 Qualys, Inc. Corporate Presentation

Qualys.

Qualys Cloud Agent provides a continuous view of assets for vulnerability management, policy compliance, file integrity monitoring, EndPoint Detection and Response, Patch Management and asset inventory without the need for credential management, scan windows, and firewall changes.

The agent is light-weight, remotely deployable, centrally managed and self-updating.

Once the agents are successfully deployed, i.e. installed and communicating with the Qualys Cloud platform, you will see respective agent hosts under the "Agents" tab in the Cloud Agent application. You do *not* see these agent hosts listed in the VMDR application under VMDR > Assets > Address Management tab.

Use the "Quick Actions" menu for any agent host listed here, to view specific asset details. The Asset Summary displays host OS details, geolocation information, names and addresses, activity updates, and Asset Tags.

There is also a Cloud Agent tag which automatically gets associated with any asset where cloud agent is deployed. This is important to know when reporting, scanning and using CSAM or GlobalAsset view. You can use this tag to include or exclude cloud agent hosts in your scans, reports and queries.

Cloud Agent Installation

1. Verify that Cloud Agent supports your OS.
2. How-Tos for Cloud Agents – This full video series will walk you through how to deploy and configure Cloud Agents.
3. Getting Started with Cloud Agent – This is the official guide for deploying Cloud Agents.
4. All Installation guides for each OS – Here are the installation guides for all Operating Systems.
5. Deploying your agents in bulk – This article will help you understand how your agents can be deployed at scale.
6. Cloud Agent Help will help you troubleshoot any connectivity issues or errors you see as part of your deployment.
7. Troubleshooting Agent Connectivity - This document will walk you through how to troubleshoot any agent connectivity issues.

ADDING HOST ASSETS

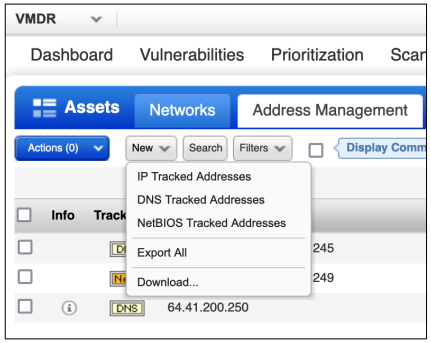
For scanning to begin, you must first add assets to your subscription.

The tracking method impacts how the hosts will be listed in scan reports (scan results are always sorted by IP address).

Hosts assigned the IP address tracking method will be listed in numerical order by IP address. Hosts assigned the DNS or NetBIOS tracking method will be listed in alphabetical order by hostname.

IPs may be entered in any of the following formats:

List of single IPs	17.16.20.5, 17.16.20.21
IP ranges	167.216.205.1-167.216.205.254
CIDR	192.168.0.87/24



12 Qualys, Inc. Corporate Presentation

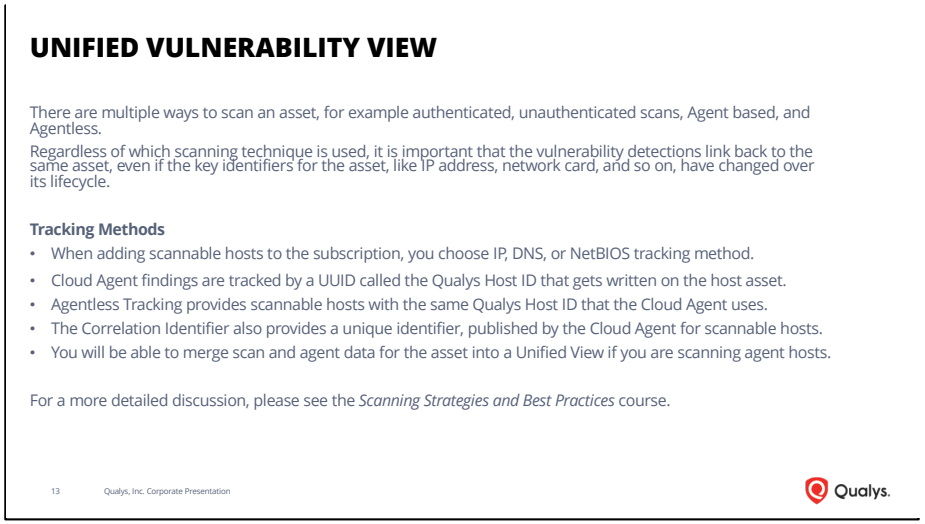
Qualys.

When you add hosts to your subscription you will then be able to scan them and report against them. You can also remove hosts from your subscription. A full purge of the data for that host is done at the time of removal. When you add hosts to your subscription you are required to identify its associated IP address; however you are also required to choose a tracking method that specifies how vulnerability findings will be tracked or indexed.

The current best practice is to add all your IP addressing as “IP Tracked” and rely on Merging, Agentless tracking, and good purging practices to keep your data in Qualys clean and up-to-date.

For easy setup, watch this video https://qualys.sharepoint.com/:v:/s/training/EYtBF

idCXoBLjaXhJqNA1YsBZwTyqAxsxiRR4zKY9LWA0g
?e=seq1TQ

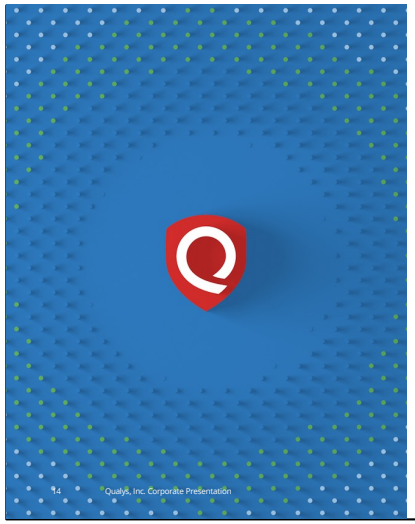


Agentless Tracking is a best practice and is recommended for dynamic environments. Findings for your scan targets will be tracked by a UUID that sticks to the host. At that point, it does not matter if the IP or name changes. It also assists in consolidating findings for hosts with multiple IP addresses.

Once the scannable host has a Qualys Host ID, the asset will have a common ID that can be used to merge scan and agent data together. Unified View refers to a single record for the asset that includes both scan and agent data.

This is covered in more detail on the Qualys Community site:

- https://blog.qualys.com/product-tech/2021/01/21/unified-vulnerability-view-of-unauthenticated-and-agent-scans
- https://qualysguard.qg3.apps.qualys.com/qwebhelp/fo_portal/host_assets/agentless_tracking.htm



KNOWLEDGEBASE

Qualys.

The objectives for this section is to learn:

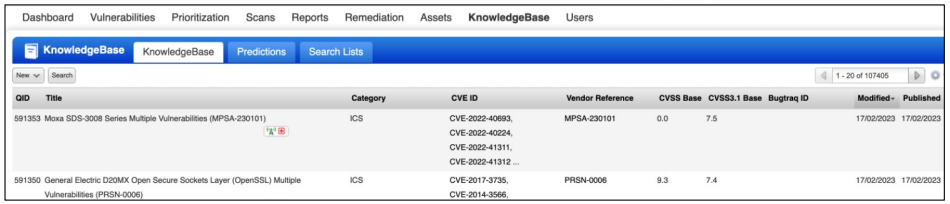
Qualys Vulnerability KnowledgeBase
Searching the KnowledgeBase
Qualys Detection Score

VMDR KNOWLEDGEBASE

The Qualys KnowledgeBase is the central location in Qualys that stores and shows all the possible vulnerability checks. It is not a list of vulnerabilities that you have in your environment.

We have the most up-to-date KnowledgeBase of vulnerabilities in the security industry, it is updated continually and managed by a dedicated team.

The KnowledgeBase table contains QID, vulnerability title, severity, CVE ID, vendor reference, CVSS scoring, CVSS3 Base score, BugTraq number, and when it was modified/created.



15 Qualys, Inc. Corporate Presentation

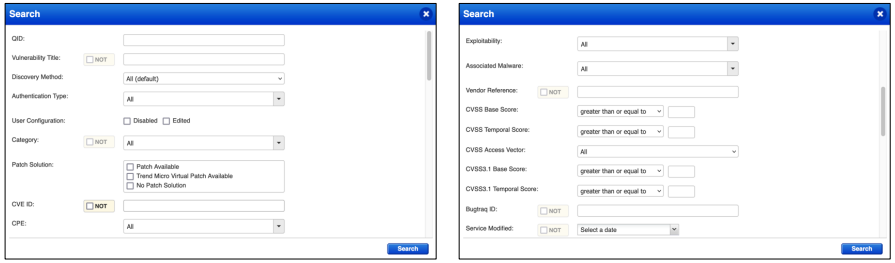
Qualys.

The colorful icons associated with a QID represent the different properties or characteristics of its associated vulnerability:

A pencil icon identifies QIDs that have been edited by a Manager user. Only the Manager user role can edit QIDs in your account knowledgebase. The green wi-fi antenna icon identifies vulnerabilities that can be detected remotely by a (Qualys Scanner Appliance) without the use of authentication. If authentication is required for successful vulnerability detection, the QID will be associated with the blue key icon. The red cross icon identifies vulnerabilities that are patchable. QIDs with the red cross icon typically provide a direct link to the vendor's patch. The black hat icon is used to identify vulnerabilities that have a known exploit. The red, hazardous material icon identifies vulnerabilities associated with malware. The blue gear icon is associated with vulnerabilities that can potentially be protected from exploits, by making specific configuration changes on the target host. The hex icon identifies vulnerabilities that are associated with services that are not currently running.

KNOWLEDGEBASE SEARCH

Use the search functionality to find vulnerabilities by QID, title, CVE ID, CVSS base score, Qualys severity level, product name, or by many other criteria.



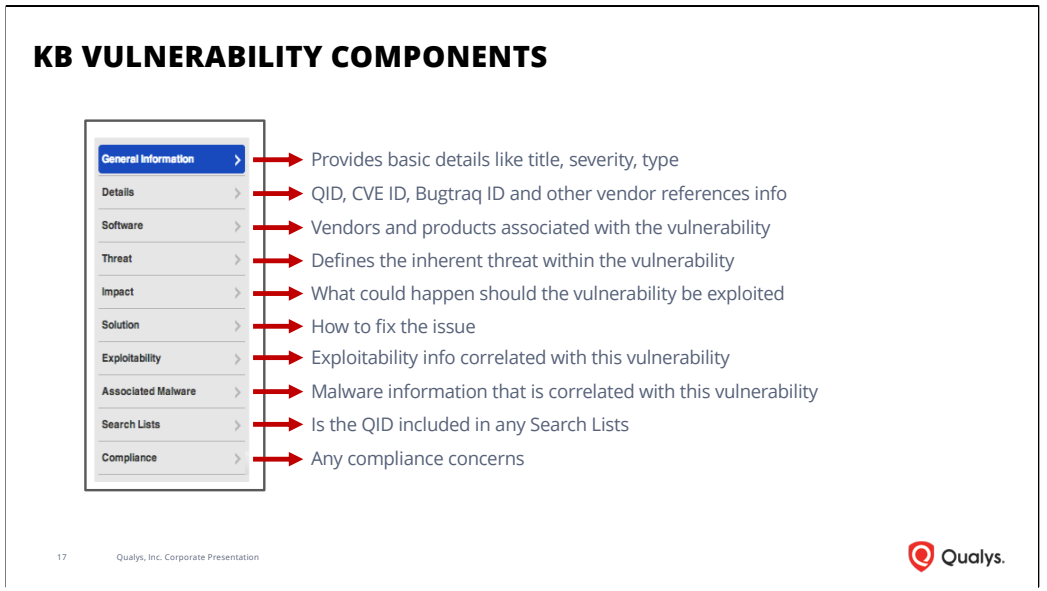
16 Qualys, Inc. Corporate Presentation

Qualys.

With tens of thousands of QIDs in the Qualys knowlegebase, you'll want to take advantage of the numerous search options available in the knowledgebase search tool. The search tool provides more than 30 different options for locating specific QIDs or types of vulnerabilities within the knowledgebase.

Some of the search options feature a NOT operator, which allows you to exclude QIDs that match your search criteria.

You can perform searches using CVE IDs, various CVSS scores, bugtraq IDs, and even the date QIDs were published or modified.



These are the components of a Qualys KnowledgeBase QID.

Here are some common terms that we use in vulnerability details:

Associated Malware
Malware information correlated with the vulnerability, obtained from the Trend Micro Threat Encyclopedia.

Bugtraq ID
The Bugtraq ID number assigned to the vulnerability by SecurityFocus.

Category
Each vulnerability is assigned to a category. Some categories are platform-specific (for example Debian and SUSE) while others are more general (for example Database and Firewall).

CVE ID
The CVE name(s) associated with the vulnerability. CVE (Common Vulnerabilities and Exposures) is a list of common names for publicly known vulnerabilities and exposures.

CVSS Access Vector
CVSS Access Vector is part of the CVSS Base metric group, and reflects the

level of access required to exploit a vulnerability. The more remote an attacker can be to exploit a vulnerability, then the higher the score and risk. CVSS Access Vector values are Local Access, Adjacent Network and Network. This value is used in reporting when CVSS Scoring is enabled for your subscription. CVSS Base Score
This score represents the fundamental, unchanging qualities of the vulnerability and is provided by NIST, unless the score is marked with the footnote [1] which indicates the score is provided by the service. This value is used in reporting when CVSS Scoring is enabled for your subscription.

CVSS Temporal Score

This score represents time dependent qualities of the vulnerability and is provided by the service. This value is used in reporting when CVSS Scoring is enabled for your subscription

Discovery Method

Identifies the type of scan that will detect the vulnerability - authenticated, remote (unauthenticated), or both.

Exploitability

Exploitability information correlated with the vulnerability, includes references to known exploits and related security resources. This field is auto-populated by scripts that search the Internet at known exploit sites. When an exploit is found, the QID is updated with a link to the exploit. Note - The QID modified date is not updated based on changes to exploitability information since these changes don't affect the signature code, scoring or the QID description.

PCI Vuln

Indicates whether the vulnerability must be fixed to pass a PCI compliance scan.

QID

The unique Qualys ID number assigned to the vulnerability.

Severity Level

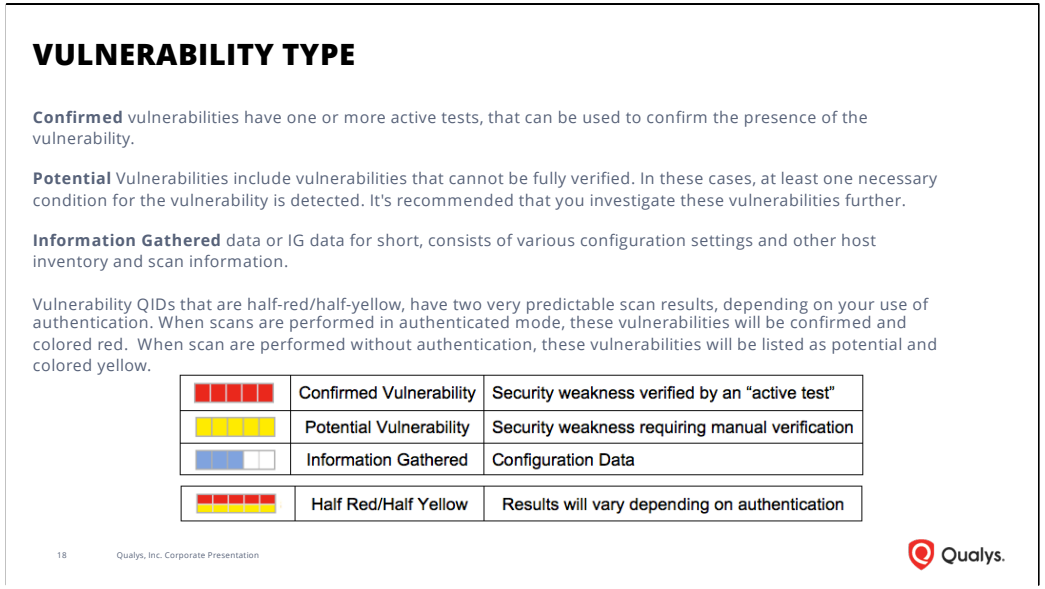
Each vulnerability is assigned a severity level (1-5) which is determined by the security risk associated with its exploitation.

Tracking Method

You must assign a tracking method to each host in your subscription: IP address, DNS Hostname or NetBIOS hostname. The tracking method determines how the host will be reported in scan reports.

Do you have Cloud Agent? Hosts with cloud agents are identified with a tracking method of Cloud Agent (or AGENT). Tip - You can quickly find your agent hosts by clicking the Search option above the list and choosing the Network "Global Cloud Agent Network".

Vendor Reference
A reference number released by the vendor in regards to the vulnerability, such as a Microsoft Security Bulletin like MS03-046.



VULNERABILITY TYPE

Confirmed vulnerabilities have one or more active tests, that can be used to confirm the presence of the vulnerability.

Potential Vulnerabilities include vulnerabilities that cannot be fully verified. In these cases, at least one necessary condition for the vulnerability is detected. It's recommended that you investigate these vulnerabilities further.

Information Gathered data or IG data for short, consists of various configuration settings and other host inventory and scan information.

Vulnerability QIDs that are half-red/half-yellow, have two very predictable scan results, depending on your use of authentication. When scans are performed in authenticated mode, these vulnerabilities will be confirmed and colored red. When scan are performed without authentication, these vulnerabilities will be listed as potential and colored yellow.

	Confirmed Vulnerability	Security weakness verified by an "active test"
	Potential Vulnerability	Security weakness requiring manual verification
	Information Gathered	Configuration Data
	Half Red/Half Yellow	Results will vary depending on authentication

18 Qualys, Inc. Corporate Presentation

Qualys.

Confirmed vulnerabilities have one or more active tests, that can be used to confirm the presence of the vulnerability. Vulnerabilities of this type are color coded: red.

Potential Vulnerabilities include vulnerabilities that cannot be fully verified. In these cases, at least one necessary condition for the vulnerability is detected. It's recommended that you investigate these vulnerabilities further. The service can verify the existence of some potential vulnerabilities when authenticated trusted scanning is enabled.

Please note that even if a QID is detected by an authenticated scan or a cloud agent that doesn't mean that the vulnerability will be categorized as Confirmed. You can have potential vulnerabilities detected by authenticated scans and agents. These often include vulnerabilities where we don't have any mechanism to detect if the patch/workaround is applied or not.

Information gathered data or IG data for short, consists of various configuration settings and other host inventory and scan information. Information gathered QIDs are not vulnerabilities and are color coded: blue.

Vulnerability QIDs that are half-red/half-yellow, have two very predictable scan results, depending on your use of authentication. When scans are performed in authenticated mode, these vulnerabilities will be confirmed and colored red. When scan are performed without authentication, these vulnerabilities will be listed as potential and colored yellow.

VULNERABILITY SEVERITY LEVELS

To help you determine which vulnerabilities to address or mitigate first, Qualys provides severity levels or rankings for both confirmed and potential vulnerabilities.

A severity level 5 vulnerability is the most urgent, because it presents the greatest risk to your organization. A severity 5 vulnerability could potentially allow an attacker to gain root or admin privileges to the vulnerable host.

Confirmed	Potential	Severity Level	Description
		Minimal (1)	Intruders can collect information about the host via open ports or services, which can lead to the disclosure of other vulnerabilities.
		Medium (2)	Intruders can collect sensitive information from the host, such as software versions installed, which can reveal known vulnerabilities.
		Serious (3)	Intruders can gain access to security settings on the host, which could lead to: access to files and disclosure of file contents, directory browsing, denial of service attacks, and unauthorized use of services.
		Critical (4)	Intruders can potentially gain control of the host, or collect highly sensitive information including: read access to files, potential backdoors, or a listing of all user accounts on the host.
		Urgent (5)	Intruders can easily gain control of the host, which can lead to the compromise of your entire network. Vulnerabilities include: read and write access to files, remote execution of commands, and backdoors.

19 Qualys, Inc. Corporate Presentation

Qualys.

The service assigns every vulnerability in the KnowledgeBase a severity level, which is determined by the security risk associated with its exploitation. The possible consequences related to each vulnerability, potential vulnerability and information gathered severity level are described below. Qualys provides severity levels or rankings for both confirmed and potential vulnerabilities.

A severity level 5 vulnerability is the most urgent, because it presents the greatest risk to your organization. A severity 5 vulnerability could potentially allow an attacker to gain root or admin privileges to the vulnerable host.

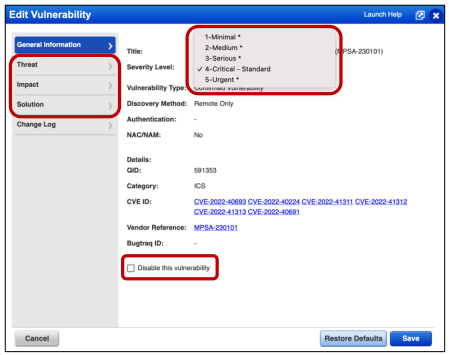
Severity level 3 and 4 vulnerabilities also involve some type of potential compromise of the host system or one of its applications or services.

A severity level 1 vulnerability is the least urgent. Severity level 1 and 2 vulnerabilities involve the disclosure of sensitive data that could potentially be very useful to an attacker.

Organizations should develop a strategy for mitigating detected vulnerabilities based on these severity levels. Because of their increased risk and exposure most organizations address the severity 3, 4, and 5 vulnerabilities first. However, the collective risk created by numerous low severity vulnerabilities should not be overlooked.

EDITING A QID

- Change Severity Levels
- Threat | Impact | Solution have user comments field
- Updates from the service not overridden
- Edited vulnerabilities are noted in Scan results
- Disabled vulnerabilities are still scanned for, but they are not reported or ticketed.
- Applies only to users with Manager role



Qualys.

Editing a vulnerability

Several vulnerability customization options give Managers greater control over how vulnerabilities appear in reports and how they are eventually prioritized for remediation. For example, by changing a vulnerability from a severity 2 to a severity 5, remediation tickets for the vulnerability could have a higher priority and shorter deadline for resolution.

About disabled vulnerabilities

When you disable a vulnerability, you need to rescan assets, so that it is globally filtered out from all hosts in all scan reports. The vulnerability is also filtered from host information, asset search results and your dashboard after the rescan. You may include disabled vulnerabilities in scan reports by changing report filter settings. Disabled vulnerabilities appear grayed out whenever referenced. They appear grayed out in the KnowledgeBase and in vulnerability scan results (only after you rescan the assets after disabling the QID).

How can I tell if a vulnerability has been edited?

A pencil appears next to the vulnerability when there is customized content and/or a changed severity level. You can also use the search option in the KnowledgeBase to find all vulnerabilities that were edited or disabled.

FURTHER RESOURCES

Page	Link	Description
Vulnerability Detection Pipeline	https://community.qualys.com/vulnerability-detection-pipeline/	Browse, filter by detection status, or search by CVE to get visibility into upcoming and new detections (QIDs) for all severities.
New Vulnerability Feature Request	https://success.qualys.com/discussions/s/article/000006767	This article will walk you through how to log a feature request

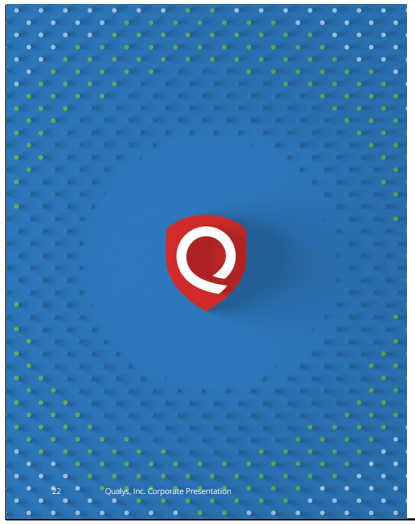
These links are also found in the Lab Tutorial Supplement - Appendix C

Qualys.

Here are some additional learning resources which you may find helpful.

https://community.qualys.com/vulnerability-detection-pipeline/
https://success.qualys.com/discussions/s/article/000006767

Recommendation - take a look at each site, and bookmark them for future use!



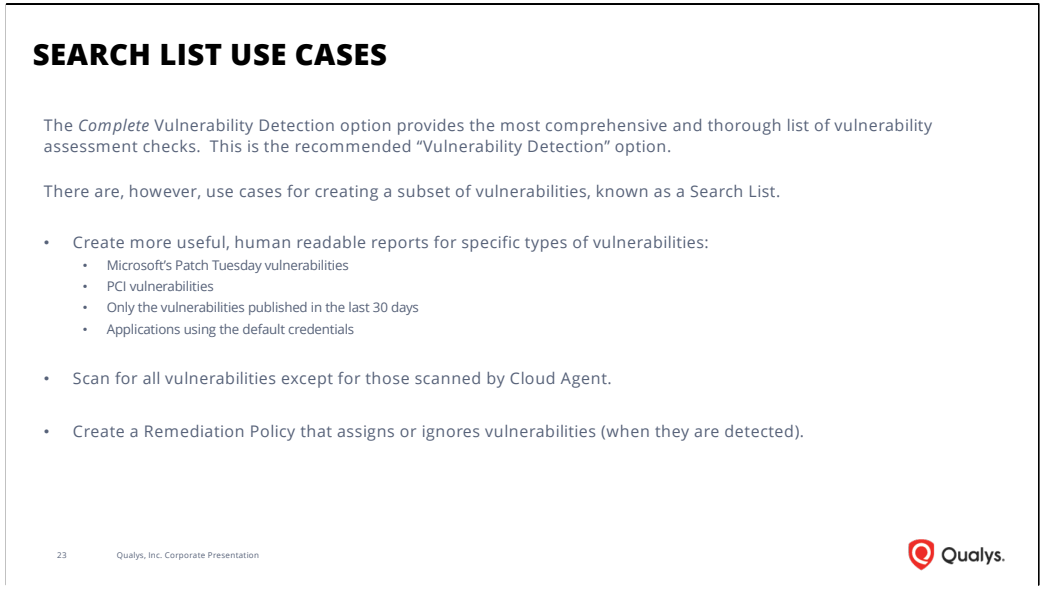
KNOWLEDGEBASE:

SEARCH LISTS

Qualys.

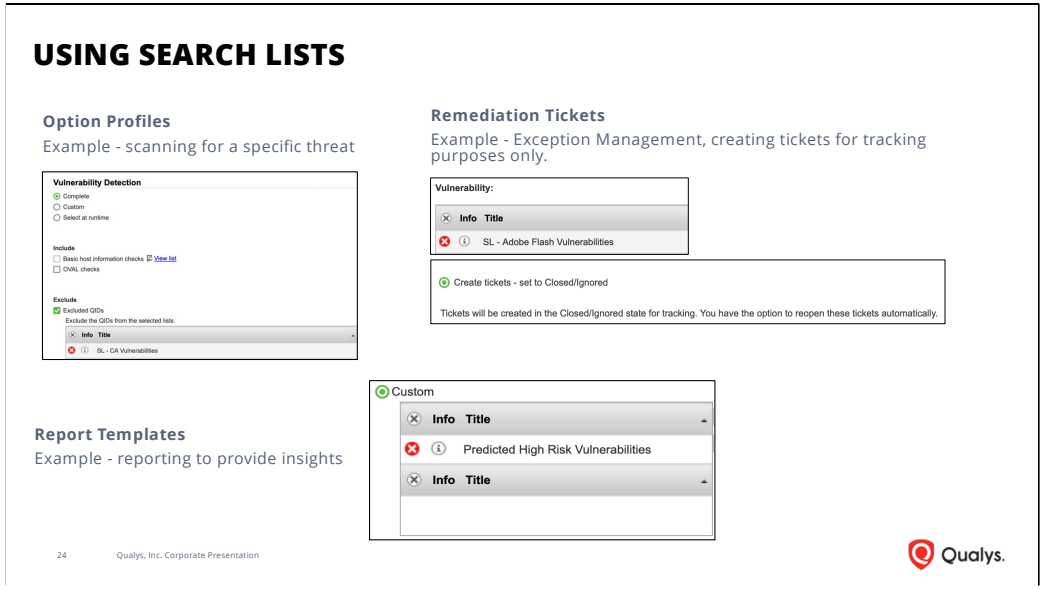
The objectives for this section is to learn:

What is a Search List
Where are they used
Why use Search Lists



Search lists are custom lists of vulnerabilities that you can save and use in order to customize vulnerability scans, reports and ticket creation.

Further ideas for Search Lists used in Reporting can be found here: https://success.qualys.com/discussions/s/article/000006215



A search list is one of the most powerful filtering tools in the Qualys Vulnerability Management application for tasks such as scanning, reporting, and remediation. You can use search lists to create vulnerability reports that focus on specific groups of vulnerabilities that are high priority targets within your organization.

You may find the need to target a specific list of vulnerability QIDs, when scanning (especially on those occasions where you don't have time to wait for a complete scan to finish). Remember: Qualys normally recommends scanning for everything, and then using Report Templates containing targeted search lists, to filter your scan results.

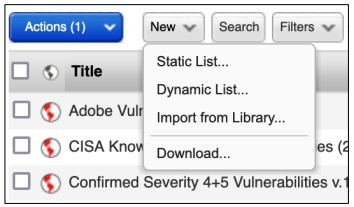
A remediation policy can be used to assign detected vulnerabilities to individuals (or operational teams) tasked with fixing or mitigating the vulnerabilities. You can also create a remediation policy that automatically ignores targeted QIDs.

SEARCH LIST OVERVIEW

There are two different types of Search List:

Static search list - Defined and updated manually.

Dynamic search list - Defined based on search criteria and updated when new QIDs are added to the knowledgebase.

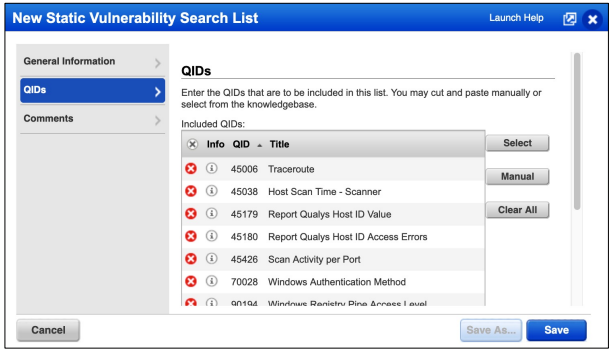


Qualys.

You can create a static list, a dynamic list or import a search list from the Qualys search list library.

STATIC SEARCH LIST

Static search list - Defined and updated manually.

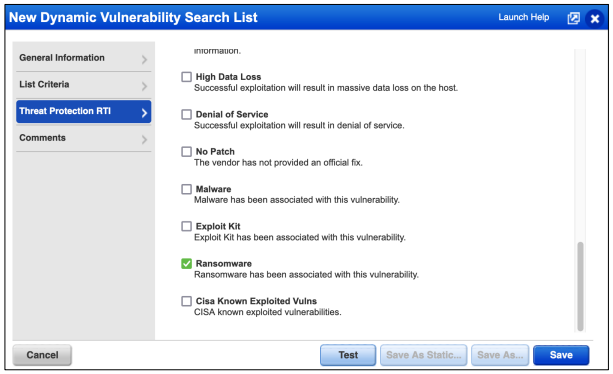


Qualys.

A static search list (as its name implies) contains a fixed number of QIDs and can only be created and updated, manually.

DYNAMIC SEARCH LIST

Dynamic search list - Defined based on search criteria and updated when new QIDs are added to the knowledgebase.

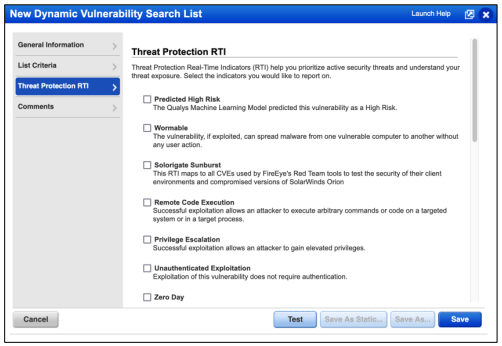


Qualys.

You can create a static list, a dynamic list or import a search list from the Qualys search list library.

For a dynamic search list, targeted QIDs must be specified using a "List Criteria" consisting of any combination of the KnowledgeBase search options. The criteria you specify here will determine which QIDs are presently added to the list, and moving forward it will determine whether or not new QIDs get added. You can use any of the search options found here in the KnowledgeBase search tool to build your own custom search lists.

USING RTI



- Risk = Threat x Vulnerability (Severity)
- Severity = Impact if vulnerability is exploited.
- Select one or more RTI options when creating a Search List.

Qualys.

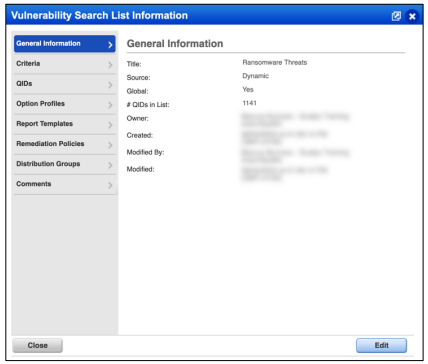
Traditionally the Qualys Vulnerability Management application has relied on severity levels (exclusively) to help you calculate the risk associated with your detected vulnerabilities. The higher the severity level the greater the risk.

With the addition of the Threat Protection application to the Qualys cloud platform, this calculation is improved by including known threats into the equation, which can have a significant impact on vulnerabilities of all severity levels.

The goal of Qualys Threat Protection is to help you pinpoint your assets that have the highest exposure to the latest known threats, so that you can prioritize and mitigate the high risk vulnerabilities quickly.

SEARCH LIST INFORMATION

- Detailed information about a Search List is available by clicking the ⓘ icon.
- General Info, list criteria, and all QIDs that match the criteria are shown.
- Also shown is a list of all report templates, option profiles and remediation rules where the list is used.

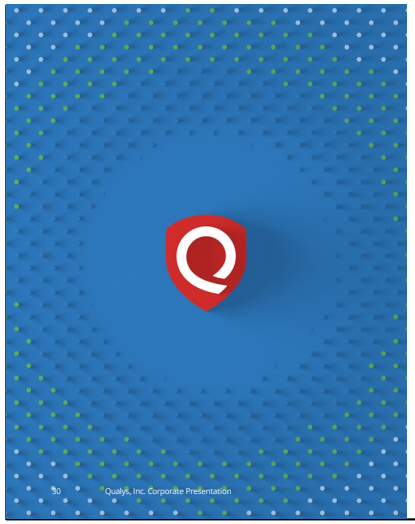


Qualys.

You can use the Quick Actions menu to edit an existing Search List or view its information.

Here you will find the list criteria, its list of QIDs, and any Option Profiles, Report Templates or Remediation Policies that use this list.

Distribution Groups can be created to receive email notifications about updates or additions to the QIDs in any list.



TRURISK

Qualys.

The objectives for this section are to learn:

What is TruRisk
What is TruRisk used for
Benefits of using TruRisk

Scoring mechanisms attempt to answer one key question: What should defenders focus on first?

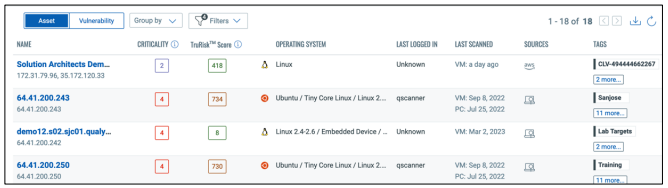
Attackers can exploit the vulnerabilities while you are in the process of reviewing, prioritizing, and patching all the reported vulnerabilities.

To address these challenges Qualys introduced Qualys VMDR 2.0 with TruRisk to help organizations prioritize vulnerabilities, assets, and groups of assets based on risk.

PRIORITIZE VULNERABILITIES BASED ON RISK

Qualys TruRisk™ assesses risk by taking into account multiple factors such as evidence of vulnerability exploitation, asset criticality, its location, and evidence of compensating controls on the asset among many other factors to assess the accurate risk posture for an organization.

With TruRisk, organizations can pinpoint which CVEs are exploited in the wild (even those that don't have a QID) and which malware, ransomware, or threat actor groups are exploiting them. These insights can then be used to prioritize vulnerabilities based on risk.

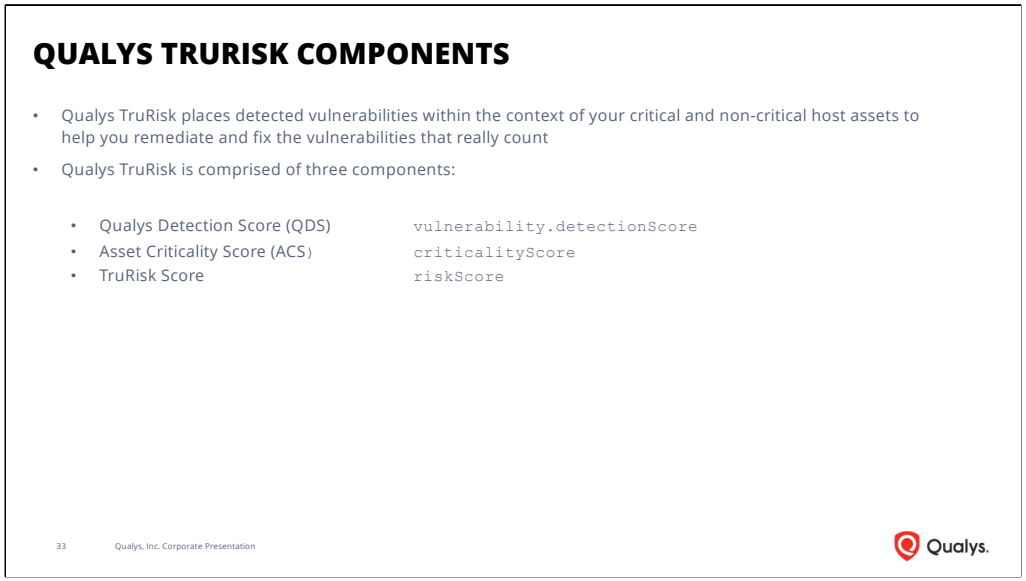


Qualys.

Qualys TruRisk assesses risk by taking into account multiple factors such as evidence of vulnerability exploitation, asset criticality, its location, and evidence of compensating controls on the asset among many other factors to assess the accurate risk posture for an organization.

With TruRisk, organizations can pinpoint which CVEs are exploited in the wild (even those that don't have a QID) and which malware, ransomware, or threat actor groups are exploiting them. These insights can then be used to prioritize vulnerabilities based on risk.

Qualys TruRisk vulnerability management include features like:
- intelligence-driven vulnerability severity scoring.
- detecting the location of assets vulnerabilities, including their business and operational criticality, association with business-critical applications, context about the asset's exposure to attack and many more.



Customers have struggled with optimizing how they prioritize responding to vulnerabilities. Using CVSS, EPSS, or even the Qualys severity levels will net thousands, or even millions, or vulnerabilities. This makes it near impossible for limited resources to figure out where priorities are. TruRisk is the brand, but the scoring is made up of 3 components you will see discussed over the next few slides. This scoring system takes into account just how critical the asset (or services it runs) is to your business, and then a understanding of the real risk of all the vulnerabilities on it.

Qualys TruRisk places detected vulnerabilities within the context of your critical and non-critical host assets to help you remediate and fix the vulnerabilities that really count.

Qualys TruRisk is comprised of three components:

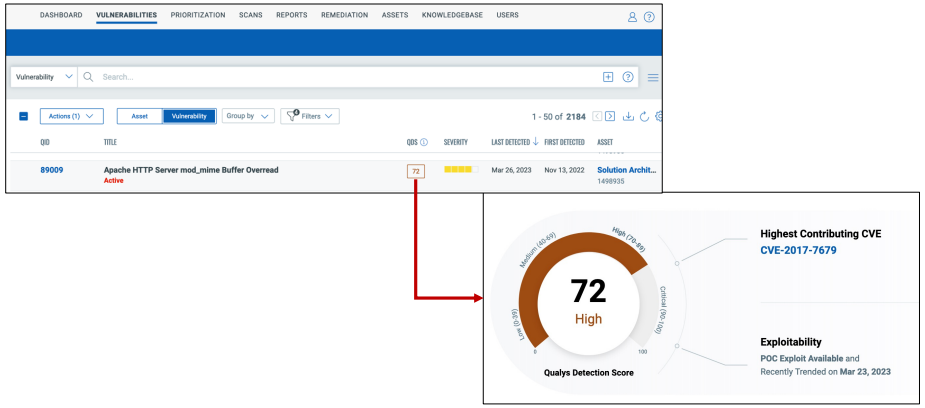
1. Qualys Detection Score (QDS) `/* token = vulnerability.detectionScore */`
2. Asset Criticality Score (ACS) `/* token = criticalityScore`

```
   */
```
3. TruRisk Score (ARS) `/* token = riskScore */`

Both QDS and ARS are calculated values, while ACS is assigned to assets via Asset Tags.

A deep dive into TruRisk can be found here:
https://blog.qualys.com/vulnerabilities-threat-research/2022/10/10/in-depth-look-into-data-driven-science-behind-qualys-trurisk

QUALYS DETECTION SCORE



34 Qualys, Inc. Corporate Presentation

Qualys.

Qualys Detection Score (QDS) begins with the CVSS base score of detected vulnerabilities. It then adds temporal factors such as Threat Intelligence (including exploit code maturity, associated malware, active threat actors, and vulnerabilities trending on the dark web) and mitigating and remediating controls related to the exposure.

QDS range is 1-100 and has four levels: Critical (90-100), High (70-89), Medium (40-69) and Low (1-39). QDS is derived from the following factors:

- Vulnerability technical details (e.g., CVSS base score)
- Vulnerability temporal details (Is the exploit code mature? Is the vuln associated with ransomware?)
- Vulnerability remediation details (Has the vendor released a patch?)

QDS considers:

- CVSS Score
- External Threat Intelligence (exploit code maturity, malware, active threat actors, and vulnerabilities trending on the dark web).
- Mitigating Controls (CIDs) associated with the vulnerability (host specific).

- Remediating Controls or patches
- It is important to note that if multiple CVEs contribute to a QID, the CVE with the highest score is considered for the QDS calculation.

A deep dive into TruRisk can be found here:
https://blog.qualys.com/vulnerabilities-threat-research/2022/10/10/in-depth-look-into-data-driven-science-behind-qualys-trurisk

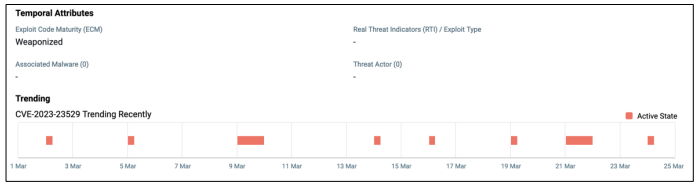
QUALYS DETECTION SCORE

Qualys Detection Score (QDS) begins with the CVSS base score of detected vulnerabilities (i.e., technical vulnerability details)

It then adds temporal factors such as Threat Intelligence (including exploit code maturity, associated malware, active threat actors, and vulnerabilities trending on the dark web)

Mitigating and remediating controls related to the exposure are included in the QDS calculation

Critical range indicates CVSS score is critical, there is a weaponized exploit available, and there is evidence of exploitation by threat actors



Qualys.

Qualys Detection Score (QDS) begins with the CVSS base score of detected vulnerabilities. It then adds temporal factors such as Threat Intelligence (including exploit code maturity, associated malware, active threat actors, and vulnerabilities trending on the dark web) and mitigating and remediating controls related to the exposure.

QDS range is 1-100 and has four levels: Critical (90-100), High (70-89), Medium (40-69) and Low (1-39). QDS is derived from the following factors:

- Vulnerability technical details (e.g., CVSS base score)
- Vulnerability temporal details (Is the exploit code mature? Is the vuln associated with ransomware?)
- Vulnerability remediation details (Has the vendor released a patch?)

QDS considers:

- CVSS Score
- External Threat Intelligence (exploit code maturity, malware, active threat actors, and vulnerabilities trending on the dark web).
- Mitigating Controls (CIDs) associated with the vulnerability (host specific).

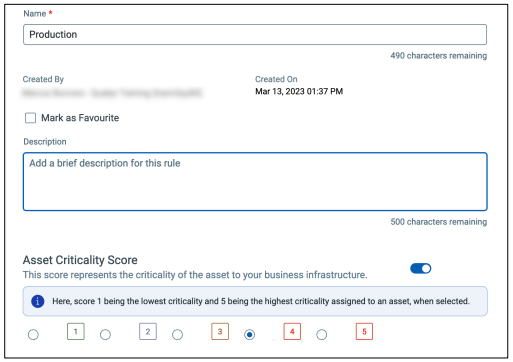
- Remediating Controls or patches
- It is important to note that if multiple CVEs contribute to a QID, the CVE with the highest score is considered for the QDS calculation.

A deep dive into TruRisk can be found here:
https://blog.qualys.com/vulnerabilities-threat-research/2022/10/10/in-depth-look-into-data-driven-science-behind-qualys-trurisk

ASSET CRITICALITY SCORE

You can configure the tags with asset criticality in the CSAM and Global AssetView apps. Navigate to CSAM > Tags

When integrated with ServiceNow CMDB, Qualys VMDR automatically imports business criticality for assets



Qualys.

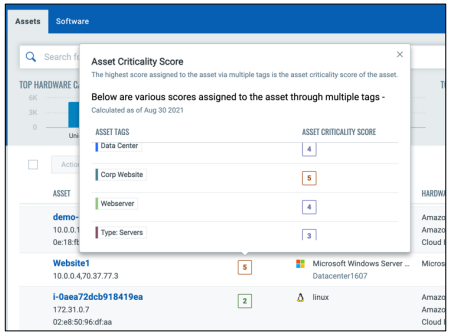
You can define the asset criticality score for a tag while creating asset tags in Global AssetView (GAV) / CyberSecurity Asset Management (CSAM).

You can set the asset criticality score between 1 to 5 with 1 being the lowest and 5 being the highest. If you don't select an asset criticality score, a criticality score of 2 is applied to the asset by default.

ASSET CRITICALITY SCORE

Asset Criticality Score (1-to-5) assigned to Asset Tags by users

Assets are then assigned the highest criticality score (evaluated across all Asset Tags presently assigned to the asset)



Qualys.

The INVENTORY section displays all assets where Qualys has collected data. Clicking on the Criticality score of an asset displays all the Asset Tags assigned to the asset along with their configured Criticality Scores. The Asset Criticality Score (ACS) is automatically calculated based on highest aggregated criticality across all tags assigned to the asset.

In this illustration, the asset has multiple tags with Criticality Scores of 5, 4 and 3. So the Asset Criticality Score of the asset is 5, that is, the highest Criticality Score among the assigned tags.

If the tags associated with your assets do not have criticality score set, by default the asset criticality score 2 will be applied to that asset.

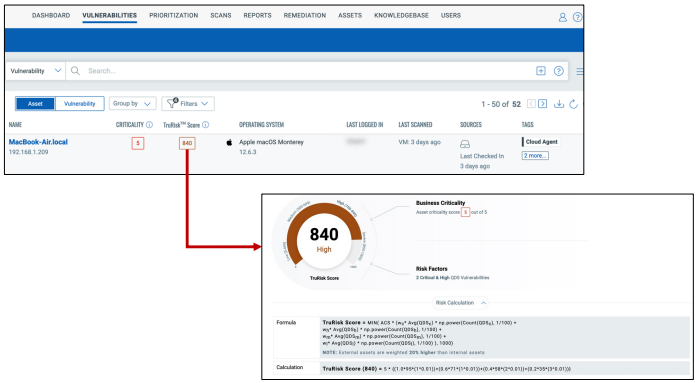
Asset criticality helps to focus your security prioritization efforts on high-importance and high-risk assets, by defining key business and technical context. Typically, asset criticality is derived by the function, environment and service the asset provides to the business.

Asset Criticality Score setting is turned off by default when creating a new

Asset Tag.

ACS has a big effect on the asset's risk score. It is very important to have a solid tagging structure and criticality values set that reflect to importance of your assets, or the services that run on them. Many customers have asked questions why an asset would have a low risk score, but high QDS scores. The reason for that is the criticality of the asset is low. There should be a company policy for defining critical assets and medium assets and low assets. This is very important because if everything is critical, then nothing is critical.

TRURISK SCORE



38 Qualys, Inc. Corporate Presentation

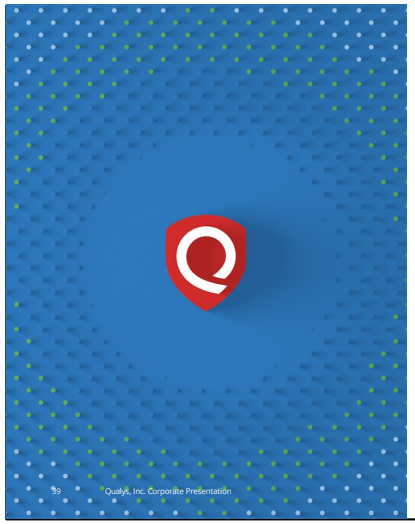
Qualys.

The TruRisk Score is the overall risk score assigned to the asset. The ARS range is between 0 to 1000, and is divided as follows:
- Severe: 850-1000
- High : 700-849
- Medium : 500-699
- Low: 0-499

TruRisk Score is calculated based on the following contributing factors:
a) Asset Criticality Score (ACS)
b) QDS scores for each QID level
c) Auto-assigned weighting factor (w) for each criticality level of QIDs

The following formula is used to calculate the TruRisk Score:
TruRisk Score = ACS * {wc(Avg(QDc)) + wh(Avg(QDSh)) + wm(Avg(QDSm)) + wl(Avg(QDSl))}
In the above formula:
ACS - Asset Criticality Score
w - weighing factor for each severity level of QIDs [critical(c), high(h), medium(m), low(l)]

Avg(QDS) - Average of Qualys risk score for each severity level of QIDs



ORGANIZING AND MANAGING ASSETS:

CATEGORIZATION, NORMALIZATION & ENRICHMENT

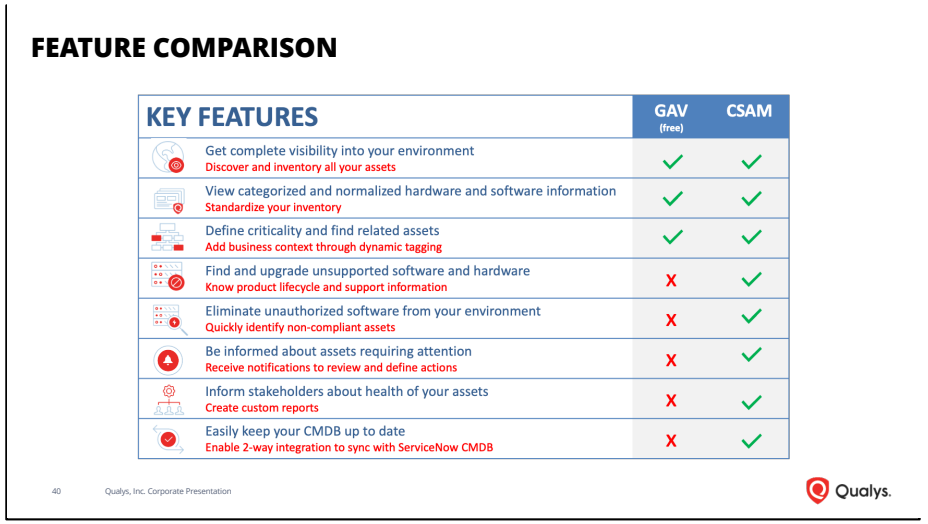
Qualys.

The objectives for this section is to learn:

The differences between Global Asset View (free) and Cybersecurity Asset Management (paid)

How GAV and CSAM categorize, normalize and enrich asset information.

How to perform a search based on the categorization, normalization and enrichment information.



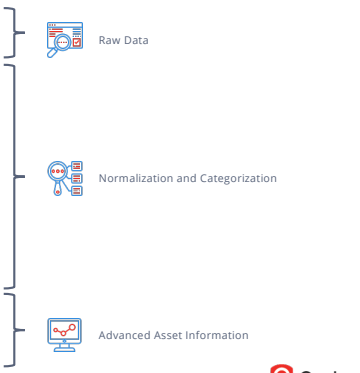
The table in the slide provides a high-level feature comparison between Global AssetView (GAV) and CyberSecurity Asset Management (CSAM). It is not meant to be an exhaustive list; you can speak to an account manager for more details on what CSAM includes over GAV.

GAV is free with any number of agents & passive scanners to give you baseline visibility of your asset inventory.

CSAM adds context for security-centric visibility with the detection of security gaps, External Attack Surface Management, CMDB integration, alerting, and response.

CATEGORIZATION, NORMALIZATION & ENRICHMENT

OPERATING SYSTEM	
Raw Data	Microsoft Windows Server 2022 Datacenter (21H2 Insider Preview Build 20348.169 64-Bit)
Category	Windows / Server
OS Publisher	Microsoft
Name	Windows Server 2022
Market Version	2022
Edition	Datacenter
Release	Microsoft Windows Server 2022 Datacenter (21H2 Insider Preview Build 20348.169)
Architecture	64-Bit
Lifecycle Stage	GA
End of Service	Oct 14 2031
License Type	Commercial



Qualys.

Normalization & categorization
Eliminates the variations in product and vendor names and categorizes them by functional category and product families. Automated normalization and classification of asset data maps
raw asset data to Qualys product catalog to obtain clean, complete, and reliable data.

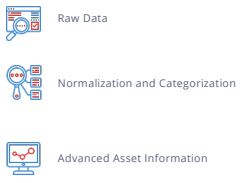
Normalized data in CyberSecurity Asset Management (CSAM) has operating systems categorized based on an internally developed classification/ categorization system.
It follows a two-level classification system – namely Level 1 Category and Level 2 Category
- Level 1 Category: Indicates the operating system family.
- Level 2 Category: Indicates whether the operating system is for client, server or virtualized environments.
Example:
a) "Apple macOS High Sierra" → Mac / Client → Level 1: Mac, Level 2: Client
b) "VMware ESXi" → Virtualization / Hypervisor Type-1 (Bare Metal) → Level

1: Virtualization, Level 2: Hypervisor Type-1 (Bare Metal)
There are currently 13 Level 1 categories and 5 Level 2 categories for classifying operating systems.

Enrichment
OS, hardware, and software data is then enriched with Lifecycle stage and support information. This information is not only important from a security perspective, it's also useful to the people in you company that are tasked with hardware and software budgeting and procurement.

CATEGORIZATION, NORMALIZATION & ENRICHMENT

HARDWARE	
Raw Data	IBM Power System S924 9009-42G
Category	Computers / Server
Manufacturer	IBM
Name	Power System
Model	S924
Lifecycle Stage	Generally Available
End of Support	Not Announced

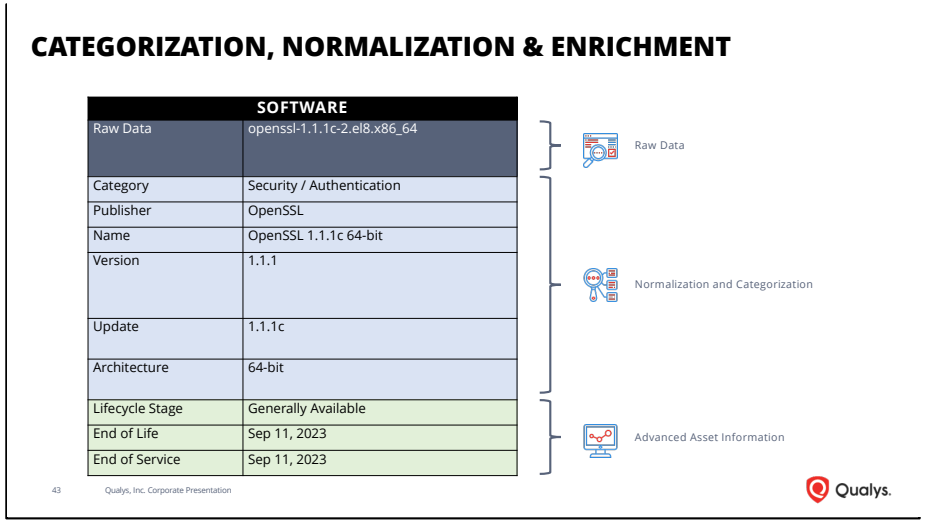


Qualys.

Normalization & categorization
Eliminates the variations in product and vendor names and categorizes them by functional category and product families. Automated normalization and classification of asset data maps
raw asset data to Qualys product catalog to obtain clean, complete, and reliable data.

Categorization
The Qualys platform categorizes hardware assets based on an internally developed classification/categorization system. The categorization, which gives the user an idea about the primary function of the product, has been derived from standard industry terms as well as other well-known industry classification systems.
It follows a two-level classification system – namely Level 1 Category and Level 2 Category
- Level 1 category: Major/ broad category to which the hardware asset belongs.
- Level 2 category: Subcategory, i.e specific to the product's primary function.

Enrichment
OS, hardware, and software data is then enriched with Lifecycle stage and support information. This information is not only important from a security perspective, it's also useful to the people in you company that are tasked with hardware and software budgeting and procurement.



Normalization & categorization
Eliminates the variations in product and vendor names and categorizes them by functional category and product families. Automated normalization and classification of asset data maps
raw asset data to Qualys product catalog to obtain clean, complete, and reliable data.

Categorization
Normalized data in CyberSecurity Asset Management (CSAM) has software applications categorized based on an internally developed classification/ categorization system. The categorization, which gives the user an idea about the primary function of the product, has been derived from standard industry terms as well as other well-known industry classification systems.
It follows a two-level classification system – namely Level 1 Category and Level 2 Category
Level 1 Category: Major or broad category to which the software application belongs.
Level 2 Category: Subcategory, i.e. specific to the product's core function.

Enrichment
OS, hardware, and software data is then enriched with Lifecycle stage and support information. This information is not only important from a security perspective, it's also useful to the people in you company that are tasked with hardware and software budgeting and procurement.

NORMALIZE SEARCHES WITH ASSET CATEGORIES

Use hardware, software, and OS tokens to help "normalize" your query conditions to uncover more precise asset details.

Syntax	Examples
`hardware.category1: value1`	`hardware.category1: `Networking Device``
`hardware.category2: value2`	`hardware.category2: `Switch``
`hardware.category: value1 / value2`	`hardware.category: `Networking Device / Switch``
`operatingSystem.category1: value1`	`operatingSystem.category1: `Windows``
`operatingSystem.category2: value2`	`operatingSystem.category2: `Server``
`operatingSystem.category: value1 / value2`	`operatingSystem.category: `Windows / Server``
`software:(category1: value1)`	`software:(category1: `Security`)`
`software:(category2: value2)`	`software:(category2: `Endpoint Protection`)`
`software:(category: value1 / value2)`	`software:(category: `Security / Endpoint Protection`)`

Qualys.

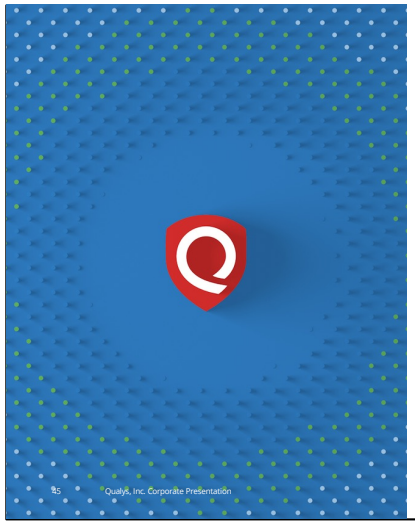
The hardware, operating system, and software categories can be handy when performing asset searches within the CyberSecurity Asset Management application.

To build a query, choose a token and provide a value. Combine category1 and category2 values using the generic "category" token (a slash character must separate the category1 and category2 values).

The Qualys catalog is vast. In the CSAM Inventory section, use the following to determine value1 and value2:

- Group Assets by – Hardware – Category
- Group Assets by – Operating System – Category
- Software – Group Software by – Category

This will show the category 1 and category 2 values of the Qualys catalog that match your asset population.



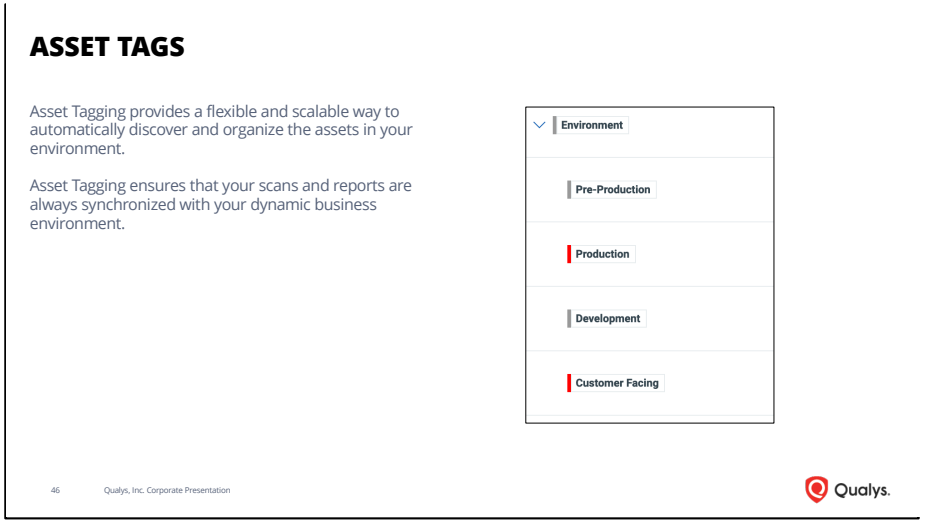
ORGANIZING AND MANAGING ASSETS:

ASSET TAGS

Qualys.

The objectives for this section is to learn:

What Asset Tags are, and how they can be used.



Asset management is key to security because of the number, variety and dynamic nature of assets. Only with a clear view of assets can they be managed and secured.

Asset Tagging is a flexible labelling system that has the ability to understand and apply one or more tags as labels to assets in an automated manner using rules. We refer to labels as tags, and they can be used to organize, search and prioritize assets across all Qualys solutions such as VMDR, Web Application Scanning, and Policy Compliance.

Asset Tagging provides a flexible and scalable way to automatically label and organize the assets in your environment and ensures that your scans and reports are always synchronized with your dynamic business environment.

Asset tags are commonly grouped or organized into Asset Tag Hierarchies. These hierarchies allow you to nest one asset tag below another, creating various parent/child relationships (the idea or objective is to build child tags that represent a subset of host assets represented by its associated parent tag).

Qualys Platform will already create the following tags for you:
Business Units

Business Units tag is a parent tag. The child tags underneath are for the business units in your account are created. Assets in a business unit are automatically assigned the tag for that BU.

Asset Groups

Asset Groups tag is a parent tag. The child tags underneath are for the asset groups in your account. Assets in an asset group are automatically assigned the tag for that asset group. You create Asset Groups in VMDR.

Asset Search Tags

Asset Search Tags is a parent tag. The child tags underneath are tags that you create from the Asset Search area of VMDR.

Cloud Agent

Cloud Agent tag is created by the system and will be applied to all assets that have the Cloud Agent deployed. This is a quick way to reference your asset population with agents deployed.

Internet Facing Assets

Internet Facing Assets tag is created and assigned to an asset if it has a public-facing IP address.

Unmanaged

All passively sensed assets that do not have a cloud agent or have not been scanned by Qualys scanner have this tag

Passive Sensor

All assets reported by the passive sensor appliance have this tag.

ICS_OCA

The assets sensed from project files uploaded by the user in the Industrial Control System (ICS) module have this tag.

EASM

All assets reported by Qualys External Attack Surface Monitoring have this tag.

Shodan

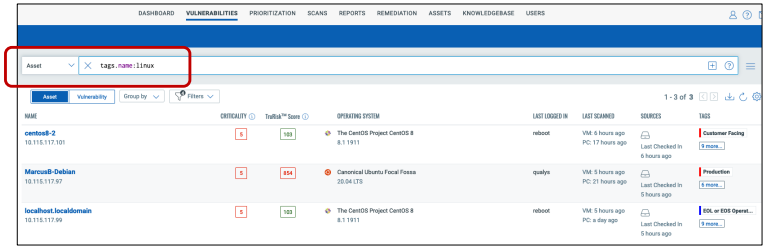
This is a legacy tag that is applied to assets when Qualys pulls information from Shodan. EASM is the tag you should reference when navigating your external inventory.

Default Dashboard Access Tag

This tag is added to new dashboards to allow by default all users to view all dashboards.

ASSET TAGS

Asset Tags can be specified with Qualys Query Language to filter list results.



47 Qualys, Inc. Corporate Presentation

Qualys.

Asset Tagging provides a flexible and scalable way to automatically label and organize the assets in your environment and ensures that your scans and reports are always synchronized with your dynamic business environment

In this example, an Asset Tag called ”Linux” is being used with the Qualys Query Language to filter search results.

ASSET TAGS

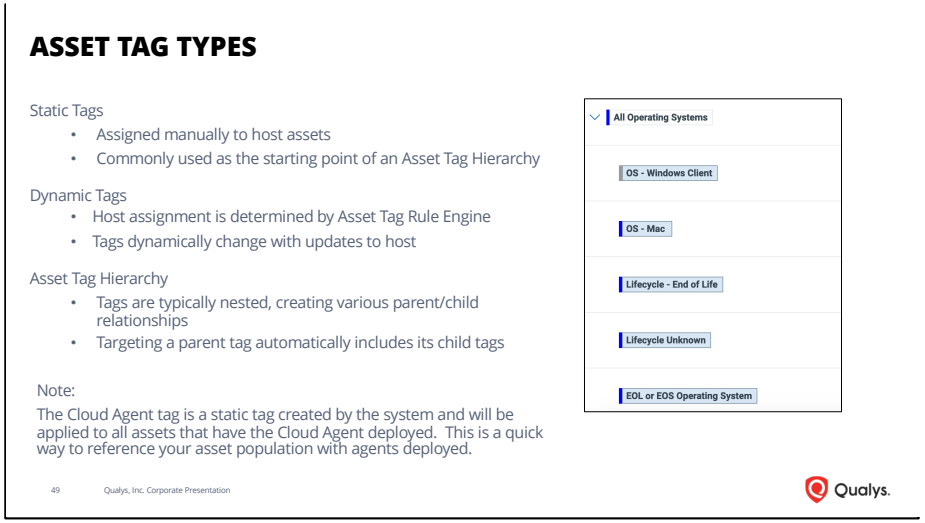
Asset Tags can be used to filter dashboard results.

48 Qualys, Inc. Corporate Presentation

Qualys.

Dashboards help you visualize your assets. Each dashboard is a collection of widgets showing resource data of interest.

Asset tags can be used to filter dashboard results.



Basic Asset Tag behaviors and characteristics:

Static tags: You can build static tags that you would then manually assign to selected host assets within your account. Static tags are commonly used to establish the starting point for individual asset tag hierarchies.

Dynamic tags: These are automatically assigned to host assets, based on their rule engine. Asset tag rule engines focus on different host attributes, and when these attributes change, so do their respective tags.

Asset tags are commonly grouped or organized into Asset Tag Hierarchies. These hierarchies allow you to nest one asset tag below another, creating various parent/child relationships (the idea or objective is to build child tags that represent a subset of host assets represented by its associated parent tag).

Qualys Platform will already create the following tags for you:

Business Units

Business Units tag is a parent tag. The child tags underneath are for the business units in your account are created. Assets in a business unit are automatically assigned the tag for that BU.

Asset Groups

Asset Groups tag is a parent tag. The child tags underneath are for the asset groups in your account. Assets in an asset group are automatically assigned the tag for that asset group. You create Asset Groups in VMDR.

Asset Search Tags
Asset Search Tags is a parent tag. The child tags underneath are tags that you create from the Asset Search area of VMDR.

Cloud Agent
Cloud Agent tag is a static tag created by the system and will be applied to all assets that have the Cloud Agent deployed. This is a quick way to reference your asset population with agents deployed.

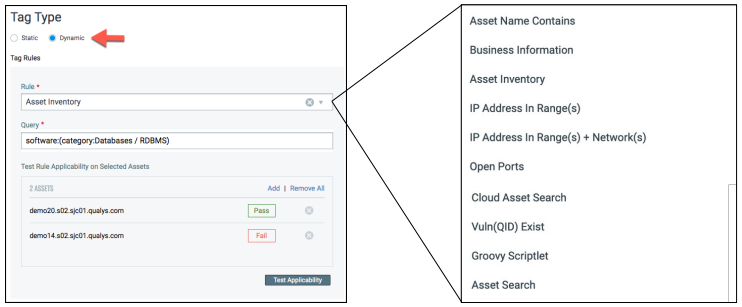
Internet Facing Assets
Internet Facing Assets tag is created and assigned to an asset if it has a public-facing IP address.

Newer Tags:
- Unmanaged: All passively sensed assets that do not have a cloud agent or have not been scanned by Qualys scanner have this tag.
- Passive Sensor: All assets reported by the passive sensor appliance have this tag.
- ICS_OCA: The assets sensed from project files uploaded by the user in the Industrial Control System (ICS) module have this tag.
- EASM: All assets reported by Qualys External Attack Surface Monitoring have this tag.
- Shodan: This is a legacy tag that is applied to assets when Qualys pulls information from Shodan. EASM is the tag you should reference when navigating your external inventory.
- Default Dashboard Access Tag: This tag is added to new dashboards to allow by default all users to view all dashboards.

DYNAMIC RULE-BASED TAGS

The “Asset Inventory” rule engine allows you to build tags using query tokens, including the Hardware, OS, and Software category tokens.

Other “dynamic” rule engines are also available.



Qualys.

Learning to build queries is a very useful skill, in the Qualys UI. From queries you can build both Dashboard Widgets and Asset Tags.

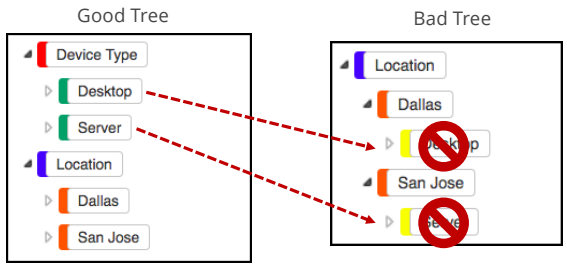
When building Asset Tags, the ”Asset Inventory” rule engine can be used to leverage the power of the hardware, OS, and software categories.

Other dynamic rule engines are also available.

Some other example use cases for Dynamic Asset Tags are:

•You are trying to get your assets listed by their operating systems or firmware versions.
•You might be looking for the active assets in your subscription.
•You need a list of software that you installed on your assets within a specific period.
•You are looking for a list of open ports on your machines.

ASSET TAG HIERARCHY DESIGN



- Attempt to group tag hierarchies (parent/child relationships) around some type of common criteria.
- Child tags do NOT inherit the attributes or properties of their parent tags.
- Multiple tags can be combined when selecting targets for scanning and reporting

Qualys.

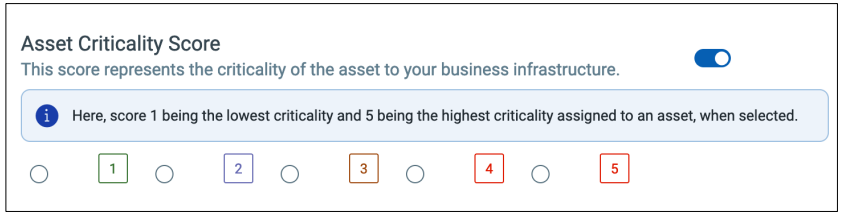
Do your best to choose tag names that are descriptive, but brief.

To help organize Asset Tag hierarchies, avoid mixing multiple types of rule engines in a single hierarchy.

With this design structure in place, multiple Asset Tags can be combined when selecting targets for scanning and reporting.

The ”Desktop” and “Server” tags in the “Bad Tree” do not inherit location information from their parents.

ASSET CRITICALITY SCORE

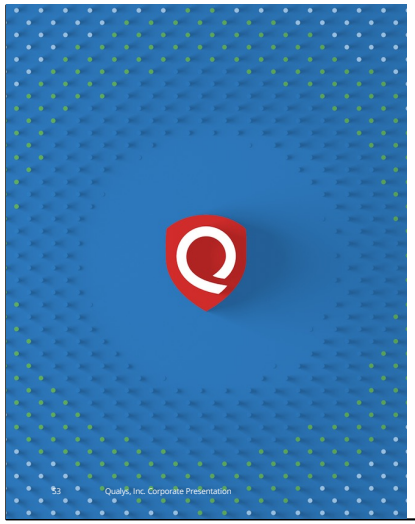


An assets criticality score is determined by its assigned Asset Tags

A default score of 2 is used for assets without assigned tags

Qualys.

An assets criticality score is determined by its assigned Asset Tags. A default score of 2 is used for assets without assigned tags.



ORGANIZING AND MANAGING ASSETS:

CMDB INTEGRATION

Qualys.

The objectives for this section is to learn:

How the Qualys platform integrates with two major third-party CMDB platforms.

SERVICENOW INTEGRATION

CERTIFIED SERVICENOW CMDB SYNC APP

- Supports 2-way sync (Qualys to ServiceNow and ServiceNow to Qualys)
- Up-to-date, categorized, normalized, and enriched ServiceNow CMDB
- Enrich Qualys assets with key CMDB business data

VMDR FOR SERVICENOW ITSM

- Automate vulnerability management and get rid of vulnerability spreadsheets and PDF files, using an integrated (closed-loop) ticketing solution
- Imported Qualys vulnerability findings will reveal FIXED vulnerabilities, along with the newly detected vulnerabilities
- Vulnerability findings are assigned to their appropriate owner, automatically
- ServiceNow tickets can be closed automatically for vulnerabilities with a FIXED status
- ITSM is included with VMDR

VMDR for ITSM Tutorial
This video describes the VMDR for ITSM app, it's features and functionalities.

Qualys.

Note: When integrated with ServiceNow CMDB, Qualys VMDR automatically imports business criticality for assets. This has an impact on how you manage Asset Criticality Score (it is otherwise assigned manually) and therefore the TruRisk score.

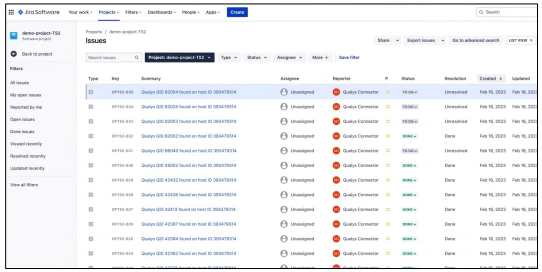
An introduction of integration with ServiceNow is provided by this video: https://vimeo.com/723255182

JIRA INTEGRATION

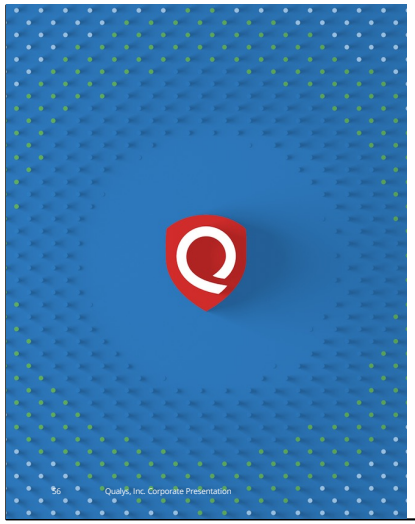
Atlassian Jira is widely used for issue and project tracking.

Seamless integration of VMDR with Jira to leverage it for tracking the vulnerabilities end to end from discovery to remediation.

Streamline IT and Security operations to reduce time for remediation.



Qualys VMDR integration with Jira helps organizations automate vulnerability remediation workflows by providing real-time visibility into vulnerability status and streamline IT and Security operations to reduce time for remediation. The integration helps you to bring vulnerability context in Jira and to streamline the overall vulnerability tracking process along with the owners. The best part is we support both Cloud and on-premises Jira instances.



ORGANIZING AND MANAGING ASSETS:

ASSET GROUPS

Qualys.

The objectives for this section is to learn:

How the Qualys platform integrates with two major third-party CMDB platforms.

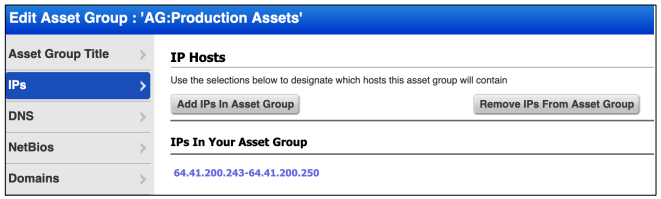
ASSET GROUPS

Asset Groups allow you to manually group “scannable” assets in your account.

You typically build multiple Asset Groups that reflect your scanning targets.

Should be IP ranges, not individual lists of IPs

A matching Asset Tag is created for each Asset Group.



Qualys.

Asset Groups are set up within VM/VMDR. Instead of typing in IP address ranges for your scan targets, you can organize these IP blocks into Asset Groups. You typically build multiple Asset Groups that reflect your customary or regular scanning targets.

An Asset Group is a logical container for IP addresses. We recommend building them by full IP ranges and not individual IP addresses.

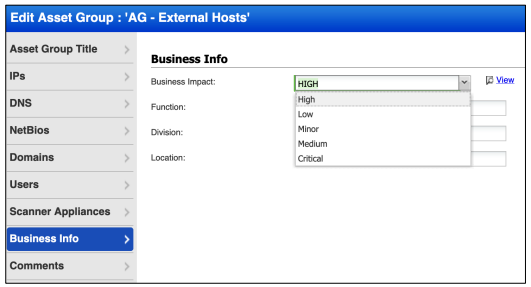
We recommend using Asset Tags to organize assets around criteria such as Operating System, device type, business priority, etc. It is best to build Asset Groups by IP range/location.

An IP address may belong to more than one Asset Group. It is not possible to nest Asset Groups (a group within a group).

BUSINESS IMPACT SCORE

Note the Business Impact setting:

- The business impact level you select is automatically applied to all hosts in the group.
- The default impact is High.
- The Business Impact level that you select has a direct relationship to the Asset Criticality Score assigned to Asset Tags.
- An Asset Tag which is automatically generated from an Asset Group will inherit the Business Impact level.



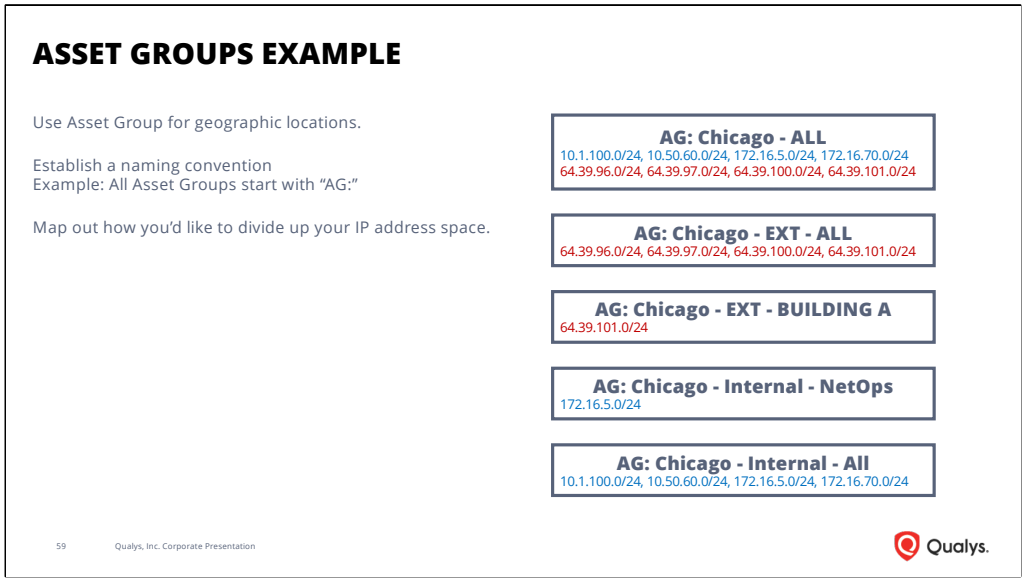
Qualys.

Note the Business Impact setting:

- The business impact level you select is automatically applied to all hosts in the group.
- The default impact is High. This means that the Asset Tag which gets created based on this Asset Group will have an Asset Criticality Score of 4.
- The Business Impact level that you select has a direct relationship to the Asset Criticality Score assigned to Asset Tags. An Asset Tag which is automatically generated from an Asset Group will inherit the Business Impact level.

Business Impact Level Critical = Asset Criticality Score 5
Business Impact Level High (default) = Asset Criticality Score 4
Business Impact Level Medium = Asset Criticality Score 3
Business Impact Level Minor = Asset Criticality Score 2
Business Impact Level Low = Asset Criticality Score 1

You should consider setting the Business Impact Level to Minor so that the Asset Tag with the same name which gets automatically created is assigned an Asset Criticality Score of 2.



Thoughtfully planning your Asset Group structure will save time scanning your hosts with a scanner appliance and when going to report. Understanding how you want to build your scans will be a piece of this puzzle.

In this example, you see Asset Groups built for a Chicago location. There are ALL groups for both internal (private IP addressing) and external (public IP addressing) Asset Groups. From there, there are smaller groups to identify the specific buildings or network segments / subnets.

We recommend prefixing Asset Group names with "AG:"
This is so that when a corresponding tag gets created, you can easily identify the Asset Groups created in VM/VMDR.

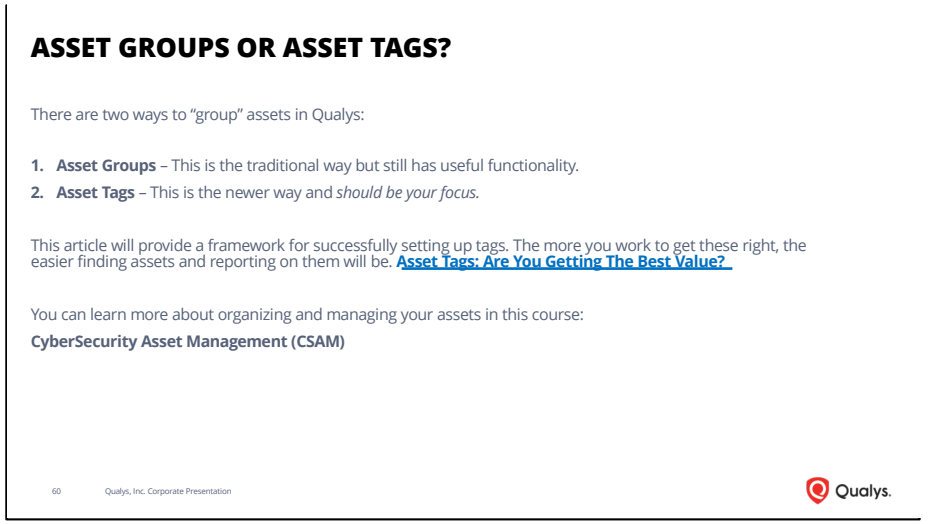
By using this type of naming convention, you can find all assets in any building or any location very easily.

The Asset Groups for each building reflect where you should deploy scanner appliances and then scan those locally (instead of trying to scan

all of Chicago from one location).

Example queries:
- Show all internal assets regardless of location
tags.name:" – Internal"

- Show all external assets regardless of location
tags.name:" – EXT"



Organize Assets

Your sensors will collect data about your assets, but you must organize them in Qualys. This is a vital piece of success and often frustrates organizations.

There are two ways to "group" assets in Qualys:

1. Asset Groups – This is the traditional way but still has useful functionality.
2. Asset Tags – *This is the newer way and should be your focus.*

When to use Asset Groups

1. Use these only when defining IP RANGES.
2. Don't use them with scattered individual IP addresses.
3. These are typically used when SCANNING (using a Scanner Appliance) full ranges of your network for vulnerabilities.
4. These are typically NOT useful when running reports (use tags instead).
5. If you set these up correctly, you'll make scanning much easier on

yourself in the long run. Use this article to help you set up both groups and tags:
https://success.qualys.com/support/s/article/000005819

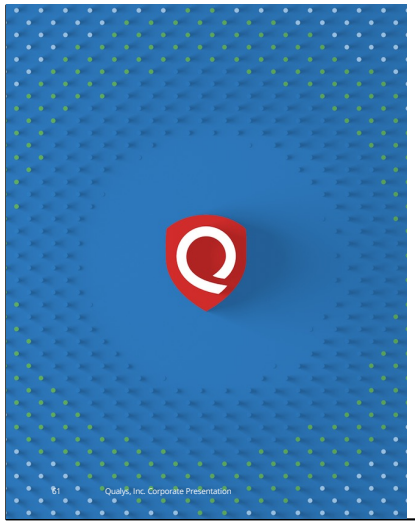
When to use Asset Tags

1. When you are grouping assets by categories like OS, Device Type, Software.
2. These allow you to set a Criticality on any asset with a given TAG. This will be VITAL later on when it comes to reporting and remediation.
3. This article will provide a framework for successfully setting up tags. The more you work to get these right, the easier finding assets and reporting on them will be. https://success.qualys.com/support/s/article/000005819
4. Don't forget about Asset Criticality - this is an important piece to helping automate where prioritization should occur in your environment. https://blog.qualys.com/product-tech/2022/12/12/operationalizing-qualys-vmdr-with-qualys-trurisk-part-1

Get certified on our CSAM application here: https://qualys.com/training

By the end of this, you should:

- Start visualizing how your Asset Groups should look
- Start visualizing how your Asset Tags should look



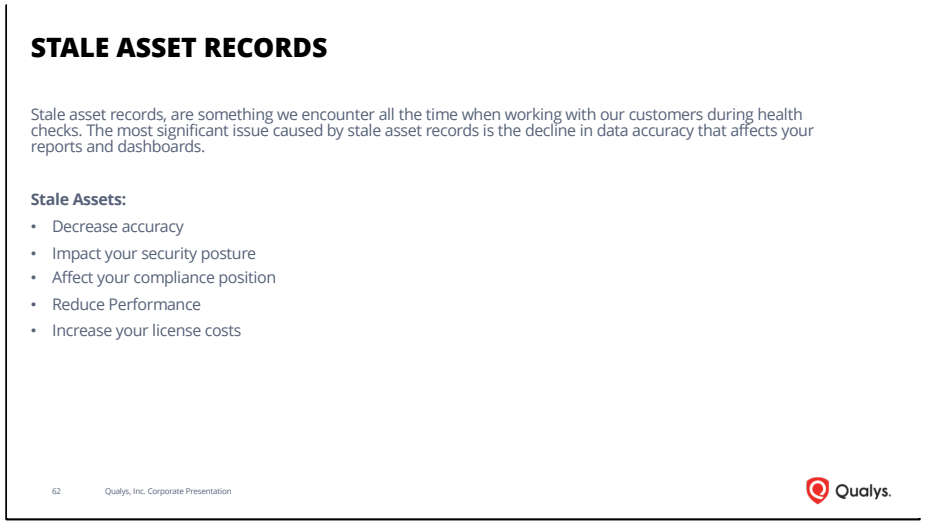
ORGANIZING AND MANAGING ASSETS:

ACCOUNT MAINTENANCE

Qualys.

The objective of this section is to learn:

How stale assets can affect your subscription
What is ”purging”.



Organizations' cloud environments and assets rapidly grow as they transition to the cloud. Many of the assets within the cloud are 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, as an issue, are something we encounter all the time when working with our customers during health checks. The most significant issue caused by stale asset records is the decline in data

accuracy that affects your reports and dashboards.

Stale Asset 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 an easily avoidable problem, with the automated purge features available in Qualys to remove these assets automatically.

Purging is covered in more detail in our *Reporting Strategies and Best Practices* course.

LEARNING RESOURCES

Link	Description
Purging: What, why, when, how, what happens to the data?	This article will walk you through how purging works.
Purging Stale Data	Watch this video on why you need a good purging practice for account maintenance. This will save you and your team time and energy in the long run.
Subscription Health Dashboard and Purging Explanation	Find the Subscription Health dashboard on this page. Download the file as a JSON file and import it into your account.
Qualys Help for setting up purge rules	This will show you the process for setting up purge rules.

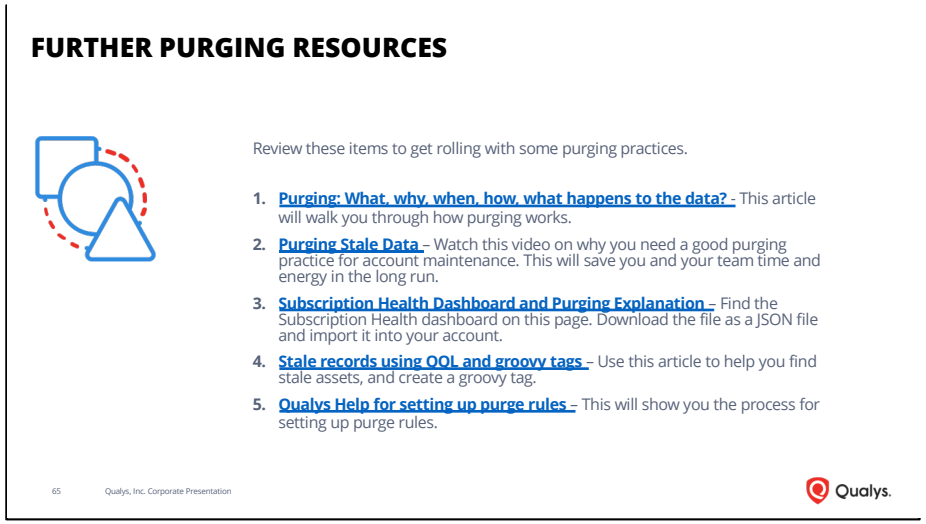
These links are also found in the Lab Tutorial Supplement - Appendix E

Qualys.

Here are some additional learning resources which you may find helpful.

https://www.qualys.com/training/
https://qualys.com/learning
https://www.qualys.com/docs/qualys-cloud-platform-whitepaper.pdf
https://www.qualys.com/documentation/
https://www.qualys.com/training/library/vmdr-onboarding/

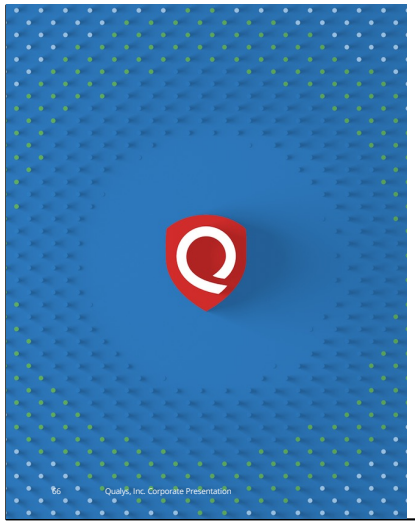
Recommendation - take a look at each site, and bookmark them for future use!



Review these items to get rolling with some purging practices.

1. Purging: What, why, when, how, what happens to the data? - This article will walk you through how purging works.
2. Purging Stale Data – Watch this video on why you need a good purging practice for account maintenance. This will save you and your team time and energy in the long run.
3. Subscription Health Dashboard and Purging Explanation – Find the Subscription Health dashboard on this page. Download the file as a JSON file and import it into your account.

4. Stale records using QQL and groovy tags – Use this article to help you find stale assets, and create a groovy tag.
5. Qualys Help for setting up purge rules – This will show you the process for setting up purge rules.



VULNERABILITY ASSESSMENT

Qualys.

The objective of this section is to learn:

The Vulnerability Scan components.

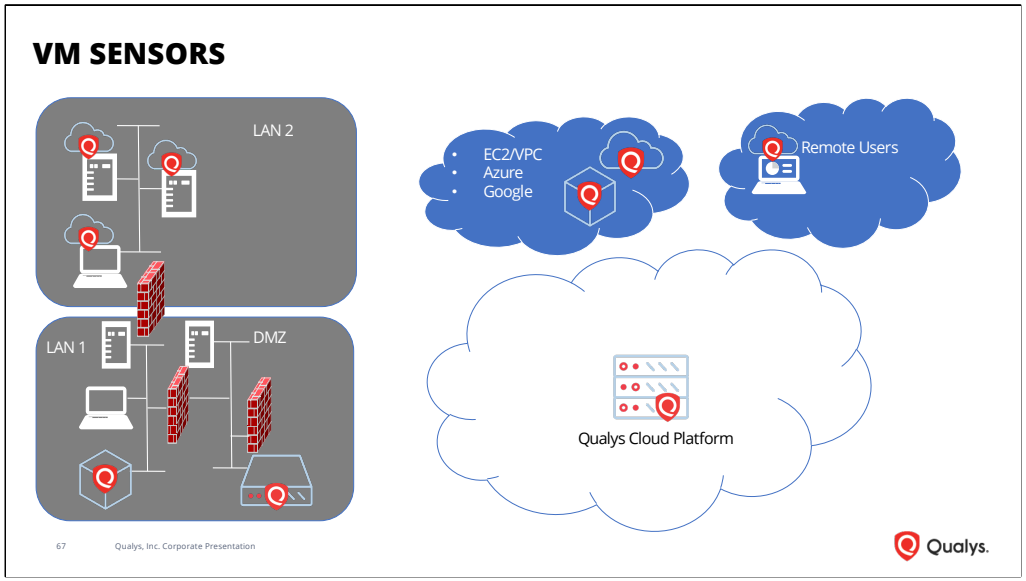
How to configure Authentication.

How to configure a scan using an Option Profile.

How to launch a scan.

How to view the raw scan results.

How data is collected from an Agent host.



The Qualys Vulnerability Management application provides more than one option for collecting the data needed to perform a host vulnerability assessment.

A Qualys Scanner Appliance has a REMOTE perspective of any host you target. Its ability to perform a vulnerability assessment test, is directly impacted by the number and type of open service ports on any given host, as well as the presence of any network filtering devices that might potentially obstruct individual scan packets.

Qualys Cloud Agent; on the other hand, is installed as a local system service on each host; one agent per host. Agents operate with system level privileges, automatically sending assessment data back to the Qualys Cloud Platform at regularly scheduled intervals.

It is common for businesses and organization to combine both agents and scanners to meet their vulnerability assessment needs.

Our training lab targets live in a typical DMZ environment, where the

perimeter firewall has been configured to allow packets from Qualys' External Scanner Pool. External scanners are ideal for scanning public facing targets, or host assets with a public IP address. By default, any Qualys user with scanning privileges, has access to the External Scanner Pool.

Internal scanner appliances are commonly used to scan host assets that reside on PRIVATE IP subnets like LAN 1 in this diagram. Deploying an internal scanner appliance as a member of this subnet, will allow you to scan subnet assets directly, without the obstacle of network filtering devices.

LAN 2 in this diagram presently does not have a scanner appliance and is isolated from the rest of the network by a firewall. To meet the vulnerability management objectives for this subnet, Qualys Cloud Agent will be installed on each host. Each agent will collect metadata from its host and send it to the Qualys Cloud Platform for processing. Vulnerability assessment tests (all the heavy lifting) are intentionally kept off of the agent, and performed within the Qualys Platform. Qualys Cloud Agent is ideal for Remote Users (or any host assets that are difficult to scan), and it can be deployed on assets hosted by your Cloud Service Providers.

HOST PERSPECTIVES

A scanner appliance has a remote perspective since it scans into the host through open ports

Cloud Agent has a local perspective since it installs as a thin service on the host's OS

Use Case for scanning a Cloud Agent host:

The Cloud Agent can see how apps are configured locally, but it cannot create network connections which direct back onto the asset to each app's hosted services or open ports

This is a use case for vulnerabilities where the assessment needs a network connection to detect/confirm the vulnerability (TLS, SSL, HTTP, etc.)

QIDs with "Remote Only" Discovery Method will not be covered by the Cloud Agent

This would be a recommended practice assets that host networking services, like Servers

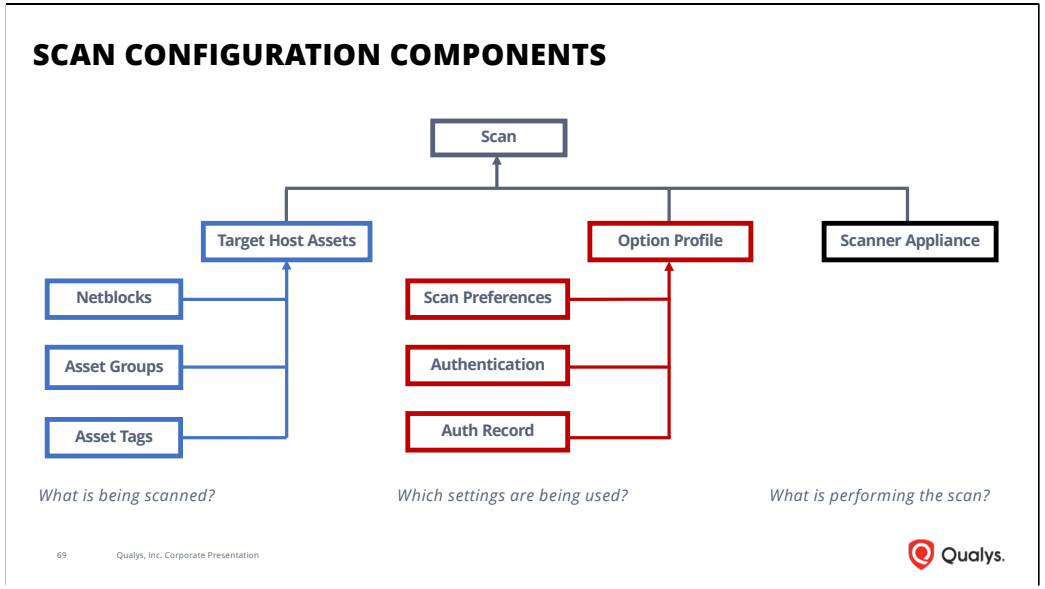
Qualys.

To better understand the benefits provided by Qualys Cloud Agent and the benefits of a Qualys Scanner Appliance, it helps to understand the different PERSPECTIVES that each option provides.

A Qualys Scanner Appliance has a REMOTE perspective of any host you target. Its ability to perform a vulnerability assessment test, is directly impacted by the number and type of open service ports on any given host, as well as the presence of any network filtering devices that might potentially obstruct individual scan packets.

Qualys Cloud Agent; on the other hand, has a LOCAL perspective of its host system. QIDs with Remote Only Discovery Method in the Qualys KnowledgeBase require a network connection to detect/confirm the vulnerability. The agent cannot create networking connections back onto the asset to assess every hosted service. This introduces a use case to run supplemental scans for agent assets that host services, like server systems. Scanning an agent host, gains the benefit of having both LOCAL and REMOTE perspectives for the same host.

Authentication can be used for the scan, but it is not a necessary condition. Remote Only Discovery QIDs are performed without authentication.

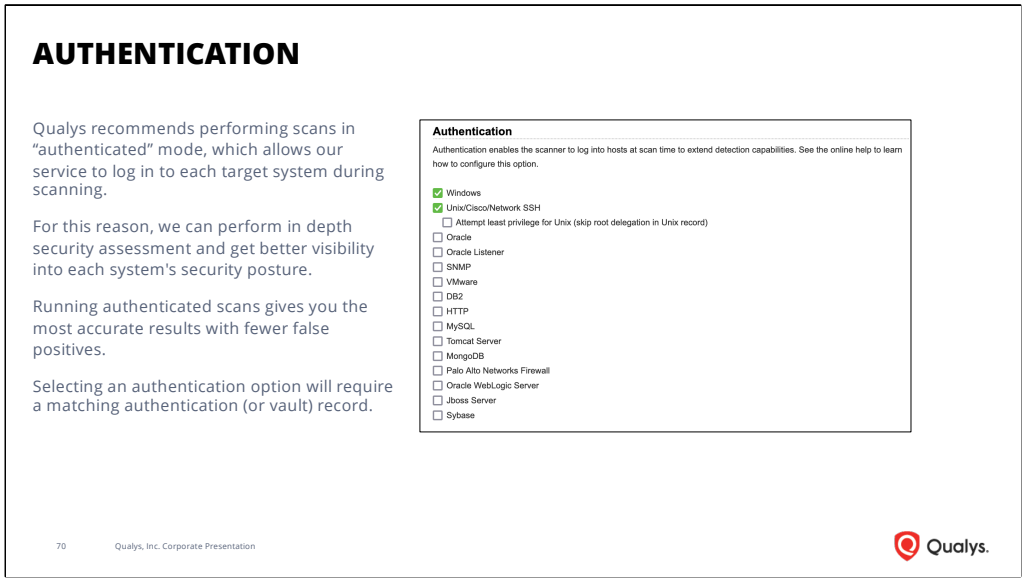


This diagram illustrates the basic components that comprise a vulnerability scan. To launch a vulnerability assessment scan you will certainly need at least one scanner appliance. The lab exercises in this course use the Qualys Cloud's Pool of External Scanners, which is the default setting for the Qualys student trial account you may be using. When selecting a scanner appliance for any scan task, you will need to consider the host assets your scan intends to target, which is another required component for launching a scan.

Your scanning targets include netblocks or specific ranges of IP addresses or even a single IP address in your Qualys subscription. Host IPs must be added to your subscription first, before you can scan them. Any host asset in your Qualys subscription can be added to an Asset Group which is another option for targeting a scan.

Asset Tags, the last scan target option, provide a dynamic and automated solution for managing host assets in your Qualys subscription.

Every vulnerability assessment scan must select an Option Profile, containing various scan preferences and scanning options. If your scan uses an Option Profile with authentication enabled, one more component, an authentication record, is added to this of required scan components.

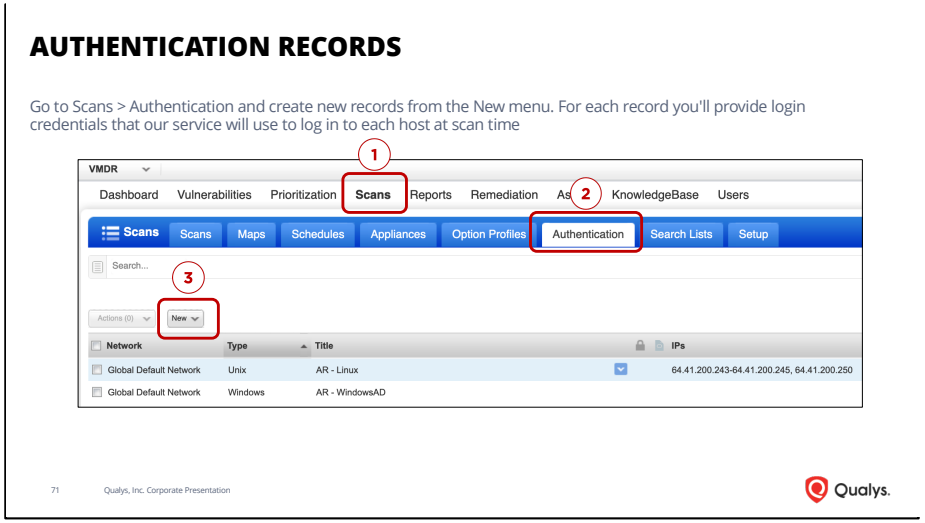


Using host authentication (trusted scanning) allows our service to log in to each target system during scanning. For this reason we can perform in depth security assessment and get better visibility into each system's security posture. Running authenticated scans gives you the most accurate results with fewer false positives.

The authentication type you select here, will require a matching authentication record under the "Authentication" tab.

Please keep in mind that some of the authentication types (such as database and application servers) are not required by the Qualys Vulnerability Management application, but are used by the Qualys Policy Compliance application, instead.

Add authentication vaults, if applicable. We support integration with multiple third party password vaults. Go to Scans > Authentication > Vaults and tell us about your vault system. Then choose Authentication Vault in your record. At scan time, we'll authenticate to hosts using credentials retrieved from your vault.



Go to Scans > Authentication and create new records from the New menu. For each record you'll provide login credentials that our service will use to log in to each host at scan time. Each record is defined for a technology, like Windows, Unix, Oracle, etc and you can have multiple records per technology.

Credentials are securely handled by the service and are only used for the duration of the scan.

Process Overview

Step 1 – Set up a Windows user account to be used by our security service for authentication.

Step 2 – Using Qualys:

1) Create Windows authentication records.

2) Select an option profile. For a vulnerability scan be sure to select “Windows” in the Authentication section.

3) Launch a scan.

4) Verify that authentication passed for each target host. Tip - Run the Authentication Report to view the authentication status (Passed or Failed)

OPTION PROFILE

The Option Profile defines the settings you want to use for a scan job.

Scan Options include:

- TCP & UDP Port config
- Performance
- Authentication
- Firewalls detected
- Load Balancers detected

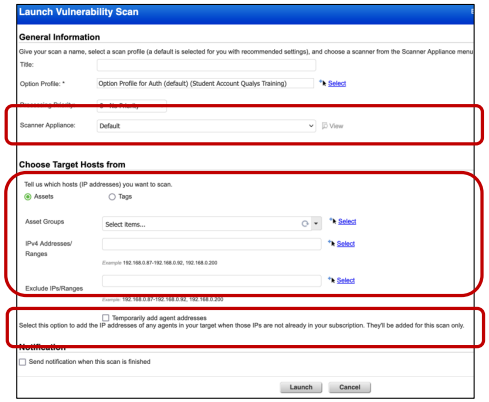
Please see the Qualys *Scanning Strategies and Best Practices* self-paced training class for a more detailed discussion and analysis of scan settings and features found in the Option Profile.

Qualys.

In this course we focus on the basic configuration settings in an option profile, such as the TCP and UDP port settings, preset scan performance options, vulnerability detection options, and the different options for performing a scan in authenticated mode.

For an extended discussion of these and other scanning topics, please see the Qualys Scanning Strategies and Best Practices training course.

LAUNCH ASSESSMENT SCAN - SCAN SETTINGS



Which scanner appliances will be used for this scan?
If this option does not appear, then your scans will use external scanners automatically.

Which assets will be scanned?
You can choose target hosts from Assets (IPs, asset groups, FQDNs) or from Tags.

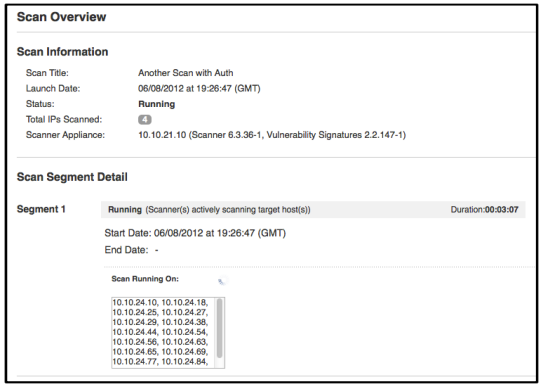
Will this scan include Cloud Agent hosts?
This option temporarily adds the IP addresses of any agents in your target to your subscription *for this scan only*. This option cannot be used with the External scanner option.

Qualys.

To launch a vulnerability scan:

1. Enter a descriptive Title.
2. Select an Option Profile.
3. Select appropriate scanner appliance(s).
4. Select scanning target(s).
5. Click the “Launch” button.

ASSESSMENT SCAN - ON DEMAND



You can monitor scans as they run.

Choose View from the Quick Actions menu for any running scan.

Qualys.

You can monitor scans as they run.

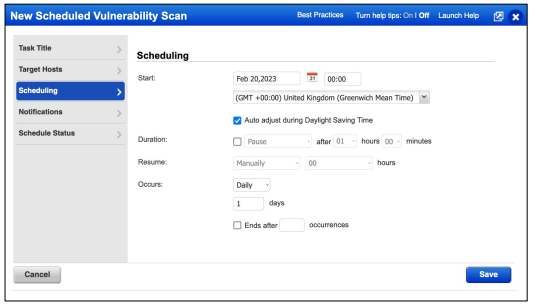
Choose View from the Quick Actions menu for any running scan. You'll see the IPs that have already been scanned, the IPs currently being scanned and the IPs waiting to be scanned. For a vulnerability scan, you can also access partial results as they become available. Once the scan is finished you'll be able to view and download the full results.

When the scan has completed, the scan status will show "Finished". At this time you can select View from the Quick Actions menu to see the full results in an HTML report.

SCHEDULING ASSESSMENT SCANS

Automate Your Scans

- Assessment scans can be scheduled to run at daily, weekly or monthly intervals.
- Schedules can be paused to comply with maintenance windows.
- Send notifications before and after each scan.



Qualys.

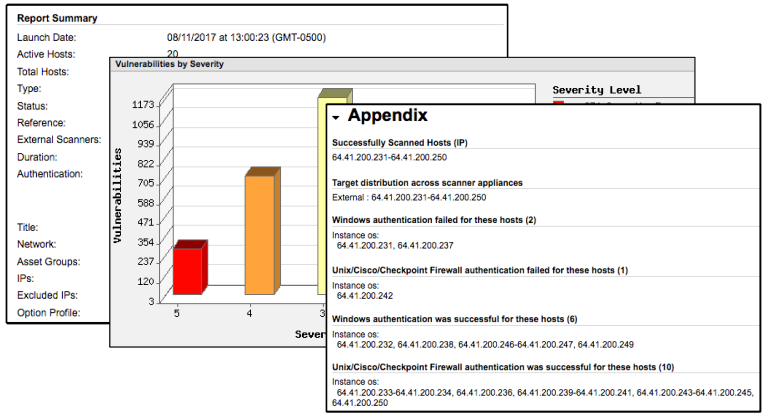
What obviously makes a scheduled scan different are the Scheduling options. Begin by selecting the date and time for this scheduled scan to start. The start time for each scheduled scan will reflect the time zone you specify.

To keep this scan from bumping into high-demand or peak capacity times of day, you can choose a maximum scan duration and the action to take, if any scan reaches this threshold. If you configure the option to pause a long running scan, you'll need to specify how and when you would like it to resume.

You can schedule your scans to run daily, weekly, or monthly. You can schedule scans that have an unlimited number of occurrences, or select the option to deactivate a scheduled scan after a set number of occurrences is reached. Notifications will automatically be sent to the owner of a scheduled scanning task.

Additional options are available for sending notifications before and after a scan, to any email distribution groups you create.

SCAN RESULTS SUMMARY



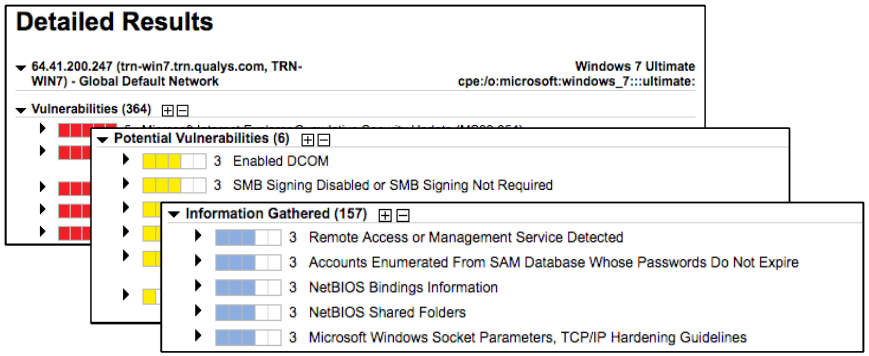
Qualys.

The "summary" section at the top of the report includes information like:

- Scan date, time and duration
- Information about the host assets targeted
- IP address of the scanner appliance
- Short summary of authentication results

The "Appendix" at the bottom provides more details about the hosts that were successfully or unsuccessfully scanned and a breakdown of the scanning options configured within the option profile

SCAN RESULTS DETAIL



Unfiltered, raw data of your scan targets

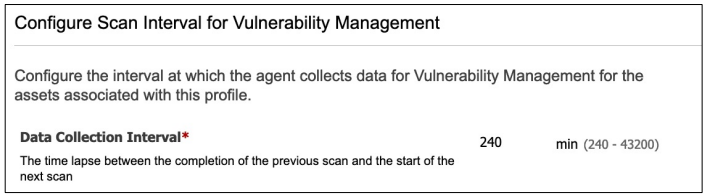
Qualys.

By default, a raw scan report is designed to display all scan findings and details, including:

- information gathered findings
- potential vulnerability findings
- confirmed vulnerability findings

Simply expand any of the findings to view the vulnerability details, such as: the vulnerability title, QID number, Solution for fixing or mitigating the vulnerability, and all other QID data items and information found in the Qualys KnowledgeBase; a raw scan report contains everything.

AGENT DATA COLLECTION INTERVAL



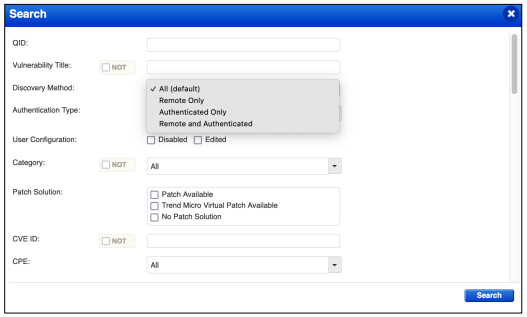
- Data Collection Interval setting specifies the frequency of VM, PC, and SCA scans.
- At each interval agents perform assigned tasks and collect host metadata (as specified in the application manifest(s).
- To complete each interval, collected data is transferred to the Qualys Platform for processing.
- NOTE: The countdown to the very next interval will begin as soon as the data transfer and post-processing steps have been completed.

Qualys.

The VM, PC, and SCA Scan Interval setting determine how often Cloud Agent collects vulnerability and compliance assessment data. Configured at its minimal value, data collections will occur every four hours.

NOTE: The countdown to the very next interval will begin as soon as the data transfer and post-processing steps have been completed. The countdown to the next interval begins at the END of the previous interval (i.e., it does NOT begin at the START of the previous interval).

REMOTE ONLY QIDS



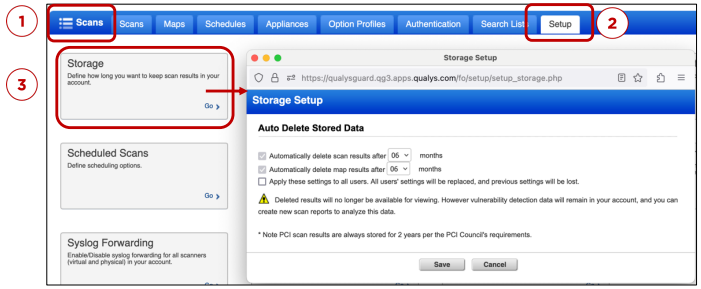
- A Qualys Scanner's "remote" perspective is required to detect "Remote Only" QIDs.
- Perform supplemental scans for agent hosts that are impacted by "Remote Only" QIDs.
- These hosts will have both SCAN data and AGENT data.

Qualys.

Supplemental scans (using a Qualys Scanner Appliance) may be performed on agent hosts, to provide coverage for "Remote Only" QIDs.

SCAN RESULTS STORAGE

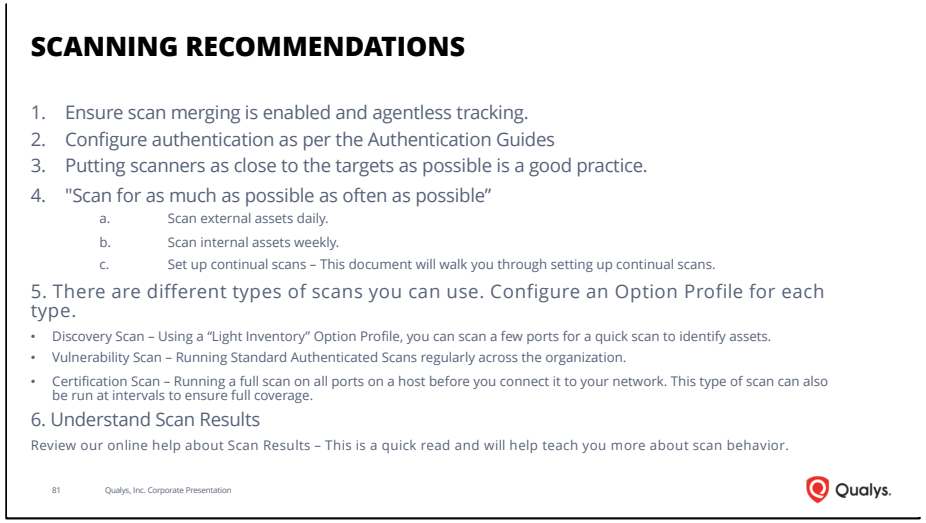
The principal contact in your organization can configure scan data storage.



Qualys.

The Storage Setup dialog shows for how long the Qualys platform will store your raw scan and map results. This can be changed as needed by the principal contact in your organization.

Any raw results older than that specified here will be discarded by the Qualys platform. These are the results you can see under than Scans tab.



Top Tips for Scanning Success

1. Ensure scan merging is enabled and agentless tracking.
2. Authentication Guides – Use these guides to set up authenticated scanning for the most thorough assessment.
3. Deploy scanners to meet the organization's demand. Putting scanners as close to the targets as possible is a good practice.
4. "Scan for as much as possible as often as possible"

a. Scan external assets daily.
b. Scan internal assets weekly.
c. Set up continual scans – This document will walk you through setting up continual scans.

5. There are different types of scans you can use. Configure an Option Profile for each type.

a. Discovery Scan – Using a "Light Inventory" Option Profile, you can scan a few ports for a quick scan to identify assets.
b. Vulnerability Scan – Running Standard Authenticated Scans regularly across the organization.
c. Certification Scan – Running a full scan on all ports on a host before you connect it to your network. This type of scan can also be run at

intervals to ensure full coverage.

6. Understand Scan Results

a. No Host Alive – If you run a scan and receive the message “No Host Alive,” you’ll want to troubleshoot your scan. Make sure you understand how hosts get discovered during a scan.

b. Review our online help about Scan Results – This is a quick read and will help teach you more about scan behavior.

c. Ghost Hosts – If IP addresses appear in your scan results as “scanned,” but you know there is no actual host associated with that IP address, this is called a “Ghost Host.”

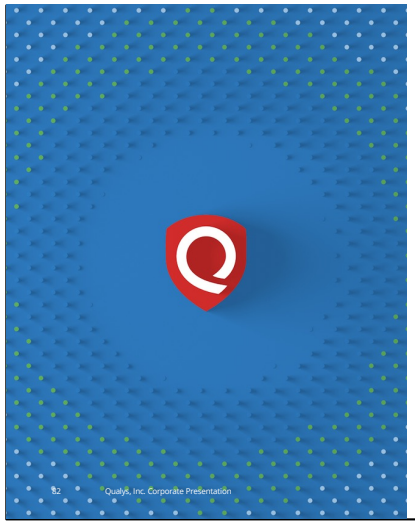
i. Here are some Solutions:

1. Place a scanner as close to the target as possible.

2. Consider using VLAN scanning.

ii. Long Scan Times - Use this article to troubleshoot long scan times.

Get Certified on Scanning Strategies and Best Practices
Go to qualys.com/training



REPORTING:

PRIORITIZATION

Qualys.

The objective of this section is to learn:

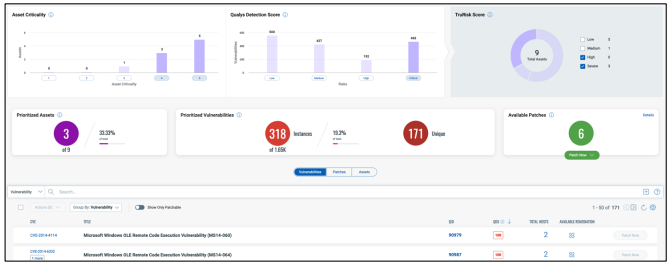
Prioritization Report - using RTIs

Prioritization Report - TruRisk Mode

VMDR PRIORITIZATION REPORT

VMDR Prioritization identifies and remediates the vulnerabilities that pose risk to your organziation and business.

The Prioritization process correlates the vulnerability information with threat intelligence and asset context to zero in on the highest risk vulnerabilities.



The VMDR Prioritization report guides you to focus resources in the right area to first patch the highest risk vulnerabilities.

Qualys.

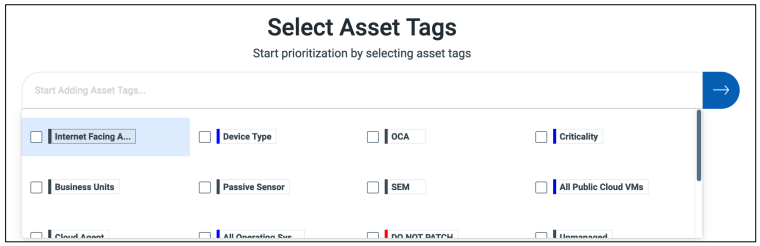
VMDR Prioritization identifies and remediates the vulnerabilities that pose risk to your organziation and business. The Prioritization process correlates the vulnerability information with threat intelligence and asset context to zero in on the highest risk vulnerabilities.

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

Patch Management app is enabled in your subscription).
- Includes only the confirmed vulnerabilities.

We provide you with the following two options to prioritize the remediation of vulnerabilites based on:
- Age, RTI, and Attack Surface,
- Qualys TruRiskTM Mode

USE ASSET TAGS TO ADD CONTEXT



- Design and build Asset Tags that help to distinguish the "context" of your assets.
- Leverage tags that use the "Asset Inventory" rule engine, along with

1) hardware 2) software and 3) OS categories

Qualys.

Not all assets within your business or enterprise architecture are the same. Some assets are considered critical, others are not. Different assets perform different functions (they provide different services) and are impacted by different vulnerabilities and threats.

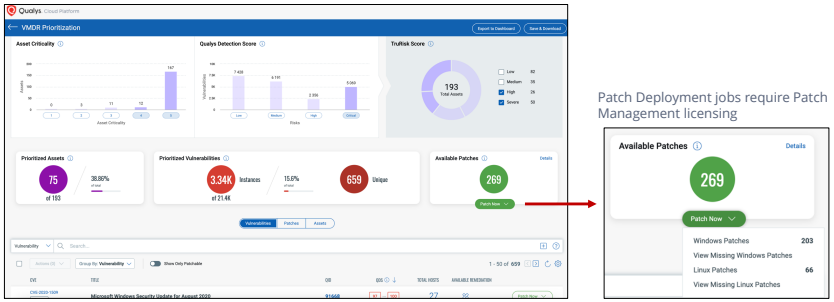
The very first step in building a Prioritization Report, provides context by targeting specific host assets. This is where the Asset Tags you create play a very important role.

The "Asset Inventory" rule engine that applies tags based on hardware, OS, and software categories can be very useful here.

You'll want to keep the Prioritization Report in mind when building and designing Asset Tags for you Qualys account.

Add one or more tags == OR operator

PRIORITY OPTIONS - TRURISK OPTION



Patch Deployment jobs require Patch Management licensing

85 Qualys, Inc. Corporate Presentation

Qualys has introduced the TruRisk feature. Using this feature, you can detect vulnerabilities within the context of your critical and non-critical host assets to help you remediate and fix the vulnerabilities that really count.

This mode provides data for Asset Criticality, Qualys Detection Score (QDS), and TruRisk Score (ARS). This mode helps prioritize Assets or Vulnerabilities based on risks generated in the result.

Qualys TruRisk™ can help streamline and automate the patch management process by providing risk-based prioritization of vulnerabilities and mapping them to the appropriate patches

Toggle the Qualys TruRisk Mode button to enable prioritization with TruRisk. The priority options change when this mode is enabled.

Asset Criticality Score:
This represents the criticality of the asset to your business infrastructure. From the picture in the slide, Cloud Agents with asset criticality of 4 and 5

will be prioritized.

Qualys Detection Score:
This is the score assigned to the respective Qualys detection, ranging from 1 to 100. It is derived from vulnerability technical, temporal, and remediation details which are discussed in the earlier slide content. The severity levels are:

- Critical = 90-100
- High = 70-89
- Medium = 40-69
- Low = 1-39

From the picture in the slide, Cloud Agents with Critical severity QDS score will be prioritized.

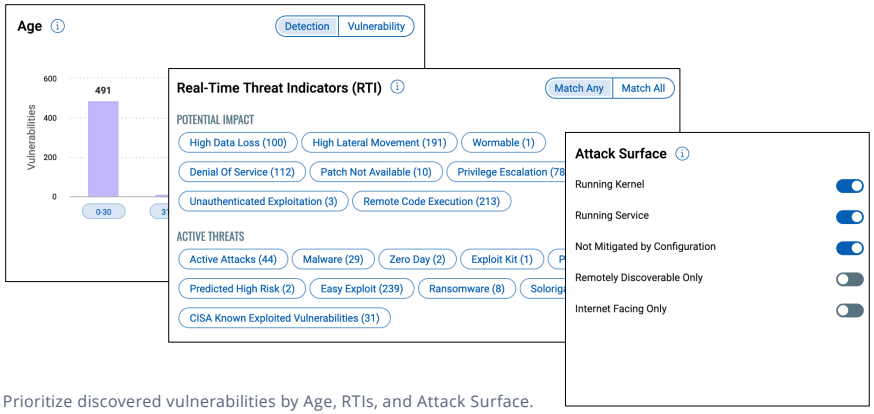
TruRisk Score:
TruRisk Score is the overall risk score assigned to an asset. It combines the Criticality Score of a single host with a weighted average of its combined vulnerability detections. While the Qualys Detection Score provides a useful metric for measuring the impact of a single vulnerability, the TruRisk Score places the vulnerability in the context of other vulnerabilities discovered on the same host.

It is dependent on:

- a. Asset Criticality Score (ACS)
- b. Qualys Detection Score (QID) for each severity level (Critical [C], High [H], Medium [M], Low [L])
- c. Auto assigned weighing factor (w) for each criticality level of QID

Tokens:
Qualys Detection Score (QDS) token = vulnerability.detectionScore
Asset Criticality Score (ACS) token = criticalityScore
TruRisk Score (ARS) token = riskScore

PRIORITY OPTIONS - TRADITIONAL METHOD

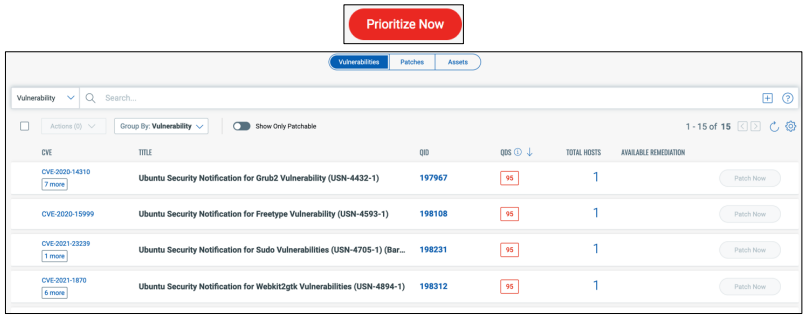


Prioritize discovered vulnerabilities by Age, RTIs, and Attack Surface.

Qualys.

We'll break-down the priority options by vulnerability age, Real-Time Threat Indicators and Attack Surface.

GENERATE PRIORITIZATION REPORT



Patchable assets have Cloud Agent installed and Patch Management activated.

Qualys.

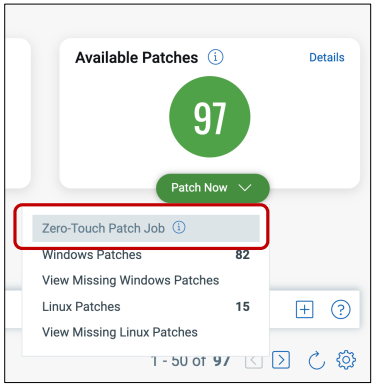
Once you establish your priority options, the last step is to click the Prioritize Now button to build your report.

By default, this report will produce a list of vulnerabilities that match your priority options. If you adjust any of the priority options, the report will be automatically updated.

You can also toggle the report view between Vulnerabilities, Patches, and Assets.

The Prioritization Report provides the option of patching vulnerabilities individually, or you can add all Available Patches to a new or existing patch job.

ZERO-TOUCH PATCH JOB - FROM PRIORITIZATION REPORT



- Select the "Zero-Touch Patch Job" option from the VMDR Prioritization Report.
- Patches are not selected individually, but instead are targeted using a query.
- Schedule patch jobs to recur daily, weekly, or monthly.
- Specific patching use-cases are ideal for "Zero-Touch" patching.

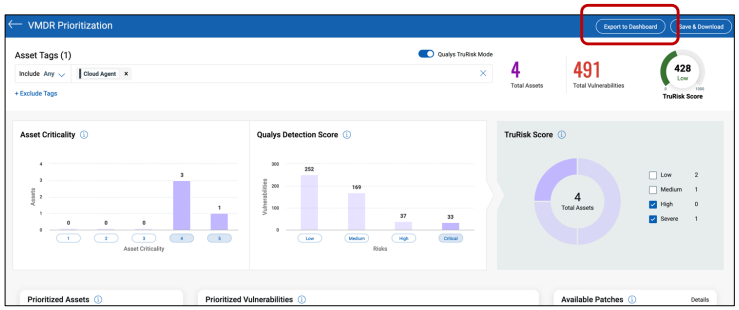
Qualys.

A "Zero-Touch Patch Job" combines two patching options:

1. Patches are selected using QQL
2. Job is scheduled to run daily, weekly, or monthly

EXPORT TO DASHBOARD

After building a Prioritization Report, simply click the "Export to Dashboard" button to build a Prioritization Report Widget and then add it to an existing Dashboard.

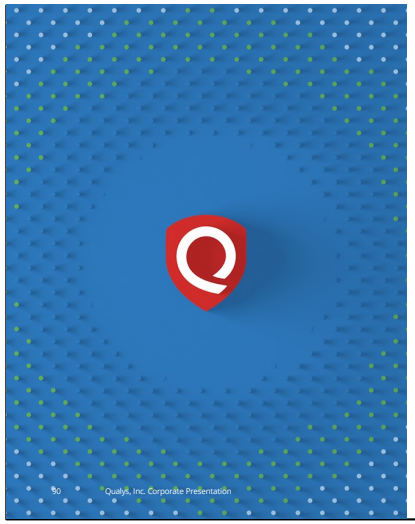


Qualys.

After building a Prioritization Report, simply click the "Export to Dashboard" button to build a Prioritization Report Widget and then add it to an existing Dashboard.

The resulting widget is dynamic, and it will be updated as conditions change.

Additionally, the report can be saved and downloaded as a CSV or PDF file format.



REPORTING:

REPORT TEMPLATES

Qualys.

The objectives for this section are to learn:

Qualys Authentication Report

Qualys Report Template Library

The difference between Scan-based and Host-based findings.

The components of a scan-based Reports.

REPORTING OPTIONS

Option	Vulnerability Details	Report Data Format
Dashboards	High Level	PDF
On-demand QQL Queries	High Level	CSV
VM Templates	High Level & Detailed	CSV, DOCX, HTML, MHT, PDF, XML
APIs (raw scan data)	Detailed	CSV, JSON*
Hybrid – VM Templates & APIs	High Level & Detailed	CSV, DOCX, HTML, MHT, PDF, XML
Third Party Integration (For example ServiceNow.)	High Level & Detailed	Varies depending on third party application
Prioritization Report	High Level & Detailed	PDF, and can export to dashboards

There are multiple ways to get data with Qualys – queries, widgets and dashboards, VM reports, and API. The table in this slide indicates the various options that can be used for reporting. Some of the factors that decide the choice of a particular option include accessibility by Qualys\non-Qualys users, interactivity, level of details that can be included in the report and report data format. Reporting using Dashboards, QQL queries and VM templates are covered in this course.

On-Demand QQL Queries are interactive in so far as you can refocus the view until you reach the format most meaningful to you.

VM Templates are Batch vs. Interactive.

*When using APIs for exporting data from your Qualys account note that not all API extracts support JSON. Please consult the API guides for specifics.
Please subscribe to the Qualys API Fundamentals Self-Paced Course for more information on using APIs for reporting.

Example Use-cases

Am I trying to get an answer to a quick one-time question?
Use queries

Am I trying to get in-depth technical vulnerability data for many hosts?
Use VM Reporting

Am I trying to export data?
Use API

Am I trying to get high-level data and trending data?
Use widgets and dashboards

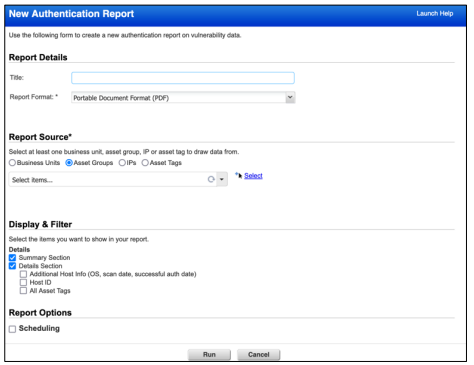
QUALYS AUTHENTICATION REPORT

The Authentication Report shows the authentication status for each scanned host:

- Passed
- Failed
- Passed with insufficient privileges
- Not Attempted

Run this report after an authenticated scan to verify that authentication was successful to the target hosts

Authentication Reports can also be scheduled.

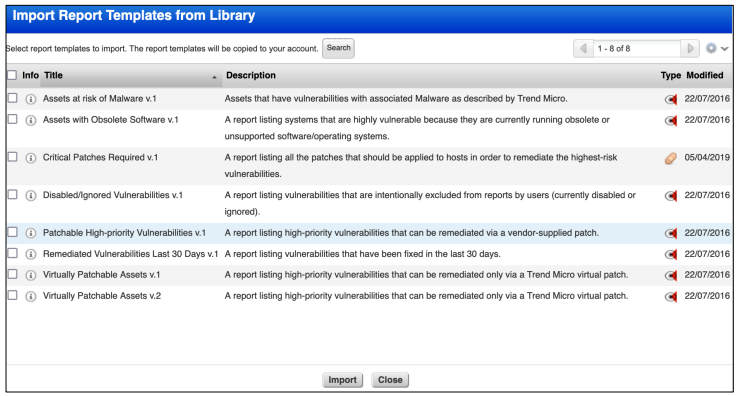


Qualys recommends performing scans in authenticated mode. However, the benefits gained from this practice, will not be seen, if the authentication attempted by your scanner appliance, fails or is obstructed in some other way.

The authentication report will help you to quickly identify authentication issues, with details that will help you to resolve the problem at hand.

https://qualys.secure.force.com/articles/Knowledge/000001087/p

REPORT TEMPLATE LIBRARY



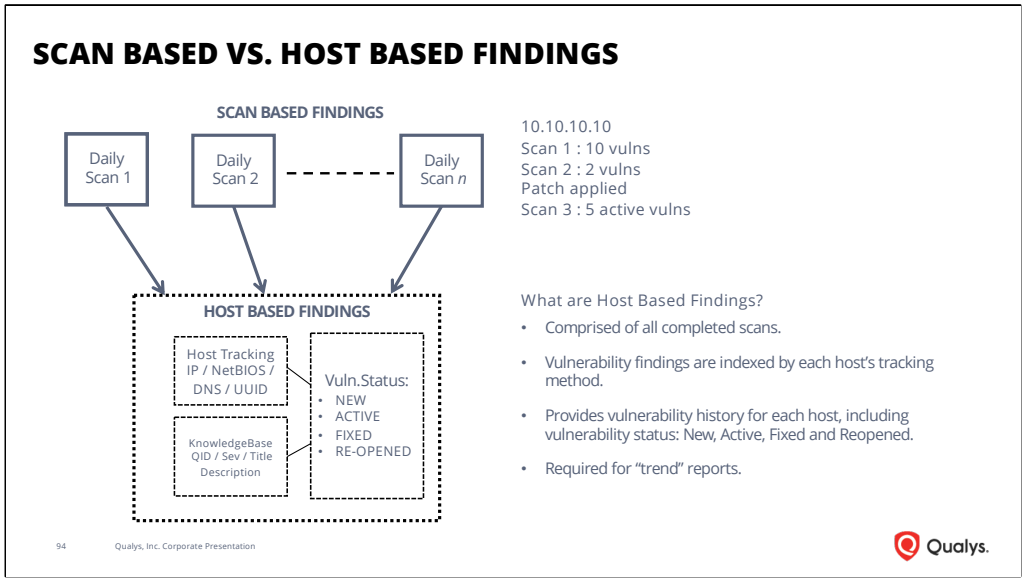
Qualys.

Report templates allow you to select from dozens of filtering and display options, which are then saved and used again and again to conveniently reproduce the same report behavior. Report templates can be customized for different target audiences within your organization. A report template simply takes the data and information from your RAW scan results and formats, filters, and displays this information in a way that is meaningful and useful to its target audience.

For example the Executive template will present vulnerability findings in a fashion that is more suitable for executive or managerial members of your organization, providing helpful graphics and summary statistics, but omitting the type of details that are more useful to patching and mitigation teams.

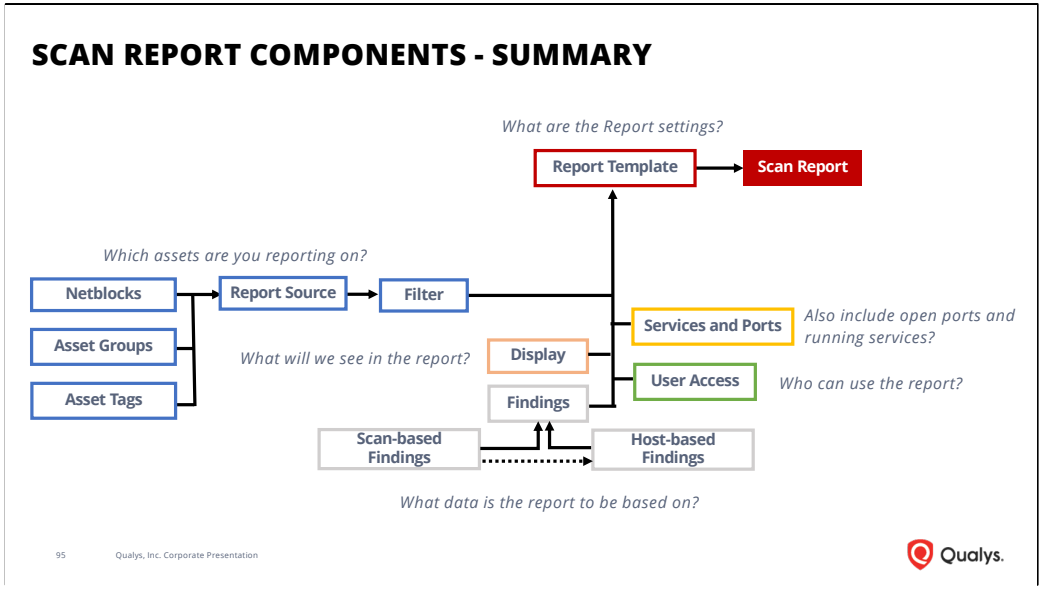
The Technical report template; on the other hand, is more suitable for members of your operational teams, because it focuses on the information and details needed to patch and mitigate detected vulnerabilities.

Under the Templates tab you'll find pre-built templates for many useful reporting tasks, and you can import more templates from the Template library.



The "scan-based" findings in your account are comprised of each individual vulnerability scan performed, where each scan tells a unique story based on its position or placement within your scanning timeline. Reports that use scan-based findings are often referred to as "snapshot" reports, because they represent an individual snapshot in time without any influence from scans that have been performed previously or scans that have occurred later in time. You'll find all of your scan-based findings listed under the Scans tab.

All scan based findings are poured into another bucket or database known as the host-based findings. The host-based findings database collects data from completed scans and indexes each detected vulnerability according to the "tracking method" you have selected for each host asset. Host-based findings will allow you to view the vulnerability history of any host asset, and
unlike scan-based findings; host-based findings allow you to create vulnerability "trend" reports that track the status of any vulnerability (from new, to active, fixed, or reopened) on any host.

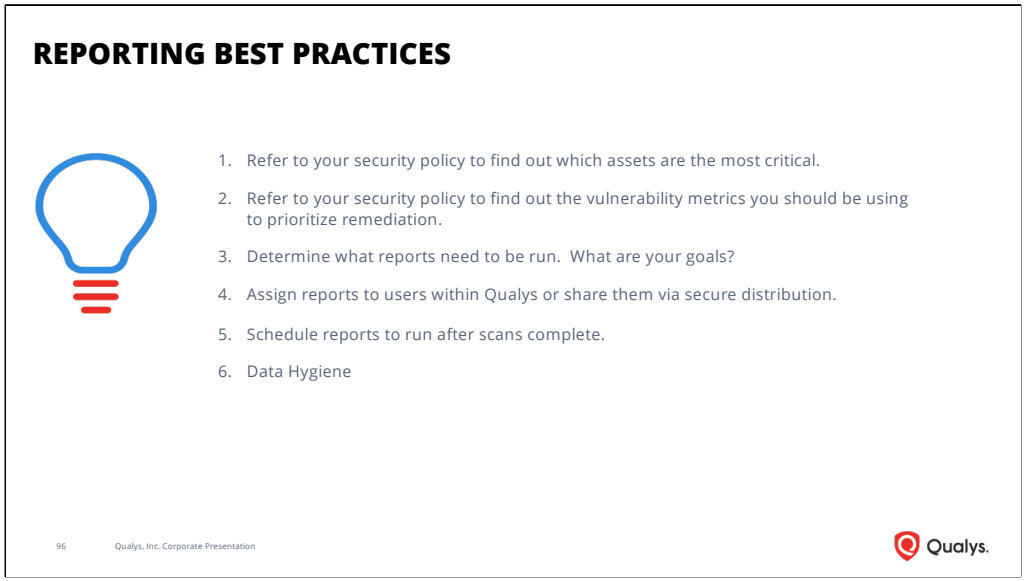


This diagram illustrates the basic components needed to build a report (scorecard reports, authentication reports and asset search reports, do not require a report template).

All report types require that you select a report source or the assets you intend to target in your report. You can accomplish this using a range of IP addresses or even a single IP, or any asset groups or asset tags you've created.

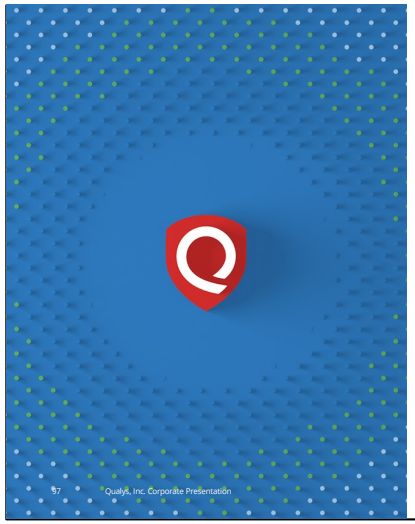
For the report types that require a report template, you can choose a custom template that you have created, or select one from the Qualys Report Template Library. A report template provides dozens of options for selecting the data and findings that will be included in your report, how that data will be displayed, and who will be able to view the reports that are generated.

Notice that a Qualys scanner appliance is not included in this diagram. Running a report does not in any way launch a scan. Scanning and reporting are separate tasks, and therefore scans must be completed, prior to building thier associated reports.



Reporting best practices include:

1. Refer to your security policy to find out which assets are the most critical.
2. Refer to your security policy to find out the vulnerability metrics you should b
3. Determine what reports need to be run. What are your goals?
4. Assign reports to users within Qualys or share them via secure distribution.
5. Schedule reports to run after scans complete.
6. Data Hygiene



REPORTING:

DASHBOARDS

Qualys.

The objective of this section is to learn:

Dashboards

Dashboard Templates

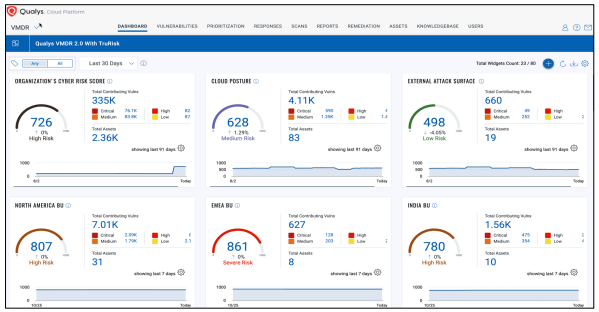
Count Widgets, including Trending, and formatting.

Risk Widgets

Dashboard Tags

DASHBOARDS

Using data visualization, dashboards visually communicate metrics to help users understand complex relationships in their data.



98 Qualys, Inc. Corporate Presentation Qualys.

Data dashboards collate, organize, and display important information from various data sources into one, easy-to-access place. A dashboard is an influential tool for information management and usage of business intelligence such as metrics and Key Performance Indicators (KPIs).

Using data visualization, dashboards visually communicate metrics to help users understand complex relationships in their data.

Dashboards help you visualize your assets. Each dashboard is a collection of widgets showing resource data of interest. You can add widgets with search queries and enhance the data visualization. You can create multiple dashboards and switch between them. You can also export and import Dashboard and Widget configurations, allowing you to share them between accounts or within the Qualys community.

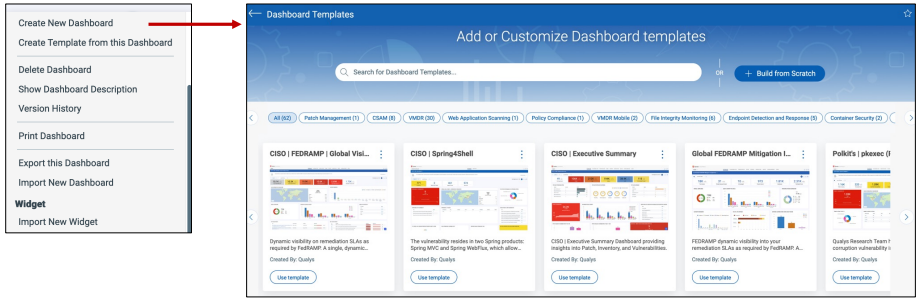
Visualize risk across your asset inventory and take actions for remediation.

This image above shows an example of a TruRisk dashboard from the Qualys demo account. You can see the overall organization's cyber risk

score, cloud posture, and external attack surface. Below the top row you see individual geos where the risk score widget is isolating to each continent via the location token.

CREATE A NEW DASHBOARD FROM A TEMPLATE

You can use the out-of-box Dashboard and Widget Templates or you can create your own custom Dashboards and Widgets.



Qualys.

Qualys VMDR comes with an extensive library of Dashboards and Widgets that allow you to monitor your assets, vulnerabilities and mitigation progress.

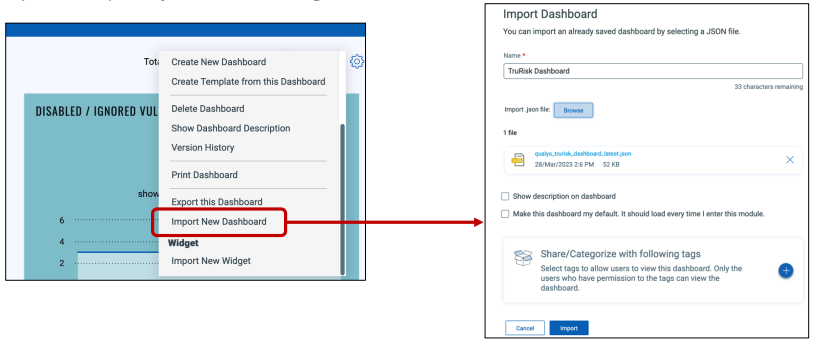
You can use the out-of-box Dashboard and Widget Templates or you can create your own custom Dashboards and Widgets.

You can even create Dashboard Widgets from the VMDR Prioritization reports you build.

When it comes time to invest in reporting, focus on the most important assets and vulnerabilities first. You will spend much time getting your dashboards and reports the way you want them, but remember the 80/20 rule and get going with the dashboards that will make the biggest impact first.

IMPORTING DASHBOARDS

You can export and import Dashboard and Widget configurations to a file in a JSON format allowing you to share them between accounts or within the Qualys community. The exported and imported dashboards or widgets are copies of the primary dashboard or widget.

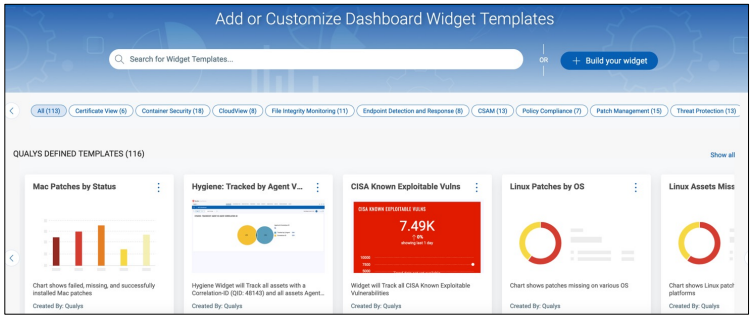


Qualys.

You can import and export Dashboard and Widget configurations to a file in a JSON format allowing you to share them between accounts or within the Qualys community. The imported and exported dashboards or widgets are copies of the primary dashboard or widget.

OUT-OF-BOX DASHBOARD TEMPLATES

We provide with ready to use templates for dashboards that you could quickly add to your list of dashboards and start monitoring your assets.

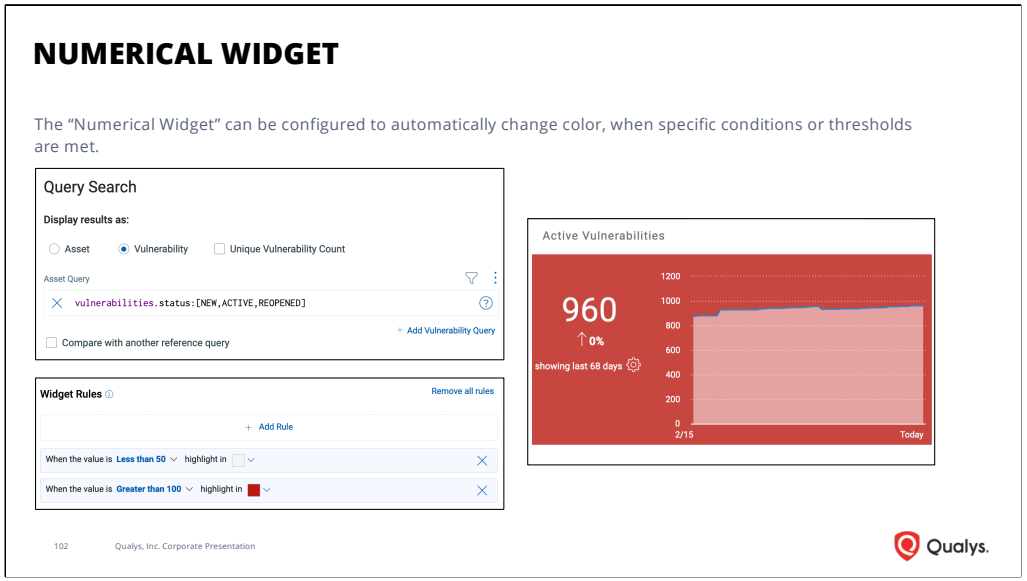


Qualys.

Qualys VMDR comes with an extensive library of Dashboards and Widgets that allow you to monitor your assets, vulnerabilities and mitigation progress.

You can use the out-of-box Dashboard and Widget Templates or you can create your own custom Dashboards and Widgets.

You can even create Dashboard Widgets from the VMDR Prioritization reports you build.



You can fetch data and display the count of mathematical operations in a numerical widget. You could also compare numbers with multiple queries. For example, you can view the count of malicious files, missing patches, or assets where patch installation is pending.

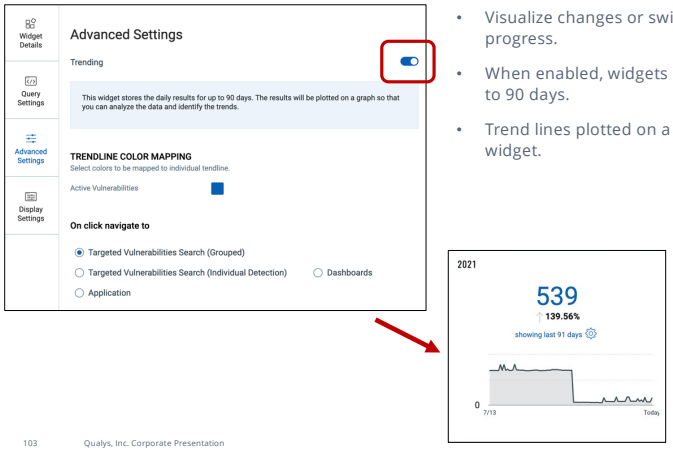
The Numerical widget can be designed to change color, when specific threshold conditions are met.

In this example we're comparing the result set of high severity vulnerabilities (in the initial query) to to the result set of all vulnerabilities (in this case all severity levels) in the reference query.

This comparison produces a percentage, which is then compared to a threshold level you configure, to change the widget color.

Note: if you do not include a reference query, ALL vulnerabilities will be used by default, as the reference query (demonstrated in the next lab tutorial).

ENABLE TRENDING IN WIDGETS



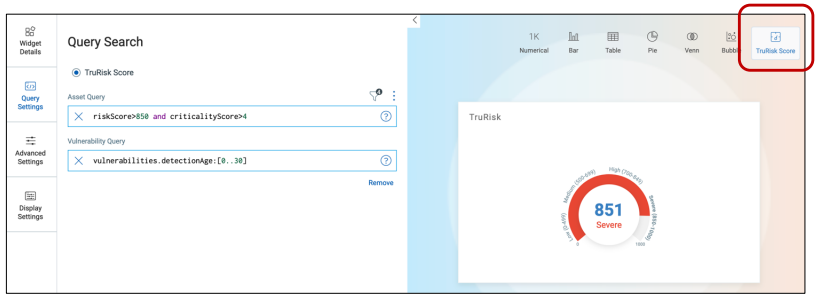
- Visualize changes or swings in momentum or progress.
- When enabled, widgets can store trend data for up to 90 days.
- Trend lines plotted on a graph are added to the widget.

Qualys.

You can configure dashboard Numerical widgets to display trend data. Enable the Collect trend data option in the dynamic widget wizard. Once enabled, the widget trend data is collected daily and stored for up to 90 days. This is used to plot a line graph in the numerical widget.

TRURISK WIDGET

The TruRisk Score widget type will show data based on the risk score of assets in your environment.



Qualys.

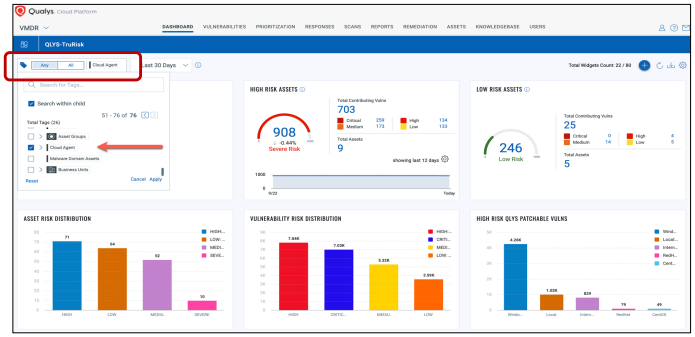
The TruRisk Score widget type will show data based on the risk score of assets in your environment.

You can recompute the risk score for a subset of assets within your environment by modifying the query score using tags.

In the Advanced Settings you can enable Trending. Enabling Contributing Factors includes the contributing vulnerabilities and total assets.

FILTER DASHBOARD DATA WITH TAGS

Dashboard visual data can be filtered based on tags.

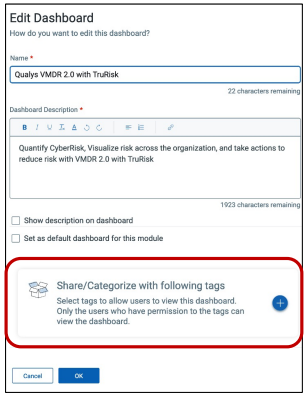


105 Qualys, Inc. Corporate Presentation Qualys.

Dashboard visual data can be filtered based on tags.

1. Click the Tag selector The tag tree displays recent and favorite tags and all tags in your account.
2. Select the tags from Recent & Favorites or All Tags. Using the Search Tags field, you can type the tag name and select the tag. Parent and Child tags are selected individually.
3. Selected tags are listed in the Selected Tags section.
4. To remove the selected tags click Reset and click Apply.

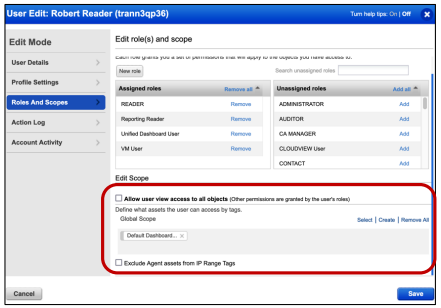
DASHBOARD TAGS



Add one or more Asset Tags through the Dashboard Editor.

The Default Dashboard Access Tag is created by Qualys.

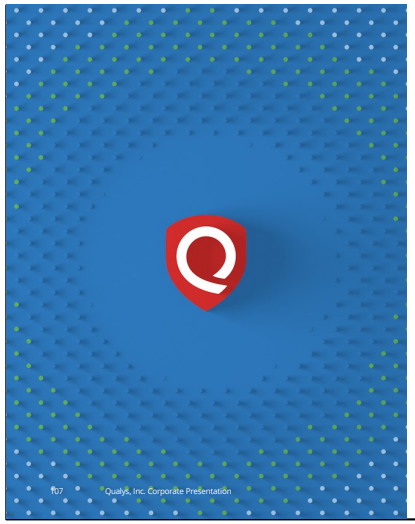
You can share dashboards with other Qualys users by assigning “dashboard” tag(s) to their accounts.



Qualys.

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

From the Administration Utility you can create custom roles to control which tagging permissions should be assigned to a user with that role. By default, a Manager user is assigned all the tagging permissions.



PATCHING VULNERABILITIES

Qualys.

The objective of this section is to learn:

The Patch Management workflow

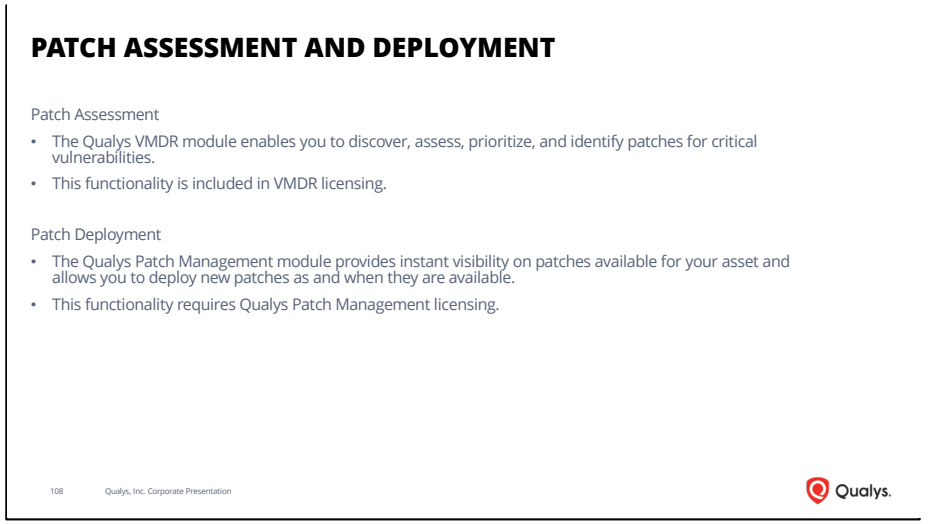
Patch Assessment Profiles

Patch Sources

Patch Catalog

Patch Supersedence

Prioritization Reports

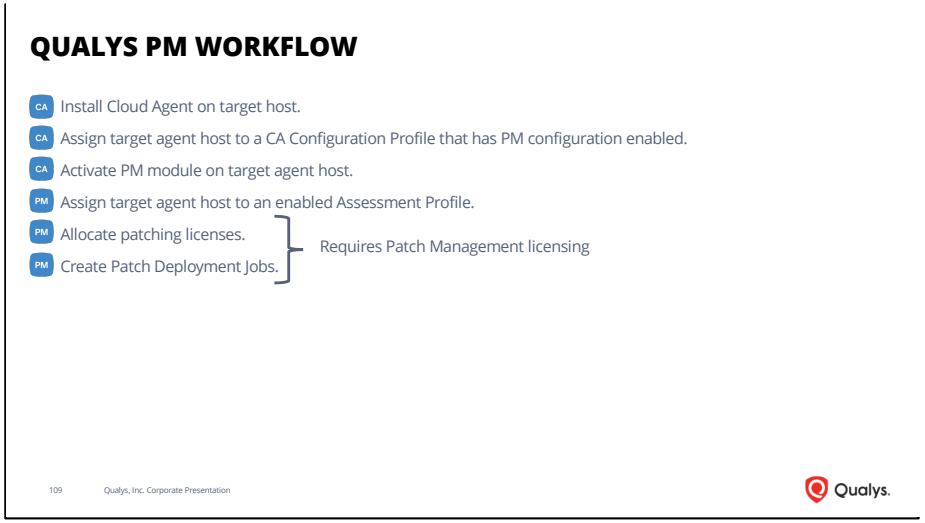


Patching is the process of remediating vulnerabilities. This process can be done with Qualys Patch Management or outside of Qualys using another tool. Over 2022, customers who used integrated patching in Qualys patched critical vulnerabilities 35% faster than those who did not use Patch Management.

Qualys Patch Management provides a comprehensive solution to manage vulnerabilities in your system and deploy patches to secure these vulnerabilities as well as keep your assets upgraded. The Qualys Vulnerability Management, Detection, and Response (VMDR) module enables you to discover, assess, prioritize, and identify patches for critical vulnerabilities.

The Patch Management module helps you save time and effort by automating patch management on Windows and Linux assets using a single patch
management application. It provides instant visibility on patches available for your asset and allows you to automatically deploy new patches as and when they are available.

The Windows Cloud Agent downloads the required patches from external sources. However, patches that require authentication cannot be downloaded by the agent. You can manually download and install such patches on the assets. Qualys Patch Management will then identify these patches as installed. The Linux Cloud Agent access the patches from the YUM repository and deploys the patches to the Linux assets in Patch Management.



Here is the list of steps, or workflow of events, that will allow Qualys PM to begin patch assessments and deployments on host assets:

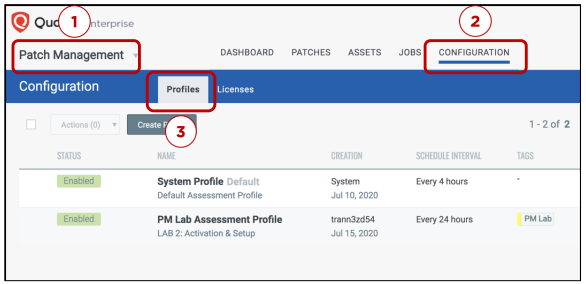
1. The first step is to install the Qualys agent on targeted host assets.
2. In step two, you'll then assign your targeted assets to a CA Configuration Profile that has PM enabled.
3. If you have not already activated the PM module, you'll perform this task in step 3. Notice that steps 1, 2, and 3 are all performed within the Cloud Agent application.
4. Step four is performed within the PM application. Here you'll assign target assets to an enabled PM Assessment Profile to perform patch assessment scans at regular intervals.
5. To perform the task of installing (or deploying) patches and perhaps even uninstalling patches, you'll need to build a patch job; step number five.
6. Step six is only needed if you decide (at a later time) to deactivate the PM module on an agent host; perhaps you would like reclaim its license and use it on another agent host.

Steps 2, 4, and 5 in this workflow can potentially precede step number

one, when Asset Tags are strategically used to assign host assets to their appropriate profiles and jobs.

Further information about Qualys Patch Management can be found in our video series:
https://www.qualys.com/training/library/patch-management/

PATCH ASSESSMENT PROFILE



Specifies frequency of patch assessment scans, which assess agent host assets for missing and/or installed patches.

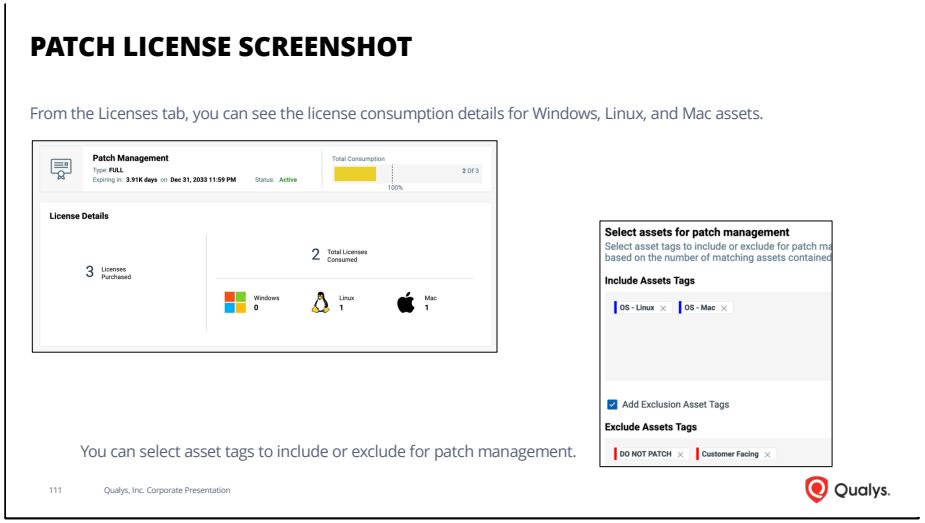
Patch Assessment is included in VMDR.

Qualys.

The Profiles tab displays a default assessment profile. Cloud Agents scan for patches (missing and installed) at a specific interval using the configuration defined in the default Assessment Profile.

When no custom assessment profile is defined, then the default assessment profile is applied to all agents, which scans the assets at an interval of 24 hours for free subscription and 4 hours for trial/paid subscription.

The profile tab Shows the assessment profile's status (enabled/disabled), name, date and time of creation, schedule (the scan interval). Asset tags show what asset tags are added to the assessment profiles.



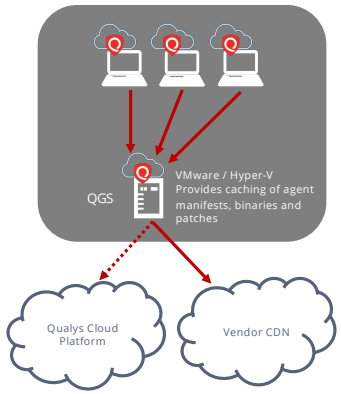
The Licenses tab, enabled only for paid subscribers, shows the number of licenses consumed by Patch Management (PM). You can include asset tags to allow patch installing and rolling back on the assets contained in those asset tags. The Total Consumption counter may exceed 100% if the number of assets activated for PM are more than the number of PM licenses you have.

Assets in the excluded asset tags are not considered for patch management and you cannot deploy patches on those assets

PATCH SOURCES

OS and Application Patches come from:

- Vendor Global CDNs (e.g., Oracle, Adobe, Microsoft, Apache, Google, etc...)
  - Qualys uses both digital signatures and hash values to validate downloaded patches, which are validated again, via Qualys Malware Insights.
- Local repository (i.e., Qualys Gateway Server)
  - Patch downloads requested by one agent, are cached on QGS and made available "locally" for other agents that need the same patch.



Qualys.

Agent host assets receive their patches from Vendor Global Content Distribution Networks (CDNs). Host assets will receive their patches directly from the vendors that created the patches; this includes both OS and application patches.

Qualys uses digital signatures and hash values to validate downloaded patches, which are validated again using Qualys Malware Insights.

Qualys Gateway Server
Qualys Gateway Server (QGS) provides the advantage of caching downloaded patches; patch downloads requested by one agent, are cached on QGS and made available locally for other agents that need the same patch.

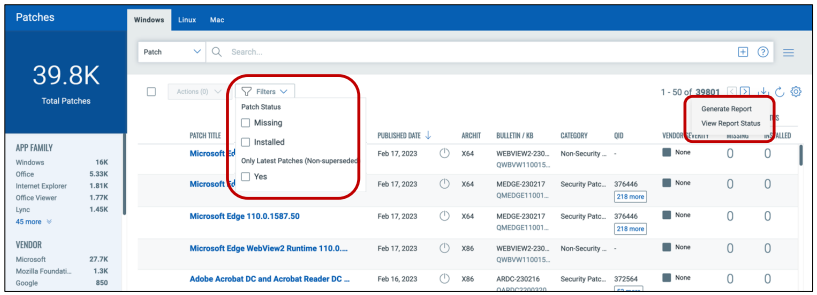
This will save Internet download bandwidth from the Qualys cloud platform to the on-premise network as only one copy of unique files will be downloaded. For environments will large number of Cloud Agents deployed, this can save a significant amount of download bandwidth.

Further information about Qualys Gateway Server:

https://www.qualys.com/docs/qualys-gateway-service-user-guide.pdf
If you are using the Qualys Gateway Server as a proxy for your Cloud Agents, this can help you configure it.

https://www.qualys.com/training/library/qgs-training/
Use this video series to understand what it does and how to configure it correctly.

PATCH CATALOG



113 Qualys, Inc. Corporate Presentation

Qualys.

The patches listed in the Patch Management patch catalog are the ones missing on your hosts which were detected using the Patch Management scan.
Patches tab lists two types of patches:

Qualys Patchable - Qualys Patchable are the patches that can be installed using Patch Management. Most of the patches listed on the Patches tab are Qualys Patchable.

AcquireFromVendor - We have certain patches which are listed under the Patches tab but cannot be installed using Patch Management. These patches are marked as "AcquireFromVendor" which means you need to manually download these patches from the vendor website and install them on the host.

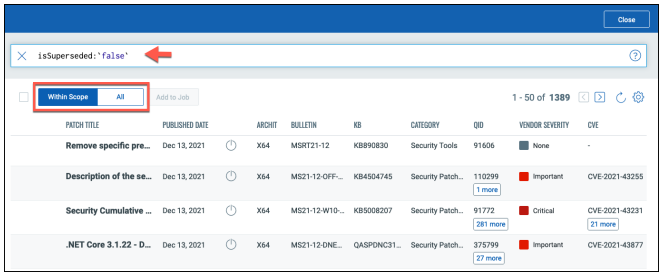
Patches which are not marked as "AcquireFromVendor" are defined as "Qualys Patchable" which mean they can be added to a patch job.

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.

PATCH SUPERSEDENCE



- Build more efficient patch jobs by targeting patches that have not been superseded.
- By default, the “Patch Selector” displays patches that are “Within Scope” of the host asset(s) your job is targeting.

Qualys.

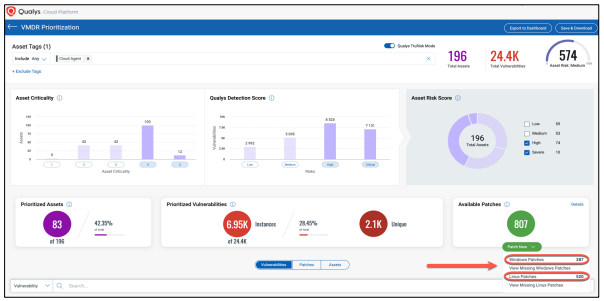
Along with search tokens, you can use filters to find missing/installed patches or non-superseded latest missing patches for Windows and Mac assets.

The filters are available in tabs as well as dashboard widgets. To improve efficiency, you can use the search field to focus on patches that have NOT been superseded (isSuperseded: false), which can significantly reduce the total number of patches to be installed.

By default, the Patch Selector only lists patches that are "Within Scope" of the host assets that are targeted.

DEPLOY PATCHES USING TRURISK PRIORITIZATION

Reduce remediation time by deploying the patches from the same platform in an integrated workflow, at the click of a button.



Qualys.

An example of deploying patches from VMDR is by using the TruRisk Prioritization Report. After clicking Prioritize Now to build the Prioritization Report, you will have the option to deploy patches.

This feature can reduce remediation time by deploying the patches from the same platform in an integrated workflow, at the click of a button.

Thank you for attending this class! We hope you found it useful!